

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

5 mars 2024

PROJET DE LOI

établissant un cadre
pour la cybersécurité des réseaux et
des systèmes d'information d'intérêt général
pour la sécurité publique

Sommaire	Pages
Résumé	3
Exposé des motifs.....	4
Avant-projet de loi	81
Avant-projet de loi - annexes	148
Avis du Conseil d'État	161
Projet de loi	177
Projet de loi - annexes	264
Tableau de correspondance projet de loi - directive.....	284
Tableau de correspondance directive - projet de loi.....	304
Coordination des articles	316
Avis de l'Autorité de protection des données.....	515

CONFORMÉMENT À L'ARTICLE 8, § 2, 1°, DE LA LOI DU 15 DÉCEMBRE 2013,
L'ANALYSE D'IMPACT N'A PAS ÉTÉ DEMANDÉE.

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

5 maart 2024

WETSONTWERP

tot vaststelling van een kader
voor de cyberbeveiliging van netwerk- en
informatiesystemen van algemeen belang
voor de openbare veiligheid

Inhoud	Blz.
Samenvatting	3
Memorie van toelichting	4
Voorontwerp van wet.....	81
Voorontwerp van wet - bijlagen.....	154
Advies van de Raad van State.....	161
Wetsontwerp	177
Wetsontwerp - bijlagen	274
Concordantietabel wetsontwerp - Richtlijn	284
Concordantietabel Richtlijn - wetsontwerp	304
Coördinatie van de artikelen	414
Advies van de Gegevensbeschermingsautoriteit	521

OVEREENKOMSTIG ARTIKEL 8, § 2, 1°, VAN DE WET VAN 15 DECEMBER 2013
WERD DE IMPACTANALYSE NIET GEVRAAGD.

Le gouvernement a déposé ce projet de loi le 5 mars 2024.

Le “bon à tirer” a été reçu à la Chambre le 12 mars 2024.

De regering heeft dit wetsontwerp op 5 maart 2024 ingediend.

De “goedkeuring tot drukken” werd op 12 maart 2024 door de Kamer ontvangen.

N-VA	: Nieuw-Vlaamse Alliantie
Écolo-Groen	: Ecologistes Confédérés pour l'organisation de luttes originales – Groen
PS	: Parti Socialiste
VB	: Vlaams Belang
MR	: Mouvement Réformateur
cd&v	: Christen-Democratisch en Vlaams
PVDA-PTB	: Partij van de Arbeid van België – Parti du Travail de Belgique
Open Vld	: Open Vlaamse liberalen en democraten
Vooruit	: Vooruit
Les Engagés	: Les Engagés
DéFI	: Démocrate Fédéraliste Indépendant
INDEP-ONAFH	: Indépendant – Onafhankelijk

Abréviations dans la numérotation des publications:		Afkorting bij de nummering van de publicaties:	
DOC 55 0000/000	Document de la 55 ^e législature, suivi du numéro de base et numéro de suivi	DOC 55 0000/000	Parlementair document van de 55 ^e zittingsperiode + basisnummer en volgnummer
QRVA	Questions et Réponses écrites	QRVA	Schriftelijke Vragen en Antwoorden
CRIV	Version provisoire du Compte Rendu Intégral	CRIV	Voorlopige versie van het Integraal Verslag
CRABV	Compte Rendu Analytique	CRABV	Beknopt Verslag
CRIV	Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)	CRIV	Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)
PLEN	Séance plénière	PLEN	Plenum
COM	Réunion de commission	COM	Commissievergadering
MOT	Motions déposées en conclusion d'interpellations (papier beige)	MOT	Moties tot besluit van interpellaties (beigegekleurig papier)

RÉSUMÉ

Ce projet de loi vise à transposer la directive (UE) 2022/2555 du Parlement Européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148, dénommée ci-après la "directive NIS2".

La directive NIS2 remplace la directive (UE) 2016/1148 du Parlement Européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, laquelle a été transposée en Belgique par la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

Les réseaux et les systèmes d'information sont devenus des éléments centraux de notre société. Cependant, le nombre, l'ampleur, la sophistication, la fréquence et l'impact des incidents de ces réseaux et systèmes représentent désormais des menaces considérables pour la population, les entreprises et les autorités publiques.

À l'instar de la directive, l'objectif de la loi est de renforcer les mesures de cybersécurité, de gestion des incidents et de supervision des entités fournissant des services essentiels au maintien d'activités sociales ou économiques critiques. Elle vise également à améliorer la coordination des politiques publiques en matière de cybersécurité.

Ainsi, les dispositions de la présente loi visent à protéger, au titre de la sécurité publique, la population, les entreprises et les autorités publiques contre les cybermenaces.

SAMENVATTING

Dit wetsontwerp beoogt de omzetting van de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148, hierna "NIS2-richtlijn" genoemd.

De NIS2-richtlijn vervangt Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, die in België werd omgezet door de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

Netwerk- en informatiesystemen hebben zich ontwikkeld tot centrale elementen van onze samenleving. Het aantal, de omvang, de complexiteit, de frequentie en de impact van incidenten met betrekking tot deze netwerk- en informatiesystemen vormen nu een aanzienlijke bedreigingen voor de bevolking, de bedrijven en de overheden.

Net zoals de richtlijn, is het doel van de wet het versterken van maatregelen op het gebied van cyberbeveiliging, de behandeling van incidenten en het toezicht van entiteiten die essentiële diensten verlenen voor het in stand houden van kritieke sociale of economische activiteiten. Daarnaast doelt ze ook op het verbeteren van de coördinatie van overheidsbeleid op het gebied van cybersecurity.

De bepalingen van de huidige wet zijn, als onderdeel van de openbare veiligheid, bedoeld om de bevolking, de bedrijven en de overheden te beschermen tegen cyberdreigingen.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

EXPOSÉ GÉNÉRAL

Ce projet de loi vise à transposer la directive (UE) 2022/2555 du Parlement Européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148, dénommée ci-après la "directive NIS2".

La directive NIS2 remplace la directive (UE) 2016/1148 du Parlement Européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, ci-après la "directive NIS1", laquelle a été transposée en Belgique par la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (ci-après, la "loi NIS1").

La directive NIS2 fixe, d'une part, des obligations en ce qui concerne les politiques nationales en matière de cybersécurité et, d'autre part, impose pour certaines entités des exigences en matière de gestion des risques de cybersécurité et de notification des incidents.

En ce qui concerne les politiques nationales, il s'agit notamment de la stratégie nationale en matière de cybersécurité, des cadres nationaux de gestion des crises cyber, des tâches des autorités compétentes et de la coopération nationale.

Au sens de la directive, la cybersécurité est définie comme "les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces".

Les réseaux et systèmes d'information sont devenus des caractéristiques essentielles de notre vie quotidienne en raison de la transformation numérique rapide et de l'interconnexion de la société.

Cette évolution a conduit à une expansion du paysage des cybermenaces et à l'émergence de nouveaux défis, qui nécessitent des réponses adaptées, coordonnées et novatrices.

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

ALGEMENE TOELICHTING

Dit wetsontwerp voorziet in de omzetting van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148, hierna "NIS2-richtlijn" genoemd.

De NIS2-richtlijn vervangt Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, hierna "NIS1-richtlijn" genoemd, die in België werd omgezet door de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (hierna "NIS1-wet" genoemd).

De NIS2-richtlijn stelt enerzijds verplichtingen vast wat betreft het nationaal cyberbeveiligingsbeleid, en legt anderzijds bepaalde entiteiten eisen op met betrekking tot het beheer van cyberbeveiligingsrisico's en de melding van incidenten.

Wat het nationaal beleid betreft, gaat het met name om de nationale cyberbeveiligingsstrategie, nationale kaders voor cybercrisisbeheer, de taken van de bevoegde autoriteiten en de nationale samenwerking.

In de zin van de richtlijn wordt cyberbeveiliging gedefinieerd als "de activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers van dergelijke systemen, en andere personen die getroffen worden door cyberdreigingen, te beschermen".

Netwerk- en informatiesystemen hebben zich ontwikkeld tot een centraal kenmerk van ons dagelijks leven door de snelle digitale transformatie en de onderlinge verbondenheid van de samenleving.

Die ontwikkeling heeft geleid tot een uitbreiding van het cyberdreigingslandschap, wat nieuwe uitdagingen met zich meebrengt, die een aangepaste, gecoördineerde en innovatieve respons vereisen.

Le champ d'application de la directive NIS2 porte sur les règles de cybersécurité limitées à certaines entités (fournissant des services essentiels au maintien d'activités sociétales ou économiques critiques), dont la protection relève en droit interne des compétences résiduelles fédérales en matière de sécurité publique. La directive NIS2 détermine, en effet, des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne pour certaines entités qualifiées comme "essentiels" ou "importantes", en raison des services qu'elles fournissent et de leur taille. Les entités concernées sont celles fournissant des services essentiels énumérés dans les "secteurs hautement critiques" de l'annexe 1 ou dans les "autres secteurs critiques" de l'annexe 2, qui constituent des entreprises moyennes en vertu de l'article 2 de l'annexe de la recommandation 2003/361/CE, ou qui dépassent les plafonds prévus au paragraphe 1 dudit article, et qui fournissent leurs services ou exercent leurs activités au sein de l'Union.

En application de la directive et de la recommandation 2003/361/CE, les "entités essentielles" sont les organisations qui fournissent un service repris dans l'annexe I et qui répondent à la notion de "grande entreprise", c'est-à-dire qui occupe min. 250 personnes ou dont le chiffre d'affaires annuel excède 50 millions d'euros (ou le total du bilan annuel excède 43 millions d'euros). Les "entités importantes" sont les organisations qui fournissent un service repris dans l'annexe I et qui répondent à la notion de "moyenne entreprise", c'est-à-dire qui occupe min. 50 personnes ou réalise un chiffre d'affaires annuel (ou le total du bilan annuel) qui excède 10 millions d'euros. Sont également des "entités importantes" les organisations qui fournissent un service repris dans l'annexe II et qui répondent aux notions de moyenne ou de grande entreprise.

L'article 6, 3) de la directive NIS2 définit la cybersécurité comme "les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces". L'article 6, 10) de la directive NIS2 détermine la notion de la cybermenace comme "toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes".

Au sens de la directive NIS2, la cybersécurité vise la protection contre des cybermenaces à la fois des réseaux et des systèmes d'information des entités qui offrent ou rendent accessibles des services essentiels mais aussi la protection des utilisateurs (personnes physiques ou morales) de ces services. Les mesures

Het toepassingsgebied van de NIS2-richtlijn heeft betrekking op cyberbeveiligingsregels die beperkt zijn tot bepaalde entiteiten (die diensten verlenen die essentieel zijn voor de instandhouding van kritieke maatschappelijke of economische activiteiten), waarvan de bescherming in nationaal recht onder de federale restbevoegdheden inzake openbare veiligheid valt. De NIS2-richtlijn stelt immers maatregelen vast voor een hoog gezamenlijk niveau van cyberbeveiliging in de Europese Unie voor bepaalde entiteiten die als "essentieel" of "belangrijk" worden aangemerkt vanwege de diensten die zij verlenen en hun omvang. Het gaat om entiteiten die essentiële diensten verlenen die vermeld zijn bij de "zeer kritieke sectoren" van bijlage 1 of bij de "andere kritieke sectoren" van bijlage 2, die in aanmerking komen als middelgrote ondernemingen uit hoofde van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG, of de in lid 1 van dat artikel vastgestelde plafonds voor middelgrote ondernemingen overschrijden, en die hun diensten verlenen of hun activiteiten verrichten in de Unie.

Overeenkomstig de richtlijn en Aanbeveling 2003/361/EG zijn "essentiële entiteiten" organisaties die een in bijlage I vermelde dienst verlenen en voldoen aan de definitie van "grote onderneming", d.w.z. een onderneming waar minstens 250 personen werkzaam zijn of waarvan de jaaromzet meer dan 50 miljoen euro bedraagt (of waarvan het jaarlijkse balanstotaal meer dan 43 miljoen euro bedraagt). "Belangrijke entiteiten" zijn organisaties die een in bijlage I vermelde dienst verlenen en voldoen aan de definitie van middelgrote onderneming, d.w.z. een onderneming waar minstens 50 personen werkzaam zijn of waarvan de jaaromzet (of het jaarlijkse balanstotaal) meer dan 10 miljoen euro bedraagt. Ook organisaties die een in bijlage II vermelde dienst verlenen en voldoen aan de definitie van middelgrote of grote onderneming zijn "belangrijke entiteiten".

Artikel 6, 3), van de NIS2-richtlijn definieert cyberbeveiliging als "de activiteiten die nodig zijn om netwerken en informatiesystemen, de gebruikers van dergelijke systemen, en andere personen die getroffen worden door cyberdreigingen, te beschermen". Artikel 6, 10), van de NIS2-richtlijn definieert het begrip "cyberdreiging" als "elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden".

Zoals vermeld in de NIS2-richtlijn heeft cyberbeveiliging tot doel om niet alleen netwerk- en informatiesystemen van entiteiten die essentiële diensten aanbieden of toegankelijk maken, maar ook de gebruikers (natuurlijke of rechtspersonen) van deze diensten te beschermen tegen cyberdreigingen. De maatregelen hebben dan ook tot

visent ainsi à protéger la population et les entreprises de manière générale en Belgique.

À plusieurs reprises, les considérants de la directive mettent en avant l'importance que revêt la protection des réseaux et systèmes d'information, face à l'augmentation des cybermenaces et des incidents pouvant causer des perturbations sociétales ou économiques majeures.

La cybersécurité constitue ainsi une matière propre, avec des règles générales communes et cohérentes applicables à tous les réseaux et systèmes d'information, indépendamment du domaine d'activités dans lesquels ceux-ci sont utilisés. En effet, il existe des menaces communes (indisponibilité, modification, vol ou perte des données, non-respect de la confidentialité ou de l'authenticité, etc.) à tous les réseaux et systèmes d'information. Il existe ainsi des normes techniques internationales en matière de sécurité de l'information générales et transversales à tous les secteurs (par exemple, les normes de la famille ISO/IEC 27.000, les *Center for Internet Security (CIS) Controls* ou encore le *National Institute of Standards and Technology (NIST) Cybersecurity framework*).

Le nombre, l'ampleur, la sophistication, la fréquence et l'impact des cyberincidents ne cessent de croître et représentent une menace considérable pour le bon fonctionnement de certaines activités sociétales ou économiques critiques ou encore des services publics.

Dans le prolongement de la directive NIS1, les entités concernées par la directive NIS2 ne sont pas toutes les organisations établies en Belgique mais bien celles fournissant des services essentiels au maintien d'activités sociétales ou économiques critiques en Belgique, spécifiées dans les annexes de la directive "secteurs hautement critiques" (annexe 1) ou "autres secteurs critiques" (annexe 2).

Là où la directive NIS1 prévoyait une procédure nationale d'identification des opérateurs de services essentiels, la directive NIS2 utilise désormais l'activité exercée au sein de l'une de ses annexes et la taille de l'entité comme critères pour déterminer si celle-ci entre ou non dans le champ d'application.

L'objectif demeure néanmoins toujours de protéger les entités fournissant un service essentiel au maintien d'activités sociétales ou économiques critiques dans des domaines tels que l'énergie, le transport, la santé, l'eau potable, les infrastructures numériques, l'espace, les fournisseurs de services de technologie de l'information et de la communication ou encore l'administration publique. Indépendamment de la taille de l'organisation, l'article 2 de la directive prévoit d'ailleurs que les États

doel om de bevolking en het bedrijfsleven in België op algemene wijze te beschermen.

In de overwegingen van de richtlijn wordt herhaaldelijk gewezen op het belang van de bescherming van netwerk- en informatiesystemen in het licht van de toenemende cyberdreigingen en incidenten die de samenleving of de economie ernstig kunnen verstoren.

Cyberbeveiliging is dus een specifieke aangelegenheid, met gemeenschappelijke en coherente algemene regels die van toepassing zijn op alle netwerk- en informatiesystemen, ongeacht het werkterrein waarin deze worden gebruikt. Er zijn immers dreigingen (onbeschikbaarheid, wijziging, diefstal of verlies van gegevens, niet-naleving van de vertrouwelijkheid of authenticiteit, enz.) die gelden voor alle netwerk- en informatiesystemen. Zo bestaan er algemene, sectoroverschrijdende internationale technische normen voor informatiebeveiliging (bijvoorbeeld, de ISO/IEC 27.000 normenreeks, de *Center for Internet Security (CIS) Controls of het National Institute of Standards and Technology (NIST) Cybersecurity framework*).

Het aantal, de omvang, de complexiteit, de frequentie en de impact van cyberincidenten nemen toe en vormen een grote bedreiging voor de goede werking van sommige kritieke maatschappelijke of economische activiteiten of van openbare diensten.

In het verlengde van de NIS1-richtlijn omvatten de entiteiten die onder de NIS2-richtlijn vallen niet alle in België gevestigde organisaties, maar wel degene die diensten verlenen die essentieel zijn voor de instandhouding van kritieke maatschappelijke of economische activiteiten in België, zoals gespecificeerd in de bijlagen bij de richtlijn "zeer kritieke sectoren" (bijlage 1) of "andere kritieke sectoren" (bijlage 2).

Terwijl de NIS1-richtlijn voorzag in een nationale procedure voor de identificatie van aanbieders van essentiële diensten, gebruikt de NIS2-richtlijn de activiteit die wordt uitgevoerd binnen een van de bijlagen ervan en de omvang van de entiteit als criteria om te bepalen of deze al dan niet onder het toepassingsgebied valt.

Niettemin is het doel nog steeds om entiteiten te beschermen die een dienst verlenen die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten op gebieden zoals energie, vervoer, gezondheid, drinkwater, digitale infrastructuur, ruimtevaart, aanbieders van informatie- en communicatietechnologie of het overheidsbestuur. Ongeacht de omvang van de organisatie, bepaalt artikel 2 van de richtlijn lidstaten ook om bepaalde entiteiten op nationaal

membres doivent inclure également au niveau national certaines entités en raison du caractère critique du service essentiel fourni, du risque systémique important ou encore de l'impact important sur la sécurité publique.

En ce qui concerne les mesures de gestion des risques en matière de cybersécurité, les entités concernées devront notamment assurer la prise de mesures adaptées aux risques encourus, en tenant compte du degré d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité de survenance d'incidents et de leur gravité, au regard des éventuelles conséquences sociétales et économiques.

La directive prévoit la notification aux autorités compétentes des incidents significatifs afin d'atténuer leur propagation potentielle, de permettre aux entités de chercher de l'aide, de gérer au mieux les situations de crises et de partager les informations techniques pertinentes avec les autres entités.

Comme exposé ci-avant, des obligations de la directive NIS2 ne s'appliquent qu'à un nombre limité d'entités faisant partie de secteurs critiques et fournissant des services d'intérêt général pour la population et les entreprises, ou critiques pour le potentiel économique du pays.

Le contenu de la directive ne règle pas la matière de la cybersécurité dans un domaine spécifique mais impose la prise de mesures minimales destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union pour certaines entités fournissant des services essentiels.

Un cyberincident est, en effet, susceptible de provoquer des perturbations opérationnelles graves de ces services essentiels et d'affecter des personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

Un incident, peut, par exemple, avoir pour conséquence de rendre inopérante la distribution d'électricité ou de rendre indisponibles des services de transport. En ce qu'ils affectent des acteurs essentiels de secteurs clés, en ce compris les pouvoirs publics, ces incidents constituent des menaces graves pour la sécurité publique. Les obligations de la directive relèvent dès lors en droit belge du domaine de la sécurité publique.

Outre les considérants, le contenu des dispositions de la directive NIS2 démontre à suffisance que la matière concrète traitée par celle-ci est bien la sécurité des citoyens (utilisateurs des services concernés), des entreprises, des biens et des autorités publiques contre

niveau op te nemen vanwege de kritieke aard van de verleende essentiële dienst, het aanzienlijke systeemrisico of de aanzienlijke gevolgen voor de openbare veiligheid.

Wat betreft de maatregelen voor het beheer van cyberbeveiligingsrisico's moeten de betrokken entiteiten er met name voor zorgen dat maatregelen worden genomen die zijn afgestemd op de risico's, waarbij rekening wordt gehouden met de mate waarin de entiteit aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, in het licht van de mogelijke maatschappelijke en economische gevolgen.

De richtlijn voorziet in de melding van significante incidenten aan de bevoegde autoriteiten om de potentiële verspreiding ervan te beperken, entiteiten in staat te stellen bijstand te vragen, crisissituaties zo goed mogelijk te beheer en relevante technische informatie met andere entiteiten te delen.

Zoals hierboven uiteengezet, zijn de verplichtingen van de NIS2-richtlijn alleen van toepassing op een beperkt aantal entiteiten die deel uitmaken van kritieke sectoren en diensten van algemeen belang verlenen voor de bevolking en ondernemingen, of kritiek zijn voor het economisch potentieel van ons land.

De inhoud van de richtlijn regelt de aangelegenheid cyberbeveiliging niet op een specifiek gebied, maar legt minimummaatregelen op voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie voor bepaalde entiteiten die essentiële diensten leveren.

Een cyberincident kan immers een ernstige operationele verstoring van deze essentiële diensten veroorzaken en natuurlijke personen of rechtspersonen treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

Een incident kan er bijvoorbeeld toe leiden dat de elektriciteitsdistributie buiten werking wordt gesteld of vervoersdiensten niet meer beschikbaar zijn. Aangezien deze incidenten essentiële spelers in sleutelsectoren, waaronder overheden, treffen, vormen ze een ernstige bedreiging voor de openbare veiligheid. Bijgevolg vallen de verplichtingen van de richtlijn in Belgisch recht onder de openbare veiligheid.

Naast de overwegingen toont de inhoud van de bepalingen van de NIS2-richtlijn voldoende aan dat de concrete aangelegenheid die hier wordt behandeld, inderdaad de beveiliging van burgers (gebruikers van de betrokken diensten), ondernemingen, goederen

les cybermenaces et les cyberincidents. En effet, la défaillance ou la compromission des réseaux et systèmes d'information de certaines entités jugées nécessaires au maintien de diverses fonctions centrales pour la vie de la Nation (car elles fournissent des services essentiels au maintien d'activités sociétales ou économiques critiques) peut avoir des conséquences importantes pour la société et l'économie. La cybersécurité des "entités essentielles" ou "entités importantes" NIS2 relève dès lors clairement de la protection exercée dans le domaine général de la sécurité publique (la protection des personnes physiques, des personnes morales et des biens).

Par ailleurs, la directive NIS2 ne détermine pas des règles de cybersécurité applicables à toutes les organisations actives dans un domaine particulier. Elle fixe des mesures minimales communes de gestion des risques en matière de cybersécurité et de notification des incidents importants (ou des cybermenaces importantes) à toutes les entités essentielles et importantes, sans distinction entre et uniquement pour les secteurs d'activités mentionnés dans les annexes de la loi.

La nature générale (transsectorielle) et commune, au sein des secteurs repris dans les annexes de la loi, des mesures envisagées par la directive (visant à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne) démontre, en matière de répartition des compétences, l'absence de lien entre la matière concrète traitée par la directive et les différents secteurs repris dans ses annexes (les actes juridiques sectoriels de l'Union sont d'ailleurs explicitement exclus du champ d'application de la directive par l'article 4).

Comme la directive NIS1, la transposition de cette directive met principalement en œuvre la matière de la protection préventive exercée dans le domaine de la sécurité publique, qui relève des compétences résiduelles exclusives du législateur fédéral (voir notamment les avis du Conseil d'État n° 63.296/4 du 2 mai 2018 sur l'avant-projet devenu la loi NIS1 et n° 48.989/VR du 9 décembre 2010 relatif à un avant-projet de loi devenue la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques).

Dans son avis 74.861/4 du 10 janvier 2024, le Conseil d'État a explicitement confirmé, comme pour l'avant-projet de loi devenu la loi du 7 avril 2019 "établissant un cadre pour la sécurité des réseaux et systèmes d'information

en overheidsinstanties tegen cyberdreigingen en cyberincidenten is. Het uitvallen of het aantasten van de netwerk- en informatiesystemen van bepaalde entiteiten die noodzakelijk worden geacht voor de instandhouding van diverse centrale functies voor het maatschappelijke leven kunnen immers grote gevolgen hebben voor de maatschappij en de economie (omdat ze diensten leveren die essentieel zijn voor de instandhouding van kritieke maatschappelijke en economische activiteiten). De cyberbeveiliging van "essentiële" of "belangrijke" NIS2-entiteiten maakt daarom duidelijk deel uit van de bescherming die wordt geboden op het gebied van openbare veiligheid in het algemeen (de bescherming van personen, rechtspersonen en eigendommen).

Bovendien stelt de NIS2-richtlijn geen specifieke cyberbeveiligingsregels vast die van toepassing zijn op alle organisaties die op een bepaald gebied actief zijn. Ze voorziet in gezamenlijke minimale maatregelen voor het beheer van cyberbeveiligingsrisico's en voor de melding van significante incidenten (of significante cyberdreigingen) voor alle essentiële en belangrijke entiteiten, en dit uitsluitend voor de activiteitssectoren vermeld in de bijlagen bij de wet en zonder een onderscheid te maken tussen deze sectoren.

Het algemene (sectoroverschrijdende) en gezamenlijke karakter, binnen de in de bijlagen bij de wet opgesomde sectoren, van de door de richtlijn voorgenen maatregelen (voor een hoog gezamenlijk niveau van cyberbeveiliging in de Europese Unie) toont, wat de verdeling van bevoegdheden betreft, dat er geen verband bestaat tussen de concrete aangelegenheid die in de richtlijn wordt behandeld en de verschillende sectoren vermeld in de bijlagen ervan (de sectorspecifieke rechtsinstrumenten van de Unie worden overigens uitdrukkelijk uitgesloten van het toepassingsgebied van de richtlijn door artikel 4).

Net als de NIS1-richtlijn leidt de omzetting van deze richtlijn hoofdzakelijk tot de tenuitvoerlegging van de aangelegenheid van de preventieve bescherming op het gebied van openbare veiligheid, die tot de exclusieve restbevoegdheid van de federale wetgever behoort (zie met name de adviezen van de Raad van State nr. 63.296/4 van 2 mei 2018 over het voorontwerp dat de NIS1-wet is geworden en nr. 48.989/VR van 9 december 2010 over een voorontwerp van wet dat de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur is geworden).

In advies nr. 74.861/4 van 10 januari 2024 heeft de Raad van State uitdrukkelijk bevestigd, zoals wat betreft het voorontwerp van de wet die de wet van 7 april 2019 "tot vaststelling van een kader voor de beveiliging van

d'intérêt général pour la sécurité publique" que le présent projet de loi ne soulevait aucun problème de compétence.

La circonstance que le fondement juridique de la directive en droit européen repose sur des considérations relatives au bon fonctionnement du marché intérieur ne détermine pas la matière au sens du niveau national qui est réglée par le contenu de celle-ci. Or, c'est en fonction de cette matière uniquement qu'il convient de s'interroger sur le niveau de pouvoir compétent, en droit interne, pour légiférer dans cette matière et, partant, pour transposer la directive.

En effet, si le législateur européen ne peut s'appuyer directement sur une compétence en matière de sécurité publique et utilise donc ses compétences relatives au bon fonctionnement du marché intérieur, le législateur national peut lui s'appuyer directement sur celle-ci.

La mise en œuvre de mesures communes minimales de cybersécurité au niveau national pour certaines entités critiques constitue avant tout des mesures de protection de la population et les entreprises du pays. La continuité des échanges économiques au sein du marché intérieur n'est qu'une conséquence indirecte de ces mesures de protection.

Il faut en conclure que la transposition de la directive NIS2, qui vise à définir des règles minimales concernant le fonctionnement d'un cadre réglementaire coordonné en matière de cybersécurité, relève de la compétence générale de la sécurité publique de l'État fédéral.

L'exercice de la compétence fédérale dans le projet de loi reste, en tout état de cause, proportionné et n'a pas pour conséquence de rendre impossible ou exagérément difficile l'exercice normal des compétences régionales ou communautaires dans les domaines d'activités de certaines entités essentielles ou importantes concernées. D'ailleurs, il est prévu dans le projet de loi de consulter, de manière facultative et en manière telle que leur éventuelle abstention de collaborer n'empêche pas l'adoption des mesures envisagées par l'autorité fédérale, les entités fédérées lorsque certaines entités seraient, pour d'autres aspects de leurs activités, soumis à des règles régionales ou communautaires.

La directive NIS2 doit être transposée en droit belge pour le 17 octobre 2024 au plus tard et être applicable le 18 octobre 2024.

netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid" is geworden, dat huidige voorontwerp van de wet geen bevoegdheidsvraagstuk opwerpt.

Uit het feit dat de rechtsgrond van de richtlijn in Europees recht gebaseerd is op overwegingen die verband houden met de goede werking van de interne markt, bepaalt niet welke aangelegenheid in de zin van het nationaal recht door de inhoud van deze richtlijn wordt geregeld. Het is echter enkel in functie van deze aangelegenheid dat men zich moet afvragen welk beleidsniveau in nationaal recht bevoegd is om ter zake wetgeving vast te stellen en dus om de richtlijn om te zetten.

Terwijl de Europese wetgever zich niet rechtstreeks kan baseren op een bevoegdheid inzake openbare veiligheid en daarom gebruik maakt van zijn bevoegdheden met betrekking tot de goede werking van de interne markt, kan de nationale wetgever zich hier wel rechtstreeks op baseren.

De uitvoering van minimale gemeenschappelijke cyberbeveiligingsmaatregelen op nationaal niveau voor bepaalde kritieke entiteiten is in de eerste plaats een middel om de bevolking en ondernemingen van ons land te beschermen. De continuïteit van het economisch verkeer in de interne markt is slechts een onrechtstreeks gevolg van deze beschermingsmaatregelen.

Hieruit moet worden besloten dat de omzetting van de NIS2-richtlijn, die tot doel heeft minimumvoorschriften vast te stellen voor de werking van een gecoördineerd regelgevingskader op het gebied van cyberbeveiliging, onder de algemene bevoegdheid inzake openbare veiligheid van de Federale Staat valt.

De uitoefening van de federale bevoegdheid in het wetsontwerp blijft in elk geval in verhouding en heeft niet tot gevolg dat het voor de gewesten of gemeenschappen onmogelijk of bovenmatig moeilijk zou zijn om hun bevoegdheden op de werkerterreinen van sommige betrokken essentiële of belangrijke entiteiten gewoon uit te oefenen. Bovendien bepaalt het wetsontwerp dat de deelgebieden worden geraadpleegd wanneer sommige entiteiten voor andere aspecten van hun activiteiten onderworpen zouden zijn aan gewestelijke of gemeenschapsregels. Deze raadpleging is facultatief en gebeurt op een zodanige wijze dat, indien de deelgebieden verzuimen om mee te werken, dit niet verhindert dat de federale overheid de voorgenomen maatregelen kan nemen.

De NIS2-richtlijn moet uiterlijk op 17 oktober 2024 omgezet zijn in Belgisch recht en moet van toepassing zijn op 18 oktober 2024.

COMMENTAIRES DES ARTICLES**TITRE 1^{ER}***Définitions et dispositions générales***CHAPITRE 1^{ER}****Objet et champ d'application****Section 1^{re}***Objet***Art. 1^{er}**

Cet article précise le fondement constitutionnel du présent projet de loi.

Art. 2

Cet article précise la directive transposée par la loi, à savoir la directive NIS2.

Art. 3

Cet article définit le champ d'application personnel du présent projet de loi.

Pour être considéré comme une entité publique ou privée d'un type visé à l'annexe I ou II de la loi, il suffit d'exercer, indépendamment de sa forme juridique, au moins une des activités reprises dans les annexes I ou II de la loi, même si ce service ne constitue qu'une partie accessoire de ses activités et de dépasser les plafonds visés au paragraphe 1^{er} ou de rencontrer un des critères visés aux paragraphes 3 et suivants (voir *infra*).

Il est important de souligner que, contrairement à la loi NIS1, le champ d'application de la loi NIS2 porte sur l'ensemble de l'entité concernée et non uniquement sur ses activités reprises dans les annexes de la loi.

Le paragraphe 1^{er} établit le principe selon lequel les entités reprises aux annexes qui constituent des entreprises moyennes au sens de la recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (ci-après, la "recommandation UE 2003/361") ou qui dépassent le plafond établi à l'article 2 de l'annexe de ladite recommandation rentrent dans le champ d'application du présent projet de loi.

TOELICHTING BIJ DE ARTIKELN**TITEL 1***Definities en algemene bepalingen***HOOFDSTUK 1****Onderwerp en toepassingsgebied****Afdeling 1***Onderwerp***Art. 1**

Dit artikel bevat de grondwettelijke grondslag van dit wetsontwerp.

Art. 2

Dit artikel vermeldt de richtlijn die door de wet wordt omgezet, namelijk de NIS2-richtlijn.

Art. 3

Dit artikel bepaalt het personele toepassingsgebied van dit wetsontwerp.

Om te worden beschouwd als een publieke of private entiteit van een type dat is opgenomen in bijlage I of II van de wet, is het voldoende om, ongeacht de rechtsvorm, ten minste één van de activiteiten uit te oefenen die zijn opgenomen in bijlage I of II van de wet, zelfs als deze dienst slechts een bijkomstig deel van de activiteiten uitmaakt, en de in paragraaf 1 bedoelde plafonds te overschrijden of voldoen aan een van de in paragraaf 3 en volgende bedoelde criteria (zie *infra*).

Het is belangrijk om te benadrukken dat, in tegenstelling tot de NIS1-wet, het toepassingsgebied van de NIS2-wet de hele betrokken entiteit omvat en niet alleen de activiteiten die zijn opgenomen in de bijlagen bij de wet.

Paragraaf 1 stelt het beginsel vast volgens hetwelk de in de bijlagen opgenomen entiteiten die middelgrote ondernemingen zijn als bedoeld in de Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (hierna "EU-aanbeveling 2003/361") of die het in artikel 2 van de bijlage bij deze aanbeveling vastgestelde plafond overschrijden, onder het toepassingsgebied van dit wetsontwerp vallen.

Pour les besoins du champ d'application de la loi, la taille de l'entité est calculée sur base des règles de l'annexe de la recommandation UE 2003/361.

L'article 6 de l'annexe de la recommandation UE 2003/361 prévoit notamment que le calcul de la taille d'une entité qui fait partie d'un groupe d'entités implique une consolidation des données des différentes entités de ce groupement.

L'article 3 de l'annexe de la recommandation UE 2003/361 définit les entreprises liées comme les entreprises qui entretiennent entre elles l'une des relations suivantes:

a) une entreprise a la majorité des droits de vote des actionnaires ou associés d'une autre entreprise;

b) une entreprise a le droit de nommer ou de révoquer la majorité des membres de l'organe d'administration, de direction ou de surveillance d'une autre entreprise;

c) une entreprise a le droit d'exercer une influence dominante sur une autre entreprise en vertu d'un contrat conclu avec celle-ci ou en vertu d'une clause des statuts de celle-ci;

d) une entreprise actionnaire ou associée d'une autre entreprise contrôle seule, en vertu d'un accord conclu avec d'autres actionnaires ou associés de cette autre entreprise, la majorité des droits de vote des actionnaires ou associés de celle-ci.

Sauf certaines exceptions, l'article 3 de l'annexe de la Recommandation UE 2003/361 qualifie d'"entreprises partenaires" toutes les entreprises qui ne sont pas qualifiées comme entreprises liées et qui entre lesquelles existe la relation suivante: une entreprise (entreprise en amont) détient, seule ou conjointement avec une ou plusieurs entreprises liées, 25 % ou plus du capital ou des droits de vote d'une autre entreprise (entreprise en aval).

Toutefois et par dérogation aux règles précitées, le paragraphe 2 de l'article 3 implique que l'autorité nationale de cybersécurité devra prendre en compte le degré d'indépendance d'une organisation, vis-à-vis d'éventuelles entreprises partenaires ou d'entreprises liées au sens de l'annexe de la recommandation 2003/361/CE.

Om van het toepassingsgebied van de wet te bepalen, wordt de omvang van de entiteit berekend op basis van de regels van de bijlage bij Aanbeveling EU 2003/361.

Art. 6 van de bijlage bij Aanbeveling EU 2003/361 bepaalt dat voor de berekening van de omvang van een entiteit die deel uitmaakt van een groep entiteiten, de gegevens van de verschillende entiteiten in de groep moeten worden geconsolideerd.

In artikel 3 van de bijlage bij Aanbeveling EU 2003/361 worden verbonden ondernemingen gedefinieerd als ondernemingen die met elkaar een van de volgende banden onderhouden:

a) een onderneming heeft de meerderheid van de stemrechten van de aandeelhouders of vennoten van een andere onderneming;

b) een onderneming heeft het recht de meerderheid van de leden van het bestuurs-, leidinggevend of toezichthoudend orgaan van een andere onderneming te benoemen of te ontslaan;

c) een onderneming heeft het recht een overheersende invloed op een andere onderneming uit te oefenen op grond van een met deze onderneming gesloten overeenkomst of een bepaling in de statuten van laatstgenoemde onderneming;

d) een onderneming die aandeelhouder of vennoot is van een andere onderneming, heeft op grond van een met andere aandeelhouders of vennoten van die andere onderneming gesloten overeenkomst als enige zeggenschap over de meerderheid van de stemrechten van de aandeelhouders of vennoten van laatstgenoemde onderneming.

Behoudens bepaalde uitzonderingen kwalificeert artikel 3 van de bijlage bij Aanbeveling EU 2003/361 als "partnerondernemingen" alle ondernemingen die niet als verbonden ondernemingen worden aangemerkt en waartussen de volgende band bestaat: een onderneming (van een hoger niveau) heeft, alleen of samen met een of meer verbonden ondernemingen, 25 % of meer van het kapitaal of de stemrechten van een andere onderneming (van een lager niveau).

In afwijking van voornoemde regels impliceert artikel 3, lid 2, echter dat de nationale cyberbeveiligingsautoriteit rekening moet houden met de mate van onafhankelijkheid van een organisatie ten opzichte van eventuele partnerondernemingen of verbonden ondernemingen als bedoeld in de bijlage bij Aanbeveling 2003/361/EG.

En effet, le considérant 16 de la directive précise que “afin d’éviter que des entités ayant des entreprises partenaires ou des entreprises liées ne soient considérées comme des entités essentielles ou importantes lorsque cela serait disproportionné, les États membres sont en mesure de tenir compte du degré d’indépendance dont jouit une entité à l’égard de ses partenaires et de ses entreprises liées lorsqu’ils appliquent l’article 6, paragraphe 2, de l’annexe de la recommandation 2003/361/CE. En particulier, les États membres sont en mesure de tenir compte du fait qu’une entité est indépendante de son partenaire ou d’entreprises liées en ce qui concerne le réseau et les systèmes d’information qu’elle utilise pour fournir ses services et en ce qui concerne les services qu’elle fournit. Sur cette base, s’il y a lieu, les États membres peuvent considérer qu’une telle entité ne constitue pas une entreprise moyenne en vertu de l’article 2 de l’annexe de la recommandation 2003/361/CE, ou ne dépasse pas les plafonds applicables à une entreprise moyenne prévus au paragraphe 1 dudit article, si, après prise en compte du degré d’indépendance de ladite entité, celle-ci n’aurait pas été considérée comme constituant une entreprise moyenne ou dépassant lesdits plafonds si seules ses propres données avaient été prises en compte”.

Le mécanisme envisagé permettrait ainsi de qualifier une entité d’importante (plutôt qu’essentielle) ou de l’exclure du champ d’application lorsque l’entreprise petite ou moyenne fait partie d’un groupe d’entreprises (liées ou partenaires) mais utilise des réseaux ou des systèmes d’information indépendants de ces autres entreprises pour fournir ses services dans l’Union européenne et que l’application des règles du calcul de la taille de l’entreprise (consolidation des chiffres d’affaires et des membres du personnel entre entreprises) s’avère disproportionnée.

Au besoin, il est prévu que le Roi peut déterminer les critères précis sur base desquels le degré d’indépendance dont jouit une entité à l’égard de ses partenaires et de ses entreprises liées est évalué.

Les paragraphes 3 à 5 de l’article 3 établissent les exceptions au principe établi au paragraphe 1^{er} au travers desquelles la loi s’applique à certains types d’entités, quelle que soit leur taille.

Le 3^o du troisième paragraphe spécifie en particulier que la loi NIS2 s’applique aux entités de l’administration publique qui “dépendent de” l’état fédéral, des entités

Overweging 16 van de richtlijn luidt immers als volgt: “Om te voorkomen dat entiteiten met partnerondernemingen of verbonden ondernemingen als essentiële of belangrijke entiteiten worden beschouwd wanneer dit onevenredig zou zijn, kunnen de lidstaten bij de toepassing van artikel 6, lid 2, van de bijlage bij Aanbeveling 2003/361/EG rekening houden met de mate van onafhankelijkheid welke die entiteiten ten opzichte van hun partnerondernemingen of verbonden ondernemingen genieten. Meer bepaald kunnen de lidstaten rekening houden met het feit dat een entiteit onafhankelijk is van haar partnerondernemingen of verbonden ondernemingen wat de netwerk- en informatiesystemen betreft waarvan die entiteit gebruikmaakt bij het verlenen van haar diensten en wat de diensten betreft die de entiteit verleent. Op basis daarvan kunnen de lidstaten een dergelijke entiteit in voorkomend geval beschouwen als een entiteit die niet wordt aangemerkt als een middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG, noch de plafonds voor een middelgrote onderneming als bepaald in lid 1 van dat artikel overschrijdt, indien die entiteit, rekening houdend met de mate van onafhankelijkheid die zij geniet, niet als middelgrote onderneming zou worden aangemerkt of niet zou worden geacht die plafonds te overschrijden ingeval alleen rekening zou worden gehouden met haar eigen gegevens.”

Het bedoelde mechanisme zou het aldus mogelijk maken een entiteit als belangrijk (in plaats van essentieel) aan te merken of van het toepassingsgebied uit te sluiten, indien de kleine of middelgrote onderneming deel uitmaakt van een groep van ondernemingen (verbonden ondernemingen of partnerondernemingen), maar gebruik maakt van netwerk- of informatiesystemen die onafhankelijk zijn van deze andere ondernemingen om haar diensten in de Europese Unie te verlenen en de toepassing van de regels voor de berekening van de grootte van de onderneming (consolidatie van de omzet en personeelsleden tussen ondernemingen) onevenredig blijkt.

Indien nodig is voorzien dat de Koning de precieze criteria kan bepalen op basis waarvan de mate van onafhankelijkheid van een entiteit ten opzichte van haar partnerondernemingen en verbonden ondernemingen wordt aangetoond.

De paragrafen 3 tot 5 van artikel 3 stellen de uitzonderingen vast op het in paragraaf 1 bepaalde beginsel waardoor de wet van toepassing is op bepaalde soorten entiteiten, ongeacht hun omvang.

In het bijzonder, specificeert 3^o van de derde paragraaf dat de NIS2-wet van toepassing is op overheidsinstanties die “afhangen van” de Federale Staat, de gefedereerde

fédérées (en cas d'identification formelle) et qui constituent des zones de secours au sens large. La notion de dépendance, inspirée par l'article 5 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, permet d'englober notamment des entités qui font partie du niveau fédéral et du niveau fédéré, qui ont été créés par ces autorités publiques, dont l'activité est financée majoritairement par les autorités publiques, dont la gestion est soumise à un contrôle de ces autorités ou organismes, ou encore dont plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par ces autorités ou organismes.

Il convient de préciser que les autorités locales (communes, provinces, intercommunales, CPAS, etc.) ne sont pas des entités de l'administration publique qui dépendent de l'État fédéral ou qui dépendent des entités fédérées ne sont pas reprises à l'annexe I.

Toutefois, elles peuvent être soumises aux dispositions de la loi lorsqu'elles exercent une activité reprise à l'annexe I ou II (par exemple la distribution d'eau potable, la gestion des déchets, la distribution d'électricité, etc.).

Les autorités locales peuvent également faire l'objet d'une identification par le biais de l'article 11, § 1 (désignation par l'autorité nationale de cybersécurité), moyennant le respect des procédures de concertation prévues par l'article 11, § 3. L'initiative d'une telle identification pourrait être effectuée, éventuellement à la demande de l'entité concernée, de l'autorité nationale de cybersécurité, d'une Région ou du NCCN.

Le dernier paragraphe donne la compétence au Roi d'ajouter des secteurs ou sous-secteurs aux annexes I et II du présent projet de loi. De cette manière, lorsqu'il apparaît, dans le futur, qu'un secteur ne se trouvant pas encore dans le champ d'application du présent projet de loi devrait y être intégré, en raison de son importance pour des activités sociétales et/ou économiques critiques, les annexes pourront être étendues.

Art. 4

Cette disposition définit le champ d'application territorial du présent projet de loi.

Le paragraphe 1^{er} établit le principe selon lequel la loi s'applique aux entités qui sont établies en Belgique et qui fournissent leurs services ou exercent leurs activités au sein de l'Union européenne.

entiteiten (in het geval van formele identificatie) en die hulpverleningszones in ruime zin uitmaken. Het begrip afhangen volgt uit artikel 5 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens die het met name mogelijk maakt om entiteiten te omvatten die deel uitmaken van het federale en gefedereerde niveau, die door deze overheden zijn opgericht, waarvan de activiteiten in hoofdzaak door de overheden worden gefinancierd, waarvan het beheer onderworpen is aan het toezicht door deze overheden of instellingen, hetzij waarvan de leden van het bestuursorgaan, leidinggevend orgaan of toezichthoudend orgaan voor meer dan de helft door deze overheden of instellingen zijn aangewezen.

Opgemerkt wordt dat lokale besturen (gemeenten, provincies, intercommunales, OCMW's, enz.) geen overheidsinstanties zijn die afhangen van de Federale Staat of die afhangen van de gefedereerde entiteiten. Ze zijn bijgevolg niet opgenomen in bijlage I.

Zij kunnen echter wel onderworpen zijn aan de bepalingen van de wet wanneer zij een in bijlage I of II opgenomen activiteit uitoefenen (bijvoorbeeld distributie van drinkwater, afvalbeheer, distributie van elektriciteit, enz.).

Lokale besturen kunnen daarnaast ook worden geïdentificeerd op basis van artikel 11, § 1 (aanwijzing door de nationale cyberbeveiligingsautoriteit), met inachtneming van de overlegprocedures van artikel 11, § 3. Het initiatief voor een dergelijke identificatie kan worden genomen, eventueel op verzoek van de betrokken entiteit, door de nationale cyberbeveiligingsautoriteit, een gewest of het NCCN.

De laatste paragraaf verleent de Koning de bevoegdheid om sectoren of deelsectoren toe te voegen aan de bijlagen I en II van dit wetsontwerp. Op die manier kunnen de bijlagen worden uitgebreid wanneer in de toekomst blijkt dat een sector die nog niet onder het toepassingsgebied van dit wetsontwerp valt, daarin moet worden opgenomen vanwege het belang ervan voor kritieke maatschappelijke en/of economische activiteiten.

Art. 4

Deze bepaling omschrijft het territoriale toepassingsgebied van dit wetsontwerp.

Paragraaf 1 legt het beginsel vast dat de wet van toepassing is op entiteiten die gevestigd zijn in België en die hun diensten verlenen of hun activiteiten verrichten in de Europese Unie.

Comme le confirme le considérant 114 de la directive NIS2, la notion d'établissement suppose l'exercice effectif d'une activité au moyen d'une installation stable, indépendamment de la forme juridique retenue, qu'il s'agisse du siège social, d'une simple succursale ou d'une filiale ayant la personnalité juridique.

Le paragraphe 2 prévoit des exceptions par rapport à certains types d'entités, pour lesquels la loi s'applique soit lorsqu'ils fournissent leurs services en Belgique, soit lorsqu'ils ont leur établissement principal en Belgique (notion d'établissement principal à ne pas confondre avec la notion d'établissement reprise au paragraphe 1^{er}).

Le paragraphe 3 prévoit qu'une entité qui n'est pas établie dans l'Union européenne mais y fournit des services désigne un représentant dans l'Union.

Les paragraphes 4 et 5 prévoient un système en cascade permettant de déterminer si une entité a son établissement principal en Belgique ou non.

Art. 5

Cet article précise certaines exceptions et exclusions au champ d'application du présent projet de loi.

La disposition précise que la loi ne porte pas préjudice à l'application du RGPD, aux lois et règlements qui le complètent ou le précisent ainsi qu'à la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Il est aussi rappelé que les dispositions du présent projet de loi ne portent pas préjudice à l'application de certaines autres dispositions légales, dont celles relatives au traitement des informations classifiées au sens de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé ainsi que les règles applicables aux documents nucléaires au sens de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire. Par ailleurs, la présente loi ne porte pas préjudice à la loi du 5 août 1992 sur la fonction de police.

Par exemple, si certaines informations qui doivent être échangées en application du projet de loi sont classifiées en tout ou en partie en vertu de la loi du 11 décembre

Zoals wordt bevestigd in overweging 114 van de NIS2-richtlijn, houdt het vestigingscriterium de daadwerkelijke uitoefening van de activiteit in door middel van stabiele regelingen, ongeacht de gekozen rechtsvorm, hetzij via de maatschappelijke zetel, hetzij via een filiaal, hetzij via een dochteronderneming met rechtspersoonlijkheid.

Paragraaf 2 voorziet in uitzonderingen bij bepaalde soorten entiteiten, waarvoor de wet van toepassing is wanneer zij hun diensten in België verlenen of wanneer zij hun hoofdvestiging in België hebben (het begrip "hoofdvestiging" mag niet worden verward met het begrip "vestiging" in paragraaf 1).

Paragraaf 3 bepaalt dat een entiteit die niet in de Europese Unie is gevestigd maar er diensten verleent, een vertegenwoordiger in de Unie aanwijst.

De paragrafen 4 en 5 voorzien in een cascadesysteem om te bepalen of een entiteit haar hoofdvestiging al dan niet in België heeft.

Art. 5

Dit artikel bepaalt een aantal uitzonderingen en uitsluitingen van het toepassingsgebied van dit wetsontwerp.

De bepaling verduidelijkt dat de wet geen afbreuk doet aan de toepassing van de AVG, aan de wetten en reglementen die deze aanvullen of verduidelijken noch aan de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

Tevens wordt erop gewezen dat de bepalingen van dit wetsontwerp geen afbreuk doen aan de toepassing van een aantal andere wettelijke bepalingen, waaronder die betreffende de verwerking van geclassificeerde informatie als bedoeld in de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst, noch aan de regels die van toepassing zijn op nucleaire documenten als bedoeld in de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle. Bovendien doet deze wet geen afbreuk aan de wet van 5 augustus 1992 op het politieambt.

Indien bijvoorbeeld bepaalde informatie die overeenkomstig het wetsontwerp moet worden uitgewisseld, volledig of gedeeltelijk geclassificeerd is krachtens

1998 précitée, cette dernière et ses actes d'exécution demeurent entièrement applicables.

Par ailleurs, les systèmes de communication et d'information approuvés pour utiliser des informations classifiées sous forme électronique dans le cadre de la loi précitée ne sont pas soumis aux dispositions du présent projet de loi, notamment en matière de mesures de gestion des risques en matière de cybersécurité. Cela a pour conséquence que certaines entités seront soumises au projet de loi et devront appliquer les dispositions de la présente loi à leurs réseaux et systèmes d'information, à l'exclusion des systèmes de communication et d'information approuvés dans le cadre de la loi précitée du 11 décembre 1998. Cette exception au champ d'application ne permet pas à une entité d'être complètement exclue du champ d'application. Elle permet, du point de vue du champ d'application matériel, d'exclure ces systèmes approuvés des obligations en matière d'analyses des risques, de mesures de sécurité à adopter, de notifications, etc.

Le paragraphe 4 précise que seules quelques dispositions de la loi s'appliquent à certaines administrations publiques ou entités limitativement énumérées. En ce qui concerne les services de renseignement et de sécurité, l'OCAM, le Ministère de la Défense, les services et l'inspection générale de la police, les autorités judiciaires, le SPF Justice, les missions diplomatiques et consulaires belges dans des pays tiers à l'Union européenne, ainsi que les établissements nucléaires de classe I, l'ensemble des obligations incombant aux entités essentielles et importantes mentionnées dans la présente loi ne leur sont pas applicables, dans la mesure où ces obligations sont liées à la transposition de la directive (EU) 2022/2555.

L'article 2, §§ 7 et 8, de la directive exclut effectivement de son champ d'application les entités de l'administration publique ou des entités spécifiques qui exercent leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense, ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière, pour autant qu'ils ne constituent pas des prestataires de services de confiance (l'article 2, § 9, de la directive). Les articles 8 et 38, ainsi que le titre 2 de la présente loi regroupant principalement des aspects liés aux missions légales du CCB, sont applicables auxdits services, dans le cadre des missions précitées.

En son article 2, § 6, la directive rappelle également qu'elle est sans préjudice de la responsabilité des États membres en matière de sauvegarde de la sécurité nationale et de leur pouvoir de garantir d'autres fonctions essentielles de l'État, notamment celles qui ont

voornemde wet van 11 december 1998, blijven de laatstgenoemde wet en de uitvoeringsbesluiten ervan volledig van toepassing.

Bovendien zijn communicatie- en informatiesystemen die in het kader van voornoemde wet zijn goedgekeurd om geclassificeerde informatie in elektronische vorm te gebruiken, niet onderworpen aan de bepalingen van dit wetsontwerp, met name wat betreft de maatregelen voor het beheer van cyberbeveiligingsrisico's. Bijgevolg zullen bepaalde entiteiten onderworpen zijn aan het wetsontwerp en zullen zij de bepalingen van deze wet moeten toepassen op hun netwerk- en informatiesystemen, met uitzondering van de communicatie- en informatiesystemen die in het kader van voornoemde wet van 11 december 1998 goedgekeurd zijn. Deze uitzondering op het toepassingsgebied laat niet toe dat een entiteit hiervan volledig wordt uitgesloten. Wat het materiële toepassingsgebied betreft, laat ze toe dat deze goedgekeurde systemen worden uitgesloten van de verplichtingen met betrekking tot risicoanalyses, te nemen beveiligingsmaatregelen, meldingen, enz.

Paragraaf 4 verduidelijkt dat slechts enkele bepalingen van de wet van toepassing zijn op bepaalde limitatief opgesomde overheidsinstanties of entiteiten. Wat de inlichtingen- en veiligheidsdiensten, het OCAD, het Ministerie van Landsverdediging, de politiediensten en de algemene inspectie van de politie, de rechtelijke overheden, de FOD Justitie, de Belgische diplomatieke en consulaire missies in landen buiten de Europese Unie, evenals de nucleaire inrichtingen van klasse I betreft, is het geheel van de verplichtingen die deze wet oplegt aan essentiële en belangrijke entiteiten, niet op hen van toepassing. Deze verplichtingen houden immers verband met de omzetting van Richtlijn (EU) 2022/2555.

Art. 2, leden 7 en 8, van de richtlijn sluit overheidsinstanties of specifieke entiteiten die activiteiten uitoefenen op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, inderdaad uit van het toepassingsgebied, voor zover zij geen aanbieders van vertrouwensdiensten zijn (artikel 2, lid 9, van de richtlijn). De artikelen 8 en 38, alsook titel 2 van deze wet, die hoofdzakelijk betrekking hebben op aspecten die verband houden met de wettelijke opdrachten van het CCB, zijn van toepassing op deze diensten, in het kader van voornoemde opdrachten.

Tevens wijst artikel 2, lid 6, van de richtlijn erop dat de richtlijn de verantwoordelijkheid van de lidstaten om de nationale veiligheid te beschermen en hun bevoegdheid om andere essentiële staatsfuncties te beschermen, waaronder het verdedigen van de territoriale integriteit

pour objet d'assurer l'intégrité territoriale de l'État et de maintenir l'ordre public.

Dans le même contexte, il est prévu d'exclure les établissements de classe I au sens de l'article 3.1 de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants. Ceux-ci sont soumis à des exigences nationales et internationales spécifiques, sous le contrôle de l'Agence fédérale de contrôle nucléaire.

À l'instar de la loi NIS actuelle, il est néanmoins prévu que les éléments d'une installation nucléaire destinée à la production industrielle d'électricité et qui servent au transport de l'électricité demeurent eux soumis à la présente loi. Concrètement, cela signifie que les parties des réseaux et systèmes d'information d'une installation nucléaire qui ne sont pas destinée à la production industrielle d'électricité et qui ne servent au transport de l'électricité ne sont pas soumis aux exigences de la présente loi.

Le paragraphe exclut aussi les réseaux et systèmes d'information des missions diplomatiques et consulaires belges dans des pays tiers à l'Union européenne, dès lors que les règles de la directive ne s'appliquent pas à ceux-ci, comme le mentionne le considérant 8 de la directive.

L'exclusion des mesures de gestion des risques en matière de cybersécurité, de notification des incidents et de supervision du présent projet de loi ne signifie pas que les administrations et entités concernées ne doivent pas mettre en œuvre des mesures de cybersécurité. Compte tenu de leur caractère critique, ces administrations doivent au contraire atteindre un niveau équivalent, voire supérieur aux exigences minimales imposées aux entités essentielles.

Comme cela est déjà le cas actuellement, les cyberincidents significatifs (pour autant qu'ils ne concernent pas des réseaux et systèmes d'information approuvés pour traiter des informations classifiées) sont notifiés au Centre pour la Cybersécurité Belgique (ci-après, CCB), dans le respect des exigences liées à la sécurité nationale et du plan national d'urgence cyber, selon des modalités particulières.

En outre, les activités les plus sensibles des administrations précitées sont réalisées au moyen des réseaux et systèmes approuvés pour traiter des informations classifiées.

van de staat en het handhaven van de openbare orde, onverlet laat.

In dezelfde context wordt voorzien in een uitsluiting van inrichtingen van klasse I als bedoeld in artikel 3.1 van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen. Deze zijn onderworpen aan specifieke nationale en internationale eisen, onder toezicht van het Federaal Agentschap voor Nucleaire Controle.

Net als in de huidige NIS-wet wordt niettemin bepaald dat de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit en die dienen voor de transmissie van elektriciteit, onderworpen blijven aan deze wet. Concreet betekent dit dat de delen van de netwerk- en informatiesystemen van een nucleaire installatie die niet bestemd zijn voor de industriële productie van elektriciteit en niet dienen voor de transmissie van elektriciteit, niet onderworpen zijn aan de voorschriften van deze wet.

In de paragraaf worden tevens de netwerk- en informatiesystemen van Belgische diplomatieke en consulaire missies in landen buiten de Europese Unie uitgesloten, aangezien de regels van de richtlijn hierop niet van toepassing zijn, zoals vermeld in overweging 8 van de richtlijn.

Het feit dat de betrokken overheidsinstanties en entiteiten worden uitgesloten van de maatregelen van dit wetsontwerp voor het beheer van cyberbeveiligingsrisico's, de melding van incidenten en het toezicht, betekent niet dat zij geen cyberbeveiligingsmaatregelen moeten nemen. Gelet op hun kritieke aard moeten deze overheidsinstanties integendeel een gelijkwaardig of zelfs hoger niveau bereiken dan het basisniveau dat aan essentiële entiteiten wordt opgelegd.

Zoals momenteel al het geval is, worden significante cyberincidenten (voor zover ze geen betrekking hebben op netwerk- en informatiesystemen die zijn goedgekeurd om geclassificeerde informatie te verwerken) gemeld aan het Centrum voor Cybersecurity België (hierna CCB), met inachtneming van de eisen in verband met de nationale veiligheid en het nationaal cybernoodplan, volgens bijzondere modaliteiten.

Verder worden de meest gevoelige activiteiten van voornoemde overheidsinstanties uitgevoerd door middel van netwerken en systemen die zijn goedgekeurd voor de verwerking van geclassificeerde informatie.

Selon le paragraphe 5, les titres 3 à 5 du présent projet de loi ne sont pas applicables au NCCN et au CCB. Il demeure nécessaire de rendre applicables à ces administrations publiques certaines parties du présent projet de loi, à savoir les titres 1^{er} “Définitions et dispositions générales”, 2 “Autorités compétentes et coopération au niveau national”, 6 “Traitement des données à caractère personnel” et 7 “Dispositions finales”. Ces dispositions s’avèrent, en effet, nécessaires pour permettre l’échange d’informations, notamment sur les notifications d’incidents, et la coopération (en ce compris le traitement de données à caractère personnel).

Les autorités relevant des pouvoirs législatifs ne sont pas mentionnées dans cette disposition car elles ne sont pas incluses dans la notion d’entité de l’administration publique.

Art. 6

Cet article, qui transpose l’article 4 de la directive NIS2, prévoit un mécanisme permettant de déroger à certaines dispositions de la loi lorsque des instruments juridiques sectoriels de l’Union européenne prévoient des mesures de gestion des risques en matière de cybersécurité et/ou des mesures en matière de notification d’incidents significatifs et que ces mesures ont un effet au moins équivalent à celui des obligations du présent projet de loi. Le paragraphe 2 de cet article précise ce qu’il faut entendre par effet équivalent.

Sur base de cette disposition, certains articles du présent projet de loi, pour lesquels il existe un équivalent au travers d’un instrument juridique sectoriel de l’Union européenne, ne sont pas applicables aux entités concernées.

Le paragraphe 3 porte sur un tel acte juridique sectoriel de l’Union européenne, à savoir le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) n° 2016/1011, ci-après le règlement DORA, et sur les dérogations au présent projet de loi qui en découlent.

Ce paragraphe prévoit que les entités relevant des secteurs bancaires et des infrastructures des marchés financiers qui tombent dans le champ d’application du règlement DORA ne sont pas soumises aux dispositions relatives à la gestion des risques de cybersécurité, à la notification d’incidents, à la supervision et à l’exécution.

Volgens paragraaf 5 zijn de titels 3 tot 5 van dit wetsontwerp niet van toepassing op het NCCN en het CCB. Het blijft noodzakelijk om bepaalde delen van dit wetsontwerp toepasselijk te maken op deze overheidsinstanties, namelijk titel 1 “Definities en algemene bepalingen”, titel 2 “Bevoegde autoriteiten en samenwerking op nationaal niveau”, titel 6 “Verwerking van persoonsgegevens” en titel 7 “Slotbepalingen”. Deze bepalingen zijn immers nodig om de uitwisseling van informatie, met name over meldingen van incidenten, en de samenwerking (met inbegrip van de verwerking van persoonsgegevens) mogelijk te maken.

Autoriteiten van de wetgevende macht worden in deze bepaling niet vermeld, omdat zij niet onder het begrip “overheidsinstantie” vallen.

Art. 6

Dit artikel, dat voorziet in de omzetting van artikel 4 van de NIS2-richtlijn, stelt een mechanisme vast om af te wijken van sommige bepalingen van de wet indien sectorspecifieke rechtsinstrumenten van de Europese Unie voorzien in maatregelen voor het beheer van cyberbeveiligingsrisico’s en/of maatregelen voor de melding van significante incidenten en deze maatregelen ten minste gelijkwaardig zijn aan de verplichtingen van dit wetsontwerp. Paragraaf 2 van dit artikel verduidelijkt wat onder “gelijkwaardig” wordt verstaan.

Op basis van deze bepaling zijn sommige artikelen van dit wetsontwerp, waarvoor een equivalent bestaat via een sectorspecifiek rechtsinstrument van de Europese Unie, niet van toepassing op de betrokken entiteiten.

Paragraaf 3 heeft betrekking op een dergelijk sector-specifiek rechtsinstrument van de Europese Unie, namelijk Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) nr. 2016/1011, hierna de DORA-verordening, en op de daaruit voortvloeiende afwijkingen van dit wetsontwerp.

Deze paragraaf bepaalt dat entiteiten die behoren tot de sectoren van het bankwezen en de infrastructuur voor de financiële markt die onder het toepassingsgebied van de DORA-verordening vallen, niet onderworpen zijn aan de bepalingen met betrekking tot het beheer van cyberbeveiligingsrisico’s, de melding van incidenten, het toezicht en de handhaving.

Le paragraphe 4 met également en œuvre la dérogation visée au paragraphe 1^{er} dans le secteur bancaire. Selon ce paragraphe, les dispositions du projet de loi relatives aux mesures de gestion des risques en matière de cybersécurité, à la supervision et à l'exécution ne s'appliquent pas aux entités listées. Il est important de noter que les dispositions en matière de notification d'incidents sont, elles, toujours applicables.

La dérogation du paragraphe 4 s'applique d'abord à la Banque nationale de Belgique, ci-après, la "BNB". En effet, la BNB, en tant que banque centrale, fait partie du système européen de banques centrales (le "SEBC"), constitué de l'ensemble des banques centrales européennes. Le SEBC impose toute une série d'orientations et d'instructions en matière de sécurité informatique applicables à toutes les banques centrales.

Art. 7

Sur base de l'article 6, la dérogation au champ d'application s'applique *de jure*, sans nécessairement d'intervention du Roi. Cette habilitation dévolue au Roi permet d'explicitier, de manière non exhaustive, des instruments juridiques sectoriels de l'Union européenne (présents ou futurs) comme équivalents, en vue d'améliorer la prévisibilité et la sécurité juridique. Cette disposition donne également compétence au Roi d'établir les règles spécifiques en matière d'échange d'informations et de notification d'incidents entre les autorités compétentes, dans le cadre de la dérogation visée aux paragraphes 3 et 4 de l'article 6. Cette dernière attribution de compétence permet d'assurer un échange d'informations adéquats lors d'incidents de cybersécurité.

CHAPITRE 2

Définitions

Art. 8

Cet article reprend pour l'essentiel les définitions telles qu'établies par la directive NIS2 ainsi que certains éléments spécifiques au cadre législatif belge.

La notion de réseau et système d'information, défini à l'article 6, 1^o, de la directive NIS2 est complétée à l'article 8, 1^o, b) pour préciser, entre autres choses, que sont bien inclus dans cette définition les réseaux interconnectés de manière permanente ou temporaire et les composants numériques, électroniques ou mécaniques d'un dispositif permettant notamment l'automatisation

Paragraphe 4 implementeert de in de eerste paragraaf bedoelde afwijking ook in het bankwezen. Volgens deze paragraaf zijn de bepalingen van het wetsontwerp betreffende de maatregelen voor het beheer van cyberbeveiligingsrisico's, het toezicht en de handhaving niet van toepassing op de opgelijste entiteiten. Het is belangrijk op te merken dat de bepalingen over de melding van incidenten wel van toepassing zijn.

De afwijking van paragraaf 4 is in de eerste plaats van toepassing op de Nationale Bank van België, hierna de "NBB". Als centrale bank maakt de NBB immers deel uit van het Europees Stelsel van Centrale Banken (het "ESCB"), dat bestaat uit alle Europese centrale banken. Het ESCB legt alle centrale banken een hele reeks richtsnoeren en instructies inzake IT-beveiliging op.

Art. 7

Op basis van artikel 6 is de afwijking van het toepassingsgebied *de jure* van toepassing, zonder dat de tussenkomst van de Koning vereist is. Deze machtiging aan de Koning maakt het mogelijk om (huidige of toekomstige) sectorspecifieke rechtsinstrumenten van de Europese Unie op niet-exhaustieve wijze uitdrukkelijk als gelijkwaardig aan te duiden, met het oog op een betere voorspelbaarheid en rechtszekerheid. Deze bepaling geeft de Koning ook de bevoegdheid om specifieke regels vast te stellen met betrekking tot de uitwisseling van informatie en de melding van incidenten tussen de bevoegde autoriteiten, in het kader van de afwijking bedoeld in de paragrafen 3 en 4 van artikel 6. Deze laatste bevoegdheidstoekenning zorgt voor een adequate informatie-uitwisseling bij cyberbeveiligingsincidenten.

HOOFDSTUK 2

Definities

Art. 8

Dit artikel bevat in hoofdzaak de definities zoals die zijn vastgesteld door de NIS2-richtlijn, alsook sommige aspecten die specifiek betrekking hebben op het Belgische wetgevende kader.

Het begrip "netwerk- en informatiesysteem", gedefinieerd in artikel 6, 1^o, van de NIS2-richtlijn, wordt aangevuld in artikel 8, 1^o, b), om onder andere te verduidelijken dat deze definitie ook betrekking heeft op netwerken die permanent of tijdelijk met elkaar verbonden zijn en op de digitale, elektronische of mechanische componenten van een apparaat die met name de automatisering van

de processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel.

Il s'agit de confirmer explicitement l'application de la directive notamment aux systèmes d'acquisition et de contrôle de données industriels (en anglais "Supervisory Control And Data Acquisition", en abrégé "SCADA"), ainsi que les dispositifs interconnectés de manière permanente ou temporaire.

Pour la définition d'une entité de l'administration publique, l'article 6, 35) de la directive précise que la notion doit être reconnue comme telle conformément au droit national, à l'exclusion de la justice, des parlements et des banques centrales. Ainsi, il a été choisi de faire référence à des notions existantes en droit belge qui couvrent les entités concernées afin de ne pas multiplier l'application de notions différentes.

En l'occurrence, la définition reprend la notion d'autorité administrative visée à l'article 14, § 1^{er}, alinéa 1^{er}, des lois coordonnées du 12 janvier 1973 sur le Conseil d'État, à laquelle sont rajoutés les critères de ne pas avoir de caractère industriel ou commercial, de ne pas exercer à titre principal une activité relevant de l'un des autres secteurs ou sous-secteurs repris dans les annexes du présent projet de loi et de ne pas être une personne morale de droit privé.

Ce choix s'explique de par le fait que la plupart des critères repris dans la définition de la directive se retrouvent dans les critères qui délimitent la notion d'autorité administrative au sens des lois coordonnées sur le Conseil d'État.

S'agissant de l'absence de caractère industriel ou commercial, l'appréciation doit se faire sur base d'indices objectifs au cas par cas. À cet égard, il est intéressant de relever que la notion de "besoins d'intérêt général ayant un caractère autre qu'industriel et commercial" est issue du droit dérivé européen, et plus particulièrement des directives européennes sur la passation des marchés publics. Il s'ensuit que les entités qui sont qualifiées de pouvoirs adjudicateurs au sens de l'article 2, 1^o, c) de la loi du 17 juin 2016 relative aux marchés publics remplissent la condition de la satisfaction d'un besoin d'intérêt général ayant un caractère autre qu'industriel et commercial. Sur cette condition spécifique, il peut donc être pertinent de se référer notamment à la liste non limitative des "pouvoirs adjudicateurs" au sens de la loi précitée, dressée dans l'arrêté royal du 18 avril

het operationele proces, de controle op afstand of het verkrijgen van werkingsgegevens in real time mogelijk maken.

Doel is uitdrukkelijk te bevestigen dat de richtlijn met name van toepassing is op SCADA-systemen (waarbij SCADA staat voor "Supervisory Control And Data Acquisition") en op apparaten die permanent of tijdelijk met elkaar verbonden zijn.

Voor de definitie van een overheidsinstantie verduidelijkt artikel 6, 35), van de richtlijn dat het begrip overeenkomstig het nationale recht als zodanig erkend moet zijn, met uitzondering van de rechterlijke macht, parlementen en centrale banken. Daarom werd ervoor gekozen te verwijzen naar bestaande begrippen in het Belgisch recht die de betrokken entiteiten omvatten, zodat er niet te veel verschillende begrippen zouden worden toegepast.

In dit geval verwijst de definitie naar het begrip "administratieve overheid" als bedoeld in artikel 14, § 1, eerste lid, van de gecoördineerde wetten van 12 januari 1973 op de Raad van State, waaraan criteria zijn toegevoegd: zij mag niet van industriële of commerciële aard zijn, niet hoofdzakelijk een activiteit uitoefenen die tot een van de andere sectoren of deelsectoren opgenomen in de bijlagen bij dit wetsontwerp behoort en geen privaatrechtelijke rechtspersoon zijn.

Deze keuze wordt verklaard door het feit dat de meeste criteria in de definitie van de richtlijn terug te vinden zijn in de criteria die het begrip "administratieve overheid" als bedoeld in de gecoördineerde wetten op de Raad van State afbakenen.

Wat betreft het feit dat de overheidsinstantie niet van industriële of commerciële aard mag zijn, moet de beoordeling geval per geval gebeuren op basis van objectieve aanwijzingen. In dit verband is het interessant op te merken dat het begrip "behoeften van algemeen belang die niet van industriële of commerciële aard zijn" ontleend is aan het Europese afgeleide recht, en meer bepaald aan de Europese richtlijnen betreffende de plaatsing van overheidsopdrachten. Hieruit volgt dat entiteiten die worden beschouwd als aanbestedende overheden in de zin van artikel 2, 1^o, c), van de wet van 17 juni 2016 inzake overheidsopdrachten, voldoen aan de voorwaarde dat zij voorzien in een behoefte van algemeen belang die niet van industriële of commerciële aard is. Wat deze specifieke voorwaarde betreft, kan het dus relevant zijn om met name te verwijzen naar de

2017 relatif à la passation des marchés publics dans les secteurs classiques.

Les conditions de ne pas être une personne morale de droit privé et de ne pas exercer à titre principal une activité énumérée dans la colonne type d'entité d'un autre secteur (ou sous-secteur) de l'une des annexes de la loi, visent à limiter le secteur de l'administration publique aux autorités administratives qui sont des personnes morales de droit public et qui n'exercent pas principalement une activité relevant déjà d'un secteur soumis à la loi.

Cette dernière condition permet également de ne pas créer de différence de traitement entre les entités publiques et privées actives dans un même secteur ou sous-secteur, notamment en ce qui concerne les sanctions administratives éventuellement applicables.

Cet article définit également diverses notions reprises de la directive afin d'en clarifier le contenu (voir les définitions aux 42°, 48°, 49°, 51° et 57° à 59°).

Par ailleurs, des notions spécifiques à la loi sont définies, aux 43° à 47°, 50° et 52° au 56°, notamment l'autorité nationale de cybersécurité, désignée par le Roi, qui joue un rôle central dans la mise en œuvre de la loi (voir ci-dessous, les articles 17 et suivants) ou l'autorité sectorielle, jouant le cas échéant un rôle spécifique dans le secteur auquel elle se rapporte.

CHAPITRE 3

Catégories d'entités

Art. 9

Cette disposition énumère les types d'entités qualifiées d'essentielles.

La distinction précédemment établie par la directive NIS1 entre les "opérateurs de services essentiels" (OSE) et de "fournisseurs de service numérique" (FSN) disparaît et laisse place à une distinction entre entités "essentielles" et "importantes". Désormais, cette distinction se fait en principe automatiquement sur la base de la taille de l'entité et du type d'entité concernée figurant dans l'une des deux annexes du projet de loi. Cette distinction joue un rôle important dans les régimes de supervision et d'exécution applicables à ces deux catégories d'entités, afin de garantir un juste équilibre entre les exigences

niet-limitatieve lijst van "aanbestedende overheden" als bedoeld in voornoemde wet, die is opgenomen in het koninklijk besluit plaatsing overheidsopdrachten in de klassieke sectoren van 18 april 2017.

De voorwaarden om niet hoofdzakelijk een activiteit opgesomd in de kolom soort entiteit van een andere sector of deelsector van een van de bijlagen uit te oefenen en om geen privaatrechtelijke rechtspersoon te zijn, zijn bedoeld om de overheidssector te beperken tot de administratieve overheden die publiekrechtelijke rechtspersonen zijn en die niet hoofdzakelijk een activiteit uitoefenen die al onder een andere sector van de wet valt.

Deze laatste voorwaarde zorgt er ook voor dat publieke en private entiteiten die in dezelfde sector of deelsector actief zijn, niet verschillend behandeld worden, met name wat eventueel toepasselijke administratieve sancties betreft.

In dit artikel worden ook verschillende begrippen omschreven die afkomstig zijn uit de richtlijn, om de inhoud ervan te verduidelijken (zie de definities in de punten 42°, 48°, 49°, 51° en 57° tot 59°).

Daarnaast worden in de punten 43° tot 47°, 50° en 52° tot 56° begrippen gedefinieerd die specifiek zijn voor de wet, met name de nationale cyberbeveiligingsautoriteit, aangewezen door de Koning, die een centrale rol speelt bij de uitvoering van dit wetsontwerp (zie artikel 17 en volgende hierna) of de sectorale overheid, die in voorkomend geval een specifieke rol speelt in de sector waarop zij betrekking heeft.

HOOFDSTUK 3

Categorieën van entiteiten

Art. 9

Deze bepaling somt de soorten entiteiten op die als essentieel worden beschouwd.

Het onderscheid dat voorheen in de NIS1-richtlijn werd gemaakt tussen "aanbieders van essentiële diensten" (AED's) en "digitaal dienstverleners" (DDV's) verdwijnt en wordt vervangen door een onderscheid tussen "essentiële" en "belangrijke" entiteiten. Voortaan wordt dit onderscheid in principe automatisch gemaakt op basis van de omvang van de betrokken entiteit en het soort betrokken entiteit dat in een van de twee bijlagen bij het wetsontwerp is opgenomen. Dit onderscheid speelt een belangrijke rol bij de toezichts- en handhavingsregelingen voor deze twee categorieën entiteiten, om te zorgen voor

et les obligations basées sur les risques, d'une part, et la charge administrative qui découle du contrôle de la conformité, d'autre part.

Cet article reprend le contenu de la directive NIS2 et qualifie d'essentielles les entités d'un type visé à l'annexe I qui dépassent les plafonds des entreprises moyennes; certains types d'entités actifs en matière de services de confiance ou de services de noms de domaines; les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public qui constituent au moins des moyennes entreprises; les exploitants d'infrastructures critiques au sens de la loi du 1^{er} juillet 2011; les entités publiques qui dépendent de l'État fédéral; et toute autre entité identifiée comme entité essentielle conformément à l'article 12 du présent projet de loi (voir *infra*).

Art. 10

Cette disposition énumère les types d'entités qualifiées d'importantes, à savoir les entités visées aux annexes I et II qui ne sont pas qualifiées d'essentielles sur base de l'article précédent ou qui sont identifiées comme importantes conformément à l'article 11 du présent projet de loi (voir *infra*).

CHAPITRE 4

Identification

Art. 11

Cet article permet à l'autorité nationale de cybersécurité d'identifier, en plus des entités déjà qualifiées d'essentielles ou importantes sur base des dispositions précédentes, des entités comme essentielles ou importantes, après avoir consulté l'autorité sectorielle concernée et potentiellement sur base de sa proposition (pour autant qu'une telle autorité ait été désignée pour le secteur concerné).

Le paragraphe 1^{er}, qui transpose l'article 2, § 2, b) à e), de la directive NIS2, précise les critères sur base desquels une identification peut être effectuée.

Le considérant 15 de la directive souligne que "[l]es entités qui relèvent du champ d'application de la présente directive aux fins du respect des mesures de gestion des risques en matière de cybersécurité et des obligations d'information devraient être classées en deux catégories, entités essentielles et entités importantes, en fonction de la mesure dans laquelle elles sont critiques au regard

een billijk evenwicht tussen risicogebaseerde eisen en verplichtingen enerzijds en de administratieve lasten die voortvloeien uit het toezicht op de naleving anderzijds.

Dit artikel bevat de inhoud van de NIS2-richtlijn en beschouwt de volgende entiteiten als essentiële entiteiten: entiteiten van een in bijlage I bedoelde soort die de plafonds voor middelgrote ondernemingen overschrijden; bepaalde soorten entiteiten die actief zijn op het gebied van vertrouwensdiensten of domeinnaamdiensten; aanbieders van openbare elektronische-communicatienetwerken of van openbare elektronische-communicatiediensten die minstens in aanmerking komen als middelgrote ondernemingen; exploitanten van kritieke infrastructuur als bedoeld in de wet van 1 juli 2011; overheidsinstanties die van de Federale Staat afhangen; en alle andere entiteiten die overeenkomstig artikel 12 van dit wetsontwerp worden geïdentificeerd als essentiële entiteiten (zie *infra*).

Art. 10

Deze bepaling somt de soorten entiteiten op die als "belangrijk" worden beschouwd, namelijk de entiteiten bedoeld in de bijlagen I en II die niet als essentiële entiteiten worden beschouwd op basis van het vorige artikel of die overeenkomstig artikel 11 van dit wetsontwerp als belangrijke entiteiten worden geïdentificeerd (zie *infra*).

HOOFDSTUK 4

Identificatie

Art. 11

Op grond van dit artikel kan de nationale cyberbeveiligingsautoriteit, naast de entiteiten die al op basis van de voorgaande bepalingen als essentiële of belangrijke entiteiten zijn aangemerkt, entiteiten als essentieel of belangrijk identificeren, na raadpleging van de betrokken sectorale overheid en eventueel op basis van het voorstel van die laatste (voor zover een dergelijke overheid is aangewezen voor de betrokken sector).

Paragraaf 1, die voorziet in de omzetting van artikel 2, lid 2, b) tot e), van de NIS2-richtlijn, stelt de criteria vast op basis waarvan een identificatie kan worden uitgevoerd.

Overweging 15 van de richtlijn benadrukt dat "[e]ntiteiten die voor de naleving van de maatregelen voor het beheer van cyberbeveiligingsrisico's en de rapportageverplichtingen binnen het toepassingsgebied van deze richtlijn vallen, moeten worden ingedeeld in twee categorieën, essentiële entiteiten en belangrijke entiteiten, naargelang de mate waarin zij kritiek zijn door

du secteur ou du type de service qu'elles fournissent, ainsi que de leur taille”.

L'article 2, § 2 de la directive ajoute qu'elle s'applique aux entités d'un type visé à l'annexe I ou II, quelle que soit leur taille, dans les cas suivants:

“a) les services sont fournis par:

i) des fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public;

ii) des prestataires de services de confiance;

iii) des registres des noms de domaine de premier niveau et des fournisseurs de services de système de noms de domaine;

b) l'entité est, dans un État membre, le seul prestataire d'un service qui est essentiel au maintien d'activités sociétales ou économiques critiques;

c) une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique;

d) une perturbation du service fourni par l'entité pourrait induire un risque systémique important, en particulier pour les secteurs où cette perturbation pourrait avoir un impact transfrontière.”

Il ressort des dispositions précitées que la directive tient compte, indépendamment de la taille de l'entité, dans les cas qu'elle définit, de la nature sociétale ou économique critique des activités d'une entité pour déterminer son inclusion ou non dans son champ d'application.

Le paragraphe 2 précise que l'autorité nationale de cybersécurité procède également à l'identification des administrations publiques qui dépendent des entités fédérées qui, à la suite d'une évaluation basée sur les risques, fournissent des services dont la perturbation pourrait avoir un impact important sur des activités sociétales ou économiques critiques.

En pratique, cette identification sera réalisée sur base de consultations étroites avec chaque entité fédérée. Cette dernière pourra ainsi proposer une liste des administrations publiques fournissant des services critiques et relevant de son niveau de pouvoir.

Le paragraphe 3 indique que l'autorité nationale de cybersécurité consulte les éventuelles autorités sectorielles, les entités fédérées et l'entité concerné dans le

hun sector of het soort door hen verleende diensten, alsook hun omvang.”

Art. 2, lid 2, van de richtlijn voegt hieraan toe dat de richtlijn van toepassing is op de in bijlage I of II bedoelde entiteiten, ongeacht hun omvang, wanneer:

“a) de diensten verleend worden door:

i) aanbieders van openbare elektronische communicatienetwerken of van openbare elektronische communicatiediensten;

ii) aanbieders van vertrouwensdiensten;

iii) registers voor topleveldomeinnamen en verleners van domeinnaamregistratiediensten;

b) de entiteit in een lidstaat de enige aanbieder is van een dienst die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten;

c) verstoring van de door de entiteit verleende dienst aanzienlijke gevolgen kan hebben voor de openbare veiligheid, de openbare beveiliging of de volksgezondheid;

d) verstoring van de door de entiteit verleende dienst een aanzienlijk systeemrisico met zich kan brengen, met name voor sectoren waar een dergelijke verstoring een grensoverschrijdende impact kan hebben.”

Uit de bovengenoemde bepalingen blijkt duidelijk dat de richtlijn, ongeacht de omvang van de entiteit, in de gevallen die ze definieert, rekening houdt met de kritieke sociale of economische aard van de activiteiten van een entiteit om te bepalen of deze al dan niet binnen het toepassingsgebied van de richtlijn valt.

Paragraaf 2 bepaalt dat de nationale cyberbeveiligingsautoriteit ook de overheidsinstanties die van de deelgebieden afhangen identificeert die, na een risico-beoordeling, diensten verlenen waarvan de verstoring aanzienlijke gevolgen kan hebben voor kritieke maatschappelijke of economische activiteiten.

In de praktijk zal deze identificatie gebeuren in nauw overleg nauw overleg met elk deelgebied, dat een lijst kan voorstellen van overheidsinstanties die kritieke diensten verlenen en onder zijn bevoegdheid vallen.

Paragraaf 3 licht toe dat de nationale cyberbeveiligingsautoriteit de eventuele sectorale overheden, de deelgebieden en de betrokken entiteit raadpleegt in het

cadre de la procédure d'identification. Concrètement, l'autorité nationale de cybersécurité associe dès le départ les autorités sectorielles concernées (éventuellement à l'origine de la proposition d'identification), les entités fédérées et le Centre de crise national.

Une procédure formelle d'avis de l'autorité sectorielle est mise en place. Pour des motifs liés à la sécurité public et à la procédure administrative en cours, il est mentionné explicitement que cet avis n'est pas publié. En cas d'avis défavorable de l'autorité sectorielle et si l'autorité nationale de cybersécurité souhaite maintenir son projet de décision, il est alors requis que le dossier soit soumis pour accord préalable au Comité stratégique du renseignement et de la sécurité.

Conformément à l'article 3, § 4, de la directive NIS2, l'actualisation des identifications s'effectue tous les deux ans, le cas échéant après consultation des autorités sectorielles. Il est également prévu que les identifications et actualisations sont adressées aux autorités sectorielles concernées (pour autant qu'une telle autorité ait été désignée) ainsi qu'au Centre de crise national.

La communication aux autorités sectorielles (pour autant qu'elles existent) s'explique du fait que ces autorités peuvent être compétentes pour superviser la mise en œuvre de mesures spécifiques sectorielles.

La communication au Centre national de crise et aux éventuelles autorités sectorielles permet également d'assurer une cohérence entre l'identification des entités essentielles et des entités critiques visées par la directive UE 2022/2557 du 14 décembre 2022 sur la résilience des entités critiques (directive CER).

La communication au Centre de crise nationale des identifications et actualisations visées au présent article est également prévue au vu de l'importance que revêt ces identifications dans le cadre de la gestion de crises. En effet, les incidents touchant les entités identifiées comme essentielles sont bien plus susceptibles de constituer des incidents nationaux, voire des crises nationales au sens de l'article 2 de l'arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise (ci-après: "l'AR du 18 avril 1988"), que les incidents touchant les entités identifiées comme importantes. Pour cette raison, il est important que le Centre de crise nationale, chargée de la coordination en matière de crise nationale, soit informé de l'identification et de l'actualisation d'entités essentielles.

kader van de identificatieprocedure. Concreet betekent dit dat de nationale cyberbeveiligingsautoriteit van bij het begin de betrokken sectorale overheden (die mogelijk het identificatievoorstel hebben geformuleerd), de deelgebieden en het Nationaal Crisiscentrum bij deze procedure betreft.

Er wordt een formele procedure ingevoerd om het advies van de sectorale overheid in te winnen. Om redenen die verband houden met de openbare veiligheid en de lopende administratieve procedure, wordt uitdrukkelijk vermeld dat dit advies niet wordt gepubliceerd. In geval van een ongunstig advies van de sectorale overheid en indien de nationale cyberbeveiligingsautoriteit haar ontwerpbeslissing wenst te handhaven, moet het dossier vooraf ter goedkeuring worden voorgelegd aan het Strategisch Comité voor Inlichtingen en Veiligheid.

Overeenkomstig artikel 3, lid 4, van de NIS2-richtlijn worden de identifications om de twee jaar geactualiseerd, in voorkomend geval na raadpleging van de sectorale overheden. Tevens is bepaald dat de identifications en actualisering en naar de betrokken sectorale overheden (voor zover een dergelijke overheid is aangewezen) en naar het Nationaal Crisiscentrum worden gestuurd.

De kennisgeving aan de sectorale overheden (voor zover deze bestaan) wordt verklaard door het feit dat deze overheden bevoegd kunnen zijn voor het toezicht op de uitvoering van sectorspecifieke maatregelen.

De kennisgeving aan het Nationaal Crisiscentrum en aan de eventuele sectorale overheden zorgt ook voor coherentie tussen de identificatie van de essentiële entiteiten en van kritieke entiteiten bedoeld in EU-richtlijn 2022/2557 van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten (CER-richtlijn).

De kennisgeving aan het Nationaal Crisiscentrum van de in dit artikel bedoelde identifications en actualisering is ook voorzien omdat deze identifications van belang zijn in het kader van het crisisbeheer. Incidenten die gevolgen hebben voor entiteiten die als essentiële entiteiten zijn geïdentificeerd, zijn immers veel vaker nationale incidenten of zelfs nationale crises als bedoeld in artikel 2 van het koninklijk besluit van 18 april 1988 tot oprichting van het Coördinatie- en Crisiscentrum van de regering (hierna: "het KB van 18 april 1988") dan incidenten die gevolgen hebben voor entiteiten die als belangrijke entiteiten zijn geïdentificeerd. Daarom is het belangrijk dat het Nationaal Crisiscentrum, dat belast is met de coördinatie bij nationale crises, op de hoogte wordt gebracht van de identificatie en actualisering van essentiële entiteiten.

Le paragraphe 5 prévoit la possibilité pour le Roi, par arrêté délibéré en Conseil des ministres, de désigner individuellement comme entité essentielle ou importante une entité qui ne fait pas partie des secteurs visés en annexe de la loi. En effet, une entité ou un sous-traitant particulier d'une entité NIS pourrait fournir un service critique justifiant d'être soumis aux dispositions de la loi alors que par ailleurs ses activités ne relèvent pas de l'un des secteurs repris dans les annexes de la loi. L'application de cet article est limité à des cas particuliers et implique au préalable de la décision du Comité stratégique du renseignement et de la sécurité, une concertation entre l'entité concernée, l'autorité nationale de cybersécurité, les entités fédérées et l'éventuelle autorité sectorielle.

Art. 12

Cette disposition prévoit que l'entité concernée doit transmettre toutes les informations utiles à son éventuelle identification, à la demande de l'autorité nationale de cybersécurité ou de l'autorité sectorielle lorsque cette dernière est à l'origine de la procédure.

CHAPITRE 5

Enregistrement des entités

Art. 13

Cet article organise l'enregistrement des entités essentielles et importantes auprès de l'autorité nationale de cybersécurité et détermine les informations qui doivent être renseignées par ces entités.

Pour la première fois, cet enregistrement devra être effectué dans les cinq mois de l'entrée en vigueur du présent projet de loi. Ce délai se justifie en raison du délai imposé par la directive NIS2 à l'article 3, § 3 (le 17 avril 2025). La fixation des modalités pratiques relatives à la communication de ces informations est confiée à l'autorité nationale de cybersécurité. Par rapport à ces modalités pratiques, on peut noter que la directive NIS2 précise que "les États membres devraient pouvoir mettre en place des mécanismes nationaux permettant aux entités de s'enregistrer elles-mêmes" et que, "lorsque des registres existent au niveau national, les États membres peuvent décider des mécanismes appropriés permettant d'identifier les entités relevant du champ d'application" (considérant 18 et article 3, § 4, alinéa 4, de la directive NIS2). En pratique, une plateforme, accessible par internet, sera mise à disposition des entités afin qu'elles puissent y indiquer les informations nécessaires.

Op grond van paragraaf 5 kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, een entiteit die niet tot de in de bijlagen bij de wet bedoelde sectoren behoort, individueel aanwijzen als een essentiële of belangrijke entiteit. Een entiteit of een bepaalde onderaannemer van een NIS-entiteit kan immers een kritieke dienst verlenen die rechtvaardigt dat zij of hij onderworpen is aan de bepalingen van de wet, ook al behoren haar of zijn activiteiten niet tot een van de sectoren opgenomen in de bijlagen bij de wet. De toepassing van dit artikel is beperkt tot bijzondere gevallen en houdt in dat, vóór de beslissing van het Strategisch Comité voor Inlichtingen en Veiligheid, overleg plaatsvindt tussen de betrokken entiteit, de nationale cyberbeveiligingsautoriteit, de deelgebieden en de eventuele sectorale overheid.

Art. 12

Volgens deze bepaling moet de betrokken entiteit alle informatie bezorgen die nuttig is voor haar eventuele identificatie, op verzoek van de nationale cyberbeveiligingsautoriteit of de sectorale overheid indien die laatste de procedure heeft opgestart.

HOOFDSTUK 5

Registratie van de entiteiten

Art. 13

Dit artikel regelt de registratie van essentiële en belangrijke entiteiten bij de nationale cyberbeveiligingsautoriteit, en bepaalt welke informatie door deze entiteiten moet worden verstrekt.

Deze registratie moet voor het eerst gebeuren binnen vijf maanden na de inwerkingtreding van dit wetsontwerp. Deze termijn is gerechtvaardigd gezien de termijn die is opgelegd in artikel 3, lid 3, van de NIS2-richtlijn (17 april 2025). Het vaststellen van de praktische modaliteiten voor het verstrekken van deze informatie wordt toevertrouwd aan de nationale cyberbeveiligingsautoriteit. Met betrekking tot deze praktische modaliteiten wordt opgemerkt dat de NIS2-richtlijn het volgende bepaalt: "de lidstaten [moeten] nationale mechanismen kunnen instellen voor entiteiten om zich te registreren" en "indien er registers bestaan op nationaal niveau, kunnen de lidstaten besluiten over passende mechanismen voor de identificatie van binnen het toepassingsgebied van deze richtlijn vallende entiteiten" (overweging 18 en artikel 3, lid 4, vierde alinea, van de NIS2-richtlijn). In de praktijk zal via internet een platform ter beschikking worden gesteld van de entiteiten, zodat zij hier de nodige informatie kunnen invoeren.

Afin d'assurer la mise en œuvre du principe de simplification administrative ("only once"), il est prévu qu'une entité qui a déjà communiqué à une éventuelle autorité sectorielle concernée certaines des informations, en vertu d'une obligation légale, puisse simplement compléter les informations requises auprès de cette autorité sectorielle.

Ensuite, l'autorité sectorielle concernée communique les informations collectées à l'autorité nationale de cybersécurité.

En complément de ces informations, l'autorité sectorielle transmettra sur base des éléments en sa possession une analyse de la qualification de l'entité comme essentielle ou importante.

En cas de modification des informations devant être communiquées, il appartient à l'entité concernée de notifier ces modifications à l'autorité nationale de cybersécurité ou à l'autorité sectorielle concernée.

Le paragraphe 4 prévoit que l'autorité nationale de cybersécurité prend les mesures nécessaires pour que les autorités sectorielles puissent consulter, pour les secteurs qui les concernent, les données communiquées.

Art. 14

Cet article transpose l'article 27, §§ 2, 3 et 5, de la directive NIS2. Il organise l'enregistrement pour les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les entités qui fournissent des services d'enregistrement de noms de domaine, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux et détermine les informations qui doivent être renseignées par ces entités.

Cet enregistrement devra être effectué dans les deux mois suivant l'entrée en vigueur de la loi. Ce délai est nécessaire afin de respecter l'obligation prévue à l'article 27, § 2, de la directive NIS2.

Cet article prévoit que les modalités de communication des informations sont celles prévues à l'article précédent. En effet, la directive NIS2 permet, en son article 27, § 5, que le même mécanisme peut être utilisé pour la

Om ervoor te zorgen dat het beginsel van administratieve vereenvoudiging ("only once") wordt toegepast, is voorzien dat een entiteit die al een deel van de informatie aan een eventuele betrokken sectorale overheid heeft meegedeeld krachtens een wettelijke verplichting, de vereiste informatie gewoon kan aanvullen bij deze sectorale overheid.

Vervolgens bezorgt de betrokken sectorale overheid de ingezamelde informatie aan de nationale cyberbeveiligingsautoriteit.

Naast deze informatie bezorgt de sectorale overheid, op basis van de elementen waarover zij beschikt, een analyse volgens dewelke de entiteit als essentieel of belangrijk wordt aangemerkt.

Indien de te verstrekken informatie wijzigt, moet de betrokken entiteit deze wijzigingen aan de nationale cyberbeveiligingsautoriteit of aan de betrokken sectorale overheid melden.

Paragraaf 4 bepaalt dat de nationale cyberbeveiligingsautoriteit de nodige maatregelen neemt om ervoor te zorgen dat de sectorale overheden de verstrekte gegevens kunnen raadplegen voor de sectoren die hen aangaan.

Art. 14

Dit artikel voorziet in de omzetting van artikel 27, leden 2, 3 en 5, van de NIS2-richtlijn. Het regelt de registratie voor DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputing-diensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsook aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor sociale netwerkdiensten, en bepaalt welke informatie door deze entiteiten moet worden verstrekt.

Deze registratie dient te gebeuren binnen twee maanden na de inwerkingtreding van de wet. Deze termijn is nodig om te voldoen aan de verplichting waarvan sprake in artikel 27, lid 2, van de NIS2-richtlijn.

Dit artikel bepaalt dat de modaliteiten voor het verstrekken van informatie dezelfde zijn als in het vorige artikel. Op basis van artikel 27, lid 5, van de NIS2-richtlijn kunnen de in dit artikel bedoelde entiteiten en de in

communication d'informations par les entités visées à cet article et les entités visées à l'article 14 du projet de loi.

D'une manière similaire à l'article précédent, le paragraphe 2 impose aux entités concernées de notifier toute modification des informations devant être communiquées à l'autorité nationale de cybersécurité.

Une exception est prévue au paragraphe 3 en ce qui concerne les prestataires de services de confiance qualifiés afin de garantir le respect du principe de collecte unique des données.

TITRE 2

Autorités compétentes et coopération au niveau national

CHAPITRE 1^{ER}

Autorités compétentes

Section 1^{re}

Désignation des autorités compétentes

Art. 15

Cet article désigne les autorités compétentes dans le cadre du présent projet de loi, le cas échéant au travers d'une désignation par le Roi.

L'autorité envisagée pour remplir le rôle d'autorité nationale de cybersécurité est le Centre pour la Cybersécurité Belgique. Il n'est pas directement cité dans la loi car, comme a déjà pu le préciser la section de législation du Conseil d'État, notamment dans l'avis 63.296/4, désigner directement des services du pouvoir exécutif créés par le Roi et qui dépendent de Lui serait une immixtion du pouvoir législatif dans l'organisation interne du pouvoir exécutif.

C'est en principe au Roi qu'il revient de désigner l'administration chargée d'exécuter les missions de l'autorité nationale de cybersécurité.

Le rôle et les tâches de l'autorité nationale de cybersécurité sont décrits aux articles suivants (voir *infra*).

Le paragraphe 2 laisse au Roi la possibilité de nommer des autorités sectorielles et/ou des services d'inspection

artikel 14 van het wetsontwerp bedoelde entiteiten immers hetzelfde mechanisme gebruiken voor het verstrekken van informatie.

Op vergelijkbare wijze als in het vorige artikel verplicht paragraaf 2 de betrokken entiteiten om de nationale cyberbeveiligingsautoriteit in kennis te stellen van elke wijziging van de te verstrekken informatie.

Paragraaf 3 voorziet in een uitzondering voor gekwalificeerde verleners van vertrouwensdiensten om de naleving van het beginsel van de unieke gegevensinzameling te waarborgen.

TITEL 2

Bevoegde autoriteiten en samenwerking op nationaal niveau

HOOFDSTUK 1

Bevoegde autoriteiten

Afdeling 1

Aanwijzing van de bevoegde autoriteiten

Art. 15

In dit artikel worden de autoriteiten aangewezen die in het kader van dit wetsontwerp bevoegd zijn, in voorkomend geval door middel van een aanwijzing door de Koning.

De autoriteit die de rol van nationale cyberbeveiligingsautoriteit moet vervullen, is het Centrum voor Cybersecurity België. Het wordt niet rechtstreeks in de wet vermeld omdat, zoals de afdeling Wetgeving van de Raad van State al heeft opgemerkt, met name in advies 63.296/4, het rechtstreeks aanwijzen van de diensten van de uitvoerende macht die door de Koning zijn opgericht en op Hem aangewezen zijn, een inmenging van de wetgevende macht in de interne organisatie van de uitvoerende macht zou zijn.

In principe is het aan de Koning om te bepalen welke administratie verantwoordelijk is voor het uitvoeren van de opdrachten van de nationale cyberbeveiligingsautoriteit.

De rol en de taken van de nationale cyberbeveiligingsautoriteit worden beschreven in de volgende artikelen (zie *infra*).

Paragraaf 2 biedt de Koning de mogelijkheid om sectorale overheden en/of sectorale inspectiediensten

sectoriels, après avis de l'autorité nationale de cybersécurité, pour autant que les autorités envisagées ne soient pas créées par la loi, auquel cas il revient à la loi de les désigner. Le cas échéant, selon les secteurs, le Roi peut créer des autorités composées de représentants de l'État fédéral et des entités fédérées, conformément à l'article 92^{ter} de la loi du 8 août 1980.

La disposition prévoit que le Roi, dans le cadre de la désignation des autorités sectorielles et/ou des services d'inspections sectoriels, tient compte des autorités sectorielles désignées conformément à la loi de 1^{er} juillet 2011. La directive NIS2 insiste à plusieurs reprises sur le fait que les autorités compétentes dans le cadre de la directive NIS2 et de la directive CER devraient coopérer de manière étroite.

Section 2

L'autorité nationale de cybersécurité

Art. 16

Cet article décrit le rôle de l'autorité nationale de cybersécurité.

L'objectif est de créer une autorité centralisant les compétences en matière de cybersécurité, avec un rôle particulièrement important dans la mise en œuvre du présent projet de loi. Au sens de la directive NIS2, l'autorité nationale de cybersécurité est:

1° l'autorité compétente, chargée de la cybersécurité, des tâches de supervision et de contrôler la mise en œuvre de la directive en Belgique (article 8, §§ 1 et 2, de la directive NIS2), à l'exception de la mise en œuvre de l'article 34 du présent projet de loi qui revient, le cas échéant, aux autorités sectorielles et/ou aux services d'inspection sectoriels;

2° le point de contact unique, exerçant une fonction de liaison visant à assurer la coopération transfrontière des autorités belges avec les autorités compétentes des autres États membres et, le cas échéant, avec la Commission et l'ENISA, ainsi qu'à garantir la coopération intersectorielle avec les autres autorités compétentes en Belgique (article 8, § 4, de la directive NIS2);

3° le CSIRT national, c'est-à-dire le centre national de réponse aux incidents de sécurité informatique, chargé de la gestion des incidents;

aan te wijzen, na advies van de nationale cyberbeveiligingsautoriteit, voor zover de autoriteiten in kwestie niet bij wet zijn opgericht, in welk geval het aan de wet toekomt om ze aan te wijzen. In voorkomend geval kan de Koning, naargelang de sector, autoriteiten oprichten die bestaan uit vertegenwoordigers van de Federale Staat en de deelgebieden, overeenkomstig artikel 92^{ter} van de wet van 8 augustus 1980.

De bepaling voorziet dat de Koning, in het kader van de aanwijzing van sectorale overheden en/of sectorale inspectiediensten, rekening houdt met de sectorale overheden die overeenkomstig de wet van 1 juli 2011 zijn aangewezen. In de NIS2-richtlijn wordt herhaaldelijk benadrukt dat de autoriteiten die in het kader van de NIS2-richtlijn en de CER-richtlijn bevoegd zijn, nauw moeten samenwerken.

Afdeling 2

De nationale cyberbeveiligingsautoriteit

Art. 16

In dit artikel wordt de rol van de nationale cyberbeveiligingsautoriteit beschreven.

Doel is om een autoriteit op te richten die de bevoegdheden op het gebied van cyberbeveiliging centraliseert, met een bijzonder belangrijke rol bij de uitvoering van dit wetsontwerp. In de zin van de NIS2-richtlijn is de nationale cyberbeveiligingsautoriteit:

1° de bevoegde autoriteit die verantwoordelijk is voor cyberbeveiliging, toezichhoudende taken en het monitoren van de tenuitvoerlegging van de richtlijn in België (artikel 8, leden 1 en 2, van de NIS2-richtlijn), met uitzondering van de uitvoering van artikel 34 van dit wetsontwerp, waarmee, in voorkomend geval, de sectorale overheden en/of sectorale inspectiediensten belast zijn;

2° het centrale contactpunt, dat een verbindingfunctie vervult om te zorgen voor grensoverschrijdende samenwerking van de Belgische autoriteiten met de relevante autoriteiten van andere lidstaten en in voorkomend geval met de Commissie en Enisa, alsook om te zorgen voor sectoroverschrijdende samenwerking met andere bevoegde autoriteiten in België (artikel 8, lid 4, van de NIS2-richtlijn);

3° het nationale CSIRT, d.w.z. het nationale computer security incident response team, dat verantwoordelijk is voor de behandeling van incidenten;

4° sans préjudice des dispositions nationales existantes en matière de gestion de crise, et plus précisément des compétences du Centre de crise national et du ministre de l'Intérieur, l'autorité chargée de la gestion des incidents de cybersécurité et crises cyber;

5° représentant de la Belgique dans le cadre de la coopération internationale organisée par la directive NIS2. L'autorité nationale de cybersécurité est notamment représentante de la Belgique au sein du groupe de coopération (article 14 de la directive NIS2), au sein de EU-CyCLONe (article 16, § 2, de la directive NIS2) et au sein du réseau des CSIRT (article 15 de la directive NIS2).

Sous-section 1^{re}

Tâches relatives au rôle d'autorité compétente chargée de la cybersécurité

Art. 17

Cet article énumère les tâches de l'autorité nationale de cybersécurité en sa qualité d'autorité compétente, chargée de veiller à la mise en œuvre du présent projet de loi.

Cette disposition reprend, en plus des tâches découlant de la directive NIS2, les tâches existantes dévolues au Centre pour la Cybersécurité Belgique telles que la gestion, par une approche intégrée et centralisée, des différents projets relatifs à la cybersécurité; la coordination entre les autorités publiques et le secteur privé ou le monde scientifique; la formulation de propositions pour l'adaptation du cadre légal et réglementaire en matière de cybersécurité; l'élaboration, la diffusion et la mise en œuvre des standards, directives et normes de sécurité pour les différents types de systèmes d'information; la coordination de la représentation belge aux forums internationaux sur la cybersécurité, du suivi des obligations internationales et de la présentation du point de vue national en la matière.

Afin d'assurer la coordination entre les autorités compétentes dans le cadre de l'application de la présente loi, ainsi qu'entre les différents services et autorités concernés par la cybersécurité en Belgique, l'autorité nationale de cybersécurité développera une connaissance spécifique aux différentes entités actives dans les secteurs visés par la loi.

Parmi ses tâches, l'autorité nationale de cybersécurité a également la possibilité d'accorder des subventions pour autant que cela soit possible au travers des crédits

4° onverminderd de bestaande nationale bepalingen inzake crisisbeheer, en meer bepaald de bevoegdheden van het Nationaal Crisiscentrum en van de minister van Binnenlandse Zaken, de autoriteit die verantwoordelijk is voor de behandeling van cyberbeveiligingsincidenten en cybercrises;

5° de vertegenwoordiger van België in het kader van de internationale samenwerking georganiseerd door de NIS2-richtlijn. De nationale cyberbeveiligingsautoriteit vertegenwoordigt België met name in de samenwerkingsgroep (artikel 14 van de NIS2-richtlijn), in EU-CyCLONe (artikel 16, lid 2, van de NIS2-richtlijn) en in het CSIRT-netwerk (artikel 15 van de NIS2-richtlijn).

Onderafdeling 1

Taken met betrekking tot de rol van bevoegde autoriteit belast met cyberbeveiliging

Art. 17

In dit artikel worden de taken opgesomd van de nationale cyberbeveiligingsautoriteit in haar hoedanigheid van bevoegde autoriteit die verantwoordelijk is voor de uitvoering van dit wetsontwerp.

Naast de taken die voortvloeien uit de NIS2-richtlijn, bevat deze bepaling de bestaande taken van het Centrum voor Cybersecurity België, zoals het beheer, vanuit een geïntegreerde en gecentraliseerde aanpak, van de verschillende projecten op het vlak van cyberbeveiliging; de coördinatie tussen overheden en de private sector of de wetenschappelijke wereld; het formuleren van voorstellen tot aanpassing van het wettelijk en regelgevend kader inzake cyberbeveiliging; het opstellen, verspreiden en uitvoeren van beveiligingsstandaarden, -richtlijnen en -normen voor de verschillende soorten informatiesystemen; het coördineren van de Belgische vertegenwoordiging in internationale fora voor cyberbeveiliging, van de opvolging van internationale verplichtingen en van voorstellen van het nationale standpunt op dit vlak.

Om de coördinatie te verzekeren tussen de bevoegde autoriteiten in het kader van de toepassing van deze wet, alsook tussen de verschillende diensten en autoriteiten die betrokken zijn bij cyberveiligheid in België, zal de nationale cyberbeveiligingsautoriteit specifieke kennis ontwikkelen van de verschillende entiteiten die actief zijn in de sectoren die onder de wet vallen.

Een van de taken van de nationale cyberbeveiligingsautoriteit bestaat er tevens in subsidies toe te kennen, voor zover dit mogelijk is via de begrotingskredieten

budgetaires de l'année en cours et que les conditions d'octroi aient été fixées au préalable par le Roi. Ces subventions, pour autant que des crédits y soient alloués, doivent notamment pouvoir aider les petites et moyennes entreprises à mettre en œuvre les obligations qui découlent du présent projet de loi.

Sous-section 2

Tâches relatives au rôle de gestion des crises cyber

Art. 18

Cet article transpose l'article 9, §§ 1^{er} et 2, de la directive NIS2. Il établit les tâches dévolues à l'autorité nationale de cybersécurité en sa qualité d'autorité compétente en matière de gestion de crises cyber et incidents de cybersécurité. Il est spécifiquement rappelé que ces tâches sont dévolues à l'autorité nationale de cybersécurité sans préjudice des compétences du Centre de crise national, lequel reste notamment responsable de la coordination en cas de crise nationale au sens de l'article 2 de l'arrêté royal du 18 avril 1988. Dans le cadre d'une gestion de crise cohérente, il est en effet absolument nécessaire, dès lors qu'une crise nécessite la coordination de plusieurs départements et organismes (gestion multidisciplinaire d'une crise), que cette coordination soit assurée par le Centre de crise national.

Plusieurs tâches en matière de gestion de crises cyber et incidents de cybersécurité sont d'ailleurs effectués en collaboration avec le Centre de crise national car cette autorité joue un rôle centrale dans la coordination dans le cadre de la gestion de crises.

Sous-section 3

Tâches et obligations relatives au rôle de CSIRT national

Art. 19

Cet article énumère les tâches de l'autorité nationale de cybersécurité en sa qualité de CSIRT national. Il transpose l'article 11, §§ 3 à 5, de la directive NIS2 et reprend les tâches déjà dévolues au CISRT national sur base de la loi NIS1.

Conformément au paragraphe 2, transposant l'article 11, § 3, alinéa 3, de la directive NIS2, le CSIRT national peut prioriser certaines de ses tâches par

van het lopende jaar en de toekenningsvoorwaarden vooraf zijn vastgesteld door de Koning. Deze subsidies, voor zover er kredieten aan zijn toegekend, moeten met name kleine en middelgrote ondernemingen helpen om de verplichtingen die voortvloeien uit dit wetsontwerp uit te voeren.

Onderafdeling 2

Taken met betrekking tot het cybercrisisbeheer

Art. 18

Dit artikel voorziet in de omzetting van artikel 9, leden 1 en 2, van de NIS2-richtlijn. Het bepaalt de taken van de nationale cyberbeveiligingsautoriteit in haar hoedanigheid van autoriteit die verantwoordelijk is voor het beheer van cybercrises en cyberbeveiligingsincidenten. Er wordt specifiek op gewezen dat deze taken worden toevertrouwd aan de nationale cyberbeveiligingsautoriteit, zonder afbreuk te doen aan de bevoegdheden van het Nationaal Crisiscentrum, dat met name bevoegd blijft voor de coördinatie in geval van een nationale crisis in de zin van artikel 2 van het koninklijk besluit van 18 april 1988. In het kader van een coherente crisisbeheersing is het daarom absoluut noodzakelijk dat, wanneer een crisis de coördinatie van meerdere diensten en instanties vereist, deze coördinatie wordt uitgevoerd door het Nationaal Crisiscentrum (multidisciplinair crisisbeheer).

Verschillende taken met betrekking tot het beheer van cybercrises en cyberbeveiligingsincidenten worden bovendien uitgevoerd in samenwerking met het Nationaal Crisiscentrum, aangezien deze autoriteit een centrale rol speelt bij de coördinatie in het kader van het crisisbeheer.

Onderafdeling 3

Taken en voorschriften met betrekking tot de rol van nationaal CSIRT

Art. 19

In dit artikel worden de taken opgesomd van de nationale cyberbeveiligingsautoriteit in haar hoedanigheid van nationaal CSIRT. Het voorziet in de omzetting van artikel 11, leden 3 tot 5, van de NIS2-richtlijn en bevat de taken die al op basis van de NIS1-wet aan het nationale CISRT zijn toegewezen.

Overeenkomstig paragraaf 2, dat voorziet in de omzetting van artikel 11, lid 3, derde alinea, van de NIS2-richtlijn, kan het nationale CSIRT, op grond van een

rapport à d'autres, sur base d'une approche basée sur les risques.

Comme cela lui est déjà permis dans le cadre de la loi NIS1, le CSIRT national peut procéder à un scan proactif et non intrusif des réseaux et systèmes d'information accessibles au public lorsque ce scan est effectué dans le but de détecter les réseaux et systèmes d'information vulnérables ou configurés de façon peu sûre et d'informer les entités concernées et qu'il n'a pas d'effet négatif sur le fonctionnement des services des entités. L'objectif poursuivi est d'avertir le responsable du système vulnérable afin que celui-ci puisse se protéger avant la survenance d'un incident.

La réalisation d'un scan non intrusif de réseaux et systèmes d'information accessibles au public consiste concrètement à rechercher les ports ouverts sur un serveur de réseau ou un système informatique dans le but de détecter des vulnérabilités ou défauts de configuration, lesquels pourraient être utilisés par des personnes malveillantes. En effet, la détection de vulnérabilités nécessite une certaine forme d'interaction avec les ports des systèmes informatiques concernés. Il n'est toutefois pas recueilli plus d'informations sur le système d'information que nécessaire pour déterminer l'existence d'une vulnérabilité et alerter le responsable du système affecté.

Les réseaux et systèmes d'information accessibles au public sont ceux qui sont connectés à internet et auxquels un utilisateur peut avoir accès à distance. L'absence d'effet négatif sur le fonctionnement des services des entités concernés implique que le recueil de ces informations est réalisé sans causer de dommages aux réseaux et systèmes d'informations concernés.

Enfin, l'utilisation de cette méthode de recherche de vulnérabilités par le CSIRT national depuis plusieurs années a permis de protéger nombreuses organisations en Belgique et n'a pas causé de problème technique aux organisations concernées.

Art. 20

Cet article transpose l'article 11, § 1^{er}, de la directive NIS2 et reprend les obligations auxquelles doit satisfaire le CSIRT national.

Comme le prévoit le considérant 41 de la directive NIS2, *“les CSIRT devraient se conformer aux exigences établies dans la présente directive afin de garantir l'existence de moyens effectifs et compatibles pour gérer les*

risicogebaseerde benadering, prioriteit geven aan sommige van zijn taken.

Zoals reeds toegestaan in het kader van de NIS1-wet, kan het nationale CSIRT overgaan tot het proactief en niet-intrusief scannen van openbaar toegankelijke netwerk- en informatiesystemen, wanneer een dergelijk scannen wordt uitgevoerd om kwetsbare of onveilig geconfigureerde netwerk- en informatiesystemen op te sporen en de betrokken entiteiten te informeren. Het scannen mag geen negatieve gevolgen hebben voor de werking van de diensten van de entiteiten. Het is de bedoeling om de verantwoordelijke van het kwetsbare systeem te verwittigen zodat hij zich kan beschermen voordat er een incident plaatsvindt.

Bij het niet-intrusief scannen van openbaar toegankelijke netwerk- en informatiesystemen wordt concreet gezocht naar open poorten op een netwerkserver of in een informaticasysteem om kwetsbaarheden of configuratiefouten op te sporen die door kwaadwillende personen kunnen worden gebruikt. Het opsporen van kwetsbaarheden vereist immers een zekere vorm van interactie met de poorten van de betrokken informatiesystemen. Er wordt evenwel niet meer informatie over het informatiesysteem verzameld dan nodig is om het bestaan van een kwetsbaarheid vast te stellen en de verantwoordelijke van het getroffen systeem te waarschuwen.

Openbaar toegankelijke netwerk- en informatiesystemen zijn verbonden met het internet en vanop afstand toegankelijk voor gebruikers. Het verzamelen van deze informatie mag geen negatieve gevolgen hebben voor de werking van de diensten van de betrokken entiteiten, en dus geen schade aan de betrokken netwerk- en informatiesystemen veroorzaken.

Tot slot heeft deze methode die het nationale CSIRT al een aantal jaren gebruikt voor het scannen op kwetsbaarheden, veel organisaties in België beschermd en geen technische problemen veroorzaakt voor de betrokken organisaties.

Art. 20

Dit artikel voorziet in de omzetting van artikel 11, lid 1, van de NIS2-richtlijn en bevat de voorschriften waaraan het nationale CSIRT moet voldoen.

Zoals bepaald in overweging 41 van de NIS2-richtlijn moeten *“de CSIRT's [...] voldoen aan de in deze richtlijn vastgestelde eisen om te garanderen dat zij over doeltreffende en compatibele capaciteiten beschikken*

incidents et les risques et d'assurer une coopération efficace au niveau de l'Union".

Art. 21

Cette disposition reprend le contenu de l'article 62 de la loi NIS1.

L'article précise que le CSIRT national prendra toutes les mesures adéquates, proportionnelles et prudentes afin de réaliser ses missions légales. Cette disposition permet, si nécessaire, au CSIRT national de déroger à certaines dispositions du Code pénal pour l'exécution de ses missions légales, par application de l'article 70 du Code pénal. Cela étant, les compétences du CSIRT national ne portent pas préjudice aux compétences des procureurs, des juges d'instruction, des officiers de police judiciaire ou de toute autre personne exerçant la police judiciaire. Par ailleurs, les compétences du CSIRT national ne peuvent violer le secret de l'information ni le secret de l'instruction.

De plus, la disposition permet au CSIRT national, dans le respect des conditions imposées et poursuivant certains objectifs précis, de demander des données relatives à l'utilisateur ou à l'abonné visées à l'article 2, alinéa 1^{er}, 5°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ou des métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi du 13 juin 2005 relative aux communications électroniques auprès des opérateurs de communications électroniques, lorsque cela s'avère strictement nécessaire à la réalisation de certaines de ses tâches (la diffusion d'informations sur les risques et incidents en matière de sécurité des réseaux et systèmes d'information, l'intervention en cas d'incident, l'analyse dynamique des risques et incidents, ainsi que la détection, l'observation et l'analyse des problèmes de sécurité informatique).

Cette habilitation découle de la loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, afin de mener à bien ses missions dans le cadre de la prévention et de la détection des infractions en matière de cybercriminalité, de la prévention de menaces contre la sécurité publique liées à la cybersécurité ainsi que de l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques.

om incidenten en risico's aan te pakken en om een efficiënte samenwerking op het niveau van de Unie te waarborgen".

Art. 21

Deze bepaling bevat de inhoud van artikel 62 van de NIS1-wet.

Het artikel verduidelijkt dat het nationale CSIRT alle passende, evenredige en behoedzame maatregelen zal nemen om zijn wettelijke opdrachten te verwezenlijken. Deze bepaling laat het nationale CSIRT indien nodig toe om af te wijken van sommige bepalingen van het Strafwetboek voor de uitvoering van zijn wettelijke opdrachten, met toepassing van artikel 70 van het Strafwetboek. De bevoegdheden van het nationale CSIRT doen echter geen afbreuk aan de bevoegdheden van procureurs, onderzoeksrechters, officieren van gerechtelijke politie of andere personen die de gerechtelijke politie uitoefenen. Voorts mogen de bevoegdheden van het nationale CSIRT het geheim van het opsporingsonderzoek en gerechtelijk onderzoek niet schenden.

Bovendien laat de bepaling het nationale CSIRT toe om, met inachtneming van de opgelegde voorwaarden en met het oog op bepaalde specifieke doelstellingen, gegevens op te vragen betreffende de gebruiker of abonnee, als bedoeld in artikel 2, eerste lid, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, of elektronische-communicatiemetagegevens als bedoeld in artikel 2, 93°, van de wet van 13 juni 2005 betreffende de elektronische communicatie bij elektronische-communicatieoperatoren, indien dat strikt noodzakelijk is voor de uitvoering van sommige van zijn taken (verspreiding van informatie over risico's en incidenten in verband met de beveiliging van netwerk- en informatiesystemen, reageren op incidenten, zorgen voor een dynamische risico- en incidentanalyse, alsook het opsporen, observeren en analyseren van computerbeveiligingsproblemen).

Deze machtiging vloeit voort uit de wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, om zijn opdrachten uit te voeren in het kader van het voorkomen en opsporen van misdrijven inzake cybercriminaliteit, het voorkomen van bedreigingen voor de openbare veiligheid in verband met cyberbeveiliging en het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten.

Il s'agit pour le CSIRT national de protéger les entités essentielles et importantes au sens du présent projet de loi, dont font partie, au moins partiellement, les autorités publiques.

En ce qu'ils affectent des acteurs essentiels de secteurs clés, en ce compris les pouvoirs publics, ces incidents constituent des menaces graves pour la sécurité publique.

Le CSIRT national joue également un rôle de prévention, de recherche et de détection en matière d'infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave. Il doit être en mesure, le cas échéant, d'obtenir des différents opérateurs, des données de communications électroniques afin d'accomplir ses missions légales. Les finalités poursuivies par ces différentes tâches sont énumérées au paragraphe 2, alinéa 2. Il s'agit notamment de la prévention de menaces graves contre la sécurité publique, de l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information, de la prévention et, le cas échéant, la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques. La détection et la recherche des infractions seront effectuées par les services de police, avec le soutien éventuel du CERT en tant qu'expert.

Art. 22

Cet article transpose l'article 12 de la directive NIS2 et reprend les éléments déjà existants à l'article 62/1 de la loi NIS1, tel qu'inséré par la loi du 28 novembre 2022 relative à la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé.

La disposition prévoit que le CSIRT national est coordinateur aux fins de la divulgation coordonnée des vulnérabilités. Il fait office d'intermédiaire de confiance et de facilitateur entre la personne physique ou morale qui signale une potentielle vulnérabilité et le fabricant ou le fournisseur des produits TIC ou des services TIC potentiellement vulnérables, à la demande de l'une des deux parties.

L'importance croissante des réseaux et systèmes d'information au sein de nos sociétés augmente considérablement le risque d'être confronté à des incidents liés à la sécurité de ceux-ci. Ces incidents peuvent, par exemple, avoir pour conséquence d'affecter la

Doel van het nationale CSIRT is het beschermen van de essentiële en belangrijke entiteiten als bedoeld in dit wetsontwerp, waartoe, ten minste gedeeltelijk, de overheidsinstanties behoren.

Aangezien deze incidenten essentiële spelers in sleutelsectoren, waaronder overheden, treffen, vormen ze een ernstige bedreiging voor de openbare veiligheid.

Het nationale CSIRT speelt ook een rol bij het voorkomen, onderzoeken en opsporen van misdrijven die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten. Het moet in voorkomend geval elektronische-communicatiegegevens kunnen verkrijgen van de verschillende operatoren om zijn wettelijke opdrachten uit te voeren. De doeleinden van deze verschillende taken worden opgesomd in paragraaf 2, tweede lid. Het gaat met name om het voorkomen van ernstige bedreigingen voor de openbare veiligheid, het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten of informatiesystemen, en het voorkomen en desgevallend opsporen van inbreuken die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd. Het opsporen en onderzoeken van misdrijven zal door de politieke diensten gebeuren, al dan niet met steun als expert door het CERT.

Art. 22

Dit artikel voorziet in de omzetting van artikel 12 van de NIS2-richtlijn en bevat de al bestaande elementen van artikel 62/1 van de NIS1-wet, zoals ingevoegd bij de wet van 28 november 2022 betreffende de bescherming van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de private sector.

De bepaling verduidelijkt dat het nationale CSIRT de coördinator is met het oog op een gecoördineerde bekendmaking van kwetsbaarheden. Het treedt op als betrouwbare tussenpersoon en vergemakkelijkt de interactie tussen de natuurlijke of rechtspersoon die een mogelijke kwetsbaarheid meldt enerzijds en de fabrikant of aanbieder van de mogelijk kwetsbare ICT-producten of -diensten anderzijds, op verzoek van een van beide partijen.

Het toenemende belang van netwerk- en informatiesystemen in onze samenleving leidt tot een veel hoger risico op incidenten in verband met de beveiliging van deze systemen. Deze incidenten kunnen bijvoorbeeld gevolgen hebben voor de beschikbaarheid van een

disponibilité d'un service fourni, l'intégrité, l'authenticité, ou la confidentialité de données.

Parmi les causes de ces incidents, l'existence de vulnérabilités constitue un risque majeur. Une "vulnérabilité" est définie à l'article 8, 15° comme: une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace. Celui-ci est toutefois inhérent au processus de développement, d'utilisation et de mise à jour de ces systèmes. Ces vulnérabilités peuvent être détectées tant par des personnes bien intentionnées que par des personnes mal intentionnées. Les "hackers éthiques" souhaitent eux contribuer à l'amélioration de la sécurité des technologies de l'information en identifiant les vulnérabilités existantes et en aidant à les résoudre.

Compte tenu de l'ampleur et de la technicité de ce problème, le rôle sociétal de ces "hackers éthiques" est important.

Or, un hacker éthique peut, dans certaines circonstances, remplir le rôle "lanceur d'alerte numérique" pour les vulnérabilités en matière de technologies de l'information et de la communication. À ce titre, il mérite de se voir reconnaître, moyennant le respect de certaines conditions, une protection légale, indépendamment de l'existence d'une politique de divulgation coordonnée des vulnérabilités ou des mesures adoptées par le responsable du système informatique.

Le paragraphe 2 autorise le signalement, le cas échéant anonyme, de l'existence d'une potentielle vulnérabilité. La procédure pour ce faire doit être décrite par le CSIRT national et mis à disposition en ligne.

Le troisième paragraphe dispose que le CSIRT national est tenu de préserver l'exhaustivité, l'intégrité, le stockage durable et la confidentialité des informations transmises au travers du signalement, ainsi que de l'identité de la personne à l'origine de la transmission, (lorsque le signalement n'est pas anonyme). L'auteur du signalement ne doit dès lors pas craindre, par exemple, que le CSIRT national transmette son identité à d'autres autorités publiques, quand il a demandé à rester anonyme et a respecté les conditions visées à l'article suivant.

De plus, l'accès à ces informations doit demeurer limité aux personnes habilitées par le directeur général du CSIRT national. Cette alinéa ne fait pas préjudice à l'exécution des missions légales du CSIRT national énumérées à l'article 20 et qui impliquerait le partage

verleende dienst of voor de integriteit, authenticiteit of vertrouwelijkheid van gegevens.

Wat de oorzaken van deze incidenten betreft, vormt het bestaan van kwetsbaarheden een groot risico. Een "kwetsbaarheid" wordt in artikel 8, 15°, gedefinieerd als een zwakte, vatbaarheid of gebrek van ICT-producten of ICT-diensten die door een cyberdreiging kan worden uitgebuit. Dit risico is echter inherent aan het ontwikkelings-, gebruiks- en updateproces van deze systemen. Zowel mensen met goede bedoelingen als mensen met slechte bedoelingen kunnen deze kwetsbaarheden opsporen. "Ethische hackers" willen bijdragen aan een betere beveiliging van informatietechnologieën door bestaande kwetsbaarheden op te sporen en ze te helpen oplossen.

Rekening houdend met de omvang en techniciteit van dit probleem is de maatschappelijke rol van deze "ethische hackers" belangrijk.

In bepaalde omstandigheden kunnen ethische hackers echter de rol van "digitale klokkenluider" vervullen voor kwetsbaarheden inzake informatie- en communicatietechnologie. Hierbij moeten zij onder bepaalde voorwaarden wettelijke bescherming genieten, ongeacht het bestaan van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden of de maatregelen genomen door de verantwoordelijke van het informaticasysteem.

Krachtens paragraaf 2 mag, in voorkomend geval anoniem, het bestaan van een mogelijke kwetsbaarheid worden gemeld. De procedure hiervoor moet door het nationale CSIRT worden beschreven en online beschikbaar worden gesteld.

De derde paragraaf bepaalt dat het nationale CSIRT de volledigheid, integriteit, duurzame opslag en geheimhouding moet waarborgen van de via de melding overgemaakte informatie, alsook van de identiteit van de persoon die de informatie heeft overgemaakt (wanneer de melding niet anoniem is). Melders hoeven dus bijvoorbeeld niet te vrezen dat het nationale CSIRT hun identiteit aan andere overheidsinstanties zou doorgeven, wanneer zij gevraagd hebben anoniem te blijven en de in het volgende artikel bedoelde voorwaarden hebben nageleefd.

Bovendien moet de toegang tot deze informatie beperkt blijven tot de personen die daartoe door de directeur-generaal van het nationale CSIRT gemachtigd zijn. Dit lid doet geen afbreuk aan de uitvoering van de in artikel 20 opgesomde wettelijke opdrachten van het

des informations techniques issues du signalement avec d'autres autorités publiques.

Le quatrième paragraphe autorise, dans le respect des conditions énumérées à l'article 21, §§ 1^{er} et 4, le CSIRT national à utiliser éventuellement des méthodes d'observation, d'étude et de test des mesures de sécurité d'un système d'information ou d'un réseau afin de déterminer l'existence d'une vulnérabilité potentielle et de vérifier les méthodes utilisées par l'auteur d'un signalement. Il peut s'agir notamment de méthodes d'ingénierie inversée (en anglais, reverse engineering).

Le cinquième paragraphe dispose que le CSIRT national doit coopérer avec les CSIRT des autres États membres lorsqu'une vulnérabilité signalée (que ce soit au travers d'une divulgation coordonnée ou d'un signalement) est susceptible d'avoir un impact significatif sur des entités dans plusieurs États membres.

Enfin, le sixième paragraphe prévoit que le directeur général du CSIRT national doit veiller au respect des conditions précitées par l'adoption de procédures internes.

Art. 23

La disposition a pour objectif de créer, dans certaines conditions strictes, un cadre protecteur ("*safe harbour*") pour les "hackers éthiques" ou "lanceurs d'alerte numériques", auteurs d'un signalement auprès du CSIRT national.

Afin de bénéficier de cette protection, il faut que les lanceurs d'alerte numériques respectent la procédure prévue par l'article 22 et les conditions énoncées par le présent article.

Premièrement, l'auteur du signalement (ci-après le hacker éthique) ne peut utiliser ses recherches pour des motifs frauduleux ou dans l'intention de nuire. Par exemple, celui-ci ne peut tenter de monnayer les informations découvertes auprès de l'organisation responsable (en l'absence d'un programme de récompense prédéfini) ou de tiers. De même, le hacker éthique ne peut utiliser à son profit la vulnérabilité découverte.

Deuxièmement, le hacker éthique (personne physique ou morale) doit avoir informé l'organisation concernée sans délai et au plus tard dans les 24 heures de la découverte d'une potentielle vulnérabilité.

Troisièmement, le hacker éthique doit adresser à l'organisation et au CSIRT national une notification

nationale CSIRT, waarbij technische informatie uit de melding met andere overheidsinstanties zou worden gedeeld.

Krachtens de vierde paragraaf mag het nationale CSIRT, met inachtneming van de voorwaarden opgesomd in artikel 21, leden 1 en 4, eventueel gebruikmaken van methoden voor het observeren, onderzoeken en testen van de beveiligingsmaatregelen van een netwerk- of informatiesysteem, om te bepalen of er sprake is van een mogelijke kwetsbaarheid en de door de melder gebruikte methoden na te gaan. Hierbij kunnen met name reverse engineering-methoden worden aangewend.

De vijfde paragraaf bepaalt dat het nationale CSIRT moet samenwerken met de CSIRT's van andere lidstaten wanneer een gemelde kwetsbaarheid (via een gecoördineerde bekendmaking of een melding) significante gevolgen kan hebben voor entiteiten in meer dan één lidstaat.

Tot slot wijst de zesde paragraaf erop dat de directeur-generaal van het nationale CSIRT moet zorgen voor de naleving van bovengenoemde voorwaarden en hiervoor interne procedures uitwerkt.

Art. 23

De bepaling is bedoeld om onder bepaalde strikte voorwaarden een beschermend kader ("*safe harbour*") uit te werken voor "ethische hackers" of "digitale klokkenluiders", die een melding naar het nationale CSIRT sturen.

Om deze bescherming te genieten, moeten digitale klokkenluiders de procedure van artikel 22 en de voorwaarden van dit artikel naleven.

Ten eerste mogen ethische hackers hun onderzoek niet gebruiken met bedrieglijk opzet of het oogmerk om te schaden. Ze mogen de verantwoordelijke organisatie (bij gebrek aan een vooraf bepaald beloningsprogramma) of derden bijvoorbeeld niet trachten te laten betalen voor de ontdekte informatie. Ethische hackers mogen de ontdekte kwetsbaarheid evenmin in hun voordeel gebruiken.

Ten tweede moeten ethische hackers (natuurlijke of rechtspersonen) de betrokken organisatie onverwijld en uiterlijk binnen 24 uur na de ontdekking van een mogelijke kwetsbaarheid hiervan op de hoogte hebben gebracht.

Ten derde moeten ethische hackers de organisatie en het nationale CSIRT onverwijld en uiterlijk binnen 72 uur

complète sans délai et au plus tard dans les 72 heures suivant la découverte d'une potentielle vulnérabilité.

La ou les personne(s) physique(s) ou morale(s) effectuant le signalement doivent avoir participé partiellement ou complètement aux recherches relatives à la vulnérabilité découverte. En effet, l'auteur du signalement doit pouvoir, le cas échéant, être tenu responsable des méthodes de recherches utilisées: il doit donc y avoir contribué au moins partiellement. Lorsque plusieurs chercheurs ont participé aux recherches, le signalement peut être effectué au nom de plusieurs personnes qui en assument alors collectivement la responsabilité. Par facilité, plusieurs découvertes peuvent être également communiquées dans un seul signalement.

Il n'apparaît toutefois pas pertinent d'exiger, en outre, un enregistrement préalable des hackers éthiques auprès du CSIRT national ou d'exiger d'eux l'obtention d'une certification spécifique.

En effet, de telles formalités risquent de limiter le recours à la procédure de signalement, notamment en cas de découvertes fortuites de vulnérabilités ou de personne agissant bénévolement (en dehors d'un programme de récompense – “bug bounty” en anglais).

Il faut souligner que la majorité des hackers éthiques qui utilisent actuellement la procédure de signalement des vulnérabilités auprès du Centre pour la Cybersécurité Belgique agissent de manière bénévole, sur leur temps libre, avec tout au plus la volonté de gagner un t-shirt comme récompense. Imposer des obligations supplémentaires de pré-enregistrement ou de certification dissuaderait de telles personnes.

En outre, il n'est pas exigé, dans le cadre de la législation sur les lanceurs d'alertes, que les auteurs de signalement effectuent un enregistrement préalable ou disposent d'une certification.

Quatrièmement, le hacker éthique doit s'engager dans ses actions et ses méthodes de recherches à respecter les principes de nécessité et de proportionnalité. Son attitude doit rester nécessaire et proportionnée au regard de l'objectif poursuivi de vérifier l'existence d'une vulnérabilité en vue d'améliorer la sécurité du système, du processus ou du contrôle concerné. Les techniques utilisées doivent être strictement nécessaires et proportionnées à la démonstration d'une faille de sécurité.

Si la démonstration est établie à petit échelle, il n'est pas nécessaire de l'étendre plus loin. De même, il n'est

na de ontdekking van een mogelijke kwetsbaarheid een volledige kennisgeving sturen.

De persoon of personen (natuurlijke of rechtspersonen) die de melding doen, moeten hebben deelgenomen aan het volledige onderzoek rond de ontdekte kwetsbaarheid of aan een deel ervan. In voorkomend geval moet de melder immers aansprakelijk kunnen worden gesteld voor de gebruikte onderzoeksmethoden: hij moet hier dus ten minste gedeeltelijk aan hebben bijgedragen. Indien meerdere onderzoekers aan het onderzoek hebben deelgenomen, kan de melding gebeuren namens verschillende personen, die dan samen de verantwoordelijkheid op zich nemen. Gemakshalve kunnen verschillende ontdekkingen ook in één melding worden meegedeeld.

Het blijkt echter niet gepast om van ethische hackers te verwachten dat ze zich vooraf registreren bij het nationale CSIRT of dat ze een specifieke certificering behalen.

Dergelijke formaliteiten brengen namelijk het risico met zich mee dat het gebruik van de meldingsprocedure wordt beperkt, met name in het geval van toevallige ontdekkingen van kwetsbaarheden of van mensen die vrijwillig handelen (buiten een bug bounty-programma om).

Opgemerkt wordt dat de meeste ethische hackers die momenteel gebruik maken van de procedure voor het melden van kwetsbaarheden aan het Centrum voor Cybersecurity België, dit doen op vrijwillige basis, in hun vrije tijd, met hoogstens de wens om een T-shirt te winnen als beloning. Het opleggen van bijkomende vereisten op het vlak van preregistratie of certificatie zou dergelijke mensen afschrikken.

Bovendien vereist de klokkenluiderswetgeving niet dat klokkenluiders vooraf geregistreerd of gecertificeerd zijn.

Ten vierde moeten ethische hackers zich ertoe verbinden de beginselen van noodzakelijkheid en evenredigheid in acht te nemen bij hun acties en onderzoeksmethoden. Hun gedrag moet noodzakelijk zijn om na te gaan of er sprake is van een kwetsbaarheid teneinde de beveiliging van het systeem, het proces of de controle in kwestie te verbeteren, en evenredig zijn met dit doel. De gebruikte technieken moeten strikt noodzakelijk en evenredig zijn om een beveiligingsprobleem aan te tonen.

Indien het beveiligingsprobleem op kleine schaal is aangetoond, moet niet verder worden gegaan. Het is

pas justifié de perturber la disponibilité des services fournis par l'équipement concerné.

De même, en exécution des principes de nécessité et de proportionnalité, toutes les données collectées par le hacker éthique devraient être supprimées dans un délai raisonnable après le signalement. Si cela s'avère nécessaire de conserver ces données encore pendant un certain temps ou si une procédure judiciaire est en cours, le hacker éthique doit veiller à ce que ces données sont conservées en toute sécurité durant cette période.

Afin d'aider les hackers éthiques dans cette évaluation, le CSIRT national fournira sur son site internet une liste indicative des techniques pouvant être considérées comme nécessaires et proportionnées.

Dans un tel cadre, peuvent être considérées notamment comme des actions nécessaires pour vérifier l'existence d'une vulnérabilité et pour la rapporter:

- l'accès ou la tentative d'accès non autorisée à un système informatique (art. 550*bis*, §§ 1 et 4, du Code pénal);

- le dépassement ou la tentative de dépassement d'une autorisation d'accès à un système informatique (550*bis*, §§ 2 et 4, du Code pénal);

- la reprise ou la copie de données informatiques (art. 550*bis*, § 3, du Code pénal);

- l'élaboration ou la détention de hacking tools (art. 550*bis*, § 5, du Code pénal);

- la détention, la révélation, l'usage ou la divulgation d'information issues d'un accès non autorisé – par exemple des informations disponibles sur internet (art. 550*bis*, § 7, du Code pénal);

- l'introduction ou la modification de données dans un système informatique (art. 550*ter* du Code pénal);

- l'interception ou la tentative d'interception de communications (l'article 145 de la loi du 13 juin 2005 relative aux communications électroniques);

- la violation d'une obligation de secret professionnel (art. 458 du Code pénal) ou d'une obligation contractuelle de confidentialité.

Cinquièmement, il est exigé que le hacker éthique n'ait pas publiquement divulgué les informations relatives à la vulnérabilité découverte, sans l'accord du CSIRT national.

evenmin verantwoord om de beschikbaarheid van de door de betrokken apparatuur verleende diensten te verstoren.

Voorts moeten, in uitvoering van de beginselen van noodzakelijkheid en evenredigheid, alle door ethische hackers verzamelde gegevens binnen een redelijke termijn na de melding worden verwijderd. Indien het noodzakelijk is om deze gegevens nog enige tijd te bewaren of indien er een gerechtelijke procedure loopt, moeten ethische hackers ervoor zorgen dat deze gegevens in deze periode veilig worden bewaard.

Om ethische hackers bij deze evaluatie te helpen, zal het nationale CSIRT op zijn website een indicatieve lijst van technieken publiceren die als noodzakelijk en evenredig kunnen worden beschouwd.

In dat kader kunnen met name de volgende acties als noodzakelijk worden beschouwd om het bestaan van een kwetsbaarheid na te gaan en te melden:

- het ongeoorloofd binnendringen in een informatiesysteem of de poging daartoe (art. 550*bis*, leden 1 en 4, van het Strafwetboek);

- het overschrijden van een toegangsbevoegdheid tot een informatiesysteem of de poging daartoe (art. 550*bis*, leden 2 en 4, van het Strafwetboek);

- het overnemen of kopiëren van informaticagegevens (art. 550*bis*, § 3, van het Strafwetboek);

- het ontwikkelen of bezitten van hacking tools (art. 550*bis*, § 5, van het Strafwetboek);

- het bijhouden, onthullen, gebruiken of verspreiden van informatie die door ongeoorloofde binnendringing is verkregen, bijvoorbeeld informatie die beschikbaar is op het internet (art. 550*bis*, § 7, van het Strafwetboek);

- het invoeren of wijzigen van gegevens in een informatiesysteem (art. 550*ter* van het Strafwetboek);

- het onderscheppen van communicatie of de poging daartoe (artikel 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie);

- de schending van een beroepsgeheim (artikel 458 van het Strafwetboek) of van een contractuele geheimhoudingsplicht.

Ten vijfde mogen ethische hackers geen informatie over de ontdekte kwetsbaarheid openbaar hebben gemaakt zonder toestemming van het nationale CSIRT.

En effet, la divulgation publique d'une vulnérabilité alors que celle-ci existe toujours auprès de nombreux utilisateurs, constitue un risque important de sécurité en matière de technologies de l'information. En effet, des tiers malveillants pourraient développer et répandre des outils spécifiques pour exploiter cette vulnérabilité. Il n'est donc pas souhaitable qu'une faille de sécurité soit divulguée au public, avant qu'elle n'ait été corrigée par l'organisation responsable, en lui accordant le temps nécessaire à la résolution du problème, ou avant que l'organisation responsable n'ait pu en informer préalablement ses clients ou utilisateurs.

La divulgation complète est également susceptible de retarder le déploiement efficace d'une solution à la vulnérabilité en imposant à l'organisation responsable de réagir en situation de crise. De même, la révélation publique de failles de sécurité peut porter atteinte à la réputation de l'organisation responsable et entamer la confiance des utilisateurs dans les technologies concernées.

Par voie de conséquence, la divulgation publique d'informations sur une vulnérabilité doit être réalisée avec beaucoup de précaution et de manière coordonnée au moins avec le CCB.

Sixièmement, il est prévu une condition supplémentaire pour les réseaux et systèmes d'information des organisations visées à l'article 5, §§ 4 et 5, et des organes judiciaires ainsi que pour les informations traitées par eux ou pour leur compte. Dans ce cas, il est nécessaire que le chercheur ait conclu, avant la commission de ces actes, un accord écrit avec le service compétent sur les modalités et la méthodologie à utiliser dans le cadre de la recherche de potentielles vulnérabilités. Les informations et les systèmes de certaines entités sont tels qu'ils sont non seulement particulièrement sensibles, mais qu'ils peuvent également avoir un impact considérable sur la sécurité publique et le secret des enquêtes criminelles et de renseignement. Le(s) service(s) concerné(s) peut (peuvent) alors imposer des modalités particulières obligatoires par le biais d'une "politique" annexée à l'accord. Par exemple, il est possible pour ces entités d'imposer des délais particuliers de notification et des conditions de publication ou d'identification préalable.

Moyennant le respect de ces différentes conditions et indépendamment de l'existence ou non d'une politique de divulgation coordonnée des vulnérabilités, le lanceur d'alerte n'est alors pas considéré comme ayant commis une infraction aux articles 314*bis*, 458, 550*bis*, 550*ter* du Code pénal ni à l'article 145 de la loi du 13 juin 2005.

Het openbaar maken van een kwetsbaarheid, terwijl die nog altijd bij tal van gebruikers bestaat, vormt immers een groot beveiligingsrisico inzake informatietechnologie. Derden met slechte bedoelingen zouden immers specifieke tools kunnen ontwikkelen en verspreiden om misbruik te maken van deze kwetsbaarheid. Het is dus niet wenselijk om een beveiligingsprobleem openbaar te maken voordat het door de verantwoordelijke organisatie wordt verholpen, die daarvoor de nodige tijd moet krijgen, of voordat de verantwoordelijke organisatie haar klanten of gebruikers hierover heeft kunnen informeren.

De volledige bekendmaking kan ook de doeltreffende toepassing van een oplossing voor de kwetsbaarheid vertragen door de verantwoordelijke organisatie te verplichten om in een crisissituatie te reageren. Ook kan het openbaar maken van beveiligingsproblemen de reputatie van de verantwoordelijke organisatie schaden en het vertrouwen van de gebruikers in de betrokken technologieën ondermijnen.

Daarom moet het openbaar maken van informatie over een kwetsbaarheid heel omzichtig en minstens in overleg met het CCB gebeuren.

Ten zesde is een bijkomende voorwaarde toegevoegd voor netwerk- en informatiesystemen van de in artikel 5, leden 4 en 5, bedoelde organisaties en van de rechterlijke instanties, alsook voor de informatie die door hen of namens hen wordt verwerkt. In dat geval moet de onderzoeker vóór het plegen van die daden een schriftelijke overeenkomst hebben gesloten met de bevoegde dienst over de te hanteren modaliteiten en methodologie in het kader van het onderzoek naar mogelijke kwetsbaarheden. De informatie en systemen van bepaalde entiteiten zijn van die aard dat ze niet alleen bijzonder gevoelig zijn maar tevens een enorme impact kunnen hebben op de openbare veiligheid en het geheim van strafrechtelijke en inlichtingenonderzoeken. De betrokken dienst(en) kan (kunnen) dan specifieke regels opleggen via een bij de overeenkomst gevoegde "policy". Deze entiteiten kunnen bijvoorbeeld specifieke meldingstermijnen opleggen, alsook voorwaarden inzake de bekendmaking of voorafgaande identificatie.

Indien deze verschillende voorwaarden zijn vervuld en ongeacht het eventuele bestaan van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden, wordt de klokkenluider dan niet geacht een inbreuk te hebben gepleegd op de artikelen 314*bis*, 458, 550*bis* of 550*ter* van het Strafwetboek noch op artikel 145 van de wet van 13 juni 2005.

Les actions doivent être limitées strictement aux faits nécessaires pour permettre la recherche et le signalement d'une vulnérabilité d'un réseau et système d'information.

Le troisième paragraphe rappelle que, toute autre responsabilité, en ce compris pénale, découlant d'actes ou d'omissions qui ne sont pas nécessaires à l'accomplissement de la procédure visée à l'article 22 et ne respectent pas les conditions du paragraphe premier, continue d'être régie par le droit applicable. Cela signifie que l'auteur du signalement pourra être poursuivi pénalement, civilement ou disciplinairement pour tous les actes accomplis qui n'étaient pas nécessaires pour vérifier l'existence d'une vulnérabilité. De même, l'auteur d'un signalement ne bénéficie pas de la protection légale prévue au paragraphe premier lorsqu'il agit avec une intention frauduleuse ou par dessein de nuire.

Enfin, il faut tenir compte du fait que cette protection légale est limitée à l'application du droit belge et est sans préjudice du statut juridique spécifique des organisations internationales et européennes ou des missions diplomatiques établies sur le territoire national.

Section 2

Les éventuelles autorités sectorielles

Art. 24

Cet article octroie des compétences aux éventuelles autorités sectorielles, en plus des tâches et compétences visées aux différents articles du présent projet de loi.

L'analyse et la gestion des conséquences d'un incident pour un secteur ne se confond pas avec les compétences relatives à la gestion d'incidents prévue par le présent projet de loi. Il s'agit pour l'éventuelle autorité sectorielle de gérer les conséquences hors cyber qu'un incident peut avoir pour un secteur en particulier.

CHAPITRE 2

Coopération au niveau national

Art. 25

Cet article porte sur la coopération au niveau national.

De acties moeten strikt beperkt blijven tot feiten die noodzakelijk zijn om een kwetsbaarheid in een netwerk- en informatiesysteem te kunnen opsporen en melden.

De derde paragraaf wijst erop dat het toepasselijke recht blijft gelden voor elke andere aansprakelijkheid, met inbegrip van de strafrechtelijke aansprakelijkheid, die voortvloeit uit handelingen of nalatigheden die niet noodzakelijk zijn voor de uitvoering van de in artikel 22 bedoelde procedure en die niet voldoen aan de voorwaarden van de eerste paragraaf. Dit betekent dat melders strafrechtelijk, burgerrechtelijk of tuchtrechtelijk kunnen worden vervolgd voor alle handelingen die niet noodzakelijk waren om na te gaan of er sprake was van een kwetsbaarheid. Ook komen melders niet in aanmerking voor de in de eerste paragraaf bedoelde wettelijke bescherming indien ze handelen met bedrieglijk opzet of met het oogmerk om te schaden.

Tot slot moet rekening worden gehouden met het feit dat deze wettelijke bescherming beperkt is tot de toepassing van het Belgisch recht en geen afbreuk doet aan het specifiek juridisch statuut van internationale en Europese organisaties of van diplomatieke missies die op het nationale grondgebied gevestigd zijn.

Afdeling 2

De eventuele sectorale overheden

Art. 24

Dit artikel verleent bevoegdheden aan de eventuele sectorale overheden, naast de taken en bevoegdheden waarvan sprake in de verschillende artikelen van dit wetsontwerp.

De analyse en het beheer van de gevolgen van een incident voor een sector mag niet verward worden met de bevoegdheden inzake het beheer van incidenten waarin dit wetsontwerp voorziet. De eventuele sectorale overheid moet de niet-cybergevolgen beheren die een incident voor een bepaalde sector kan hebben.

HOOFDSTUK 2

Samenwerking op nationaal niveau

Art. 25

Dit artikel is gewijd aan de samenwerking op nationaal niveau.

Le paragraphe 1^{er} dispose que les autorités compétentes dans le cadre du présent projet de loi, à savoir l'autorité nationale de cybersécurité et, le cas échéant, les autorités sectorielles, coopèrent entre elles dans le cadre de l'exécution du présent projet de loi.

Le paragraphe 2 permet également la coopération, en ce compris l'échange d'informations, entre les autorités précitées et le Centre de crise national, les services administratifs de l'État, les autorités administratives, les autorités judiciaires, les services de renseignement et de sécurité, les services de police et les autorités de contrôle des données à caractère personnel. Sont comprises dans les autorités précitées, les autorités visées à l'article 13, § 4, de la directive NIS2.

L'article dispose également que les entités essentielles et importantes doivent collaborer avec les autorités visées au paragraphe 1^{er}. La collaboration se caractérise par l'échange d'informations concernant la sécurité de leurs systèmes et réseaux d'informations.

Le paragraphe 4 transpose l'article 13, § 5, *initio*, de la directive NIS2, selon lequel les autorités compétentes en vertu des directives NIS2 et (UE) 2022/2557 (directive CER) coopèrent et échangent régulièrement des informations en matière de recensement des entités critiques, de risques, de cybermenaces et d'incidents ainsi qu'en matière de risques, menaces et incidents non cyber qui touchent les exploitants d'infrastructures critiques au sens de la loi de 1^{er} juillet 2011, qui sont pour rappel *de facto* des entités essentielles au sens du présent projet de loi.

Le paragraphe 5 transpose l'article 13, § 5, *in fine*, de la directive NIS2, selon lequel les autorités compétentes en vertu du présent projet de loi, du règlement (UE) n° 910/2014, la Banque nationale de Belgique, la FSMA et l'Institut belge des services postaux et des télécommunications échangent régulièrement des informations pertinentes.

Le dernier paragraphe impose la création d'une plateforme au sein de laquelle les autorités compétentes dans le cadre du présent projet de loi pourront échanger de l'information et se coordonner afin d'exécuter les obligations du présent projet de loi.

Au travers de cette plateforme, il sera possible d'établir des rapports d'évaluation de l'exécution de la loi, d'organiser et de coordonner les inspections, d'échanger sur les pratiques de supervision, d'offrir des formations, voire d'assurer plus de coordination entre les autorités publiques et le secteur privé ou le monde scientifique (via la consultation de parties prenantes notamment).

Paragraphe 1 bepaalt dat de uit hoofde van dit wetsontwerp bevoegde autoriteiten, namelijk de nationale cyberbeveiligingsautoriteit en, in voorkomend geval, de sectorale overheden, samenwerken in het kader van de uitvoering van dit wetsontwerp.

Paragraf 2 maakt samenwerking ook mogelijk, met inbegrip van informatie-uitwisseling, tussen voornoemde autoriteiten en het Nationaal Crisiscentrum, de administratieve diensten van de Staat, de administratieve overheden, de gerechtelijke overheden, de inlichtingen- en veiligheidsdiensten, de politiediensten en de toezichthoudende autoriteiten persoonsgegevens. Ook de in artikel 13, lid 4, van de NIS2-richtlijn bedoelde autoriteiten behoren tot voornoemde autoriteiten.

Het artikel bepaalt ook dat essentiële en belangrijke entiteiten moeten samenwerken met de in paragraaf 1 bedoelde autoriteiten. In het kader van deze samenwerking wordt informatie uitwisseld over de beveiliging van hun netwerk- en informatiesystemen.

Paragraf 4 voorziet in de omzetting van artikel 13, lid 5, *initio*, van de NIS2-richtlijn, volgens hetwelk de autoriteiten die bevoegd zijn uit hoofde van de NIS2-richtlijn en van Richtlijn (EU) 2022/2557 (de CER-richtlijn) samenwerken en regelmatig informatie uitwisselen inzake het als kritiek aanmerken van entiteiten, over cyberrisico's, -dreigingen en -incidenten alsook over niet-cyberrisico's, -dreigingen en -incidenten die gevolgen hebben voor exploitanten van kritieke infrastructuur als bedoeld in de wet van 1 juli 2011, die *de facto* immers essentiële entiteiten zijn als bedoeld in dit wetsontwerp.

Paragraf 5 voorziet in de omzetting van artikel 13, lid 5, *in fine*, van de NIS2-richtlijn, volgens hetwelk de autoriteiten die bevoegd zijn uit hoofde van dit wetsontwerp en Verordening (EU) nr. 910/2014, de Nationale Bank van België, de FSMA en het Belgisch Instituut voor postdiensten en telecommunicatie regelmatig relevante informatie uitwisselen.

Volgens de laatste paragraaf wordt een platform opgericht dat de in het kader van dit wetsontwerp bevoegde autoriteiten toelaat informatie uit te wisselen en hun optreden op elkaar af te stemmen om de verplichtingen van dit wetsontwerp uit te voeren.

Dit platform biedt de mogelijkheid om beoordelingsverslagen op te stellen over de uitvoering van de wet, inspecties te organiseren en te coördineren, toezichtspraktijken uit te wisselen, opleidingen aan te bieden en zelfs om te zorgen voor een betere coördinatie tussen de overheden en de private sector of de wetenschappelijke wereld (met name via de raadpleging van stakeholders).

CHAPITRE 3

Confidentialité et échanges d'information

Art. 26

Cet article porte sur la confidentialité et l'échange d'informations. Cela étant, cette disposition ne porte pas préjudice aux règles applicables de par la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé, la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, la loi du 11 avril 1994 relative à la publicité de l'administration ou de par d'autres dispositions légales garantissant la confidentialité des informations liées aux intérêts essentiels de la sécurité publique nationale.

L'article impose, en son paragraphe 2, un secret professionnel, au sens de l'article 458 du Code pénal, à toute personne appelée à prêter son concours professionnel à l'évaluation de la conformité ou à la supervision dans le cadre de la présente loi.

Selon cette disposition, les autorités compétentes dans le cadre du présent projet de loi, les entités essentielles et importantes et leurs sous-traitants limitent l'accès aux informations relatives à l'exécution du présent projet de loi aux personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec le présent projet de loi. De plus, les membres du personnel des entités essentielles et importantes sont soumis au secret professionnel.

L'article prévoit en son paragraphe 4 que l'échange d'informations avec des autorités de l'Union européenne, avec des autorités étrangères ou nationales, est possible pour autant que cela soit nécessaire à l'application du présent projet de loi et que cet échange d'informations respecte les dispositions légales garantissant la confidentialité des informations liées aux intérêts essentiels de la sécurité publique.

Art. 27

Cet article transpose l'article 29 de la directive NIS2. Il prévoit que, lorsque des entités échangent des informations au sein de communautés, notamment relatives aux cybermenaces, aux incidents évités ou encore aux vulnérabilités, cet échange d'informations se fait au

HOOFDSTUK 3

Vertrouwelijkheid en informatie-uitwisseling

Art. 26

Dit artikel behandelt de vertrouwelijkheid en de informatie-uitwisseling. Deze bepaling doet echter geen afbreuk aan de regels die van toepassing zijn krachtens de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst, de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, de wet van 11 april 1994 betreffende de openbaarheid van bestuur of krachtens andere wettelijke bepalingen die de vertrouwelijkheid van informatie met betrekking tot de wezenlijke belangen van de nationale openbare veiligheid waarborgen.

Paragraaf 2 van het artikel bepaalt dat eenieder die beroepshalve zijn medewerking moet verlenen aan de conformiteitsbeoordeling of het toezicht in het kader van deze wet, onderworpen is aan het beroepsgeheim bedoeld in artikel 458 van het Strafwetboek.

Volgens deze bepaling beperken de uit hoofde van dit wetsontwerp bevoegde autoriteiten, de essentiële en belangrijke entiteiten en hun onderaannemers de toegang tot de informatie betreffende de uitvoering van dit wetsontwerp tot de personen die ervan op de hoogte moeten zijn en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met dit wetsontwerp. Bovendien zijn de personeelsleden van essentiële en belangrijke entiteiten onderworpen aan het beroepsgeheim.

Volgens paragraaf 4 van het artikel kan informatie worden uitgewisseld met autoriteiten van de Europese Unie, buitenlandse of nationale autoriteiten, voor zover dit noodzakelijk is voor de toepassing van dit wetsontwerp en deze informatie-uitwisseling voldoet aan de wettelijke bepalingen die de vertrouwelijkheid van informatie met betrekking tot de wezenlijke belangen van de openbare veiligheid waarborgen.

Art. 27

Dit artikel voorziet in de omzetting van artikel 29 van de NIS2-richtlijn. Wanneer entiteiten informatie uitwisselen binnen gemeenschappen, met name betreffende cyberdreigingen, bijna-incidenten of kwetsbaarheden, deze informatie-uitwisseling gebeurt door middel van

travers d'accords de partage d'informations en matière de cybersécurité.

L'autorité nationale de cybersécurité a pour tâche de faciliter la mise en place de tels accords et reçoit des informations des entités soumises au champ d'application de la présente loi lorsque ces entités concluent de tels accords ou lorsqu'elles s'en retirent.

CHAPITRE 4

Stratégie nationale en matière de cybersécurité

Art. 28

Cet article porte sur la stratégie nationale en matière de cybersécurité, les autorités impliquées dans sa conception, ses mises à jours et son contenu.

La stratégie consiste en un cadre cohérent "prévoyant des objectifs stratégiques et des priorités dans le domaine de la cybersécurité et de la gouvernance pour les atteindre" (directive NIS2, considérant 48).

Cette stratégie comprend, entre autres, les objectifs et les priorités de la stratégie, un cadre de gouvernance visant à atteindre ces objectifs et priorités, une liste des différents acteurs et autorités concernés, un plan comprenant les mesures nécessaires en vue d'améliorer le niveau général de sensibilisation des citoyens à la cybersécurité, etc.

Dans le cadre de cette stratégie, la Belgique devra adopter des politiques, entre autres, dans le domaine de la chaîne d'approvisionnement, de la gestion des vulnérabilités et de la divulgation coordonnée des vulnérabilités, des marchés publics, du partage d'informations, etc.

Le premier paragraphe dispose que cette stratégie est adoptée par le Conseil des ministres et est mise à jour au moins tous les 5 ans, après avis du Conseil national de sécurité, des autorités compétentes dans le cadre du présent projet de loi, du Centre de crise national et des autorités de protection des données.

Les deuxième et troisième paragraphes déterminent les éléments devant être contenus dans la stratégie.

informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging.

De nationale cyberbeveiligingsautoriteit heeft als taak de vaststelling van deze regelingen te faciliteren en ontvangt informatie van de entiteiten die onderworpen zijn aan het toepassingsgebied van deze wet wanneer deze entiteiten dergelijke regelingen aangaan of zij er zich uit terugtrekken.

HOOFDSTUK 4

Nationale cyberbeveiligingsstrategie

Art. 28

Dit artikel gaat nader in op de nationale cyberbeveiligingsstrategie en de autoriteiten die betrokken zijn bij het ontwerp, de bijwerkingen en de inhoud ervan.

De strategie bestaat uit een samenhangend kader "met strategische doelstellingen en prioriteiten op het gebied van cyberbeveiliging en de governance om deze te verwezenlijken" (NIS2-richtlijn, overweging 48).

Deze strategie omvat onder meer de doelstellingen en prioriteiten van de strategie, een governancekader om deze doelstellingen en prioriteiten te verwezenlijken, een lijst van de verschillende betrokken belanghebbenden en autoriteiten, een plan met inbegrip van de noodzakelijke maatregelen om het algemene niveau van cyberbeveiligingsbewustzijn bij de burgers te verbeteren, enz.

In het kader van deze strategie moet België beleidsmaatregelen nemen, onder meer op het gebied van de toeleveringsketen, het beheer van kwetsbaarheden en de gecoördineerde bekendmaking van kwetsbaarheden, overheidsopdrachten, het delen van informatie, enz.

Paragraaf 1 bepaalt dat deze strategie wordt aangenomen bij de Ministerraad en minstens om de 5 jaar wordt bijgewerkt, na advies van de Nationale Veiligheidsraad, de uit hoofde van dit wetsontwerp bevoegde autoriteiten, het Nationaal Crisiscentrum en de gegevensbeschermingsautoriteiten.

De paragrafen 2 en 3 bepalen welke elementen de strategie moet bevatten.

CHAPITRE 5

**Le plan national de réaction
aux crises cyber et incidents
de cybersécurité**

Art. 29

Cet article transpose l'article 9, § 4, de la directive NIS2 en assurant la cohérence avec l'application du cadre national de gestion de crise.

Il dispose que le Roi adopte, par arrêté royal, un plan national de réaction aux crises cyber et incidents de cybersécurité et précise que ce plan constitue un plan national au sens l'article 9, § 2, de la loi du 15 mai 2007 relative à la sécurité civile.

Il énumère également les éléments devant se trouver dans ce plan selon l'article 9, § 4, de la directive NIS2 tout en précisant que cela est sans préjudice des éléments devant être contenus dans les plans nationaux. De cette manière, le projet de loi ajoute les exigences de la directive NIS2 relatives au contenu du plan national de gestion de crise cyber aux exigences déterminées par le cadre général de gestion de crise, qui demeure applicable.

TITRE 3

*Mesures de gestion des risques en matière de
cybersécurité et obligations d'information*CHAPITRE 1^{ER}**Mesures de gestion des risques en matière de
cybersécurité**

Art. 30

Cet article transpose l'article 21 de la directive NIS2 et contient les principales exigences légales des entités soumises à la loi en matière de mesures de cybersécurité.

Les entités essentielles et importantes ont l'obligation de prendre les mesures appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'elles utilisent et pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services ainsi que sur d'autres services. Comme le précise le considérant 77 de la directive NIS2, "dans une large mesure, il incombe aux entités essentielles et importantes de garantir la sécurité des réseaux et des systèmes d'information.

HOOFDSTUK 5

**Het nationale plan voor
cyberbeveiligingsincidenten en
cybercrisisrespons**

Art. 29

Dit artikel voorziet in de omzetting van artikel 9, lid 4, van de NIS2-richtlijn en zorgt voor samenhang met de toepassing van het nationale crisisbeheerkader.

Het bepaalt dat de Koning, bij koninklijk besluit, een nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons goedkeurt en verduidelijkt dat dit plan een nationaal plan is als bedoeld in artikel 9, § 2, van de wet van 15 mei 2007 betreffende de civiele veiligheid.

Het somt ook de elementen op die dit plan ten minste moet bevatten overeenkomstig artikel 9, lid 4, van de NIS2-richtlijn en verduidelijkt dat dit geen afbreuk doet aan de elementen die moeten worden opgenomen in de nationale plannen. Op die manier voegt het wetsontwerp de voorschriften van de NIS2-richtlijn betreffende de inhoud van het nationaal plan voor cybercrisisbeheer toe aan de voorschriften die bepaald worden door het algemene crisisbeheerkader, dat van toepassing blijft.

TITEL 3

*Maatregelen voor het beheer van
cyberbeveiligingsrisico's en rapportageverplichtingen*

HOOFDSTUK 1

**Maatregelen voor het beheer van
cyberbeveiligingsrisico's**

Art. 30

Dit artikel voorziet in de omzetting van artikel 21 van de NIS2-richtlijn en bevat de belangrijkste wettelijke voorschriften inzake cyberbeveiligingsmaatregelen voor de entiteiten die onderworpen zijn aan de wet.

Essentiële en belangrijke entiteiten zijn verplicht passende en evenredige maatregelen te nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die zij gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de ontvangers van hun diensten en voor andere diensten te beperken. Overweging 77 van de NIS2-richtlijn verduidelijkt in dit verband dat "de verantwoordelijkheid voor het waarborgen van de beveiliging van netwerken en informatiesystemen [...] voor een groot deel bij de

Il convient de promouvoir et de faire progresser une culture de la gestion des risques impliquant une analyse des risques et l'application de mesures de gestion des risques en matière de cybersécurité adaptées aux risques encourus”.

Pour rappel et conformément à la directive, l'article 8, 1° de la loi donne une définition large de la notion de “réseau et système d'information”. Les réseaux et les systèmes d'information englobent à la fois le matériel, les logiciels et les protocoles qui permettent une circulation fluide de l'information. Cela comprend à la fois les technologies de l'information (“information technology” ou “IT” en anglais) et les technologies opérationnelles (“operational Technology” ou “OT” en anglais). Les technologies de l'information englobent les technologies de mise en réseau, de traitement de l'information, les centres de données et les systèmes en nuage (“cloud”). Les technologies opérationnelles, couramment appelée systèmes d'automatisation et de contrôle industriel (“Industrial Automation and Control Systems” ou “IACS”) comprend le matériel et les logiciels qui surveillent et contrôlent les appareils, les processus et l'infrastructure, et qui sont utilisés dans les environnements industriels.

Conformément à la directive, l'article 30 prévoit que les obligations en matière de cybersécurité s'appliquent aux réseaux et des systèmes d'information que les entités “utilisent dans le cadre de leurs activités ou de la fourniture de leurs services”. En pratique, cela signifie que tous les réseaux et systèmes d'information utilisés par une entité soumise à la loi doivent respecter les exigences de la loi et non uniquement les systèmes d'information utilisés pour les services essentiels visés dans les annexes I ou II de la loi. Il s'agit d'une différence fondamentale avec l'approche mise en œuvre précédemment par la directive et la loi NIS1. L'intervention éventuelle d'un tiers (par exemple, un prestataire) dans la gestion des réseaux et systèmes d'information utilisés par l'entité ne soustrait évidemment pas ces éléments du champ d'application de la loi. L'entité devra dès lors s'assurer du respect par ce tiers des exigences de la loi.

Les mesures devant être adoptées par les entités essentielles et importantes doivent être appropriées et proportionnées. Sur ce point, la directive NIS2 précise que “[p]our éviter que la charge financière et administrative imposée aux entités essentielles et importantes ne soit disproportionnée, il convient que les mesures de gestion des risques en matière de cybersécurité soient proportionnées aux risques auxquels le réseau et le système d'information concernés sont exposés, en prenant en compte l'état de l'art de ces mesures ainsi

essentielle et belangrijke entiteiten [ligt]. Er moet een cultuur van risicobeheer worden bevorderd en ontwikkeld, die risicobeoordelingen en de uitvoering van op de risico's afgestemde maatregelen voor het beheer van cyberbeveiligingsrisico's behelst”.

Ter herinnering en in overeenstemming met de richtlijn geeft artikel 8, 1° van de wet een ruime definitie van het begrip “netwerk- en informatiesysteem”. Netwerk- en informatiesystemen omvatten zowel hardware, software en protocollen die een soepele informatiestroom mogelijk maken. Dit omvat zowel informatietechnologie (“information technology” of “IT” in het Engels) en de operationele technologie (“Operationele technologie” of “OT” in het Engels). Informatietechnologie (IT) omvat technologieën voor netwerken, informatieverwerking, datacenters en cloudsysteem (“cloud”). Operationele technologie (OT), gewoonlijk aangeduid als industriële automatiserings- en controlesystemen (“Industrial Automation and Control Systems” of “IACS”), omvat de hardware en software die apparaten, processen en infrastructuur bewaakt en regelt, en wordt gebruikt in industriële omgevingen.

Overeenkomstig de richtlijn bepaalt artikel 30 dat de cyberbeveiligingsverplichtingen van toepassing zijn op de netwerk- en informatiesystemen die entiteiten “voor hun activiteiten of voor het verlenen van hun diensten gebruiken”. In de praktijk betekent dit dat alle netwerk- en informatiesystemen die door een onder de wet vallende entiteit worden gebruikt, aan de eisen van de wet moeten voldoen en niet alleen de informatiesystemen die worden gebruikt voor de in bijlage I of II van de wet genoemde essentiële diensten. Dit is een fundamenteel verschil met de benadering die eerder werd toegepast in de NIS1-richtlijn en de NIS1-wet. De mogelijke betrokkenheid van een derde partij (bijvoorbeeld een dienstverlener) bij het beheer van de netwerk- en informatiesystemen die door de entiteit worden gebruikt, onttrekt deze elementen uiteraard niet aan het toepassingsgebied van de wet. De entiteit zal er daarom voor moeten zorgen dat de derde partij voldoet aan de eisen van de wet.

Essentiële en belangrijke entiteiten moeten maatregelen nemen die passend en evenredig zijn. Op dit punt bevat de NIS2-richtlijn de volgende toelichting: “Om te voorkomen dat aan essentiële en belangrijke entiteiten onevenredige financiële en administratieve lasten worden opgelegd, moeten de maatregelen voor het beheer van cyberbeveiligingsrisico's in verhouding staan tot de risico's voor het betrokken netwerk- en informatiesysteem, rekening houdend met de stand van de techniek van dergelijke maatregelen en, in voorkomend geval, de

que, s'il y a lieu, des normes européennes ou internationales pertinentes, et du coût de mise en œuvre de ces mesures" (considérant 81).

De plus, "les mesures de gestion des risques en matière de cybersécurité devraient être proportionnées au degré d'exposition de l'entité essentielle ou importante aux risques et à l'impact sociétal et économique potentiel d'un incident. Lors de la mise en place de mesures de gestion des risques en matière de cybersécurité adaptées aux entités essentielles et importantes, il convient de tenir dûment compte des différents niveaux d'exposition aux risques des entités essentielles et importantes, telles que la criticité de l'entité, les risques, y compris les risques sociétaux, auxquels elle est exposée, la taille de l'entité et la probabilité de survenance d'incidents et leur gravité, y compris leur impact sociétal et économique" (considérant 82, directive NIS2). Ces considérations, fondamentales dans l'évaluation des mesures à adopter, reprises dans l'article 21, § 1^{er}, de la directive NIS2, sont transposées au sein du présent article.

Le paragraphe 3 de la présente disposition contient deux obligations à charge des entités essentielles et importantes: fonder l'adoption des mesures précitées sur une approche tout risque et comprendre au moins les mesures visées à ce paragraphe. L'approche tout risque et les mesures énumérées aux points 1° à 10° transposent directement l'article 21, § 2, de la directive NIS2.

Une précision est apportée au 11° du paragraphe 3, à savoir l'exigence d'adopter une politique de divulgation coordonnée des vulnérabilités. Cet élément découle de l'article 21, § 2, sous e), de la directive qui prévoit le traitement et la divulgation des vulnérabilités, ainsi que de la politique nationale en la matière promue par le CCB.

Conformément aux lignes directrices adoptées par le Groupe européen de coopération NIS (*Guidelines on implementing national coordinated vulnerability Disclosure policies – 2023*) et étant donné l'importance des risques liés à des vulnérabilités, la disposition précise clairement que l'adoption d'une telle politique de divulgation coordonnée des vulnérabilités fait partie des mesures obligatoires requises en matière de gestion des risques. Chaque entité devra dès lors adopter et publier sur son site internet une politique de divulgation coordonnée des vulnérabilités, conforme aux recommandations du CCB en la matière et aux conditions prévues à l'article 23 de la loi.

relevante Europese en internationale normen, alsook met de kosten voor de uitvoering ervan." (overweging 81).

Bovendien moeten "maatregelen voor het beheer van cyberbeveiligingsrisico's [...] in verhouding staan tot de mate waarin de essentiële of belangrijke entiteit aan risico's is blootgesteld en de maatschappelijke en economische gevolgen die een incident zou hebben. Bij het vaststellen van maatregelen voor het beheer van cyberbeveiligingsrisico's die zijn aangepast aan essentiële en belangrijke entiteiten, moet terdege rekening worden gehouden met de uiteenlopende mate waarin essentiële en belangrijke entiteiten aan risico's zijn blootgesteld, overeenkomstig het kritieke karakter van de entiteit, de risico's, met inbegrip van maatschappelijke risico's, waaraan de entiteit is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen" (overweging 82, NIS2-richtlijn). Deze overwegingen zijn fundamenteel bij de beoordeling van de te nemen maatregelen. Ze zijn opgenomen in artikel 21, lid 1, van de NIS2-richtlijn en worden omgezet in dit artikel.

Paragraaf 3 van deze bepaling bevat twee verplichtingen voor essentiële en belangrijke entiteiten: voornoemde maatregelen moeten gebaseerd zijn op een benadering die alle gevaren omvat en ten minste betrekking hebben op de in deze paragraaf bedoelde maatregelen. De benadering die alle gevaren omvat en de maatregelen opgesomd in de punten 1° tot 10° voorzien rechtstreeks in de omzetting van artikel 21, lid 2, van de NIS2-richtlijn.

Er wordt een verduidelijking aangebracht in punt 11° van paragraaf 3, betreffende de vereiste om een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden in te voeren. Dit element vloeit voort uit artikel 21, lid 2, onder e), van de richtlijn dat voorziet in de respons op en de bekendmaking van kwetsbaarheden, alsook uit het nationale beleid ter zake dat het CCB voorstaat.

Overeenkomstig de richtsnoeren vastgesteld door de Europese NIS-samenwerkingsgroep (*Guidelines on implementing national coordinated vulnerability Disclosure policies – 2023*) en gezien het belang van de risico's van kwetsbaarheden verduidelijkt de bepaling dat de invoering van een dergelijk beleid voor de gecoördineerde bekendmaking van kwetsbaarheden een van de verplichte maatregelen voor risicobeheer is. Iedere entiteit zal daarom een gecoördineerd beleid voor de gecoördineerde bekendmaking van kwetsbaarheden moeten invoeren en op haar website moeten publiceren, in overeenstemming met de aanbevelingen van het CCB op dit gebied en in overeenstemming met de voorwaarden van artikel 23 van de Wet.

Le paragraphe 4 dispose que, dans le cadre de l'adoption des mesures précitées, les entités essentielles et importantes tiennent compte des vulnérabilités propres à chaque fournisseur et prestataire de services direct et de la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et prestataires de services, y compris de leurs procédures de développement sécurisé.

Selon la directive, "il est tout particulièrement important de répondre aux risques découlant de la chaîne d'approvisionnement d'une entité et de ses relations avec ses fournisseurs [...] vu la prévalence d'incidents dans le cadre desquels les entités ont été victimes de cyberattaques et où des acteurs malveillants ont réussi à compromettre la sécurité des réseaux et systèmes d'information d'une entité en exploitant les vulnérabilités touchant les produits et les services de tiers" (considérant 85).

Le cas échéant, des évaluations coordonnées des risques pour la sécurité de certaines chaînes d'approvisionnement pourront être effectuées par le groupe de coopération, en coopération avec la Commission européenne et l'ENISA, conformément à l'article 22, § 1^{er}, de la directive NIS2. Les mesures adoptées par les entités essentielles et importantes devront être appropriées au regard de ces évaluations.

Le paragraphe 5 précise explicitement que les entités essentielles et importantes sont tenues de réaliser une analyse des risques pour déterminer leurs mesures de cybersécurité, comme cela découle des différentes exigences de l'article 21, paragraphes 1^{er} et 2, de la directive NIS2. C'est à l'entité qu'il appartient d'effectuer son analyse des risques en fonction de ses réseaux et systèmes d'information, suivant la méthodologie qu'elle choisit. Toutefois, des recommandations seront fournies par l'autorité nationale de cybersécurité sur la manière de réaliser cette analyse de risques.

Le même paragraphe souligne également que les mesures de gestion des risques adoptées par les entités essentielles et importantes doivent être documentées au moins dans une politique de sécurité des systèmes et réseaux d'information ("P.S.I.").

Il s'agit du maintien d'une obligation qui existait déjà dans le cadre de la loi NIS1, à charge des opérateurs de services essentiels et qui se trouve de manière implicite dans la directive NIS2 au travers des mesures devant être adoptées par les entités (article 21, § 2, de la directive NIS2).

Enfin en son dernier paragraphe, la présente disposition prévoit que toute entité essentielle ou importante

Paragraaf 4 bepaalt dat, in het kader van de invoering van voornoemde maatregelen, essentiële en belangrijke entiteiten rekening houden met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures.

Volgens de richtlijn is "het aanpakken van risico's die voortvloeien uit de toeleveringsketen van een entiteit en uit haar relatie met haar leveranciers, [...] bijzonder belangrijk gezien de prevalentie van incidenten waarbij entiteiten het slachtoffer zijn geweest van cyberaanvallen en waarbij kwaadwillende daders de beveiliging van de netwerk- en informatiesystemen van een entiteit in gevaar hebben kunnen brengen door gebruik te maken van kwetsbaarheden die van invloed zijn op producten en diensten van derden" (overweging 85).

In voorkomend geval kan de samenwerkingsgroep, in samenwerking met de Europese Commissie en Enisa, gecoördineerde beveiligingsrisicobeoordelingen van bepaalde toeleveringsketens uitvoeren, overeenkomstig artikel 22, lid 1, van de NIS2-richtlijn. De door essentiële en belangrijke entiteiten genomen maatregelen moeten passend zijn in het licht van deze beoordelingen.

Paragraaf 5 bepaalt uitdrukkelijk dat essentiële en belangrijke entiteiten een risicoanalyse moeten uitvoeren om hun cyberbeveiligingsmaatregelen te bepalen, zoals volgt uit de verschillende voorschriften van artikel 21, leden 1 en 2, van de NIS2-richtlijn. Het is aan de betrokken entiteit om haar risicoanalyse met betrekking tot haar netwerk- en informatiesystemen uit te voeren volgens de door haar gekozen methodologie. De nationale cyberbeveiligingsautoriteit zal echter aanbevelingen verstrekken over de uitvoeringswijze van deze risicoanalyse.

Dezelfde paragraaf wijst er ook op dat de risicobeheersmaatregelen die essentiële en belangrijke entiteiten nemen, minstens in een beveiligingsbeleid voor de netwerk- en informatiesystemen ("I.B.B.") moeten worden gedocumenteerd.

Deze verplichting voor aanbieders van essentiële diensten die al bestond in het kader van de NIS1-wet, wordt behouden. Ze is impliciet opgenomen in de NIS2-richtlijn via de maatregelen die entiteiten moeten nemen (artikel 21, lid 2, van de NIS2-richtlijn).

Tot slot vermeldt de laatste paragraaf van deze bepaling dat elke essentiële of belangrijke entiteit die vaststelt dat

qui constate qu'elle ne se conforme pas aux mesures précitées, doit prendre, sans retard injustifié, toutes les mesures correctives nécessaires appropriées et proportionnées, conformément à l'article 21, § 4, de la directive NIS2.

Art. 31

Cet article transpose l'article 20 de la directive NIS2, selon lequel les organes de direction des entités essentielles et importantes doivent approuver les mesures évoquées au commentaire de l'article 30, superviser leur mise en œuvre et sont responsables en cas de violations des obligations visées à l'article 30 du présent projet de loi.

Le considérant 137 énonce ce qui suit: "La présente directive devrait viser à assurer un niveau de responsabilité important pour les mesures de gestion des risques en matière de cybersécurité et les obligations d'information au niveau des entités essentielles et importantes. Par conséquent, les organes de direction des entités essentielles et importantes devraient approuver les mesures de gestion des risques en matière de cybersécurité et superviser leur mise en œuvre."

À cette fin, les membres des organes de direction précités doivent suivre une formation permettant de démontrer qu'ils ont acquis des compétences suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis.

La notion de "membre d'un organe de direction" signifie toute personne physique ou morale qui:

(i) exerce une fonction au sein d'une entité ou en relation avec celle-ci l'autorisant (a) à administrer et à représenter l'entité en question ou (b) à prendre des décisions au nom et pour le compte de l'entité qui sont juridiquement liantes pour celle-ci ou à participer, au sein d'un organe de l'entité, à la prise de telles décisions, ou

(ii) exerce un contrôle de l'entité en question, soit le pouvoir de droit ou de fait d'exercer une influence décisive sur la désignation de la majorité des administrateurs ou gérants de celle-ci ou sur l'orientation de sa gestion.

Lorsque l'entité en question est une société de droit belge, tel contrôle est déterminé conformément aux articles 1:14 à 1:18 du Code des sociétés et des associations.

zij niet voldoet aan voornoemde maatregelen, onverwijld alle noodzakelijke, passende en evenredige corrigerende maatregelen moet nemen, overeenkomstig artikel 21, lid 4, van de NIS2-richtlijn.

Art. 31

Dit artikel voorziet in de omzetting van artikel 20 van de NIS2-richtlijn, volgens hetwelk de bestuursorganen van essentiële en belangrijke entiteiten de in de commentaar bij artikel 30 vermelde maatregelen moeten goedkeuren, toezien op de uitvoering ervan en aansprakelijk zijn voor inbreuken op de in artikel 30 van dit wetsontwerp bedoelde verplichtingen.

Overweging 137 van de richtlijn luidt als volgt: "Deze richtlijn moet gericht zijn op het waarborgen van een hoge mate van verantwoordelijkheid voor de risico-beheersmaatregelen en rapportageverplichtingen op het gebied van cyberbeveiliging op het niveau van de essentiële en belangrijke entiteiten. Daarom moeten de bestuursorganen van de essentiële en belangrijke entiteiten de risicobeheersmaatregelen op het gebied van cyberbeveiliging goedkeuren en toezicht houden op de uitvoering ervan."

Daartoe moeten de leden van voornoemde bestuursorganen een opleiding volgen zodat ze kunnen aantonen over voldoende vaardigheden te beschikken om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de verleende diensten te kunnen beoordelen.

Het begrip "lid van een bestuursorgaan" heeft betrekking op iedere natuurlijke persoon of rechtspersoon die:

(i) een functie uitoefent binnen of in verband met een entiteit die hem of haar in staat stelt (a) die entiteit te beheren en te vertegenwoordigen of (b) namens en voor rekening van die entiteit beslissingen te nemen die juridisch bindend zijn voor die entiteit of deel te nemen, binnen een orgaan van die entiteit, aan besluitvorming over dergelijke beslissingen, of

(ii) controle uitoefent over de entiteit, zijnde de bevoegdheid in rechte of in feite om een beslissende invloed uit te oefenen op de aanstelling van een meerderheid van de bestuurders of zaakvoerders of op de oriëntatie van het beleid.

Indien de entiteit in kwestie een vennootschap naar Belgisch recht is, wordt deze controle bepaald overeenkomstig artikel 1:14 tot 1:18 van het Wetboek van vennootschappen en verenigingen

Lorsque la personne dont le rôle est examiné est une personne morale, la notion de “membre d’un organe de direction” est examinée de façon réursive et recouvre tant la personne morale en question que tout membre d’un organe de direction de ladite personne morale.

La directive NIS2 précise, en son article 20, § 1^{er}, alinéa 2, que cette disposition ne porte pas préjudice au droit national en ce qui concerne les règles de responsabilité applicables aux institutions publiques et les règles de responsabilité des agents de la fonction publique et des responsables élus ou nommés.

Cette disposition est transposée dans le projet de loi au paragraphe 1^{er}, alinéa 2, de l’article faisant l’objet du présent commentaire. En droit belge, cela signifie que le présent projet de loi ne déroge aux règles existantes en matière de responsabilité précitées, notamment la loi du 10 février 2003 relative à la responsabilité des et pour les membres du personnel au service des personnes publiques.

Art. 32

Indépendamment des tâches éventuellement confiées à des sous-traitants, cet article rappelle que les entités essentielles et importantes demeurent responsables de l’analyse des risques à effectuer, du choix des mesures ainsi que de leur mise en œuvre dans le cadre du présent projet de loi. Cette disposition ne fait pas préjudice à l’article 31, § 1^{er}, alinéa 1^{er}, du présent projet de loi, évoqué *supra*.

Cela transparaît de la directive NIS2. L’article 21, § 1^{er}, dispose que ce sont les entités qui prennent les mesures techniques, opérationnelles et organisationnelles. Le considérant 77 explique que, “dans une large mesure, il incombe aux entités essentielles et importantes de garantir la sécurité des réseaux et des systèmes d’information”, le considérant 83 indique que “les entités essentielles et importantes devraient garantir la sécurité des réseaux et des systèmes d’information qu’elles utilisent dans le cadre de leurs activités. Il s’agit principalement de réseaux et de systèmes d’information privés qui sont gérés par les services informatiques des entités essentielles ou importantes ou dont la gestion de la sécurité a été sous-traitée. Les mesures de gestion des risques en matière de cybersécurité et les obligations d’information prévues par la présente directive devraient s’appliquer aux entités essentielles et importantes, indépendamment du fait que ces entités effectuent la maintenance de leurs réseaux et systèmes d’information en interne ou qu’elles l’externalisent” et le considérant 89 que “les entités essentielles

Wanneer de persoon wiens rol wordt onderzocht, een rechtspersoon is, wordt het begrip “lid van een bestuursorgaan” terugwerkend onderzocht en omvat het zowel de rechtspersoon in kwestie als elk lid van een bestuursorgaan van die rechtspersoon.

Art. 20, lid 1, tweede alinea, van de NIS2-richtlijn verduidelijkt dat deze bepaling geen afbreuk doet aan het nationale recht met betrekking tot de aansprakelijkheidsregels die gelden voor overheidsinstanties, alsook voor ambtenaren en verkozen of benoemde mandatarissen.

Deze bepaling wordt in het wetsontwerp omgezet via paragraaf 1, tweede lid, van het artikel waarop deze commentaar betrekking heeft. Naar Belgisch recht betekent dit dat dit wetsontwerp niet afwijkt van de bestaande aansprakelijkheidsregels waarnaar hierboven wordt verwezen, met name de wet van 10 februari 2003 betreffende de aansprakelijkheid van en voor personeelsleden in dienst van openbare rechtspersonen.

Art. 32

Ongeacht de taken die eventueel aan onderaannemers worden toevertrouwd, wijst dit artikel erop dat essentiële en belangrijke entiteiten verantwoordelijk blijven voor de uit te voeren risicoanalyse, alsook voor de keuze en uitvoering van de maatregelen in het kader van dit wetsontwerp. Deze bepaling doet geen afbreuk aan artikel 31, § 1, eerste lid, van dit wetsontwerp, waarnaar hierboven wordt verwezen.

Dat blijkt uit de NIS2-richtlijn. Art. 21, lid 1, bepaalt dat de entiteiten technische, operationele en organisatorische maatregelen moeten nemen. Volgens overweging 77 ligt “de verantwoordelijkheid voor het waarborgen van de beveiliging van netwerk- en informatiesystemen [...] voor een groot deel bij de essentiële en belangrijke entiteiten”. Overweging 83 wijst erop dat “essentiële en belangrijke entiteiten [...] de beveiliging van de netwerk- en informatiesystemen die zij bij hun activiteiten gebruiken, [moeten] waarborgen. Die systemen zijn voornamelijk particuliere netwerk- en informatiesystemen die door de interne IT-medewerkers van essentiële en belangrijke entiteiten worden beheerd of waarvan de beveiliging is uitbesteed. De maatregelen voor het beheer van cyberbeveiligingsrisico’s en de rapportageverplichtingen die in deze richtlijn zijn vastgesteld, moeten van toepassing zijn op de relevante essentiële en belangrijke entiteiten, ongeacht of deze entiteiten het onderhoud van hun netwerk- en informatiesystemen intern uitvoeren of uitbesteden” en overweging 89 voegt hieraan toe dat

et importantes devraient adopter une vaste gamme de pratiques de cyberhygiène de base, [...]”.

L'objectif du présent article est d'expliciter cette responsabilité incombant aux entités essentielles et importantes, nonobstant l'application de l'article 31, § 1^{er}, alinéa 1^{er}.

Art. 33

Cet article donne compétence au Roi, par arrêté délibéré en Conseil des ministres, d'imposer des mesures supplémentaires de gestion des risques en matière de cybersécurité spécifiques à un ou plusieurs (sous-)secteurs.

Ces mesures supplémentaires peuvent être adoptées après consultation de l'autorité nationale de cybersécurité et, le cas échéant, des autorités sectorielles concernées (pour autant qu'une autorité sectorielle ait été désignée pour le ou les (sous-)secteurs concernés) et des entités fédérées concernées.

Certains (sous-)secteurs pourraient, selon leurs spécificités, nécessiter des mesures supplémentaires. Celles-ci peuvent être de deux types soit des mesures additionnelles c'est à dire des mesures autres que celles déjà prévues par le NBN EN ISO/IEC 27.001 ou le Cyberfundamentals soit des mesures spécifiques c'est à dire des mesures qui explicitent comment comprendre la norme ISO IEC 27.001 ou le Cyberfundamentals pour le secteur concerné.

Cette disposition permet d'adopter *a posteriori* de telles mesures lorsque cela s'avère nécessaire.

CHAPITRE 2

Notification d'incidents

Section 1^{re}

Notification obligatoire

Art. 34

Cet article reprend les dispositions en matière de notifications obligatoires d'incidents de la directive NIS2, plus précisément le contenu de l'article 23, §§ 1^{er} à 3.

Tout d'abord, il est important de noter que le présent projet de loi a opté pour la terminologie “d'incidents significatifs”, dans une volonté de continuité avec la terminologie employée dans la loi NIS1, là où la directive

essentielle et belangrijke entiteiten “een breed scala aan basispraktijken op het gebied van cyberhygiène [moeten] toepassen, [...]”.

Dit artikel heeft tot doel om deze verantwoordelijkheid van de essentiële en belangrijke entiteiten toe te lichten, onverminderd de toepassing van artikel 31, § 1, eerste lid.

Art. 33

Dit artikel verleent de Koning de bevoegdheid om, bij besluit vastgesteld na overleg in de Ministerraad, bijkomende maatregelen voor het beheer van cyberbeveiligingsrisico's op te leggen die specifiek zijn voor een of meer (deel)sectoren.

Deze bijkomende maatregelen kunnen worden genomen na raadpleging van de nationale cyberbeveiligingsautoriteit en, in voorkomend geval, van de betrokken sectorale overheden (voor zover een sectorale overheid is aangewezen voor een of meer betrokken (deel)sectoren) en betrokken deelgebieden.

Sommige (deel)sectoren kunnen, naargelang hun specifieke kenmerken, aanvullende maatregelen vereisen. Deze kunnen van twee typen zijn: ofwel aanvullende maatregelen, d.w.z. maatregelen die afwijken van de maatregelen waarin NBN EN ISO/IEC 27.001 of de Cyberfundamentals al voorzien, ofwel specifieke maatregelen, d.w.z. maatregelen die uitleggen hoe de ISO IEC 27.001 norm of de Cyberfundamentals voor de betreffende sector begrepen moeten worden.

Deze bepaling maakt het mogelijk om deze maatregelen, indien nodig, achteraf te nemen.

HOOFDSTUK 2

Melding van incidenten

Afdeling 1

Verplichte melding

Art. 34

Dit artikel bevat de bepalingen inzake de verplichte melding van incidenten van de NIS2-richtlijn, meer bepaald de inhoud van artikel 23, leden 1 tot 3.

In de eerste plaats is het belangrijk om te vermelden dat in de Franse versie van dit wetsontwerp is gekozen voor de term “incidents significatifs” om redenen van coherentie met de terminologie van de NIS1-wet, terwijl

NIS2 emploie les termes “incidents importants”. Cela étant, les termes “incidents significatifs” du projet de loi doivent se comprendre comme ayant la même portée que les termes “incidents importants” de la directive.

L'approche de la directive NIS2 en matière de notification d'incidents significatifs, transposée par le présent projet de loi, établit plusieurs étapes “afin de trouver le juste équilibre entre, d'une part, la notification rapide qui aide à atténuer la propagation potentielle des incidents importants et permet aux entités essentielles et importantes de chercher de l'aide et, d'autre part, la notification approfondie qui permet de tirer des leçons précieuses des incidents individuels et d'améliorer au fil du temps la cyberrésilience des entreprises individuelles et de secteurs tout entiers” (considérant 101). La description de ces étapes et des obligations y afférentes sont transposées par les articles suivants du projet de loi.

Le présent article dispose que les entités essentielles et importantes doivent notifier tout incident significatif sur la fourniture de leurs services fournis dans les (sous-)secteurs repris aux annexes du projet de loi, en ce compris, le cas échéant, les informations qui permettent de déterminer si l'incident en question a un impact transfrontière.

La notification de l'incident significatif se fait au CSIRT national, selon les modalités fixées par un protocole conclu entre le CSIRT national et le NCCN, étant donné la nécessaire collaboration étroite entre ces deux autorités.

Le projet de loi utilise les termes “l'éventuelle” car il n'est pas certain qu'une autorité sectorielle soit désignée pour tous les secteurs repris aux annexes du projet de loi. Pour autant qu'une autorité sectorielle ait été désignée et qu'un incident impacte une entité faisant partie du secteur pour lequel l'autorité sectorielle a été désignée, la notification doit se faire également auprès de cette entité.

Les entités essentielles doivent également, le cas échéant, notifier sans retard injustifié aux destinataires de leurs services les incidents significatifs susceptibles de nuire à la fourniture des services précités.

De plus, en cas de cybermenace importante, les entités essentielles et importantes doivent notifier, encore une fois sans retard injustifié, aux destinataires de leurs services potentiellement affectés par cette cybermenace, la cybermenace elle-même (lorsque cela est approprié) et toutes les mesures ou corrections qui peuvent être

de la Franse versie van de NIS2-richtlijn de term “incidents importants” gebruikt. De term “incidents significatifs” in het wetsontwerp wordt verondersteld dezelfde draagwijdte te hebben als de term “incidents importants” in de richtlijn.

De aanpak van de NIS2-richtlijn inzake de melding van significante incidenten, die is omgezet door dit wetsontwerp, voorziet in meerdere fasen “om het juiste evenwicht te vinden tussen enerzijds een snelle melding die de potentiële verspreiding van significante incidenten helpt te beperken en essentiële en belangrijke entiteiten in staat stelt om bijstand te vragen, en anderzijds een grondige melding die het mogelijk maakt waardevolle lessen te trekken uit afzonderlijke incidenten en mettertijd de digitale weerbaarheid van afzonderlijke entiteiten en hele sectoren verbetert” (overweging 101). De beschrijving van deze fasen en de eraan verbonden verplichtingen worden omgezet door de volgende artikelen van het wetsontwerp.

Volgens dit artikel moeten essentiële en belangrijke entiteiten elk significant incident melden dat betrekking heeft op het verlenen van hun diensten in de (deel)sectoren opgenomen in de bijlagen van het wetsontwerp, met inbegrip van, in voorkomend geval, de informatie die nodig is om te bepalen of het betrokken incident grensoverschrijdende gevolgen heeft.

Significante incidenten worden aan het nationale CSIRT gemeld volgens de modaliteiten bepaald in een protocol gesloten tussen het nationale CSIRT en het NCCN. Het is immers noodzakelijk dat deze beide autoriteiten nauw samenwerken.

Het wetsontwerp gebruikt de woorden “de eventuele” omdat het niet zeker is dat een sectorale overheid wordt aangewezen voor alle sectoren opgenomen in de bijlagen van het wetsontwerp. Voor zover een sectorale overheid is aangewezen en een incident gevolgen heeft voor een entiteit die tot de sector behoort waarvoor de sectorale overheid is aangewezen, moet de melding ook aan deze entiteit worden bezorgd.

In voorkomend geval moeten essentiële entiteiten ook de ontvangers van hun diensten onverwijld in kennis stellen van significante incidenten die een nadelige invloed kunnen hebben op de verlening van voornoemde diensten.

Verder moeten essentiële en belangrijke entiteiten in geval van een significante cyberdreiging, nogmaals onverwijld, de ontvangers van hun diensten die mogelijk door deze cyberdreiging worden getroffen (indien van toepassing) in kennis stellen van de cyberdreiging zelf en hen meedelen welke maatregelen die

appliqués par ces destinataires en réponse à la cybermenace importante.

Par incidents significatifs, il faut comprendre les incidents qui “pourraient entraîner des perturbations opérationnelles graves des services ou des pertes financières pour [l’entité concernée], ou nuire à d’autres personnes physiques ou morales en causant un dommage matériel, corporel ou moral considérable. Cette évaluation initiale devrait tenir compte, entre autres, du réseau et des systèmes d’information touchés et notamment de leur importance dans la fourniture des services de l’entité, de la gravité et des caractéristiques techniques de la cybermenace et de toutes les vulnérabilités sous-jacentes qui sont exploitées ainsi que de l’expérience de l’entité en matière d’incidents similaires. Des indicateurs tels que la mesure dans laquelle le fonctionnement du service est affecté, la durée d’un incident ou le nombre de bénéficiaires de services touchés pourraient jouer un rôle important pour déterminer si la perturbation opérationnelle du service est grave” (directive NIS2, considérant 101).

Le paragraphe 3 habilite le Roi à établir, par arrêté délibéré en Conseil des ministres, après les consultations nécessaires, des seuils précis de notification en fonction du degré d’impact ou d’urgence de l’incident.

La notification devra, le cas échéant, se faire conformément aux actes d’exécution de la Commission européenne pour certaines catégories d’entités (les fournisseurs de services DNS, les registres de noms de domaine de premier niveau, les entités fournissant des services d’enregistrement de noms de domaine, les fournisseurs de services d’informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés ou les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux).

Enfin, il est indiqué que le simple fait de notifier un incident n’accroît pas la responsabilité de l’entité à l’origine de la notification.

Art. 35

Cet article détermine les étapes de la notification obligatoire d’incidents significatifs visée à l’article précédent. Il transpose l’article 23, § 4, de la directive NIS2.

Comme mentionné *supra*, la directive prévoit une approche par étapes de la notification obligatoire précitée.

ontvangers kunnen nemen in reactie op die significante cyberdreiging.

Onder significante incidenten moeten incidenten worden verstaan die een “ernstige operationele verstoring van de dienstverlening of financiële verliezen voor [de betrokken entiteit] kunnen veroorzaken of andere natuurlijke of rechtspersonen kunnen treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Bij een dergelijke initiële beoordeling moet rekening worden gehouden met onder meer de getroffen netwerk- en informatiesystemen, en met name het belang daarvan voor de door de entiteit verleende diensten, de ernst en technische kenmerken van een cyberdreiging en eventuele onderliggende kwetsbaarheden die worden uitgebuit, alsook de ervaring van de entiteit met soortgelijke incidenten. Indicatoren zoals de mate waarin de werking van de dienst wordt aangetast, de duur van een incident of het aantal getroffen afnemers van de diensten kunnen van belang zijn om vast te stellen of er sprake is van een ernstige operationele verstoring van de dienst” (NIS2-richtlijn, overweging 101).

Paragraaf 3 machtigt de Koning om, bij besluit vastgesteld na overleg in de Ministerraad en na de nodige raadplegingen, precieze meldingsdrempels te bepalen naargelang de impact of dringendheid van het incident.

De melding moet in voorkomend geval, overeenkomstig de uitvoeringsverordeningen van de Europese Commissie gebeuren voor bepaalde categorieën van entiteiten (DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten of aanbieders van onlinemarktplaatsen, onlinezoekmachines of platforms voor socialenetwerkdiensten).

Tot slot wordt vermeld dat een melding niet leidt tot blootstelling van de entiteit aan een verhoogde aansprakelijkheid.

Art. 35

Dit artikel bepaalt de fasen van de verplichte melding van significante incidenten als bedoeld in het vorige artikel. Het voorziet in de omzetting van artikel 23, lid 4, van de NIS2-richtlijn.

Zoals hierboven vermeld, voorziet de richtlijn in een gefaseerde aanpak van voornoemde verplichte melding.

En cas d'incidents significatifs, les étapes suivantes doivent être respectées par l'entité concernée dans le cadre de la notification:

1° sans retard injustifié et tout au plus dans les 24 heures après avoir pris connaissance de l'incident significatif, l'entité transmet une alerte précoce;

2° sans retard injustifié et tout au plus dans les 72 heures après avoir pris connaissance de l'incident significatif, l'entité communique une notification d'incident. À noter que les prestataires de services de confiance doivent communiquer la notification d'incident dans les 24 heures lorsque l'incident a un impact sur la fourniture de leurs services de confiance;

3° à la demande du CSIRT national ou, le cas échéant, de l'autorité sectorielle concernée (si une telle autorité a été désignée par le Roi), l'entité communique un rapport intermédiaire;

4° au plus tard un mois après la notification d'incident visée au 2°, l'entité transmet un rapport final;

5° Si le rapport final visé au 4° ne peut être transmis car l'incident est encore en cours, l'entité transmet un rapport d'avancement puis, dans le mois suivant le traitement définitif de l'incident, le rapport final.

L'alerte précoce indique si l'on suspecte que l'incident significatif pourrait avoir été causé par des actes illicites ou malveillants ou s'il pourrait avoir un impact transfrontière. Cette alerte précoce "devrait inclure uniquement les informations nécessaires pour porter l'incident important à la connaissance du CSIRT, ou, le cas échéant, de l'autorité compétente, et permettre à l'entité concernée de demander une assistance, si nécessaire" (considérant 102, directive NIS2). Cette alerte ne doit pas détourner "les ressources de l'entité effectuant la notification des activités liées à la gestion des incidents qui devraient avoir la priorité, afin d'éviter que les obligations de notification des incidents ne détournent les ressources de la gestion des incidents importants ou ne compromettent d'une autre manière les efforts déployés par l'entité à cet égard" (même considérant).

La notification d'incident visée 2° (voir *supra*) a pour objectif de mettre à jour les informations communiquées dans le cadre de l'alerte précoce. Elle fournit également une évaluation initiale de l'incident, y compris de sa gravité et de son impact, ainsi que des indicateurs de compromission, lorsqu'ils sont disponibles. Comme pour l'alerte précoce, la notification d'incident ne doit

In geval van significante incidenten moet de betrokken entiteit de volgende fasen doorlopen in het kader van de melding en bezorgt zij:

1° onverwijld en uiterlijk binnen 24 uur nadat zij kennis heeft gekregen van het significante incident, een vroegtijdige waarschuwing;

2° onverwijld en uiterlijk binnen 72 uur nadat zij kennis heeft gekregen van het significante incident, een incidentmelding. Opgemerkt wordt dat verleners van vertrouwensdiensten de incidentmelding binnen 24 uur moeten indienen wanneer het incident gevolgen heeft voor de verlening van hun vertrouwensdiensten;

3° op verzoek van het nationale CSIRT of, indien van toepassing, van de betrokken sectorale overheid (indien deze autoriteit is aangewezen door de Koning), een tussentijds verslag;

4° uiterlijk één maand na de in 2° bedoelde incidentmelding, een eindverslag;

5° Indien het in 4° bedoelde eindverslag niet kan worden ingediend omdat het incident nog aan de gang is, bezorgt de entiteit een voortgangsverslag en, binnen één maand nadat zij het incident definitief heeft afgehandeld, het eindverslag.

In de vroegtijdige waarschuwing wordt aangegeven of het significante incident vermoedelijk door een onrechtmatige of kwaadwillige handeling is veroorzaakt, dan wel grensoverschrijdende gevolgen zou kunnen hebben. Deze vroegtijdige waarschuwing "mag enkel de informatie bevatten die noodzakelijk is om het CSIRT of, in voorkomend geval, de bevoegde autoriteit op de hoogte te brengen van het significante incident en de betrokken entiteit in staat te stellen om indien nodig bijstand te vragen" (overweging 102, NIS2-richtlijn). Deze waarschuwing mag "de middelen van de meldende entiteit" niet afleiden "van activiteiten die verband houden met de behandeling van het incident en die als prioritair moeten worden aangemerkt, teneinde te voorkomen dat de verplichtingen inzake de melding van incidenten middelen onttrekken aan de respons op significante incidenten of de inspanningen van de entiteit op dat gebied anderszins in gevaar brengen" (dezelfde overweging).

De in 2° bedoelde incidentmelding (zie hierboven) heeft tot doel de informatie bij te werken die bij de vroegtijdige waarschuwing is ingediend. Ze bevat ook een initiële beoordeling van het incident, met inbegrip van de ernst en de gevolgen ervan en, indien beschikbaar, de indicatoren voor aantasting. Net zoals bij de vroegtijdige waarschuwing mag de incidentmelding de middelen van

pas détourner les ressources de l'entité effectuant la notification des activités liées à la gestion des incidents qui devraient avoir la priorité, afin d'éviter que les obligations de notification des incidents ne détournent les ressources de la gestion des incidents significatifs ou ne compromettent d'une autre manière les efforts déployés par l'entité à cet égard.

Le rapport intermédiaire contient les mises à jour pertinentes de la situation.

Le rapport final doit comprendre une description détaillée de l'incident, y compris de sa gravité et de son impact; le type de menace ou la cause profonde qui a probablement déclenché l'incident; les mesures d'atténuation appliquées et en cours; le cas échéant, l'impact transfrontière de l'incident.

Le rapport d'avancement contient les informations qui devraient se trouver dans le rapport final et qui sont en la possession de l'entité au moment de la communication du rapport d'avancement.

Art. 36

Cet article transpose l'article 23, § 5, de la directive NIS2, portant sur une partie des obligations du CSIRT national en matière de notifications obligatoires d'incidents.

Dans le cadre d'une notification obligatoire d'un incident significatif, le CSIRT national doit fournir sans retard injustifié et si possible dans les 24 heures suivant la réception de l'alerte précoce, une réponse à l'entité émettrice, en ce compris un retour d'information initial sur l'incident significatif et, à la demande de l'entité, des orientations ou des conseils opérationnels sur la mise en œuvre d'éventuelles mesures d'atténuation.

De plus, à la demande de l'entité, le CSIRT national doit fournir un soutien technique supplémentaire. S'il existe des suspicions que l'incident est de nature criminelle, le CSIRT national fournit également des orientations sur les modalités de notification de l'incident significatif aux autorités répressives.

Il est important de noter que, dans le cadre de ses missions, y compris les présentes tâches liées à l'intervention en cas d'incidents significatifs, le CSIRT national peut donner la priorité à certaines tâches plutôt qu'à d'autres, sur la base d'une approche basée sur les risques. Ainsi, si les ressources du CSIRT national sont fortement monopolisées par un incident particulièrement grave, et qu'il n'est pas possible de fournir une réponse

de la meldende entiteit niet afleiden van activiteiten die verband houden met de behandeling van het incident en die als prioritair moeten worden aangemerkt, teneinde te voorkomen dat de verplichtingen inzake de melding van incidenten middelen onttrekken aan de respons op significante incidenten of de inspanningen van de entiteit op dat gebied anderszins in gevaar brengen.

Het tussentijds verslag bevat relevante updates van de situatie.

Het eindverslag bevat een gedetailleerde beschrijving van het incident, met inbegrip van de ernst en de gevolgen ervan; het soort bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid; de toegepaste en lopende risicobeperkende maatregelen; in voorkomend geval, de grensoverschrijdende gevolgen van het incident.

Het voortgangsverslag bevat de informatie die in het eindverslag zou moeten staan, en waarover de entiteit beschikt op het moment dat het voortgangsverslag wordt ingediend.

Art. 36

Dit artikel voorziet in de omzetting van artikel 23, lid 5, van de NIS2-richtlijn, dat betrekking heeft op een deel van de verplichtingen van het nationale CSIRT inzake de verplichte melding van incidenten.

In het kader van de verplichte melding van een significant incident verstrekt het nationale CSIRT onverwijld, en zo mogelijk binnen 24 uur na ontvangst van de vroegtijdige waarschuwing, een antwoord aan de meldende entiteit, met inbegrip van een eerste feedback over het significante incident en, op verzoek van de entiteit, richtsnoeren of operationeel advies voor de uitvoering van mogelijke risicobeperkende maatregelen.

Bovendien moet het nationale CSIRT aanvullende technische ondersteuning verlenen indien de entiteit daarom verzoekt. Wanneer het vermoeden bestaat dat het incident van criminele aard is, verstrekt het nationale CSIRT ook richtsnoeren voor het melden van het significante incident aan de rechtshandavingsinstanties.

Het is belangrijk te vermelden dat het nationale CSIRT, in het kader van zijn opdrachten, met inbegrip van deze taken in verband met de respons op significante incidenten, voorrang kan geven aan bepaalde taken boven andere taken, op grond van een risicogebaseerde benadering. Indien de middelen van het nationale CSIRT bijvoorbeeld sterk in beslag worden genomen door een bijzonder ernstig incident, en het niet mogelijk is om

à une alerte précoce dans les 24 heures ou de fournir, sans retard, un soutien technique à une entité ayant soumis une notification d'incident sans compromettre son intervention dans le cadre de l'incident particulièrement grave précité, le CSIRT national peut privilégier l'intervention dans le cadre de l'incident particulièrement grave pour autant que cela se justifie du point de vue des risques.

Art. 37

Cet article transpose l'article 23, §§ 6 à 10, et porte sur le reste des obligations du CSIRT national et des autorités compétentes dans le cadre du présent projet de loi.

En premier lieu, lorsqu'un incident significatif concerne deux États membres ou plus (ou de manière générale, lorsque c'est approprié), le CSIRT national doit informer sans retard injustifié les autres États membres touchés par l'incident en question. Dans ce cadre, sont partagées des informations similaires à ce qui est communiqué au CSIRT national dans le cadre des alertes précoces, notifications d'incidents et rapports subséquents visés à l'article 35 du projet de loi. Ce faisant, le CSIRT national doit, dans le respect du droit de l'Union européenne ou du droit national, préserver la sécurité et les intérêts commerciaux de l'entité ainsi que la confidentialité des informations communiquées.

Ensuite, lorsque la sensibilisation du public est nécessaire pour prévenir un incident significatif ou pour faire face à un incident significatif en cours, ou encore lorsque la divulgation de l'incident significatif est dans l'intérêt public, le CSIRT national a la possibilité d'informer le public de l'incident significatif ou exiger que l'entité informe elle-même le public de cet incident. Pour ce faire, le CSIRT national doit avoir consulté au préalable l'entité concernée, le NCCN, l'autorité concernée (lorsqu'une telle autorité a été désignée) et, si l'entité concernée relève du pouvoir exécutif fédéral, le ministre compétent.

Conformément au paragraphe 3, le CSIRT national transmet les notifications obligatoires d'incidents significatifs reçues aux points de contact des autres États membres touchés par les incidents en question. Cette communication peut également se faire à la demande d'une autorité sectorielle.

En exécution de la directive NIS2, l'autorité nationale de cybersécurité doit rédiger des rapports de synthèse comprenant des données anonymisées et agrégées

binnen 24 uur te reageren op een vroegtijdige waarschuwing of onverwijld technische ondersteuning te bieden aan een entiteit die een incidentmelding heeft ingediend, zonder zijn respons op voornoemd ernstig incident in het gedrang te brengen, kan het nationale CSIRT voorrang geven aan de respons op het bijzonder ernstige incident voor zover dit gerechtvaardigd is wat de risico's betreft.

Art. 37

Dit artikel voorziet in de omzetting van artikel 23, leden 6 tot 10, en heeft betrekking op de overige verplichtingen van het nationale CSIRT en van de uit hoofde van dit wetsontwerp bevoegde autoriteiten.

In de eerste plaats moet het nationale CSIRT, wanneer een significant incident betrekking heeft op twee of meer lidstaten (of in het algemeen, indien van toepassing), de andere lidstaten die door het betrokken incident zijn getroffen onverwijld in kennis stellen. Daarbij wordt informatie gedeeld die vergelijkbaar is met die welke aan het nationale CSIRT wordt verstrekt in het kader van vroegtijdige waarschuwingen, incidentmeldingen en daaropvolgende verslagen als bedoeld in artikel 35 van het wetsontwerp. Daarbij moet het nationale CSIRT, overeenkomstig het Unie- of het nationale recht, de beveiligings- en commerciële belangen van de entiteit, alsook de vertrouwelijkheid van de verstrekte informatie beschermen.

Wanneer publieke bewustmaking nodig is om een significant incident te voorkomen of een lopend incident aan te pakken, of nog wanneer de bekendmaking van het significante incident in het algemeen belang is, heeft het nationale CSIRT vervolgens de mogelijkheid om het publiek te informeren over het significante incident of van de entiteit te verlangen dat zij het publiek zelf informeert over dat incident. Daartoe moet het nationale CSIRT vooraf de betrokken entiteit, het NCCN, de betrokken autoriteit (wanneer deze autoriteit is aangewezen) en, indien de betrokken entiteit tot de federale uitvoerende macht behoort, de bevoegde minister raadplegen.

Overeenkomstig paragraaf 3 stuurt het nationale CSIRT de ontvangen verplichte meldingen van significante incidenten door naar de contactpunten van de andere lidstaten die getroffen zijn door de betrokken incidenten. Deze kennisgeving kan ook gebeuren op verzoek van een sectorale overheid.

In uitvoering van de NIS2-richtlijn moet de nationale cyberbeveiligingsautoriteit samenvattende verslagen opstellen met geanonimiseerde en geaggregeerde

sur les incidents significatifs, les incidents, les cybermenaces et les incidents évités notifiés conformément à l'article 34, § 1^{er}, et à l'article 38, § 1^{er}, du projet de loi, afin de les communiquer à l'ENISA tous les 3 mois.

Enfin, dans le cadre de la coopération accrue avec les autorités compétentes dans le cadre de la loi de 1^{er} juillet 2011, le CSIRT national fournit à ces autorités des informations sur les incidents significatifs, les incidents, les cybermenaces et les incidents évités notifiés conformément à l'article 34, § 1^{er}, et à l'article 38, § 1^{er}, par les entités identifiées comme des entités critiques en vertu de la loi de 1^{er} juillet 2011.

Section 2

Notification volontaire

Art. 38

Cette article transpose l'article 30 de la directive NIS2 et porte sur la notification volontaire d'incidents.

La disposition fait la différence entre deux possibilités:

Premièrement, les entités essentielles et importantes peuvent notifier les incidents (non significatifs, qui eux *doivent* être notifiés), les cybermenaces et les incidents évités.

Deuxièmement, les entités autres que les entités essentielles et importantes, même si elles ne relèvent pas du champ d'application du projet de loi, peuvent notifier les incidents significatifs, les cybermenaces et les incidents évités.

Dans ces deux situations, le CSIRT national doit traiter ces notifications de la même manière que les notifications obligatoires évoquées *supra*. Cela étant, les notifications obligatoires peuvent être traitées de manière prioritaire par rapport aux notifications volontaires.

En principe, un signalement volontaire n'a pas pour effet direct de mener à une inspection visée à l'article 44 de l'entité ayant effectué le signalement ou de lui imposer des obligations supplémentaires auxquelles elle n'aurait pas été soumise si elle n'avait pas transmis la notification.

gegevens over significante incidenten, incidenten, cyberdreigingen en bijna-incidenten die overeenkomstig artikel 34, § 1, en artikel 38, § 1, van het wetsontwerp zijn gemeld, teneinde deze om de 3 maanden aan Enisa te bezorgen.

Tot slot verstrekt het nationale CSIRT de uit hoofde van de wet van 1 juli 2011 bevoegde autoriteiten, in het kader van de nauwere samenwerking met deze autoriteiten, informatie over significante incidenten, incidenten, cyberdreigingen en bijna-incidenten die overeenkomstig artikel 34, § 1, en artikel 38, § 1, zijn gemeld door entiteiten die uit hoofde van de wet van 1 juli 2011 als kritieke entiteiten zijn aangemerkt.

Afdeling 2

Vrijwillige melding

Art. 38

Dit artikel voorziet in de omzetting van artikel 30 van de NIS2-richtlijn en heeft betrekking op de vrijwillige melding van incidenten.

De bepaling maakt een onderscheid tussen twee mogelijkheden:

In de eerste plaats kunnen essentiële en belangrijke entiteiten (niet-significante) incidenten (significante incidenten *moeten* immers worden gemeld), cyberdreigingen en bijna-incidenten melden.

Op de tweede plaats kunnen andere entiteiten dan essentiële en belangrijke entiteiten, ook al behoren ze niet tot het toepassingsgebied van het wetsontwerp, significante incidenten, cyberdreigingen en bijna-incidenten melden.

In deze beide situaties moet het nationale CSIRT deze meldingen op dezelfde wijze verwerken als bovenvermelde verplichte meldingen. Er kan echter voorrang worden gegeven aan de verwerking van verplichte meldingen boven die van vrijwillige meldingen.

In principe geldt dat een vrijwillige melding er niet direct toe mag leiden dat een inspectie van de meldende entiteit volgens artikel 44 wordt opgestart of dat er bijkomende verplichtingen worden opgelegd waaraan zij niet zou zijn onderworpen indien zij de vrijwillige melding niet had ingediend.

TITRE 4

*Supervision et sanctions*CHAPITRE 1^{ER}**Supervision****Section 1^{re}***Evaluation périodique de la conformité*

Art. 39

Cet article établit l'obligation pour les entités essentielles de se soumettre à une évaluation périodique de la conformité de la mise en œuvre des mesures de gestion des risques en matière de cybersécurité et habilite le Roi à déterminer les modalités de cette évaluation ainsi que les cadres de références sur base desquels l'évaluation est effectuée. La fréquence de l'évaluation sera déterminée par les cadres de références eux-mêmes. Pour être conforme aux exigences de la loi en matière de cybersécurité, le champ d'application des mesures décrites dans ces cadres de références (par exemple, la norme NBN EN ISO/IEC 27.001) devra nécessairement correspondre à l'ensemble des réseaux et systèmes d'information utilisés par l'entité concernée.

L'évaluation régulière de la conformité peut consister soit en une évaluation effectuée par un organisme d'évaluation de la conformité agréé, soit en une inspection régulière effectuée par le service d'inspection de l'autorité nationale de cybersécurité. À la demande des autorités sectorielles, ces inspections peuvent être menées de manière conjointe sous la direction de l'autorité nationale de cybersécurité. À la demande des autorités sectorielles et moyennant l'accord de l'autorité nationale de cybersécurité, cette dernière peut ordonner au service d'inspection sectoriel d'effectuer l'inspection en ce qui concerne son secteur ou ses sous-secteurs.

Si le Roi a établi des mesures supplémentaires (additionnelles ou spécifiques) pour un ou plusieurs secteurs, ces mesures font l'objet d'une inspection par les services d'inspection des autorités sectorielles concernées. L'autorité nationale de cybersécurité reçoit copie des rapports d'inspection ou participe, à sa demande, aux inspections de manière conjointe, sous la direction de l'autorité sectorielle concernée.

Lorsque plusieurs cadres de références sont déterminés par le Roi, les entités essentielles choisissent librement parmi ces cadres de références, lequel ils appliquent dans le cadre de l'évaluation de la conformité.

TITEL 4

Toezicht en sancties

HOOFDSTUK 1

Toezicht**Afdeling 1***Regelmatische conformiteitsbeoordeling*

Art. 39

Dit artikel bepaalt dat essentiële entiteiten verplicht zijn zich te onderwerpen aan een regelmatige conformiteitsbeoordeling van de uitvoering van de maatregelen voor het beheer van cyberbeveiligingsrisico's en machtigt de Koning om de modaliteiten van deze beoordeling te bepalen, alsook de referentiekaders op basis waarvan de beoordeling gebeurt. De frequentie van de beoordeling wordt bepaald door de referentiekaders zelf. Om te voldoen aan de eisen van de wet op het vlak van cyberbeveiliging, moet het toepassingsgebied van de maatregelen die in deze referentiekaders worden beschreven (bijvoorbeeld de norm NBN EN ISO/IEC 27.001) noodzakelijkerwijs overeenstemmen met alle netwerk- en informatiesystemen die door de betrokken entiteit worden gebruikt.

De regelmatige conformiteitsbeoordeling kan ofwel een beoordeling door een erkende conformiteitsbeoordelingsinstantie zijn, of de vorm aannemen van een regelmatige inspectie door de inspectiedienst van de nationale cyberbeveiligingsautoriteit. Op verzoek van de sectorale overheden kunnen deze inspecties gezamenlijk worden uitgevoerd onder leiding van de nationale cyberveiligheidsautoriteit. Op verzoek van de sectorale overheden en mits akkoord van de nationale cyberbeveiligingsautoriteit kan deze laatste de sectorale inspectiedienst gelasten om de inspectie voor wat betreft haar sector of subsectoren alleen uit te voeren.

Indien de Koning bijkomende of bijzondere maatregelen (specifieke of aanvullende) voor één of meerdere sectoren heeft vastgelegd, worden deze maatregelen geïnspecteerd door de inspectiediensten van de betrokken sectorale overheden. De cyberbeveiligingsautoriteit ontvangt een kopie van de inspectieverslagen of neemt, of op verzoek, deel aan de inspecties gezamenlijk, onder leiding van de betrokken sectorale overheid.

Wanneer de Koning meerdere referentiekaders bepaalt, staat het essentiële entiteiten vrij om te kiezen welk referentiekader ze gebruiken in het kader van de conformiteitsbeoordeling.

Un tel mécanisme d'évaluation de la conformité a pour objectif non seulement de s'assurer de la conformité d'une entité à un moment donné, à l'issue d'un cycle d'évaluation périodique de la conformité mais également de permettre un premier contrôle ainsi que de fournir aux entités un processus d'auto-évaluation des risques encourus, des mesures mises en place et de la maturité de l'entité. L'usage de ces cadres de références est toujours basé sur l'analyse des risques réalisée par l'entité.

Dans le cadre de cette évaluation périodique de la conformité, l'autorité nationale de cybersécurité fournira des outils permettant aux entités essentielles d'effectuer une analyse des risques encourus. L'autorité développera également un cadre de référence, basé sur des normes et bonnes pratiques internationalement reconnus, qui sera mis à disposition gratuitement.

Art. 40

Cet article porte sur l'évaluation périodique de la conformité effectuée par un organisme d'évaluation de la conformité.

Cet organisme d'évaluation de la conformité doit pouvoir être en mesure d'évaluer adéquatement les entités essentielles sur base des cadres de références déterminés par le Roi. Pour s'en assurer, les organismes d'évaluation de la conformité devront être agréés selon les conditions fixées par le Roi. L'objectif de cette agrégation est de s'assurer que les organismes d'évaluation de la conformité respectent les conditions nécessaires à l'évaluation de la conformité visée à l'article 39, alinéa 1^{er}, 1°. L'agrégation permet également d'ajouter des conditions particulières, nécessaires pour la sécurité d'un ou plusieurs secteurs spécifiques.

Pour pouvoir vérifier que les organismes d'évaluation de la conformité agréés continuent de respecter les conditions de l'agrégation, le service d'inspection de l'autorité nationale de cybersécurité peut faire usage de ses pouvoirs de contrôle.

Par ailleurs, lorsque l'évaluation de la conformité concerne des entités critiques ou des entités de l'administration publique, l'organisme d'évaluation de la conformité ainsi que les personnes physiques qui effectueront l'évaluation devront disposer d'une habilitation de sécurité, obtenue conformément à la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé.

Doel van een dergelijk conformiteitsbeoordelingsmechanisme is niet alleen om na te gaan of een entiteit op een bepaald ogenblik, na afloop van een regelmatige conformiteitsbeoordelingscyclus, aan de conformiteitsregels voldoet, maar ook om een eerste controle mogelijk te maken, alsook om entiteiten een zelfbeoordelingsproces te bieden van de risico's die ze hebben gelopen, de maatregelen die ze hebben genomen en van de maturiteit van de entiteit. Het gebruik van deze referentiekaders wordt altijd gebaseerd op de risicoanalyse die door de entiteit gerealiseerd wordt.

In het kader van deze regelmatige conformiteitsbeoordeling zal de nationale cyberbeveiligingsautoriteit instrumenten beschikbaar stellen waarmee essentiële entiteiten een risicoanalyse kunnen uitvoeren. De autoriteit zal ook een referentiekader uitwerken op basis van internationaal erkende normen en goede praktijken, dat gratis ter beschikking zal worden gesteld.

Art. 40

Dit artikel heeft betrekking op de regelmatige conformiteitsbeoordeling die wordt uitgevoerd door een conformiteitsbeoordelingsinstantie.

Deze conformiteitsbeoordelingsinstantie moet essentiële entiteiten adequaat kunnen beoordelen op basis van door de Koning bepaalde referentiekaders. Daartoe moeten conformiteitsbeoordelingsinstanties erkend zijn volgens de door de Koning bepaalde voorwaarden. Deze erkenning heeft tot doel te waarborgen dat deze instanties voldoen aan de voorwaarden die nodig zijn voor de in artikel 39, eerste lid, 1°, bedoelde conformiteitsbeoordeling. De erkenning maakt het ook mogelijk om specifieke voorwaarden toe te voegen die nodig zijn voor de veiligheid van een of meer specifieke sectoren.

Om na te gaan of erkende conformiteitsbeoordelingsinstanties nog aan de erkenningsvoorwaarden voldoen, kan de inspectiedienst van de nationale cyberbeveiligingsautoriteit gebruik maken van zijn toezichtsbevoegdheden.

Wanneer de conformiteitsbeoordeling betrekking heeft op kritieke entiteiten of overheidsinstanties, moeten de conformiteitsbeoordelingsinstantie en de natuurlijke personen die de beoordeling uitvoeren bovendien over een veiligheidsmachtiging beschikken, die wordt verkregen overeenkomstig de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst.

Art. 41

Cet article permet aux entités importantes de se soumettre également à une évaluation périodique de la conformité. Une telle évaluation ne leur est pas imposée car, conformément à l'article 33, § 1^{er}, de la directive NIS2, ces entités ne sont soumises qu'à un contrôle *ex post* dans le cadre du présent projet de loi.

Art. 42

Selon cet article, toute entité qui se soumet à l'évaluation de la conformité visée aux articles 39, alinéa 1^{er}, 1°, et 41 bénéficie d'une présomption de conformité des obligations visées à l'article 30. Cette présomption peut être renversée par le service d'inspection compétent lorsque ce dernier constate des manquements aux obligations créées par le présent projet de loi.

Art. 43

Cet article prévoit que l'autorité nationale de cybersécurité doit établir, maintenir à jour et rendre disponible une liste des organismes d'évaluation de la conformité agréés par elle.

Section 2

Dispositions générales relatives au service d'inspection

Art. 44

Cet article porte sur les autorités pouvant être compétentes en matière de supervision et sur leurs tâches de contrôle.

Le service d'inspection de l'autorité nationale de cybersécurité a pour tâche de réaliser des contrôles du respect par les entités essentielles et importantes des mesures de gestion des risques en matière de cybersécurité et des règles de notification des incidents.

Il est possible que, dans le cadre du projet de loi, des dispositions (sous-)sectorielles spécifiques en matière de mesures de gestion des risques en matière de cybersécurité aient été adoptées conformément à l'article 33.

En principe, l'autorité sectorielle compétente ou le service d'inspection sectoriel compétent pour un (sous-)secteur pour lequel il existe de telles dispositions (sous-)sectorielles spécifiques doit réaliser des contrôles du respect par les entités essentielles et importantes relevant dudit (sous-)secteur des dispositions (sous-)sectorielles

Art. 41

Dit artikel wijst erop dat belangrijke entiteiten zich ook kunnen onderwerpen aan een regelmatige conformiteitsbeoordeling. Deze beoordeling is niet verplicht omdat deze entiteiten, overeenkomstig artikel 33, lid 1, van de NIS2-richtlijn, in het kader van dit wetsontwerp alleen onderworpen zijn aan toezicht achteraf ("*ex post*").

Art. 42

Volgens dit artikel geniet elke entiteit die zich onderwerpt aan de in de artikelen 39, eerste lid, 1°, en 41 bedoelde conformiteitsbeoordeling het vermoeden dat de in artikel 30 bedoelde verplichtingen worden nageleefd. Dit vermoeden kan worden weerlegd door de bevoegde inspectiedienst wanneer deze laatste inbreuken vaststelt op de door dit wetsontwerp ingevoerde verplichtingen.

Art. 43

Dit artikel bepaalt dat de nationale cyberbeveiligingsautoriteit een lijst van de door haar erkende conformiteitsbeoordelingsinstanties moet opstellen, bijhouden en beschikbaar stellen.

Afdeling 2

Algemene bepalingen betreffende de inspectiedienst

Art. 44

Dit artikel heeft betrekking op de autoriteiten die bevoegd kunnen zijn voor het toezicht en op hun toezichthoudende taken.

De inspectiedienst van de nationale cyberbeveiligingsautoriteit heeft als taak controles uit te voeren om na te gaan of essentiële en belangrijke entiteiten de maatregelen voor het beheer van cyberbeveiligingsrisico's en de regels voor het melden van incidenten naleven.

Het is mogelijk dat, in het kader van het wetsontwerp, specifieke (deel)sectorale bepalingen inzake maatregelen voor het beheer van cyberbeveiligingsrisico's zijn aangenomen overeenkomstig artikel 33.

In principe moet de bevoegde sectorale overheid of de sectorale inspectiedienst die bevoegd is voor een (deel)sector waarin deze specifieke (deel)sectorale bepalingen gelden, controles uitvoeren om na te gaan of essentiële en belangrijke entiteiten die tot deze (deel)sector behoren, voornoemde specifieke (deel)sectorale bepalingen

spécifiques précitées. Cela étant, en l'absence d'autorité sectorielle ou de service d'inspection sectoriel compétent, le service d'inspection de l'autorité nationale de cybersécurité réalise les contrôles précités.

Dans le cadre du commentaires des articles du présent projet de loi, le service d'inspection de l'autorité nationale de cybersécurité, les autorités sectorielles (dans le cadre de leurs potentielles compétences de contrôle) et/ou les services d'inspection sectoriels sont collectivement appelés les autorités compétentes pour le contrôle.

Le présent article dispose que, dans le cadre d'une demande d'informations ou de preuves, les autorités compétentes pour le contrôle doivent mentionner la finalité de la demande, les informations ou preuves précises demandées et le délai dans lequel celles-ci doivent être fournies par l'entité à qui s'adresse la demande.

Le cas échéant, les autorités compétentes pour le contrôle peuvent faire appel à des experts dans le cadre de leur tâches de contrôle ou fixer des priorités dans l'exécution de leurs tâches.

Art. 45

Cet article porte sur la coopération et l'échange d'informations entre autorités dans le cadre du projet de loi, lorsque les entités inspectées relèvent par ailleurs du champ d'application de la directive CER ou du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (ci-après le "règlement DORA"), conformément aux articles 32, §§ 9 et 10, et 33, § 6, de la directive NIS2.

Ces trois textes juridiques sont fortement liés, raison pour laquelle "il convient d'assurer la cohérence des approches entre la directive (UE) 2022/2557, [...]. Les autorités compétentes en vertu de la [directive NIS2] et les autorités compétentes en vertu de la directive [CER] devraient, si possible en temps réel, coopérer et échanger des informations à cette fin." (considérant 30, directive NIS2) et "il est important de conserver une relation forte et de maintenir l'échange d'informations avec le secteur financier dans le cadre de la présente directive. À cet effet, le règlement [DORA] permet aux autorités européennes de surveillance (AES) et aux autorités compétentes en vertu dudit règlement de participer aux activités du groupe de coopération, ainsi que d'échanger des informations et de coopérer avec les points de contact uniques ainsi qu'avec les CSIRT

naleven. Bij gebrek aan een bevoegde sectorale overheid of sectorale inspectiedienst voert de inspectiedienst van de nationale cyberbeveiligingsautoriteit de genoemde controles uit.

In het kader van de commentaar bij de artikelen van dit wetsontwerp worden de inspectiedienst van de nationale cyberbeveiligingsautoriteit, de sectorale overheden (in het kader van hun mogelijke toezichtsbevoegdheden) en/of de sectorale inspectiediensten samen de voor het toezicht bevoegde autoriteiten genoemd.

Dit artikel bepaalt dat, in het kader van een verzoek om informatie of bewijzen, de voor het toezicht bevoegde autoriteiten het doeleinde van het verzoek, de precieze informatie of bewijzen die worden gevraagd en de termijn waarbinnen deze moeten worden verstrekt door de entiteit aan wie het verzoek is gericht, moeten vermelden.

In voorkomend geval kunnen de voor het toezicht bevoegde autoriteiten een beroep doen op experts in het kader van hun toezichthoudende taken of prioriteiten bepalen bij de uitvoering van hun taken.

Art. 45

Dit artikel is gewijd aan de samenwerking en informatie-uitwisseling tussen autoriteiten in het kader van het wetsontwerp, wanneer de geïnspecteerde entiteiten bovendien tot het toepassingsgebied behoren van de CER-richtlijn of van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector (hierna "DORA-verordening"), overeenkomstig de artikelen 32, leden 9 en 10, en 33, lid 6, van de NIS2-richtlijn.

Deze drie juridische teksten zijn nauw met elkaar verweven. Om die reden "moet een coherente aanpak worden gewaarborgd tussen Richtlijn (EU) 2022/2557 [...]. Daartoe moeten de uit hoofde van [de NIS2-richtlijn] bevoegde autoriteiten en die uit hoofde van [de CER-richtlijn], indien mogelijk in realtime, samenwerken en informatie uitwisselen." (overweging 30, NIS2-richtlijn) en "is het van belang een sterke relatie en de uitwisseling van informatie met de financiële sector uit hoofde van deze richtlijn in stand te houden. Daartoe biedt [de DORA-verordening] de Europese toezichthoudende autoriteiten (ETA's) en de uit hoofde van die verordening bevoegde autoriteit en de mogelijkheid deel te nemen aan de activiteiten van de samenwerkingsgroep en informatie uit te wisselen en samen te werken met de centrale contactpunten en met de CSIRT's en de uit

et les autorités compétentes en vertu de la [directive NIS2]" (considérant 28, directive NIS2).

Art. 46

Cet article porte sur l'assistance mutuelle entre autorités des États membres dans le cadre de la supervision et de l'exécution des lois nationales transposant la directive NIS2.

Selon la directive NIS2, "afin de garantir le respect par les entités des obligations qui leur incombent en vertu de la présente directive, les États membres devraient coopérer et se prêter mutuellement assistance en ce qui concerne les mesures de supervision et d'exécution, en particulier lorsqu'une entité fournit des services dans plus d'un État membre ou lorsque son réseau et ses systèmes d'information sont situés dans un État membre autre que celui où elle fournit des services" (considérant 134).

Ainsi, la disposition permet aux autorités compétentes pour le contrôle de solliciter la coopération et l'assistance des autorités d'autres États membres compétentes dans le cadre de leur propre loi de transposition de la directive NIS2. Cette sollicitation peut porter sur des mesures de supervision et d'exécution ou consister en une demande (motivée) d'assistance mutuelle en vue d'assurer la mise en œuvre effective, efficace et cohérente des mesures de supervision ou d'exécution. Une demande d'assistance mutuelle peut porter sur des demandes d'informations et des mesures de contrôle.

Selon la directive toujours, "lorsqu'une autorité compétente fournit une assistance qui lui est demandée, elle devrait prendre des mesures de supervision ou d'exécution conformément au droit national" (considérant 134). Ainsi, "l'État membre qui a reçu une demande d'assistance mutuelle devraient [sic], dans les limites de cette demande, prendre des mesures de supervision et d'exécution appropriées à l'égard de l'entité faisant l'objet de cette demande et qui fournit des services ou possède un réseau et un système d'information sur le territoire dudit État membre" (considérant 135).

Conformément à la directive (les considérants précités et l'article 35), le présent article prévoit en son paragraphe 2 que les autorités compétentes pour le contrôle coopèrent avec et apportent leur assistance aux autorités de contrôle compétentes en matière de cybersécurité d'autres États membres qui en font la demande, lorsque les réseaux et les systèmes d'information de l'entité concerné sont situés dans le territoire belge. Cette coopération et/ou assistance de la part des

hoofde van [de NIS2-richtlijn] bevoegde autoriteiten." (overweging 28, NIS2-richtlijn).

Art. 46

Dit artikel heeft betrekking op de wederzijdse bijstand tussen autoriteiten van lidstaten in het kader van het toezicht op en de uitvoering van de nationale wetten die voorzien in de omzetting van de NIS2-richtlijn.

Volgens de NIS2-richtlijn moeten lidstaten "om ervoor te zorgen dat entiteiten hun in deze richtlijn vastgelegde verplichtingen nakomen, [...] met elkaar samenwerken en elkaar bijstaan op het gebied van toezicht- en handhavingsmaatregelen, met name wanneer een entiteit diensten verleent in meer dan één lidstaat of wanneer haar netwerk- en informatiesystemen zich bevinden in een andere lidstaat dan die waar zij diensten verleent." (overweging 134).

Zo verduidelijkt de bepaling dat de voor het toezicht bevoegde autoriteiten de autoriteiten van andere bevoegde lidstaten om samenwerking en bijstand kunnen verzoeken in het kader van hun eigen omzettingswet van de NIS2-richtlijn. Dit verzoek kan betrekking hebben op toezichts- en handhavingsmaatregelen of op een (met redenen omkleed) verzoek om wederzijdse bijstand zijn met het oog op een effectieve, efficiënte en consistente uitvoering van de toezichts- of handhavingsmaatregelen. Een verzoek om wederzijdse bijstand kan betrekking hebben op verzoeken om informatie en toezichtsmaatregelen.

Verder wijst de richtlijn op het volgende: "Bij het verlenen van bijstand moet de aangezochte bevoegde autoriteit toezicht- of handhavingsmaatregelen nemen overeenkomstig het nationale recht." (overweging 134). Zo "moet een lidstaat die een verzoek om wederzijdse bijstand heeft ontvangen, binnen de grenzen van dat verzoek passende toezichts- en handhavingsmaatregelen nemen ten aanzien van de entiteit die het voorwerp van dat verzoek is, en die diensten verleent of over een netwerk- en informatiesysteem op het grondgebied van die lidstaat beschikt" (overweging 135).

Overeenkomstig de richtlijn (voornoemde overwegingen en artikel 35) bepaalt paragraaf 2 van dit artikel dat de voor het toezicht bevoegde autoriteiten samenwerken met en bijstand verlenen aan de toezichthoudende autoriteiten bevoegd voor cyberbeveiliging van andere lidstaten indien deze hierom verzoeken en de netwerk- en informatiesystemen van de betrokken entiteit zich op Belgisch grondgebied bevinden. Deze samenwerking en/of bijstand door de Belgische autoriteiten moet in

autorités belges doit se faire de manière proportionnée à leurs ressources et rentrer dans le cadre de leurs compétences.

Dans le cadre de cette coopération et/ou assistance, les autorités belges compétentes pour le contrôle appliquent les dispositions du présent projet de loi et pas celles des lois de transposition des autres États membres.

La demande précitée peut porter sur des mesures de supervision et d'exécution ou consister en une demande (motivée) d'assistance mutuelle en vue d'assurer la mise en œuvre effective, efficace et cohérente des mesures de supervision ou d'exécution. Une demande d'assistance mutuelle peut porter sur des demandes d'informations et des mesures de contrôle.

Dans le cadre de cette coopération et/ou assistance de la part des autorités belges, l'autorité nationale de cybersécurité doit, en tant que point de contact unique, rassembler les informations, y compris concernant les consultations, en ce qui concerne les mesures de supervision et d'exécution prises au niveau national et les communiquer aux autorités de contrôle compétentes en matière de cybersécurité d'autres États membres.

Une demande de coopération ou d'assistance d'un autre État membre ne peut être refusée que s'il est établi que l'autorité concernée par la demande n'est pas compétente pour fournir l'assistance demandée, que l'assistance demandée n'est pas proportionnée aux tâches de supervision de ladite autorité ou que la demande concerne des informations ou implique des activités dont la divulgation ou l'exercice seraient contraires aux intérêts essentiels de la sécurité nationale, la sécurité publique ou la défense de la Belgique. Avant de pouvoir refuser la demande, l'autorité faisant l'objet de la demande doit consulter les autres autorités concernées et, le cas échéant, la Commission européenne et l'ENISA si un État membre le demande.

Art. 47

Cet article porte sur les membres des autorités compétentes pour le contrôle qui effectuent les tâches d'inspection.

Ces membres doivent être dotés d'une carte de légitimation afin de pouvoir prouver leur identité et leur appartenance à l'une des autorités compétentes pour le contrôle. La compétence de fixer le modèle de cette carte de légitimation est dévolue au Roi.

verhouding staan tot hun middelen en binnen hun bevoegdheden vallen.

In het kader van deze samenwerking en/of bijstand passen de voor het toezicht bevoegde Belgische autoriteiten de bepalingen van dit wetsontwerp toe en niet de omzettingswetten van de andere lidstaten.

Voornoemd verzoek kan betrekking hebben op toezichts- en handhavingsmaatregelen of een (met redenen omkleed) verzoek om wederzijdse bijstand zijn met het oog op een effectieve, efficiënte en consistente uitvoering van de toezichts- of handhavingsmaatregelen. Een verzoek om wederzijdse bijstand kan betrekking hebben op verzoeken om informatie en toezichtsmaatregelen.

In het kader van deze samenwerking en/of bijstand door de Belgische autoriteiten moet de nationale cyberbeveiligingsautoriteit, als centraal contactpunt, informatie verzamelen, met inbegrip van informatie inzake raadplegingen, over de toezichts- en handhavingsmaatregelen die op nationaal niveau zijn genomen en deze aan de autoriteiten van andere lidstaten bezorgen die bevoegd zijn voor het toezicht inzake cyberbeveiliging.

Een verzoek om samenwerking of bijstand van een andere lidstaat mag alleen worden geweigerd indien wordt vastgesteld dat de autoriteit aan wie het verzoek is gericht, niet bevoegd is om de gevraagde bijstand te verlenen, de gevraagde bijstand niet in verhouding staat tot de toezichthoudende taken van deze autoriteit of het verzoek betrekking heeft op informatie of activiteiten inhoudt die, indien ze openbaar zouden worden gemaakt of zouden worden uitgevoerd, in strijd zouden zijn met de wezenlijke belangen van de nationale veiligheid, de openbare veiligheid of de defensie van België. Alvorens het verzoek te kunnen afwijzen, moet de autoriteit aan wie het verzoek is gericht, de andere betrokken autoriteiten raadplegen en, in voorkomend geval, de Europese Commissie en Enisa indien een lidstaat hierom verzoekt.

Art. 47

Dit artikel heeft betrekking op de leden van de voor het toezicht bevoegde autoriteiten die inspectietaken uitvoeren.

Deze leden beschikken over een legitimatiekaart om hun identiteit te bewijzen en aan te tonen dat zij tot een van de voor het toezicht bevoegde autoriteiten behoren. De Koning is bevoegd om het model van deze legitimatiekaart te bepalen.

Le paragraphe 2 de cette disposition porte sur les conflits d'intérêts. Par principe, les membres des autorités compétentes pour le contrôle qui effectuent les tâches de contrôle ne peuvent avoir d'intérêt dans les entités qu'ils doivent contrôler, susceptible de compromettre leur objectivité, impartialité ou indépendance, quel qu'il soit. Ces personnes doivent prêter serment auprès du fonctionnaire dirigeant de leur service.

Les membres des autorités compétentes pour le contrôle qui effectuent les tâches d'inspection ne peuvent pas non plus recevoir d'instructions de personnes tierces dans le cadre de leurs attributions. Par ailleurs, afin d'éviter les situations de conflits d'intérêt, il leur est interdit d'être présents lors d'une délibération ou décision sur les dossiers pour lesquels ils ont un intérêt quelconque.

La compétence de désigner d'autres situations comme constituant des conflits d'intérêts est dévolue au Roi.

Les autorités compétentes pour le contrôle doivent prendre les mesures nécessaires pour assurer l'indépendance de leurs membres qui effectuent les tâches de contrôle. Ces mesures doivent permettre de prévenir, d'identifier et, le cas échéant, de résoudre les conflits d'intérêts actuels ou potentiels.

Section 3

*La supervision des entités par
le service d'inspection*

Art. 48

Cet article porte sur les pouvoirs en matière de contrôle des autorités compétentes pour le contrôle et les garde-fous y afférents afin de garantir le respect des droits des personnes inspectées. Ces autorités disposent de larges pouvoirs afin d'effectuer des contrôles approfondis du respect du projet de loi. Étant donné l'étendue des pouvoirs conférés à ces autorités, l'article précise, en son paragraphe 7, que les moyens mis en œuvre par les membres assermentés des autorités compétentes pour le contrôle doivent être appropriés et nécessaires au contrôle du respect du projet de loi. Par ailleurs, il faut souligner que les membres assermentés ne sont pas des officiers de police judiciaire. Ils ne peuvent faire usage de la contrainte à l'encontre des personnes contrôlées et ne peuvent, dès lors, forcer l'accès aux informations, *a fortiori* aux informations protégées par l'article 458 du Code pénal.

Paragraaf 2 van deze bepaling behandelt de belangenconflicten. In principe mogen de leden van de voor het toezicht bevoegde autoriteiten die toezichthoudende taken uitvoeren, geen enkel belang hebben in de entiteiten waarop zij toezicht dienen uit te oefenen, waardoor hun objectiviteit, onpartijdigheid of onafhankelijkheid in het gedrang zou kunnen komen. Deze personen moeten de eed afleggen de eed bij de leidend ambtenaar van hun dienst.

De leden van de voor het toezicht bevoegde autoriteiten die inspectietaken uitvoeren, mogen evenmin instructies van derden krijgen in het kader van hun bevoegdheden. Om belangenconflicten te voorkomen is het hen bovendien verboden aanwezig te zijn bij een beraadslaging of beslissing over dossiers waarin zij enig belang hebben.

De Koning is bevoegd om andere situaties te benoemen als belangenconflicten.

De voor het toezicht bevoegde autoriteiten moeten de nodige maatregelen nemen om de onafhankelijkheid te waarborgen van hun leden die toezichthoudende taken uitvoeren. Deze maatregelen hebben tot doel de huidige of mogelijke belangenconflicten te voorkomen, te identificeren en, in voorkomend geval, op te lossen.

Afdeling 3

*Het door de inspectiedienst uitgeoefende toezicht
op de entiteiten*

Art. 48

Dit artikel heeft betrekking op de toezichthoudende bevoegdheden van de voor het toezicht bevoegde autoriteiten en de eraan verbonden waarborgen om ervoor te zorgen dat de rechten van de geïnspecteerde personen worden gerespecteerd. Deze autoriteiten beschikken over ruime bevoegdheden om grondige controles uit te voeren op de naleving van het wetsontwerp. Gezien de omvang van de bevoegdheden van deze autoriteiten verduidelijkt paragraaf 7 van dit artikel dat de middelen die de beëdigde leden van de voor het toezicht bevoegde autoriteiten gebruiken, passend en noodzakelijk moeten zijn voor het toezicht op de naleving van het wetsontwerp. Voorts moet worden benadrukt dat de beëdigde leden geen officieren van gerechtelijke politie zijn. Zij mogen geen gebruik maken van dwang jegens gecontroleerde personen en kunnen bijgevolg geen toegang afdwingen tot informatie, *a fortiori* tot informatie die door artikel 458 van het Strafwetboek beschermd is.

La disposition reprend les pouvoirs listés aux articles 32, § 2, et 33, § 2, de la directive NIS2. De plus, d'autres pouvoirs sont conférés aux autorités compétentes pour le contrôle afin qu'elles puissent mener à bien leurs tâches de contrôle et d'imposition de mesures administratives.

Les autorités compétentes pour le contrôle peuvent notamment prendre l'identité des personnes présentes lors d'un contrôle et pénétrer sans avertissement préalable dans tous les locaux utilisés par l'entité contrôlée. En pratique, le nom des personnes pouvant pénétrer sans avertissement préalable peut être fourni à l'avance pour plus de prévisibilité. Lorsqu'il s'agit de locaux habités, ces autorités ne peuvent y pénétrer que moyennant l'autorisation préalable d'un juge d'instruction. Les paragraphes 2 et 3 déterminent la procédure et les éléments à fournir au juge d'instruction. Les autorités compétentes peuvent aussi demander l'assistance des services de la police fédérale ou locale. À noter qu'il ne s'agit pas pour les services de police locale ou fédérale d'une obligation d'assistance. Lorsque, par exemple, l'état de leur effectif ne leur permet pas d'assister l'autorité compétente pour le contrôle qui aurait introduit une demande, les services de police peuvent évidemment refuser cette demande.

Il est précisé également les règles à respecter en cas d'audition et celles relatives aux données consultables.

Dans le cadre des contrôles, les autorités compétentes pour le contrôle peuvent consulter tous les supports d'information et les données qu'ils contiennent, se faire produire le système informatique et les données qu'il contient dont ils ont besoin pour leurs examens et constatations, et en prendre ou en demander gratuitement des extraits, des duplicatas ou des copies.

Lorsque les autorités compétentes pour le contrôle constatent une violation de données à caractère personnel au sens du règlement européen 2016/679 (RGPD), ils doivent informer l'Autorité de protection des données sans retard injustifié.

Pour finir, les contrôles auprès des entités importantes ne peuvent s'organiser que de manière réactive (*ex post*).

Art. 49

Cet article dispose que chaque autorité compétente pour le contrôle rédige un rapport à la fin de chaque

De bepaling bevat de bevoegdheden die zijn opgesomd in de artikelen 32, lid 2, en 33, lid 2, van de NIS2-richtlijn. Bovendien worden andere bevoegdheden toevertrouwd aan de voor het toezicht bevoegde autoriteiten met het oog op de uitvoering van hun toezichthoudende taken en het opleggen van administratieve maatregelen.

De voor het toezicht bevoegde autoriteiten mogen met name de identiteit opnemen van de personen die aanwezig zijn bij een controle en zonder voorafgaande verwittiging alle lokalen betreden die door de gecontroleerde entiteit worden gebruikt. In de praktijk kunnen de namen van de personen die zonder voorafgaande verwittiging mogen binnengaan, vooraf worden verstrekt om de voorspelbaarheid te verbeteren. Indien de lokalen bewoond zijn, mogen deze autoriteiten de lokalen alleen betreden mits vooraf een machtiging is uitgereikt door de onderzoeksrechter. De paragrafen 2 en 3 gaan nader in op de procedure en de informatie die aan de onderzoeksrechter moet worden verstrekt. De bevoegde autoriteiten kunnen ook bijstand vragen aan de federale of lokale politiediensten. Opgemerkt wordt dat federale of lokale politiediensten niet verplicht zijn om deze bijstand te verlenen. Wanneer hun personeelsbestand bijvoorbeeld niet toelaat om bijstand te verlenen aan de voor het toezicht bevoegde autoriteit die een verzoek heeft ingediend, kunnen de politiediensten dit verzoek uiteraard weigeren.

Voorts komen de na te leven regels aan bod in geval van een verhoor en met betrekking tot de gegevens die mogen worden geraadpleegd.

In het kader van de controles mogen de voor het toezicht bevoegde autoriteiten alle informatiedragers en de erin opgenomen gegevens raadplegen, zich het informaticasysteem en de erin opgenomen gegevens die zij nodig hebben voor hun onderzoeken en vaststellingen doen voorleggen, en er kosteloos uittreksels, duplicaten of kopieën van nemen of vragen.

Wanneer de voor het toezicht bevoegde autoriteiten een inbreuk in verband met persoonsgegevens zoals gedefinieerd in de Europese Verordening 2016/679 (AVG) vaststellen, moeten zij de Gegevensbeschermingsautoriteit daarvan onverwijld in kennis stellen.

Tot slot mogen controles van belangrijke entiteiten alleen achteraf (*ex post*) worden georganiseerd.

Art. 49

Dit artikel bepaalt dat elke voor het toezicht bevoegde autoriteit een verslag opstelt na afloop van elke controle

contrôle et le communiquer, d'abord à l'entité inspectée, ensuite aux autres autorités compétentes pour le contrôle.

Art. 50

Cet article impose à l'entité contrôlée d'apporter son entière collaboration aux autorités compétentes pour le contrôle.

Le Roi est habilité à déterminer, par (sous-) secteur, des rétributions, en ce compris les modalités de calcul et de paiement, relatives aux prestations d'inspection. Une telle décision ne peut avoir lieu qu'après avis de l'autorité nationale de cybersécurité, par arrêté délibéré en Conseil des ministres.

Pour rappel, n'étant pas des officiers de police judiciaire, les membres des autorités compétentes pour le contrôle qui effectuent les tâches de contrôle ne peuvent forcer l'entité à coopérer. Cela étant, ils peuvent consigner dans un procès-verbal le refus de l'entité d'apporter sa collaboration lors du contrôle, voir la communication volontaire d'informations inexacts ou incomplètes ou l'empêchement ou l'entrave volontaire de l'exécution du contrôle par les autorités compétentes pour le contrôle, conformément au paragraphe 3.

CHAPITRE 2

Les mesures et amendes administratives

Section 1^{re}

Procédure

Dans le cadre de la présente section, il faut préciser qu'en l'absence de dispositions spécifiques, le Conseil d'État est compétent pour les recours en annulation des décisions imposant des mesures administratives prises en exécution du présent projet de loi.

Art. 51

Cet article détermine la procédure à l'issue de laquelle des mesures administratives peuvent être prises par les autorités compétentes pour le contrôle à l'égard d'entités essentielles ou importantes qui ne respecteraient pas le projet de loi.

Dans un premier temps, les manquements doivent être constatés dans un procès-verbal par les membres

en het eerst aan de geïnspecteerde entiteit bezorgt en vervolgens aan de andere voor het toezicht bevoegde autoriteiten.

Art. 50

Dit artikel bepaalt dat de gecontroleerde entiteit haar volledige medewerking moet verlenen aan de voor het toezicht bevoegde autoriteiten.

De Koning is gemachtigd om, per (deel)sector, retributies te bepalen, met inbegrip van de berekenings- en betalingsregels, voor de inspectieprestaties. Een dergelijke beslissing kan slechts worden genomen na advies van de nationale cyberbeveiligingsautoriteit, bij besluit vastgesteld na overleg in de Ministerraad.

Ter herinnering, aangezien zij geen officieren van gerechtelijke politie zijn, mogen de leden van de voor het toezicht bevoegde autoriteiten die toezichthoudende taken uitvoeren, de entiteit niet dwingen om mee te werken. Zij kunnen echter in een proces-verbaal optekenen dat de entiteit weigert mee te werken bij een controle, of zelfs opzettelijk foutieve of onvolledige informatie verstrekt of de uitvoering van een controle door de voor het toezicht bevoegde autoriteiten opzettelijk verhindert of belemmert, overeenkomstig paragraaf 3.

HOOFDSTUK 2

De administratieve maatregelen en geldboetes

Afdeling 1

Procedure

In het kader van deze afdeling moet worden verduidelijkt dat, indien geen specifieke bepalingen van toepassing zijn, de Raad van State bevoegd is voor beroepen tot nietigverklaring van beslissingen die administratieve maatregelen opleggen die in uitvoering van dit wetsontwerp worden genomen.

Art. 51

Dit artikel bepaalt de procedure na afloop waarvan de voor het toezicht bevoegde autoriteiten administratieve maatregelen kunnen nemen ten aanzien van essentiële of belangrijke entiteiten die het wetsontwerp niet zouden naleven.

Eerst moeten de inbreuken worden opgetekend in een proces-verbaal door de beëdigde leden van de voor het

assermentés des autorités compétentes pour le contrôle. En principe, les manquements aux dispositions du projet de loi relèvent de la compétence de l'autorité nationale de cybersécurité. Cela étant, les manquements aux mesures de gestion des risques en matière de cybersécurité sectorielles ou sous-sectorielles supplémentaires visées à l'article 34 relèvent de l'autorité sectorielle compétente ou du service d'inspection compétent, pour autant qu'une telle autorité ait été désignée.

De plus, l'autorité nationale de cybersécurité peut accepter de déléguer l'imposition de mesures administratives à une autorité sectorielle. Cette procédure permet de garantir le suivi des dossiers en cas de charges de travail importantes.

Sur la base du procès-verbal évoqué *supra* et des rapports des autorités compétentes pour le contrôle, l'autorité compétente pour le contrôle rédige un projet de décision contenant une ou plusieurs mesures pouvant être prises en constatation de manquements et/ou une amende. Ces mesures et amendes se trouvent aux articles 58 et 59 qui transposent les articles 32, § 4, 33, § 4 et 34, §§ 3 à 5, de la directive NIS2. Le projet de décision, non définitif, comprend également le délai qui serait laissé à l'entité concernée pour exécuter les mesures. Ce délai doit prendre en considération les conditions de fonctionnement de l'entité et les mesures elles-mêmes.

Ensuite, ce projet de décision est envoyé à l'entité concernée avec d'une part, les motifs relatifs aux mesures et/ou amendes envisagés et, d'autre part, l'information que l'entité a 30 jours, à partir de la réception du projet de décision, pour formuler par écrit ses moyens de défense ou de demander à être entendu. L'information est présumée avoir été portée à la connaissance de l'entité concernée 6 jours après l'envoi du projet de décision.

Le projet de loi prévoit qu'il est possible de déroger à la communication du projet de décision, uniquement dans de très rares cas où cette communication empêcherait une intervention immédiate pour prévenir un incident ou y répondre. L'usage de cette exception doit être dûment motivé.

Après que l'entité concernée ait pu faire valoir ses moyens de défenses, par écrit ou en étant directement entendu, à la fin du délai de 30 jours en l'absence de réaction de la part de l'entité ou dans le cas d'exception où la communication du projet de décision ne doit pas être faite, l'autorité compétente pour le contrôle maintient, modifie ou renonce au projet de décision. Pour ce

toezicht bevoegde autoriteiten. In principe is de nationale cyberbeveiligingsautoriteit bevoegd voor inbreuken op de bepalingen van het wetsontwerp. Inbreuken op bijkomende sectorale of deelsectorale maatregelen voor het beheer van cyberbeveiligingsrisico's, als bedoeld in artikel 34, behoren echter tot de bevoegdheid van de bevoegde sectorale overheid of inspectiedienst, voor zover een dergelijke autoriteit is aangewezen.

Daarnaast kan de nationale cyberbeveiligingsautoriteit ermee instemmen om het opleggen van administratieve maatregelen te delegeren aan een sectorale overheid. Deze procedure waarborgt de opvolging van de dossiers in geval van hoge werklast.

Op basis van voornoemd proces-verbaal en de verslagen van de voor het toezicht bevoegde autoriteit stelt de voor het toezicht bevoegde autoriteit een ontwerp van beslissing op dat een of meer mogelijke maatregelen voor de vaststelling van inbreuken en/of een geldboete bevat. Deze maatregelen en geldboetes komen aan bod in de artikelen 58 en 59 die voorzien in de omzetting van de artikelen 32, lid 4, 33, lid 4 en 34, leden 3 tot 5, van de NIS2-richtlijn. Het ontwerp van beslissing, dat nog niet definitief is, vermeldt ook de termijn waarover de betrokken entiteit beschikt om de maatregelen uit te voeren. Deze termijn moet rekening houden met de werkingsomstandigheden van de entiteit en met de maatregelen zelf.

Vervolgens wordt dit ontwerp van beslissing naar de betrokken entiteit gestuurd, samen met de motivering voor de overwogen maatregelen en/of geldboetes en de mededeling dat de entiteit over 30 dagen beschikt, vanaf de ontvangst van het ontwerp van beslissing, om haar verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. De betrokken entiteit wordt geacht in kennis te zijn gesteld van de informatie 6 dagen na de verzending van het ontwerp van beslissing.

Het wetsontwerp bepaalt dat het enkel mogelijk is om af te wijken van de verplichting om het ontwerp van beslissing mee te delen in heel zeldzame gevallen waarin een onmiddellijk optreden om een incident te voorkomen of erop te reageren anders zou worden belemmerd. Het gebruik van deze uitzondering moet naar behoren worden gemotiveerd.

Nadat de betrokken entiteit haar verweermiddelen heeft kunnen aanvoeren, schriftelijk of door rechtstreeks te worden gehoord, op het einde van de termijn van 30 dagen bij het uitblijven van een reactie van de entiteit of in het uitzonderlijke geval waarin het ontwerp van beslissing niet moet worden meegedeeld, zal de voor het toezicht bevoegde autoriteit het ontwerp van beslissing

faire, elle doit prendre en compte la catégorie d'entité à laquelle appartient l'entité concernée (essentielle ou importante), les moyens de défense avancés par l'entité et les éléments visés à l'article 54. L'article 54 transpose l'article 32, § 7, de la directive NIS2 et porte sur les éléments qui doivent être pris en considération lors d'une prise de décision (nous renvoyons au commentaire de cet article *infra* pour plus de détails). Une décision devra toujours être proportionnée, spécifique par rapport aux circonstances des faits. Dans ce cadre, l'amende n'est pas considérée comme la mesure ou la sanction par défaut. Une amende n'est infligée que lorsque cela est proportionné.

Si maintenue ou modifiée, l'entité doit se conformer à la décision prise par l'autorité, sans préjudice de son droit à faire appel de la décision (voir *infra*).

Art. 52

Cet article porte sur la procédure à suivre lorsqu'une entité essentielle ne se conforme pas à une décision prise par une autorité compétente pour le contrôle, visée à l'article précédent.

Cette disposition transpose l'article 32, § 5, de la directive NIS2. Au premier paragraphe, si les mesures d'exécution adoptées en vertu de l'article 58, 1° à 4° et 6° sont inefficaces, elle donne d'abord à l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente la possibilité de mettre en place un délai pour que les entités essentielles puissent prendre les mesures nécessaires pour pallier les insuffisances ou satisfaire aux exigences de ces autorités.

Ensuite, si une entité essentielle concernée ne se conforme pas dans le délai imparti, le second paragraphe reprend les différentes mesures administratives pouvant être prises par les autorités compétentes à l'encontre de l'entité.

Il est renvoyé *mutatis mutandis* au commentaire de l'article précédent. En effet, la procédure est la même. La seule différence est que les mesures administratives possibles, lorsque l'entité essentielle ne se conforme pas à une décision de l'autorité prise conformément à l'article 51, sont celles visées aux articles 59 et 60, transposant l'article 32, § 6, de la directive NIS2. Les amendes sont toujours possibles.

handhaven, wijzigen of ervan afzien. Daartoe moet zij rekening houden met de entiteitscategorie waartoe de betrokken (essentiële of belangrijke) entiteit behoort, de door de entiteit aangevoerde verweermiddelen en de in artikel 54 bedoelde elementen. Art. 54 voorziet in de omzetting van artikel 32, lid 7, van de NIS2-richtlijn en heeft betrekking op de elementen waarmee rekening moet worden gehouden bij het nemen van een beslissing (voor meer informatie verwijzen we naar de commentaar bij dit artikel hieronder). Een beslissing moet altijd evenredig zijn en rekening houden met de specifieke omstandigheden van de feiten. In dit kader wordt de geldboete niet als een standaardmaatregel of -sanctie beschouwd. Een geldboete wordt alleen opgelegd als die evenredig is.

De entiteit moet de beslissing van de autoriteit naleven, ongeacht of deze behouden of gewijzigd wordt, onverminderd haar recht om in beroep te gaan tegen de beslissing (zie *infra*).

Art. 52

Dit artikel beschrijft de te volgen procedure wanneer een essentiële entiteit geen gevolg geeft aan een beslissing van een voor het toezicht bevoegde autoriteit, als bedoeld in het vorige artikel.

Deze bepaling voorziet in de omzetting van artikel 32, lid 5, van de NIS2-richtlijn. Indien de op grond van artikel 58, 1° tot 4° en 6° genomen handhavingsmaatregelen ondoeltreffend zijn, geeft de eerste paragraaf aan de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid eerst de mogelijkheid om een termijn vast te stellen waarbinnen de essentiële entiteit wordt verzocht de noodzakelijke maatregelen te nemen om tekortkomingen te verhelpen of aan de eisen van deze autoriteiten te voldoen.

Indien een betrokken essentiële entiteit vervolgens niet binnen de gestelde termijn aan de eisen voldoet, bevat de tweede paragraaf de verschillende administratieve maatregelen die de voor het toezicht bevoegde autoriteiten kunnen nemen ten aanzien van de entiteit.

Er wordt *mutatis mutandis* verwezen naar de commentaar bij het vorige artikel. De procedure is immers dezelfde. Het enige verschil is dat de mogelijke administratieve maatregelen, wanneer de essentiële entiteit geen gevolg geeft aan een door de autoriteit genomen beslissing overeenkomstig artikel 51, de maatregelen bedoeld in de artikelen 59 en 60 zijn, die voorzien in de omzetting van artikel 32, lid 6, van de NIS2-richtlijn. Geldboetes zijn altijd mogelijk.

Art. 53

Conformément à cet article, les procès-verbaux des membres assermentés de l'autorité compétente pour le contrôle font foi jusqu'à preuve du contraire.

Art. 54

Cet article énumère les éléments qui doivent être pris en compte par le directeur de l'autorité compétente pour le contrôle avant de prendre une décision au sens des articles 51 et 52.

La disposition transpose l'article 32, § 7, de la directive NIS2. Elle rappelle l'obligation de respecter les droits de la défense et de tenir compte des circonstances propres à chaque cas. Il est important de noter que le respect des droits de la défense est assuré, en plus du présent article, par les articles 51, §§ 3 et 4, et 52, §§ 3 et 4, qui mettent en place le principe *audi alteram partem*.

La disposition énumère les circonstances minimum auxquelles il doit être tenu compte. Parmi celles-ci, se trouvent la catégorie à laquelle appartient l'entité, le caractère répété ou non des violations, la durée de la violation, les dommages causés, ...

L'article précise par ailleurs que, lorsque l'Autorité de protection des données a imposé une amende pour un ou plusieurs faits, les autorités compétentes pour le contrôle ne peuvent plus imposer d'amendes pour les mêmes faits. Il s'agit là d'une application du principe *non bis in idem*.

Art. 55

Cet article porte sur la communication de la décision finale prise par l'autorité compétente pour le contrôle et le délai endéans lequel l'entité doit s'acquitter de l'amende.

Les décisions précitées sont envoyées par envoi recommandé.

Conformément à l'article 14, § 1^{er} des lois coordonnées sur le Conseil d'État, cette décision peut, le cas échéant, faire l'objet d'un recours en annulation devant la section du contentieux administratif du Conseil d'État.

Art. 53

Overeenkomstig dit artikel hebben de processen-verbaal van de beëdigde leden van de voor het toezicht bevoegde autoriteit bewijskracht tot het tegendeel is bewezen.

Art. 54

Dit artikel somt de elementen op waarmee de directeur van de voor het toezicht bevoegde autoriteit rekening moet houden alvorens een beslissing te nemen als bedoeld in artikelen 51 en 52.

De bepaling voorziet in de omzetting van artikel 32, lid 7, van de NIS2-richtlijn. Ze herinnert aan de verplichting om de rechten van de verdediging te eerbiedigen en rekening te houden met de omstandigheden van elk afzonderlijk geval. Het is belangrijk te vermelden dat de eerbiediging van de rechten van de verdediging, behalve door dit artikel, ook gewaarborgd wordt door de artikelen 51, §§ 3 en 4, en 52, §§ 3 en 4, die het beginsel *audi alteram partem* vastleggen.

De bepaling somt de minimale omstandigheden op waarmee rekening moet worden gehouden. Deze omvatten de categorie waartoe de entiteit behoort, het al dan niet herhaaldelijke karakter van inbreuken, de duur van de inbreuk, de veroorzaakte schade, ...

Het artikel verduidelijkt bovendien dat, wanneer de Gegevensbeschermingsautoriteit een geldboete heeft opgelegd voor een of meer feiten, de voor het toezicht bevoegde autoriteiten geen geldboetes meer kunnen opleggen voor dezelfde feiten. Dit is een toepassing van het beginsel *non bis in idem*.

Art. 55

Dit artikel gaat nader in op de mededeling van de definitieve beslissing van de voor het toezicht bevoegde autoriteit en de termijn waarbinnen de entiteit de geldboete moet betalen.

Voorname beslissingen worden aangetekend verzonden.

Overeenkomstig artikel 14, § 1, van de gecoördineerde wetten op de Raad van State kan deze beslissing in voorkomend geval het voorwerp uitmaken van een beroep tot nietigverklaring, ingesteld bij de afdeling bestuursrechtspraak van de Raad van State.

Les amendes administratives doivent être acquittées dans le 60 jours. Ce délai est réputé commencer au plus tard 6 jours après l'envoi par recommandé de la décision.

Pour les autres mesures administratives, la décision précise le délai d'exécution des mesures imposées.

Art. 56

Cet article porte sur les conséquences d'un défaut de paiement d'une amende administrative imposée à une entité au travers d'une décision visée à l'article 51 ou 52.

En cas de défaut de paiement, l'autorité compétente pour le paiement peut décerner une contrainte au travers du représentant légal de cette autorité ou d'un membre habilité à cette fin.

Cette contrainte doit être signifiée par exploit d'un huissier de justice et contenir un commandement à l'entité de payer l'amende dans les 48 heures, à peine d'exécution par voie de saisie, de même qu'une justification comptable des sommes exigées ainsi que copie de l'exécutoire.

L'entité peut former opposition à la contrainte devant le juge des saisies, de manière motivée, au travers d'une citation de l'autorité compétente pour le contrôle dans les 15 jours à partir de la signification de la contrainte. En ce cas, les dispositions pertinentes du Code judiciaire sont applicables à ce délai.

L'exercice de l'opposition suspend l'exécution de la contrainte le temps qu'il soit statué sur le fond, les saisies déjà effectuées gardant leur caractère conservatoire.

Le paragraphe 4 du présent article permet à l'autorité compétente pour le contrôle de pratiquer des saisies conservatoires et d'exécuter la contrainte par les voies d'exécutions de la cinquième partie du Code judiciaire.

Les frais de signification par exploit d'huissier, établis conformément aux règles établies pour ces actes de signification sont à charge de l'entité concernée.

Administratieve geldboetes moeten binnen de 60 dagen worden betaald. Deze termijn wordt geacht in te gaan uiterlijk 6 dagen nadat de beslissing aangetekend is verzonden.

Voor de andere administratieve maatregelen vermeldt de beslissing de uitvoeringstermijn van de opgelegde maatregelen.

Art. 56

Dit artikel behandelt de gevolgen van het niet betalen van een administratieve geldboete die is opgelegd aan een entiteit bij een in artikel 51 of 52 bedoelde beslissing.

In geval van wanbetaling kan de voor de betaling bevoegde overheid een dwangbevel uitvaardigen via de wettelijke vertegenwoordiger van deze overheid of een daartoe gemachtigd personeelslid.

Dit dwangbevel moet bij gerechtsdeurwaarderexploot worden betekend en een aan de entiteit gericht bevel bevatten om de geldboete te betalen binnen 48 uur, op straffe van tenuitvoerlegging door beslag, alsook een boekhoudkundige verantwoording van de gevorderde bedragen en een afschrift van de uitvoerbaarverklaring.

De entiteit kan tegen het dwangbevel verzet aantekenen bij de beslagrechter, mits motivering, door middel van een dagvaarding van de voor het toezicht bevoegde autoriteit binnen 15 dagen vanaf de betekening van het dwangbevel. In elk geval zijn de relevante bepalingen van het Gerechtelijk Wetboek van toepassing op deze termijn.

De uitoefening van verzet schorst de tenuitvoerlegging van het dwangbevel tot uitspraak ten gronde is gedaan, waarbij de reeds gelegde beslagen hun bewarend karakter behouden.

Paragraaf 4 van dit artikel staat de voor het toezicht bevoegde autoriteit toe om bewarend beslag te leggen en het dwangbevel uit te voeren met de middelen tot tenuitvoerlegging van het vijfde deel van het Gerechtelijk Wetboek.

De kosten voor de betekening bij gerechtsdeurwaarderexploot die worden bepaald volgens de regels die gelden voor deze betekeningsakten, zijn ten laste van de betrokken entiteit.

Art. 57

Cet article établit le délai de prescription extinctive des faits pouvant mener à une enquête ou poursuite par un service d'inspection ainsi que pour les mesures et amendes administratives pouvant être imposées en vertu du projet de loi.

Le délai pour les faits pouvant mener à une enquête ou poursuite par un service d'inspection est fixé à trois ans, à compter du jour de leur commission. Ce délai sera interrompu lorsque des actes d'enquête ou de poursuite par un service d'inspection seront posés. À partir de ce moment-là, un nouveau délai de trois ans prendra cours, et cela même à l'encontre des personnes qui n'auraient pas été impliquées dans les enquêtes ou poursuites.

Le délai pour les mesures et amendes administratives est fixé à cinq ans, à compter de la date à laquelle ces dernières doivent être exécutées. Ce délai sera suspendu lorsqu'un recours contre la décision administrative, dans laquelle il trouve son origine, sera introduit. Si le recours n'aboutit pas, le délai reprendra cours.

Le délai pour les mesures et amendes administratives est aligné sur le délai inscrit à l'article 106 de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, pour assurer une cohérence lors de la prise de sanctions administratives. Ce corps de texte est en effet fortement lié au présent texte en matière de violations de sécurité.

Cet article est sans préjudice du principe *non bis in idem* qui se doit d'être respecté en toute circonstance.

Section 2

Mesures et amendes administratives

Art. 58

Cet article transpose les articles 32, § 4, et 33, § 4, de la directive NIS2. Il reprend les différentes mesures administratives pouvant être prises par les autorités compétentes pour le contrôle en cas de constatation de manquements par les entités essentielles ou importantes.

La disposition spécifie les mesures qui ne s'appliqueraient qu'à une catégorie d'entité. Le corollaire de cette spécification est que chaque mesure pour laquelle rien n'est spécifié peut être prise à l'encontre des entités, qu'elles soient essentielles ou importantes.

Art. 57

Dit artikel bepaalt de bevrijdende verjaringstermijn voor feiten die kunnen leiden tot een onderzoek of vervolging door een inspectiedienst alsook voor de administratieve maatregelen en geldboetes die kunnen worden opgelegd krachtens het wetsontwerp.

De termijn voor de feiten die kunnen leiden tot een onderzoek of vervolging door een inspectiedienst is vastgesteld op drie jaar, te rekenen vanaf de dag waarop ze worden gepleegd. Deze termijn wordt gestuit wanneer de feiten door een inspectiedienst worden onderzocht of vervolgd. Vanaf dan geldt een nieuwe termijn van drie jaar, zelfs voor personen die niet betrokken waren bij de onderzoeken of de vervolgingen.

De termijn voor de administratieve maatregelen en geldboetes is vastgesteld op 5 jaar, te rekenen vanaf de datum waarop ze moeten worden uitgevoerd. Deze termijn wordt opgeschort als beroep wordt aangetekend tegen de administratieve beslissing dat de oorzaak vormt. Als het beroep niet succesvol is, wordt de termijn hervat.

De termijn voor administratieve maatregelen en geldboetes wordt afgestemd op de termijn in artikel 106 van de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, om coherentie te waarborgen bij het opleggen van administratieve sancties. Deze tekst is sterk verbonden met de huidige tekst met betrekking tot inbreuken op de beveiliging.

Dit artikel doet geen afbreuk aan het beginsel *non bis in idem*- beginsel, dat in alle omstandigheden gerespecteerd dient te worden.

Afdeling 2

Administratieve maatregelen en geldboetes

Art. 58

Dit artikel voorziet in de omzetting van de artikelen 32, lid 4, en 33, lid 4, van de NIS2-richtlijn. Het beschrijft de verschillende administratieve maatregelen die de voor het toezicht bevoegde autoriteiten kunnen nemen indien inbreuken door essentiële of belangrijke entiteiten worden vastgesteld.

De bepaling specificeert welke maatregelen alleen gelden voor een entiteitscategorie. Deze specificering heeft tot gevolg dat elke maatregel waarvoor niets gespecificeerd is kan worden genomen ten aanzien van entiteiten, ongeacht of ze essentieel of belangrijk zijn.

Art. 59

Cet article énumère les amendes administratives qui peuvent être imposées. L'article se réfère à la procédure prévu aux articles 51 et 52 de la loi. Pour rappel, ces articles prévoient la procédure au terme de laquelle les autorités compétentes en matière de contrôle peuvent prendre des mesures administratives à l'encontre d'entités essentielles, importantes et des personnes physiques qui ne respecteraient pas la législation.

La disposition spécifie les amendes qui ne s'appliqueraient qu'à une catégorie d'entité et les amendes qui s'appliqueraient à quiconque. Le corollaire de cette spécification est que chaque amende pour laquelle rien n'est spécifié peut être infligée aux entités, qu'elles soient essentielles ou importantes.

L'alinéa 1^{er}, 4^o et 5^o, transpose l'article 34, §§ 4 et 5, de la directive NIS2. Le reste de la disposition reprend le contenu des articles 52, §§ 4, 5 et 6, et 55, § 4, alinéa 2, et § 5, de la loi NIS1.

Art. 60

Cette disposition transpose l'article 32, § 5, a) et b), de la directive NIS2. Il comprend les mesures qui peuvent être prises par les autorités compétentes sur base de l'article 52.

Ces mesures sont uniquement appliquées jusqu'à ce que l'entité concernée prenne les mesures nécessaires pour remédier aux insuffisances ou se conformer aux exigences de l'autorité compétente pour le contrôle.

Art. 61

Cette disposition transpose les articles 32, § 6, et 32, § 5, de la directive NIS2. Selon cet article, sans préjudice des dispositions nationales spécifiques en matière de responsabilité des agents de la fonction publique, les personnes physiques responsables d'une entité ou agissant en qualité de représentant légal d'une entité doivent avoir le pouvoir de veiller au respect, par l'entité, du présente projet de loi.

Art. 59

Dit artikel somt de administratieve geldboetes op die kunnen worden opgelegd. Het artikel verwijst hierbij naar de procedure in de artikelen 51 en 52 van de wet. Ter herinnering, deze artikelen bepalen de procedure na afloop waarvan de voor het toezicht bevoegde autoriteiten administratieve maatregelen kunnen nemen ten aanzien van essentiële en belangrijke entiteiten en natuurlijke personen die de wetgeving niet zouden naleven.

De bepaling specificeert welke geldboetes alleen gelden voor een entiteitscategorie en welke voor eenieder gelden. Deze specificering heeft tot gevolg dat elke geldboete waarvoor niets gespecificeerd is kan worden opgelegd aan entiteiten, ongeacht of ze essentieel of belangrijk zijn.

Het eerste lid, 4^o en 5^o, voorziet in de omzetting van artikel 34, leden 4 en 5, van de NIS2-richtlijn. Voor het overige bevat de bepaling de inhoud van de artikelen 52, §§ 4, 5 en 6, en 55, § 4, tweede lid, en § 5, van de NIS1-wet.

Art. 60

Deze bepaling voorziet in de omzetting van artikel 32, lid 5, a) en b), van de NIS2-richtlijn. Dit bevat de maatregelen die de bevoegde autoriteiten op basis van artikel 52 kunnen nemen.

Deze maatregelen worden alleen toegepast tot de betrokken entiteit de nodige maatregelen neemt om de tekortkomingen te verhelpen of te voldoen aan de eisen van de voor het toezicht bevoegde autoriteit.

Art. 61

Deze bepaling voorziet in de omzetting van de artikelen 32, lid 6, en 32, lid 5, van de NIS2-richtlijn. Volgens dit artikel moeten de natuurlijke personen die aansprakelijk zijn voor een entiteit of optreden als wettelijke vertegenwoordiger van een entiteit, onverminderd de specifieke nationale bepalingen inzake de aansprakelijkheid van ambtenaren, de bevoegdheid hebben om ervoor te zorgen dat de entiteit dit wetsontwerp naleeft.

TITRE 5

*Dispositions spécifiques au secteur de
l'administration publique*

Art. 62

Cet article rend inapplicables les amendes et les mesures des articles 60 et 61 aux entités faisant partie du secteur de l'administration publique. Cette dérogation est, en partie, laissée à l'appréciation des États membres par la directive NIS2, au travers de l'article 34, § 7 (en matière d'amendes administratives) et, pour l'autre partie, prévue par la directive NIS2 elle-même, au travers de l'article 32, § 5, alinéa 3.

Art. 63

Cette disposition habilite le Roi à désigner une ou plusieurs autorités comme organismes d'évaluation de la conformité spécifiques au secteur des entités de l'administration publique. Par autorité, il faut entendre autorité publique.

L'évaluation de la conformité se fait selon les conditions fixées par le Roi conformément à l'article 39, alinéa 1^{er}, 1^o du projet de loi.

En tant qu'organisme d'évaluation de la conformité, l'autorité désignée doit être agréée par l'autorité nationale de cybersécurité avant d'effectuer des évaluations de la conformité. La détermination des conditions de l'agrément est laissée au Roi.

Comme le prévoit le paragraphe 3, lorsqu'une autorité a été désignée comme organisme d'évaluation de la conformité pour des entités de l'administration publique, ces entités doivent effectuer leurs audits auprès de ladite autorité.

Les entités de l'administration publique conservent la possibilité d'effectuer l'évaluation de la conformité, soit par l'autorité désignée comme organisme d'évaluation de la conformité, soit par le service d'inspection de l'autorité nationale de cybersécurité.

Art. 64

Cet article établit les règles spécifiques relatives aux services d'inspection compétents pour les entités de l'administration publique.

TITEL 5

*Specifieke bepalingen
voor de overheidssector*

Art. 62

Dit artikel bepaalt dat de geldboetes en maatregelen bedoeld in de artikelen 60 en 61 niet van toepassing zijn op entiteiten die deel uitmaken van de overheidssector. De NIS2-richtlijn laat deze afwijking gedeeltelijk over aan het oordeel van de lidstaten, via artikel 34, lid 7 (inzake administratieve geldboetes) en, voor het overige gedeelte, waarin de NIS2-richtlijn zelf voorziet, via artikel 32, lid 5, derde alinea.

Art. 63

Deze bepaling machtigt de Koning om een of meer autoriteiten aan te wijzen als specifieke conformiteitsbeoordelingsinstanties voor de overheidssector. In de Franse versie moet onder "autorité" "autorité publique" worden verstaan.

De conformiteitsbeoordeling gebeurt volgens de voorwaarden bepaald door de Koning overeenkomstig artikel 39, eerste lid, 1^o, van het wetsontwerp.

De autoriteit die is aangewezen als conformiteitsbeoordelingsinstantie moet door de nationale cyberbeveiligingsautoriteit worden erkend, alvorens conformiteitsbeoordelingen te kunnen uitvoeren. Het bepalen van de erkenningsvoorwaarden wordt overgelaten aan de Koning.

Zoals bepaald in paragraaf 3, wanneer een autoriteit is aangewezen als conformiteitsbeoordelingsinstantie voor overheidsinstanties, moeten deze instanties hun audits uitvoeren bij deze autoriteit.

De overheidsinstanties behouden de mogelijkheid om een conformiteitsbeoordeling te laten uitvoeren door de autoriteit die is aangewezen als conformiteitsbeoordelingsinstantie, of door de inspectiedienst van de nationale cyberbeveiligingsautoriteit.

Art. 64

Dit artikel bevat specifieke regels voor de inspectiediensten die bevoegd zijn voor de overheidsinstanties.

En l'absence de désignation par le Roi, le service d'inspection de l'autorité nationale de cybersécurité est compétent pour exercer les tâches de supervision déterminées par le présent projet de loi. En tous les cas, l'autorité compétente pour le contrôle doit jouir d'une indépendance opérationnelle vis-à-vis des entités supervisées.

Art. 65

Conformément à cette disposition, quelle que soit l'autorité compétente pour le contrôle vis-à-vis des entités de l'administration publique, les dispositions relatives aux situations de conflits d'intérêts lui sont applicables.

TITRE 6

Traitement des données à caractère personnel

CHAPITRE 1^{ER}

Principes relatifs au traitement

Art. 66

Cette disposition rend applicable les définitions du règlement européen 2016/679 (ci-après, le "RGPD") au titre 6 du projet de loi.

À noter qu'il ne s'agit pas ici d'une répétition des dispositions du RGPD (interdite car le RGPD, en tant que règlement européen, est d'application directe en droit nationale, de sorte que les obligations légales du RGPD ne peuvent être répétées en droit national) mais de l'utilisation des définitions du règlement pour assurer la cohérence dans les notions utilisées.

Art. 67

Cette disposition énumère les finalités sur base desquelles des données à caractère personnel (délimitées au sein de l'article suivant) peuvent être traitées.

Art. 68

Cet article détermine, pour chaque finalité, les types de données à caractère personnel qui peuvent être traitées.

La détermination des données à caractère personnel pouvant être traitées est systématiquement liée avec

Bij gebrek aan een aanwijzing door de Koning is de inspectiedienst van de nationale cyberbeveiligingsautoriteit bevoegd om de toezichthoudende taken uit te voeren die dit wetsontwerp bepaalt. In elk geval moet de voor het toezicht bevoegde autoriteit operationeel onafhankelijk zijn van de instanties waarop zij toezicht houdt.

Art. 65

Volgens deze bepaling zijn de bepalingen inzake belangenconflicten van toepassing ongeacht de voor het toezicht bevoegde autoriteit ten aanzien van overheidsinstanties.

TITEL 6

Verwerking van persoonsgegevens

HOOFDSTUK 1

Beginnelsen betreffende de verwerking

Art. 66

Volgens deze bepaling zijn de definities van de Europese Verordening 2016/679 (hierna de "AVG") van toepassing op titel 6 van het wetsontwerp.

Het gaat hier niet om een herhaling van de bepalingen van de AVG (wat verboden is omdat de AVG, als Europese verordening, rechtstreeks van toepassing is in het nationale recht, zodat de wettelijke verplichtingen van de AVG niet mogen worden herhaald in het nationale recht). De definities van de verordening worden echter gebruikt met het oog op de samenhang tussen de gebruikte begrippen.

Art. 67

Deze bepaling somt de doeleinden op waarvoor persoonsgegevens (gedefinieerd in het volgende artikel) mogen worden verwerkt.

Art. 68

Dit artikel bepaalt, voor elk doeleinde, de soorten persoonsgegevens die mogen worden verwerkt.

De persoonsgegevens die mogen worden verwerkt, worden systematisch gekoppeld aan een doeleinde om

une finalité afin d'encadrer les traitements de données à caractère personnel effectués en exécution du projet de loi.

Art. 69

Cet article détermine les personnes concernées par les traitements.

Art. 70

Cette disposition détermine les responsables de traitement dans le cadre de l'exécution du projet de loi.

Par principe, chaque personne est responsable des traitements qu'elle effectue. Cela signifie, par exemple, que l'autorité nationale de cybersécurité est responsable de traitement dans le cadre de l'enregistrement des entités car c'est auprès de cette entité que ces enregistrements sont effectués, ou encore qu'un service d'inspection sectoriel est responsable des traitements qu'il effectue dans le cadre de la supervision des mesures spécifiques à son secteur visées à l'article 33, notamment lors d'une audition.

CHAPITRE 2

Durée de conservation

Art. 71

Cette disposition fixe la durée de conservation des données à caractère personnel traitées dans le cadre du projet de loi à 5 ans après la fin du dernier traitement effectué, sans que cette durée de conservation ne puisse dépasser 10 ans à partir du premier traitement effectué.

CHAPITRE 3

Limitation des droits des personnes concernées

Art. 72

Cette disposition met en œuvre l'article 23 du RGPD. Afin d'assurer l'exécution des contrôles et de la supervision organisés par le projet de loi, il peut être dérogé à certains droits des personnes concernées. Les droits en question sont le droit à la transparence des informations et des communications; le droit à l'accès aux informations lors de la collecte de données; le droit d'accès; le droit de rectification; le droit à la limitation du traitement et

de la verwerking van persoonsgegevens in uitvoering van het wetsontwerp te regelen.

Art. 69

Dit artikel bepaalt de personen die betrokken zijn bij de verwerkingen.

Art. 70

Deze bepaling verduidelijkt wie de verwerkingsverantwoordelijken zijn in het kader van de uitvoering van het wetsontwerp.

In principe is elke persoon verantwoordelijk voor de verwerkingen die hij uitvoert. Dit betekent bijvoorbeeld dat de nationale cyberbeveiligingsautoriteit verantwoordelijk is voor verwerkingen in het kader van de registratie van entiteiten omdat zij de registraties uitvoert, of nog dat een sectorale inspectiedienst verantwoordelijk is voor de verwerkingen die hij uitvoert in het kader van het toezicht op de in artikel 33 bedoelde specifieke maatregelen voor zijn sector, met name bij een verhoor.

HOOFDSTUK 2

Bewaartermijn

Art. 71

Volgens deze bepaling bedraagt de bewaartermijn van de persoonsgegevens die in het kader van het wetsontwerp worden verwerkt, 5 jaar na afloop van de laatste verwerking en maximaal 10 jaar vanaf de eerste verwerking.

HOOFDSTUK 3

Beperking van de rechten van de betrokkenen

Art. 72

Deze bepaling geeft uitvoering aan artikel 23 van de AVG. Met het oog op de uitvoering van de in het wetsontwerp geregelde controles en toezicht kan worden afgeweken van sommige rechten van betrokkenen. De rechten in kwestie zijn het recht op transparante informatie en communicatie; het recht op toegang tot informatie bij de gegevensverzameling; het recht op inzage; het recht op rectificatie; het recht op beperking van de verwerking

l'obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel (voir les articles 12 à 16, 18 et 19 du RGPD).

L'article permet, sous des conditions et limitations qu'il détermine, de déroger aux droits des personnes précitées.

L'exemption ne vaut que pour la finalité de contrôle et de supervision des entités essentielles et importantes, pour les catégories de données concernées par cette finalité.

L'exemption ne s'applique que pendant la période au cours de laquelle une personne concernée fait l'objet d'un contrôle, ou en tous les cas au cours de laquelle ses données sont traitées dans le cadre dudit contrôle. Cette période ne peut durer plus d'un an, deux en comptant les actes préparatoires.

De plus, si un responsable de traitement ne respecte pas les conditions de l'exemption, il ne peut en bénéficier et risque donc d'effectuer un manquement au RGPD.

Art. 73

Dans le cadre de l'exemption visée à l'article précédent, le responsable doit tout de même fournir des informations aux personnes concernées, autant que possible et tant que cela ne compromet pas la finalité pour laquelle l'exemption est possible, à savoir le contrôle et l'inspection des entités dans le cadre du projet de loi.

Cet article dispose que l'exemption visée à l'article précédent doit être levée lors de la fin du contrôle, de la supervision ou des actes préparatoires ou lorsque l'exemption n'est plus nécessaire pour le contrôle. En tous les cas, le délégué à la protection informe les personnes concernées à la levée de l'exemption.

CHAPITRE 4

Limitations aux obligations de notification des violations de données à caractère personnel

Art. 74

L'article introduit une autre dérogation, plus limitée, concernant l'article 34 du RGPD et l'obligation de notification individuelle en cas de violation de données personnelles. Ce n'est qu'avec l'autorisation de l'autorité nationale de cybersécurité, et seulement dans la

en de kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens (zie de artikelen 12 tot 16, 18 en 19 van de AVG).

Het artikel maakt het mogelijk om, onder de voorwaarden en beperkingen die het bepaalt, af te wijken van de rechten van voornoemde personen.

De vrijstelling geldt alleen voor het doeleinde op het gebied van de controle en het toezicht ten aanzien van essentiële en belangrijke entiteiten, voor de gegevenscategorieën waarop dit doeleinde betrekking heeft.

De vrijstelling geldt alleen voor de periode waarin een betrokkene onderworpen is aan een controle, of in elk geval waarin zijn gegevens worden verwerkt in het kader van die controle. Deze periode mag niet langer duren dan één jaar, of twee jaar als men rekening houdt met de voorbereidende werkzaamheden.

Indien een verwerkingsverantwoordelijke de voorwaarden van de vrijstelling niet naleeft, kan hij er bovendien geen gebruik van maken en loopt hij dus het risico dat hij de AVG overtreedt.

Art. 73

In het kader van de in het vorige artikel bedoelde vrijstelling moet de verantwoordelijke de betrokkenen wel informatie bezorgen, voor zover mogelijk en zolang dit het doeleinde waarvoor de vrijstelling mogelijk is niet in het gedrang brengt, namelijk de controle en inspectie van de entiteiten in het kader van het wetsontwerp.

Dit artikel bepaalt dat de in het vorige artikel bedoelde vrijstelling moet worden opgeheven op het einde van de controle, het toezicht of de voorbereidende werkzaamheden of wanneer de vrijstelling niet meer nodig is voor de controle. In elk geval informeert de functionaris voor gegevensbescherming de betrokkenen dat de vrijstelling is opgeheven.

HOOFDSTUK 4

Beperkingen inzake de verplichte melding van inbreuken in verband met persoonsgegevens

Art. 74

Het artikel voorziet in een andere, beperktere afwijking met betrekking tot artikel 34 van de AVG en de verplichte individuele kennisgeving in geval van een inbreuk in verband met persoonsgegevens. Deze individuele kennisgeving zou niet meer verplicht zijn mits toestemming

mesure nécessaire pour préserver les finalités visées à l'article 74, § 2, du projet de loi, que cette notification individuelle ne serait plus obligatoire.

TITRE 7

Dispositions finales

CHAPITRE 1^{ER}

Disposition transitoire

Art. 75

Cette disposition habilite le Roi à fixer le délai endéans lequel l'évaluation périodique de la conformité doit, pour la première fois, être effectuée par les entités essentielles (nous renvoyons au commentaire de l'article 39 pour plus de détails sur l'évaluation périodique de la conformité). Etant donné que le Roi fixe les modalités de cette évaluation ainsi que les cadres de référence utilisés, il doit lui revenir également de fixer un délai permettant aux entités essentielles de se mettre en conformité avec cette nouvelle obligation.

CHAPITRE 2

Dispositions modificatives

Section 1^{re}

Modifications de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire

Les articles 76 et 77 visent à adapter la loi du 15 avril 1994 et n'appellent pas de commentaire particulier.

Section 2

Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique

Les articles 78 à 80 visent à adapter la loi du 22 février 1998 et n'appellent pas de commentaire particulier.

TITEL 7

Slotbepalingen

HOOFDSTUK 1

Overgangsbepaling

Art. 75

Deze bepaling machtigt de Koning om de termijn vast te stellen waarbinnen essentiële entiteiten de regelmatige conformiteitsbeoordeling voor het eerst moeten uitvoeren (we verwijzen naar de commentaar bij artikel 39 voor meer informatie over de regelmatige conformiteitsbeoordeling). Aangezien de Koning de modaliteiten van deze beoordeling en de gebruikte referentiekaders vaststelt, komt het Hem ook toe een termijn te bepalen waarbinnen essentiële entiteiten aan deze nieuwe verplichting moeten voldoen.

HOOFDSTUK 2

Wijzigingsbepalingen

Afdeling 1

Wijzigingen van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle

De artikelen 76 en 77 passen de wet van 15 april 1994 aan en behoeven geen verdere commentaar.

Afdeling 2

Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België

De artikelen 78 tot 80 passen de wet van 22 februari 1998 aan en behoeven geen verdere commentaar.

Section 3

Modification de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

L'article 81 vise à adapter la loi du 2 août 2002 et n'appelle pas de commentaire particulier.

Section 4

Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges

Les articles 82 et 83 visent à adapter la loi du 17 janvier 2003.

Un des secteurs visés par la directive NIS2 est le secteur des infrastructures numériques.

Lors de la transposition de la directive NIS2 en droit belge, il a été décidé que l'IBPT serait l'autorité sectorielle pour l'ensemble des entités de ce secteur, à l'exception des prestataires de services de confiance, pour lesquelles l'autorité sectorielle reste le ministre de l'Économie (et le SPF Économie par délégation).

Comme il a été considéré que les fournisseurs de services d'informatique en nuage ("cloud"), les fournisseurs de services de centres de données ("data center") et les fournisseurs de réseaux de diffusion de contenu, qui sont des entités du secteur des infrastructures numériques, relèvent de la compétence du ministre qui a l'Économie dans ses attributions, ce dernier est impliqué pour ces entités de la manière suivante.

D'abord, ce ministre reste compétent pour la réglementation de ces entités.

Ensuite, ce ministre est aussi visé dans la loi relative au statut de l'IBPT. Ainsi, l'article 14 de cette loi prévoit que le ministre qui a l'Économie dans ses attributions peut demander un avis à l'IBPT, dans la limite de ses attributions.

L'article 19 de cette même loi prévoit que les décisions du Conseil de l'IBPT sont notifiées aux personnes directement et personnellement concernées, au ministre compétent pour les Télécommunications, ainsi qu'au ministre qui a l'Économie dans ses attributions, dans la limite de leurs attributions respectives.

Afdeling 3

Wijziging van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

Art. 81 past de wet van 2 augustus 2002 aan en behoeft geen verdere commentaar.

Afdeling 4

Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

De artikelen 82 en 83 passen de wet van 17 januari 2003 aan.

Een van de in de NIS2-richtlijn bedoelde sectoren is de sector digitale infrastructuur.

Bij de omzetting van de NIS2-richtlijn in Belgisch recht is beslist dat het BIPT de sectorale overheid zou zijn voor alle entiteiten van deze sector, met uitzondering van de verleners van vertrouwensdiensten, waarvoor de sectorale overheid de minister van Economie blijft (en de FOD Economie bij delegatie).

Aangezien werd geoordeeld dat de minister van Economie bevoegd is voor de aanbieders van cloudcomputingdiensten ("cloud"), de aanbieders van datacentra ("data center") en de aanbieders van netwerken voor de levering van inhoud, die entiteiten zijn van de sector van de digitale infrastructuur, is genoemde minister betrokken bij deze entiteiten zoals hierna uiteengezet.

In de eerste plaats blijft deze minister bevoegd voor de regelgeving wat deze entiteiten betreft.

Vervolgens wordt deze minister ook genoemd in de wet met betrekking tot het statuut van het BIPT. Zo bepaalt artikel 14 van deze wet dat de minister bevoegd voor Economie advies kan vragen aan het BIPT, binnen de grenzen van zijn bevoegdheden.

Art. 19 van diezelfde wet bepaalt dat de beslissingen van de Raad van het BIPT worden meegedeeld aan de personen die rechtstreeks en persoonlijk betrokken zijn, aan de minister bevoegd voor Telecommunicatie en aan de minister bevoegd voor Economie, binnen de grenzen van hun respectievelijke bevoegdheden.

Section 5

Modification de la loi du 13 juin 2005 relative aux communications électroniques

Les articles 84 à 92 visent à adapter la loi du 13 juin 2005. Les articles 84 à 86 et 88 à 91 n'appellent pas de commentaires particuliers.

Pour ce qui concerne l'article 87, étant donné que le nombre d'entités relevant du règlement NIS augmentera considérablement en raison des *size caps* fixés par la directive NIS2, il est décidé de limiter le champ d'application de l'article 105 de la loi relative aux communications électroniques. Seuls les exploitants d'un réseau privé de communications électroniques désignés comme exploitants d'une infrastructure critique sont encore tenus d'obtenir une autorisation ministérielle pour leur réseau 5G.

L'article 92 transpose l'article 28 de la directive NIS2 dans le nouvel article 164/3 de la loi du 13 juin 2005 relative aux communications électroniques. L'article 28 est expliqué plus avant dans les considérants 109 à 112 de la directive NIS2.

En vertu du RGPD, les registres de noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine ne peuvent plus publier de données à caractère personnel sur les titulaires des noms de domaine (WHOIS). Cela complique fortement le travail des services de police et de sécurité, par exemple.

L'article 92 introduit l'obligation pour les différents acteurs au sein de l'écosystème des noms de domaine de tenir à jour certaines données minimales des titulaires de noms de domaine dans une base de données (le "WHOIS") et veille également à ce que ces données soient les plus exactes possible. Les demandeurs d'accès légitimes se voient octroyer le droit de demander ces données, moyennant motivation. Ainsi les titulaires des noms de domaine enfreignant la réglementation peuvent être identifiés et détectés.

L'article 164/3 en projet fait l'objet des commentaires spécifiques suivants.

Premièrement, plusieurs contributions à la consultation publique mettent en avant le risque de créer une distorsion de concurrence entre États membres, en imposant aux registres de noms de domaine et aux entités fournissant des services d'enregistrement de noms de domaine qui sont soumis à la loi belge des règles et instructions qui seraient plus strictes que celles imposées dans les autres États membres.

Afdeling 5

Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie

De artikelen 84 tot 92 passen de wet van 13 juni 2005 aan. De artikelen 84 tot 86 en 88 tot 91 behoeven geen verdere commentaar.

Voor wat betreft artikel 87, gezien het aantal entiteiten die onder de NIS-regelgeving valt vele malen groter zal worden ten gevolge van de *size caps* onder NIS2, wordt de keuze gemaakt om het toepassingsgebied van artikel 105 van de wet betreffende de elektronische communicatie te beperken. Enkel de exploitanten van een privaat elektronische-communicatienetwerk die zijn aangewezen als exploitant van een kritieke infrastructuur zijn er nog toe gehouden om een ministeriële machtiging voor hun 5G-netwerk te verkrijgen.

Art. 92 zet artikel 28 van de NIS2-richtlijn om in het nieuwe artikel 164/3 van de wet van 13 juni 2005 betreffende de elektronische communicatie. Art. 28 wordt verder uitgelegd in rechtsoverwegingen 109 tot en met 112 van de NIS2-richtlijn.

Krachtens de AVG mogen registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen geen persoonsgegevens meer publiceren over de houders van de domeinnamen (WHOIS). Dit bemoeilijkt in sterke mate het werk van bijvoorbeeld politie- en veiligheidsdiensten.

Art. 92 voert de verplichting in voor de diverse actoren in het domeinnaamecosysteem om minimaal bepaalde gegevens van de houders van domeinnamen bij te houden in een database ("de WHOIS") en zorgt er eveneens voor dat deze gegevens zo accuraat mogelijk zijn. Legitieme partijen verkrijgen het recht om deze gegevens op te vragen indien dit kan worden gemotiveerd. Zo kunnen houders van domeinnamen die inbreuken plegen op wet- en regelgeving worden geïdentificeerd en opgespoord.

Aangaande het ontwerp van artikel 164/3 worden de volgende specifieke opmerkingen gemaakt.

In de eerste plaats wijzen verschillende bijdragen aan de openbare raadpleging op het risico dat de mededinging tussen de lidstaten wordt verstoord door aan registers voor domeinnamen en entiteiten die domeinnaamregistratiediensten verlenen die onderworpen zijn aan de Belgische wetgeving, regels en instructies op te leggen die strenger zouden zijn dan die welke in andere lidstaten worden opgelegd.

Il convient de noter que cette distorsion de concurrence pourrait exister entre différents noms de domaine (par exemple entre le nom de domaine.be et un nom de domaine soumis à la législation d'un autre pays) mais pas au sein d'un même nom de domaine (donc pas au sein des noms de domaine.be ou.eu).

Il est tenu compte de cette remarque comme suit:

— les ajouts dans l'article 164/3 de la loi du 13 juin 2005 relative aux communications électroniques par rapport à l'article 28 de la directive NIS2 n'ont été apportés que lorsque c'était indispensable;

— les arrêtés royaux qui pourraient être adoptés sur base de l'article 164/3 et les instructions contraignantes que l'IBPT pourrait imposer sur base de même article prendront en compte les discussions au niveau du groupe de travail au sein du groupe de coopération NIS.

D'un autre côté, comme il ressort de plusieurs contributions à la consultation publique, il est également nécessaire de ne pas se contenter de recopier dans la loi belge l'article 28 de la directive, étant donné que certains ajouts sont nécessaires afin d'atteindre les objectifs fixés par cet article.

Deuxièmement, de nombreuses contributions à la consultation publique ont également mis en avant la problématique suivante à laquelle les demandeurs d'accès légitimes sont confrontés: pour obtenir les données d'enregistrement de noms de domaine, ils doivent s'adresser au registre des noms de domaine de premier niveau ("*registry*"), qui les renvoie vers un bureau d'enregistrement ("*registrar*"), qui les renvoie vers un fournisseur ou revendeur de services d'anonymisation ou d'enregistrement fiduciaire.

Ces mêmes contributions demandent de préciser dans l'article 164/3 que si un service d'anonymisation ou d'enregistrement fiduciaire a été utilisé, toutes les données qui doivent être collectées doivent contenir les informations relatives à l'utilisateur bénéficiaire, au titulaire de licence et/ou au client du service d'anonymisation ou d'enregistrement fiduciaire.

Cette manière de procéder pose cependant les problèmes suivants:

— cela reviendrait à s'écarter du système mis en place par l'article 28 de la directive NIS2;

— cela reviendrait à rendre impossible en pratique les services d'anonymisation ou d'enregistrement fiduciaire;

Er zij op gewezen dat deze verstoorde mededinging zou kunnen bestaan tussen verschillende domeinnamen (bijvoorbeeld tussen de.be-domeinnaam en een domeinnaam die onder de wetgeving van een ander land valt) maar niet binnen dezelfde domeinnaam (dus niet binnen.be- of.eu-domeinnamen).

Met deze opmerking wordt als volgt rekening gehouden:

— de toevoegingen aan artikel 164/3 van de wet van 13 juni 2005 betreffende de elektronische communicatie in verband met artikel 28 van de NIS2-richtlijn zijn alleen gedaan waar dat onontbeerlijk was;

— in de koninklijke besluiten die op grond van artikel 164/3 zouden kunnen worden aangenomen en de bindende instructies die het BIPT op grond van hetzelfde artikel zou kunnen opleggen, zal rekening worden gehouden met de besprekingen van de werkgroep binnen de NIS-samenwerkingsgroep.

Anderzijds is het, zoals blijkt uit verschillende bijdragen aan de openbare raadpleging, ook noodzakelijk om zich er niet toe te beperken artikel 28 van de richtlijn woordelijk in de Belgische wetgeving over te nemen, aangezien bepaalde aanvullingen noodzakelijk zijn om de door dat artikel vastgestelde doelstellingen te verwezenlijken.

Ten tweede hebben talrijke bijdragen aan de openbare raadpleging ook het volgende probleem aan het licht gebracht waarmee verzoekers om legitieme toegang worden geconfronteerd: om domeinnaamregistratiegegevens te verkrijgen, moeten zij zich wenden tot het register voor topleveldomeinnamen ("*registry*"), dat hen verwijst naar een registrator ("*registrar*"), die hen verwijst naar een aanbieder of wederverkoper van privacy- of proxyregistratiediensten.

In dezelfde bijdragen wordt gevraagd in artikel 164/3 te verduidelijken dat, indien gebruik is gemaakt van een privacy- of proxyregistratiedienst, alle te verzamelen gegevens informatie moeten bevatten over de begunstigde gebruiker, de vergunninghouder en/of de klant van de privacy- of proxyregistratiedienst.

Deze werkwijze levert echter de volgende problemen op:

— dit zou neerkomen op een afwijking van het door artikel 28 van de NIS2-richtlijn ingevoerde systeem;

— dit zou betekenen dat privacy- of proxyregistratiediensten in de praktijk onmogelijk zouden zijn;

— en cas de recours à un service d'anonymisation ou d'enregistrement fiduciaire, le registre des noms de domaine de premier niveau ("*registry*") et le bureau d'enregistrement ("*registrar*") ne disposent pas de ces données.

Néanmoins, pour tenir compte de la préoccupation des contributeurs à la consultation publique, une autre solution a été suivie, à savoir de donner le pouvoir au Roi d'obliger les services d'anonymisation et d'enregistrement fiduciaire à transférer les données d'enregistrement de noms de domaine vers les bureaux d'enregistrement ("*registrars*"), soit de manière *ad hoc* (pour répondre à une demande d'un demandeur d'accès légitime soit de manière systématique.

Cette délégation au Roi pourrait être mise en œuvre s'il apparaît de la pratique que le fonctionnement des services d'anonymisation ou d'enregistrement fiduciaire pose un problème majeur et si les obligations qui seraient imposées sont réalistes.

Troisièmement, selon le considérant 109 de la directive NIS2, l'obligation de mise en place des bases de données de données d'enregistrement de noms de domaine (données WHOIS) "ne devrait pas aboutir à recueillir les mêmes données à de multiples reprises. Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine devraient coopérer entre eux afin d'éviter la duplication de cette tâche."

Ce considérant implique qu'il ne peut être l'intention de récolter plusieurs fois les mêmes données auprès du titulaire des noms de domaine. Cependant, cela n'empêche pas un échange d'informations entre les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine.

Quatrièmement, il est nécessaire de définir ce qu'on entend par "demandeurs d'accès légitimes". Le considérant 110 de la directive NIS2 indique que "Par "demandeurs d'accès légitimes", il convient d'entendre toute personne physique ou morale qui formule une demande en vertu du droit de l'Union ou du droit national." Ce même considérant ajoute ce qui suit: "Il peut s'agir des autorités compétentes en vertu de la présente directive et des autorités compétentes en vertu du droit de l'Union ou du droit national en matière de prévention et de détection d'infractions pénales, d'enquêtes et de poursuites en la matière, et des CERT ou des CSIRT."

— in geval van gebruik van een privacy- of proxyregistratiedienst, hebben het register voor topleveldomeinnamen ("*registry*") en de registrar ("*registrar*") deze gegevens niet.

Om rekening te houden met de bezorgdheid van de bijdragers aan de openbare raadpleging, werd echter een andere oplossing gevolgd, namelijk de Koning de bevoegdheid te geven privacy- of proxyregistratiediensten te verplichten domeinnaamregistratiegegevens aan registrars ("*registrars*") over te dragen, hetzij op ad-hocbasis (om te reageren op een vraag van een verzoeker om legitieme toegang), hetzij systematisch.

Deze delegatie aan de Koning zou kunnen worden ingevoerd als uit de praktijk blijkt dat de werking van de privacy- of proxyregistratiediensten een groot probleem vormt en als de verplichtingen die zouden worden opgelegd, realistisch zijn.

Ten derde mag, volgens overweging 109 van de NIS2-richtlijn, de verplichting om databanken met domeinnaamregistratiegegevens (WHOIS-gegevens) te creëren er niet toe "leiden dat dezelfde gegevens meermaals worden verzameld. Registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, moeten met elkaar samenwerken om dubbel werk te voorkomen."

Deze considerans impliceert dat het niet de bedoeling kan zijn om dezelfde gegevens meermaals te verzamelen bij de houder van de domeinnamen. Dit sluit echter de uitwisseling niet uit van informatie tussen de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen.

Ten vierde moet worden gedefinieerd wat wordt bedoeld met "verzoekers om legitieme toegang." In overweging 110 van de NIS2-richtlijn staat "Onder verzoeker om legitieme toegang wordt verstaan elke natuurlijke of rechtspersoon die een verzoek indient krachtens het Unie- of nationale recht." Diezelfde overweging voegt het volgende toe: "Het kan gaan om autoriteiten die uit hoofde van deze richtlijn bevoegd zijn en om autoriteiten die krachtens het Unie- of nationale recht bevoegd zijn voor het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten, evenals om CERT's of CSIRT's."

Cependant, cette définition n'est pas assez précise pour être opérationnelle. C'est pourquoi, elle a été davantage précisée sur base des contributions à la consultation publique.

Cinquièmement, comme il ressort de plusieurs contributions à la consultation publique, les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine doivent fournir aux demandeurs d'accès légitimes, dans les 72 heures de leur requête, les données demandées et non un accusé de réception.

Sixièmement, des cas de danger de mort nécessitant un accès très rapide aux données du titulaire du nom de domaine peuvent survenir. C'est la raison pour laquelle un régime spécial est prévu, impliquant la communication des données dans un délai de 24 heures.

Section 6

Modifications de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la directive 2014/65/UE

Les articles 93 et 94 visent à adapter la loi du 21 novembre 2017 et n'appellent pas de commentaire particulier.

CHAPITRE 3

Disposition abrogatoire

Art. 95

Cet article abroge la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, que le projet de loi vient remplacer.

CHAPITRE 4

Entrée en vigueur

Art. 96

Cet article fixe la date d'entrée en vigueur du projet de loi au 18 octobre 2024, conformément à l'article 41, § 1^{er}, alinéa 2, de la directive NIS2.

Les obligations découlant de la directive (mesures de cybersécurité, notifications des incidents), sont applicables

Deze definitie is echter niet nauwkeurig genoeg om inzetbaar te zijn. Daarom is ze verder verduidelijkt op basis van de bijdragen aan de openbare raadpleging.

Ten vijfde moeten, zoals blijkt uit verschillende bijdragen aan de openbare raadpleging, registers voor topleveldomeinnamen en entiteiten die domeinnaam-registratiediensten verlenen, verzoekers om legitieme toegang binnen 72 uur na hun verzoek de gevraagde gegevens verstrekken en geen ontvangstbevestiging.

Ten zesde, er kunnen levensbedreigende situaties ontstaan waarbij een zeer snelle toegang tot de gegevens van de houder van de domeinnaam vereist is. Daarom wordt een speciaal regime voorzien waarbij de gegevens moeten worden verstrekt binnen de 24 uur.

Afdeling 6

Wijzigingen van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU

De artikelen 93 en 94 passen de wet van 21 november 2017 aan en behoeven geen verdere commentaar.

HOOFDSTUK 3

Opheffingsbepaling

Art. 95

Dit artikel voorziet in de opheffing van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, die door het wetsontwerp vervangen wordt.

HOOFDSTUK 4

Inwerkingtreding

Art. 96

Dit artikel legt de datum van inwerkingtreding van het wetsontwerp vast op 18 oktober 2024, overeenkomstig artikel 41, lid 1, tweede alinea, van de NIS2-richtlijn.

De verplichtingen die voortvloeien uit de richtlijn (cyberbeveiligingsmaatregelen, meldingen van incidenten),

dès l'entrée en vigueur de la loi, à savoir le 18 octobre 2024. Toutefois, certaines mesures nationales de supervision (comme l'évaluation périodique de la conformité régulière des entités essentielles) qui seront adoptées par le Roi feront l'objet d'une mise en œuvre progressive.

Voici, Mesdames, Messieurs, la portée des dispositions du projet que le gouvernement a l'honneur de soumettre à votre approbation.

Le premier ministre,

Alexander De Croo

La ministre de l'Intérieur,

Annelies Verlinden

zullen van toepassing zijn vanaf de inwerkingtreding van de wet, namelijk 18 oktober 2024. Bepaalde nationale maatregelen voor het toezicht op essentiële entiteiten die door de Koning zullen worden aangenomen, zullen echter geleidelijk ten uitvoer worden gelegd.

Dit is, dames en heren, de draagwijdte van de bepalingen van het ontwerp dat de regering de eer heeft aan Uw beraadslaging voor te leggen.

De eerste minister,

Alexander De Croo

De minister van Binnenlandse Zaken,

Annelies Verlinden

AVANT-PROJET DE LOI**soumis à l'avis du Conseil d'État**

Avant-projet de loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

Titre 1^{er}. - Définitions et dispositions générales**CHAPITRE 1^{ER} – Objet et champ d'application**Section 1^{re}. Objet

Article 1^{er}. La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2. La présente loi vise notamment à transposer la directive européenne (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148. Cette directive est dénommée ci-après la "directive NIS2".

Section 2. Champ d'application

Art. 3. § 1^{er}. Dans les limites de l'article 4 et sans préjudice de l'article 6, la présente loi s'applique aux entités publiques ou privées d'un type visé à l'annexe I ou II et qui constituent:

1° une entreprise moyenne en vertu de l'article 2 de l'annexe de la recommandation n° 2003/361/CE; ou

2° une entreprise qui dépasse les plafonds prévus au § 1^{er} du même article de cette annexe.

L'article 3, § 4, de l'annexe de la recommandation n° 2003/361/CE ne s'applique pas aux fins de la présente loi.

§ 2. Dans le cadre de l'application de l'article 6, paragraphe 2, de l'annexe de la recommandation 2003/361/CE, l'autorité nationale de cybersécurité tient compte du degré d'indépendance dont jouit une entité à l'égard de ses partenaires et de ses entreprises liées, en particulier en ce qui concerne les réseaux et les systèmes d'information qu'elle utilise pour fournir ses services et en ce qui concerne les services qu'elle fournit.

Sur base de l'alinéa 1^{er}, l'autorité nationale de cybersécurité considère qu'une telle entité ne constitue pas une entreprise moyenne en vertu de l'article 2 de l'annexe de la recommandation 2003/361/CE, ou ne dépasse pas les plafonds applicables à une entreprise moyenne prévus au paragraphe 1 dudit article, si, après prise en compte du degré d'indépendance de ladite entité, celle-ci n'aurait pas été considérée comme constituant

VOORONTWERP VAN WET**onderworpen aan het advies van de Raad van State**

Voorontwerp van wet tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

Titel 1. - Definities en algemene bepalingen**HOOFDSTUK 1 – Onderwerp en toepassingsgebied****Afdeling 1. Onderwerp**

Artikel 1. Deze wet regelt een materie als bedoeld in artikel 74 van de Grondwet.

Art. 2. Deze wet voorziet met name in de omzetting van de Europese Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148. Deze richtlijn wordt hierna de "NIS2-richtlijn" genoemd.

Afdeling 2. Toepassingsgebied

Art. 3. § 1. Binnen de grenzen van artikel 4 en onverminderd artikel 6 is deze wet van toepassing op publieke of private entiteiten van een in bijlage I of II bedoelde soort die:

1° een middelgrote onderneming zijn krachtens artikel 2 van de bijlage bij Aanbeveling nr. 2003/361/EG; of

2° een onderneming die de plafonds overschrijdt zoals vastgesteld in lid 1 van hetzelfde artikel van deze bijlage.

Artikel 3, § 4, van de bijlage bij Aanbeveling nr. 2003/361/EG geldt niet voor de toepassing van deze wet.

§ 2. In het kader van de toepassing van artikel 6, lid 2, van de bijlage bij Aanbeveling 2003/361/EG houdt de nationale cyberbeveiligingsautoriteit rekening met de mate van onafhankelijkheid van een entiteit ten opzichte van haar partnerondernemingen of verbonden ondernemingen, meer bepaald wat de netwerk- en informatiesystemen betreft waarvan zij gebruikmaakt bij het verlenen van haar diensten en wat de diensten betreft die zij verleent.

Op basis van het eerste lid beschouwt de nationale cyberbeveiligingsautoriteit een dergelijke entiteit als een entiteit die niet wordt aangemerkt als een middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG, noch de plafonds voor een middelgrote onderneming als bepaald in lid 1 van dat artikel overschrijdt, indien die entiteit, rekening houdend met de mate van onafhankelijkheid

une entreprise moyenne ou dépassant lesdits plafonds si seules ses propres données avaient été prises en compte.

Le Roi peut déterminer les critères sur base desquels le degré d'indépendance dont jouit une entité à l'égard de ses partenaires et de ses entreprises liées est évalué.

§ 3. Sans préjudice de l'article 6, la présente loi s'applique également aux entités d'un type visé à l'annexe I ou II, quelle que soit leur taille, dans un des cas suivants:

1° les services sont fournis par:

a) des fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public;

a) des prestataires de services de confiance;

b) des registres de noms de domaine de premier niveau et des fournisseurs de services de systèmes de noms de domaine;

2° l'entité est identifiée comme une entité essentielle ou importante conformément au chapitre 4 du présent titre;

3° l'entité est une entité de l'administration publique:

a) au niveau fédéral;

b) au niveau fédéré, identifiée conformément à l'article 11, § 2.

§ 4. Sans préjudice de l'article 6, quelle que soit leur taille, la présente loi s'applique aux entités identifiées comme **[exploitant d'une infrastructure critique au sens de la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques / entité critique au sens de la loi CER]**.

§ 5. Quelle que soit leur taille, la présente loi s'applique aux entités fournissant des services d'enregistrement de noms de domaine.

§ 6. Après consultation des éventuelles autorités sectorielles concernées et de l'autorité nationale de cybersécurité, le Roi peut, par arrêté délibéré en Conseil des ministres, ajouter d'autres secteurs et/ou sous-secteurs à l'annexe I ou II ou élargir les secteurs et/ou sous-secteurs existants.

Art. 4. § 1^{er}. La présente loi s'applique aux entités visées à l'article 3 qui sont établies en Belgique et qui fournissent leurs services ou exercent leurs activités au sein de l'Union européenne.

§ 2. Par exception au paragraphe 1^{er}, la présente loi s'applique:

die zij geniet, niet als middelgrote onderneming zou worden aangemerkt of niet zou worden geacht die plafonds te overschrijden ingeval alleen rekening zou worden gehouden met haar eigen gegevens.

De Koning kan de criteria bepalen op basis waarvan de mate van onafhankelijkheid van een entiteit ten opzichte van haar partnerondernemingen of verbonden ondernemingen wordt beoordeeld.

§ 3. Onverminderd artikel 6 is deze wet ook van toepassing op entiteiten van een in bijlage I of II bedoelde soort, ongeacht hun omvang, in een van de volgende gevallen:

1° de diensten worden verleend door:

b) aanbieders van openbare elektronische-communicatienetwerken of van openbare elektronische-communicatiediensten;

b) verleners van vertrouwensdiensten;

c) registers voor topleveldomeinnamen en domeinnaamsysteem-dienstverleners;

2° de entiteit wordt geïdentificeerd als een essentiële of belangrijke entiteit overeenkomstig hoofdstuk 4 van deze titel;

3° de entiteit is een overheidsinstantie:

a) op federaal niveau;

b) op het niveau van de deelgebieden, die overeenkomstig artikel 11, § 2, geïdentificeerd is.

§ 4. Onverminderd artikel 6 is deze wet van toepassing op entiteiten, ongeacht hun omvang, die worden geïdentificeerd als **[exploitant van een kritieke infrastructuur als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren / kritieke entiteit als bedoeld in de CER-wet]**.

§ 5. Deze wet is van toepassing op entiteiten, ongeacht hun omvang, die domeinnaamregistratiediensten verlenen.

§ 6. Na raadpleging van de eventuele betrokken sectorale overheden en de nationale cyberbeveiligingsautoriteit kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, andere sectoren en/of deelsectoren toevoegen aan bijlage I of II of de bestaande sectoren en/of deelsectoren uitbreiden.

Art. 4. § 1. Deze wet is van toepassing op de in artikel 3 bedoelde entiteiten die gevestigd zijn in België en die hun diensten verlenen of hun activiteiten verrichten in de Europese Unie.

§ 2. In afwijking van paragraaf 1 is deze wet van toepassing op:

1° aux fournisseurs de réseaux de communications électroniques publics ou aux fournisseurs de services de communications électroniques accessibles au public, lorsqu'ils fournissent ces services en Belgique;

2° aux fournisseurs de services DNS, registres de noms de domaine de premier niveau, entités fournissant des services d'enregistrement de noms de domaine, fournisseurs de services d'informatique en nuage, fournisseurs de services de centres de données, fournisseurs de réseaux de diffusion de contenu, fournisseurs de services gérés, fournisseurs de services de sécurité gérés, ainsi qu'aux fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux, lorsqu'ils ont leur établissement principal en Belgique, conformément aux paragraphes 4 et 5.

§ 3. Si une entité visée au paragraphe 2, 2°, n'est pas établie dans l'Union européenne mais y fournit des services, elle désigne un représentant dans l'Union. Le représentant est établi dans l'un des États membres où les services sont fournis.

§ 4. Pour l'application de la présente loi, les entités visées au paragraphe 2, 2°, ont leur établissement principal en Belgique lorsqu'elles y prennent principalement les décisions liées aux mesures de gestion des risques de cybersécurité.

Si l'endroit où ces décisions sont prises ne peut être déterminé ou ne se trouve pas dans l'Union européenne, les entités visées au paragraphe 2, 2°, sont réputées avoir leur établissement principal en Belgique lorsqu'elles y conduisent leurs opérations de cybersécurité.

Si l'endroit où sont conduites ces opérations ne peut être déterminé, les entités visées au paragraphe 2, 2°, sont réputées avoir leur établissement principal en Belgique lorsque s'y trouve leur établissement avec le plus grand nombre d'employés.

§ 5. Les entités visées au paragraphe 2, 2°, sont réputées avoir leur établissement principal en Belgique, pour l'application de la présente loi, lorsqu'elles ne sont pas établies dans l'Union européenne mais qu'elles fournissent leurs services dans l'Union et que leur représentant dans l'Union européenne est établi en Belgique.

§ 6. La désignation d'un représentant par une entité visée au paragraphe 2, 2°, est sans préjudice d'actions en justice qui pourraient être intentées contre l'entité elle-même.

Art. 5. § 1^{er}. La présente loi ne porte pas préjudice à l'application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ni aux dispositions légales et réglementaires qui complètent ou précisent ledit règlement ni à la loi du 30 juillet

1° aanbieders van openbare elektronische-communicatienetwerken of aanbieders van openbare elektronische-communicatiediensten, wanneer zij deze diensten in België verlenen;

2° DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsook op aanbieders van onlinemarktplaatsen, onlinezoekmachines of platforms voor socialenetwerkdiensten, wanneer zij hun hoofdvesting in België hebben, overeenkomstig paragraaf 4 en 5.

§ 3. Indien een entiteit als bedoeld in paragraaf 2, 2°, niet in de Europese Unie is gevestigd, maar diensten in de Unie aanbiedt, wijst zij een vertegenwoordiger in de Unie aan. De vertegenwoordiger is gevestigd in een van de lidstaten waar de diensten worden verleend.

§ 4. Voor de toepassing van deze wet hebben de in paragraaf 2, 2°, bedoelde entiteiten hun hoofdvesting in België wanneer zij er hoofdzakelijk de beslissingen nemen rond maatregelen voor het beheer van cyberbeveiligingsrisico's.

Indien de plaats waar deze beslissingen worden genomen niet kan worden bepaald of zich niet in de Europese Unie bevindt, worden de in paragraaf 2, 2°, bedoelde entiteiten geacht hun hoofdvesting in België te hebben wanneer zij er hun cyberbeveiligingsactiviteiten uitvoeren.

Indien de plaats waar deze activiteiten plaatsvinden niet kan worden bepaald, worden de in paragraaf 2, 2°, bedoelde entiteiten geacht hun hoofdvesting in België te hebben wanneer hun vestiging met het grootste aantal werknemers zich daar bevindt.

§ 5. Voor de toepassing van deze wet worden de in paragraaf 2, 2°, bedoelde entiteiten geacht hun hoofdvesting in België te hebben, wanneer zij niet gevestigd zijn in de Europese Unie maar hun diensten verlenen in de Unie en hun vertegenwoordiger in de Europese Unie in België gevestigd is.

§ 6. De aanwijzing van een vertegenwoordiger door een entiteit als bedoeld in paragraaf 2, 2°, doet geen afbreuk aan juridische stappen die tegen de entiteit zelf kunnen worden ingesteld.

Art. 5. § 1. Deze wet doet geen afbreuk aan de toepassing van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), aan de wettelijke en reglementaire bepalingen die deze verordening aanvullen of

2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

§ 2. La présente loi est sans préjudice de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé et ne s'applique pas aux systèmes de communication et d'information approuvés pour utiliser des informations classifiées sous forme électronique conformément à la loi précitée.

§ 3. La présente loi est sans préjudice des règles applicables aux documents nucléaires, au sens de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire.

§ 4. La présente loi ne s'applique pas:

1° aux services de renseignement et de sécurité visés à l'article 2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

2° à l'Organe de coordination pour l'analyse de la menace créé par l'article 5 de la loi du 10 juillet 2006 relative à l'analyse de la menace;

3° au Ministère de la Défense visé à l'article 1^{er} de l'arrêté royal du 2 décembre 2018 déterminant la structure générale du Ministère de la Défense et fixant les attributions de certaines autorités;

4° aux services de police visés à l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux;

5° aux autorités judiciaires, entendues comme les organes du pouvoir judiciaire, le Ministère public inclus;

6° le Service public fédéral Justice créé par l'arrêté royal du 23 mai 2001 portant création du Service public fédéral Justice, lorsqu'il gère des banques de données pour les autorités judiciaires visés au 5°;

7° aux réseaux et systèmes d'information des missions diplomatiques et consulaires belges dans des pays tiers à l'Union européenne;

8° aux établissements de classe I au sens de l'article 3.1 de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants.

Par dérogation à l'alinéa 1^{er}, 8°, la présente loi est applicable aux éléments d'une installation nucléaire destinée à la production industrielle d'électricité et qui servent au transport de l'électricité.

verduidelijken of aan de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

§ 2. Deze wet doet geen afbreuk aan de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek geregeerde dienst en is niet van toepassing op communicatie- en informatiesystemen die zijn goedgekeurd om geclassificeerde informatie in elektronische vorm te gebruiken overeenkomstig de bovengenoemde wet.

§ 3. Deze wet doet geen afbreuk aan de regels die van toepassing zijn op nucleaire documenten in de zin van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.

§ 4. Deze wet is niet van toepassing op:

1° de inlichtingen- en veiligheidsdiensten bedoeld in artikel 2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

2° het Coördinatieorgaan voor de dreigingsanalyse opgericht bij artikel 5 van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

3° het Ministerie van Landsverdediging bedoeld in artikel 1 van het koninklijk besluit van 2 december 2018 tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en tot vaststelling van de bevoegdheden van bepaalde autoriteiten;

4° de politiediensten bedoeld in artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus;

5° de rechterlijke overheden, begrepen als de organen van de rechterlijke macht, met inbegrip van het Openbaar Ministerie;

6° de Federale Overheidsdienst Justitie opgericht bij het koninklijk besluit van 23 mei 2001 houdende oprichting van de Federale Overheidsdienst Justitie, wanneer deze databanken beheert voor de rechterlijke overheden bedoeld in 5°;

7° netwerk- en informatiesystemen van diplomatieke en consulaire missies in landen buiten de Europese Unie;

8° de inrichtingen van klasse I als bedoeld in artikel 3.1 van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen.

In afwijking van het eerste lid, 8°, is deze wet van toepassing op de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit.

§ 5. Les dispositions du titre 3, du titre 4 et du titre 5 ne s'appliquent pas:

1° à la Direction générale Centre de Crise du Service public fédéral Intérieur, **[créée par l'arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise /la loi NCCN];**

2° à l'Autorité nationale de cybersécurité visé à l'article 16.

§ 6. Les paragraphes 4 et 5 ne s'applique pas lorsqu'une de ces entités agit en tant que prestataire de services de confiance.

Art. 6. § 1^{er}. Lorsqu'un instrument juridique sectoriel de l'Union européenne impose aux entités qui entrent dans le champ d'application de la présente loi d'adopter des mesures de gestion des risques en matière de cybersécurité ou de notifier des incidents significatifs et lorsque ces exigences ont un effet au moins équivalent à celui des obligations prévues par la présente loi, les dispositions pertinentes de la présente loi ne sont pas applicables à ces entités.

Lorsqu'un instrument juridique sectoriel de l'Union européenne visé à l'alinéa 1^{er} ne couvre pas l'ensemble des entités d'un secteur spécifique entrant dans le champ d'application de la présente loi, les dispositions pertinentes de la présente loi s'appliquent aux entités non couvertes par cet instrument juridique sectoriel de l'Union européenne.

§ 2. Les exigences visées au paragraphe 1^{er}, alinéa 1^{er}, sont considérées comme ayant un effet équivalent aux obligations de la présente loi lorsque:

1° les mesures de gestion des risques en matière de cybersécurité ont un effet au moins équivalent à celui des mesures prévues à l'article 30; ou

2° l'instrument juridique sectoriel de l'Union européenne prévoit un accès immédiat, s'il y a lieu automatique et direct, aux notifications d'incidents pour le CSIRT national et lorsque les exigences relatives à la notification des incidents importants sont au moins équivalentes aux obligations prévues aux articles 34 à 37.

§ 3. Les dispositions du titre 3, du titre 4 et du titre 5 ne s'appliquent pas aux entités relevant des secteurs bancaire et infrastructures des marchés financiers au sens de l'annexe I qui tombent dans le champ d'application du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) n° 2016/1011, en ce compris l'activité de dépositaire central de titres exercée par la Banque nationale de Belgique.

§ 4. Les dispositions du titre 3, chapitre 1^{er}, du titre 4 et du titre 5 ne s'appliquent pas:

§ 5. De bepalingen van titel 3, 4 en 5 zijn niet van toepassing op:

1° de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken, opgericht **[bij het koninklijk besluit van 18 april 1988 tot oprichting van het coördinatie- en Crisiscentrum van de regering /bij de NCCN-wet];**

2° de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16.

§ 6. De paragrafen 4 en 5 zijn niet van toepassing wanneer een van deze instanties optreedt als aanbieder van vertrouwensdiensten.

Art. 6. § 1. Indien een sectorspecifiek rechtsinstrument van de Europese Unie vereist dat entiteiten die tot het toepassingsgebied van deze wet behoren, maatregelen nemen voor het beheer van cyberbeveiligingsrisico's of significante incidenten melden en indien deze eisen ten minste gelijkwaardig zijn aan de in deze wet vastgestelde verplichtingen, zijn de relevante bepalingen van deze wet niet van toepassing op deze entiteiten.

Indien een in het eerste lid bedoeld sectorspecifiek rechtsinstrument van de Europese Unie niet op alle entiteiten in een specifieke sector betrekking heeft die tot het toepassingsgebied van deze wet behoren, zijn de relevante bepalingen van deze wet van toepassing op de entiteiten waarop dit sectorspecifieke rechtsinstrument van de Europese Unie geen betrekking heeft.

§ 2. De in paragraaf 1, eerste lid, bedoelde eisen worden geacht gelijkwaardig te zijn aan de verplichtingen van deze wet wanneer:

1° de maatregelen voor het beheer van cyberbeveiligingsrisico's ten minste gelijkwaardig zijn aan de maatregelen bedoeld in artikel 30; of

2° het sectorspecifieke rechtsinstrument van de Europese Unie in onmiddellijke toegang voorziet, in voorkomend geval automatisch en rechtstreeks, tot de meldingen van incidenten voor het nationale CSIRT en wanneer de eisen voor het melden van significante incidenten ten minste gelijkwaardig zijn aan de verplichtingen bedoeld in de artikelen 34 tot 37.

§ 3. De bepalingen van titel 3, 4 en 5 zijn niet van toepassing op entiteiten die behoren tot de sectoren van het bankwezen en de infrastructuur voor de financiële markt in de zin van bijlage I die onder het toepassingsgebied vallen van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011, met inbegrip van de activiteit van centrale effectenbewaarinstituut verricht door de Nationale Bank van België.

§ 4. De bepalingen van titel 3, hoofdstuk 1, van titel 4 en van titel 5 zijn niet van toepassing:

1° à la Banque nationale de Belgique, exception faite de son activité de dépositaire central de titres à laquelle s'applique le paragraphe 3;

2° aux établissements financiers soumis à la supervision de la Banque nationale de Belgique en vertu des articles 8 et 12bis de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique qui ne relèvent pas du paragraphe 3.

Art. 7. Le Roi peut, par arrêté délibéré en Conseil des ministres:

1° préciser les instruments juridiques sectoriels équivalents visés à l'article 6, § 1^{er}, alinéa 1^{er};

2° définir des règles particulières relatives à la coordination de l'échange d'informations, en ce compris des exigences relatives à la notification des incidents importants, entre les entités visées à l'article 6, § 3 et § 4, l'autorité sectorielle concernée, l'autorité nationale de cybersécurité et l'autorité chargée de la gestion des risques cyber.

CHAPITRE 2 – Définitions

Art. 8. Pour l'application de la présente loi, il faut entendre par:

1° "réseau et système d'information":

a) un réseau de communications électroniques au sens de l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques;

b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation du processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel; ou

c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance;

2° "sécurité des réseaux et des systèmes d'information": la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à tout événement susceptible de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, ou des services que ces réseaux et systèmes d'information offrent ou rendent accessibles;

3° "cybersécurité": la cybersécurité au sens de l'article 2, 1), du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de

1° op de Nationale Bank van België, met uitzondering van haar activiteit van centrale effectenbewaarinstituering waarop paragraaf 3 van toepassing is;

2° op financiële instellingen die onderworpen zijn aan het toezicht van de Nationale Bank van België krachtens artikel 8 en 12bis van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België en die niet onder paragraaf 3 vallen.

Art. 7. De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad,:

1° de gelijkwaardige sectorspecifieke rechtsinstrumenten als bedoeld in artikel 6, § 1, eerste lid, nader bepalen;

2° bijzondere regels vaststellen met betrekking tot de coördinatie van de informatie-uitwisseling, met inbegrip van de eisen voor het melden van significante incidenten, tussen de entiteiten bedoeld in artikel 6, § 3 en § 4, de betrokken sectorale overheid, de nationale cyberbeveiligingsautoriteit en de autoriteit belast met het beheer van cyber risico's.

HOOFDSTUK 2 – Definities

Art. 8. Voor de toepassing van deze wet moet worden verstaan onder:

1° "netwerk- en informatiesysteem":

a) een elektronische-communicatienetwerk als bedoeld in artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

b) elk apparaat of elke groep van onderling verbonden of bij elkaar behorende apparaten, waarvan er een of meer, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische componenten van dat apparaat die met name de automatisering van het operationele proces, de controle op afstand of het verkrijgen van werkingsgegevens in real time mogelijk maken; of

c) digitale gegevens die worden opgeslagen, verwerkt, opgehaald of verzonden met behulp van de in punten a) en b) bedoelde elementen met het oog op de werking, het gebruik, de bescherming en het onderhoud ervan;

2° "beveiliging van netwerk- en informatiesystemen": het vermogen van netwerk- en informatiesystemen om op een bepaald niveau van betrouwbaarheid weerstand te bieden aan elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die door of via deze netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen;

3° "cyberbeveiliging": cyberbeveiliging als bedoeld in artikel 2, 1), van Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en

cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité), ci-après le "règlement sur la cybersécurité";

4° "stratégie nationale en matière de cybersécurité": le cadre cohérent fournissant des objectifs et des priorités stratégiques dans le domaine de la cybersécurité et de la gouvernance en vue de les réaliser en Belgique;

5° "incident": un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles;

6° "incident évité": un événement qui aurait pu compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles, mais dont la réalisation a pu être empêchée ou ne s'est pas produite;

7° "incident de cybersécurité majeur": un incident qui provoque des perturbations dépassant les capacités de réaction du seul État membre de l'Union européenne concerné ou qui a un impact significatif sur au moins deux États membres de l'Union européenne;

8° "traitement des incidents": toutes les actions et procédures visant à prévenir, détecter, analyser et contenir un incident ou à y répondre et à y remédier;

9° "risque": le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et de la probabilité qu'un tel incident se produise;

10° "cybermenace": une cybermenace au sens de l'article 2, 8), du règlement sur la cybersécurité;

11° "cybermenace importante": une cybermenace qui, compte tenu de ses caractéristiques techniques, peut être considérée comme susceptible d'avoir un impact grave sur les réseaux et les systèmes d'information d'une entité ou les utilisateurs des services de l'entité, en causant un dommage matériel, corporel ou moral considérable;

12° "produit TIC": un produit TIC au sens de l'article 2, 12), du règlement sur la cybersécurité;

13° "service TIC": un service TIC au sens de l'article 2, 13), du règlement sur la cybersécurité;

14° "processus TIC": un processus TIC au sens de l'article 2, 14), du règlement sur la cybersécurité;

15° "vulnérabilité": une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace;

inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening), hierna de "cyberbeveiligingsverordening" genoemd;

4° "nationale cyberbeveiligingsstrategie": een samenhangend kader met strategische doelstellingen en prioriteiten op het vlak van cyberbeveiliging en governance om die doelstellingen en prioriteiten in België te verwezenlijken;

5° "incident": een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt;

6° "bijna-incident": een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar had kunnen brengen, maar die met succes is voorkomen of zich niet heeft voorgedaan;

7° "grootschalig cyberbeveiligingsincident": een incident dat leidt tot een verstoringniveau dat te groot is om door een getroffen lidstaat van de Europese Unie alleen te worden verholpen of dat significante gevolgen heeft voor ten minste twee lidstaten van de Europese Unie;

8° "incidentenbehandeling": alle acties en procedures die gericht zijn op het voorkomen, opsporen, analyseren en indammen van of het reageren op en het herstellen van een incident;

9° "risico": de mogelijkheid van verlies of verstoring als gevolg van een incident, wat wordt uitgedrukt als een combinatie van de omvang van een dergelijk verlies of een dergelijke verstoring en de waarschijnlijkheid dat het incident zich voordoet;

10° "cyberdreiging": een cyberdreiging als bedoeld in artikel 2, 8), van de cyberbeveiligingsverordening;

11° "significante cyberdreiging": een cyberdreiging waarvan op basis van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerk- en informatiesystemen van een entiteit of de gebruikers van de diensten van de entiteit door het veroorzaken van aanzienlijke materiële of immateriële schade;

12° "ICT-product": een ICT-product als bedoeld in artikel 2, 12), van de cyberbeveiligingsverordening;

13° "ICT-dienst": een ICT-dienst als bedoeld in artikel 2, 13), van de cyberbeveiligingsverordening;

14° "ICT-proces": een ICT-proces als bedoeld in artikel 2, 14), van de cyberbeveiligingsverordening;

15° "kwetsbaarheid": een zwakheid, vatbaarheid of gebrek van ICT-producten of ICT-diensten die door een cyberdreiging kan worden uitgebuit;

16° “norme”: une norme au sens de l'article 2, 1), du règlement (UE) n°1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil, ci-après le “règlement (UE) n°1025/2012”;

17° “point d'échange internet”: une structure de réseau qui permet l'interconnexion de plus de deux réseaux indépendants (systèmes autonomes), essentiellement aux fins de faciliter l'échange de trafic internet, qui n'assure l'interconnexion que pour des systèmes autonomes et qui n'exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic;

18° “système de nom de domaine” ou “DNS”: un système hiérarchique et distribué d'affectation de noms qui permet l'identification des services et des ressources internet, ce qui rend possible l'utilisation de services de routage et de connectivité internet par les dispositifs des utilisateurs finaux pour accéder à ces services et ressources;

19° “fournisseur de services DNS”: une entité qui fournit:

a) des services de résolution de noms de domaine récurrents accessibles au public destinés aux utilisateurs finaux de l'internet; ou

b) des services de résolution de noms de domaine faisant autorité pour une utilisation par des tiers, à l'exception des serveurs de noms de racines;

20° “registre de noms de domaine de premier niveau”: une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration du domaine de premier niveau, y compris de l'enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage;

21° “entité fournissant des services d'enregistrement de noms de domaine”: un bureau d'enregistrement ou un agent agissant pour le compte de bureaux d'enregistrement, tel qu'un fournisseur ou revendeur de services d'anonymisation ou d'enregistrement fiduciaire;

22° “service numérique”: un service au sens de l'article 1^{er}, § 1^{er}, b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure

16° “norm”: een norm als bedoeld in artikel 2, 1), van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad, hierna “Verordening (EU) nr. 1025/2012”;

17° “internetknooppunt”: een netwerkfaciliteit die de interconnectie van meer dan twee onafhankelijke netwerken (autonome systemen) mogelijk maakt, voornamelijk ter vergemakkelijking van de uitwisseling van internetverkeer, die alleen interconnectie voor autonome systemen biedt en die niet vereist dat het internetverkeer dat tussen een paar deelnemende autonome systemen verloopt, via een derde autonoom systeem verloopt, noch dat verkeer wijzigt of anderszins verstoort;

18° “domeinnaamsysteem” of “DNS”: een hiërarchisch gedistribueerd naamgevingssysteem dat het mogelijk maakt internetdiensten en -bronnen te identificeren, waardoor eindgebruikersapparaten in staat worden gesteld routing- en connectiviteitsdiensten op het internet te gebruiken om die diensten en bronnen te bereiken;

19° “DNS-dienstverlener”: een entiteit die de volgende diensten verleent:

a) openbare recursieve domeinnaamomzettingssdiensten voor interneteindgebruikers; of

b) gezaghebbende domeinnaamomzettingssdiensten voor gebruik door derden, met uitzondering van root-naamserver;

20° “register voor topleveldomeinnamen”: een entiteit waaraan een specifieke topleveldomeinnaam is gedelegeerd en die verantwoordelijk is voor het beheer van de topleveldomeinnaam, met inbegrip van de registratie van domeinnamen onder de topleveldomeinnaam en de technische exploitatie van de topleveldomeinnaam, met inbegrip van de exploitatie van de naamserver, het onderhoud van de databases en de verdeling van de zonebestanden van de topleveldomeinnaam over de naamserver, ongeacht of die activiteiten door de entiteit zelf worden uitgevoerd of worden uitbesteed, maar met uitzondering van situaties waarin topleveldomeinnamen uitsluitend voor eigen gebruik worden aangewend door een register;

21° “entiteit die domeinnaamregistratiediensten aanbiedt”: een registrar of een agent die namens registrators optreedt, zoals een aanbieder van privacy- of proxy-registratiediensten of wederverkoper;

22° “digitale dienst”: een dienst als bedoeld in artikel 1, lid 1, b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015

d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information;

23° "service de confiance": un service de confiance au sens de l'article 3, 16., du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, ci-après le "règlement eIDAS";

24° "prestataire de service de confiance": un prestataire de services de confiance au sens de l'article 3, 19., du règlement eIDAS;

25° "service de confiance qualifié": un service de confiance qualifié au sens de l'article 3, 17., du règlement eIDAS;

26° "prestataire de services de confiance qualifiés": un prestataire de services de confiance qualifié au sens de l'article 3, 20., du règlement eIDAS;

27° "place de marché en ligne": une place de marché en ligne au sens de l'article I.8, 41°, du Code de droit économique;

28° "moteur de recherche en ligne": un moteur de recherche en ligne au sens de l'article 2, 5), du règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne;

29° "service d'informatique en nuage": un service numérique qui permet l'administration à la demande et l'accès large à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris lorsque ces ressources sont réparties à différents endroits;

30° "service de centre de données": un service qui englobe les structures, ou groupes de structures, dédiées à l'hébergement, l'interconnexion et l'exploitation centralisées des équipements informatiques et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l'ensemble des installations et infrastructures de distribution d'électricité et de contrôle environnemental;

31° "réseau de diffusion de contenu": un réseau de serveurs géographiquement répartis visant à assurer la haute disponibilité, l'accessibilité ou la fourniture rapide de contenu et de services numériques aux utilisateurs d'internet pour le compte de fournisseurs de contenu et de services;

32° "plateforme de services de réseaux sociaux": une plateforme qui permet aux utilisateurs finaux de se connecter, de partager, de découvrir et de communiquer entre eux sur plusieurs terminaux, notamment par conversations en ligne, publications, vidéos et recommandations;

33° "représentant": une personne physique ou morale établie dans l'Union européenne qui est expressément désignée pour agir pour le compte d'un fournisseur de services DNS,

betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij;

23° "vertrouwensdienst": een vertrouwensdienst als bedoeld in artikel 3, 16., van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, hierna de "eIDAS-verordening" genoemd;

24° "verlener van vertrouwensdiensten": een verlener van vertrouwensdiensten als bedoeld in artikel 3, 19., van de eIDAS-verordening;

25° "gekwalficeerde vertrouwensdienst": een gekwalificeerde vertrouwensdienst als bedoeld in artikel 3, 17., van de eIDAS-verordening;

26° "gekwalficeerde verlener van vertrouwensdiensten": een gekwalificeerde verlener van vertrouwensdiensten als bedoeld in artikel 3, 20., van de eIDAS-verordening;

27° "onlinemarktplaats": een onlinemarktplaats als bedoeld in artikel I.8, 41°, van het Wetboek van economisch recht;

28° "onlinezoekmachine": een onlinezoekmachine als bedoeld in artikel 2, 5), van Verordening (EU) 2019/1150 van het Europees Parlement en de Raad van 20 juni 2019 ter bevordering van billijkheid en transparantie voor zakelijke gebruikers van onlinetussenhandelsdiensten;

29° "cloudcomputingdienst": een digitale dienst die administratie op aanvraag en brede toegang op afstand tot een schaalbare en elastische pool van deelbare computerbronnen mogelijk maakt, ook wanneer die bronnen over verschillende locaties verspreid zijn;

30° "datacentrumdienst": een dienst die structuren of groepen van structuren omvat die bestemd zijn voor de gecentraliseerde accommodatie, de interconnectie en de exploitatie van IT- en netwerkkapparatuur die diensten op het gebied van gegevensopslag, -verwerking en -transport aanbiedt, samen met alle faciliteiten en infrastructuur voor energiedistributie en omgevingscontrole;

31° "netwerk voor de levering van inhoud": een netwerk van geografisch verspreide servers met het oog op een hoge beschikbaarheid, toegankelijkheid of snelle levering van digitale inhoud en diensten aan internetgebruikers ten behoeve van aanbieders van inhoud en diensten;

32° "platform voor socialenetwerkdiensten": een platform dat eindgebruikers in staat stelt zich met elkaar te verbinden, te delen, te ontdekken en met elkaar te communiceren via meerdere apparaten, met name via chats, posts, video's en aanbevelingen;

33° "vertegenwoordiger": een in de Europese Unie gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om op te treden namens een DNS-dienstverlener, een register

d'un registre de noms de domaine de premier niveau, d'une entité fournissant des services d'enregistrement de noms de domaine, d'un fournisseur d'informatique en nuage, d'un fournisseur de services de centre de données, d'un fournisseur de réseau de diffusion de contenu, d'un fournisseur de services gérés, d'un fournisseur de services de sécurité gérés ou d'un fournisseur de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux non établi dans l'Union européenne, qui peut être contactée par l'autorité nationale de cybersécurité à la place de l'entité elle-même concernant les obligations incombant à ladite entité en vertu de la présente loi;

34° "entité de l'administration publique": une autorité administrative visée à l'article 14, § 1^{er}, alinéa 1^{er}, des lois coordonnées sur le Conseil d'État qui satisfait aux critères suivants:

1° elle n'a pas de caractère industriel ou commercial;

2° elle n'exerce pas à titre principal une activité énumérée dans la colonne type d'entité d'un autre secteur ou sous-secteur de l'une des annexes de la loi

3° elle n'exerce pas à titre principal ses activités dans le domaine de la sécurité nationale, de la défense ou de la sécurité publique;

35° "réseau de communications électroniques public": un réseau public de communications électroniques au sens de l'article 2, 10°, de la loi du 13 juin 2005 relative aux communications électroniques;

36° "service de communications électroniques": un service de communications électroniques au sens de l'article 2, 5°, de la loi du 13 juin 2005 relative aux communications électroniques;

37° "entité": une personne physique ou morale constituée et reconnue comme telle en vertu du droit national de son lieu de constitution, et ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations;

38° "fournisseur de services gérés": une entité qui fournit des services liés à l'installation, à la gestion, à l'exploitation ou à l'entretien de produits, de réseaux, d'infrastructures ou d'applications TIC ou d'autres réseaux et systèmes d'information, par l'intermédiaire d'une assistance ou d'une administration active, soit dans les locaux des clients, soit à distance;

39° "fournisseur de services de sécurité gérés": un fournisseur de services gérés qui effectue ou fournit une assistance pour des activités liées à la gestion des risques en matière de cybersécurité;

40° "organisme de recherche": une entité dont l'objectif premier est de mener des activités de recherche appliquée ou de développement expérimental en vue d'exploiter les résultats de cette recherche à des fins commerciales, à l'exclusion des établissements d'enseignement;

voor topleveldomeinnamen, een entiteit die domeinnaamregistratiediensten verleent, een aanbieder van cloudcomputingdiensten, een aanbieder van datacentrumdiensten, een aanbieder van een netwerk voor de levering van inhoud, een aanbieder van beheerde diensten, een aanbieder van beheerde beveiligingsdiensten, of een aanbieder van een onlinemarktplaats, van een onlinezoekmachine of van een platform voor socialenetwerkdiensten die niet in de Europese Unie is gevestigd, en die door de nationale cyberbeveiligingsautoriteit kan worden gecontacteerd in plaats van de entiteit zelf met betrekking tot de verplichtingen van die entiteit uit hoofde van deze wet;

34° "overheidsinstantie": een administratieve overheid als bedoeld in artikel 14, § 1, eerste lid, van de gecoördineerde wetten op de Raad van State die aan de volgende criteria voldoet:

1° zij is niet van industriële of commerciële aard;

2° zij oefent niet hoofdzakelijk een activiteit opgesomd in de kolom soort entiteit van een van de andere sector of deelsector van een van de bijlagen;

3° zij oefent niet hoofdzakelijk activiteiten uit op het gebied van nationale veiligheid, defensie of openbare veiligheid;

35° "openbaar elektronische-communicatienetwerk": een openbaar elektronische-communicatienetwerk als bedoeld in artikel 2, 10°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

36° "elektronische-communicatiedienst": een elektronische-communicatiedienst als bedoeld in artikel 2, 5°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

37° "entiteit": een natuurlijke of rechtspersoon die als zodanig is opgericht en erkend volgens het nationale recht van zijn vestigingsplaats, en die in eigen naam rechten kan uitoefenen en aan verplichtingen kan worden onderworpen;

38° "aanbieder van beheerde diensten": een entiteit die diensten verleent die verband houden met de installatie, het beheer, de exploitatie of het onderhoud van ICT-producten, -netwerken, -infrastructuur, -toepassingen of andere netwerken en informatiesystemen, via bijstand of actieve administratie bij de klanten ter plaatse of op afstand;

39° "aanbieder van beheerde beveiligingsdiensten": een aanbieder van beheerde diensten die bijstand biedt of verleent voor activiteiten die verband houden met risicobeheer op het gebied van cyberbeveiliging;

40° "onderzoeksorganisatie": een entiteit die als hoofddoel heeft het verrichten van toegepast onderzoek of experimentele ontwikkeling met het oog op de exploitatie van de resultaten van dat onderzoek voor commerciële doeleinden, met uitsluiting van onderwijsinstellingen;

41° “recommandation n° 2003/361/CE”: la Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises;

42° “loi du 13 juin 2005”: la loi du 13 juin 2005 relative aux communications électroniques;

[43° “loi CER”: la loi [CER];

43° “loi du 1^{er} juillet 2011”: la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques;]

[44° “loi NPU”: la loi [NPU];]

[45° “loi NCCN”: la loi [NCCN];

45° “arrêté royal NCCN”: l’arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise]

46° “autorité nationale de cybersécurité”: l’autorité visée à l’article 16;

47° “CSIRT national”: le centre national de réponse aux incidents de sécurité informatique;

48° “ENISA”: l’Agence de l’Union européenne pour la cybersécurité instituée par le règlement sur la cybersécurité;

49° “NCCN”: le Centre de crise national organisé par [la loi NCCN/l’arrêté royal NCCN];

50° “règlement (UE) 2016/679”: le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données);

51° “Autorité de protection des données”: autorité de contrôle au sens de l’article 4, 21°, du règlement (UE) 2016/679;

52° “organisme national d’accréditation”: l’organisme visé à l’article 2, point 11, du règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l’accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, ci-après le “règlement (CE) n° 765/2008”;

53° la politique de sécurité des systèmes et réseaux d’information (“P.S.I.”): la politique consignée dans un document visé à l’article 30, reprenant les mesures de sécurité des réseaux et des systèmes d’information, à adopter par une entité essentielle ou importante;

54° “organisme d’évaluation de la conformité”: l’organisme visé à l’article 2, point 13, du règlement (CE) n° 765/2008;

41° “Aanbeveling nr. 2003/361/EG”: de Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen;

42° “wet van 13 juni 2005”: de wet van 13 juni 2005 betreffende de elektronische communicatie;

[43° “CER-wet”: de wet [CER];

43° “wet van 1 juli 2011”: de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur;]

[44° “NPU-wet”: de wet [NPU];]

[45° “NCCN-wet”: de wet [NCCN];

45° “NCCN-koninklijk besluit”: het koninklijk besluit van 18 april 1988 tot oprichting van het coördinatie- en Crisiscentrum van de regering]

46° “nationale cyberbeveiligingsautoriteit”: de autoriteit bedoeld in artikel 16;

47° “nationaal CSIRT”: het nationale computer security incident response team;

48° “Enisa”: het Agentschap van de Europese Unie voor cyberbeveiliging opgericht bij de cyberbeveiligingsverordening;

49° “NCCN”: het Nationaal Crisiscentrum georganiseerd door [de NCCN-wet/het NCCN-koninklijk besluit];

50° “Verordening (EU) 2016/679”: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);

51° “Gegevensbeschermingsautoriteit”: toezichthoudende autoriteit in de zin van artikel 4, 21°, van Verordening (EU) 2016/679;

52° “nationale accreditatie-instantie”: de instantie bedoeld in artikel 2, punt 11, van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93, hierna “Verordening (EG) nr. 765/2008”;

53° beveiligingsbeleid voor de netwerk- en informatiesystemen (“I.B.B.”): het beleid vastgelegd in een document als bedoeld in artikel 30, met de te nemen maatregelen voor de beveiliging van netwerk- en informatiesystemen die een essentiële of belangrijke entiteit heeft genomen;

54° “conformiteitsbeoordelingsinstantie”: de instantie bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008;

55° “autorité sectorielle”: l'autorité visée à l'article 15, § 2;

56° “réseau des CSIRT”: le réseau des CSIRT nationaux institué par l'article 15 de la directive NIS2;

57° “groupe de coopération”: le groupe de coopération institué par l'article 14 de la directive NIS2;

58° “incident significatif”: tout incident ayant un impact significatif sur la fourniture de l'un des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II de la loi et qui:

1° a causé ou est susceptible de causer une perturbation opérationnelle grave de l'un des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II ou des pertes financières pour l'entité concernée; ou

2° a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

59° “crise cyber”: tout incident de cybersécurité qui, par sa nature ou ses conséquences:

1° menace les intérêts vitaux du pays ou les besoins essentiels de la population;

2° requiert des décisions urgentes;

3° demande une action coordonnée de plusieurs départements et organisations;

60° “Institut”: l'Institut belge des services postaux et des télécommunications tel que visé à l'article 13 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.

CHAPITRE 3 – Catégories d'entités

Art. 9. Sont des entités essentielles:

1° les entités d'un type visé à l'annexe I qui excèdent les plafonds applicables aux moyennes entreprises prévus à l'article 2, § 1^{er}, de l'annexe de la recommandation n° 2003/361/CE;

2° les prestataires de services de confiance qualifiés et les registres de noms de domaines de premier niveau ainsi que les fournisseurs de services DNS, quelle que soit leur taille;

3° les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public qui constituent au moins des moyennes entreprises, en vertu de l'article 2 de l'annexe de la recommandation n° 2003/361/CE;

4° les entités de l'administration publique qui relèvent de l'État fédéral;

55° “sectorale overheid”: de overheid bedoeld in artikel 15, § 2;

56° “CSIRT-netwerk”: het netwerk van nationale CSIRT's opgericht bij artikel 15 van de NIS2-richtlijn;

57° “samenwerkingsgroep”: de samenwerkingsgroep opgericht bij artikel 14 van de NIS2-richtlijn;

58° “significant incident”: elk incident dat significante gevolgen heeft voor de verlening van een van de diensten in de sectoren of deelsectoren van bijlage I en II van de wet en dat:

1° een ernstige operationele verstoring van een van de diensten in de sectoren of deelsectoren van bijlage I en II of financiële verliezen voor de betrokken entiteit heeft veroorzaakt of kan veroorzaken; of

2° andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

59° “cybercrisis”: elk cyberbeveiligingsincident dat wegens zijn aard of gevolgen:

1° de vitale belangen van het land of de essentiële behoeften van de bevolking bedreigt;

2° een dringende besluitvorming vereist;

3° en de gecoördineerde inzet van verscheidene departementen en organismen vergt;

60° “Instituut”: het Belgisch Instituut voor postdiensten en telecommunicatie zoals bedoeld in artikel 13 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.

HOOFDSTUK 3 – Categorieën van entiteiten

Art. 9. Zijn essentiële entiteiten:

1° de entiteiten van een in bijlage I bedoelde soort die de plafonds voor middelgrote ondernemingen overschrijden die zijn vastgesteld in artikel 2, lid 1, van de bijlage bij Aanbeveling nr. 2003/361/EG;

2° de gekwalificeerde verleners van vertrouwensdiensten en de registers voor topleveldomeinnamen, alsook de DNS-dienstverleners, ongeacht hun omvang;

3° de aanbieders van openbare elektronische-communicatienetwerken of van openbare elektronische-communicatiediensten die minstens in aanmerking komen als middelgrote ondernemingen uit hoofde van artikel 2 van de bijlage bij Aanbeveling nr. 2003/361/EG;

4° de overheidsinstanties die tot de Federale Staat behoren;

5° les entités visées à l'article 3, § 4;

6° toute autre entité d'un type visé à l'annexe I ou II qui est identifiée comme entité essentielle conformément à l'article 11.

Art. 10. Sont des entités importantes:

1° les entités d'un type visé à l'annexe I ou II qui ne sont pas qualifiées d'entités essentielles sur la base de l'article 9;

2° les entités identifiées comme entités importantes conformément à l'article 11.

CHAPITRE 4 – Identification

Art. 11. § 1^{er}. Sans préjudice de l'article 6, d'initiative ou sur proposition de l'éventuelle autorité sectorielle concernée, l'autorité nationale de cybersécurité identifie une entité comme entité essentielle ou importante, quelle que soit sa taille, dans les cas suivants:

1° l'entité est le seul prestataire, en Belgique, d'au moins un service essentiel au maintien d'activités sociétales ou économiques critiques, notamment dans l'un des secteurs ou sous-secteurs repris aux annexes I et II de la loi;

2° une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique;

3° une perturbation du service fourni par l'entité pourrait induire un risque systémique important, en particulier pour les secteurs où une telle interruption pourrait avoir un impact transfrontière;

4° l'entité est critique en raison de son importance spécifique au niveau national ou régional pour le secteur ou le type de service en question, ou pour d'autres secteurs interdépendants, en Belgique.

§ 2. En ce qui concerne les entités fédérées, l'autorité nationale de cybersécurité identifie les administrations publiques qui, à la suite d'une évaluation basée sur les risques, fournissent des services dont la perturbation pourrait avoir un impact important sur des activités sociétales ou économiques critiques.

§ 3. Dans le cadre de l'identification visée au paragraphe 1^{er} et 2, l'autorité nationale de cybersécurité soumet préalablement un projet de décision à l'entité concernée et ensuite aux éventuelles entités fédérées concernées et autorités sectorielles, qui rendent un avis non publié endéans les soixante jours.

Lorsqu'aucun avis n'est rendu dans le délai visé à l'alinéa 1^{er}, l'avis est réputé être favorable.

En cas d'avis défavorable d'une autorité sectorielle et si l'autorité nationale de cybersécurité souhaite maintenir son projet de décision, le projet de décision, accompagné de

5° de entiteiten bedoeld in artikel 3, § 4;

6° alle andere entiteiten van een in bijlage I of II bedoelde soort die worden geïdentificeerd als essentiële entiteiten overeenkomstig artikel 11.

Art. 10. Zijn belangrijke entiteiten:

1° de entiteiten van een in bijlage I of II bedoelde soort die niet als essentiële entiteiten worden beschouwd op basis van artikel 9;

2° de entiteiten die worden geïdentificeerd als belangrijke entiteiten overeenkomstig artikel 11.

HOOFDSTUK 4 – Identificatie

Art. 11. § 1. Onverminderd artikel 6 identificeert de nationale cyberbeveiligingsautoriteit, op eigen initiatief of op voorstel van de eventuele betrokken sectorale overheid, een entiteit als een essentiële of belangrijke entiteit ongeacht haar omvang in de volgende gevallen:

1° de entiteit is de enige aanbieder, in België, van minstens één dienst die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten, met name in een van de sectoren of deelsectoren van bijlage I en II van de wet;

2° een verstoring van de door de entiteit verleende dienst kan aanzienlijke gevolgen hebben voor de openbare veiligheid, de openbare beveiliging of de volksgezondheid;

3° een verstoring van de door de entiteit verleende dienst kan een aanzienlijk systeemrisico met zich brengen, met name voor sectoren waar een dergelijke verstoring een grensoverschrijdende impact kan hebben;

4° de entiteit is kritiek vanwege het specifieke belang ervan op nationaal of regionaal niveau voor de specifieke sector of het specifieke type dienst, of voor andere onderling afhankelijke sectoren in België.

§ 2. Wat de deelgebieden betreft, identificeert de nationale cyberbeveiligingsautoriteit overheidsinstanties die, na een risicobeoordeling, diensten verlenen waarvan de verstoring aanzienlijke gevolgen kan hebben voor kritieke maatschappelijke of economische activiteiten.

§ 3. In het kader van de identificatie bedoeld in paragraaf 1 en 2 legt de nationale cyberbeveiligingsautoriteit vooraf een ontwerpbeslissing voor aan de betrokken entiteit en vervolgens aan de eventuele betrokken deelgebieden en sectorale overheden, die binnen zestig dagen een niet-gepubliceerd advies uitbrengen.

Indien binnen de in het eerste lid bedoelde termijn geen advies is uitgebracht, wordt het advies geacht gunstig te zijn.

In geval van een ongunstig advies van een sectorale overheid en indien de nationale cyberbeveiligingsautoriteit haar ontwerpbeslissing wenst te handhaven, wordt de

l'avis, est soumis au Comité stratégique du renseignement et de la sécurité, créé par l'arrêté royal du 22 décembre 2020 portant création du Conseil national de sécurité, du Comité stratégique du renseignement et de la sécurité et du Comité de coordination du renseignement et de la sécurité.

§ 4. L'autorité nationale de cybersécurité évalue et, le cas échéant, met à jour l'identification des entités essentielles et importantes au moins tous les deux ans, selon les modalités visées aux paragraphes 1^{er} à 3.

L'autorité nationale de cybersécurité adresse les identifications et actualisations des entités essentielles au NCCN et à l'éventuelle autorité sectorielle concernée.

L'autorité nationale de cybersécurité adresse les identifications et actualisations des entités importantes à l'éventuelle autorité sectorielle concernée.

§ 5. Dans les cas visés au paragraphe 1^{er}, le Roi peut, par arrêté délibéré en Conseil des ministres, désigner comme entité essentielle ou importante une entité qui ne fait pas partie des secteurs visés en annexe.

Art. 12. Dans le cadre de l'identification visée à l'article 11, l'entité concernée transmet toutes les informations utiles à son éventuelle identification, à la demande de l'autorité nationale de cybersécurité ou de l'autorité sectorielle.

CHAPITRE 5 – Enregistrement des entités

Art. 13. § 1^{er}. Dans les cinq mois suivant l'entrée en vigueur de la loi ou l'identification visée à l'article 11, les entités essentielles, les entités importantes et les entités fournissant des services d'enregistrement de noms de domaine s'enregistrent auprès de l'autorité nationale de cybersécurité selon les modalités pratiques fixées par cette autorité et lui communiquent les informations suivantes:

1° leur dénomination ainsi que leur numéro d'enregistrement auprès de la Banque-carrefour des entreprises (BCE) ou un enregistrement équivalent dans l'Union européenne;

2° leur adresse et leurs coordonnées actualisées, y compris leur adresse de courrier électronique, leurs plages d'IP et leur numéro de téléphone;

3° le cas échéant, le secteur et le sous-secteur concernés visés à l'annexe I ou II; et

4° le cas échéant, une liste des États membres dans lesquels elles fournissent des services relevant du champ d'application de la présente loi.

Le Roi peut compléter cette liste d'informations.

§ 2. Par dérogation au paragraphe 1^{er}, alinéa 1^{er}, lorsque l'entité visée au paragraphe précité communique déjà à l'autorité sectorielle concernée certaines des informations visées au

ontwerpbeslissing samen met het advies voorgelegd aan het Strategisch Comité Inlichtingen en Veiligheid, opgericht bij het koninklijk besluit van 22 december 2020 tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité Inlichtingen en Veiligheid en het Coördinatiecomité Inlichtingen en Veiligheid.

§ 3. De nationale cyberbeveiligingsautoriteit evalueert en actualiseert, in voorkomend geval, minstens om de twee jaar de identificatie van essentiële en belangrijke entiteiten volgens de modaliteiten bedoeld in paragraaf 1 tot 3.

De nationale cyberbeveiligingsautoriteit stuurt de identifications en actualiseringen van essentiële entiteiten naar het NCCN en naar de eventuele betrokken sectorale overheid.

De nationale cyberbeveiligingsautoriteit stuurt de identifications en actualiseringen van belangrijke entiteiten naar de eventuele betrokken sectorale autoriteit.

§ 5. In de gevallen bedoeld in paragraaf 1 kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, een entiteit die geen deel uitmaakt van de in de bijlage bedoelde sectoren, aanwijzen als een essentiële of belangrijke entiteit.

Art. 12. In het kader van de identificatie bedoeld in artikel 11 bezorgt de betrokken entiteit op verzoek van de nationale cyberbeveiligingsautoriteit of de sectorale overheid alle informatie die nuttig is voor haar eventuele identificatie.

HOOFDSTUK 5 – Registratie van de entiteiten

Art. 13. § 1. Binnen vijf maanden na de inwerkingtreding van de wet of de in artikel 11 bedoelde identificatie registreren essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen zich bij de nationale cyberbeveiligingsautoriteit volgens de door deze autoriteit vastgestelde praktische modaliteiten en bezorgen haar de volgende informatie:

1° hun naam, alsook hun registratienummer bij de Kruispuntbank van Ondernemingen (KBO) of een gelijkwaardige registratie in de Europese Unie;

2° hun adres en hun actuele contactgegevens, waaronder hun e-mailadres, hun IP-bereik en hun telefoonnummer;

3° indien van toepassing, de relevante sector en deelsector als bedoeld in bijlage I of II, en

4° indien van toepassing, een lijst van de lidstaten waar zij diensten verlenen die binnen het toepassingsgebied van deze wet vallen.

De Koning kan deze lijst met informatie aanvullen.

§ 2. In afwijking van paragraaf 1, eerste lid, vervolledigt de in voornoemde paragraaf bedoelde entiteit, wanneer zij krachtens een wettelijke verplichting al een deel van de in

paragraphe précité, en vertu d'une obligation légale, l'entité complète auprès de cette autorité sectorielle ces informations.

L'entité visée au paragraphe 1^{er}, alinéa 1^{er}, communique les informations dans les cinq mois suivant l'entrée en vigueur de la loi, selon les modalités pratiques fixées par l'autorité précitée.

§ 3. Les entités visées au paragraphe 1^{er}, alinéa 1^{er}, communiquent sans tarder toute modification des informations qu'elles ont communiquées conformément au paragraphe 1^{er}, alinéa 1^{er}, et paragraphe 2, alinéa 1^{er}, et, en tout état de cause, dans un délai de deux semaines à compter de la date de la modification.

§ 4. L'autorité sectorielle concernée communique les informations collectées en vertu des paragraphes 2 et 3 à l'autorité nationale de cybersécurité.

L'autorité nationale de cybersécurité prend les mesures nécessaires pour que les autorités sectorielles puissent consulter, pour les secteurs qui les concernent, les données communiquées.

Art. 14. § 1^{er}. Dans les deux mois suivant l'entrée en vigueur de la loi, les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les entités qui fournissent des services d'enregistrement de noms de domaine, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux communiquent à l'autorité nationale de cybersécurité, selon les modalités visées à l'article 13, § 1^{er}, alinéa 1^{er}, au moins les informations suivantes:

1° leur nom;

2° leur secteur, sous-secteur et type d'entité concernés, visés à l'annexe I ou II, le cas échéant;

3° l'adresse de leur établissement principal et de leurs autres établissements légaux dans l'Union ou, s'ils ne sont pas établis dans l'Union, de leur représentant désigné conformément à l'article 4, § 3;

4° leurs coordonnées actualisées, y compris les adresses de courrier électronique et les numéros de téléphone et, le cas échéant, celles de leur représentant désigné conformément à l'article 4, § 3;

5° les États membres dans lesquels ils fournissent leurs services relevant du champ d'application de la présente loi; et

6° leurs pages d'IP.

§ 2. Les entités visées au paragraphe 1^{er} notifient à l'autorité nationale de cybersécurité toute modification des informations

voornomde paragraaf bedoelde informatie meedeelt aan de betrokken sectorale overheid, deze informatie bij deze sectorale overheid.

De in paragraaf 1, eerste lid, bedoelde entiteit bezorgt de informatie binnen vijf maanden na de inwerkingtreding van de wet, volgens de door voornoemde overheid vastgestelde praktische modaliteiten.

§ 3. De in paragraaf 1, eerste lid, bedoelde entiteiten bezorgen onmiddellijk elke wijziging in de bijzonderheden die zij op grond van paragraaf 1, eerste lid, en paragraaf 2, eerste lid, hebben ingediend, en in elk geval binnen twee weken na de datum van de wijziging.

§ 4. De betrokken sectorale overheid bezorgt de krachtens paragraaf 2 en 3 verzamelde informatie aan de nationale cyberbeveiligingsautoriteit.

De nationale cyberbeveiligingsautoriteit neemt de nodige maatregelen om ervoor te zorgen dat de sectorale overheden de meegedeelde gegevens kunnen raadplegen voor de sectoren die hen aangaan.

Art. 14. § 1. Binnen twee maanden na de inwerkingtreding van de wet verstrekken DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsmede aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor sociale netwerkdiensten de nationale cyberbeveiligingsautoriteit volgens de modaliteiten bedoeld in artikel 13, § 1, eerste lid, ten minste de volgende informatie:

1° hun naam;

2° hun relevante sector, deelsector en soort entiteit bedoeld in bijlage I of II, waar van toepassing;

3° het adres van hun hoofdvestiging en hun andere wettelijke vestigingen in de Unie of, indien deze niet in de Unie zijn gevestigd, van hun op grond van artikel 4, § 3, aangewezen vertegenwoordiger;

4° hun actuele contactgegevens, met inbegrip van e-mailadressen en telefoonnummers en, indien van toepassing, deze van hun op grond van artikel 4, § 3, aangewezen vertegenwoordiger;

5° de lidstaten waar ze hun diensten verlenen die tot het toepassingsgebied van deze wet behoren; en

6° hun IP-bereiken.

§ 2. De in paragraaf 1 bedoelde entiteiten stellen de nationale cyberbeveiligingsautoriteit onverwijld en in elk geval

qu'elles ont communiquées en vertu du paragraphe 1^{er} sans tarder et, en tout état de cause, dans un délai de trois mois à compter de la date de la modification.

§ 3. Par dérogation au paragraphe 1^{er}, les données visées au même paragraphe, relatives aux prestataires de services de confiance qualifiés en Belgique, qui ont déjà été communiquées à l'organe de contrôle visé à l'article 17 du règlement eIDAS sont transmises par cet organe à l'autorité nationale de cybersécurité, selon les modalités fixées par le Roi.

Titre 2. Autorités compétentes et coopération au niveau national

CHAPITRE 1^{ER} – Autorités compétentes

Section 1^{re}. Désignation des autorités compétentes

Art. 15. § 1^{er}. Le Roi désigne l'autorité nationale de cybersécurité.

§ 2. Après avis de l'autorité nationale de cybersécurité, le Roi peut, par arrêté délibéré en Conseil des ministres, désigner une autorité sectorielle et, le cas échéant, un service d'inspection sectoriel chargé, pour un secteur ou sous-secteur spécifique, de la supervision de la mise en œuvre des mesures sectorielles ou sous-sectorielles supplémentaires de gestion des risques en matière de cybersécurité visées à l'article 33.

Dans le cadre de la désignation visée à l'alinéa 1^{er}, le Roi tient compte de l'identité des autorités sectorielles désignées dans le cadre de la loi [CER /du 1^{er} juillet 2011].

Le Roi peut, par arrêté délibéré en Conseil des ministres, créer des autorités sectorielles, composées de représentants de l'État fédéral, des Communautés et des Régions, conformément aux modalités prévues à l'article 92^{ter} de la loi spéciale du 8 août 1980 de réformes institutionnelles.

Par dérogation à l'alinéa 1^{er}, la loi désigne elle-même les autorités sectorielles et les services d'inspection créés et régies par la loi.

Section 2. L'autorité nationale de cybersécurité

Art. 16. L'autorité nationale de cybersécurité est chargée du suivi et de la coordination de la mise en œuvre de la présente loi, de veiller à la mise en œuvre de la présente loi par les entités essentielles et importantes ainsi que, de la gestion des crises et incidents de cybersécurité conformément à l'article 18.

A ce titre, l'autorité nationale de cybersécurité assure les tâches d'autorité compétente pour les entités essentielles et importantes, de CSIRT national, de point de contact national unique pour l'exécution de la présente loi et de représentation de la Belgique au sein du groupe de coopération, du réseau

binnen drie maanden na de datum waarop de wijziging van kracht is geworden, in kennis van eventuele wijzigingen in de gegevens die zij op grond van paragraaf 1 hebben ingediend.

§ 3. In afwijking van paragraaf 1 worden de in diezelfde paragraaf bedoelde gegevens met betrekking tot gekwalificeerde verleners van vertrouwensdiensten in België, die al zijn verstrekt aan het in artikel 17 van de eIDAS-verordening bedoelde toezichthoudende orgaan, door dat orgaan doorgestuurd naar de nationale cyberbeveiligingsautoriteit, volgens de door de Koning vastgestelde modaliteiten.

Titel 2. Bevoegde autoriteiten en samenwerking op nationaal niveau

HOOFDSTUK 1 – Bevoegde autoriteiten

Afdeling 1. Aanwijzing van de bevoegde autoriteiten

Art. 15. § 1. De Koning wijst de nationale cyberbeveiligingsautoriteit aan.

§ 2. Na advies van de nationale cyberbeveiligingsautoriteit kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, een sectorale overheid en, in voorkomend geval, een sectorale inspectiedienst aanwijzen die voor een specifieke sector of deelsector belast is met het toezicht op de uitvoering van de bijkomende sectorale of deelsectorale maatregelen voor het beheer van cyberbeveiligingsrisico's als bedoeld in artikel 33.

In het kader van de aanwijzing bedoeld in het eerste lid houdt de Koning rekening met de identiteit van de [in het kader van de **CER-wet/wet van 1 juli 2011** aangewezen sectorale overheden].

De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad, sectorale overheden oprichten, bestaande uit vertegenwoordigers van de Federale Staat, de Gemeenschappen en de Gewesten, overeenkomstig de modaliteiten bepaald in artikel 92^{ter} van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.

In afwijking van het eerste lid wijst de wet zelf de bij wet opgerichte en geregelde sectorale overheden en sectorale inspectiediensten aan.

Afdeling 2. De nationale cyberbeveiligingsautoriteit

Art. 16. De nationale cyberbeveiligingsautoriteit is belast met de opvolging en coördinatie van de uitvoering van deze wet, het toezicht op de uitvoering ervan door de essentiële en belangrijke entiteiten, alsook, met het beheer van cyberbeveiligingscrises en -incidenten overeenkomstig artikel 18.

Daartoe vervult de nationale cyberbeveiligingsautoriteit de taken van bevoegde autoriteit voor essentiële en belangrijke entiteiten, van nationaal CSIRT, van centraal nationaal contactpunt voor de uitvoering van deze wet, en vertegenwoordigt zij België in de samenwerkingsgroep, het CSIRT-netwerk en het

des CSIRT et du réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe) visé à l'article 16 de la directive NIS2.

Sous-section 1^{re}. Tâches relatives au rôle d'autorité compétente chargée de la cybersécurité

Art. 17. Les tâches de l'autorité nationale de cybersécurité sont les suivantes:

1° assurer la coordination entre les autorités compétentes dans le cadre de l'application de la présente loi, ainsi qu'entre les différents services et autorités concernés par la cybersécurité en Belgique;

2° superviser, coordonner et veiller à la mise en œuvre de la stratégie nationale en matière de cybersécurité visée à l'article 28;

3° identifier des entités essentielles et importantes conformément à l'article 11;

4° superviser la mise en œuvre de la loi par les entités essentielles et importantes conformément au titre 4;

5° assurer la coordination entre les autorités publiques et le secteur privé ou le monde scientifique;

6° formuler des propositions pour l'adaptation du cadre légal et réglementaire en matière de cybersécurité;

7° élaborer, diffuser et veiller à la mise en œuvre des standards, directives et normes pour la cybersécurité des différents types de systèmes d'information;

8° coordonner la représentation belge aux forums internationaux sur la cybersécurité, le suivi des obligations internationales et la présentation du point de vue national en la matière;

9° servir de point de contact unique exerçant une fonction de liaison visant à assurer, dans le cadre de l'application de la présente loi, la coopération transfrontière des autorités belges avec les autorités compétentes des autres États membres de l'Union européenne et, le cas échéant, avec la Commission et l'ENISA, ainsi qu'à garantir la coopération intersectorielle avec les autres autorités compétentes belges;

10° coordonner l'évaluation et la certification de la sécurité des systèmes d'information et de communication;

11° informer et sensibiliser les utilisateurs des systèmes d'information et de communication;

12° accorder des subventions pour des projets et activités relatifs à la cybersécurité, dans les limites de ses crédits budgétaires et selon les conditions établies par le Roi;

Europees netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe) bedoeld in artikel 16 van de NIS2-richtlijn.

Onderafdeling 1. Taken met betrekking tot de rol van bevoegde autoriteit belast met cyberbeveiliging

Art. 17. De nationale cyberbeveiligingsautoriteit heeft de volgende taken:

1° het zorgen voor coördinatie tussen de bevoegde autoriteiten in het kader van de toepassing van deze wet, alsook tussen de verschillende diensten en autoriteiten die betrokken zijn bij cyberbeveiliging in België;

2° het opvolgen en coördineren van en toezien op de uitvoering van de nationale cyberbeveiligingsstrategie bedoeld in artikel 28;

3° het identificeren van de essentiële en belangrijke entiteiten overeenkomstig artikel 11;

4° het toezien op de uitvoering van de wet door de essentiële en belangrijke entiteiten overeenkomstig titel 4;

5° het zorgen voor coördinatie tussen de overheden en de particuliere sector of de wetenschappelijke wereld;

6° het formuleren van voorstellen tot aanpassing van het wettelijk en regelgevend kader op het vlak van cyberbeveiliging;

7° het opstellen, verspreiden en toezien op de uitvoering van standaarden, richtlijnen en normen voor de cyberbeveiliging van de verschillende soorten informatiesystemen;

8° het coördineren van de Belgische vertegenwoordiging in internationale fora voor cyberbeveiliging, van de opvolging van internationale verplichtingen en van voorstellen van het nationale standpunt op dit vlak;

9° het fungeren als centraal contactpunt dat een verbindingfunctie vervult om, in het kader van de toepassing van deze wet, te zorgen voor grensoverschrijdende samenwerking van de Belgische autoriteiten met de bevoegde autoriteiten van andere lidstaten van de Europese Unie en in voorkomend geval met de Commissie en Enisa, alsmede om te zorgen voor sectoroverschrijdende samenwerking met andere bevoegde Belgische autoriteiten;

10° het coördineren van de evaluatie en certificering van de beveiliging van informatie- en communicatiesystemen;

11° het informeren en sensibiliseren van gebruikers van informatie- en communicatiesystemen;

12° het toekennen van subsidies voor projecten en activiteiten rond cyberbeveiliging, binnen de grenzen van haar begrotingskredieten en volgens de voorwaarden bepaald door de Koning;

13° faciliter et encourager l'organisation de formations en matière de cybersécurité pour les membres du personnel des entités essentielles ou importantes;

14° établir une liste des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine. Par la suite, réexaminer cette liste et, le cas échéant, la mettre à jour régulièrement et au moins tous les deux ans.

Sous-section 2. Tâches relatives au rôle de gestion des crises cyber

Art. 18. Sans préjudice des dispositions [de la loi NPU], de [la loi NCCN/l'arrêté royal NCCN] et de leurs arrêtés d'exécution les tâches de l'autorité nationale de cybersécurité relatives au rôle de gestion des crises cyber sont les suivantes:

1° en collaboration avec le NCCN, recenser les capacités, les moyens et les procédures qui peuvent être déployés en cas de crise cyber;

2° [par dérogation à l'article 24, 1°, de la loi NCCN], superviser, en collaboration avec le NCCN, la rédaction, l'actualisation et l'opérationnalisation du plan national de réaction aux crises et incidents de cybersécurité majeurs visé à l'article 29;

3° assurer le rôle de coordinateur dans la gestion des crises et incidents de cybersécurité, le cas échéant conformément au plan visé au 2°, pour autant que ces crises et incidents ne constituent pas des crises nationales [au sens de la loi NPU].

Sous-section 3. Tâches et obligations relatives au rôle de CSIRT national

Art. 19. § 1^{er}. Les tâches du CSIRT national, sont les suivantes:

1° surveiller et analyser les cybermenaces, les vulnérabilités et les incidents au niveau national et, sur demande, apporter une assistance aux entités essentielles et importantes concernées pour surveiller en temps réel ou quasi réel leurs réseaux et systèmes d'information;

2° activer le mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les cybermenaces, les vulnérabilités et les incidents auprès des entités essentielles et importantes concernées ainsi qu'auprès des autorités compétentes et des autres parties prenantes concernées, si possible en temps quasi réel;

3° réagir aux incidents et apporter une assistance aux entités essentielles et importantes concernées, le cas échéant;

4° rassembler et analyser des données forensiques, et assurer une analyse dynamique des risques et incidents et une appréciation de la situation en matière de cybersécurité;

13° het faciliteren en aanmoedigen van de organisatie van opleidingen rond cyberbeveiliging voor personeelsleden van essentiële of belangrijke entiteiten;

14° het opstellen van een lijst van essentiële en belangrijke entiteiten, alsook van entiteiten die domeinnaamregistratiediensten verlenen. Vervolgens het regelmatig en ten minste om de twee jaar evalueren en, in voorkomend geval, actualiseren van die lijst.

Onderafdeling 2. Taken met betrekking tot het cybercrisisbeheer

Art. 18. Onverminderd de bepalingen van [de NPU-wet], [de NCCN-wet/het NCCN-koninklijk besluit] en de uitvoeringsbesluiten ervan vervult de nationale cyberbeveiligingsautoriteit de volgende taken met betrekking tot het cybercrisisbeheer:

1° in samenwerking met het NCCN, het vaststellen van de capaciteiten, middelen en procedures die in geval van een cybercrisis kunnen worden ingezet;

2° [in afwijking van artikel 24, 1°, van de NCCN-wet], het opvolgen van de opmaak, actualisering en operationalisering van het nationale plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons bedoeld in artikel 29, in samenwerking met het NCCN;

3° het vervullen van de rol van coördinator bij het beheer van cyberbeveiligingscrises en -incidenten, in voorkomend geval overeenkomstig het in 2° bedoelde plan, voor zover deze crises en incidenten geen nationale crises zijn [als bedoeld in de NPU-wet].

Onderafdeling 3. Taken en voorschriften met betrekking tot de rol van nationaal CSIRT

Art. 19. § 1. Het nationale CSIRT heeft de volgende taken:

1° het monitoren en analyseren van cyberdreigingen, kwetsbaarheden en incidenten op nationaal niveau, en, op verzoek, het verlenen van bijstand aan de betrokken essentiële en belangrijke entiteiten met betrekking tot het realtime of bijna-realtime monitoren van hun netwerk- en informatiesystemen;

2° het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie onder de betrokken essentiële en belangrijke entiteiten en aan de bevoegde autoriteiten en andere relevante belanghebbenden over cyberdreigingen, kwetsbaarheden en incidenten, in bijna-realtime indien mogelijk;

3° het reageren op incidenten en verlenen van bijstand aan de betrokken essentiële en belangrijke entiteiten, indien van toepassing;

4° het verzamelen en analyseren van forensische gegevens en het zorgen voor dynamische risico- en incidentenanalyse en situationeel bewustzijn met betrekking tot cyberbeveiliging;

5° réaliser, à la demande d'une entité essentielle ou importante, un scan proactif du réseau et des systèmes d'information de l'entité concernée afin de détecter les vulnérabilités susceptibles d'avoir un impact important;

6° participer au réseau des CSIRT, coopérer de manière effective, efficace et sécurisée au sein de ce réseau et apporter une assistance mutuelle en fonction de ses capacités et de ses compétences aux autres membres du réseau des CSIRT à leur demande;

7° le cas échéant, agir en qualité de coordinateur aux fins du processus de divulgation coordonnée des vulnérabilités en vertu de l'article 22;

8° contribuer au déploiement d'outils sécurisés de partage d'informations;

9° procéder à un scan proactif et non intrusif des réseaux et systèmes d'information accessibles au public lorsque ce scan est effectué dans le but de détecter les réseaux et systèmes d'information vulnérables ou configurés de façon peu sûre et d'informer les entités concernées et qu'il n'a pas d'effet négatif sur le fonctionnement des services des entités;

10° détecter, observer et analyser des problèmes de sécurité informatique;

11° établir des relations de coopération avec les acteurs concernés du secteur privé, en vue d'atteindre les objectifs de la présente loi;

12° faciliter la coopération visée au 11° en encourageant l'adoption et l'utilisation de pratiques, de systèmes de classification et de taxonomies communs ou normalisés en ce qui concerne:

- a) les procédures de gestion des incidents;
- b) la gestion de crise; et
- c) la divulgation coordonnée des vulnérabilités en vertu de l'article 22;

13° coopérer et, le cas échéant, échanger des informations pertinentes conformément à l'article 27 avec les communautés visées au même article;

14° participer aux évaluations par les pairs organisées conformément à l'article 19 de la directive NIS2.

Après avis du CSIRT national, le Roi peut, par arrêté délibéré en Conseil des ministres, lui confier des tâches supplémentaires.

§ 2. Lorsqu'il exécute les tâches visées au paragraphe 1^{er}, le CSIRT national peut donner la priorité à certaines tâches sur la base d'une approche basée sur les risques.

5° op verzoek van een essentiële of belangrijke entiteit: het proactief scannen van de netwerk- en informatiesystemen van de betrokken entiteit om kwetsbaarheden met mogelijk significante gevolgen op te sporen;

6° het deelnemen aan het CSIRT-netwerk, het doeltreffend, efficiënt en veilig samenwerken in dit netwerk en, in overeenstemming met zijn capaciteiten en bevoegdheden, het verlenen van wederzijdse bijstand aan andere leden van dit netwerk op hun verzoek;

7° indien van toepassing, het optreden als coördinator ten behoeve van het in artikel 22 bedoelde proces van gecoördineerde bekendmaking van kwetsbaarheden;

8° het bijdragen aan de uitrol van veilige instrumenten voor het delen van informatie;

9° het proactief en niet-intrusief scannen van openbaar toegankelijke netwerk- en informatiesystemen als deze scan wordt uitgevoerd om kwetsbare of onveilig geconfigureerde netwerk- en informatiesystemen op te sporen en de betrokken entiteiten te informeren en deze geen negatieve gevolgen heeft voor de werking van de diensten van de entiteiten;

10° het opsporen, observeren en analyseren van computerbeveiligingsproblemen;

11° het tot stand brengen van samenwerkingsrelaties met relevante belanghebbenden in de particuliere sector, teneinde de doelstellingen van deze wet te verwezenlijken;

12° het vergemakkelijken van de in punt 11° bedoelde samenwerking door de invoering en het gebruik te bevorderen van gemeenschappelijke of gestandaardiseerde praktijken, classificatieschema's en taxonomieën met betrekking tot:

- a) procedures voor de incidentenbehandeling;
- b) crisisbeheer; en
- c) de gecoördineerde bekendmaking van kwetsbaarheden uit hoofde van artikel 22;

13° het samenwerken en in voorkomend geval uitwisselen van relevante informatie overeenkomstig artikel 27 met de in datzelfde artikel bedoelde gemeenschappen;

14° het deelnemen aan de overeenkomstig artikel 19 van de NIS2-richtlijn georganiseerde collegiale toetsingen.

Na advies van het nationale CSIRT kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, dit CSIRT bijkomende taken toevertrouwen.

§ 2. Bij de uitvoering van de in paragraaf 1 bedoelde taken kan het nationale CSIRT, op grond van een risicogebaseerde benadering, prioriteit geven aan bepaalde taken.

Art. 20. Les obligations du CSIRT national sont les suivantes:

1° disposer d'une infrastructure de communication et d'information adaptée, sécurisée et résiliente lui permettant d'échanger des informations avec les entités essentielles et importantes et les autres parties prenantes;

2° veiller à un niveau élevé de disponibilité de ses canaux de communication en évitant les points uniques de défaillance et disposer de plusieurs moyens pour être contacté et contacter autrui à tout moment; spécifier clairement les canaux de communication et les faire connaître aux partenaires et collaborateurs;

3° disposer de locaux et de systèmes d'information se trouvant sur des sites sécurisés;

4° être doté d'un système approprié de gestion et de routage des demandes afin, notamment, de faciliter les transferts effectifs et efficaces;

5° garantir la confidentialité et la fiabilité de ses opérations;

6° être doté des effectifs adéquats afin de pouvoir garantir une disponibilité permanente de ses services et veiller à ce que son personnel reçoive une formation appropriée;

7° être doté de systèmes redondants et d'un espace de travail de secours pour assurer la continuité de ses services.

Art. 21. § 1^{er}. Dans le cadre de l'exercice de ses compétences, le CSIRT national prend toutes les mesures adéquates afin de réaliser les objectifs définis aux articles 19 et 20. Ces mesures doivent être proportionnelles à ces objectifs, et respecter les principes d'objectivité, de transparence et de non-discrimination.

§ 2. Lorsque cela s'avère strictement nécessaire à la réalisation de ses tâches énumérées à l'article 19, § 1^{er}, 1° à 5°, le CSIRT national peut obtenir d'un opérateur visé à l'article 2, 11°, de la loi du 13 juin 2005, des données d'identification visées à l'article 2, alinéa 1^{er}, 5°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ou des métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi précitée du 13 juin 2005 conservées par celui-ci.

Les finalités poursuivies par les tâches précitées sont:

1° sans préjudice des compétences des personnes exerçant la police judiciaire [, notamment des procureurs du Roi, du procureur fédéral ou des procureurs généraux, ni des compétences des juges d'instruction], la prévention, la recherche et la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave;

Art. 20. De voorschriften voor het nationale CSIRT omvatten het volgende:

1° beschikken over een passende, veilige en weerbare communicatie- en informatie-infrastructuur waardoor informatie kan worden uitgewisseld met essentiële en belangrijke entiteiten en andere relevante belanghebbenden;

2° een hoge mate van beschikbaarheid van zijn communicatiekanalen garanderen door zwakke punten (single points of failure) te voorkomen, en beschikken over diverse kanalen waarlangs te allen tijde contact met het nationale CSIRT kan worden opgenomen en contact met anderen kan worden opgenomen; de communicatiekanalen duidelijk specificeren en meedelen aan de gebruikersgroep en de samenwerkingspartners;

3° beschikken over lokalen en informatiesystemen die zich op beveiligde locaties bevinden;

4° uitgerust zijn met een adequaat systeem voor het beheren en routeren van verzoeken met het oog op doeltreffende en efficiënte overdrachten;

5° de vertrouwelijkheid en betrouwbaarheid van zijn activiteiten waarborgen;

6° beschikken over voldoende personeel om te allen tijde de beschikbaarheid van zijn diensten te garanderen, en ervoor zorgen dat zijn personeel naar behoren wordt opgeleid;

7° uitgerust zijn met redundante systemen en reservewerkruimten om de continuïteit van zijn diensten te waarborgen.

Art. 21. § 1. In het kader van de uitoefening van zijn bevoegdheden neemt het nationale CSIRT alle passende maatregelen om de in artikel 19 en 20 bepaalde doelstellingen te verwezenlijken. Deze maatregelen moeten evenredig zijn met die doelstellingen, en in overeenstemming met de beginselen van objectiviteit, transparantie en non-discriminatie.

§ 2. Indien dat strikt noodzakelijk is voor de uitvoering van zijn taken opgesomd in artikel 19, § 1, 1° tot 5°, kan het nationale CSIRT identificatiegegevens bedoeld in artikel 2, eerste lid, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector of elektronische-communicatiemetagegegevens als bedoeld in artikel 2, 93°, van de wet van 13 juni 2005 verkrijgen van een operator als bedoeld in artikel 2, 11°, van de voormelde wet van 13 juni 2005, die deze gegevens bewaart.

De doeleinden van voornoemde taken zijn:

1° onverminderd de bevoegdheden van de personen die de gerechtelijke politie uitoefenen [, met name de procureurs des Konings, de federale procureur of de procureurs-generaal.] het voorkomen, onderzoeken en opsporen van inbreuken die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten;

2° la prévention de menaces graves contre la sécurité publique;

3° l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information;

Le CSIRT national peut déterminer le délai endéans lequel l'opérateur répond à sa demande, en fonction de l'urgence de celle-ci.

§ 3. Lorsque le CSIRT national adresse à un opérateur une demande de données d'identification visées à l'article 2, alinéa 1^{er}, 5°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, cette demande est autorisée par le supérieur hiérarchique.

§ 4. Lorsque le CSIRT national adresse à un opérateur une demande de métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi du 13 juin 2005 autres que celles visées au paragraphe 3, cette demande fait l'objet d'un contrôle préalable par l'Autorité de protection des données.

En cas de situation urgente dûment justifiée, le CSIRT national peut se passer du contrôle préalable visé à l'alinéa 1^{er} et solliciter directement les données. Cette demande est envoyée sans délai à l'autorité visée à l'alinéa 1^{er} pour permettre un contrôle ultérieur.

Lorsqu'à la suite du contrôle visé à l'alinéa 2, l'Autorité de protection des données refuse de confirmer la validité de la demande de métadonnées de communications électroniques visée à l'alinéa 1^{er}, le CSIRT national le notifie sans délai à l'opérateur concerné et supprime les métadonnées reçues.

§ 5. Le directeur général du CSIRT national désigne expressément les personnes habilitées à traiter les données de communications électroniques visées au présent article.

§ 6. Le CSIRT national informe, dans la mesure du possible, les personnes physiques concernées de l'accès à leurs données de communications électroniques lorsque cela n'est plus susceptible de compromettre le bon déroulement de ses tâches ou d'une enquête en cours et lorsque ces personnes peuvent être identifiées.

§ 7. Sans préjudice des articles 28quinquies, § 1^{er}, et 57, § 1^{er}, du Code d'instruction criminelle, pour atteindre ces objectifs, le CSIRT national est autorisé à détenir, à divulguer, à diffuser ou à faire usage de toutes les informations disponibles, même si celles-ci sont issues d'un accès non autorisé à un système informatique par un tiers.

§ 8. Dans l'accomplissement de ses missions, le CSIRT national use de la prudence que l'on est en droit d'attendre d'une autorité publique, en veillant toujours en priorité à ne

2° het voorkomen van ernstige bedreigingen voor de openbare veiligheid;

3° het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten of informatiesystemen.

Het nationale CSIRT kan bepalen binnen welke termijn de operator op zijn verzoek moet reageren, naargelang de dringendheid hiervan.

§ 3. Indien het nationale CSIRT een operator een verzoek om identificatiegegevens bedoeld in artikel 2, eerste lid, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector stuurt, wordt dat verzoek toegestaan door de hiërarchische meerdere.

§ 4. Indien het nationale CSIRT een operator een verzoek om elektronische-communicatiemetagegegevens als bedoeld in artikel 2, 93°, van de wet van 13 juni 2005 die geen in paragraaf 3 bedoelde gegevens zijn, stuurt, wordt dat verzoek vooraf gecontroleerd door de Gegevensbeschermingsautoriteit.

In dringende en naar behoren met redenen omklede gevallen kan het nationale CSIRT optreden zonder de voorafgaande controle bedoeld in het eerste lid, en de gegevens rechtstreeks opvragen. Dit verzoek wordt onverwijld naar de in het eerste lid bedoelde overheid gestuurd om een latere controle mogelijk te maken.

Indien de Gegevensbeschermingsautoriteit, na de in het tweede lid bedoelde controle, weigert de geldigheid van het in het eerste lid bedoelde verzoek om elektronische-communicatiemetagegegevens te bevestigen, stelt het nationale CSIRT de betrokken operator daarvan onverwijld in kennis en verwijdt het de ontvangen metagegegevens.

§ 5. De directeur-generaal van het nationale CSIRT wijst uitdrukkelijk de personen aan die gemachtigd zijn om de in dit artikel bedoelde elektronische-communicatiegegevens te verwerken.

§ 6. Het nationale CSIRT brengt de betrokken natuurlijke personen voor zover mogelijk op de hoogte van de toegang tot hun elektronische-communicatiegegevens als de uitvoering van zijn taken of van een lopend onderzoek hierdoor niet meer in het gedrang kan komen en als deze personen kunnen worden geïdentificeerd.

§ 7. Onverminderd de artikelen 28quinquies, § 1, en 57, § 1, van het Wetboek van strafvordering mag het nationale CSIRT, om die doelstellingen te verwezenlijken, alle beschikbare gegevens bezitten, onthullen of verspreiden, of er enig gebruik van maken, zelfs als die gegevens voortkomen uit een ongerechtigde toegang tot een informaticasysteem door een derde.

§ 8. Het nationale CSIRT vervult zijn opdrachten met de nodige behoedzaamheid die verwacht mag worden van een overheid, waarbij er steeds bij voorrang voor wordt gezorgd dat

pas perturber le fonctionnement du système informatique et en prenant toutes précautions raisonnables afin qu'aucun dommage matériel ne soit causé au système informatique.

Le directeur général du CSIRT national veille, par l'adoption de procédures internes, au respect des conditions visées au présent article.

Art. 22. § 1^{er}. Dans son rôle de coordinateur aux fins de la divulgation coordonnée des vulnérabilités, le CSIRT national fait office d'intermédiaire de confiance en facilitant, si nécessaire, les interactions entre la personne physique ou morale qui signale une potentielle vulnérabilité et le fabricant ou le fournisseur des produits TIC ou des services TIC potentiellement vulnérables, à la demande de l'une des deux parties.

Dans ce cadre, les tâches du CSIRT national consistent notamment à:

1° identifier et contacter les entités concernées;

2° apporter une assistance aux personnes physiques ou morales signalant une vulnérabilité; et

3° négocier des délais de divulgation et gérer les vulnérabilités qui touchent plusieurs entités.

§ 2. Toute personne physique ou morale peut signaler, même de manière anonyme lorsqu'elle le demande, au CSIRT national l'existence d'une potentielle vulnérabilité.

Le signalement est effectué par écrit, selon la procédure détaillée sur le site internet du CSIRT national.

Ce signalement est sans préjudice de l'application de la loi du 28 novembre 2022 sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé ou des dispositions légales sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur public.

§ 3. Le CSIRT national veille à ce que des mesures de suivi diligentes soient prises en ce qui concerne la vulnérabilité signalée et veille à l'anonymat de la personne physique ou morale signalant la vulnérabilité, pour autant que cette personne le demande et respecte les conditions visées à l'article 23.

Le CSIRT national préserve l'exhaustivité, l'intégrité, le stockage durable et la confidentialité des informations transmises au travers du signalement.

L'accès à ces informations est limité aux personnes habilitées par le directeur général du CSIRT national, sauf lorsque le partage de ces informations s'avère nécessaire à l'exécution des tâches énumérées au présent article.

de werking van het informaticasysteem niet wordt verstoord en alle redelijke voorzorgen worden genomen om te voorkomen dat het informaticasysteem materiële schade oploopt.

De directeur-generaal van het nationale CSIRT zorgt voor de naleving van de in dit artikel vermelde voorwaarden. Daartoe werkt hij interne procedures uit.

Art. 22. § 1. In zijn rol van coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden treedt het nationale CSIRT op als een betrouwbare tussenpersoon en vergemakkelijkt, waar nodig, de interactie tussen de natuurlijke of rechtspersoon die een mogelijke kwetsbaarheid meldt enerzijds en de fabrikant of aanbieder van de mogelijk kwetsbare ICT-producten of -diensten anderzijds, op verzoek van een van beide partijen.

In dat kader omvatten de taken van het nationale CSIRT met name:

1° het identificeren van en contact opnemen met de betrokken entiteiten;

2° het bijstaan van de natuurlijke of rechtspersonen die een kwetsbaarheid melden; en

3° het onderhandelen over tijdschema's voor de bekendmaking, en het beheren van kwetsbaarheden die van invloed zijn op meerdere entiteiten.

§ 2. Iedere natuurlijke of rechtspersoon kan, zelfs desgevraagd anoniem, aan het nationale CSIRT het bestaan van een mogelijke kwetsbaarheid melden.

De melding gebeurt schriftelijk, volgens de procedure die op de website van het nationale CSIRT beschreven is.

Deze melding doet geen afbreuk aan de toepassing van de wet van 28 november 2022 betreffende de bescherming van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de particuliere sector of van wettelijke bepalingen betreffende de bescherming van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de overheidssector.

§ 3. Het nationale CSIRT ziet erop toe dat de gemelde kwetsbaarheid zorgvuldig wordt opgevolgd en waarborgt de anonimiteit van de natuurlijke of rechtspersoon die de kwetsbaarheid meldt, voor zover deze persoon hierom verzoekt en de in artikel 23 bedoelde voorwaarden naleeft.

Het nationale CSIRT waarborgt de volledigheid, integriteit, duurzame opslag en geheimhouding van de informatie die via de melding wordt overgemaakt.

De toegang tot deze informatie wordt beperkt tot personen die daartoe door de directeur-generaal van het nationale CSIRT gemachtigd zijn, behalve indien het delen van deze informatie noodzakelijk is voor de uitvoering van de taken opgesomd in dit artikel.

§ 4. Tout en respectant les conditions énumérées à l'article 21, § 1^{er} et 4, le CSIRT national peut observer, étudier ou tester la sécurité d'un réseau et système d'information afin de déterminer l'existence d'une vulnérabilité potentielle ou de vérifier les méthodes utilisées par l'auteur de signalement.

§ 5. Lorsque la vulnérabilité signalée est susceptible d'avoir un impact significatif sur des entités dans plusieurs États membres, le CSIRT national coopère, le cas échéant, avec les autres CSIRT désignés comme coordinateurs au sein du réseau des CSIRT.

§ 6. Le directeur général du CSIRT national veille, par l'adoption de procédures internes, au respect des conditions visées au présent article.

Art. 23. § 1^{er}. Dans le cadre de la procédure visée à l'article 22, les auteurs de signalement ne commettent pas d'infraction aux articles 314*bis*, 458, 550*bis*, 550*ter* du Code pénal et de l'article 145 de la loi du 13 juin 2005 à condition:

1° qu'ils aient agi sans intention frauduleuse, ni dessein de nuire;

2° qu'ils aient adressé une notification simplifiée qui reprend l'identification du système concerné et une description simple de la vulnérabilité potentielle, sans délai et au plus tard dans les 24 heures de la découverte d'une potentielle vulnérabilité, à l'organisation responsable du système et au CSIRT national;

3° qu'ils aient adressé une notification complète, sans délai et au plus tard dans les 72 heures de la découverte d'une potentielle vulnérabilité, à l'organisation responsable du système, le cas échéant dans le respect des modalités de signalement établis par cette organisation, et au CSIRT national, conformément à la procédure prévue à l'article 22, § 2;

4° qu'ils n'aient pas agi au-delà de ce qui était nécessaire et proportionné pour vérifier l'existence d'une vulnérabilité et pour la rapporter;

5° qu'ils n'aient pas publiquement divulgué les informations relatives à la vulnérabilité découverte et aux systèmes vulnérables, sans l'accord du CSIRT national.

6° en ce qui concerne les réseaux et systèmes des organisations visées à l'article 5, § 4 et § 5, et des organes judiciaires ainsi que les informations traitées par eux ou pour leur compte, qu'ils aient, avant la commission de ces actes, conclu un accord écrit avec le service compétent sur les modalités et la méthodologie à utiliser dans le cadre de la recherche de potentielles vulnérabilités.

§ 2. Lorsque des personnes signalent des informations sur une potentielle vulnérabilité dont ils ont eu connaissance dans leur contexte professionnel, elles ne sont pas considérées comme ayant enfreint leur obligation de secret professionnel et n'encourent aucune responsabilité d'aucune sorte concernant

§ 4. Met inachtneming van de voorwaarden opgesomd in artikel 21, § 1 en 4, kan het nationale CSIRT de beveiliging van een netwerk- en informatiesysteem observeren, onderzoeken en testen om te bepalen of er sprake is van een mogelijke kwetsbaarheid of om de door de melder gebruikte methoden na te gaan.

§ 5. Wanneer een gemelde kwetsbaarheid significante gevolgen kan hebben voor entiteiten in meer dan één lidstaat, werkt het nationale CSIRT, in voorkomend geval, samen met andere als coördinator aangewezen CSIRT's binnen het CSIRT-netwerk.

§ 6. De directeur-generaal van het nationale CSIRT zorgt voor de naleving van de in dit artikel vermelde voorwaarden. Daartoe werkt hij interne procedures uit.

Art. 23. § 1. In het kader van de procedure bedoeld in artikel 22 plegen melders geen inbreuk op de artikelen 314*bis*, 458, 550*bis* en 550*ter* van het Strafwetboek en op artikel 145 van de wet van 13 juni 2005, op voorwaarde dat:

1° zij zonder bedrieglijk opzet of het oogmerk om te schaden hebben gehandeld;

2° zij onverwijld en uiterlijk binnen 24 uur na de ontdekking van een mogelijke kwetsbaarheid een vereenvoudigde kennisgeving met de identificatie van het betrokken systeem en een eenvoudige beschrijving van de mogelijke kwetsbaarheid hebben gestuurd naar de organisatie die verantwoordelijk is voor het systeem en naar het nationale CSIRT;

3° zij onverwijld en uiterlijk binnen 72 uur na de ontdekking van een mogelijke kwetsbaarheid een volledige kennisgeving hebben gestuurd naar de organisatie die verantwoordelijk is voor het systeem, in voorkomend geval met inachtneming van de door deze organisatie vastgestelde meldingsmodaliteiten, en naar het nationale CSIRT, overeenkomstig de in artikel 22, § 2, bedoelde procedure;

4° zij niet verder zijn gegaan dan nodig en evenredig was om het bestaan van een kwetsbaarheid na te gaan en die te melden;

5° zij de informatie over de ontdekte kwetsbaarheid en de kwetsbare systemen niet openbaar hebben gemaakt zonder de toestemming van het nationale CSIRT.

6° zij, wat betreft de netwerken en systemen van de in artikel 5, § 4 en § 5, bedoelde organisaties en van de rechterlijke instanties, en de informatie die door hen of namens hen wordt verwerkt, vóór het plegen van die daden een schriftelijke overeenkomst hebben gesloten met de bevoegde dienst over de modaliteiten en de te hanteren methodologie in het kader van het onderzoek naar mogelijke kwetsbaarheden.

§ 2. Personen die informatie melden over een mogelijke kwetsbaarheid waarvan zij in het kader van hun beroep kennis hebben gekregen, worden niet geacht hun beroepsgeheim te hebben geschonden en kunnen op generlei wijze aansprakelijk worden gesteld voor de overdracht van informatie die

la transmission d'informations nécessaires pour signaler une potentielle vulnérabilité au CSIRT national.

§ 3. Toute autre responsabilité éventuelle des auteurs de signalement découlant d'actes ou d'omissions qui ne sont pas nécessaires à l'accomplissement de la procédure visée à l'article 22 et ne respectent pas les conditions du paragraphe 1^{er} continue d'être régie par le droit applicable.

Section 3. Les éventuelles autorités sectorielles

Art. 24. Sans préjudice des autres dispositions, l'autorité sectorielle peut:

1° organiser des exercices sectoriels, les coordonner ou y participer, pour ce qui concerne les mesures visées aux articles 30 et 33;

2° analyser et gérer les conséquences d'un incident pour le secteur;

3° participer aux travaux du groupe de coopération pour ce qui concerne les sujets qui touchent à ses compétences;

4° sensibiliser les entités relevant de son secteur.

CHAPITRE 2 – Coopération au niveau national

Art. 25. § 1^{er}. Les autorités visées au chapitre 1^{er} du présent titre coopèrent les unes avec les autres afin de respecter les obligations énoncées dans la présente loi.

§ 2. En fonction des besoins nécessaires à l'exécution de la présente loi, les autorités visées au paragraphe 1^{er} coopèrent également, au niveau national, avec le NCCN, les services administratifs de l'État, les autorités administratives, en ce compris les [autorités nationales en vertu des règlements (CE) n° 300/2008 et n° 2018/1139], les organes de contrôle au titre du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, la Banque nationale de Belgique, l'Autorité des services et marchés financiers, l'Institut, les autorités compétentes en vertu de la loi CER, les autorités judiciaires, les services de renseignement et de sécurité visés par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, les services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux et avec les Autorités de protection des données.

§ 3. Les entités essentielles et importantes et les autorités visées au chapitre 1^{er} du présent titre collaborent en tout temps, par un échange adéquat d'informations concernant la sécurité des systèmes et réseaux d'informations.

§ 4. Les autorités visées au chapitre 1^{er} du présent titre et les autorités compétentes dans le cadre de la loi [CER/du 1^{er} juillet 2011] coopèrent et échangent régulièrement des

noodzakelijk was om een mogelijke kwetsbaarheid aan het nationale CSIRT te melden.

§ 3. Voor elke andere mogelijke aansprakelijkheid van melders die voortvloeit uit handelingen of nalatigheden die niet noodzakelijk zijn voor de uitvoering van de in artikel 22 bedoelde procedure en die niet voldoen aan de voorwaarden van paragraaf 1, blijft het toepasselijke recht gelden.

Afdeling 3. De eventuele sectorale overheden

Art. 24. Onverminderd de andere bepalingen kan de sectorale overheid:

1° sectorale oefeningen organiseren, coördineren of eraan deelnemen, voor wat betreft de maatregelen bedoeld in artikelen 30 en 33;

2° de gevolgen van een incident voor de sector analyseren en beheren;

3° deelnemen aan de werkzaamheden van de samenwerkingsgroep voor de onderwerpen die betrekking hebben op haar bevoegdheden;

4° de entiteiten die onder haar sector vallen sensibiliseren.

HOOFDSTUK 2 – Samenwerking op nationaal niveau

Art. 25. § 1. De autoriteiten bedoeld in hoofdstuk 1 van deze titel werken samen om de in deze wet vastgestelde verplichtingen na te komen.

§ 2. Naargelang de behoeften die nodig zijn voor de uitvoering van deze wet werken de in paragraaf 1 bedoelde autoriteiten op nationaal niveau ook samen met het NCCN, de administratieve diensten van de Staat, de administratieve overheden, met inbegrip van de [nationale autoriteiten krachtens Verordening (EG) nr. 300/2008 en nr. 2018/1139], de toezichthoudende organen uit hoofde van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, de Nationale Bank van België, de Autoriteit voor Financiële Diensten en Markten, het Instituut, de krachtens de CER-wet bevoegde autoriteiten, de gerechtelijke overheden, de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, en de Gegevensbeschermingsautoriteiten.

§ 3. De essentiële en belangrijke entiteiten en de autoriteiten bedoeld in hoofdstuk 1 van deze titel werken te allen tijde samen door een adequate uitwisseling van informatie over de beveiliging van netwerk- en informatiesystemen.

§ 4. De in hoofdstuk 1 van deze titel bedoelde autoriteiten en de in het kader van de [CER-wet/wet van 1 juli 2011] bevoegde autoriteiten werken samen en wisselen regelmatig

informations sur le recensement des [entités/infrastructures] critiques, les risques, les cybermenaces et les incidents, ainsi que sur les risques, menaces et incidents non cyber qui touchent les entités recensées [en tant qu'entités critiques] en vertu de la loi [CER /du 1^{er} juillet 2011] et sur les mesures prises pour faire face à ces risques, menaces et incidents.

§ 5. Les autorités visées au chapitre 1^{er} du présent titre et les autorités compétentes en vertu du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 et de la loi du 13 juin 2005, échantent régulièrement des informations pertinentes, y compris en ce qui concerne les incidents et les cybermenaces concernés.

§ 6. L'autorité nationale de cybersécurité crée une plateforme de coordination et d'évaluation afin que les autorités visées à l'article 15 et le NCCN échangent de l'information et se coordonnent dans le cadre de l'exécution de la présente loi.

CHAPITRE 3 – Confidentialité et échanges d'information

Art. 26. § 1^{er}. Le présent article ne porte pas préjudice à l'application de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé, de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, de la loi du 11 avril 1994 relative à la publicité de l'administration ou d'autres dispositions légales garantissant la confidentialité des informations liées aux intérêts essentiels de la sécurité publique nationale.

§ 2. Toute personne qui est appelée à prêter son concours professionnel à l'évaluation de la conformité ou à la supervision est tenue au secret. Celui qui viole ce secret est puni des peines prévues à l'article 458 du Code pénal.

Les personnes dépositaires, par état ou par profession, des secrets qu'on leur confie sont autorisées à faire connaître ces secrets pour l'exécution de la présente loi.

Ces personnes obtiennent l'accord des autorités visées à l'article 5, § 4, lorsque ces autorités sont concernées par le secret.

§ 3. Les autorités visées au chapitre 1^{er} du présent titre, les entités essentielles ou importantes, ou leurs sous-traitants,

informatie uit inzake het als kritiek aanmerken van [entiteiten/infrastructuren], over risico's, cyberdreigingen en incidenten, alsook over niet-cyberrisico's, -dreigingen en -incidenten die gevolgen hebben voor entiteiten die uit hoofde van de [CER-wet/wet van 1 juli 2011] [als kritieke entiteiten] zijn aangemerkt, en over de maatregelen die in reactie op dergelijke risico's, dreigingen en incidenten zijn genomen.

§ 5. De in hoofdstuk 1 van deze titel bedoelde autoriteiten en de autoriteiten die bevoegd zijn krachtens Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 en de wet van 13 juni 2005, wisselen regelmatig relevante informatie uit, onder meer met betrekking tot relevante incidenten en cyberdreigingen.

§ 6. De nationale cyberbeveiligingsautoriteit richt een coördinatie- en evaluatieplatform opdat de in artikel 15 bedoelde autoriteiten en het NCCN toelaat informatie uit te wisselen en hun optreden in het kader van de uitvoering van deze wet op elkaar af te stemmen.

HOOFDSTUK 3 – Vertrouwelijkheid en informatie-uitwisseling

Art. 26. § 1. Dit artikel doet geen afbreuk aan de toepassing van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst, de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, de wet van 11 april 1994 betreffende de openbaarheid van bestuur of andere wettelijke bepalingen die de vertrouwelijkheid van informatie met betrekking tot de wezenlijke belangen van de nationale openbare veiligheid waarborgen.

§ 2. Eenieder die beroepshalve zijn medewerking dient te verlenen aan de conformiteitsbeoordeling of het toezicht is tot geheimhouding verplicht. Diegene die dit geheim schendt, wordt gestraft met de straffen bepaald in artikel 458 van het Strafwetboek.

Personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd, mogen deze geheimen bekendmaken voor de uitvoering van deze wet.

Deze personen verkrijgen de akkoord van de autoriteiten bedoeld in artikel 5, § 4, wanneer deze autoriteiten bij het geheim betrokken zijn.

§ 3. De autoriteiten bedoeld in hoofdstuk 1 van deze titel en de essentiële of belangrijke entiteiten, of hun onderaannemers,

limitent l'accès aux informations dans le cadre de la présente loi aux personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec l'exécution de la présente loi.

§ 4. Les informations fournies aux autorités visées au chapitre 1^{er} du présent titre par les entités essentielles ou importantes, peuvent être échangées avec des autorités de l'Union européenne, avec des autorités belges ou étrangères, lorsque cet échange est nécessaire à l'application de dispositions légales.

Les informations échangées se limitent à ce qui est pertinent et sont proportionnées à l'objectif de cet échange, notamment dans le respect du règlement (UE) 2016/679. Cet échange d'informations préserve la confidentialité des informations concernées et protège la sécurité et les intérêts commerciaux des entités essentielles ou importantes.

Art. 27. § 1^{er}. A titre volontaire, les entités relevant du champ d'application de la présente loi et, le cas échéant, les autres entités concernées ne relevant pas du champ d'application de la présente loi peuvent échanger, entre elles, au sein de communautés, des informations pertinentes en matière de cybersécurité, y compris des informations relatives aux cybermenaces, aux incidents évités, aux vulnérabilités, aux techniques et procédures, aux indicateurs de compromission, aux tactiques adverses, ainsi que des informations spécifiques sur les acteurs de la menace, des alertes de cybersécurité et des recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberattaques, lorsque ce partage d'informations:

1° vise à prévenir et à détecter les incidents, à y réagir, à s'en rétablir ou à atténuer leur impact;

2° renforce le niveau de cybersécurité, notamment en sensibilisant aux cybermenaces, en limitant ou en empêchant leur capacité de se propager, en soutenant une série de capacités de défense, en remédiant aux vulnérabilités et en les révélant, en mettant en œuvre des techniques de détection, d'endiguement et de prévention des menaces, des stratégies d'atténuation ou des étapes de réaction et de rétablissement, ou en encourageant la recherche collaborative en matière de cybermenaces entre les entités publiques et privées.

§ 2. L'échange d'informations visé au paragraphe 1^{er} est mis en œuvre au moyen d'accords de partage d'informations en matière de cybersécurité, compte tenu de la nature potentiellement sensible des informations partagées.

§ 3. L'autorité nationale de cybersécurité facilite la mise en place des accords de partage d'informations en matière de cybersécurité visés au paragraphe 2. Ces accords peuvent préciser les éléments opérationnels, y compris l'utilisation de plateformes TIC spécialisées et d'outils d'automatisation, le contenu et les conditions des accords de partage d'informations.

beperken de toegang tot de informatie in het kader van deze wet tot de personen die ervan op de hoogte moeten zijn en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met de uitvoering van deze wet.

§ 4. De informatie die door essentiële of belangrijke entiteiten aan de autoriteiten bedoeld in hoofdstuk 1 van deze titel wordt bezorgd, mag worden uitgewisseld met autoriteiten van de Europese Unie, Belgische of buitenlandse autoriteiten, wanneer die uitwisseling noodzakelijk is voor de toepassing van wettelijke bepalingen.

De uitgewisselde informatie wordt beperkt tot hetgeen relevant is voor en evenredig is met het doel van die uitwisseling, met name overeenkomstig Verordening (EU) 2016/679. Bij die uitwisseling van informatie wordt de vertrouwelijkheid van de informatie gewaarborgd en worden de beveiligings- en commerciële belangen van essentiële of belangrijke entiteiten beschermd.

Art. 27. § 1. Binnen het toepassingsgebied van deze wet vallende entiteiten en, indien van toepassing, andere entiteiten die niet binnen het toepassingsgebied van deze wet vallen, kunnen op vrijwillige basis onderling, binnen gemeenschappen, relevante informatie over cyberbeveiliging uitwisselen, met inbegrip van informatie over cyberdreigingen, bijna-incidenten, kwetsbaarheden, technieken en procedures, indicatoren voor aantasting, vijandige tactieken, dreigingsactorspecifieke informatie, cyberbeveiligingswaarschuwingen en aanbevelingen betreffende de configuratie van cyberbeveiligingsinstrumenten om cyberaanvallen te detecteren, wanneer dat uitwisselen van informatie:

1° beoogt incidenten te voorkomen, te detecteren, erop te reageren of ervan te herstellen of de gevolgen ervan te beperken;

2° het niveau van de cyberbeveiliging verhoogt, met name door de bewustwording met betrekking tot cyberdreigingen te vergroten, het vermogen van dergelijke dreigingen om zich te verspreiden te beperken of te belemmeren, een reeks verdedigingscapaciteiten, het herstel en openbaarmaking van kwetsbaarheden, het opsporen van dreigingen, beheersings- en preventietechnieken, beperkingsstrategieën of respons- en herstelfasen te ondersteunen of gezamenlijk onderzoek naar cyberdreigingen door publieke en particuliere entiteiten te bevorderen.

§ 2. De informatie-uitwisseling bedoeld in paragraaf 1 wordt uitgevoerd door middel van informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging met betrekking tot de potentieel gevoelige aard van de uitgewisselde informatie.

§ 3. De nationale cyberbeveiligingsautoriteit faciliteert de vaststelling van de in paragraaf 2 bedoelde informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging. In dergelijke regelingen kunnen de operationele elementen, met inbegrip van het gebruik van specifieke ICT-platforms en automatiseringshulpmiddelen, de inhoud en de voorwaarden

L'autorité nationale de cybersécurité et les éventuelles autorités sectorielles peuvent imposer des conditions d'utilisation des informations qu'elles mettent à disposition des communautés visées au paragraphe 1^{er}.

§ 4. Les entités essentielles et importantes notifient à l'autorité nationale de cybersécurité leur participation aux accords de partage d'informations en matière de cybersécurité visés au paragraphe 2, lorsqu'elles concluent de tels accords ou, le cas échéant, lorsqu'elles se retirent de ces accords, une fois que le retrait prend effet.

CHAPITRE 4 – Stratégie nationale en matière de cybersécurité

Art. 28. § 1^{er}. Les ministres réunis en Conseil adoptent la stratégie nationale en matière de cybersécurité et la mettent à jour au moins tous les 5 ans, sur la base d'indicateurs de performance, après avis du Conseil national de sécurité, des autorités visées à l'article 15, du NCCN et, le cas échéant, des autorités de contrôle des données à caractère personnel.

Cette stratégie définit les objectifs stratégiques, les ressources nécessaires pour atteindre ces objectifs, ainsi que les mesures politiques et réglementaires appropriées, en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir.

§ 2. La stratégie nationale en matière de cybersécurité comprend, entre autres:

1° les objectifs et les priorités de la stratégie nationale en matière de cybersécurité, couvrant en particulier les secteurs visés aux annexes I et II;

2° un cadre de gouvernance visant à atteindre les objectifs et les priorités visés au 1°, y compris les tâches et les responsabilités des autorités publiques et des autres acteurs concernés ainsi que les politiques visées au paragraphe 3;

3° un cadre de gouvernance précisant les rôles et les responsabilités des parties prenantes en Belgique, et sur lequel reposent la coopération et la coordination, en Belgique, entre les autorités visées au chapitre 1^{er} du présent titre ainsi que la coopération et la coordination entre ces autorités et les autorités compétentes en vertu d'instruments juridiques sectoriels de l'Union européenne;

4° un mécanisme visant à identifier les actifs pertinents et une évaluation des risques en Belgique;

5° un inventaire des mesures garantissant la préparation, la réaction et la récupération des services après incident, y compris la coopération entre les secteurs public et privé;

6° une liste des différents acteurs et autorités concernés par la mise en œuvre de la stratégie nationale en matière de cybersécurité;

van de informatie-uitwisselingsregelingen worden gespecificeerd. De nationale cyberbeveiligingsautoriteit en de eventuele sectorale overheden kunnen voorwaarden opleggen aan het gebruik van de informatie die zij ter beschikking stellen van de gemeenschappen bedoeld in paragraaf 1.

§ 4. De essentiële en belangrijke entiteiten stellen de nationale cyberbeveiligingsautoriteit in kennis van hun deelname aan de in paragraaf 2 bedoelde informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging wanneer zij dergelijke regelingen aangaan, of, indien van toepassing, van hun terugtrekking uit dergelijke regelingen, zodra de terugtrekking van kracht wordt.

HOOFDSTUK 4 – Nationale cyberbeveiligingsstrategie

Art. 28. § 1. De in Raad vergaderde ministers keuren de nationale cyberbeveiligingsstrategie goed en werken deze minstens om de 5 jaar bij op basis van prestatie-indicatoren, na advies van de Nationale Veiligheidsraad, de in artikel 15 bedoelde autoriteiten, het NCCN en, in voorkomend geval, de toezichhoudende autoriteiten persoonsgegevens.

Deze strategie bepaalt de strategische doelstellingen, de middelen die nodig zijn om die doelstellingen te behalen, en passende beleids- en regelgevingsmaatregelen, om een hoog niveau van cyberbeveiliging te bereiken en te handhaven.

§ 2. De nationale cyberbeveiligingsstrategie omvat onder meer:

1° de doelstellingen en prioriteiten van de nationale cyberbeveiligingsstrategie, met name inzake de in de bijlagen I en II bedoelde sectoren;

2° een governancekader om de in punt 1° bedoelde doelstellingen en prioriteiten te verwezenlijken, met inbegrip van de taken en verantwoordelijkheden van de overheid en de andere belanghebbenden alsook van het in paragraaf 3 bedoelde beleid;

3° een governancekader dat de taken en verantwoordelijkheden van de belanghebbenden in België verduidelijkt, ter onderbouwing van de samenwerking en coördinatie, in België, tussen de autoriteiten bedoeld in hoofdstuk 1 van deze titel, alsook van de samenwerking en coördinatie tussen die autoriteiten en uit hoofde van sectorspecifieke rechtsinstrumenten van de Europese Unie bevoegde autoriteiten;

4° een mechanisme om relevante activa vast te stellen en een beoordeling van de risico's in België;

5° een inventarisatie van de maatregelen om te zorgen voor paraatheid, respons en herstel bij incidenten, met inbegrip van samenwerking tussen de publieke en de particuliere sector;

6° een lijst van de verschillende belanghebbenden en autoriteiten die betrokken zijn bij de uitvoering van de nationale cyberbeveiligingsstrategie;

7° un cadre politique visant une coordination renforcée entre les autorités visées au chapitre 1^{er} du présent titre et les autorités compétentes en vertu de la loi **[CER/du 1^{er} juillet 2011]** aux fins du partage d'informations relatives aux risques, aux menaces et aux incidents dans les domaines cyber et non cyber et de l'exercice des tâches de supervision, le cas échéant;

8° un plan comprenant les mesures nécessaires en vue d'améliorer le niveau général de sensibilisation des citoyens à la cybersécurité;

9° un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de cybersécurité;

10° un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de cybersécurité.

§ 3. Des politiques, parties intégrantes de la stratégie nationale en matière de cybersécurité, sont adoptées et portent sur les éléments suivants:

1° la cybersécurité dans le cadre de la chaîne d'approvisionnement des produits et services TIC utilisés par des entités pour la fourniture de leurs services;

2° l'inclusion et la spécification d'exigences liées à la cybersécurité pour les produits et services TIC dans les marchés publics, y compris concernant la certification de cybersécurité, le chiffrage et l'utilisation de produits de cybersécurité en sources ouvertes;

3° la gestion des vulnérabilités, y compris la promotion et la facilitation de la divulgation coordonnée des vulnérabilités conformément à l'article 22;

4° le maintien de la disponibilité générale, de l'intégrité et de la confidentialité du noyau public de l'internet ouvert, y compris, le cas échéant, la cybersécurité des câbles de communication sous-marins;

5° la promotion du développement et de l'intégration de technologies avancées pertinentes visant à mettre en œuvre des mesures de pointe dans la gestion des risques en matière de cybersécurité;

6° la promotion et le développement de l'éducation et de la formation en matière de cybersécurité, des compétences en matière de cybersécurité, des initiatives de sensibilisation et de recherche et de développement en matière de cybersécurité, ainsi que des orientations sur les bonnes pratiques de cyberhygiène et les contrôles, à l'intention des citoyens, des parties prenantes et des entités;

7° le soutien aux institutions universitaires et de recherche visant à développer, améliorer et promouvoir le déploiement des outils de cybersécurité et à sécuriser les infrastructures de réseau;

7° een beleidskader voor versterkte coördinatie tussen de autoriteiten bedoeld in hoofdstuk 1 van deze titel en de uit hoofde van de **[CER-wet/wet van 10 juli 2011]** bevoegde autoriteiten, met als doel het delen van informatie over risico's, cyberdreigingen en incidenten, alsook over niet-cyberrisico's, -dreigingen en -incidenten, en in voorkomend geval de uitvoering van toezichhoudende taken;

8° een plan, met inbegrip van de noodzakelijke maatregelen, om het algemene niveau van cyberbeveiligingsbewustzijn bij de burgers te verbeteren;

9° een overzicht van de onderwijs-, bewustmakings- en opleidingsprogramma's met betrekking tot de nationale cyberbeveiligingsstrategie;

10° een overzicht van de plannen voor onderzoek en ontwikkeling met betrekking tot de nationale cyberbeveiligingsstrategie.

§ 3. Er worden beleidsmaatregelen genomen die integraal deel uitmaken van de nationale cyberbeveiligingsstrategie:

1° inzake cyberbeveiliging in de toeleveringsketen voor ICT-producten en ICT-diensten die door entiteiten worden gebruikt voor het verlenen van hun diensten;

2° inzake het opnemen en specificeren van cyberbeveiligingsgerelateerde eisen voor ICT-producten en ICT-diensten bij overheidsopdrachten, onder meer met betrekking tot cyberbeveiligingscertificering, versleuteling en het gebruik van open-source-cyberbeveiligingsproducten;

3° voor het beheer van kwetsbaarheden, met inbegrip van de bevordering en vergemakkelijking van de gecoördineerde bekendmaking van kwetsbaarheden overeenkomstig artikel 22;

4° inzake het in stand houden van de algemene beschikbaarheid, integriteit en vertrouwelijkheid van de openbare kern van het open internet, in voorkomend geval met inbegrip van de cyberbeveiliging van onderzeese communicatiekabels;

5° voor het bevorderen van de ontwikkeling en integratie van relevante geavanceerde technologieën met het oog op de toepassing van geavanceerde risicobeheersmaatregelen op het gebied van cyberbeveiliging;

6° voor het bevorderen en ontwikkelen van onderwijs en opleiding op het gebied van cyberbeveiliging, cyberbeveiligingsvaardigheden, bewustmakings- en onderzoeks- en ontwikkelingsinitiatieven rond cyberbeveiliging, alsook van richtsnoeren voor goede praktijken en controles op het gebied van cyberhygiène, gericht op burgers, belanghebbenden en entiteiten;

7° voor het ondersteunen van academische en onderzoeksinstellingen bij de ontwikkeling, versterking en bevordering van de uitrol van instrumenten voor cyberbeveiliging en een veilige netwerkinfrastructuur;

8° la mise en place de procédures pertinentes et d'outils de partage d'informations appropriés visant à soutenir le partage volontaire d'informations sur la cybersécurité entre les entités;

9° le renforcement des valeurs de cyberrésilience et de cyberhygiène des petites et moyennes entreprises, en particulier celles qui sont exclues du champ d'application de la présente loi, en fournissant des orientations et un soutien facilement accessibles pour répondre à leurs besoins spécifiques;

10° la promotion d'une cyberprotection active.

CHAPITRE 5 – Le plan national de réaction aux crises et incidents de cybersécurité majeurs

Art. 29. § 1^{er}. Le Roi établit, par arrêté délibéré en Conseil des ministres, un plan national de réaction aux crises et incidents de cybersécurité. Ce plan constitue un plan national [au sens de l'article 21 de la loi NPU].

§ 2. Sans préjudice des éléments devant être contenus dans les plans nationaux [conformément à la loi NPU], le plan national de réaction aux crises et incidents de cybersécurité contient au moins les éléments suivants:

1° les objectifs des mesures et activités nationales de préparation;

2° les tâches et responsabilités des autorités de gestion des crises cyber;

3° les procédures de gestion des crises cyber, y compris leur intégration dans le cadre national général de gestion des crises et les canaux d'échange d'informations;

4° les mesures de préparation nationales, y compris des exercices et des activités de formation;

5° les parties prenantes et les infrastructures des secteurs public et privé concernées;

6° les procédures et arrangements nationaux entre les autorités et les organismes nationaux compétents visant à garantir la participation et le soutien effectifs de la Belgique à la gestion coordonnée des crises et incidents de cybersécurité majeurs au niveau de l'Union européenne.

Titre 3. – Mesures de gestion des risques en matière de cybersécurité et obligations d'information

CHAPITRE 1 – Mesures de gestion des risques en matière de cybersécurité

Art. 30. § 1^{er} Les entités essentielles et importantes prennent les mesures appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour

8° met inbegrip van relevante procedures en passende instrumenten voor het delen van informatie, ter ondersteuning van het vrijwillige delen van cyberbeveiligingsinformatie tussen entiteiten;

9° voor het versterken van de digitale weerbaarheid en het basisniveau van cyberhygiëne van kleine en middelgrote ondernemingen, met name die welke van het toepassingsgebied van deze wet zijn uitgesloten, door te voorzien in gemakkelijk toegankelijke richtsnoeren en bijstand voor hun specifieke behoeften;

10° voor het bevorderen van actieve cyberbescherming.

HOOFDSTUK 5 – Het nationale plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons

Art. 29. § 1. De Koning stelt, bij besluit vastgesteld na overleg in de Ministerraad, een nationaal plan voor cyberbeveiligingsincidenten en crisisrespons op. Dit plan is een nationaal plan [als bedoeld in artikel 21 van de NPU-wet].

§ 2. Onverminderd de elementen die moeten worden opgenomen in de nationale plannen [overeenkomstig de NPU-wet], bevat het nationale plan voor cyberbeveiligingsincidenten en crisisrespons ten minste:

1° de doelstellingen van de nationale paraatheidsmaatregelen en -activiteiten;

2° de taken en verantwoordelijkheden van de cybercrisisbeheerautoriteiten;

3° de cybercrisisbeheerprocedures, met inbegrip van de integratie ervan in het algemene nationale crisisbeheerkader en in de informatie-uitwisselingskanalen;

4° de nationale paraatheidsmaatregelen, met inbegrip van oefeningen en opleidingsactiviteiten;

5° de relevante publieke en particuliere belanghebbenden en betrokken infrastructuur;

6° de nationale procedures en regelingen tussen de betrokken nationale autoriteiten en instanties om de effectieve deelname van België aan het gecoördineerde beheer van grootschalige cyberbeveiligingscrises en -incidenten op het niveau van de Europese Unie en de ondersteuning daarvan te waarborgen.

Titel 3. - Maatregelen voor het beheer van cyberbeveiligingsrisico's en rapportageverplichtingen

HOOFDSTUK 1 – Maatregelen voor het beheer van cyberbeveiligingsrisico's

Art. 30. § 1. De essentiële en belangrijke entiteiten nemen passende en evenredige maatregelen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die zij voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de

éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services.

§ 2. Les mesures visées au paragraphe 1^{er} garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, en tenant compte de l'état des connaissances et, s'il y a lieu, des normes européennes et internationales applicables, ainsi que du coût de mise en œuvre. Lors de l'évaluation de la proportionnalité de ces mesures, il convient de tenir dûment compte du degré d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales et économiques.

§ 3. Les mesures visées au paragraphe 1^{er} sont fondées sur une approche "tous risques" qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents, et elles portent au moins sur:

1° les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information;

2° la gestion des incidents;

3° la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises;

4° la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs;

5° la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités;

6° des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité;

7° les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité;

8° des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement;

9° la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs;

10° l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins;

11° une politique de divulgation coordonnée des vulnérabilités.

gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken.

§ 2. Rekening houdend met de stand van de techniek en, indien van toepassing, de desbetreffende Europese en internationale normen, alsook met de uitvoeringskosten, zorgen de in paragraaf 1 bedoelde maatregelen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen. Bij de beoordeling van de evenredigheid van die maatregelen wordt naar behoren rekening gehouden met de mate waarin de entiteit aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen.

§ 3. De in paragraaf 1 bedoelde maatregelen zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen, en hebben ten minste betrekking op het volgende:

1° beleid inzake risicoanalyse en beveiliging van informatiesystemen;

2° incidentenbehandeling;

3° bedrijfscontinuïteit, zoals back-upbeheer, noodvoorzieningenplannen en crisisbeheer;

4° de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;

5° beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;

6° beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;

7° basispraktijken op het gebied van cyberhygiène en opleiding op het gebied van cyberbeveiliging;

8° beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;

9° beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;

10° wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit;

11° een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden.

§ 4. Lorsque les entités essentielles et importantes examinent lesquelles des mesures visées au paragraphe 3, 4°, sont appropriées, elles tiennent compte des vulnérabilités propres à chaque fournisseur et prestataire de services direct et de la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et prestataires de services, y compris de leurs procédures de développement sécurisé.

Ces mesures doivent être appropriées au regard des résultats des évaluations coordonnées au niveau de l'Union européenne des risques pour la sécurité des chaînes d'approvisionnement critiques.

§ 5. Chaque entité essentielle et importante effectue une analyse des risques fondée sur une approche "tous risques" qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents et élabore, sur la base de cette analyse, une P.S.I. reprenant au moins les aspects visés au paragraphe 3.

§ 6. Lorsqu'une entité essentielle ou importante constate qu'elle ne se conforme pas aux mesures prévues au paragraphe 3, elle prend, sans retard injustifié, toutes les mesures correctives nécessaires appropriées et proportionnées.

Art. 31. § 1^{er}. Les organes de direction des entités essentielles et importantes approuvent les mesures de gestion des risques en matière de cybersécurité que ces entités prennent afin de se conformer à l'article 30, supervisent leur mise en œuvre et sont responsables de la violation dudit article par ces entités.

Cet article est sans préjudice des règles en matière de responsabilité applicables aux institutions publiques, ainsi que de responsabilité des agents de la fonction publique et des responsables élus ou nommés.

§ 2. Les membres des organes de direction des entités essentielles et importantes suivent une formation pour que leurs connaissances et compétences soient suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité.

Art. 32. L'entité essentielle ou importante est responsable de l'analyse des risques effectuée ainsi que du choix et de la mise en œuvre des mesures visées à l'article 30, § 1^{er}.

Art. 33. Après consultation de l'autorité nationale de cybersécurité, de l'éventuelle autorité sectorielle concernée et des entités fédérées concernées, le Roi peut, par arrêté délibéré en Conseil des ministres, imposer des mesures supplémentaires de gestion des risques en matière de cybersécurité appropriées et proportionnées.

CHAPITRE 2 – Notification d'incidents

Section 1^{re}. Notification obligatoire

Art. 34. § 1^{er}. Les entités essentielles et importantes notifient tout incident significatif sans retard injustifié au CSIRT

§ 4. Wanneer essentiële en belangrijke entiteiten nagaan welke maatregelen als bedoeld in paragraaf 3, 4°, passend zijn, houden zij rekening met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures.

Deze maatregelen moeten passend zijn in het licht van de resultaten van de op het niveau van de Europese Unie gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens.

§ 5. Iedere essentiële en belangrijke entiteit voert een risicoanalyse uit gebaseerd op een benadering die alle gevaren omvat en tot doel heeft de netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen en werkt, op basis daarvan, een I.B.B. uit dat minstens de in paragraaf 3 bedoelde aspecten bevat.

§ 6. Een essentiële of belangrijke entiteit die vaststelt dat zij niet voldoet aan de in paragraaf 3 bedoelde maatregelen, neemt onverwijld alle noodzakelijke, passende en evenredige corrigerende maatregelen.

Art. 31. § 1. De bestuursorganen van essentiële en belangrijke entiteiten keuren de maatregelen voor het beheer van cyberbeveiligingsrisico's goed die deze entiteiten nemen om te voldoen aan artikel 30, zien toe op de uitvoering ervan en zijn aansprakelijk voor inbreuken door deze entiteiten op dat artikel.

Dit artikel doet geen afbreuk aan de aansprakelijkheidsregels die gelden voor overheidsinstanties, alsook voor ambtenaren en verkozen of benoemde mandatarissen.

§ 2. De leden van de bestuursorganen van essentiële en belangrijke entiteiten volgen een opleiding zodat ze over voldoende kennis en vaardigheden beschikken om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.

Art. 32. De essentiële of belangrijke entiteit is verantwoordelijk voor de uitgevoerde risicoanalyse, alsook voor de keuze en uitvoering van de maatregelen bedoeld in artikel 30, § 1.

Art. 33. Na raadpleging van de nationale cyberbeveiligingsautoriteit en van de eventuele betrokken sectorale overheid en deelgebieden kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, passende en evenredige bijkomende maatregelen voor het beheer van cyberbeveiligingsrisico's opleggen.

HOOFDSTUK 2 – Melding van incidenten

Afdeling 1. Verplichte melding

Art. 34. § 1. De essentiële en belangrijke entiteiten melden elk significant incident onverwijld aan het nationale CSIRT,

national, selon les modalités établies dans un protocole conclu entre lui et le NCCN. Ces entités signalent, entre autres, toute information permettant au CSIRT national de déterminer si l'incident a un impact transfrontière.

Le cas échéant, les entités concernées notifient, sans retard injustifié, aux destinataires de leurs services les incidents significatifs susceptibles de nuire à la fourniture des services relatifs aux secteurs ou sous-secteurs repris à l'annexe I et II.

Le CSIRT national communique immédiatement les notifications visées à l'alinéa 1^{er} aux éventuelles autorités sectorielles compétentes. Les notifications des entités essentielles sont également transmises au NCCN.

§ 2. Le cas échéant, les entités concernées communiquent, sans retard injustifié, aux destinataires de leurs services qui sont potentiellement affectés par une cybermenace importante toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace. Le cas échéant, les entités informent également ces destinataires de la cybermenace importante elle-même.

§ 3. Après consultation de l'autorité nationale de cyber-sécurité, des autorités sectorielles, le NCCN et des entités fédérées, le Roi peut déterminer, par arrêté délibéré en Conseil des ministres, des seuils précis de notification en fonction du degré d'impact ou d'urgence de l'incident.

§ 4. Le cas échéant, la notification se fait conformément aux actes d'exécution de la Commission européenne, dont celui du [xxx portant modalités d'application de la directive (UE) 2022/2255 du Parlement européen et du Conseil précisant les éléments à prendre en considération par certaines entités pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif].

§ 5. Le simple fait de notifier un incident n'accroît pas la responsabilité de l'entité qui est à l'origine de la notification.

Art 35. § 1^{er}. Aux fins de la notification visée à l'article 34, § 1^{er}, alinéa 1^{er}, les entités concernées soumettent CSIRT national:

1° sans retard injustifié et en tout état de cause dans les vingt-quatre heures après avoir eu connaissance de l'incident significatif, une alerte précoce qui, le cas échéant, indique si l'on suspecte que l'incident significatif a été causé par des actes illicites ou malveillants ou s'il pourrait avoir un impact transfrontière;

2° sans retard injustifié et en tout état de cause dans les 72 heures après avoir eu connaissance de l'incident significatif, une notification d'incident qui, le cas échéant, met à jour les informations visées au 1° et fournit une évaluation initiale de

volgens de modaliteiten bepaald in een protocol gesloten tussen het nationale CSIRT en het NCCN. Deze entiteiten rapporteren onder meer alle informatie die het nationale CSIRT in staat stelt om eventuele grensoverschrijdende gevolgen van het incident te bepalen.

In voorkomend geval stellen de betrokken entiteiten de ontvangers van hun diensten onverwijld in kennis van significante incidenten die een nadelige invloed kunnen hebben op de verlening van de diensten betreffende de sectoren of deelsectoren van bijlage I en II.

Het nationale CSIRT bezorgt de in het eerste lid bedoelde meldingen onmiddellijk aan de eventuele bevoegde sectorale overheden. Meldingen van essentiële entiteiten worden ook doorgestuurd naar het NCCN.

§ 2. Indien van toepassing delen de betrokken entiteiten de ontvangers van hun diensten die mogelijk wordt getroffen door een significante cyberdreiging worden getroffen, onverwijld mee welke maatregelen die ontvangers kunnen nemen in reactie op die dreiging. Indien nodig stellen de entiteiten die ontvangers ook in kennis van de significante cyberdreiging zelf.

§ 3. Na raadpleging van de nationale cyberbeveiligingsautoriteit, de sectorale overheden, het NCCN en de deelgebieden kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, precieze meldingsdrempels bepalen naargelang de impact of dringendheid van het incident.

§ 4. In voorkomend geval gebeurt de melding overeenkomstig de uitvoeringshandelingen van de Europese Commissie, waaronder die van [xxx tot vaststelling van toepassingsbepalingen voor Richtlijn (EU) 2022/2255 van het Europees Parlement en de Raad wat betreft de nadere specificatie van de door bepaalde entiteiten in aanmerking te nemen elementen voor het beheer van de risico's in verband met de beveiliging van netwerk- en informatiesystemen en van de parameters om te bepalen of een incident aanzienlijke gevolgen heeft].

§ 5. Een melding leidt niet tot blootstelling van de entiteit aan een verhoogde aansprakelijkheid.

Art. 35. § 1. Voor de in artikel 34, § 1, eerste lid, bedoelde melding bezorgen de betrokken entiteiten het nationale CSIRT:

1° onverwijld en in elk geval binnen vierentwintig uur nadat zij kennis hebben gekregen van het significante incident, een vroegtijdige waarschuwing waarin, indien van toepassing, wordt aangegeven of het significante incident vermoedelijk door een onrechtmatige of kwaadwillige handeling is veroorzaakt, dan wel grensoverschrijdende gevolgen zou kunnen hebben;

2° onverwijld en in elk geval binnen 72 uur nadat zij kennis hebben gekregen van het significante incident, een incidentmelding met, indien van toepassing, een update van de in 1° bedoelde informatie, een initiële beoordeling van het significante

l'incident significatif, y compris de sa gravité et de son impact, ainsi que des indicateurs de compromission, lorsqu'ils sont disponibles;

3° à la demande du CSIRT national ou de l'éventuelle autorité sectorielle concernée, un rapport intermédiaire sur les mises à jour pertinentes de la situation;

4° un rapport final au plus tard un mois après la présentation de la notification d'incident visée au 2°, comprenant les éléments suivants:

- a) une description détaillée de l'incident, y compris de sa gravité et de son impact;
- b) le type de menace ou la cause profonde qui a probablement déclenché l'incident;
- c) les mesures d'atténuation appliquées et en cours;
- d) le cas échéant, l'impact transfrontière de l'incident;

5° en cas d'incident en cours au moment de la présentation du rapport final visé au 4°, les entités concernées fournissent à ce moment-là un rapport d'avancement puis un rapport final dans un délai d'un mois à compter du traitement définitif de l'incident.

§ 2. Par dérogation au paragraphe 1^{er}, 2°, un prestataire de services de confiance notifie au CSIRT national les incidents significatifs qui ont un impact sur la fourniture de ses services de confiance, sans retard injustifié et en tout état de cause dans les vingt-quatre heures après avoir eu connaissance de l'incident significatif.

§ 3. Le CSIRT national communique, immédiatement, les notifications visées aux paragraphes 1^{er} et 2 aux éventuelles autorités sectorielles compétentes. Les notifications des entités essentielles sont également transmises au NCCN.

Art. 36. § 1^{er} Le CSIRT national fournit, sans retard injustifié et si possible dans les vingt-quatre heures suivant la réception de l'alerte précoce visée à l'article 35, § 1^{er}, 1°, une réponse à l'entité émettrice de la notification, y compris un retour d'information initial sur l'incident significatif et, à la demande de l'entité, des orientations ou des conseils opérationnels sur la mise en œuvre d'éventuelles mesures d'atténuation.

§ 2. Le CSIRT national fournit un soutien technique supplémentaire si l'entité concernée le demande. Lorsqu'il y a lieu de suspecter que l'incident est de nature criminelle, le CSIRT national fournit également des orientations sur les modalités de notification de l'incident significatif aux autorités répressives.

Art. 37. § 1^{er}. Lorsque c'est approprié, et notamment si l'incident significatif concerne deux États membres ou plus, le CSIRT national informe sans retard injustifié les autres États membres touchés et l'ENISA de l'incident significatif. Sont alors partagées des informations du type de celles reçues

incident, met inbegrip van de ernst en de gevolgen ervan en, indien beschikbaar, de indicatoren voor aantasting;

3° op verzoek van het nationale CSIRT of van de eventuele betrokken sectorale overheid, een tussentijds verslag over relevante updates van de situatie;

4° uiterlijk één maand na de indiening van de in 2° bedoelde incidentmelding, een eindverslag waarin het volgende is opgenomen:

- a) een gedetailleerde beschrijving van het incident, met inbegrip van de ernst en de gevolgen ervan;
- b) het soort bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid;
- c) toegepaste en lopende risicobeperkende maatregelen;
- d) in voorkomend geval, de grensoverschrijdende gevolgen van het incident;

5° indien het incident nog aan de gang is op het moment dat het in 4° bedoelde eindverslag moet worden ingediend, dienen de betrokken entiteiten op dat moment een voortgangsverslag in, en binnen één maand nadat zij het incident definitief hebben afgehandeld, een eindverslag.

§ 2. In afwijking van paragraaf 1, 2°, meldt een verlener van vertrouwensdiensten significante incidenten die gevolgen hebben voor de verlening van zijn vertrouwensdiensten onverwijld, en in elk geval binnen vierentwintig uur nadat hij er kennis van heeft gekregen, aan het nationale CSIRT.

§ 3. Het nationale CSIRT bezorgt de in paragrafen 1 en 2 bedoelde meldingen onmiddellijk aan de eventuele bevoegde sectorale overheden. Meldingen van essentiële entiteiten worden ook doorgestuurd naar het NCCN.

Art. 36. § 1. Het nationale CSIRT verstrekt onverwijld en zo mogelijk binnen vierentwintig uur na ontvangst van de in artikel 35, § 1, bedoelde vroegtijdige waarschuwing een antwoord aan de meldende entiteit, met inbegrip van een eerste feedback over het significante incident en, op verzoek van de entiteit, richtsnoeren of operationeel advies voor de uitvoering van mogelijke risicobeperkende maatregelen.

§ 2. Het nationale CSIRT verleent aanvullende technische ondersteuning indien de betrokken entiteit daarom verzoekt. Wanneer wordt vermoed dat het significante incident van criminele aard is, geeft het nationale CSIRT ook richtsnoeren voor het melden van het significante incident aan de rechtshandavingsinstanties.

Art. 37. § 1. In voorkomend geval, en met name wanneer het significante incident betrekking heeft op twee of meer lidstaten, stelt het nationale CSIRT de andere getroffen lidstaten en Enisa onverwijld in kennis van het significante incident. Die informatie omvat het soort informatie dat overeenkomstig

conformément à l'article 35. Ce faisant, le CSIRT national doit, dans le respect du droit de l'Union européenne ou du droit national, préserver la sécurité et les intérêts commerciaux de l'entité ainsi que la confidentialité des informations communiquées.

§ 2. Lorsque la sensibilisation du public est nécessaire pour prévenir un incident significatif ou pour faire face à un incident significatif en cours, ou lorsque la divulgation de l'incident significatif est par ailleurs dans l'intérêt public, le CSIRT national peut, après avoir consulté l'entité concernée, le NCCN, l'éventuelle autorité sectorielle concernée et le ministre concerné, informer le public de l'incident significatif ou exiger de l'entité qu'elle le fasse.

§ 3. À la demande de l'éventuelle autorité sectorielle concernée, l'autorité nationale de cybersécurité transmet les notifications reçues en vertu de l'article 34, § 1^{er}, alinéa 1^{er}, aux points de contact uniques des autres États membres touchés.

§ 4. L'autorité nationale de cybersécurité soumet tous les trois mois à l'ENISA un rapport de synthèse comprenant des données anonymisées et agrégées sur les incidents significatifs, les incidents, les cybermenaces et les incidents évités notifiés conformément à l'article 34, § 1^{er}, alinéa 1^{er}, et à l'article 38, § 1^{er}.

§ 5. Le CSIRT national fournit aux autorités compétentes en vertu de la loi [CER /du 1^{er} juillet 2011] des informations sur les incidents significatifs, les incidents, les cybermenaces et les incidents évités notifiés conformément l'article 34, § 1^{er}, alinéa 1^{er}, et à l'article 38, § 1^{er}, par les entités identifiées [comme des entités critiques] en vertu de la loi [CER /du 1^{er} juillet 2011].

Section 2. Notification volontaire

Art. 38. § 1^{er}. Outre les obligations de notification prévues à l'article 34, peuvent être notifiés à titre volontaire au CSIRT national par:

1° les entités essentielles et importantes, les incidents, les cybermenaces et les incidents évités;

2° les entités autres que celles visées au 1°, indépendamment du fait qu'elles relèvent ou non du champ d'application de la présente loi, les incidents significatifs, les cybermenaces et les incidents évités.

§ 2. Les notifications volontaires visées au paragraphe 1^{er} sont traitées de la même manière que les notifications obligatoires visées à la section 1^{re} du présent chapitre.

Les notifications obligatoires peuvent néanmoins être traitées de manière prioritaire par rapport aux notifications volontaires.

Sans préjudice de la prévention et de la détection d'infractions pénales et des enquêtes et poursuites en la matière, un signalement volontaire n'a pas pour effet d'imposer à l'entité

artikel 35 is ontvangen. Daarbij beschermt het nationale CSIRT, overeenkomstig het Unie- of het nationale recht, de beveiligings- en commerciële belangen van de entiteit, alsook de vertrouwelijkheid van de verstrekte informatie.

§ 2. Wanneer publieke bewustmaking nodig is om een significant incident te voorkomen of een lopend incident aan te pakken, of wanneer de bekendmaking van het significante incident anderszins in het algemeen belang is, kan het nationale CSIRT, na raadpleging van de betrokken entiteit, het NCCN, de eventuele betrokken sectorale overheid en de betrokken minister, het publiek over het significante incident informeren of van de entiteit verlangen dat zij dit doet.

§ 3. De nationale cyberbeveiligingsautoriteit stuurt, op verzoek van de eventuele betrokken sectorale overheid, de op grond van artikel 34, § 1, eerste lid, ontvangen meldingen door naar de centrale contactpunten van de andere betrokken lidstaten.

§ 4. De nationale cyberbeveiligingsautoriteit dient om de drie maanden bij Enisa een samenvattend verslag in met geanonimiseerde en geaggregeerde gegevens over significante incidenten, incidenten, cyberdreigingen en bijna-incidenten die overeenkomstig artikel 34, § 1, eerste lid, en artikel 38, § 1, zijn gemeld.

§ 5. Het nationale CSIRT verstrekt de uit hoofde van de [CER-wet/wet van 1 juli 2011] bevoegde autoriteiten informatie over significante incidenten, incidenten, cyberdreigingen en bijna-incidenten die overeenkomstig artikel 34, § 1, eerste lid, en artikel 38, § 1, zijn gemeld door entiteiten die uit hoofde van de [CER-wet/wet van 1 juli 2011] [als kritieke entiteiten] zijn aangemerkt.

Afdeling 2. Vrijwillige melding

Art. 38. § 1. Naast de in artikel 34 bedoelde meldingsverplichtingen kunnen vrijwillig aan het nationale CSIRT worden gemeld door:

1° essentiële en belangrijke entiteiten: incidenten, cyberdreigingen en bijna-incidenten;

2° andere dan in 1° bedoelde entiteiten, ongeacht of zij tot het toepassingsgebied van deze wet behoren: significante incidenten, cyberdreigingen en bijna-incidenten.

§ 2. De in paragraaf 1 bedoelde vrijwillige meldingen worden op dezelfde wijze verwerkt als de verplichte meldingen bedoeld in afdeling 1 van dit hoofdstuk.

Er kan evenwel voorrang worden gegeven aan de verwerking van verplichte meldingen boven die van vrijwillige meldingen.

Onverminderd het voorkomen, opsporen, onderzoeken en vervolgen van misdrijven, mag een vrijwillige melding er niet toe leiden dat de meldende entiteit bijkomende verplichtingen

ayant effectué la notification des obligations supplémentaires auxquelles elle n'aurait pas été soumise si elle n'avait pas transmis la notification.

Titre 4. – Supervision et sanctions

CHAPITRE 1^{ER} – Supervision

Section 1^{re}. Évaluation périodique de la conformité

Art. 39. Les entités essentielles se soumettent à une évaluation périodique de la conformité de la mise en œuvre des mesures de gestion des risques en matière de cybersécurité visées à l'article 30, sur base des modalités et des cadres de référence déterminés par le Roi:

1° Soit en choisissant une évaluation périodique de la conformité visée à l'article 40, sur base de l'un des cadres de référence déterminé par le Roi;

2° Soit en se soumettant à une inspection par l'autorité nationale de cybersécurité, sur base des modalités déterminées par le Roi.

Par dérogation à l'alinéa 1^{er}, et à la demande de l'autorité sectorielle concernée, les inspections visées à l'alinéa 1^{er}, 2°, sont effectuées de manière conjointe, sous la direction de l'autorité nationale de cybersécurité ou sont déléguées à l'éventuel service d'inspection concerné moyennant l'accord de l'autorité nationale de cybersécurité.

Lorsque le Roi détermine plusieurs cadres de référence, les entités essentielles choisissent le cadre de référence auquel ils se soumettent.

Art. 40. § 1^{er}. L'évaluation périodique de la conformité visée à l'article 39, alinéa 1^{er}, 1°, est effectuée par un organisme d'évaluation de la conformité agréé par l'autorité nationale de cybersécurité selon les conditions fixées par le Roi.

Pour le contrôle des entités **[critiques au sens de la loi [CER] identifiées dans le cadre de la loi du 1^{er} juillet 2011]** et des entités de l'administration publique, l'organisme d'évaluation de la conformité ainsi que les personnes physiques qui évaluent la conformité disposent d'une habilitation de sécurité.

§ 2. Le service d'inspection de l'autorité nationale de cybersécurité peut à tout moment vérifier le respect des conditions d'agrément visées au paragraphe 1^{er} par les organismes d'évaluation de la conformité, conformément aux dispositions du présent chapitre.

Art. 41. Les entités importantes peuvent, de manière volontaire, se soumettre à une évaluation périodique de la conformité visée à l'article 39, alinéa 1^{er}, 1°, de la mise en œuvre des mesures de gestion des risques en matière de cybersécurité visées à l'article 30, § 3, sur base des modalités et des cadres de référence déterminés par le Roi.

worden opgelegd waaraan zij niet zou zijn onderworpen indien zij de melding niet had ingediend.

Titel 4. – Toezicht en sancties

HOOFDSTUK 1 – Toezicht

Afdeling 1. Regelmatige conformiteitsbeoordeling

Art. 39. Essentiële entiteiten onderwerpen zich aan een regelmatige conformiteitsbeoordeling van de uitvoering van de maatregelen voor het beheer van cyberbeveiligingsrisico's bedoeld in artikel 30, op basis van de door de Koning bepaalde modaliteiten en referentiekaders:

1° ofwel opteren zij voor een in artikel 40 bedoelde regelmatige conformiteitsbeoordeling, op basis van een van de door de Koning bepaalde referentiekaders;

2° ofwel onderwerpen zij zich aan een inspectie door de nationale cyberbeveiligingsautoriteit, op basis van de door de Koning bepaalde nadere regels.

In afwijking van het eerste lid en op verzoek van de betrokken sectorale overheid worden de in het eerste lid, 2°, bedoelde inspecties gezamenlijk uitgevoerd, onder leiding van de nationale cyberbeveiligingsautoriteit of worden gedelegeerd aan de betrokken inspectiedienst mits akkoord van de nationale cyberbeveiligingsautoriteit.

Indien de Koning meerdere referentiekaders bepaalt, kiezen essentiële entiteiten aan welk referentiekader zij zich onderwerpen.

Art. 40. § 1. De in artikel 39, eerste lid, 1°, bedoelde regelmatige conformiteitsbeoordeling wordt verricht door een conformiteitsbeoordelingsinstantie die erkend is door de nationale cyberbeveiligingsautoriteit volgens de door de Koning bepaalde voorwaarden.

Voor het toezicht op **[kritieke entiteiten als bedoeld in de [CER]-wet die in het kader van de wet van 1 juli 2011 zijn geïdentificeerd]** en overheidsinstanties beschikken de conformiteitsbeoordelingsinstantie en de natuurlijke personen die de conformiteit beoordelen over een veiligheidsmachtiging.

§ 2. De inspectiedienst van de nationale cyberbeveiligingsautoriteit kan op elk ogenblik nagaan of de conformiteitsbeoordelingsinstanties de in paragraaf 1 bedoelde erkenningsvoorwaarden naleven, overeenkomstig de bepalingen van dit hoofdstuk.

Art. 41. Belangrijke entiteiten kunnen zich vrijwillig onderwerpen aan een regelmatige conformiteitsbeoordeling, als bedoeld in artikel 39, eerste lid, 1°, van de uitvoering van de maatregelen voor het beheer van cyberbeveiligingsrisico's bedoeld in artikel 30, § 3, op basis van de door de Koning bepaalde modaliteiten en referentiekaders.

Art. 42. Les entités essentielles et importantes qui se soumettent à une évaluation périodique de la conformité visée à l'article 39, alinéa 1^{er}, 1°, respectivement conformément à l'article 39 et 41 sont, jusqu'à preuve du contraire, présumées respecter les obligations visées à l'article 30.

Art. 43. Une liste des organismes d'évaluation de la conformité agréés par l'autorité nationale de cybersécurité conformément à l'article 40 est disponible auprès de l'autorité nationale de cybersécurité, qui la tient à jour.

Section 2. Dispositions générales relatives au service d'inspection

Art. 44. § 1^{er}. Le service d'inspection de l'autorité nationale de cybersécurité réalise des contrôles du respect par les entités essentielles et importantes des mesures de gestion des risques en matière de cybersécurité et des règles de notification des incidents.

Par dérogation à l'alinéa 1^{er}, et à la demande de l'autorité sectorielle concernée, ces contrôles sont effectués de manière conjointe, sous la direction de l'autorité nationale de cybersécurité, ou sont délégués à l'éventuel service d'inspection concerné moyennant l'accord de l'autorité nationale de cybersécurité.

L'autorité sectorielle ou le service d'inspection sectoriel compétent, ou, lorsqu'aucun service d'inspection sectoriel n'a été désigné par la loi ou par le Roi, le service d'inspection de l'autorité nationale de cybersécurité peut réaliser des contrôles du respect par les entités essentielles et importantes des mesures de gestion des risques en matière de cybersécurité sectorielles ou sous-sectorielles supplémentaires visées à l'article 33.

§ 2. Au moment de formuler une demande d'informations ou de preuves, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent mentionnent la finalité de la demande, les informations ou preuves précises demandées et le délai dans lequel celles-ci doivent être fournies.

Le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent peuvent faire appel à des experts.

§ 3. Le service d'inspection de l'autorité nationale de cybersécurité ainsi que les éventuels autorités sectorielles et services d'inspection sectoriels peuvent fixer des priorités en ce qui concerne les tâches de supervision visées au présent titre selon une approche basée sur les risques.

§ 4. Lorsqu'ils traitent des incidents donnant lieu à des violations de données à caractère personnel, le service d'inspection de l'autorité nationale de cybersécurité ainsi que les éventuels autorités sectorielles et services d'inspection sectoriels coopèrent étroitement avec les Autorités de protection des données, sans préjudice de la compétence et des missions de ces dernières.

Art. 42. Essentiële en belangrijke entiteiten die zich aan een regelmatige conformiteitsbeoordeling, als bedoeld in artikel 39, eerste lid, 1°, onderwerpen, respectievelijk overeenkomstig artikel 39 en 41, worden tot bewijs van het tegendeel geacht de in artikel 30 bedoelde verplichtingen na te leven.

Art. 43. Een lijst van de conformiteitsbeoordelingsinstanties die overeenkomstig artikel 40 erkend zijn door de nationale cyberbeveiligingsautoriteit, is beschikbaar bij laatstgenoemde autoriteit die ze actueel houdt.

Afdeling 2. Algemene bepalingen betreffende de inspectiedienst

Art. 44. § 1. De inspectiedienst van de nationale cyberbeveiligingsautoriteit voert controles uit om na te gaan of de essentiële en belangrijke entiteiten de maatregelen voor het beheer van cyberbeveiligingsrisico's en de regels voor het melden van incidenten naleven.

In afwijking van het eerste lid en op verzoek van de betrokken sectorale overheid worden deze controles gezamenlijk uitgevoerd, onder leiding van de nationale cyberbeveiligingsautoriteit, of gedelegeerd aan de eventuele betrokken inspectiedienst mits akkoord van de nationale cyberbeveiligingsautoriteit.

De bevoegde sectorale overheid of sectorale inspectiedienst of, indien geen sectorale inspectiedienst is aangewezen door de wet of de Koning, de inspectiedienst van de nationale cyberbeveiligingsautoriteit kan controles uitvoeren om na te gaan of de essentiële en belangrijke entiteiten de bijkomende sectorale of deelsectorale maatregelen voor het beheer van cyberbeveiligingsrisico's bedoeld in artikel 33 naleven.

§ 2. Bij het formuleren van een verzoek om informatie of bewijzen vermelden de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst het doeleinde van het verzoek, de precieze informatie of bewijzen die worden gevraagd en de termijn waarbinnen deze moeten worden verstrekt.

De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst kunnen een beroep doen op experts.

§ 3. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele sectorale overheden en sectorale inspectiediensten kunnen prioriteit geven aan de in deze titel bedoelde toezichtstaken volgens een risicogebaseerde benadering.

§ 4. Bij de aanpak van incidenten die leiden tot inbreuken in verband met persoonsgegevens, werken de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele sectorale overheden en sectorale inspectiediensten nauw samen met de Gegevensbeschermingsautoriteiten, onverminderd de bevoegdheid en taken van deze laatsten.

Art. 45. § 1^{er}. Le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent informent les autorités compétentes en vertu de la loi [CER /du 1^{er} juillet 2011] lorsqu'ils exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'une entité définie comme critique en vertu de la loi [CER /du 1^{er} juillet 2011] respecte la présente loi. S'il y a lieu, les autorités compétentes en vertu de la loi [CER /du 1^{er} juillet 2011] peuvent demander au service d'inspection de l'autorité nationale de cybersécurité et à l'éventuelle autorité sectorielle ou à l'éventuel service d'inspection sectoriel compétent d'exercer leurs pouvoirs de supervision et d'exécution à l'égard d'une entité qui est définie comme entité critique en vertu de la loi [CER /du 1^{er} juillet 2011].

§ 2. Le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent coopèrent avec les autorités compétentes pertinentes en vertu du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011. En particulier, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent informent le forum de supervision institué en vertu de l'article 32, paragraphe 1, dudit règlement lorsqu'ils exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'une entité essentielle ou importante qui a été désignée comme étant un prestataire tiers critique de services TIC au titre de l'article 31 dudit règlement respecte la présente loi.

Art. 46. § 1^{er}. Lorsque les réseaux et les systèmes d'information d'une entité sont situés en dehors du territoire belge, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent, en concertation avec l'autorité nationale de cybersécurité, peuvent solliciter la coopération et l'assistance des autorités de contrôle compétentes d'autres États membres.

Dans le cadre de la sollicitation visée à l'alinéa 1^{er}:

1° le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent peuvent demander aux autorités de contrôle compétentes d'autres États membres de prendre des mesures de supervision ou d'exécution;

2° le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent peuvent demander, de manière motivée, aux autorités de contrôle compétentes d'autres États membres une assistance mutuelle afin que les mesures de supervision ou d'exécution puissent être mises en œuvre de manière effective, efficace et cohérente.

Art. 45. § 1. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst stellen de uit hoofde van de [CER-wet/wet van 1 juli 2011] bevoegde autoriteiten in kennis wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat een entiteit die op grond van de [CER-wet/wet van 1 juli 2011] als kritieke entiteit wordt aangemerkt, voldoet aan deze wet. In voorkomend geval kunnen de uit hoofde van de [CER-wet/wet van 1 juli 2011] bevoegde autoriteiten de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst verzoeken hun toezichts- en handhavingsbevoegdheden uit te oefenen ten aanzien van een entiteit die is aangemerkt als kritieke entiteit uit hoofde van de [CER-wet/wet van 1 juli 2011].

§ 2. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst werken samen met de relevante autoriteiten die bevoegd zijn uit hoofde van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst stellen met name het oversightforum dat is opgericht op grond van artikel 32, lid 1, van bovengenoemde verordening in kennis wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat een essentiële of belangrijke entiteit die op grond van artikel 31 van bovengenoemde verordening als kritieke derde aanbieder van ICT-diensten is aangewezen, voldoet aan deze wet.

Art. 46. § 1. Wanneer de netwerk- en informatiesystemen van een entiteit zich buiten het Belgische grondgebied bevinden, kunnen de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst, in overleg met de nationale cyberbeveiligingsautoriteit, de bevoegde toezichthoudende autoriteiten van andere lidstaten om samenwerking en bijstand verzoeken.

In het kader van het verzoek bedoeld in het eerste lid:

1° kunnen de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst de bevoegde toezichthoudende autoriteiten van andere lidstaten verzoeken om toezichts- of handhavingsmaatregelen te nemen;

2° kunnen de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst de bevoegde toezichthoudende autoriteiten van andere lidstaten gemotiveerd om wederzijdse bijstand verzoeken, zodat de toezichts- of handhavingsmaatregelen op een effectieve, efficiënte en consistente wijze kunnen worden uitgevoerd.

L'assistance mutuelle visée à l'alinéa 2, 2°, peut porter sur des demandes d'informations et des mesures de contrôle, y compris des demandes de procéder à des inspections sur place, à des contrôles à distance ou à des audits de sécurité ciblés.

§ 2. De manière proportionnée à leurs ressources et pour autant que cela rentre dans le cadre de leurs compétences, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent coopèrent et apportent leur assistance aux autorités de contrôle compétentes en matière de cybersécurité d'autres États membres qui en font la demande, lorsque les réseaux et les systèmes d'information de l'entité concernée sont situés dans le territoire belge.

Dans le cadre de la demande visée à l'alinéa 1^{er}:

1° L'autorité nationale de cybersécurité centralise les informations et consultations en ce qui concerne les mesures de supervision et d'exécution prises par elle-même, par l'éventuelle autorité sectorielle et par l'éventuel service d'inspection sectoriel compétent et les communique aux autorités de contrôle compétentes en matière de cybersécurité d'autres États membres;

2° ladite demande peut porter sur des mesures de supervision ou d'exécution;

3° ladite demande peut, de manière motivée, porter sur une assistance mutuelle afin que les mesures de supervision ou d'exécution puissent être mises en œuvre de manière effective, efficace et cohérente.

L'assistance mutuelle visée à l'alinéa 2, 3°, peut porter sur des demandes d'informations et des mesures de contrôle, y compris des demandes de procéder à des inspections sur place, à des contrôles à distance ou à des audits de sécurité ciblés.

L'autorité à laquelle une demande d'assistance est adressée ne peut refuser cette demande que s'il est établi que ladite autorité n'est pas compétente pour fournir l'assistance demandée, que l'assistance demandée n'est pas proportionnée aux tâches de supervision de ladite autorité ou que la demande concerne des informations ou implique des activités dont la divulgation ou l'exercice seraient contraires aux intérêts essentiels de la sécurité nationale, la sécurité publique ou la défense de la Belgique. Avant de refuser une telle demande, ladite autorité consulte les autres autorités compétentes concernées ainsi que, à la demande de l'un des États membres concernés, la Commission et l'ENISA.

§ 3. D'un commun accord, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent peuvent mener à bien des actions communes de supervision entre elles et/ou avec les autorités de contrôle compétentes d'autres États membres.

De wederzijdse bijstand bedoeld in het tweede lid, 2°, kan betrekking hebben op verzoeken om informatie en toezichtsmaatregelen, met inbegrip van verzoeken om inspecties ter plaatse, toezicht elders of gerichte beveiligingsaudits uit te voeren.

§ 2. In verhouding tot hun middelen en voor zover dit binnen hun bevoegdheden valt, werken de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst samen met de toezichthoudende autoriteiten bevoegd voor cyberbeveiliging van andere lidstaten en verlenen ze bijstand aan deze autoriteiten indien deze hierom verzoeken en de netwerk- en informatiesystemen van de betrokken entiteit zich op Belgisch grondgebied bevinden.

In het kader van het verzoek bedoeld in het eerste lid:

1° centraliseert de nationale cyberbeveiligingsautoriteit de informatie en raadplegingen met betrekking tot de toezichts- en handhavingsmaatregelen die zichzelf of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst heeft genomen, en deelt deze mee aan de toezichthoudende autoriteiten bevoegd voor cyberbeveiliging van andere lidstaten;

2° dit verzoek kan betrekking hebben op toezichts- of handhavingsmaatregelen;

3° dit verzoek kan, indien het gemotiveerd wordt, betrekking hebben op wederzijdse bijstand, zodat de toezichts- of handhavingsmaatregelen op een effectieve, efficiënte en consistente wijze kunnen worden uitgevoerd.

De wederzijdse bijstand bedoeld in het tweede lid, 3°, kan betrekking hebben op verzoeken om informatie en toezichtsmaatregelen, met inbegrip van verzoeken om inspecties ter plaatse, toezicht elders of gerichte beveiligingsaudits uit te voeren.

De autoriteit waaraan een verzoek om bijstand is gericht, mag dat verzoek niet weigeren, tenzij wordt vastgesteld dat zij niet bevoegd is om de gevraagde bijstand te verlenen, de gevraagde bijstand niet in verhouding staat tot de toezichthoudende taken van deze autoriteit, of het verzoek betrekking heeft op informatie of activiteiten inhoudt die, indien ze openbaar zouden worden gemaakt of zouden worden uitgevoerd, in strijd zouden zijn met de wezenlijke belangen van de nationale veiligheid, de openbare veiligheid of de defensie van België. Alvorens een dergelijk verzoek af te wijzen, raadpleegt voornoemde autoriteit de andere betrokken bevoegde autoriteiten alsook, op verzoek van een van de betrokken lidstaten, de Commissie en Enisa.

§ 3. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst kunnen in onderlinge overeenstemming gezamenlijke toezichtsacties uitvoeren, en dit onderling en/of met de bevoegde toezichthoudende autoriteiten van andere lidstaten.

§ 4. Le présent article n'est pas applicable aux missions diplomatiques et consulaires.

Art. 47. § 1^{er}. Les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent sont dotés d'une carte de légitimation dont le modèle est fixé par le Roi.

§ 2. Les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent et les experts appelés à participer à l'inspection ne peuvent avoir un intérêt quelconque, direct ou indirect, dans les entreprises ou institutions qu'ils sont chargés de contrôler, susceptible de compromettre leur objectivité. Ils prêtent serment auprès du fonctionnaire dirigeant de leur service.

Les autorités visées à l'article 44, § 1^{er}, prennent les mesures nécessaires afin d'assurer l'indépendance des membres de leur personnel, de prévenir, d'identifier et de résoudre efficacement les conflits d'intérêts lors de l'exécution de leurs tâches.

La notion de conflit d'intérêts vise au moins les situations dans lesquelles un membre du personnel des autorités visées à l'article 44, § 1^{er}, a, directement ou indirectement, un intérêt financier, économique ou un autre intérêt personnel qui pourrait être perçu comme compromettant son impartialité et son indépendance dans le cadre de sa mission ou de ses fonctions.

§ 3. Les membres du personnel des autorités visées à l'article 44, § 1^{er}, ne reçoivent ni ne cherchent pas, dans les limites de leurs attributions, de façon directe ou indirecte, d'instructions de personne tierce.

Il leur est interdit d'être présents lors d'une délibération ou décision sur les dossiers pour lesquels ils ont un intérêt personnel ou direct ou pour lesquels leurs parents ou alliés jusqu'au troisième degré ont un intérêt personnel ou direct.

Le Roi peut également désigner d'autres situations comme étant des conflits d'intérêts.

Section 3. La supervision des entités par le service d'inspection

Art. 48. § 1^{er}. Sans préjudice des attributions des officiers de police judiciaire visées à l'article 8 du Code d'instruction criminelle, les membres assermentés du service d'inspection de l'autorité nationale de cybersécurité et les membres assermentés de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent disposent, dans l'exercice de leur mission de supervision, des compétences de contrôle suivantes, tant dans le cadre de démarches administratives que dans le cadre de la constatation de violations de la présente loi:

1° demander l'accès à et obtenir une copie de tout document ou toute information nécessaire à l'exercice de leur mission

§ 4. Dit artikel is niet van toepassing op diplomatieke en consulaire missies.

Art. 47. § 1. De leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst beschikken over een legitimatiekaart waarvan het model door de Koning wordt bepaald.

§ 2. De leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst en de experten die deelnemen aan de inspectie, mogen geen enkel rechtstreeks of onrechtstreeks belang hebben in de ondernemingen of instellingen waarop zij toezicht dienen uit te oefenen, waardoor hun objectiviteit in het gedrang zou kunnen komen. Zij leggen de eed af bij de leidend ambtenaar van hun dienst.

De autoriteiten bedoeld in artikel 44, § 1, nemen de nodige maatregelen om, bij de uitvoering van hun taken, de onafhankelijkheid van hun personeelsleden te garanderen en om belangenconflicten doeltreffend te voorkomen, te identificeren en op te lossen.

Het begrip "belangenconflict" heeft minstens betrekking op situaties waarin een personeelslid van de autoriteiten bedoeld in artikel 44, § 1, rechtstreeks of onrechtstreeks financiële, economische of andere persoonlijke belangen heeft die geacht kunnen worden zijn onpartijdigheid en onafhankelijkheid in het kader van zijn opdracht of functie in het gedrang te brengen.

§ 3. De personeelsleden van de autoriteiten bedoeld in artikel 44, § 1, krijgen noch vragen binnen de grenzen van hun bevoegdheden op directe of indirecte wijze instructies van derden.

Het is hen verboden aanwezig te zijn bij een beraadslaging of besluit over dossiers waarin zij een persoonlijk of rechtstreeks belang hebben of waarin hun bloed- of aanverwanten tot en met de derde graad een persoonlijk of rechtstreeks belang hebben.

De Koning kan ook andere situaties benoemen als belangenconflicten.

Afdeling 3. Het door de inspectiedienst uitgeoefende toezicht op de entiteiten

Art. 48. § 1. Onverminderd de bevoegdheden van de officieren van gerechtelijke politie bedoeld in artikel 8 van het Wetboek van strafvordering beschikken de beëdigde leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de beëdigde leden van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst bij de uitoefening van hun toezichtsoverdracht over de volgende toezichtsbevoegdheden, en dit zowel in het kader van administratieve handelingen als in het kader van de vaststelling van inbreuken op deze wet:

1° toegang vragen tot alle documenten of informatie die nodig zijn voor de uitoefening van hun toezichtsoverdracht en

de supervision, notamment les preuves de la mise en œuvre de politiques de cybersécurité, telles que les résultats des évaluations de la conformité ou de tout autre audit de sécurité effectué par un auditeur qualifié et les éléments de preuve sous-jacents correspondants;

2° procéder, sur place ou à distance, à tout examen, contrôle et audition, y compris des contrôles aléatoires effectués par des professionnels formés;

3° soumettre les entités essentielles à des audits de sécurité réguliers et ciblés réalisés par un organisme indépendant, basés sur des évaluations des risques effectuées par le service d'inspection concerné ou l'entité contrôlée, ou sur d'autres informations disponibles relatives aux risques;

4° requérir toutes les informations qu'ils estiment nécessaires à l'évaluation des mesures de gestion des risques en matière de cybersécurité adoptées par l'entité concernée, notamment les politiques de cybersécurité consignées par écrit, du respect de l'obligation de soumettre des informations à l'autorité nationale de cybersécurité ou à l'éventuelle autorité sectorielle conformément au titre 1^{er} et de la mise en œuvre de la présente loi;

5° réaliser un audit ad hoc, notamment lorsqu'il est justifié en raison d'un incident significatif ou d'une violation de la présente loi;

6° effectuer des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération de l'entité concernée;

7° prendre l'identité des personnes qui se trouvent sur les lieux utilisés par l'entité et dont ils estiment l'audition nécessaire pour l'exercice de leur mission. A cet effet, ils peuvent exiger de ces personnes la présentation de documents officiels d'identification;

8° le cas échéant, demander l'assistance des services de la police fédérale ou locale dans le cadre de l'usage de la force;

9° solliciter des informations auprès des membres du personnel visés à l'article 9 de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, pour les besoins de l'exécution des dispositions de la présente loi;

10° pénétrer sans avertissement préalable, sur présentation de leur carte de légitimation, dans tous les lieux utilisés par l'entité; ils n'ont accès aux locaux habités que moyennant autorisation préalable délivrée par le juge d'instruction.

§ 2. Dans le cadre de l'inspection des entités importantes, les compétences de contrôle visées au paragraphe 1^{er} s'exercent de manière *ex post*, sur base d'éléments de preuve,

hiervan een kopie verkrijgen, met name de bewijzen van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van conformiteitsbeoordelingen of andere beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de respectieve onderliggende bewijzen;

2° overgaan, ter plaatse of elders, tot elk onderzoek, elke controle en elk verhoor, met inbegrip van steekproefsgewijze controles die worden uitgevoerd door daartoe opgeleide professionals;

3° essentiële entiteiten onderwerpen aan regelmatige en gerichte beveiligingsaudits die worden uitgevoerd door een onafhankelijke instantie, gebaseerd op door de betrokken inspectiedienst of de gecontroleerde entiteit verrichte risico-beoordelingen of op andere beschikbare risicogerelateerde informatie;

4° alle inlichtingen inwinnen die zij nodig achten voor de beoordeling van de door de betrokken entiteit genomen maatregelen voor het beheer van cyberbeveiligingsrisico's, met name betreffende het gedocumenteerde cyberbeveiligingsbeleid, de naleving van de verplichting om informatie in te dienen bij de nationale cyberbeveiligingsautoriteit of bij de eventuele sectorale overheid overeenkomstig titel 1 en de uitvoering van deze wet;

5° een ad-hoc audit uitvoeren, ook in gevallen waarin dat gerechtvaardigd is op grond van een significant incident of een inbreuk op deze wet;

6° beveiligingsscan uitvoeren op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria, indien nodig in samenwerking met de betrokken entiteit;

7° de identiteit opnemen van de personen die zich op de door de entiteit gebruikte plaatsen bevinden en van wie ze het verhoor nodig achten voor de uitoefening van hun opdracht. Daartoe kunnen ze van deze personen eisen dat ze officiële identificatiedocumenten voorleggen;

8° in voorkomend geval, de bijstand vragen van de federale of lokale politiediensten in het kader van het gebruik van geweld;

9° inlichtingen inwinnen bij de personeelsleden bedoeld in artikel 9 van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, voor de uitvoering van de bepalingen van deze wet;

10° zonder voorafgaande verwittiging, op vertoon van hun legitimatiekaart, alle door de entiteit gebruikte plaatsen betreden; zij hebben slechts toegang tot bewoonde lokalen mits vooraf een machtiging is uitgereikt door de onderzoeksrechter.

§ 2. In het kader van de inspectie van belangrijke entiteiten worden de toezichtsbevoegdheden bedoeld in paragraaf 1 achteraf ("*ex post*") uitgeoefend, op basis van bewijzen,

d'indications ou d'informations selon lesquels une entité importante ne respecterait pas la présente loi.

§ 3. Pour obtenir l'autorisation de pénétrer dans des locaux habités, les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent adressent une demande motivée au juge d'instruction. Cette demande contient au moins les données suivantes:

1° l'identification des espaces habités auxquels ils souhaitent avoir accès;

2° les infractions éventuelles qui font l'objet du contrôle;

3° tous les documents et renseignements desquels il ressort que l'utilisation de ce moyen est nécessaire.

Le juge d'instruction décide dans un délai de quarante-huit heures maximum après réception de la demande. La décision du juge d'instruction est motivée. En l'absence de décision dans le délai prescrit, la visite des lieux est réputée être refusée. Le service d'inspection de l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent peut introduire un recours contre la décision de refus ou l'absence de décision devant la chambre des mises en accusation dans les quinze jours de la notification de la décision ou de l'expiration du délai.

Les visites sans autorisation de l'occupant dans des locaux habités se font entre cinq et vingt-et-une heures par au moins deux membres du service d'inspection agissant conjointement.

§ 4. Au début de toute audition, il est communiqué à la personne interrogée:

1° que ses déclarations peuvent être utilisées comme preuve en justice;

2° qu'elle peut demander que toutes les questions qui lui sont posées et les réponses qu'elle donne soient actées dans les termes utilisés;

3° qu'elle a le droit de garder le silence et de ne pas contribuer à sa propre incrimination.

Toute personne interrogée peut utiliser les documents en sa possession, sans que cela puisse entraîner le report de l'audition. Elle peut, lors de l'audition ou ultérieurement, exiger que ces documents soient joints à l'audition.

L'audition mentionne avec précision l'heure à laquelle elle a pris cours, est éventuellement interrompue et reprise, et prend fin. Elle mentionne l'identité des personnes qui interviennent lors de l'audition ou lors d'une partie de celle-ci.

A la fin de l'audition, la personne interrogée a le droit de relire celle-ci ou de demander que lecture lui en soit faite. Elle

aanwijzingen of informatie waaruit blijkt dat een belangrijke entiteit deze wet niet zou naleven.

§ 3. Om een machtiging tot betreding van bewoonde lokalen te bekomen, richten de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst een met redenen omkleed verzoek aan de onderzoeksrechter. Dit verzoek bevat minstens de volgende gegevens:

1° de identificatie van de bewoonde ruimten waartoe zij toegang wensen te hebben;

2° de eventuele inbreuken die het voorwerp zijn van het toezicht;

3° alle documenten en inlichtingen waaruit blijkt dat het gebruik van dit middel nodig is.

De onderzoeksrechter beslist binnen een termijn van maximum achtenveertig uur na ontvangst van het verzoek. De beslissing van de onderzoeksrechter is met redenen omkleed. Bij gebrek aan een beslissing binnen de voorgeschreven termijn wordt het plaatsbezoek geacht te zijn geweigerd. De inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst kan beroep instellen tegen de weigeringsbeslissing of het gebrek aan een beslissing bij de kamer van inbeschuldigingstelling binnen vijftien dagen na de kennisgeving van de beslissing of het verstrijken van de termijn.

Bezoeken aan bewoonde lokalen zonder toestemming van de bewoner gebeuren tussen vijf en eenentwintig uur door minstens twee leden van de inspectiedienst die samen optreden.

§ 4. Bij het begin van elk verhoor wordt aan de ondervraagde persoon meegedeeld:

1° dat zijn verklaringen voor een rechtbank als bewijs kunnen worden gebruikt;

2° dat hij kan vragen dat alle vragen die hem worden gesteld en de antwoorden die hij geeft, worden genoteerd in de gebruikte bewoordingen;

3° dat hij het recht heeft om te zwijgen en niet bij te dragen tot zijn eigen beschuldiging.

Elke ondervraagde persoon mag de documenten in zijn bezit gebruiken, zonder dat daardoor het verhoor uitgesteld wordt. Hij mag tijdens het verhoor of later vragen om die documenten bij het verhoor te voegen.

Het verhoor vermeldt nauwkeurig het tijdstip waarop het wordt aangevat, eventueel onderbroken en hervat, alsook beëindigd. Het vermeldt de identiteit van de personen die tussenkomen tijdens het verhoor of een deel ervan.

Aan het einde van het verhoor heeft de ondervraagde persoon het recht om zijn verhoor te lezen of het te laten

peut demander à ce que ses déclarations soient corrigées ou complétées.

Les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent peuvent consulter tous les supports d'information et les données qu'ils contiennent. Ils peuvent se faire produire sur place le système informatique et les données qu'il contient dont ils ont besoin pour leurs examens et constatations, et en prendre ou en demander gratuitement des extraits, des duplicatas ou des copies, sous une forme lisible et intelligible qu'ils ont demandée.

§ 5. Les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent peuvent consulter tous les supports d'information et les données qu'ils contiennent. Ils peuvent se faire produire sur place le système informatique et les données qu'il contient dont ils ont besoin pour leurs examens et constatations, et en prendre ou en demander gratuitement des extraits, des duplicatas ou des copies, sous une forme lisible et intelligible qu'ils ont demandée.

S'il n'est pas possible de prendre des copies sur place, les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent peuvent saisir, contre récépissé contenant un inventaire, le système informatique et les données qu'il contient.

§ 6. Pour étendre les recherches dans un système informatique ou une partie de celui-ci, entamées sur la base du paragraphe 5, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée, le service d'inspection de l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent peut solliciter l'intervention d'un juge d'instruction.

§ 7. Lorsque le service d'inspection de l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent prend connaissance, dans le cadre de la supervision ou de l'exécution, du fait que la violation commise par une entité essentielle ou importante à l'égard des obligations énoncées aux articles 30 et 34 à 37 peut donner lieu à une violation de données à caractère personnel au sens de l'article 4, point 12, du règlement (UE) 2016/679, devant être notifiée en vertu de l'article 33 dudit règlement, ils en informent sans retard injustifié les Autorités de protection des données.

Lorsque l'autorité de protection des données compétente est établie dans un autre État membre que la Belgique, le service d'inspection de l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent informe l'autorité de protection des données compétente établie en Belgique de la violation potentielle de données à caractère personnel visée à l'alinéa 1^{er}.

§ 8. Lors de l'exécution de leurs pouvoirs de contrôle visés au présent article, les membres assermentés des autorités visées à l'article 44, § 1^{er}, veillent à ce que les moyens qu'ils utilisent soient appropriés et nécessaires pour ledit contrôle.

voorlezen. Hij mag zijn verklaringen laten verbeteren of er iets aan laten toevoegen.

De leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst die een persoon onderwerpen, delen hem mee dat hij een kopie mag vragen van de tekst van zijn verhoor. Deze kopie wordt gratis verstrekt.

§ 5. De leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst mogen alle informatiedragers en de erin opgenomen gegevens raadplegen. Zij mogen zich ter plaatse het informaticasysteem en de erin opgenomen gegevens die zij nodig hebben voor hun onderzoeken en vaststellingen doen voorleggen en er kosteloos uittreksels, duplicaten of kopieën van nemen of vragen in een door hen gevraagde leesbare en verstaanbare vorm.

Indien het niet mogelijk is om ter plaatse kopieën te nemen, mogen de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst, tegen een ontvangstbewijs dat een inventaris bevat, het informaticasysteem en de erin opgenomen gegevens in beslag nemen.

§ 6. Om de zoekactie in een informaticasysteem of een deel hiervan die op basis van paragraaf 5 werd opgestart uit te breiden naar een informaticasysteem of een deel hiervan dat zich op een andere plaats bevindt dan die van de zoekactie, kan de inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst een onderzoeksrechter vragen om op te treden.

§ 7. Wanneer de inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst er bij toezicht of handhaving kennis van krijgen dat de inbreuk door een essentiële of belangrijke entiteit op de in de artikelen 30 en 34 tot 37 vastgestelde verplichtingen een inbreuk in verband met persoonsgegevens zoals gedefinieerd in artikel 4, punt 12, van Verordening (EU) 2016/679 kan inhouden, die op grond van artikel 33 van die verordening moet worden gemeld, stellen zij de Gegevensbeschermingsautoriteiten daarvan onverwijld in kennis.

Wanneer de bevoegde gegevensbeschermingsautoriteit in een andere lidstaat dan België gevestigd is, stelt de inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst de in België gevestigde bevoegde gegevensbeschermingsautoriteit in kennis van de in het eerste lid bedoelde potentiële inbreuk in verband met persoonsgegevens.

§ 8. Bij de uitvoering van hun toezichtsbevoegdheden bedoeld in dit artikel zorgen de beëdigde leden van de autoriteiten bedoeld in artikel 44, § 1, ervoor dat de door hen gebruikte middelen passend en noodzakelijk zijn voor dit toezicht.

Art. 49. § 1^{er}. Après chaque inspection, les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent rédigent un rapport et en transmettent une copie à l'entité inspectée.

§ 2. L'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle se communiquent mutuellement leur rapport d'inspection.

Art. 50. § 1^{er}. L'entité supervisée apporte son entière collaboration aux membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent dans l'exercice de leurs fonctions et notamment pour informer ceux-ci au mieux de toutes les mesures de sécurité existantes.

Si nécessaire, l'entité met à disposition des membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent le matériel nécessaire de manière à ce qu'ils remplissent les consignes de sécurité lors des inspections.

§ 2. Les coûts des inspections ne sont pas mis à charge des entités.

Par dérogation à l'alinéa précédent, le Roi peut déterminer, par secteur ou sous-secteur, par arrêté délibéré en Conseil des ministres et après avis de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle concernée, des rétributions relatives aux prestations d'inspections. Il en fixe les modalités de calcul et de paiement.

§ 3. Le fait pour quiconque d'empêcher ou d'entraver volontairement l'exécution d'un contrôle effectué par les membres du service d'inspection de l'autorité nationale de cybersécurité ou de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent, de refuser de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle, ou de communiquer sciemment des informations inexacts ou incomplètes est constaté dans un procès-verbal par les membres assermentés du service d'inspection de l'autorité nationale de cybersécurité ou de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent.

CHAPITRE 2 – Les mesures et amendes administratives

Section 1^{re}. Procédure

Art. 51. § 1^{er}. Lorsqu'un ou plusieurs manquements aux exigences imposées par la présente loi, ses arrêtés d'exécution ou les décisions administratives individuelles y afférentes sont observés, les faits peuvent être constatés dans un procès-verbal rédigé par les membres assermentés du service d'inspection de l'autorité nationale de cybersécurité, de l'éventuel service d'inspection sectoriel ou de l'éventuelle autorité sectorielle concernée, conformément à l'article 44, § 1^{er}

Art. 49. § 1. Na elke inspectie stellen de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst een verslag op en bezorgen ze daarvan een kopie aan de geïnspecteerde entiteit.

§ 2. De nationale cyberbeveiligingsautoriteit en de eventuele sectorale overheid wisselen hun inspectieverslagen uit.

Art. 50. § 1. De entiteit waarop toezicht wordt uitgeoefend, verleent haar volledige medewerking aan de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst bij de uitoefening van hun functie en met name om deze zo goed mogelijk te informeren over alle bestaande beveiligingsmaatregelen.

Indien nodig stelt de entiteit het nodige materiaal ter beschikking van de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst, zodat ze de veiligheidsvoorschriften kunnen naleven tijdens de inspecties.

§ 2. De kosten van de inspecties zijn niet ten laste van de entiteiten.

In afwijking van het vorige lid, kan de Koning, voor elke sector of deelsector, bij besluit vastgesteld na overleg in de Ministerraad en na advies van de nationale cyberbeveiligingsautoriteit en van de eventuele betrokken sectorale overheid, retributies bepalen voor de inspectieprestaties. De Koning bepaalt de berekenings- en betalingsregels

§ 3. Het feit dat iemand de uitvoering van een controle door de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst opzettelijk verhindert of belemmert, de informatie die hem gevraagd wordt naar aanleiding van deze controle weigert mee te delen, of bewust foutieve of onvolledige informatie verstrekt, wordt opgetekend in een proces-verbaal door de beëdigde leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst.

HOOFDSTUK 2 – De administratieve maatregelen en geldboetes

Afdeling 1. Procedure

Art. 51. § 1. Wanneer een of meer inbreuken op de eisen van deze wet, de uitvoeringsbesluiten ervan of de eraan verbonden individuele administratieve beslissingen worden vastgesteld, kunnen de feiten opgetekend worden in een proces-verbaal door de beëdigde leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit, van de eventuele sectorale inspectiedienst of van de eventuele betrokken sectorale overheid, overeenkomstig artikel 44, § 1.

Moyennant l'accord de l'autorité nationale de cybersécurité, l'autorité sectorielle peut imposer à une entité des mesures et amendes administratives visées à la section 2.

L'autorité nationale de cybersécurité informe l'autorité sectorielle concernée lorsqu'elle a l'intention d'imposer à une entité des mesures et amendes administratives visées aux articles 58 et 59.

Lorsque les autorités visées aux alinéas 1^{er} et 2 prennent connaissance, dans le cadre de leur mission de supervision, du fait qu'un manquement visé à l'alinéa 1^{er} ou 2, commis par une entité essentielle ou importante, peut donner lieu à une violation de données à caractère personnel au sens de l'article 4, 12), du règlement (UE) 2016/679, devant être notifiée en vertu de l'article 33 dudit règlement, elles en informent sans retard injustifié les autorités de protection des données compétentes.

§ 2. Sur la base du procès-verbal visé au paragraphe 1^{er} et, le cas échéant, des rapports pertinents visés à l'article 49, § 1^{er}, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente, peut rédiger un projet de décision contenant au moins les références du procès-verbal qui constate l'infraction et qui relate les faits à propos desquels la procédure est entamée et une ou plusieurs mesures ou amendes administratives visées à l'article 58 et/ou 59 envisagées ainsi que le délai endéans lequel l'entité concernée exécuterait les mesures administratives.

Le délai visé à l'alinéa 1^{er} est déterminé en tenant compte des conditions de fonctionnement de l'entité et des mesures à mettre en œuvre.

§ 3. L'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente envoie le projet de décision visé au paragraphe 2 à l'entité concernée en exposant, en détail, les motifs relatifs aux mesures et/ou amendes administratives envisagées et lui fait part de son droit, dans les quinze jours de la réception de cette information, de formuler par écrit ses moyens de défense ou de solliciter d'être entendu. L'information est présumée reçue par le contrevenant le sixième jour suivant l'envoi du projet de décision précité.

Par exception à l'alinéa 1^{er}, le projet de décision n'est pas envoyé au préalable à l'entité concernée dans des cas exceptionnels, dûment motivés, où cela entraverait une intervention immédiate pour prévenir un incident ou y répondre.

§ 4. Après que l'entité concernée a pu faire valoir ses moyens de défense, à la fin du délai visé au paragraphe 3, alinéa 1^{er}, ou dans le cas visé au paragraphe 3, alinéa 2, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente maintient ou modifie le projet de décision visé au paragraphe 2, alinéa 1^{er} ou y renonce, en tenant compte de la catégorie d'entité à laquelle appartient l'entité concernée, des moyens de défense de cette dernière et des éléments visés à l'article 54.

Mits de nationale cyberbeveiligingsautoriteit akkoord gaat, kan de sectorale overheid administratieve maatregelen en geldboetes, als bedoeld in afdeling 2, opleggen aan een entiteit.

De nationale cyberbeveiligingsautoriteit informeert de betrokken sectorale overheid wanneer zij overweegt om administratieve maatregelen en geldboetes, als bedoeld in artikel 58 en 59, op te leggen aan een entiteit.

Wanneer de autoriteiten bedoeld in het eerste en tweede lid er tijdens hun toezichtsovereenkomst kennis van krijgen dat een in het eerste of tweede lid bedoelde inbreuk door een essentiële of belangrijke entiteit een inbreuk in verband met persoonsgegevens zoals gedefinieerd in artikel 4, 12), van Verordening (EU) 2016/679 kan inhouden, die op grond van artikel 33 van die verordening moet worden gemeld, stellen zij de bevoegde gegevensbeschermingsautoriteiten daarvan onverwijld in kennis.

§ 2. Op basis van het in paragraaf 1 bedoelde proces-verbaal en, in voorkomend geval, van de relevante verslagen bedoeld in artikel 49, § 1, kan de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid een ontwerp van beslissing opstellen dat minstens de referenties van het proces-verbaal dat de inbreuk vaststelt en de feiten beschrijft die aanleiding hebben gegeven tot de procedure, en een of meer overwogen administratieve maatregelen of geldboetes als bedoeld in artikel 58 en/of 59 bevat, alsook de termijn waarbinnen de betrokken entiteit de administratieve maatregelen zou uitvoeren.

De in het eerste lid bedoelde termijn wordt bepaald rekening houdend met de werkingsomstandigheden van de entiteit en de te nemen maatregelen.

§ 3. De nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid verstuurt het in paragraaf 2 bedoelde ontwerp van beslissing naar de betrokken entiteit, met een gedetailleerde motivering voor de overwogen administratieve maatregelen en/of geldboetes, en laat haar weten dat zij het recht heeft om, binnen vijftien dagen na ontvangst van deze informatie, haar verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. De informatie wordt geacht te zijn ontvangen door de overtreder de zesde dag na de verzending van voormeld ontwerp van beslissing.

In afwijking van het eerste lid wordt het ontwerp van beslissing niet vooraf naar de betrokken entiteit gestuurd in naar behoren gemotiveerde uitzonderlijke gevallen waarin een onmiddellijk optreden om incidenten te voorkomen of erop te reageren anders zou worden belemmerd.

§ 4. Nadat de betrokken entiteit haar verweermiddelen heeft kunnen aanvoeren, op het einde van de termijn bedoeld in paragraaf 3, eerste lid, of in het geval bedoeld in paragraaf 3, tweede lid, zal de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid het ontwerp van beslissing bedoeld in paragraaf 2, eerste lid, handhaven, wijzigen of ervan afzien, rekening houdend met de entiteitscategorie waartoe de betrokken entiteit behoort, de verweermiddelen van deze laatste en de in artikel 54 bedoelde elementen.

Art. 52. § 1^{er}. Lorsqu'une entité essentielle ne se conforme pas à la ou aux mesures contenues dans la décision visée à l'article 51, § 4, l'autorité qui a pris cette décision constate les faits dans un procès-verbal.

§ 2. Sur la base du procès-verbal visé au paragraphe 1^{er}, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente rédige un projet de décision contenant au moins une ou plusieurs mesures ou amendes administratives visées aux articles 59 et/ou 60 envisagées.

§ 3. L'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente envoie le projet de décision visé au paragraphe 2 à l'entité concernée en exposant, en détail, les motifs relatifs aux mesures et/ou amende administratives envisagées et lui fait part de son droit, dans les quinze jours de la réception de cette information, de formuler par écrit ses moyens de défense ou de solliciter d'être d'entendu. L'information est présumée reçue par le contrevenant le sixième jour suivant l'envoi du projet de décision précité.

Par exception à l'alinéa 1^{er}, le projet de décision n'est pas envoyé au préalable à l'entité concernée dans des cas exceptionnels, dûment motivés, où cela entraverait une intervention immédiate pour prévenir un incident ou y répondre.

§ 4. Après que l'entité concernée ait pu faire valoir ses moyens de défense, à la fin du délai visé au paragraphe 3, alinéa 1^{er}, ou dans le cas visé au paragraphe 3, alinéa 2, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente maintient ou modifie le projet de décision visé au paragraphe 2 ou y renonce en tenant compte des moyens de défense de l'entité concernée et des éléments visés à l'article 54.

Art. 53. Les procès-verbaux rédigés par les membres assermentés du service d'inspection font foi jusqu'à preuve du contraire.

Art. 54. § 1^{er}. Lorsqu'elle prend toute mesure d'exécution dans le cadre des procédures visées aux articles 51 et 52, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente respecte les droits de la défense, tient compte des circonstances propres à chaque cas et, au minimum, tient dûment compte:

1° de la catégorie visée aux articles 9 et 10 à laquelle l'entité concernée appartient;

2° de la gravité de la violation et de l'importance des dispositions enfreintes, les faits suivants, entre autres, devant être considérés en tout état de cause comme graves:

- a) les violations répétées;
- b) le fait de ne pas notifier des incidents significatifs ou de ne pas y remédier;

Art. 52. § 1. Indien een essentiële entiteit geen gevolg geeft aan een of meer maatregelen vermeld in de beslissing bedoeld in artikel 51, § 4, stelt de autoriteit die deze beslissing heeft genomen de feiten vast in een proces-verbaal.

§ 2. Op basis van het in paragraaf 1 bedoelde proces-verbaal stelt de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid een ontwerp van beslissing op dat minstens een of meer overwogen administratieve maatregelen of geldboetes als bedoeld in artikel 59 en/of 60 bevat.

§ 3. De nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid verstuurt het in paragraaf 2 bedoelde ontwerp van beslissing naar de betrokken entiteit, met een gedetailleerde motivering voor de overwogen administratieve maatregelen en/of geldboetes, en laat haar weten dat zij het recht heeft om, binnen vijftien dagen na ontvangst van deze informatie, haar verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. De informatie wordt geacht te zijn ontvangen door de overtreder de zesde dag na de verzending van voormeld ontwerp van beslissing.

In afwijking van het eerste lid wordt het ontwerp van beslissing niet vooraf naar de betrokken entiteit gestuurd in naar behoren gemotiveerde uitzonderlijke gevallen waarin een onmiddellijk optreden om incidenten te voorkomen of erop te reageren anders zou worden belemmerd.

§ 4. Nadat de betrokken entiteit haar verweermiddelen heeft kunnen aanvoeren, op het einde van de termijn bedoeld in paragraaf 3, eerste lid, of in het geval bedoeld in paragraaf 3, tweede lid, zal de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid het in paragraaf 2 bedoelde ontwerp van beslissing handhaven, wijzigen of ervan afzien, rekening houdend met de verweermiddelen van de betrokken entiteit en de in artikel 54 bedoelde elementen.

Art. 53. De processen-verbaal van de beëdigde leden van de inspectiedienst hebben bewijskracht tot het tegendeel is bewezen.

Art. 54. § 1. Bij het nemen van de handhavingsmaatregelen in het kader van de in artikel 51 en 52 bedoelde procedures eerbiedigt de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid de rechten van de verdediging, houdt zij rekening met de omstandigheden van elk afzonderlijk geval en houdt zij ten minste naar behoren rekening met:

1° de in artikel 9 en 10 bedoelde categorie waartoe de betrokken entiteit behoort;

2° de ernst van de inbreuk en het belang van de geschonden bepalingen, waarbij onder meer het volgende in ieder geval een ernstige inbreuk vormt:

- a) herhaalde inbreuken;
- b) het niet melden of niet verhelpen van significante incidenten;

c) le fait de ne pas pallier les insuffisances à la suite d'instructions contraignantes des autorités compétentes;

d) le fait d'entraver des audits ou des activités de contrôle ordonnées par le service d'inspection de l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent à la suite de la constatation d'une violation;

e) la fourniture d'informations fausses ou manifestement inexactes relatives aux mesures de gestion des risques en matière de cybersécurité ou aux notifications d'incidents prévues au titre 3;

3° de la durée de la violation;

4° de toute violation antérieure pertinente commise par l'entité concernée;

5° des dommages matériels, corporels ou moraux causés, y compris des pertes financières ou économiques, des effets sur d'autres services et du nombre d'utilisateurs touchés;

6° du fait que l'auteur de la violation a agi délibérément ou par négligence;

7° des mesures prises par l'entité pour prévenir ou atténuer les dommages matériels, corporels ou moraux;

8° de l'application de codes de conduite approuvés ou de mécanismes de certification approuvés;

9° du degré de coopération avec le service d'inspection de l'autorité nationale de cybersécurité ou avec l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent des personnes physiques ou morales tenues pour responsables.

§ 2. Lorsque les Autorités de protection des données imposent une amende administrative en vertu de l'article 58, paragraphe 2, point i), du règlement (UE) 2016/679, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente n'impose pas d'amende administrative pour une violation découlant du même comportement que celui qui a fait l'objet d'une amende administrative au titre de l'article 58, paragraphe 2, point i), dudit règlement.

Art. 55. § 1^{er}. Les décisions visées aux articles 51 et 52 sont notifiées par envoi recommandé au contrevenant.

§ 2. Les amendes administratives imposées par une décision visée à l'article 51 ou 52 doivent être acquittées dans les soixante jours qui suivent la réception de l'envoi recommandé visé au paragraphe 1^{er}.

Ce délai peut être augmenté en fonction du montant de l'amende administrative.

c) het niet verhelpen van tekortkomingen naar aanleiding van bindende aanwijzingen van de bevoegde autoriteiten;

d) het belemmeren van audits of monitoringsactiviteiten waartoe de inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst opdracht heeft gegeven naar aanleiding van de vaststelling van een inbreuk;

e) het verstrekken van valse of zeer onnauwkeurige informatie met betrekking tot de maatregelen voor het beheer van cyberbeveiligingsrisico's of de in titel 3 bedoelde melding van incidenten;

3° de duur van de inbreuk;

4° eventuele relevante eerdere inbreuken door de betrokken entiteit;

5° elke veroorzaakte materiële of immateriële schade, met inbegrip van elke financiële of economische schade, gevolgen voor andere diensten en het aantal getroffen gebruikers;

6° opzet of nalatigheid van de pleger van de inbreuk;

7° door de entiteit genomen maatregelen om de materiële of immateriële schade te voorkomen of te beperken;

8° de naleving van goedgekeurde gedragscodes of goedgekeurde certificeringsmechanismen;

9° de mate waarin de aansprakelijk gestelde natuurlijke of rechtspersonen meewerken met de inspectiedienst van de nationale cyberbeveiligingsautoriteit of met de eventuele bevoegde sectorale overheid of sectorale inspectiedienst.

§ 2. Indien de Gegevensbeschermingsautoriteiten een administratieve geldboete opleggen op grond van artikel 58, lid 2, punt i), van Verordening (EU) 2016/679, legt de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid geen geldboete op voor een inbreuk die voortvloeit uit dezelfde gedraging als die waarvoor een administratieve geldboete uit hoofde van artikel 58, lid 2, punt i), van die verordening is opgelegd.

Art. 55. § 1. De in artikel 51 en 52 bedoelde beslissingen worden bij aangetekende zending ter kennis gebracht van de overtreder.

§ 2. De geldboetes die worden opgelegd door een in artikel 51 of 52 bedoelde beslissing, moeten worden betaald binnen de zestig dagen na ontvangst van de in paragraaf 1 bedoelde aangetekende zending.

Deze termijn kan verlengd worden in functie van het bedrag van de geldboete.

Le délai visé à l'alinéa 1^{er} est réputé commencer au plus tard six jours après l'envoi recommandé visé au paragraphe 1^{er}.

§ 3. Lorsqu'une décision visée à l'article 51 ou 52 impose une mesure administrative autre qu'une amende administrative, cette décision précise le délai endéans lequel la mesure doit être exécutée.

§ 4. L'autorité nationale de cybersécurité et, le cas échéant, l'éventuelle autorité sectorielle se communiquent mutuellement leur décision visée à l'article 51 ou 52.

Art. 56. § 1^{er}. Lorsque l'entité concernée reste en défaut de payer l'amende administrative dans le délai imparti, la décision d'infliger une amende administrative a force exécutoire et l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente peut décerner une contrainte.

La contrainte est décernée par un représentant légal de l'autorité nationale de cybersécurité ou de l'éventuelle autorité sectorielle compétente ou par un membre du personnel habilité à cette fin.

§ 2. La contrainte est signifiée au contrevenant par exploit d'huissier de justice. La signification contient un commandement de payer dans les quarante-huit heures, à peine d'exécution par voie de saisie, de même qu'une justification comptable des sommes exigées ainsi que copie de l'exécutoire.

§ 3. Le contrevenant peut former opposition à la contrainte devant le juge des saisies.

L'opposition est motivée à peine de nullité. Elle est formée au moyen d'une citation de l'autorité nationale de cybersécurité ou de l'éventuelle autorité sectorielle compétente signifiée par exploit d'huissier dans les quinze jours à partir de la signification de la contrainte.

Les dispositions du chapitre VIII de la première partie du Code judiciaire sont applicables à ce délai, y compris les prorogations prévues à l'article 50, alinéa 2, et à l'article 55 de ce Code.

L'exercice de l'opposition à la contrainte suspend l'exécution de celle-ci, ainsi que la prescription des créances contenues dans la contrainte, jusqu'à ce qu'il ait été statué sur son bien-fondé. Les saisies déjà pratiquées antérieurement conservent leur caractère conservatoire.

§ 4. L'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente peut faire pratiquer la saisie conservatoire et exécuter la contrainte en usant des voies d'exécution prévues à la cinquième partie du Code judiciaire.

Les paiements partiels effectués en suite de la signification d'une contrainte ne font pas obstacle à la continuation des poursuites.

De in het eerste lid bedoelde termijn wordt geacht in te gaan uiterlijk zes dagen na de in paragraaf 1 bedoelde aangetekende zending.

§ 3. Wanneer een in artikel 51 of 52 bedoelde beslissing een andere administratieve maatregel dan een administratieve geldboete oplegt, vermeldt deze beslissing de termijn waarbinnen de maatregel moet worden uitgevoerd.

§ 4. De nationale cyberbeveiligingsautoriteit en, desgevalend, de eventuele sectorale overheid wisselen hun in artikel 51 of 52 bedoelde beslissing uit.

Art. 56. § 1. Als de betrokken entiteit de administratieve geldboete niet betaalt binnen de gestelde termijn, is de beslissing om een administratieve geldboete op te leggen uitvoerbaar en kan de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid een dwangbevel uitvaardigen.

Het dwangbevel wordt uitgevaardigd door een wettelijke vertegenwoordiger van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of door een daartoe gemachtigd personeelslid.

§ 2. Het dwangbevel wordt aan de overtreder bij gerechtsdeurwaarderexploot betekend. De betekening bevat een bevel om te betalen binnen achtenveertig uur op straffe van tenuitvoerlegging door beslag, alsook een boekhoudkundige verantwoording van de gevorderde bedragen en een afschrift van de uitvoerbaarverklaring.

§ 3. De overtreder kan tegen het dwangbevel verzet aantekenen bij de beslagrechter.

Het verzet is, op straffe van nietigheid, met redenen omkleed. Het moet worden ingediend door middel van een dagvaarding van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid bij gerechtsdeurwaarderexploot binnen vijftien dagen te rekenen vanaf de betekening van het dwangbevel.

De bepalingen van hoofdstuk VIII van het eerste deel van het Gerechtelijk Wetboek zijn van toepassing op deze termijn, met inbegrip van de verlengingen bepaald in artikel 50, tweede lid, en artikel 55 van dit Wetboek.

De uitoefening van verzet tegen het dwangbevel schorst de tenuitvoerlegging hiervan, alsook de verjaring van de schuldvorderingen opgenomen in het dwangbevel, tot uitspraak is gedaan over de gegrondheid ervan. De reeds eerder gelegde beslagen behouden hun bewarend karakter.

§ 4. De nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid mag bewarend beslag laten leggen en het dwangbevel uitvoeren met gebruikmaking van de middelen tot tenuitvoerlegging bepaald in het vijfde deel van het Gerechtelijk Wetboek.

De gedeeltelijke betalingen gedaan ingevolge de betekening van een dwangbevel verhinderen de voortzetting van de vervolging niet.

§ 5. Les frais de signification de la contrainte de même que les frais de l'exécution ou des mesures conservatoires sont à charge du contrevenant.

Ils sont déterminés suivant les règles établies pour les actes accomplis par les huissiers de justice en matière civile et commerciale.

Art. 57. L'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente ne peut imposer de mesures administratives ni d'amendes administratives à l'échéance d'un délai de trois ans, à compter du jour où le fait a été commis.

Le paiement selon la procédure administrative éteint également la possibilité d'engager des poursuites pénales pour les faits visés.

Section 2. Mesures et amendes administratives

Art. 58. Les mesures administratives suivantes peuvent être imposées aux entités sur la base de l'article 51:

1° émettre des avertissements concernant les violations de la présente loi par les entités concernées;

2° adopter des instructions contraignantes ou une injonction exigeant des entités concernées qu'elles remédient aux insuffisances constatées ou aux violations de la présente loi;

3° ordonner aux entités concernées de mettre un terme à un comportement qui viole la présente loi et de ne pas le réitérer;

4° ordonner aux entités concernées de garantir la conformité de leurs mesures de gestion des risques en matière de cybersécurité avec le titre 3 ou de respecter les obligations en matière de notification d'incidents énoncées au même titre, de manière spécifique et dans un délai déterminé;

5° ordonner aux entités concernées d'informer les personnes physiques ou morales à l'égard desquelles elles fournissent des services ou exercent des activités susceptibles d'être affectées par une cybermenace importante de la nature de la menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace;

6° ordonner aux entités concernées de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable;

7° ordonner aux entités concernées de rendre publics les aspects de violations de la présente loi de manière spécifique;

8° lorsque l'entité concernée est une entité essentielle, désigner, pour une période déterminée, un responsable du contrôle ayant des tâches bien définies pour superviser le respect, par les entités concernées, des mesures de gestion

§ 5. De betekeniskosten van het dwangbevel evenals de kosten van tenuitvoerlegging of van bewarende maatregelen zijn ten laste van de overtreder.

Ze worden bepaald volgens de regels die gelden voor de akten van gerechtsdeurwaarders in burgerlijke zaken en handelszaken.

Art. 57. De nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid kan geen administratieve maatregelen of administratieve geldboetes opleggen na het verstrijken van een termijn van drie jaar, te rekenen vanaf de dag waarop het feit werd gepleegd.

De betaling volgens de administratieve procedure doet ook de mogelijkheid vervallen om strafrechtelijke vervolging in te stellen voor de bedoelde feiten.

Afdeling 2. Administratieve maatregelen en geldboetes

Art. 58. De volgende administratieve maatregelen kunnen aan entiteiten worden opgelegd op basis van artikel 51:

1° waarschuwingen geven over inbreuken door de betrokken entiteiten op deze wet;

2° bindende aanwijzingen vaststellen of een bevel uitvaardigen waarin de betrokken entiteiten worden verplicht de vastgestelde tekortkomingen of de inbreuken op deze wet te verhelpen;

3° de betrokken entiteiten gelasten een einde te maken aan gedragingen die inbreuk maken op deze wet en af te zien van herhaling van die gedragingen;

4° de betrokken entiteiten gelasten er op een gespecificeerde wijze en binnen een gespecificeerde termijn voor te zorgen dat hun maatregelen voor het beheer van cyberbeveiligingsrisico's in overeenstemming zijn met titel 3 of te voldoen aan de verplichtingen inzake het melden van incidenten bedoeld in dezelfde titel;

5° de betrokken entiteiten gelasten de natuurlijke of rechtspersonen aan wie zij diensten verlenen of voor wie zij activiteiten uitvoeren die mogelijkwerijs door een significante cyberdreiging worden beïnvloed, in kennis te stellen van de aard van de dreiging en van alle mogelijke beschermings- of herstelmaatregelen die deze natuurlijke of rechtspersonen kunnen nemen als reactie op die dreiging;

6° de betrokken entiteiten gelasten de naar aanleiding van een beveiligingsaudit gedane aanbevelingen binnen een redelijke termijn uit te voeren;

7° de betrokken entiteiten gelasten aspecten van inbreuken op deze wet op een bepaalde manier openbaar te maken;

8° wanneer de betrokken entiteit een essentiële entiteit is, een controlefunctionaris aanwijzen die gedurende een bepaalde periode duidelijk omschreven taken heeft om erop toe te zien dat de betrokken entiteiten voldoen aan de maatregelen voor

des risques en matière de cybersécurité et de notification d'incidents visées au titre 3.

Lorsque l'entité concernée est une entité essentielle, les instructions contraignantes visées à l'alinéa 1^{er}, 2°, concernent également les mesures nécessaires pour éviter un incident ou y remédier, ainsi que les délais pour mettre en œuvre ces mesures et rendre compte de cette mise en œuvre.

Art. 59. Les amendes administratives suivantes peuvent être imposées aux entités sur la base de l'article 51 ou 52:

1° est puni d'une amende de 500 à 125.000 euros qui-
conque ne se conforme pas aux obligations d'information
visées à l'article 11, § 5;

2° est punie d'une amende de 500 à 200.000 euros l'entité
qui fait subir des conséquences négatives à une personne
agissant pour son compte en raison de l'exécution, de bonne
foi et dans le cadre de ses fonctions, des obligations découlant
de la présente loi;

3° Est puni d'une amende de 500 à 200.000 euros qui-
conque ne se conforme pas aux obligations de contrôle visées
au présent titre;

4° est punie d'une amende de 500 à 7.000.000 euros ou
1,4 % du chiffre d'affaires annuel mondial total de l'exercice
précédent de l'entreprise à laquelle l'entité importante appar-
tient, le montant le plus élevé étant retenu, l'entité importante
qui ne se conforme pas aux obligations relatives aux mesures
de gestion des risques en matière de cybersécurité et/ou de
notification d'incidents visées au titre 3;

5° est punie d'une amende de 500 à 10.000.000 euros ou
2 % du chiffre d'affaires annuel mondial total de l'exercice
précédent de l'entreprise à laquelle l'entité essentielle appar-
tient, le montant le plus élevé étant retenu, l'entité essentielle
qui ne se conforme pas aux obligations relatives aux mesures
de gestion des risques en matière de cybersécurité et/ou de
notification d'incidents visées au titre 3.

L'amende administrative est doublée en cas de récidive
pour les mêmes faits dans un délai de trois ans.

Le concours de plusieurs manquements peut donner lieu à
une amende administrative unique proportionnelle à la gravité
de l'ensemble des faits.

Art. 60. A défaut de prendre les mesures nécessaires
dans le délai imposé par le service d'inspection, les mesures
administratives suivantes peuvent être imposées aux entités
essentiels sur la base de l'article 52:

1° demander à l'autorité nationale de cybersécurité de
suspendre temporairement une certification ou une autorisa-
tion concernant tout ou partie des services pertinents fournis
ou des activités pertinentes menées par l'entité concernée;

het beheer van cyberbeveiligingsrisico's en inzake het melden
van incidenten bedoeld in titel 3.

Wanneer de betrokken entiteit een essentiële entiteit is,
omvatten de bindende aanwijzingen bedoeld in het eerste
lid, 2°, ook de maatregelen die nodig zijn om een incident te
voorkomen of te verhelpen, alsmede uiterste termijnen voor de
uitvoering van dergelijke maatregelen en voor verslaggeving
over de uitvoering ervan.

Art. 59. De volgende administratieve geldboetes kunnen
aan entiteiten worden opgelegd op basis van artikel 51 of 52:

1° eenieder die niet voldoet aan de in artikel 11, § 5, bedoelde
rapportageverplichtingen wordt bestraft met een geldboete
van 500 tot 125.000 euro;

2° een entiteit die een persoon die optreedt voor haar
rekening nadelige gevolgen berokkent ingevolge de uitvoe-
ring, te goeder trouw en in het kader van zijn functie, van de
verplichtingen die voortvloeien uit deze wet, wordt bestraft
met een geldboete van 500 tot 200.000 euro;

3° eenieder die niet voldoet aan de in deze titel bedoelde
toezichtverplichtingen wordt bestraft met een geldboete van
500 tot 200.000 euro;

4° een belangrijke entiteit die niet voldoet aan de ver-
plichtingen betreffende de maatregelen voor het beheer van
cyberbeveiligingsrisico's en/of aan de rapportageverplichtingen
bedoeld in titel 3 wordt bestraft met een geldboete van 500
tot 7.000.000 euro of van 1,4 % van de totale wereldwijde
jaaromzet in het voorgaande boekjaar van de onderneming
waartoe de belangrijke entiteit behoort, afhankelijk van welk
bedrag het hoogst is;

5° een essentiële entiteit die niet voldoet aan de verplich-
tingen betreffende de maatregelen voor het beheer van cy-
berbeveiligingsrisico's en/of aan de rapportageverplichtingen
bedoeld in titel 3 wordt bestraft met een geldboete van 500
tot 10.000.000 euro of van 2 % van de totale wereldwijde
jaaromzet in het voorgaande boekjaar van de onderneming
waartoe de essentiële entiteit behoort, afhankelijk van welk
bedrag het hoogst is.

De administratieve geldboete wordt verdubbeld in geval van
herhaling van dezelfde feiten binnen een termijn van drie jaar.

De samenloop van meerdere inbreuken kan aanleiding geven
tot één enkele administratieve geldboete die in verhouding
staat tot de ernst van het geheel van de feiten.

Art. 60. Indien de nodige maatregelen niet binnen de door
de inspectiedienst gestelde termijn worden genomen, kunnen
aan essentiële entiteiten op grond van artikel 52 de volgende
administratieve maatregelen worden opgelegd:

1° de nationale cyberbeveiligingsautoriteit verzoeken een
certificering of vergunning tijdelijk op te schorten met betrek-
king tot alle of een deel van de relevante door de betrokken
entiteit verleende diensten of verrichte activiteiten;

2° interdire temporairement à toute personne physique exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal dans l'entité concernée d'exercer des responsabilités dirigeantes dans cette entité.

Les suspensions ou interdictions temporaires visées à l'alinéa 1^{er} sont uniquement appliquées jusqu'à ce que l'entité concernée ait pris les mesures nécessaires pour remédier aux insuffisances ou se conformer aux exigences de l'autorité compétente à l'origine de l'application de ces mesures d'exécution.

Art. 61. Toute personne physique responsable d'une entité essentielle ou importante ou agissant en qualité de représentant légal d'une entité essentielle ou importante sur la base du pouvoir de la représenter, de prendre des décisions en son nom ou d'exercer son contrôle a le pouvoir de veiller au respect, par l'entité, de la présente loi. Ces personnes sont responsables des manquements à leur devoir de veiller au respect de la présente loi.

Cet article est sans préjudice des règles en matière de responsabilité applicables aux institutions publiques, ainsi que de responsabilité des agents de la fonction publique et des responsables élus ou nommés.

Titre 5. – Dispositions spécifiques au secteur de l'administration publique

Art. 62. Les mesures et amendes administratives visées aux articles 59 et 60 ne s'appliquent pas aux entités faisant partie du secteur de l'administration publique.

Art. 63. § 1^{er}. Le Roi est habilité à désigner une autorité comme organisme d'évaluation de la conformité de tout ou partie des entités de l'administration publique.

§ 2. L'autorité visée au paragraphe 1^{er} est agréée par l'autorité nationale de cybersécurité, selon les modalités fixées par le Roi, afin d'effectuer l'évaluation périodique de la conformité visée à l'article 39, alinéa 1^{er}, 1°.

L'agrément visé à l'alinéa 1^{er} porte sur un ou plusieurs des cadres de référence visés à l'article 39.

Art. 64. Le service d'inspection de l'autorité nationale de cybersécurité ou, le cas échéant, le service d'inspection sectoriel désigné par le Roi pour le secteur de l'administration publique exerce ses tâches de supervision en jouissant d'une indépendance opérationnelle vis-à-vis des entités de l'administration publique supervisées.

Art. 65. L'article 47 est applicable au service d'inspection visé à l'alinéa 1^{er}.

Titre 6. - Traitement des données à caractère personnel

CHAPITRE 1^{ER} – Principes relatifs au traitement

2° een natuurlijke persoon met leidinggevende verantwoordelijkheden op het niveau van de algemeen directeur of de wettelijke vertegenwoordiger in de betrokken entiteit tijdelijk verbieden leidinggevende functies in die entiteit uit te oefenen.

De in het eerste lid bedoelde tijdelijke opschortingen of verboden worden slechts toegepast tot de betrokken entiteit de maatregelen heeft genomen die nodig zijn om de tekortkomingen te verhelpen of te voldoen aan de vereisten van de bevoegde autoriteit die deze handhavingsmaatregelen heeft opgelegd.

Art. 61. Elke natuurlijke persoon die verantwoordelijk is voor of optreedt als wettelijke vertegenwoordiger van een essentiële of een belangrijke entiteit op basis van de bevoegdheid om deze te vertegenwoordigen, de bevoegdheid om namens deze entiteit beslissingen te nemen of de bevoegdheid om controle uit te oefenen op deze entiteit, heeft de bevoegdheid om ervoor te zorgen dat deze entiteit deze wet nakomt. Deze personen zijn aansprakelijk voor het niet nakomen van hun verplichtingen om te zorgen voor de naleving van deze wet.

Dit artikel doet geen afbreuk aan de aansprakelijkheidsregels die gelden voor overheidsinstanties, alsook voor ambtenaren en verkozen of benoemde mandatarissen.

Titel 5. - Specifieke bepalingen voor de overheidssector

Art. 62. De administratieve maatregelen en geldboetes bedoeld in artikel 59 en 60 zijn niet van toepassing op entiteiten die deel uitmaken van de overheidssector.

Art. 63. § 1. De Koning wordt gemachtigd een autoriteit aan te wijzen als conformiteitsbeoordelingsinstantie voor alle of een deel van de overheidsinstanties.

§ 2. De in paragraaf 1 bedoelde autoriteit wordt erkend door de nationale cyberbeveiligingsautoriteit, volgens de door de Koning bepaalde modaliteiten, om de in artikel 39, eerste lid, 1°, bedoelde regelmatige conformiteitsbeoordeling uit te voeren.

De in het eerste lid bedoelde erkenning heeft betrekking op een of meer van de in artikel 39 bedoelde referentiekaders.

Art. 64. De inspectiedienst van de nationale cyberbeveiligingsautoriteit of, in voorkomend geval, de sectorale inspectiedienst die door de Koning is aangewezen voor de overheidssector, is bij de uitvoering van zijn toezichthoudende taken operationeel onafhankelijk van de overheidsinstanties waarop hij toezicht houdt.

Art. 65. Artikel 47 is van toepassing op de inspectiedienst bedoeld in het eerste lid.

Titel 6. - Verwerking van persoonsgegevens

HOOFDSTUK 1 – Beginselen betreffende de verwerking

Art. 66. Les définitions du règlement (UE) 2016/679 sont d'application pour le présent titre.

Art. 67. Les finalités pour lesquelles des traitements de données à caractère personnel sont effectués, sont les suivantes:

1° l'amélioration de la cybersécurité à travers la recherche d'un niveau accru de protection des réseaux et systèmes d'information, le renforcement des politiques de prévention et de sécurité, la prévention des incidents de sécurité et la défense contre les cybermenaces;

2° l'exécution des tâches de l'autorité nationale de cybersécurité, notamment l'identification des entités, l'information et la sensibilisation des utilisateurs des systèmes d'information et de communication, l'octroi de subventions, la coopération internationale entre l'autorité nationale de cybersécurité, des autorités compétentes des autres États membres, des forums internationaux de cybersécurité, l'ENISA et la Commission européenne;

3° la gestion des crises et incidents de cybersécurité;

4° l'exécution des tâches du CSIRT national visées aux articles suivants:

- a) 19, § 1^{er};
- b) 21, § 2, al. 2, 1° à 3°;
- c) 22, § 2 à § 6;
- d) 37, § 1^{er} à § 3, et § 5;

5° la coopération, notamment l'échange d'informations entre l'autorité nationale de cybersécurité, les éventuelles autorités sectorielles, le NCCN et les autorités compétentes dans le cadre de la loi CER, ainsi que les autorités visées à l'article 25, § 2 dans le cadre de l'exécution de la présente loi et la loi CER;

6° la coopération entre les entités essentielles et importantes et les autorités visées au titre 2, chapitre 1^{er};

7° le partage d'informations entre les autorités visées à l'article 25, § 5;

8° la continuité des services prestés par les entités importantes ou essentielles;

9° la notification d'incidents et d'incidents évités;

10° le contrôle et la supervision des entités essentielles et importantes, ainsi que la préparation, l'organisation, la gestion et le suivi de mesures et d'amendes administratives.

Art. 68. Les catégories de données à caractère personnel traitées par les responsables de traitement sont les suivantes:

Art. 66. De definities van Verordening (EU) 2016/679 zijn van toepassing op deze titel.

Art. 67. De verwerking van persoonsgegevens vindt plaats voor de volgende doeleinden:

1° de verbetering van de cyberbeveiliging dankzij een betere bescherming van de netwerk- en informatiesystemen, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsincidenten en de bescherming tegen cyberdreigingen;

2° de uitvoering van de taken van de nationale cyberbeveiligingsautoriteit, met name het identificeren van de entiteiten, het informeren en sensibiliseren van gebruikers van informatie- en communicatiesystemen, het toekennen van subsidies, de internationale samenwerking tussen de nationale cyberbeveiligingsautoriteit, de bevoegde autoriteiten van andere lidstaten, internationale fora voor cyberbeveiliging, Enisa en de Europese Commissie;

3° het beheer van cyberbeveiligingscrises en -incidenten;

4° de uitvoering van de taken van het nationale CSIRT bedoeld in de volgende artikelen:

- a) 19, § 1;
- b) 21, § 2, tweede lid, 1° tot 3°;
- c) 22, § 2 tot § 6;
- d) 37, § 1 tot § 3, en § 5;

5° de samenwerking, met name de informatie-uitwisseling tussen de nationale cyberbeveiligingsautoriteit, de eventuele sectorale overheden, het NCCN en de autoriteiten die bevoegd zijn in het kader van de CER-wet, alsook de autoriteiten bedoeld in artikel 25, § 2, in het kader van de uitvoering van deze wet en de CER-wet;

6° de samenwerking tussen essentiële en belangrijke entiteiten en de autoriteiten bedoeld in titel 2, hoofdstuk 1;

7° het delen van informatie tussen de autoriteiten bedoeld in artikel 25, § 5;

8° de continuïteit van de dienstverlening door belangrijke of essentiële entiteiten;

9° het melden van incidenten en bijna-incidenten;

10° de controle van en het toezicht op essentiële en belangrijke entiteiten, alsook de voorbereiding, de organisatie, het beheer en de opvolging van administratieve maatregelen en geldboetes.

Art. 68. De verwerkingsverantwoordelijken verwerken de volgende categorieën van persoonsgegevens:

1° pour la finalité visée à l'article 67, 1°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par les missions d'amélioration de la cybersécurité, de renforcement des politiques de prévention et de sécurité, de prévention des incidents de sécurité et de défense contre les cybermenaces visées à l'article 67, 1°;

2° pour la finalité visée à l'article 67, 2°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par l'exécution des tâches de l'autorité nationale de cybersécurité;

3° pour la finalité visée à l'article 67, 3°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par les crises et incidents de cybersécurité;

4° pour la finalité visée à l'article 67, 4°: les données d'identification, de connexion, de localisation, de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005 et des métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi précitée du 13 juin 2005, des personnes concernées par l'exécution des tâches du CSIRT;

5° pour la finalité visée à l'article 67, 5°: les données d'identification des personnes concernées par la coopération dans le cadre de la loi CER;

6° pour la finalité visée à l'article 67, 6°: les données d'identification des personnes concernées par la coopération;

7° pour la finalité visée à l'article 67, 7°: les données d'identification des personnes concernées par le partage d'informations;

8° pour la finalité visée à l'article 67, 8°: les données d'identification des personnes concernées par l'assurance d'une continuité des services;

9° pour la finalité visée à l'article 67, 9°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par l'exercice de notification;

10° pour la finalité visée à l'article 67, 10°: les données à caractère personnel nécessaires et pertinentes à l'exercice des missions de contrôle, de supervision et de sanction, des personnes concernées par ces contrôles, cette supervision ou ces sanctions.

Art. 69. Les catégories de personnes dont les données à caractère personnel sont susceptibles de faire l'objet de traitement sont les suivantes:

1° voor het doeleinde bedoeld in artikel 67, 1°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij de opdrachten rond de verbetering van de cyberbeveiliging, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsincidenten en de bescherming tegen cyberdreigingen bedoeld in artikel 67, 1°;

2° voor het doeleinde bedoeld in artikel 67, 2°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij de uitvoering van de taken van de nationale cyberbeveiligingsautoriteit;

3° voor het doeleinde bedoeld in artikel 67, 3°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij cyberbeveiligingscrises en -incidenten;

4° voor het doeleinde bedoeld in artikel 67, 4°: de identificatie-, verbindings-, locatie-, elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, en elektronische-communicatiemetagegegevens als bedoeld in artikel 2, 93°, van voornoemde wet van 13 juni 2005, van de personen die betrokken zijn bij de uitvoering van de taken van het CSIRT;

5° voor het doeleinde bedoeld in artikel 67, 5°: de identificatiegegevens van de personen die betrokken zijn bij de samenwerking in het kader van de CER-wet;

6° voor het doeleinde bedoeld in artikel 67, 6°: de identificatiegegevens van de personen die betrokken zijn bij de samenwerking;

7° voor het doeleinde bedoeld in artikel 67, 7°: de identificatiegegevens van de personen die betrokken zijn bij het delen van informatie;

8° voor het doeleinde bedoeld in artikel 67, 8°: de identificatiegegevens van de personen die betrokken zijn bij het waarborgen van de continuïteit van de dienstverlening;

9° voor het doeleinde bedoeld in artikel 67, 9°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij de melding;

10° voor het doeleinde bedoeld in artikel 67, 10°: de persoonsgegevens die nodig en relevant zijn voor de uitoefening van de controle-, toezichts- en sanctieopdrachten, van de personen die betrokken zijn bij deze controles, dit toezicht of deze sancties.

Art. 69. De persoonsgegevens van de volgende categorieën van personen kunnen het voorwerp uitmaken van verwerkingen:

1° les personnes participant directement aux missions confiées à l'autorité nationale de cybersécurité en vertu du titre 2;

2° les personnes visées par les obligations qui incombent aux entités essentielles et importantes en vertu du titre 3;

3° les personnes impliquées dans un incident;

4° les personnes directement impliquées dans les exercices de supervision, de contrôle, et de sanction, visés au titre 4.

Art. 70. Les entités suivantes sont responsables des traitements qu'elles effectuent pour la réalisation des finalités visées à l'article 67:

1° l'autorité nationale de cybersécurité;

2° le NCCN;

3° l'éventuelle autorité sectorielle;

4° l'éventuel service d'inspection sectoriel;

5° les entités essentielles et importantes;

6° les entités fournissant des services d'enregistrement de noms de domaine;

7° les autorités visées à l'article 23, § 1^{er}, 6°.

CHAPITRE 2 – Durée de conservation

Art. 71. Les données à caractère personnel traitées dans le cadre des traitements visés par la présente loi en vue de réaliser les finalités prévues à l'article 67, sont conservées, sans préjudice de recours éventuels, par le responsable du traitement cinq ans après la fin du dernier traitement effectué et 10 ans maximum après le premier traitement effectué.

CHAPITRE 3 – Limitation des droits des personnes concernées

Art. 72. § 1^{er}. En application de l'article 23.1, a), b), c), d), e), h), du règlement (UE) 2016/679, certaines obligations et droits prévus par ledit règlement sont limités ou exclus, conformément aux dispositions du présent chapitre. Ces limitations ou exclusions ne peuvent porter préjudice à l'essence des libertés et droits fondamentaux et doivent être appliquées dans la stricte mesure nécessaire au but poursuivi.

§ 2. Les articles 12 à 16, 18 et 19 dudit règlement ne sont pas applicables aux traitements de données à caractère personnel effectués par une autorité visée à l'article 15 pour la finalité visée à l'article 67, 10°, dans la mesure où l'exercice

1° de personen die rechtstreeks deelnemen aan de opdrachten die krachtens titel 2 zijn toevertrouwd aan de nationale cyberbeveiligingsautoriteit;

2° de personen bedoeld in het kader van de verplichtingen voor essentiële en belangrijke entiteiten die voortvloeien uit titel 3;

3° de personen die betrokken zijn bij een incident;

4° de personen die rechtstreeks betrokken zijn bij het toezicht, de controle en de sancties bedoeld in titel 4.

Art. 70. De volgende entiteiten zijn verantwoordelijk voor de verwerkingen die zij uitvoeren voor de verwezenlijking van de doeleinden bedoeld in artikel 67:

1° de nationale cyberbeveiligingsautoriteit;

2° het NCCN;

3° de eventuele sectorale overheid;

4° de eventuele sectorale inspectiedienst;

5° de essentiële en belangrijke entiteiten;

6° de entiteiten die domeinnaamregistratiediensten verlenen;

7° de autoriteiten bedoeld in artikel 23, § 1, 6°.

HOOFDSTUK 2 – Bewaartermijn

Art. 71. De verwerkingsverantwoordelijke bewaart de persoonsgegevens die verwerkt worden in het kader van de in deze wet bedoelde verwerkingen om de doeleinden bedoeld in artikel 67 te realiseren, onverminderd eventuele beroepsprocedures, gedurende vijf jaar na afloop van de laatste verwerking en maximaal gedurende tien jaar na de eerste verwerking.

HOOFDSTUK 3 – Beperking van de rechten van de betrokkenen

Art. 72. § 1. Met toepassing van artikel 23.1, a), b), c), d), e), h), van Verordening (EU) 2016/679 worden sommige verplichtingen en rechten van deze verordening beperkt of uitgesloten, overeenkomstig de bepalingen van dit hoofdstuk. Deze beperkingen of uitsluitingen mogen geen afbreuk doen aan de wezenlijke inhoud van de grondrechten en fundamentele vrijheden en moeten worden toegepast voor zover dit strikt noodzakelijk is voor het nagestreefde doel.

§ 2. De artikelen 12 tot 16, 18 en 19 van voornoemde verordening zijn niet van toepassing op verwerkingen van persoonsgegevens die worden verricht door een autoriteit bedoeld in artikel 15 voor het doeleinde bedoeld in artikel 67,

des droits consacrés par ces articles nuirait aux besoins du contrôle, de la supervision ou des actes préparatoires à celui-ci.

§ 3. L'exemption vaut pour les catégories de données à caractère personnel visées à l'article 68, 10°. Cette exemption vaut également pour les actes préparatoires ou pour les procédures visant à l'application éventuelle d'une sanction administrative.

§ 4. L'exemption ne s'applique que pendant la période au cours de laquelle la personne concernée fait l'objet d'un contrôle, d'une supervision ou d'actes préparatoires à ceux-ci, dans la mesure où l'exercice des droits faisant l'objet de la dérogation visée au présent article nuirait aux besoins du contrôle, de la supervision ou des actes préparatoires à ceux-ci et, en tous les cas, ne s'applique que jusqu'à un an après le début d'un contrôle, d'une supervision ou d'actes préparatoires à ceux-ci.

La durée des actes préparatoires, visés à l'alinéa 1^{er}, pendant laquelle les articles visés au paragraphe 2 ne sont pas applicables, ne peut excéder un an à partir de la réception d'une demande relative à l'application d'un des droits consacrés par ces articles.

§ 5. Le responsable du traitement qui ne se conforme pas à toutes les dispositions du présent titre et en particulier de l'article 73, ne peut bénéficier de l'exemption.

Art. 73. § 1^{er}. Le responsable du traitement concerné donne accès à la personne concernée à des informations limitées concernant le traitement de ses données à caractère personnel, pour autant que cette communication ne compromette pas la réalisation des objectifs de la présente loi et de manière telle que la personne concernée se trouve dans l'impossibilité de savoir si elle fait l'objet d'une enquête ou pas, et sans pouvoir en aucun cas rectifier, effacer, limiter, notifier, transmettre à un tiers des données à caractère personnel, ni cesser toute forme de traitement desdites données qui soit nécessaire dans le cadre défini ci-avant.

§ 2. La mesure de refus ou de limitation des droits consacrés par les articles visés à l'article 72, § 2, doit être levée:

1° pour les mesures justifiées par les obligations en matière de notification d'incidents, lors de la clôture du traitement d'un incident par les autorités visées aux articles 34 et 38;

2° pour les mesures justifiées par les obligations en vertu du titre 4, lors de la clôture du contrôle, de la supervision ou des actes préparatoires à ceux-ci effectués par le service d'inspection, ainsi que pendant la période durant laquelle l'éventuelle autorité sectorielle traite les pièces provenant du service d'inspection en vue d'exercer des poursuites;

3° au plus tard un an à partir de la réception de la demande introduite en application des articles visés à l'article 72, § 2, sauf si un contrôle ou une supervision sont en cours.

10°, pour zover de uitoefening van de in deze artikelen vastgelegde rechten nadelig zou zijn voor de controle, het toezicht of de voorbereidende werkzaamheden ervan.

§ 3. De vrijstelling geldt voor de categorieën van persoonsgegevens bedoeld in artikel 68, 10°. Deze vrijstelling geldt ook voor voorbereidende werkzaamheden of procedures met het oog op de eventuele toepassing van een administratieve sanctie.

§ 4. De vrijstelling geldt enkel voor de periode tijdens dewelke de betrokkene onderworpen is aan een controle, toezicht of de voorbereidende werkzaamheden ervan, voor zover de uitoefening van de rechten die het voorwerp uitmaken van de in dit artikel bedoelde afwijking nadelig zou zijn voor de controle, het toezicht of de voorbereidende werkzaamheden ervan. In ieder geval geldt ze slechts maximaal één jaar na aanvang van een controle, toezicht of de voorbereidende werkzaamheden ervan.

De duur van de voorbereidende werkzaamheden bedoeld in het eerste lid, tijdens dewelke de in paragraaf 2 bedoelde artikelen niet van toepassing zijn, is beperkt tot maximaal één jaar na ontvangst van een verzoek betreffende de toepassing van een van de in deze artikelen vastgelegde rechten.

§ 5. De verwerkingsverantwoordelijke die niet voldoet aan alle bepalingen van deze titel en met name van artikel 73, kan geen gebruik maken van de vrijstelling.

Art. 73. § 1. De betrokken verwerkingsverantwoordelijke verleent de betrokkene toegang tot beperkte informatie over de verwerking van zijn persoonsgegevens, voor zover deze kennisgeving de verwezenlijking van de doelstellingen van deze wet niet in het gedrang brengt. Hierbij moet het voor de betrokkene onmogelijk zijn om na te gaan of hij al dan niet het voorwerp uitmaakt van een onderzoek, en kan hij in geen geval persoonsgegevens rechtzetten, wissen, beperken, meedelen, of aan derden overdragen, noch enige vorm van verwerking van voormelde gegevens die in het bovenvermelde kader noodzakelijk is, stopzetten.

§ 2. De maatregel betreffende de weigering of beperking van de rechten die zijn vastgelegd in de artikelen bedoeld in artikel 72, § 2, moet worden opgeheven:

1° voor maatregelen die gerechtvaardigd zijn door de verplichtingen inzake het melden van incidenten, bij het afsluiten van de verwerking van een incident door de autoriteiten bedoeld in artikel 34 en 38;

2° voor maatregelen die gerechtvaardigd zijn door de verplichtingen krachtens titel 4, bij het afsluiten van de controle, het toezicht of de voorbereidende werkzaamheden ervan door de inspectiedienst, alsook in de periode tijdens dewelke de eventuele sectorale overheid de stukken verwerkt die afkomstig zijn van de inspectiedienst met het oog op vervolging;

3° uiterlijk één jaar na ontvangst van het verzoek dat is ingediend overeenkomstig de artikelen bedoeld in artikel 72, § 2, behalve indien een controle of toezicht loopt.

§ 3. Le responsable du traitement concerné lève également la mesure de refus ou de limitation des droits consacrés par les articles visés à l'article 72, § 2, dès qu'une telle mesure n'est plus nécessaire au respect d'une des finalités visées à l'article 67.

§ 4. Dans tous les cas d'application des paragraphes 2 et 3, le délégué à la protection des données informe par écrit la ou les personnes concernées de la levée de la mesure de refus ou de limitation.

CHAPITRE 4 – Limitations aux obligations de notification des violations de données à caractère personnel

Art. 74. Le responsable du traitement concerné est dispensé de communiquer une violation de données à caractère personnel à une ou des personnes concernées bien déterminées, au sens de l'article 34 du règlement (UE) 2016/679, moyennant l'autorisation de l'autorité nationale de cybersécurité, pour autant que et dans la mesure où une telle notification individuelle risque de compromettre la réalisation des finalités visées à l'article 72, § 2.

Titre 7. - Dispositions finales

CHAPITRE 1^{ER} – Disposition transitoire

Art. 75. Le Roi fixe les délais endéans lesquels les entités essentielles effectuent leurs premières évaluations périodiques de la conformité visées à l'article 39.

CHAPITRE 2 – Dispositions modificatives

Section 1^{re}. Modifications de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire

Art. 76. A l'article 1^{er} de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, modifié en dernier lieu par la loi du 19 décembre 2021, les mots “- la loi du 7 avril 2019”: la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;” sont remplacés par les mots “- la loi NIS2: la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;”.

Art. 77. Dans la section 1^{re} du chapitre III de la même loi, l'article 15^{ter}, inséré par la loi du 7 avril 2019, est remplacé par ce qui suit:

“Art. 15^{ter}. L'Agence est désignée comme service d'inspection sectoriel, au sens de la loi NIS2, pour le secteur de l'énergie, en ce qui concerne les mesures supplémentaires de gestion des risques en matière de cybersécurité applicables aux éléments d'une installation nucléaire destinée à la

§ 3. De betrokken verwerkingsverantwoordelijke heft de maatregel betreffende de weigering of beperking van de rechten die zijn vastgelegd in de artikelen bedoeld in artikel 72, § 2, ook op zodra deze maatregel niet meer nodig is voor het nakomen van een van de doeleinden bedoeld in artikel 67.

§ 4. In alle toepassingsgevallen van paragraaf 2 en 3 informeert de functionaris voor gegevensbescherming de betrokkene of betrokkenen schriftelijk dat de maatregel betreffende de weigering of beperking is opgeheven.

HOOFDSTUK 4 – Beperkingen inzake de verplichte melding van inbreuken in verband met persoonsgegevens

Art. 74. De betrokken verwerkingsverantwoordelijke is vrijgesteld van het meedelen van een inbreuk in verband met persoonsgegevens aan een of meer welbepaalde betrokkenen, in de zin van artikel 34 van Verordening EU 2016/679, mits toestemming van de nationale cyberbeveiligingsautoriteit, voor zover deze individuele kennisgeving de verwezenlijking van de doeleinden bedoeld in artikel 72, § 2, in het gedrang zou brengen.

Titel 7. - Slotbepalingen

HOOFDSTUK 1 – Overgangsbepaling

Art. 75. De Koning stelt de termijnen vast waarbinnen essentiële entiteiten hun eerste regelmatige conformiteitsbeoordelingen als bedoeld in artikel 39 uitvoeren.

HOOFDSTUK 2 – Wijzigingsbepalingen

Afdeling 1. Wijzigingen van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle

Art. 76. In artikel 1 van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, het laatst gewijzigd bij de wet van 19 december 2021, worden de woorden “- “de wet van 7 april 2019”: de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;” vervangen door de woorden “- de NIS2-wet: de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;”.

Art. 77. In afdeling 1 van hoofdstuk III van dezelfde wet wordt artikel 15^{ter}, ingevoegd bij de wet van 7 april 2019, vervangen als volgt:

“Art. 15^{ter}. Het Agentschap wordt aangewezen als sectorale inspectiedienst in de zin van de NIS2-wet voor de sector energie, wat betreft de bijkomende maatregelen voor het beheer van cyberbeveiligingsrisico's die van toepassing zijn op de elementen van een nucleaire installatie bestemd voor

production industrielle d'électricité et qui servent au transport de l'électricité.

Le Roi fixe les modalités pratiques des inspections, après avis de l'Agence."

Section 2. Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique

Art. 78. A l'article 36/1 de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique, modifié en dernier lieu par la loi du 20 juillet 2022, le 28° est remplacé par ce qui suit:

"la loi NIS2": la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;"

Art. 79. A l'article 36/14 de la même loi, modifié en dernier lieu par la loi du 20 juillet 2022, les modifications suivantes sont apportées:

1° au paragraphe 1^{er}, 20°, les mots "à l'autorité visée à l'article 7, § 1^{er}, de la loi du 7 avril 2019" sont remplacés par les mots "à l'autorité nationale de cybersécurité visée à l'article 8, 47°, de la loi NIS2";

2° au même paragraphe, 20° /1, les mots "à l'autorité visée à l'article 7, § 1^{er}, de la loi du 7 avril 2019 [établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique - loi NIS]" sont remplacés par les mots "à l'autorité nationale de cybersécurité visée à l'article 8, 47°, de la loi NIS2 et au CSIRT national visé à l'article 8, 47°, de la même loi";

3° au même paragraphe, 24°, les mots "aux autorités visées à l'article 7 de la loi du 7 avril 2019 pour les besoins de l'exécution des dispositions de la loi du 7 avril 2019" sont remplacés par les mots "aux autorités visées à l'article 15 de la loi NIS2 pour les besoins de l'exécution des dispositions de la loi NIS2".

Art. 80. L'article 36/47 de la même loi, inséré par la loi du 7 avril 2019, est remplacé par ce qui suit:

"Art. 36/47. Pour l'application de la loi NIS2, la Banque est désignée comme autorité sectorielle et service d'inspection sectoriel pour les entités du secteur des finances, à l'exception des opérateurs de plate-forme de négociation au sens de l'article 3, 6°, de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la directive 2014/65/UE.

Si elle le juge utile, la Banque partage le plus vite possible avec la BCE les informations pertinentes sur les notifications d'incident qu'elle reçoit en vertu de la loi NIS2 ou du Règlement 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle

de l'industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit.

De Koning bepaalt de praktische inspectiemodaliteiten, na advies van het Agentschap."

Afdeling 2. Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België

Art. 78. In artikel 36/1 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, het laatst gewijzigd bij de wet van 20 juli 2022, wordt punt 28° vervangen als volgt:

"de NIS2-wet": de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;"

Art. 79. In artikel 36/14 van dezelfde wet, het laatst gewijzigd bij de wet van 20 juli 2022, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, 20°, worden de woorden "aan de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019" vervangen door de woorden "aan de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 47°, van de NIS2-wet";

2° in dezelfde paragraaf, 20° /1, worden de woorden "aan de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid - NIS-wet" vervangen door de woorden "aan de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 47°, van de NIS2-wet en aan het nationaal CSIRT bedoeld in artikel 8, 47°, van dezelfde wet";

3° in dezelfde paragraaf, 24°, worden de woorden "aan de autoriteiten bedoeld in artikel 7 van de wet van 7 april 2019 voor de uitvoering van de bepalingen van de wet van 7 april 2019" vervangen door de woorden "aan de autoriteiten bedoeld in artikel 15 van de NIS2-wet voor de uitvoering van de bepalingen van de NIS2-wet".

Art. 80. Artikel 36/47 van dezelfde wet, ingevoegd bij de wet van 7 april 2019, wordt vervangen als volgt:

"Art. 36/47. Voor de toepassing van de NIS2-wet wordt de Bank aangewezen als sectorale overheid en sectorale inspectiedienst voor de entiteiten van de sector financiën, met uitzondering van de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU.

Wanneer zij dit nuttig acht, deelt De Bank zo snel mogelijk met de ECB relevante informatie over incidentmeldingen die zij ontvangt krachtens de NIS2-Wet of Verordening 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor

numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.”

Section 3. Modification de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

Art. 81. A l'article 75, § 1^{er}, 15°, de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, modifié en dernier lieu par la loi du 20 juillet 2020, les mots “l'article 7 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique” sont remplacés par les mots “l'article 15 de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique”.

Section 4. Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges

Art. 82. A l'article 1^{er}/1 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, remplacé par la loi du 21 décembre 2021, le 1° est remplacé par ce qui suit:

“1° la directive européenne (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148;”.

Art. 83. A l'article 14 de la même loi, modifié en dernier lieu par la loi du 20 juillet 2022, les modifications suivantes sont apportées:

1° au paragraphe 1^{er}, les mots “loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique” sont remplacés par les mots “loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique”;

2° au même paragraphe, le 3°, alinéa 1^{er}, h), est remplacé par ce qui suit:

“h) la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, pour ce qui concerne les tâches dévolues à l'autorité sectorielle pour le secteur des infrastructures numériques, à l'exception des prestataires de services de confiance;”;

3° au même paragraphe, le 3°, alinéa 2, est remplacé par ce qui suit:

de la financière sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011.”

Afdeling 3. Wijziging van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

Art. 81. In artikel 75, § 1, 15°, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, het laatst gewijzigd bij de wet van 20 juli 2020, worden de woorden “artikel 7 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid” vervangen door de woorden “artikel 15 van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid”.

Afdeling 4. Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecomunicatiesector

Art. 82. In artikel 1/1 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecomunicatiesector, vervangen door de wet van 21 december 2021, wordt punt 1° vervangen als volgt:

“1° Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148;”.

Art. 83. In artikel 14 van dezelfde wet, het laatst gewijzigd bij de wet van 20 juli 2022, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 worden de woorden “wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid” vervangen door de woorden “wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid”;

2° in dezelfde paragraaf wordt punt 3°, eerste lid, h), vervangen als volgt:

“h) de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, voor wat betreft de taken toegewezen aan de sectorale overheid voor de sector digitaal infrastructuur, met uitzondering van de verleners van vertrouwensdiensten;”;

3° in dezelfde paragraaf wordt punt 3°, tweede lid, vervangen als volgt:

“Pour l’application de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique, l’Institut est désigné comme autorité sectorielle et service d’inspection sectoriel pour le secteur des infrastructures numériques, à l’exception des prestataires de services de confiance.”

Section 5. Modifications de la loi du 13 juin 2005 relative aux communications électroniques

Art. 84. A l’article 1^{er} de la loi du 13 juin 2005 relative aux communications électroniques, modifiée en dernier lieu par la loi du 30 août 2023, les modifications suivantes sont apportées:

1° à l’alinéa 2, à la fin du 6°, le point est remplacé par un point-virgule;

2° le même alinéa est complété par un 7°, rédigé comme suit:

“7° directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l’ensemble de l’Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148.”

Art. 85. A l’article 2 de la même loi, les modifications suivantes sont apportées:

1° le 48/1° est remplacé par ce qui suit:

“48/1° “registre de noms de domaine de premier niveau”: une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l’administration du domaine de premier niveau, y compris de l’enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l’exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par l’entité elle-même ou qu’elles soient sous-traitées, mais à l’exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage;

2° le 48/3° est inséré, rédigé comme suit:

“48/3° “entité fournissant des services d’enregistrement de noms de domaine”: un bureau d’enregistrement ou un agent agissant pour le compte de bureaux d’enregistrement, tel qu’un fournisseur ou revendeur de services d’anonymisation ou d’enregistrement fiduciaire;”

3° les 62/2° et 62/3° sont remplacés par ce qui suit:

“62/2° “réseau et système d’information”:

“Voor de toepassing van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wordt het Instituut aangewezen als sectorale overheid en sectorale inspectiedienst voor de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten.”

Afdeling 5. Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie

Art. 84. In artikel 1 van de wet van 13 juni 2005 betreffende de elektronische communicatie, het laatst gewijzigd bij de wet van 30 augustus 2023, worden de volgende wijzigingen aangebracht:

1° in het tweede lid, aan het einde van punt 6°, wordt het punt vervangen door een puntkomma;

2° hetzelfde lid wordt aangevuld met de bepaling onder 7°, luidende:

“7° Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148.”

Art. 85. In artikel 2 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de bepaling onder 48/1° wordt vervangt als volgt:

“48/1° “register voor topleveldomeinnamen”: een entiteit waaraan een specifieke topleveldomeinnaam is gedelegeerd en die verantwoordelijk is voor het beheer van de topleveldomeinnaam, met inbegrip van de registratie van domeinnamen onder de topleveldomeinnaam en de technische exploitatie van de topleveldomeinnaam, met inbegrip van de exploitatie van de naamsservers, het onderhoud van de databases en de verdeling van de zonebestanden van de topleveldomeinnaam over de naamsservers, ongeacht of die activiteiten door de entiteit zelf worden uitgevoerd of worden uitbesteed, maar met uitzondering van situaties waarin topleveldomeinnamen uitsluitend voor eigen gebruik worden aangewend door een register;

2° de bepaling onder 48/3° is ingevoegd, luidende:

“48/3° “entiteit die domeinnaamregistratiediensten aanbiedt”: een registrar of een agent die namens registrators optreedt, zoals een aanbieder van privacy- of proxy-registratiediensten of wederverkoper;”

3° de bepalingen onder 62/2° en 62/3° worden vervangt als volgt:

“62/2° “netwerk- en informatiesysteem”:

a) un réseau de communications électroniques au sens du 3°;

b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation du processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel; ou

c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance;

62/3° "sécurité des réseaux et des systèmes d'information": la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à tout événement susceptible de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, ou des services que ces réseaux et systèmes d'information offrent ou rendent accessibles;

4° les 62/4° à 62/8° sont insérés, rédigés comme suit:

62/4° "incident de sécurité": un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles;

62/5° "cybersécurité": la cybersécurité au sens de l'article 2, point 1), du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité);

62/6° "traitement des incidents": toutes les actions et procédures visant à prévenir, détecter, analyser et contenir un incident ou à y répondre et à y remédier;

62/7° "cybermenace": une cybermenace au sens de l'article 2, point 8), du règlement (UE) 2019/881;

62/8° "cybermenace importante": une cybermenace qui, compte tenu de ses caractéristiques techniques, peut être considérée comme susceptible d'avoir un impact grave sur les réseaux et les systèmes d'information d'une entité ou les utilisateurs des services de l'entité, en causant un dommage matériel, corporel ou moral considérable;

5° l'article est complété par un 94°, rédigé comme suit:

a) een elektronische-communicatienetwerk als bedoeld in 3°;

b) elk apparaat of elke groep van onderling verbonden of bij elkaar behorende apparaten, waarvan er een of meer, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische componenten van dat apparaat die met name de automatisering van het operationele proces, de controle op afstand of het verkrijgen van werkingsgegevens in real time mogelijk maken; of

c) digitale gegevens die worden opgeslagen, verwerkt, opgehaald of verzonden met behulp van de in punten a) en b) bedoelde elementen met het oog op de werking, het gebruik, de bescherming en het onderhoud ervan;

62/3° "beveiliging van netwerk- en informatiesystemen": het vermogen van netwerken informatiesystemen om op een bepaald niveau van betrouwbaarheid weerstand te bieden aan elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die door of via deze netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen;

4° de bepalingen onder 62/4° tot 62/8° worden ingevoegd, luidende:

62/4° "beveiligingsincident": een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt;

62/5° "cyberbeveiliging": cyberbeveiliging als bedoeld in artikel 2, 1), van Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening);

62/6° "incidentenbehandeling": alle acties en procedures die gericht zijn op het voorkomen, opsporen, analyseren en indammen van of het reageren op en het herstellen van een beveiligingsincident;

62/7° "cyberdreiging": een cyberdreiging als bedoeld in artikel 2, 8), van de cyberbeveiligingsverordening;

62/8° "significante cyberdreiging": een cyberdreiging waarvan op basis van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerk- en informatiesystemen van een entiteit of de gebruikers van de diensten van de entiteit door het veroorzaken van aanzienlijke materiële of immateriële schade;"

5° het artikel wordt aangevuld met de bepaling onder 94°, luidende:

“94° “opérateur d’infrastructure numérique”: une entité qui relève du secteur infrastructure numérique, à l’exception des prestataires de services de confiance, comme prévu dans la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique.”

Art. 86. Dans l’article 6, 4°, de la même loi, les mots “réseaux et services” sont remplacés par les mots “réseaux et systèmes d’information”.

Art. 87. Dans la même loi, les articles 107/2 à 107/4 sont remplacés par ce qui suit:

“Art. 107/2. § 1^{er}. Sans préjudice des dispositions de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique, les opérateurs d’infrastructure numérique analysent les risques pour la sécurité de leurs réseaux et systèmes d’information. L’Institut peut fixer des modalités de cette analyse de risque.

§ 2. Sans préjudice du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, ci-après dénommé “RGPD” et de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel, ci-après dénommée “loi du 30 juillet 2018”, les opérateurs veillent pour le moins à:

1° garantir que seules des personnes habilitées à agir à des fins légalement autorisées puissent avoir accès aux données à caractère personnel qu’ils traitent;

2° protéger les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l’altération accidentelles et le stockage, le traitement, l’accès et la divulgation non autorisés ou illicites; et

3° assurer la mise en oeuvre d’une politique de sécurité relative au traitement des données à caractère personnel.

L’Institut est habilité à vérifier les mesures prises par ces opérateurs ainsi qu’à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient permettre d’atteindre.

§ 3. Les opérateurs prennent toutes les mesures nécessaires, y compris préventives, pour assurer la disponibilité la plus complète possible des services de communications vocales et des services d’accès à l’internet en cas de défaillance exceptionnelle des réseaux ou de force majeure.

Le Roi, sur proposition de l’Institut ou d’initiative, sur avis de celui-ci, peut préciser ces mesures.

“94° “aanbieder van digitale infrastructuur”: een entiteit die behoort tot de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten, zoals bedoeld in de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.”

Art. 86. In artikel 6, 4°, van dezelfde wet, worden de woorden “netwerk en diensten” vervangen door de woorden “netwerk- en informatiesystemen”.

Art. 87. In dezelfde wet worden de artikelen 107/2 tot 107/4 vervangen als volgt:

“Art. 107/2. § 1. Onverminderd de bepalingen van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid analyseren de aanbieders van digitale infrastructuur de risico’s voor de beveiliging van hun netwerk- en informatiesystemen. Het Instituut kan de nadere regels van deze risicoanalyse vaststellen.

§ 2. Onverminderd Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, hierna “AVG” genoemd, en de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, hierna “wet van 30 juli 2018” genoemd, zorgen operatoren ervoor dat in ieder geval:

1° wordt gewaarborgd dat alleen gemachtigd personeel voor wettelijk toegestane doeleinden toegang heeft tot de persoonsgegevens die ze verwerken;

2° opgeslagen of verzonden persoonsgegevens worden beschermd tegen onbedoelde of onwettige vernietiging, onbedoeld verlies of wijziging, en niet-toegestane of onwettige opslag, verwerking, toegang of vrijgave, en

3° een beveiligingsbeleid wordt ingevoerd met betrekking tot de verwerking van persoonsgegevens.

Het Instituut kan de door deze operatoren genomen maatregelen controleren en aanbevelingen formuleren over de beste praktijken betreffende het beveiligingspeil dat met deze maatregelen moet worden gehaald.

§ 3. De operatoren nemen alle noodzakelijke maatregelen, inclusief preventieve, om de beschikbaarheid van de spraakcommunicatiediensten en de internettoegangsdiensten zo volledig mogelijk te waarborgen in geval van uitzonderlijke netwerkuitval of in geval van overmacht.

Op voorstel van het Instituut of op eigen initiatief, en na advies van het Instituut, kan de Koning deze maatregelen preciseren.

§ 4. Les opérateurs offrent gratuitement à leurs abonnés, compte tenu des possibilités techniques, les services sécurisés adéquats, afin de permettre aux utilisateurs finaux d'éviter toute forme de communication électronique non souhaitée.

Art. 107/3. § 1^{er}. En cas de cybermenace particulière et importante, l'opérateur d'infrastructure numérique informe l'Institut de la cybermenace, de toute mesure de protection ou correctrice que ses utilisateurs peuvent prendre ainsi que des mesures qu'il a prises ou envisage de prendre.

L'Institut peut préciser les cas dans lesquels une information doit être notifiée ainsi que les modalités de cette communication.

§ 2. En cas de violation de données à caractère personnel, l'opérateur de services de communications électroniques avertit sans délai l'Autorité de protection des données, qui en avertit sans délai l'Institut.

Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, l'opérateur de services de communications électroniques avertit également sans délai l'abonné ou le particulier concerné de la violation.

L'Autorité de protection des données examine si l'opérateur se conforme à cette obligation et informe l'Institut lorsqu'elle estime que cela n'est pas le cas.

La notification d'une violation des données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si l'opérateur de services de communications électroniques a prouvé, à la satisfaction de l'Institut, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

Sans préjudice de l'obligation de l'opérateur de service de communications électroniques d'informer les abonnés et les particuliers concernés, si cet opérateur n'a pas déjà averti l'abonné ou le particulier de la violation de données à caractère personnel, l'Institut peut, à la demande de l'Autorité de protection des données, après avoir examiné les effets potentiellement négatifs de cette violation, exiger qu'il s'exécute.

La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel.

La notification faite à l'Autorité de protection des données décrit en outre les conséquences de la violation de données

§ 4. De operatoren bieden hun abonnees kosteloos, rekening houdend met de stand van de techniek, de gepaste beveiligde diensten aan die de eindgebruikers in staat stellen ongewenste elektronische communicatie in alle vormen te verhinderen.

Art. 107/3. § 1. In geval van een specifieke en significante cyberdreiging informeert de aanbieder van digitale infrastructuur het Instituut over de dreiging, over mogelijke beschermingsmaatregelen of oplossingen die de gebruikers kunnen toepassen, alsook over de maatregelen die hij heeft genomen of overweegt te nemen.

Het Instituut kan de gevallen preciseren waarin informatie moet worden verstrekt alsook de nadere regels voor die kennisgeving.

§ 2. In geval van inbreuk in verband met persoonsgegevens verwittigt de operator van elektronische-communicatiediensten onverwijld de Gegevensbeschermingsautoriteit, die onverwijld het Instituut verwittigt.

Indien de inbreuk in verband met persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor de persoonsgegevens of persoonlijke levenssfeer van een abonnee of een individueel persoon, stelt de operator van elektronische-communicatiediensten onverwijld ook de betrokken abonnee of individuele persoon in kennis van de inbreuk.

De Gegevensbeschermingsautoriteit gaat na of de operator deze verplichting nakomt en brengt het Instituut op de hoogte wanneer ze van oordeel is dat dit niet het geval is.

De kennisgeving van een inbreuk in verband met persoonsgegevens aan een betrokken abonnee of individuele persoon is niet vereist wanneer de operator van elektronische-communicatiediensten tot voldoening van het Instituut heeft aangetoond dat hij de gepaste technologische beschermingsmaatregelen heeft genomen en dat deze maatregelen werden toegepast op de data die bij de beveiligingsinbreuk betrokken waren. Dergelijke technologische beschermingsmaatregelen maken de gegevens onbegrijpelijk voor eenieder die geen recht op toegang daartoe heeft.

Onverminderd de verplichting van de operator van elektronische-communicatiediensten om de betrokken abonnees en individuele personen in kennis te stellen, indien deze operator de abonnee of individuele persoon niet reeds in kennis heeft gesteld van de inbreuk in verband met persoonsgegevens, kan het Instituut op verzoek van de Gegevensbeschermingsautoriteit hem, na te hebben gezien of en welke ongunstige gevolgen uit de inbreuk voortvloeien, verzoeken dat te doen.

In de kennisgeving aan de abonnee of de individuele persoon worden ten minste de aard van de inbreuk in verband met persoonsgegevens, alsmede de contactpunten voor meer informatie vermeld, en worden er maatregelen aanbevolen om mogelijke negatieve gevolgen van de inbreuk in verband met persoonsgegevens te verlichten.

De kennisgeving aan de Gegevensbeschermingsautoriteit bevat bovendien een omschrijving van de gevolgen van de inbreuk

à caractère personnel, et les mesures proposées ou prises par l'opérateur de services de communications électroniques pour y remédier.

§ 3. Sous réserve de mesures d'exécution techniques émanant de la Commission européenne conformément à l'article 4, point 5, de la directive 2002/58/CE, et après avis de l'Autorité de protection des données, l'Institut peut adopter des lignes directrices et, le cas échéant, édicter des instructions précisant les circonstances dans lesquelles les opérateurs de services de communications électroniques sont tenus de notifier la violation de données à caractère personnel.

Sous réserve de mesures techniques d'application émanant de la Commission européenne conformément à l'article 4, point 5, de la directive 2002/58/CE, et après avis de l'Institut, l'Autorité de protection des données peut adopter des lignes directrices et, le cas échéant, édicter des instructions précisant le format applicable à cette notification et sa procédure de transmission.

Les opérateurs de services de communications électroniques tiennent à jour un inventaire des violations de données à caractère personnel, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier, de sorte que l'Autorité de protection des données et l'Institut puissent vérifier le respect des dispositions du paragraphe 2. Cet inventaire comprend uniquement les informations nécessaires à cette fin.

Art. 107/4. § 1^{er}. Le présent article s'applique sans préjudice des dispositions de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, notamment en ce qui concerne les pouvoirs de supervision accordés à l'autorité sectorielle ou au service d'inspection sectoriel.

§ 2. L'Institut peut donner des instructions contraignantes dans le cadre des articles 107/2, 107/3 ainsi que des articles 30 et 33 de la loi du [xx xxx xxxx] précitée à un opérateur d'infrastructure numérique, y compris les mesures requises pour remédier à un incident de sécurité ou empêcher qu'un tel incident ne se produise lorsqu'une cybermenace importante a été identifiée, ainsi que les dates limites de mise en œuvre de ces instructions.

§ 3. Dans le cadre de la supervision des articles 107/2 et 107/3 ainsi que des articles 30 et 33 de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut peut soumettre l'opérateur d'infrastructure numérique à:

a) des inspections sur place et des contrôles à distance, y compris des contrôles aléatoires effectués par des professionnels formés;

b) des audits de sécurité réguliers et ciblés réalisés par un organisme indépendant ou par l'Institut;

in verband met persoonsgegevens en van de door de operator van elektronische-communicatiediensten voorgestelde of getroffen maatregelen om die inbreuk te verhelpen.

§ 3. Onder voorbehoud van technische uitvoeringsmaatregelen van de Europese Commissie overeenkomstig artikel 4, punt 5, van Richtlijn 2002/58/EG, en na advies van de Gegevensbeschermingsautoriteit, kan het Instituut richtsnoeren aannemen en, waar nodig, instructies uitvaardigen betreffende de omstandigheden waarin de kennisgeving van de inbreuk in verband met persoonsgegevens door de operatoren van elektronische-communicatiediensten noodzakelijk is.

Onder voorbehoud van technische uitvoeringsmaatregelen van de Europese Commissie overeenkomstig artikel 4, punt 5, van Richtlijn 2002/58/EG, en na advies van het Instituut, kan de Gegevensbeschermingsautoriteit richtsnoeren aannemen en, waar nodig, instructies uitvaardigen betreffende het voor deze kennisgeving toepasselijke formaat, alsmede de manier waarop de kennisgeving geschiedt.

De operatoren van elektronische-communicatiediensten houden een inventaris bij van inbreuken in verband met persoonsgegevens, onder meer met de feiten in verband met deze inbreuken, de gevolgen ervan en de herstelmaatregelen die zijn genomen, zodat de Gegevensbeschermingsautoriteit en het Instituut kunnen nagaan of de bepalingen van paragraaf 2 werden nageleefd. Deze inventaris bevat uitsluitend de voor dit doel noodzakelijke gegevens.

Art. 107/4. § 1. Dit artikel is van toepassing onverminderd de bepalingen van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid met name voor wat betreft de toezichtsbevoegdheden verleend aan de sectorale overheid of de sectorale inspectiedienst.

§ 2. Het Instituut kan een aanbieder van digitale infrastructuur bindende instructies geven in het kader van artikelen 107/2 en 107/3 en van artikelen 30 en 33 van de bovengenoemd wet van [xx xxx xxxx], onder meer de maatregelen die nodig zijn om een beveiligingsincident op te lossen of te voorkomen wanneer een significante dreiging is vastgesteld, alsook het tijdschema voor de uitvoering van die instructies.

§ 3. In het kader van het toezicht op de artikelen 107/2 en 107/3 en van artikelen 30 en 33 van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, kan het Instituut de aanbieder van digitale infrastructuur onderwerpen aan:

a) inspecties ter plaatse en toezicht elders, met inbegrip van steekproefsgewijze controles, die worden uitgevoerd door daartoe opgeleide professionals;

b) regelmatige en gerichte beveiligingsaudits die worden uitgevoerd door het Instituut of door een onafhankelijke instantie;

c) des audits ad hoc;

d) des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération de l'opérateur d'infrastructure digitale;

e) des demandes d'informations nécessaires à l'évaluation des mesures de gestion des risques en matière de cybersécurité adoptées par l'opérateur d'infrastructure digitale concerné;

f) des demandes d'accès à des données, à des documents et à toutes informations nécessaires à l'Institut pour l'accomplissement de ses tâches de supervision;

g) des demandes de preuves de la mise en oeuvre de politiques de cybersécurité, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants.

Les audits de sécurité ciblés visés au premier alinéa, point b), sont basés sur des évaluations des risques effectuées par l'Institut ou l'entité contrôlée, ou sur d'autres informations disponibles relatives aux risques.

Lorsque l'audit de sécurité visé à l'alinéa 1^{er}, point b) est effectué par un organisme indépendant, l'opérateur d'infrastructure numérique propose à l'Institut un ou plusieurs organismes pour accord. L'Institut donne son accord lorsque l'organisme indépendant est qualifié pour effectuer l'audit et est indépendant par rapport à l'opérateur d'infrastructure numérique. A défaut d'accord de l'Institut dans le délai qu'il a fixé lors de la demande, l'Institut désigne lui-même l'organisme indépendant. Ce dernier communique à l'Institut le rapport complet et les résultats de cet audit. Les coûts de l'audit sont à la charge de l'opérateur d'infrastructure numérique, sauf lorsque l'Institut en décide autrement dans des cas dûment motivés.

Lorsqu'il exerce ses pouvoirs en vertu du paragraphe 1, point e), f) ou g), l'Institut précise la finalité de la demande et les informations exigées.

L'Institut peut fixer les modalités de la fourniture par l'opérateur d'infrastructure numérique des informations concernant l'analyse de risque.

A la demande de l'Institut, un opérateur d'infrastructure numérique participe à un exercice relatif à la sécurité des réseaux et systèmes d'information ou organise un tel exercice.

A la demande de l'Institut et dans le cadre de la gestion des incidents de sécurité, un opérateur d'infrastructure numérique communique à l'Institut un point de contact disponible en permanence.

§ 4. A la demande de l'Institut et pour enquêter sur un cas de non-conformité par rapport aux articles 30 et 33 de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité

c) ad-hocaudits;

d) beveiligingsscan op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria, indien nodig in samenwerking met de betrokken aanbieder van digitale infrastructuur;

e) verzoeken om informatie die nodig is om de door de betrokken aanbieder van digitale infrastructuur genomen maatregelen voor het beheer van cyberbeveiligingsrisico's

f) verzoeken van alle gegevens, documenten en informatie die het Instituut nodig acht voor de uitoefening van haar toezichthoudende taken;

g) verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de respectieve onderliggende bewijzen.

De in het eerste lid, punt b), bedoelde gerichte beveiligingsaudits zijn gebaseerd op door het Instituut of de gecontroleerde entiteit verrichte risicobeoordelingen of op andere beschikbare risicogerelateerde informatie.

Wanneer de in het eerste lid, punt b) bedoelde beveiligingsaudit wordt uitgevoerd door een onafhankelijke instantie, dan stelt de aanbieder van digitale infrastructuur een of meer instanties ter goedkeuring aan het Instituut voor. Het Instituut geeft zijn akkoord wanneer de onafhankelijke instantie gekwalificeerd is om de audit uit te voeren en onafhankelijk is van de aanbieder van digitale infrastructuur. Bij uitblijven van een akkoord vanwege het Instituut binnen de termijn die het bij het verzoek heeft vastgesteld, wijst het Instituut zelf de onafhankelijk instantie aan. Deze laatste bezorgt aan het Instituut het volledige verslag en de resultaten van deze audit en de kosten van de audit zijn ten laste van de aanbieder van digitale infrastructuur, behalve in naar behoren gemotiveerde gevallen waarin het Instituut anders besluit.

Bij de uitoefening van zijn bevoegdheden uit hoofde van lid 1, punt e), f) of g), vermeldt het Instituut het doel van het verzoek en de gevraagde informatie.

Het Instituut kan bepalen op welke wijze de aanbieder van digitale infrastructuur informatie over de risicoanalyse moet verstrekken.

Op verzoek van het Instituut neemt een aanbieder van digitale infrastructuur deel aan een oefening in verband met de beveiliging van de netwerk- en informatiesystemen of organiseert hij een dergelijke oefening.

Op verzoek van het Instituut en in het kader van het beheer van beveiligingsincidenten, deelt een aanbieder van digitale infrastructuur het Instituut een contactpersoon mee die steeds bereikbaar is.

§ 4. Op verzoek van het Instituut en om een onderzoek in te stellen naar een geval van niet-conformiteit met artikelen 30 en 33 van de wet van [xx xxxx xxxx] tot vaststelling van een kader

des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ou à une mesure d'exécution ainsi que sur son effet sur la sécurité des réseaux et systèmes d'information, l'opérateur d'infrastructure numérique lui donne accès à tout élément de son réseau.

§ 5. Sans préjudice des compétences de l'autorité nationale de cybersécurité, l'Institut coordonne les initiatives relatives à la sécurité des réseaux publics de communications électroniques et des services de communications électroniques accessibles au public.

Il supervise la détection, l'observation et l'analyse des problèmes de sécurité, et peut fournir aux utilisateurs des informations en la matière.

§ 6. Le non-respect par un opérateur d'infrastructure numérique du présent article ou d'une décision de l'Institut prise sur base du présent article peut faire l'objet des mesures ou amendes administratives visées dans le chapitre 2 de la loi NIS 2."

Art. 88. A l'article 126/3, § 3, I), de la même loi, les mots "essentiels des fournisseurs de service essentiels désignés sur la base de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique" sont remplacés par les mots "des entités essentielles au sens de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique".

Art. 89. A l'article 164/1 de la même loi, les modifications suivantes sont apportées:

1° les mots "bureau d'enregistrement de noms de domaine Internet du domaine de premier niveau" sont remplacés par les mots "registre de noms de domaine de premier niveau du domaine de premier niveau";

2° au 4°, les mots "bureau d'enregistrement des noms de domaine" sont remplacés par les mots "registre de noms de domaine de premier niveau".

3° au 4°, les mots "bureau d'enregistrement des noms de domaine Internet" sont remplacés par les mots "registre de noms de domaine de premier niveau";

4° au 5°, dans le texte en néerlandais, le mot "topniveau-domein" est remplacé par le mot "topleveldomein".

Art. 90. A l'article 164/2 de la même loi, les modifications suivantes sont apportées:

1° les mots "bureau d'enregistrement de noms de domaine Internet" sont chaque fois remplacés par les mots "registre de noms de domaine de premier niveau";

voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, of met een uitvoeringsmaatregel, alsook naar de gevolgen ervan voor de beveiliging van netwerk- en informatiesystemen, geeft de aanbieder van digitale infrastructuur het Instituut toegang tot alle elementen van zijn netwerk.

§ 5. Onverminderd de bevoegdheden van de nationale cyberbeveiligingsautoriteit coördineert het Instituut de initiatieven rond de beveiliging van openbare elektronische-communicatienetwerken en openbare elektronische-communicatiediensten.

Het ziet toe op het opsporen, observeren en analyseren van beveiligingsproblemen, en kan de gebruikers hierover informatie verstrekken.

§ 6. Indien een aanbieder van digitale infrastructuur dit artikel of een op grond van dit artikel genomen beslissing van het Instituut niet naleeft, kunnen de in hoofdstuk 2 van de NIS2-wet bedoelde administratieve maatregelen of geldboetes worden opgelegd."

Art. 88. In artikel 126/3, § 3, I), worden de woorden "essentiële diensten van aanbieders van essentiële diensten ondersteunen aangeduid op basis van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid" vervangen door de woorden "diensten van essentiële entiteiten in de zin van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid".

Art. 89. In artikel 164/1 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de woorden "Internetdomeinnaamregistreerbureau van het topniveaudomein" worden vervangen door de woorden "register voor topleveldomeinnamen van het topleveldomein";

2° in de bepaling onder 4° wordt het woord "domeinnaamregistreerbureau" vervangen door de woorden "register voor topleveldomeinnamen";

3° in de bepaling onder 4° wordt het woord "Internetdomeinnaamregistreerbureau" vervagen door de woorden "register voor topleveldomeinnamen";

4° in de bepaling onder 5°, in de Nederlandse tekst, wordt het woord "topniveaudomein" vervangen door het woord "topleveldomein".

Art. 90. In artikel 164/2 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de woorden "Internetdomeinnaamregistreerbureau" worden vervangen door de woorden "register voor topleveldomeinnamen";

2° dans le texte en néerlandais, le mot “topniveaudomein” est à chaque fois remplacé par le mot “topeleveldomein”.

Art. 91. Dans le titre VI, chapitre 3, de la même loi, il est inséré un article 164/3, rédigé comme suit:

“**Art. 164/3. § 1^{er}.** Les registres des noms de domaine de premier niveau et les entités fournissant des services d’enregistrement de noms de domaine collectent les données d’enregistrement de noms de domaine et les maintiennent exactes et complètes au sein d’une base de données spécialisée avec la diligence requise par le droit de l’Union en matière de protection des données pour ce qui concerne les données à caractère personnel.

§ 2. La base de données visée au paragraphe 1^{er} contient les informations nécessaires pour identifier et contacter les titulaires des noms de domaine et les points de contact qui gèrent les noms de domaine relevant des domaines de premier niveau. Ces informations comprennent au moins les éléments suivants:

1° le nom de domaine;

2° la date d’enregistrement;

3° le nom du titulaire, l’adresse de courrier électronique et le numéro de téléphone permettant de le contacter;

4° l’adresse de courrier électronique et le numéro de téléphone permettant de contacter le point de contact qui gère le nom de domaine, si ces coordonnées sont différentes de celles du titulaire.

§ 3. Les registres des noms de domaine de premier niveau et les entités fournissant des services d’enregistrement de noms de domaine mettent en place des politiques et des procédures, notamment des procédures de vérification, visant à garantir que les bases de données visées au paragraphe 1^{er} contiennent des informations exactes et complètes. Ces politiques et procédures sont mises à la disposition du public.

L’Institut peut donner des instructions contraignantes à un registre de noms de domaine de premier niveau ou à une entité fournissant des services d’enregistrement de noms de domaine, en vue du respect de l’alinéa 1^{er}.

§ 4. Les registres des noms de domaine de premier niveau et les entités fournissant des services d’enregistrement de noms de domaine rendent publiques, sans retard injustifié après l’enregistrement d’un nom de domaine, les données d’enregistrement du nom de domaine qui ne sont pas des données à caractère personnel.

§ 5. Les registres des noms de domaine de premier niveau et les entités fournissant des services d’enregistrement de noms de domaine donnent accès aux données spécifiques d’enregistrement de noms de domaine sur demande légitime et dûment motivée des demandeurs d’accès légitimes. Les registres des noms de domaine de premier niveau et les entités fournissant des services d’enregistrement de noms

2° in de Nederlandse tekst wordt het woord “topniveaudomein” vervangen door het woord “topeleveldomein”.

Art. 91. In titel VI, hoofdstuk 3, van dezelfde wet, wordt een artikel 164/3 ingevoegd, luidende:

“**Art. 164/3. § 1.** Registers voor topeleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, verzamelen met de nodige zorgvuldigheid nauwkeurige en volledige domeinnaamregistratiegegevens en houden deze bij in een speciale database overeenkomstig het Unierecht inzake gegevensbescherming voor wat betreft gegevens die persoonsgegevens zijn.

§ 2. De database bedoeld in paragraaf 1 bevat de noodzakelijke informatie om de houders van de domeinnamen en de contactpunten die de domeinnamen onder de topeleveldomeinnamen beheren, te identificeren en te contacteren. Die informatie omvat ten minste:

1° de domeinnaam;

2° de registratiedatum;

3° de naam, het e-mailadres en het telefoonnummer van de registrant;

4° het e-mailadres en het telefoonnummer van het contactpunt dat de domeinnaam beheert, indien deze verschillen van die van de registrant.

§ 3. De registers voor topeleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, beschikken over beleidslijnen en procedures, waaronder verificatieprocedures, om ervoor te zorgen dat de in paragraaf 1 bedoelde databases juiste en volledige informatie bevatten. Deze beleidslijnen en procedures worden openbaar gemaakt.

Het Instituut kan een register voor topeleveldomeinnamen of een entiteit die domeinnaamregistratiediensten verleent bindende instructies geven, met het oog op de naleving van het eerste lid.

§ 4. De registers voor topeleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, maken de domeinnaamregistratiegegevens die geen persoonsgegevens zijn, onverwijld openbaar na de registratie van een domeinnaam.

§ 5. De registers voor topeleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, verschaffen, op rechtmatig en naar behoren gemotiveerd verzoek van legitieme toegangsvragende partijen, toegang tot specifieke gegevens over de registratie van domeinnamen. Registers voor topeleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, beantwoorden verzoeken om toegang onverwijld en

de domaine répondent sans retard injustifié et en tout état de cause dans un délai de 72 heures après réception de toute demande d'accès. Les politiques et procédures de divulgation de ces données sont rendues publiques.

Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine, offrent au demandeur la possibilité d'introduire aisément sa demande, dans au moins une des langues nationales.

L'Institut peut donner des instructions contraignantes à un registre de noms de domaine de premier niveau ou à une entité fournissant des services d'enregistrement de noms de domaine, en vue du respect des alinéas 1^{er} et 2.

Après avis de l'Institut, le Roi peut préciser qui est considéré comme demandeur d'accès légitime et à quelles données spécifiques d'enregistrement de noms de domaine il convient de donner accès.

§ 6. Le respect des obligations visées au présent article n'entraîne pas de répétition inutile de la collecte des données d'enregistrement de noms de domaine. A cet effet, les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine coopèrent entre eux.

Après avis de l'Institut, le Roi peut préciser les modalités de cette coopération.

Section 6. Modifications de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la directive 2014/65/UE

Art. 92. A l'article 71 de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la directive 2014/65/UE, modifié par la loi du 7 avril 2019, les mots "et du titre 2 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique. Pour l'exécution des missions précitées concernant la loi du 7 avril 2019, la FSMA peut néanmoins charger un prestataire externe spécialisé de l'exécution de tâches déterminées de contrôle ou obtenir l'assistance d'un tel prestataire" sont supprimés.

Art. 93. L'article 79, § 4, de la même loi, inséré par la loi du 7 avril 2019, est abrogé.

CHAPITRE 3 – Disposition abrogatoire

Art. 94. La loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique est abrogée.

in elk geval binnen 72 uur na ontvangst van het verzoek. Het beleid en de procedures met betrekking tot de bekendmaking van deze gegevens worden openbaar gemaakt.

De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, stellen de verzoeker in staat om gemakkelijk, in ten minste één van de nationale talen, zijn verzoek in te dienen.

Het Instituut kan een register voor topleveldomeinnamen of een entiteit die domeinnaamregistratiediensten verleent bindende instructies geven, met het oog op de naleving van het eerste lid en het tweede lid.

De Koning kan, na advies van het Instituut, preciseren wie als legitieme toegangsvragende partij wordt beschouwd en tot welke specifieke gegevens over de registratie van domeinnamen toegang moet worden gegeven.

§ 6. De naleving van de in dit artikel vastgestelde verplichtingen mag er niet toe leiden dat domeinnaamregistratiegegevens tweemaal moeten worden verzameld. Daartoe werken registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, met elkaar samen.

De Koning kan, na advies van het Instituut, de modaliteiten van deze samenwerking preciseren.

Afdeling 6. Wijzigingen van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU

Art. 92. In artikel 71 van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU, gewijzigd bij de wet van 7 april 2019, worden de woorden "en van titel 2 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid. Voor de uitvoering van de voormelde opdrachten betreffende de wet van 7 april 2019 kan de FSMA niettemin een gespecialiseerde externe dienstverlener belasten met de uitvoering van welbepaalde toezichtopdrachten of de bijstand van een dergelijke dienstverlener verkrijgen" geschrapt.

Art. 93. Artikel 79, § 4, van dezelfde wet, ingevoegd bij de wet van 7 april 2019, wordt opgeheven.

HOOFDSTUK 3 – Opheffingsbepaling

Art. 94. De wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid wordt opgeheven.

CHAPITRE 4 – Entrée en vigueur

Art. 95. La présente loi entre en vigueur le 18 octobre 2024.

HOOFDSTUK 4 – Inwerkingtreding

Art. 95. Deze wet treedt in werking op 18 oktober 2024.

Annexe I – Secteurs hautement critiques		
Secteur	Sous-secteur	Type d'entité
1. Énergie	a) Électricité	- Entreprises d'électricité au sens de l'article 2, point 57), de la directive (UE) 2019/944 du Parlement européen et du Conseil, qui remplissent la fonction de «fourniture» au sens de l'article 2, point 12), de ladite directive
		- Gestionnaires de réseau de distribution au sens de l'article 2, point 29), de la directive (UE) 2019/944
		- Gestionnaires de réseau de transport au sens de l'article 2, point 35), de la directive (UE) 2019/944
		- Producteurs au sens de l'article 2, point 38), de la directive (UE) 2019/944
		- Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8), du règlement (UE) 2019/943 du Parlement européen et du Conseil
		- Acteurs du marché au sens de l'article 2, point 25), du règlement (UE) 2019/943 fournissant des services d'agrégation, de participation active de la demande ou de stockage d'énergie au sens de l'article 2, points 18), 20) et 59), de la directive (UE) 2019/944
		- Exploitants d'un point de recharge qui sont responsables de la gestion et de l'exploitation d'un point de recharge, lequel fournit un service de recharge aux utilisateurs finals, y compris au nom et pour le compte d'un prestataire de services de mobilité
	b) Réseau de chaleur et de froid	- Opérateurs de réseaux de chaleur ou de réseaux de froid au sens de l'article 2, point 19), de la directive (UE) 2018/2001 du Parlement européen et du Conseil
	c) Pétrole	- Exploitants d'oléoducs
		- Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
		- Entités centrales de stockage au sens de l'article 2, point f), de la directive 2009/119/CE du Conseil
	d) Gaz	- Entreprises de fourniture au sens de l'article 2, point 8, de la directive 2009/73/CE du Parlement européen et du Conseil
		- Gestionnaires de réseau de distribution au sens de l'article 2, point 6, de la directive 2009/73/CE

		- Gestionnaires de réseau de transport au sens de l'article 2, point 4, de la directive 2009/73/CE
		- Gestionnaires d'installation de stockage au sens de l'article 2, point 10, de la directive 2009/73/CE
		- Gestionnaires d'installation de GNL au sens de l'article 2, point 12, de la directive 2009/73/CE
		- Entreprises de gaz naturel au sens de l'article 2, point 1, de la directive 2009/73/CE
		- Exploitants d'installations de raffinage et de traitement de gaz naturel
	e) Hydrogène	- Exploitants de systèmes de production, de stockage et de transport d'hydrogène
2. Transports	a) Transports aériens	Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) no 300/2008 utilisés à des fins commerciales
		Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de la directive 2009/12/CE du Parlement européen et du Conseil, aéroports au sens de l'article 2, point 1), de ladite directive, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) no 1315/2013 du Parlement européen et du Conseil, et entités exploitant les installations annexes se trouvant dans les aéroports
		Services du contrôle de la circulation aérienne au sens de l'article 2, point 1), du règlement (CE) no 549/2004 du Parlement européen et du Conseil
	b) Transports ferroviaires	Gestionnaires de l'infrastructure au sens de l'article 3, point 2), de la directive 2012/34/UE du Parlement européen et du Conseil
		Entreprises ferroviaires au sens de l'article 3, point 1), de la directive 2012/34/UE, y compris les exploitants d'installation de service au sens de l'article 3, point 12), de ladite directive
	c) Transports par eau	Sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret, telles qu'elles sont définies pour le domaine du transport maritime à l'annexe I du règlement (CE) no 725/2004 du Parlement européen et du Conseil, à l'exclusion des navires exploités à titre individuel par ces sociétés
		Entités gestionnaires des ports au sens de l'article 3, point 1), de la directive 2005/65/CE du Parlement européen et du Conseil, y compris les installations portuaires au sens de l'article 2, point 11), du règlement (CE) no 725/2004, ainsi que les entités exploitant des

		infrastructures et des équipements à l'intérieur des ports
		Exploitants de services de trafic maritime (STM) au sens de l'article 3, point o), de la directive 2002/59/CE du Parlement européen et du Conseil
	d) Transports routiers	Autorités routières au sens de l'article 2, point 12), du règlement délégué (UE) 2015/962 de la Commission chargées du contrôle de la gestion de la circulation, à l'exclusion des entités publiques pour lesquelles la gestion de la circulation ou l'exploitation de systèmes de transport intelligents constituent une partie non essentielle de leur activité générale Exploitants de systèmes de transport intelligents au sens de l'article 4, point 1), de la directive 2010/40/UE du Parlement européen et du Conseil
3. Secteur bancaire		Établissements de crédit au sens de l'article 4, point 1), du règlement (UE) no 575/2013 du Parlement européen et du Conseil
4. Infrastructures des marchés financiers		Exploitants de plates-formes de négociation au sens de l'article 4, point 24), de la directive 2014/65/UE du Parlement européen et du Conseil
		Contreparties centrales au sens de l'article 2, point 1), du règlement (UE) no 648/2012 du Parlement européen et du Conseil
5. Santé		Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil
		Laboratoires de référence de l'Union européenne visés à l'article 15 du règlement (UE) 2022/2371 du Parlement européen et du Conseil
		Entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1er, point 2, de la directive 2001/83/CE du Parlement européen et du Conseil
		Entités fabricant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de la NACE Rév. 2, section C, division 21
		Entités fabricant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique (liste des dispositifs médicaux critiques en cas d'urgence de santé publique) au sens de l'article 22 du règlement (UE) 2022/123 du Parlement européen et du Conseil

6. Eau potable		Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) a), de la directive (UE) 2020/2184 du Parlement européen et du Conseil, à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine constitue une partie non essentielle de leur activité générale de distribution d'autres produits et biens
7. Eaux usées		Entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, les eaux ménagères usées ou les eaux industrielles usées au sens de l'article 2, points 1), 2) et 3), de la directive 91/271/CEE du Conseil, à l'exclusion des entreprises pour lesquelles la collecte, l'évacuation ou le traitement des eaux urbaines résiduaires, des eaux ménagères usées ou des eaux industrielles usées constituent une partie non essentielle de leur activité générale
8. Infrastructure numérique		Fournisseurs de points d'échange internet
		Fournisseurs de services DNS, à l'exclusion des opérateurs de serveurs racines de noms de domaine
		Registres de noms de domaine de premier niveau
		Fournisseurs de services d'informatique en nuage
		Fournisseurs de services de centres de données
		Fournisseurs de réseaux de diffusion de contenu
		Prestataires de services de confiance
		Fournisseurs de réseaux de communications électroniques publics
		Fournisseurs de services de communications électroniques accessibles au public
9. Gestion des services TIC (interentreprises)		Fournisseurs de services gérés
		Fournisseurs de services de sécurité gérés
10. Administration publique		Entités de l'administration publique fédérale
		Entités de l'administration publique des entités fédérées, identifiés conformément à l'article 11, § 2 de la loi.
11. Espace		Exploitants d'infrastructures terrestres, détenues, gérées et exploitées par des États membres ou par des parties privées, qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics

Annexe II - Autres secteurs critiques		
Secteur	Sous-secteur	Type d'entité
1. Services postaux et d'expédition		- Prestataires de services postaux au sens de l'article 2, point 1 bis), de la directive 97/67/CE, y compris les prestataires de services d'expédition
2. Gestion des déchets		- Entreprises exécutant des opérations de gestion des déchets au sens de l'article 3, point 9), de la directive 2008/98/CE du Parlement européen et du Conseil, à l'exclusion des entreprises pour lesquelles la gestion des déchets n'est pas la principale activité économique
3. Fabrication, production et distribution de produits chimiques		Entreprises procédant à la fabrication de substances et à la distribution de substances ou de mélanges au sens de l'article 3, points 9 et 14, du règlement (CE) no 1907/2006 du Parlement européen et du Conseil et entreprises procédant à la production d'articles au sens de l'article 3, point 3), dudit règlement, à partir de substances ou de mélanges
4. Production, transformation et distribution des denrées alimentaires		Entreprises du secteur alimentaire au sens de l'article 3, point 2), du règlement (CE) no 178/2002 du Parlement européen et du Conseil qui exercent des activités de distribution en gros ainsi que de production et de transformation industrielles
5. Fabrication	a) Fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro	- Entités fabriquant des dispositifs médicaux au sens de l'article 2, point 1), du règlement (UE)

		2017/745 du Parlement européen et du Conseil et entités fabriquant des dispositifs médicaux de diagnostic in vitro au sens de l'article 2, point 2), du règlement (UE) 2017/746 du Parlement européen et du Conseil, à l'exception des entités fabriquant des dispositifs médicaux mentionnés à l'annexe I, point 5, cinquième tiret, de la présente directive
	b) Fabrication de produits informatiques, électroniques et optiques	- Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 26
	c) Fabrication d'équipements électriques	- Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 27
	d) Fabrication de machines et équipements n.c.a.	- Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 28
	e) Construction de véhicules automobiles, remorques et semi-remorques	- Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 29
	f) Fabrication d'autres matériels de transport	- Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 30
6. Fournisseurs numériques		- Fournisseurs de places de marché en ligne
		- Fournisseurs de moteurs de recherche en ligne
		- Fournisseurs de plateformes de services de réseaux sociaux
7. Recherche		- Organismes de recherche

Bijlage I - Zeer kritieke sectoren		
Sector	Deelsector	Soort entiteit
1. Energie	a) Elektriciteit	- Elektriciteitsbedrijven zoals gedefinieerd in artikel 2, punt 57, van Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad, die de functie verrichten van “levering” zoals gedefinieerd in artikel 2, punt 12, van die richtlijn
		- Distributiesysteembeheerders zoals gedefinieerd in artikel 2, punt 29, van Richtlijn (EU) 2019/944
		- Transmissiesysteembeheerders zoals gedefinieerd in artikel 2, punt 35, van Richtlijn (EU) 2019/944
		- Producenten zoals gedefinieerd in artikel 2, punt 38, van Richtlijn (EU) 2019/944
		- Benoemde elektriciteitsmarktbeheerders zoals gedefinieerd in artikel 2, punt 8, van Verordening (EU) 2019/943 van het Europees Parlement en de Raad
		- Marktdelnemers zoals gedefinieerd in artikel 2, punt 25, van Verordening (EU) 2019/943 die aggregatie verrichten of vraagrespons- of energieopslagdiensten verstrekken zoals gedefinieerd in artikel 2, punten 18, 20 en 59, van Richtlijn (EU) 2019/944
		- Exploitanten van een laadpunt die verantwoordelijk zijn voor het beheer en de exploitatie van een laadpunt dat een laaddienst levert aan eindgebruikers, onder meer namens en voor rekening van een aanbieder van mobiliteitsdiensten
	b) Stadsverwarming en -koeling	- Exploitanten van stadsverwarming of stadskoeling zoals gedefinieerd in artikel 2, punt 19, van Richtlijn (EU) 2018/2001 van het Europees Parlement en de Raad
	c) Aardolie	- Exploitanten van oliepijpleidingen
		- Exploitanten van voorzieningen voor de productie, raffinage en behandeling van olie, opslag en transport
		- Centrale entiteiten voor de voorraadvorming zoals gedefinieerd in artikel 2, punt f), van Richtlijn 2009/119/EG van de Raad
	d) Aardgas	- Leveringsbedrijven zoals gedefinieerd in artikel 2, punt 8, van Richtlijn 2009/73/EG van het Europees Parlement en de Raad
		- Distributiesysteembeheerders zoals gedefinieerd in artikel 2, punt 6, van Richtlijn 2009/73/EG
		- Transmissiesysteembeheerders zoals gedefinieerd in artikel 2, punt 4, van Richtlijn 2009/73/EG

		- Opslagsysteembeheerders zoals gedefinieerd in artikel 2, punt 10, van Richtlijn 2009/73/EG - LNG-systeembeheerders zoals gedefinieerd in artikel 2, punt 12, van Richtlijn 2009/73/EG - Aardgasbedrijven zoals gedefinieerd in artikel 2, punt 1, van Richtlijn 2009/73/EG - Exploitanten van voorzieningen voor de raffinage en behandeling van aardgas
	e) Waterstof	- Exploitanten van voorzieningen voor de productie, opslag en transmissie van waterstof
2. Vervoer	a) Lucht	- Luchtvaartmaatschappijen zoals gedefinieerd in artikel 3, punt 4, Verordening (EG) nr. 300/2008 die voor commerciële doeleinden worden gebruikt - Luchthavenbeheerders zoals gedefinieerd in artikel 2, punt 2, van Richtlijn 2009/12/EG van het Europees Parlement en de Raad, luchthavens als bedoeld in artikel 2, punt 1, van die richtlijn, met inbegrip van de kernluchthavens die in bijlage II, afdeling 2, bij Verordening (EU) 1315/2013 van het Europees Parlement en de Raad zijn opgenomen, alsook de entiteiten die bijbehorende installaties bedienen welke zich op luchthavens bevinden - Exploitanten op het gebied van verkeersbeheer en -controle die luchtverkeersleidingssystemen zoals gedefinieerd in artikel 2, punt 1, van Verordening (EG) nr. 549/2004 van het Europees Parlement en de Raad aanbieden
	b) Spoor	- Infrastructuurbeheerders zoals gedefinieerd in artikel 3, punt 2, van Richtlijn 2012/34/EU van het Europees Parlement en de Raad - Spoorwegondernemingen zoals gedefinieerd in artikel 3, punt 1, van Richtlijn 2012/34/EU, inclusief exploitanten van dienstvoorzieningen zoals gedefinieerd in artikel 3, punt 12, van die richtlijn
	c) Water	- Bedrijven voor vervoer over water (binnenvaart, kust- en zeevervoer) van passagiers en vracht, die in bijlage I bij Verordening (EG) nr. 725/2004 van het Europees Parlement en de Raad als bedrijven in maritiem vervoer worden gedefinieerd, met uitzondering van de door deze bedrijven geëxploiteerde individuele vaartuigen - Beheerders van havens zoals gedefinieerd in artikel 3, punt 1, van Richtlijn 2005/65/EG van het Europees Parlement en de Raad, inclusief hun havenfaciliteiten zoals gedefinieerd in artikel 2, punt 11, van Verordening (EG) nr. 725/2004; alsook entiteiten die werken en uitrusting in havens beheren - Exploitanten van verkeersbegeleidingssystemen (VBS) zoals gedefinieerd in artikel 3, punt o), van

		Richtlijn 2002/59/EG van het Europees Parlement en de Raad
	d) Weg	- Wegenautoriteiten zoals gedefinieerd in artikel 2, punt 12, van gedelegeerde Verordening (EU) 2015/962 van de Commissie die verantwoordelijk zijn voor het verkeersbeheer, met uitzondering van overheidsinstanties waarvoor verkeersbeheer of de exploitatie van intelligente vervoerssystemen slechts een niet-essentieel onderdeel van hun algemene activiteit is - Exploitanten van intelligente vervoerssystemen zoals gedefinieerd in artikel 4, punt 1, van Richtlijn 2010/40/EU van het Europees Parlement en de Raad
3. Bankwezen		- Kredietinstellingen zoals gedefinieerd in artikel 4, punt 1, Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad
4. Infrastructuur voor de financiële markt		- Exploitanten van handelsplatformen zoals gedefinieerd in artikel 4, punt 24, van Richtlijn 2014/65/EU van het Europees Parlement en de Raad - Centrale tegenpartijen zoals gedefinieerd in artikel 2, punt 1, Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad
5. Gezondheidszorg		- Zorgaanbieders zoals gedefinieerd in artikel 3, punt g), van Richtlijn 2011/24/EU van het Europees Parlement en de Raad - EU-referentielaboratoria als bedoeld in artikel 15 van Verordening (EU) 2022/2371 van het Europees Parlement en de Raad inzake ernstige grensoverschrijdende bedreigingen van de gezondheid - Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen zoals gedefinieerd in artikel 1, punt 2, van Richtlijn 2001/83/EG van het Europees Parlement en de Raad - Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen als bedoeld in sectie C, afdeling 21, van NACE Rev. 2 vervaardigen - Entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd ("de lijst van in een noodsituatie op het gebied van de volksgezondheid kritieke hulpmiddelen") in de zin van artikel 22 van Verordening (EU) 2022/123 van het Europees Parlement en de Raad
6. Drinkwater		- Leveranciers en distributeurs van voor menselijke consumptie bestemd water zoals gedefinieerd in artikel 2, punt 1, a), van Richtlijn (EU) 2020/2184

		van het Europees Parlement en de Raad, met uitzondering van distributeurs waarvoor de distributie van water voor menselijke consumptie een niet-essentieel deel is van hun algemene activiteit van distributie van andere waren en goederen die niet worden beschouwd als essentiële of belangrijke diensten
7. Afvalwater		- Ondernemingen die stedelijk afvalwater, huishoudelijk afvalwater of industrieel afvalwater zoals gedefinieerd in artikel 2, punten 1, 2 en 3, van Richtlijn 91/271/EEG van de Raad opvangen, lozen of behandelen, met uitzondering van ondernemingen waarvoor het opvangen, lozen of behandelen van stedelijk afvalwater, huishoudelijk afvalwater of industrieel afvalwater een niet-essentieel onderdeel van hun algemene activiteit is
8. Digitale infrastructuur		- Aanbieders van internetknooppunten
		- DNS-dienstverleners, met uitzondering van exploitanten van root-naamserveren
		- Register voor topleveldomeinnamen
		- Aanbieders van cloudcomputingdiensten
		- Aanbieders van datacenterdiensten
		- Aanbieders van netwerken voor de levering van inhoud
		- Verleners van vertrouwensdiensten
		- Aanbieders van openbare elektronische communicatienetwerken
9. Beheer van ICT-diensten (business-to-business)		- Aanbieders van beheerde diensten
		- Aanbieders van beheerde beveiligingsdiensten
10. Overheid		- Federale overheidsinstanties
		- Gefedereerde overheidsinstanties die worden geïdentificeerd overeenkomstig artikel 11, §2.
11. Ruimtevaart		- Exploitanten van grondfaciliteiten die in het bezit zijn van of beheerd of geëxploiteerd worden door de lidstaten of door particuliere partijen en die de verlening van vanuit de ruimte opererende diensten ondersteunen, met uitzondering van aanbieders van openbare elektronische communicatienetwerken

Bijlage II - Andere kritieke sectoren		
Sector	Deel-sector	Soort entiteit
1. Post- en koeriersdiensten		- Aanbieders van postdiensten zoals gedefinieerd in artikel 2, punt 1 bis, van Richtlijn 97/67/EG, met inbegrip van aanbieders van koeriersdiensten
2. Afvalstoffenbeheer		- Ondernemingen die handelingen in het kader van afvalstoffenbeheer uitvoeren zoals gedefinieerd in artikel 3, punt 9, van Richtlijn 2008/98/EG van het Europees Parlement en de Raad, met uitzondering van ondernemingen waarvoor afvalstoffenbeheer niet de voornaamste economische activiteit is
3. Vervaardiging, productie en distributie van chemische stoffen		- Ondernemingen die stoffen vervaardigen en stoffen of mengsels distribueren als bedoeld in artikel 3, punten 9 en 14, van Verordening (EG) nr. 1907/2006 van het Europees Parlement en de Raad en ondernemingen die voorwerpen zoals gedefinieerd in artikel 3, punt 3, van die verordening produceren uit stoffen of mengsels
4. Productie, verwerking en distributie van levensmiddelen		- Levensmiddelenbedrijven zoals gedefinieerd in artikel 3, punt 2, Verordening (EG) nr. 178/2002 van het Europees Parlement en de Raad die zich bezighouden met groothandel en industriële productie en verwerking
5. Vervaardiging	a) Vervaardiging van medische hulpmiddelen en medische	- Entiteiten die medische hulpmiddelen zoals

	hulpmiddelen voor in-vitrodiagnostiek	gedefinieerd in artikel 2, punt 1, van Verordening (EU) 2017/745 van het Europees Parlement en de Raad vervaardigen en entiteiten die medische hulpmiddelen voor in-vitrodiagnostiek zoals gedefinieerd in artikel 2, punt 2, van Verordening (EU) 2017/746 van het Europees Parlement en de Raad vervaardigen, met uitzondering van entiteiten die medische hulpmiddelen vervaardigen als bedoeld in bijlage I, punt 5, vijfde streepje, van deze richtlijn
	b) Vervaardiging van informaticaproducten en van elektronische en optische producten	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 26, van NACE Rev. 2
	c) Vervaardiging van elektrische apparatuur	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 27, van NACE Rev. 2
	d) Vervaardiging van machines, apparaten en werktuigen, n.e.g.	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 28, van NACE Rev. 2
	e) Vervaardiging van motorvoertuigen, aanhangers en opleggers	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 29, van NACE Rev. 2
	f) Vervaardiging van andere transportmiddelen	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 30, van NACE Rev. 2
6. Digitale aanbieders		- Aanbieders van onlinemarktplaatsen
		- Aanbieders van onlinezoekmachines
		- Aanbieders van platforms voor
		socialenetwerkdiensten

7. Onderzoek		- Onderzoeksorganisaties

AVIS DU CONSEIL D'ÉTAT
N° 74.861/4 DU 10 JANVIER 2024

Le 13 novembre 2023, le Conseil d'État, section de législation, a été invité par le Premier ministre à communiquer un avis dans un délai de trente jours, sur un avant-projet de loi 'établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique'.

L'avant-projet a été examiné par la quatrième chambre le 10 janvier 2024. La chambre était composée de Bernard BLERO, président de chambre, Luc CAMBIER et Dimitri YERNAULT, conseillers d'État, Christian BEHRENDT et Jacques ENGLEBERT, assessseurs, et Charles-Henri VAN HOVE, greffier.

Le rapport a été présenté par Roger WIMMER, premier auditeur, et Xavier MINY, auditeur adjoint.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Bernard BLERO.

L'avis, dont le texte suit, a été donné le 10 janvier 2024.

*

Comme la demande d'avis est introduite sur la base de l'article 84, § 1^{er}, alinéa 1^{er}, 2^o, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique de l'avant-projet[†], à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, l'avant-projet appelle les observations suivantes.

FORMALITÉ PRÉALABLE

L'avant-projet de loi à l'examen comporte diverses dispositions portant sur un traitement de données à caractère personnel, en particulier son titre 6.

L'article 36, paragraphe 4, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 'relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)', combiné avec son article 57, paragraphe 1, c), le considérant 96 de son préambule et, le cas échéant, l'article 2, alinéa 2, de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel',

[†] S'agissant d'amendements à un projet de loi, on entend par "fondement juridique" la conformité aux normes supérieures.

ADVIES VAN DE RAAD VAN STATE
NR. 74.861/4 VAN 10 JANUARI 2024

Op 13 november 2023 is de Raad van State, afdeling Wetgeving, door de Eerste minister verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet 'tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid'.

Het voorontwerp is door de vierde kamer onderzocht op 10 januari 2024. De kamer was samengesteld uit Bernard BLERO, kamervoorzitter, Luc CAMBIER en Dimitri YERNAULT, staatsraden, Christian BEHRENDT en Jacques ENGLEBERT, assessoren, en Charles-Henri VAN HOVE, griffier.

Het verslag is uitgebracht door Roger WIMMER, eerste auditeur, en Xavier MINY, adjunct-auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Bernard BLERO.

Het advies, waarvan de tekst hierna volgt, is gegeven op 10 januari 2024.

*

Aangezien de adviesaanvraag is ingediend op basis van artikel 84, § 1, eerste lid, 2^o, van de wetten 'op de Raad van State', gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het voorontwerp,[†] de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geeft het voorontwerp aanleiding tot de volgende opmerkingen.

VOORAFGAANDE VORMVEREISTE

Het voorliggende voorontwerp van wet bevat verschillende bepalingen, met name in titel 6, die betrekking hebben op de verwerking van persoonsgegevens.

Artikel 36, lid 4, van verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 'betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)', gelezen in samenhang met artikel 57, lid 1, c), en overweging 96 van de preambule van die verordening en in voorkomend geval met artikel 2, tweede lid, van de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de

[†] Aangezien het om amendementen op een wetsontwerp gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere rechtsnormen verstaan.

prévoit une obligation de consulter l'autorité de contrôle, en l'occurrence l'Autorité de protection des données visée dans la loi du 3 décembre 2017 'portant création de l'Autorité de protection des données', dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement de données à caractère personnel.

Il ressort du dossier transmis et des informations communiquées à la section de législation que l'avant-projet a été envoyé pour avis à l'Autorité de protection des données simultanément à la saisine de la section de législation.

Si l'accomplissement de cette formalité devait encore donner lieu à des modifications du texte soumis au Conseil d'État sur des points autres que de pure forme et ne résultant pas des suites réservées au présent avis, les dispositions modifiées ou ajoutées devraient être soumises à nouveau à l'avis de la section de législation conformément à l'article 3, § 1^{er}, alinéa 1^{er}, des lois coordonnées 'sur le Conseil d'État'.

OBSERVATIONS GÉNÉRALES

1. Concernant la compétence de l'autorité fédérale dans le cadre de la transposition de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 'concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)' (ci-après, "la directive NIS2"), le délégué du Premier ministre a fourni les explications suivantes:

"Le champ d'application de la directive NIS2 porte sur les règles de cybersécurité applicables à certaines entités (fournissant des services essentiels au maintien d'activités sociétales ou économiques critiques), dont la protection relève en droit interne des compétences résiduelles fédérales en matière de sécurité publique. La directive NIS2 détermine, en effet, des mesures destinées à assurer un niveau commun de cybersécurité dans l'ensemble de l'Union européenne pour certaines entités qualifiées comme 'essentielles' ou 'importantes', en raison des services qu'elles fournissent et de leur taille (voir ci-après). Les entités concernées sont celles fournissant des services essentiels énumérés dans les 'secteurs hautement critiques' de l'annexe I ou dans les 'autres secteurs critiques' de l'annexe II.

En application de la directive NIS2 et de la recommandation 2003/361/CE, les 'entités essentielles' sont les organisations qui fournissent un service repris dans l'annexe I et qui répondent à la notion de 'grande entreprise', c'est-à-dire qui occupe min. 250 personnes ou dont le chiffre d'affaires annuel excède 50 millions d'euros (ou le total du bilan annuel excède 43 millions d'euros).

Les 'entités importantes' sont les organisations qui fournissent un service repris dans l'annexe I et qui répondent à la notion de 'moyenne entreprise', c'est-à-dire qui occupe

verwerking van persoonsgegevens', schrijft voor dat de toezichthoudende autoriteit, *in casu* de Gegevensbeschermingsautoriteit bedoeld in de wet van 3 december 2017 'tot oprichting van de Gegevensbeschermingsautoriteit', wordt geraadpleegd bij het opstellen van een voorstel voor een door een nationaal parlement vast te stellen wetgevingsmaatregel, of een daarop gebaseerde regelgevingsmaatregel, in verband met de verwerking van persoonsgegevens.

Uit het dossier en de informatie die aan de afdeling Wetgeving zijn bezorgd, blijkt dat de Gegevensbeschermingsautoriteit tegelijk met de afdeling Wetgeving om advies over het voorontwerp is verzocht.

Indien de aan de Raad van State voorgelegde tekst naar aanleiding van het vervullen van dat vormvereiste nog wijzigingen zou ondergaan die niet louter vormelijk zijn en niet voortvloeien uit het gevolg dat aan dit advies wordt gegeven, moeten de gewijzigde of toegevoegde bepalingen op hun beurt om advies aan de afdeling Wetgeving worden voorgelegd, overeenkomstig artikel 3, § 1, eerste lid, van de gecoördineerde wetten 'op de Raad van State'.

ALGEMENE OPMERKINGEN

1. Met betrekking tot de bevoegdheid van de federale overheid in het kader van de omzetting van richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 'betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn)' (hierna: "de NIS 2-richtlijn"), heeft de gemachtigde van de eerste minister de volgende toelichting gegeven:

"Le champ d'application de la directive NIS2 porte sur les règles de cybersécurité applicables à certaines entités (fournissant des services essentiels au maintien d'activités sociétales ou économiques critiques), dont la protection relève en droit interne des compétences résiduelles fédérales en matière de sécurité publique. La directive NIS2 détermine, en effet, des mesures destinées à assurer un niveau commun de cybersécurité dans l'ensemble de l'Union européenne pour certaines entités qualifiées comme 'essentielles' ou 'importantes', en raison des services qu'elles fournissent et de leur taille (voir ci-après). Les entités concernées sont celles fournissant des services essentiels énumérés dans les 'secteurs hautement critiques' de l'annexe I ou dans les 'autres secteurs critiques' de l'annexe II.

En application de la directive NIS2 et de la recommandation 2003/361/CE, les 'entités essentielles' sont les organisations qui fournissent un service repris dans l'annexe I et qui répondent à la notion de 'grande entreprise', c'est-à-dire qui occupe min. 250 personnes ou dont le chiffre d'affaires annuel excède 50 millions d'euros (ou le total du bilan annuel excède 43 millions d'euros).

Les 'entités importantes' sont les organisations qui fournissent un service repris dans l'annexe I et qui répondent à la notion de 'moyenne entreprise', c'est-à-dire qui occupe

min. 50 personnes ou réalise un chiffre d'affaires annuel (ou le total du bilan annuel) qui excède 10 millions d'euros. Sont également des 'entités importantes' les organisations qui fournissent un service repris dans l'annexe II et qui répondent aux notions de moyenne ou de grande entreprise.

Outre les considérants, le contenu des dispositions de la directive NIS2 démontre à suffisance que la matière concrète traitée par celle-ci est bien la sécurité des citoyens (utilisateurs des services concernés), des entreprises, des biens et des autorités publiques contre les cybermenaces et les cyberincidents. En effet, la défaillance ou la compromission des réseaux et systèmes d'information de certaines entités jugées nécessaires au maintien de diverses fonctions centrales pour la vie de la Nation (car elles fournissent des services essentiels au maintien d'activités sociétales ou économiques critiques) peut avoir des conséquences importantes pour la société et l'économie. La cybersécurité des 'entités essentielles' ou 'entités importantes' NIS2 relève dès lors clairement de la protection exercée dans le domaine général de la sécurité publique (la protection des personnes physiques, des personnes morales et des biens).

Par ailleurs, la directive NIS2 ne détermine pas des règles de cybersécurité applicables à toutes les organisations actives dans un domaine particulier. Elle fixe des mesures minimales communes de gestion des risques en matière de cybersécurité et de notification des incidents importants (ou des cybermenaces importantes) à toutes les entités essentielles et importantes, sans distinction entre leur secteur d'activités.

La nature générale (transsectorielle) et commune des mesures envisagées par la directive (visant à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne) démontre l'absence de lien entre la matière concrète traitée par la directive et les différents secteurs repris dans ses annexes (les actes juridiques sectoriels de l'Union sont d'ailleurs explicitement exclus du champ d'application de la directive par l'article 4).

Cette analyse juridique a été confirmée par la section législation du Conseil d'État dans son avis sur le projet qui allait devenir la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (ci-après la 'loi NIS1') qui a transposé la directive européenne (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (ci-après la 'directive NIS1').

Dans son avis sur la loi NIS1 (n° 62.296/4 du 2 mai 2018), le Conseil d'État a souligné que la transposition de la directive NIS1 pouvait 'soulever en soi des questions de compétence lorsque les infrastructures à protéger dépendent d'opérateurs qui exercent leurs activités dans l'orbite de compétences qui ont été attribuées aux entités fédérées ou à certaines d'entre-elles et que la loi fédérale entend associer de manière unilatérale ces entités à l'identification des infrastructures à protéger, identification que l'État fédéral entreprend pour ce qui le concerne sous le couvert des compétences résiduelles

min. 50 personnes ou réalise un chiffre d'affaires annuel (ou le total du bilan annuel) qui excède 10 millions d'euros. Sont également des 'entités importantes' les organisations qui fournissent un service repris dans l'annexe II et qui répondent aux notions de moyenne ou de grande entreprise.

Outre les considérants, le contenu des dispositions de la directive NIS2 démontre à suffisance que la matière concrète traitée par celle-ci est bien la sécurité des citoyens (utilisateurs des services concernés), des entreprises, des biens et des autorités publiques contre les cybermenaces et les cyberincidents. En effet, la défaillance ou la compromission des réseaux et systèmes d'information de certaines entités jugées nécessaires au maintien de diverses fonctions centrales pour la vie de la Nation (car elles fournissent des services essentiels au maintien d'activités sociétales ou économiques critiques) peut avoir des conséquences importantes pour la société et l'économie. La cybersécurité des 'entités essentielles' ou 'entités importantes' NIS2 relève dès lors clairement de la protection exercée dans le domaine général de la sécurité publique (la protection des personnes physiques, des personnes morales et des biens).

Par ailleurs, la directive NIS2 ne détermine pas des règles de cybersécurité applicables à toutes les organisations actives dans un domaine particulier. Elle fixe des mesures minimales communes de gestion des risques en matière de cybersécurité et de notification des incidents importants (ou des cybermenaces importantes) à toutes les entités essentielles et importantes, sans distinction entre leur secteur d'activités.

La nature générale (transsectorielle) et commune des mesures envisagées par la directive (visant à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne) démontre l'absence de lien entre la matière concrète traitée par la directive et les différents secteurs repris dans ses annexes (les actes juridiques sectoriels de l'Union sont d'ailleurs explicitement exclus du champ d'application de la directive par l'article 4).

Cette analyse juridique a été confirmée par la section législation du Conseil d'État dans son avis sur le projet qui allait devenir la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (ci-après la 'loi NIS1') qui a transposé la directive européenne (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (ci-après la 'directive NIS1').

Dans son avis sur la loi NIS1 (n° 62.296/4 du 2 mai 2018), le Conseil d'État a souligné que la transposition de la directive NIS1 pouvait 'soulever en soi des questions de compétence lorsque les infrastructures à protéger dépendent d'opérateurs qui exercent leurs activités dans l'orbite de compétences qui ont été attribuées aux entités fédérées ou à certaines d'entre-elles et que la loi fédérale entend associer de manière unilatérale ces entités à l'identification des infrastructures à protéger, identification que l'État fédéral entreprend pour ce qui le concerne sous le couvert des compétences résiduelles

qu'il exerce dans le domaine de la sécurité publique' mais que le projet ne soulevait aucun problème de compétence.

À cet égard, le Conseil d'État a rappelé l'analyse formulée à propos de la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques (avis n° 48.989/VR 1 du 9 décembre 2010):

'[...] L'infrastructure critique est en substance définie par l'article 2, a), de la directive comme le point [...] qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif [...] du fait de la défaillance de ces fonctions [...].

Eu égard à ce qui précède, il y a lieu de considérer que la transposition de cette directive met principalement en œuvre la matière de la protection préventive exercée dans le domaine de la sécurité publique, qui relève des compétences résiduelles exclusives du législateur fédéral.

Il en va de même pour ce qui concerne les autres dispositions de l'avant-projet qui, tout en n'ayant pas pour objet de transposer la directive, tendent à l'adoption de mesures analogues pour ce qui concerne les infrastructures critiques nationales ainsi que les autres points d'intérêt fédéral et les points d'intérêt local".

Dans l'avis 63.296/4 donné le 2 mai 2018 sur un avant-projet devenu la loi du 7 avril 2019 'établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique', la section de législation a en effet observé ce qui suit:

"Ce n'est pas la première fois que la section de législation est saisie d'un avant-projet de loi visant, en exécution d'une directive européenne à transposer, à recenser des opérateurs de services essentiels en vue d'assurer de manière préventive la protection de certaines de leurs infrastructures jugées nécessaires au maintien de diverses fonctions centrales pour la vie de la Nation.

Cette opération peut soulever en soi des questions de compétence lorsque les infrastructures à protéger dépendent d'opérateurs qui exercent leurs activités dans l'orbite de compétences qui ont été attribuées aux entités fédérées ou à certaines d'entre-elles et que la loi fédérale entend associer de manière unilatérale ces entités à l'identification des infrastructures à protéger, identification que l'État fédéral entreprend pour ce qui le concerne sous le couvert des compétences résiduelles qu'il exerce dans le domaine de la sécurité publique.

Cette question de compétence a été analysée dans les termes suivants à l'occasion de l'avis n° 48.989/VR¹ donné le

qu'il exerce dans le domaine de la sécurité publique' mais que le projet ne soulevait aucun problème de compétence.

À cet égard, le Conseil d'État a rappelé l'analyse formulée à propos de la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques (avis n° 48.989/VR 1 du 9 décembre 2010):

'(...) L'infrastructure critique est en substance définie par l'article 2, a), de la directive comme le point (...) qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif (...) du fait de la défaillance de ces fonctions (...).

Eu égard à ce qui précède, il y a lieu de considérer que la transposition de cette directive met principalement en œuvre la matière de la protection préventive exercée dans le domaine de la sécurité publique, qui relève des compétences résiduelles exclusives du législateur fédéral.

Il en va de même pour ce qui concerne les autres dispositions de l'avant-projet qui, tout en n'ayant pas pour objet de transposer la directive, tendent à l'adoption de mesures analogues pour ce qui concerne les infrastructures critiques nationales ainsi que les autres points d'intérêt fédéral et les points d'intérêt local."

In advies 63.296/4, op 2 mei 2018 gegeven over een voorontwerp dat heeft geleid tot de wet van 7 april 2019 'tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid', heeft de afdeling Wetgeving immers het volgende opgemerkt:

"Het is niet voor het eerst dat de afdeling Wetgeving advies moet uitbrengen over een voorontwerp van wet dat, met toepassing van een om te zetten Europese richtlijn, aanbieders van essentiële diensten beoogt te inventariseren teneinde sommige van hun infrastructuur die noodzakelijk worden geacht voor het behoud van verschillende centrale functies voor het bestaan van de Natie, preventief te beschermen.

Die onderneming kan op zichzelf bevoegdheidsproblemen doen rijzen, wanneer de te beschermen infrastructuur afhangen van operatoren die hun activiteiten uitoefenen op gebieden waarvoor de deelstaten of sommige deelstaten bevoegd zijn gemaakt, en wanneer de federale wet die deelstaten eenzijdig wil betrekken bij de identificatie van de te beschermen infrastructuur, een identificatie die de Federale Staat, wat hem betreft, doet krachtens de restbevoegdheden die hij op het gebied van de openbare veiligheid uitoefent.

Die bevoegdheidskwestie is als volgt geanalyseerd in advies 48.989/VR,¹ op 9 december 2010 gegeven over een

¹ Note de bas de page n° 1 de l'avis cité: Doc. parl., Chambre, 2010-2011, n° 1357/001, pp. 53-64, <http://www.raadvst-consetat.be/dbx/avis/48989.pdf>.

¹ Voetnoot 1 van het geciteerde advies: Parl.St. Kamer 2010-11, nr. 1357/001, 53-64, <http://www.raadvst-consetat.be/dbx/adviezen/48989.pdf>.

9 décembre 2010 sur un avant-projet devenu la loi du 1^{er} juillet 2011 'relative à la sécurité et la protection des infrastructures critiques':

'1. Ainsi que l'exprime son article 2, alinéa 1^{er}, l'avant-projet à l'examen a notamment pour objet de transposer la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (ci-après, la directive).

Comme l'énonce l'article 1^{er} de la directive, il s'agit d'établir une procédure de recensement et de désignation des infrastructures critiques européennes en vue d'éventuellement améliorer leur protection afin de contribuer à la protection des personnes. L'infrastructure critique est en substance définie par l'article 2, a), de la directive comme 'le point (...) qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif (...) du fait de la défaillance de ces fonctions'. L'article 3, paragraphe 3, de la directive mentionne qu'elle s'applique pour l'instant uniquement dans les secteurs de l'énergie et des transports. Selon le premier considérant de la directive, ses auteurs ont d'abord eu en vue l'adoption de 'mesures en vue de renforcer la prévention, la préparation et la réponse de l'Union européenne face aux attaques terroristes contre des infrastructures critiques'. Par la suite, tout en maintenant 'une priorité donnée à la lutte contre la menace terroriste', le programme européen de protection des infrastructures critiques, dont la directive est un instrument, s'est fondé sur 'une approche tous risques (qui) tient compte des risques d'origine humaine, des menaces technologiques et des catastrophes naturelles dans le processus de protection des infrastructures critiques' (troisième considérant).

Eu égard à ce qui précède, il y a lieu de considérer que la transposition de cette directive met principalement en œuvre la matière de la protection préventive exercée dans le domaine de la sécurité publique, qui relève des compétences résiduelles exclusives du législateur fédéral².

Il en va de même pour ce qui concerne les autres dispositions de l'avant-projet qui, tout en n'ayant pas pour objet de transposer la directive, tendent à l'adoption de mesures

voorontwerp dat heeft geleid tot de wet van 1 juli 2001 'betreffende de beveiliging en de bescherming van de kritieke infrastructuur':

'1. Het voorliggende voorontwerp voorziet, zoals te lezen staat in artikel 2, eerste lid, ervan, inzonderheid in de omzetting van richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuur, de aanmerking van infrastructuur als Europese kritieke infrastructuur en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuur te verbeteren (hierna 'de richtlijn' genoemd).

Artikel 1 van de richtlijn geeft aan dat bij deze richtlijn een procedure wordt ingesteld voor de identificatie en de aanmerking van Europese kritieke infrastructuur, om de bescherming van de mensen te bevorderen. De kritieke infrastructuur wordt in artikel 2, a), van de richtlijn in wezen gedefinieerd als 'een voorziening (...), die van essentieel belang is voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, waarvan de verstoring of vernietiging (...) aanzienlijke gevolgen zou hebben doordat die functies ontregeld zouden raken'. Artikel 3, lid 3, van de richtlijn bepaalt dat deze op dit ogenblik uitsluitend van toepassing is in de sectoren energie en vervoer. Volgens de eerste overweging van de richtlijn hebben de stellers ervan in de eerste plaats het aannemen van 'voorstellen (beoogd) over de wijze waarop de preventie van, de paraatheid bij en de reactie op terreuraanslagen op kritieke infrastructuur in Europa kunnen worden verbeterd'. In dat verband is besloten dat het Europese programma voor de bescherming van kritieke infrastructuur, waarvan de richtlijn een beleidsmiddel is, 'gebaseerd moet zijn op een alle risico's omvattende aanpak, waarbij de bestrijding van terroristische dreigingen als prioriteit zou gelden', een aanpak waarbij 'in het proces ter bescherming van kritieke infrastructuur rekening (dient) te worden gehouden met door mensen veroorzaakte dreigingen, technologische dreigingen en natuurrampen' (derde overweging).

Gelet op hetgeen voorafgaat, moet worden beschouwd dat de omzetting van deze richtlijn hoofdzakelijk leidt tot de tenuitvoerlegging van de aangelegenheid van de preventieve bescherming op het gebied van de openbare veiligheid, die tot de exclusieve restbevoegdheid van de federale wetgever behoort.²

Hetzelfde geldt voor de overige bepalingen van het voorontwerp die weliswaar niet voorzien in de omzetting van de richtlijn, maar strekken tot het aannemen van analoge maatregelen met

² *Note de bas de page n° 2 de l'avis cité:* Note de bas de page n° 1 de l'avis cité: C.E., État belge, n° 175.462, 8 octobre 2007. Pour d'autres exemples de lois adoptées par l'État fédéral en vue d'assurer la protection préventive des "fonctions vitales de la société", voir la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité qui vise notamment à protéger "le potentiel économique du pays" ou la loi du 10 juillet 2006 relative à l'analyse de la menace qui a notamment en vue les "intérêts fondamentaux" du pays.

² *Voetnoot 2 van het geciteerde advies:* Voetnoot 1 van het geciteerde advies: Raad van State, Belgische Staat, nr. 175.462, 8 oktober 2007. Andere voorbeelden van wetten die de Federale Staat heeft aangenomen met het oog op de preventieve bescherming van de "vitale maatschappelijke functies": de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, die onder meer de bescherming van het "economisch potentieel van het land" beoogt, of de wet van 10 juli 2006 betreffende de analyse van de dreiging, die onder meer 's lands "fundamentele belangen" beoogt.

analogues pour ce qui concerne les infrastructures critiques nationales ainsi que les autres points d'intérêt fédéral et les points d'intérêt local.

2. Toutefois, les mesures qui seront prises sur la base de l'avant-projet seront susceptibles de concerner des opérateurs exploitant des infrastructures qui, envisagées d'un autre point de vue, pourraient relever de la compétence matérielle des régions, s'agissant spécialement des secteurs de l'énergie et du transport, auxquels la directive s'applique (article 6, § 1^{er}, VII et X, de la loi spéciale du 8 août 1980 de réformes institutionnelles).

L'auteur de l'avant-projet est d'ailleurs sensible à cet aspect des choses puisqu'il a le souci d'"associer" les régions à la réglementation applicable et à sa mise en œuvre, comme en témoignent les dispositions suivantes de l'avant-projet:

– l'article 5, § 1^{er}, alinéa 2, selon lequel l'autorité sectorielle³ procède à l'identification des infrastructures critiques européennes 'après avis conforme des régions pour les infrastructures critiques potentielles relevant de leurs compétences';

– l'article 6, § 2, selon lequel l'autorité sectorielle 'établit des critères sectoriels auxquels doivent répondre les infrastructures critiques européennes eu égard aux caractéristiques particulières du secteur concerné, (...), le cas échéant, après avis conforme des régions concernées';

– l'article 6, § 5, selon lequel 'l'autorité sectorielle établit au cas par cas les seuils applicables aux critères intersectoriels auxquels doivent répondre les infrastructures critiques européennes, (...), le cas échéant après avis conforme des régions concernées';

– l'article 7, § 2, alinéa 2, selon lequel la Direction générale Centre de Crise du service public fédéral Intérieur (ci-après, DGCC) 'est chargée en collaboration (...) le cas échéant, avec les régions concernées (...) de mener des discussions bilatérales ou multilatérales avec les États membres de l'Union européenne concernés (...) en ce qui concerne les infrastructures critiques européennes potentielles identifiées sur le territoire belge (...)';

– l'article 13, § 6, alinéa 2, selon lequel 'le Roi, le cas échéant, en accord avec les régions concernées, détermine pour un secteur ou un sous-secteur déterminé la fréquence des exercices et des mises à jour' du plan de sécurité de l'exploitant d'une infrastructure critique européenne;

– l'article 24, § 2, alinéa 2, selon lequel le Roi 'peut fixer les modalités du contrôle, le cas échéant en accord avec

³ Note de bas de page n° 3 de l'avis cité: Note de bas de page n° 2 de l'avis cité: Pour les infrastructures critiques européennes, l'autorité sectorielle est le ministre fédéral ayant les Transports dans ses attributions ou son délégué (article 3, 3°, a, de l'avant-projet) ou le ministre fédéral ayant l'Énergie dans ses attributions ou son délégué (article 3, 3°, b), de l'avant-projet.

betrekking tot de nationale kritieke infrastructuur, de andere punten van federaal belang en de punten van lokaal belang.

2. De maatregelen die op basis van het voorontwerp zullen worden getroffen, kunnen evenwel een weerslag hebben op operatoren die een infrastructuur exploiteren welke, uit een ander oogpunt beschouwd, tot de bevoegdheid ratione materiae van de gewesten kan behoren, meer in het bijzonder wat betreft de sectoren energie en vervoer, waarop de richtlijn toepassing vindt (artikel 6, § 1, VII en X, van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen).

De steller van het voorontwerp heeft overigens oog gehad voor dit aspect, daar hij de gewesten wenst te 'betrekken' bij het uitwerken van de toepasselijke regelgeving en bij de uitvoering ervan, zoals blijkt uit de volgende bepalingen van het voorontwerp:

– artikel 5, § 1, tweede lid, naar luid waarvan de sectorale overheid³ de Europese kritieke infrastructuur identificeert 'na eensluidend advies van de gewesten voor de potentiële kritieke infrastructuur die onder hun bevoegdheden vallen';

– artikel 6, § 2, naar luid waarvan de sectorale overheid 'de sectorale criteria (bepaalt) waaraan de Europese kritieke infrastructuur moeten beantwoorden, rekening houdend met de bijzondere karakteristieken van de betrokken sector, (...), in voorkomend geval, na eensluidend advies van de betrokken gewesten';

– artikel 6, § 5, naar luid waarvan de sectorale overheid 'geval per geval de drempelwaarden (bepaalt) die van toepassing zijn op de intersectorale criteria waaraan de Europese kritieke infrastructuur dienen te beantwoorden, (...), in voorkomend geval, na eensluidend advies van de betrokken gewesten';

– artikel 7, § 2, tweede lid, naar luid waarvan de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken (hierna 'ADCC' genoemd) 'in samenwerking met (...), in voorkomend geval (...) de betrokken gewesten, belast (is) met het voeren van bilaterale of multilaterale besprekingen met de betrokken lidstaten van de Europese Unie, (...) inzake de potentiële Europese kritieke infrastructuur geïdentificeerd op Belgisch grondgebied (...)';

– artikel 13, § 6, tweede lid, naar luid waarvan 'de Koning bepaalt, in voorkomend geval, met instemming van de betrokken gewesten, voor een bepaalde sector of een deelsector, de frequentie van de oefeningen en van de bijwerkingen' van het beveiligingsplan van de exploitant van een Europese kritieke infrastructuur;

– artikel 24, § 2, tweede lid, naar luid waarvan de Koning 'de nadere regels van [de controle van de inachtneming van

³ Voetnoot 3 van het geciteerde advies: Voetnoot 2 van het geciteerde advies: Voor de Europese kritieke infrastructuur is de federale minister bevoegd voor het Vervoer of diens gemachtigde (artikel 3, 3°, a), van het voorontwerp, dan wel de federale minister bevoegd voor de Energie of diens gemachtigde (artikel 3, 3°, b), van het voorontwerp de sectorale overheid.

les régions concernées', du respect des dispositions de la loi en projet par les exploitants d'infrastructures concernées par celle-ci.

3. Comme les régions détiennent des compétences dans les domaines de l'énergie et du transport, qu'il pourrait en être de même pour d'autres secteurs auxquels la loi en projet s'appliquerait et que, selon l'auteur de l'avant-projet lui-même, dans l'exécution de la loi, l'incidence de certaines des mesures envisagées pourrait affecter la gestion d'infrastructures relevant des compétences régionales, il est admissible d'associer les régions à l'adoption des mesures d'exécution du texte en projet.

Toutefois, ce faisant, il doit le faire d'une manière qui respecte l'autonomie des différents niveaux de pouvoir. Le législateur fédéral ne peut imposer unilatéralement – par le biais d'une loi ordinaire – une collaboration forcée des régions au système mis en place par l'avant-projet. L'intervention des régions ne peut être prévue, si nécessaire, que de façon facultative et en manière telle que leur éventuelle abstention n'empêche pas l'adoption des mesures envisagées par l'autorité fédérale compétente.

4. Si, dans l'avenir, il devait s'avérer que l'adoption des mesures d'exécution de la loi devait impliquer l'exercice conjoint de compétences propres à l'autorité fédérale et aux régions, et non plus uniquement la mise en œuvre de la seule compétence fédérale en matière de sécurité publique, il conviendrait de conclure un accord de coopération avec les régions sur ces questions⁴.

Cette observation vaut *mutatis mutandis* pour l'avant-projet à l'examen, dans le cadre duquel les régions et/ou les communautés sont associées au processus opératoire par l'effet des articles 3, § 3, 3°, 11, §§ 3 et 4, 15, § 2, alinéa 3, et 44, § 1^{er}, alinéa 2, de l'avant-projet, chaque fois d'une manière compatible avec les principes dégagés ci-dessus.

Il ne peut par ailleurs pas être exclu que les communautés et les régions, agissant dans le cadre de leurs compétences matérielles, puissent également elles-mêmes protéger certaines catégories d'intérêts de sécurité qui coïncident avec des éléments sur lesquels se fonde l'appréciation de la sécurité publique⁵.

L'avant-projet ne soulève dès lors aucun problème de compétence au regard de ces principes.

2. De manière complémentaire aux règles générales d'identification, l'article 11 de l'avant-projet charge l'autorité nationale de cybersécurité d'identifier dans certaines circonstances une entité comme entité essentielle ou importante.

⁴ Doc. parl., Chambre, 2018-2019, n° 54-3340/001, pp. 75-87.

⁵ Voir en ce sens l'avis 67.887/1 donné le 28 septembre 2020 sur un avant-projet de loi "visant à instaurer un mécanisme de filtrage des investissements directs étrangers", observation n° 3.1.

de bepalingen van de ontworpen wet door de exploitanten van de bij deze wet bedoelde infrastructuur] kan vastleggen, in voorkomend geval met instemming van de betrokken gewesten'.

3. Aangezien de gewesten bevoegdheden bezitten op het gebied van energie en vervoer, aangezien dit eveneens zou kunnen gelden voor andere sectoren waarop de ontworpen wet toepassing zou vinden en volgens de steller zelf van het voorontwerp bij de uitvoering van de wet de weerslag van sommige van de voorgenoemde maatregelen voelbaar zou kunnen zijn in het beheer van infrastructuur die tot de bevoegdheid van de gewesten behoren, kan worden aanvaard dat de gewesten worden betrokken bij het aannemen van de uitvoeringsmaatregelen omschreven in de ontworpen tekst.

De steller van het voorontwerp moet evenwel aldus te werk gaan dat de autonomie van de verschillende beleidsniveaus in acht wordt genomen. De federale wetgever kan niet eenzijdig – bij wege van een gewone wet – een gedwongen medewerking van de gewesten aan het bij het voorontwerp uitgestippelde systeem opleggen. De medewerking van de gewesten kan dus indien nodig alleen facultatief zijn, en op een zodanige wijze dat, indien ze dat verzuimen, zulks niet verhindert dat de bevoegde federale overheid de voorgenoemde maatregelen kan nemen.

4. Indien in de toekomst mocht blijken dat het aannemen van maatregelen ter uitvoering van de wet inhoudt dat bevoegdheden eigen aan de federale overheid en aan de gewesten gezamenlijk worden uitgeoefend, en niet meer dat uitsluitend de enkele federale bevoegdheid op het gebied van de openbare veiligheid wordt uitgeoefend, moet daaromtrent met de gewesten een samenwerkingsakkoord worden gesloten.⁴

Deze opmerking geldt *mutatis mutandis* voor het voorliggende voorontwerp, in het kader waarvan de gewesten en/of de gemeenschappen bij de gang van zaken worden betrokken ingevolge de artikelen 3, § 3, 3°, 11, §§ 3 en 4, 15, § 2, derde lid, en 44, § 1, tweede lid, van het voorontwerp, telkens op een wijze die verenigbaar is met de hierboven naar voren gebrachte principes.

Voorts valt niet uit te sluiten dat de gemeenschappen en de gewesten, handelend binnen hun materiële bevoegdheden, zelf ook bepaalde categorieën veiligheidsbelangen kunnen beschermen die samenvallen met elementen die de basis vormen voor de beoordeling van de nationale veiligheid.⁵

Ten aanzien van die principes doet het voorontwerp dan ook geen enkel bevoegdheidsprobleem rijzen.

2. In aanvulling op de algemene regels inzake identificatie belast artikel 11 van het voorontwerp de nationale cyberveiligheidsautoriteit ermee om in bepaalde omstandigheden een entiteit als een essentiële of belangrijke entiteit te identificeren.

⁴ Parl.St. Kamer 2018-19, nr. 54-3340/001, 75-87.

⁵ Zie in die zin advies 67.887/1 van 28 september 2020 over een voorontwerp van wet 'tot het invoeren van een mechanisme voor de screening van buitenlandse directe investeringen', opmerking 3.1.

Interrogé quant aux motifs pour lesquels cette mission est confiée à l'autorité nationale de cybersécurité, le délégué du Premier ministre a répondu ce qui suit:

“Les entités essentielles et importantes visées par la directive 2022/2555 (‘directive NIS2’) sont principalement celles répondant aux définitions reprises aux annexes I ou II de la directive NIS2 et, sauf exception, à la taille (équivalente à une entreprise moyenne ou large au sens de l’annexe de la recommandation 2003/361/CE). Il n’y a pas d’identification nécessaire pour ces entités (celles-ci auront au contraire l’obligation de s’enregistrer voir l’art. 13 de l’APL).

Toutefois, les articles 2 (2) b)-e) et 3 (1) e) & (2) de la directive imposent le maintien d’un processus d’identification au niveau national pour certaines entités essentielles ou importantes complémentaires.

Conformément à l’article 11 de l’APL, le choix a été fait de confier à l’autorité nationale de cybersécurité (le projet d’arrêté royal approuvé par le Conseil des ministres prévoit la désignation du Centre pour la Cybersécurité Belgique – ‘CCB’ pour assurer ce rôle) le soin de coordonner le processus d’identification complémentaire et de prendre la décision formelle d’identification, après différentes consultations préalables (l’entité concernée, les éventuelles entités fédérées concernées, les autorités sectorielles concernées ou encore le Comité stratégique du renseignement et de la sécurité).

Il s’agit d’assurer une cohérence avec les autres missions légales confiées à l’autorité nationale de cybersécurité par l’APL (voir l’art. 16 et s. de l’APL): mission de coordination de la loi, mission de supervision (service d’inspection et de sanction), mission de CSIRT national (gestion des incidents), mission de représentation au niveau européen, etc.

S’agissant d’un acte administratif motivé d’une autorité administrative (CCB), l’identification formelle pourra être contestée devant la section du contentieux administratif du Conseil d’État. Ce faisant, les garanties prévues par les lois coordonnées sur le Conseil d’État et la loi sur la motivation formelle des actes administratifs s’appliqueront”.

Néanmoins, en désignant directement des services du pouvoir exécutif pour exercer des missions liées à l’exécution de l’avant-projet et pour prendre des décisions formelles d’identification, le pouvoir législatif s’immisce dans l’organisation interne du pouvoir exécutif. C’est en principe au Roi qu’il revient de désigner ceux de ses services qui seront chargés d’intervenir dans le processus d’identification qui résulte de la mise en œuvre de la loi.

C’est ainsi au Roi qu’il appartient de compléter la liste des entités essentielles et importantes soumises à la loi en application de la directive NIS2 ou de déléguer ce pouvoir à un service relevant de son autorité.

3. Le dispositif en projet fait référence à des textes législatifs en cours d’élaboration.

Op de vraag waarom die opdracht aan de nationale cyberbeveiligingsautoriteit wordt toevertrouwd, heeft de gemachtigde van de eerste minister het volgende geantwoord:

“Les entités essentielles et importantes visées par la directive 2022/2555 (‘directive NIS2’) sont principalement celles répondant aux définitions reprises aux annexes I ou II de la directive NIS2 et, sauf exception, à la taille (équivalente à une entreprise moyenne ou large au sens de l’annexe de la recommandation 2003/361/CE). Il n’y a pas d’identification nécessaire pour ces entités (celles-ci auront au contraire l’obligation de s’enregistrer voir l’art. 13 de l’APL).

Toutefois, les articles 2 (2) b)-e) et 3 (1) e) & (2) de la directive imposent le maintien d’un processus d’identification au niveau national pour certaines entités essentielles ou importantes complémentaires.

Conformément à l’article 11 de l’APL, le choix a été fait de confier à l’autorité nationale de cybersécurité (le projet d’arrêté royal approuvé par le Conseil des ministres prévoit la désignation du Centre pour la Cybersécurité Belgique – ‘CCB’ pour assurer ce rôle) le soin de coordonner le processus d’identification complémentaire et de prendre la décision formelle d’identification, après différentes consultations préalables (l’entité concernée, les éventuelles entités fédérées concernées, les autorités sectorielles concernées ou encore le Comité stratégique du renseignement et de la sécurité).

Il s’agit d’assurer une cohérence avec les autres missions légales confiées à l’autorité nationale de cybersécurité par l’APL (voir l’art. 16 et s. de l’APL): mission de coordination de la loi, mission de supervision (service d’inspection et de sanction), mission de CSIRT national (gestion des incidents), mission de représentation au niveau européen, etc.

S’agissant d’un acte administratif motivé d’une autorité administrative (CCB), l’identification formelle pourra être contestée devant la section du contentieux administratif du Conseil d’État. Ce faisant, les garanties prévues par les lois coordonnées sur le Conseil d’État et la loi sur la motivation formelle des actes administratifs s’appliqueront.”

Niettemin, doordat de wetgevende macht rechtstreeks diensten van de uitvoerende macht aanwijst om opdrachten in verband met de uitvoering van het voorontwerp uit te voeren en om formele beslissingen inzake identificatie te nemen, mengt ze zich in de interne organisatie van de uitvoerende macht. In principe staat het aan de Koning te bepalen welke van zijn diensten een rol dienen te spelen bij de identificatieprocedure die voortvloeit uit de tenuitvoerlegging van de wet.

Zo staat het aan de Koning de lijst van de essentiële en belangrijke entiteiten waarop de wet met toepassing van de NIS 2-richtlijn van toepassing is, aan te vullen, of die bevoegdheid te delegeren aan een dienst die onder zijn gezag ressorteert.

3. In het ontworpen dispositief wordt verwezen naar wetteksten die zich nog in de ontwerpfase bevinden.

Ainsi, à l'article 8, les définitions prévues aux 43°, 45° et 49° comportent une double référence, d'une part, à des textes qui existent et, d'autre part, à des projets de textes législatifs, à savoir respectivement la loi CER et la loi NCCN. La définition prévue au 44° renvoie également à un projet de texte législatif, la loi NPU. L'avant-projet contient en outre, dans diverses dispositions, des références faites aux lois CER, NCCN et NPU.

À ce propos, le délégué du Premier ministre a communiqué les informations suivantes:

“Sur base des dernières informations reçues de nos collègues du Centre de crise national (NCCN), il s'avère l'avant-projet de loi relatif à la planification d'urgence et à la gestion de crise (loi NPU) devrait être soumise prochainement au Conseil des ministres. Pour les autres avant-projets de lois, il semble toutefois que ceux-ci ne seront, en définitive, pas adoptés avant la présente loi.

Ces références ont été volontairement accompagnées ou mentionnées entre crochets dans le dispositif du présent avant-projet de loi pour être adaptées en fonction des derniers développements de ces autres avant-projets.

Il faudra dès lors vraisemblablement remplacer les mentions 'loi CER' par la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques et les mentions 'loi NCCN' par l'arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise”.

Une telle manière de faire ne permet pas à la section de législation de déterminer avec suffisamment de précision la portée et le contenu de certaines dispositions. Tel est le cas, par exemple, de l'article 29 de l'avant-projet portant sur le plan national de réaction aux crises et incidents de cybersécurité majeurs qui renvoie à la loi NPU dont l'avant-projet n'a pas encore été soumis au Conseil des ministres, ainsi que de l'article 68, 5°, de l'avant-projet qui énonce que pour la finalité mentionnée à l'article 67, 5°, de l'avant-projet, sont traitées “les données d'identification des personnes concernées par la coopération dans le cadre de la loi CER”.

Le dispositif sera revu afin de renvoyer aux dispositions pertinentes, à savoir celles qui seront en vigueur au moment où la loi en projet sera publiée et entrera elle-même en vigueur. L'auteur de l'avant-projet s'assurera par ailleurs de la cohérence de l'avant-projet avec les dispositifs légaux auxquels celui-ci renvoie.

Compte tenu de ces incertitudes, il va de soi que l'absence d'observation sur tel ou tel aspect de l'avant-projet dans le présent avis ne saurait être interprétée en ce sens que ces aspects ne soulèvent aucune difficulté juridique en ce qui concerne la correcte transposition de la directive NIS2 et la conformité du dispositif à l'examen aux normes de droit supérieures pertinentes.

Zo bevatten de definities in de punten 43°, 45° en 49° van artikel 8 een dubbele verwijzing, enerzijds naar bestaande teksten en anderzijds naar ontwerpen van wetteksten, namelijk respectievelijk de CER-wet en de NCCN-wet. De definitie in punt 44° verwijst eveneens naar een ontwerp van wettekst, namelijk de NPU-wet. Voorts bevatten verschillende bepalingen van het voorontwerp verwijzingen naar de CER-wet, de NCCN-wet en de NPU-wet.

In dat verband heeft de gemachtigde van de eerste minister de volgende informatie verstrekt:

“Sur base des dernières informations reçues de nos collègues du Centre de crise national (NCCN), il s'avère l'avant-projet de loi relatif à la planification d'urgence et à la gestion de crise (loi NPU) devrait être soumise prochainement au Conseil des ministres. Pour les autres avant-projets de lois, il semble toutefois que ceux-ci ne seront, en définitive, pas adoptés avant la présente loi.

Ces références ont été volontairement accompagnées ou mentionnées entre crochets dans le dispositif du présent avant-projet de loi pour être adaptées en fonction des derniers développements de ces autres avant-projets.

Il faudra dès lors vraisemblablement remplacer les mentions 'loi CER' par la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques et les mentions 'loi NCCN' par l'arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise.”

Met zo'n werkwijze is het voor de afdeling Wetgeving niet mogelijk de draagwijdte en de inhoud van sommige bepalingen nauwkeurig genoeg te bepalen. Dat is bijvoorbeeld het geval met artikel 29 van het voorontwerp, dat betrekking heeft op het nationale plan voor crisisrespons en grootschalige cyberbeveiligingsincidenten en dat verwijst naar de NPU-wet waarvan het voorontwerp nog niet aan de Ministerraad is voorgelegd, alsook met artikel 68, 5°, van het voorontwerp, waarin wordt bepaald dat voor het doeleinde bedoeld in artikel 67, 5°, van het voorontwerp “de identificatiegegevens [worden verwerkt] van de personen die betrokken zijn bij de samenwerking in het kader van de CER-wet”.

Het dispositief moet worden herzien zodat het verwijst naar de relevante bepalingen, namelijk die welke van kracht zullen zijn op het ogenblik dat de ontworpen wet wordt bekendgemaakt en zelf in werking treedt. Voorts moet de steller van het voorontwerp voor samenhang zorgen tussen het voorontwerp en de wetteksten waarnaar het verwijst.

Gezien die onduidelijkheden kan het feit dat in dit advies geen opmerking wordt gemaakt over een of ander aspect van het voorontwerp, vanzelfsprekend niet zo worden geïnterpreteerd dat die aspecten geen enkel juridisch probleem zouden doen rijzen wat betreft de correcte omzetting van de NIS 2-richtlijn en de overeenstemming van het voorliggende dispositief met de relevante hogere rechtsnormen.

OBSERVATIONS PARTICULIÈRESArticle 11

1. Au paragraphe 3, alinéa 2, au lieu de prévoir que lorsqu'aucun avis d'une entité visée à l'alinéa 1^{er} n'est rendu dans le délai prévu par ce même alinéa, "l'avis est réputé être favorable", il sera prévu qu'en l'absence d'un avis rendu dans le délai visé à l'alinéa 1^{er}, il peut être passé outre à l'absence d'avis.

2. Au paragraphe 5, il est prévu ce qui suit:

"Dans les cas visés au paragraphe 1^{er}, le Roi peut, par arrêté délibéré en Conseil des ministres désigner comme entité essentielle ou importante une entité qui ne fait pas partie des secteurs visés en annexe".

Selon le commentaire de l'article,

"[L]e paragraphe 5 prévoit la possibilité pour le Roi, par arrêté délibéré en Conseil des ministres, de désigner individuellement comme entité essentielle ou importante une entité qui ne fait pas partie des secteurs visés en annexe de la loi. En effet, une entité ou un sous-traitant particulier d'une entité NIS pourrait fournir un service critique justifiant d'être soumis aux dispositions de la loi alors que par ailleurs ses activités ne relèvent pas de l'un des secteurs repris dans les annexes de la loi. L'application de cet article est limitée à des cas particuliers et implique au préalable de la décision du Comité stratégique du renseignement et de la sécurité, une concertation entre l'entité concernée, l'autorité nationale de cybersécurité, les entités fédérées et l'éventuelle autorité sectorielle".

Il en résulte que préalablement à la décision du Comité stratégique du renseignement et de la sécurité, "une concertation entre l'entité concernée, l'autorité nationale de cybersécurité, les entités fédérées et l'éventuelle autorité sectorielle" doit avoir lieu.

La disposition sera revue et complétée pour y faire figurer l'encadrement procédural de l'habilitation faite au Roi.

Article 21

Au paragraphe 2, alinéa 2, il est prévu ce qui suit:

"Les finalités poursuivies par les tâches précitées sont:

1° sans préjudice des compétences des personnes exerçant la police judiciaire, notamment des procureurs du Roi, du procureur fédéral ou des procureurs généraux, ni des compétences des juges d'instruction, la prévention, la recherche et la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave;

BIJZONDERE OPMERKINGENArtikel 11

1. In plaats van in paragraaf 3, tweede lid, te bepalen dat "het advies geacht [wordt] gunstig te zijn" indien de in het eerste lid bedoelde entiteit geen advies heeft uitgebracht binnen de daar bedoelde termijn, dient men te schrijven dat wanneer binnen de in het eerste lid bedoelde termijn geen advies is uitgebracht, kan worden voorbijgegaan aan het feit dat geen advies is gegeven.

2. Paragraaf 5 luidt als volgt:

"In de gevallen bedoeld in paragraaf 1 kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, een entiteit die geen deel uitmaakt van de in de bijlage bedoelde sectoren, aanwijzen als een essentiële of belangrijke entiteit."

In de toelichting bij het artikel staat het volgende te lezen:

"Op grond van paragraaf 5 kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, een entiteit die niet tot de in de bijlage bij de wet bedoelde sectoren behoort, individueel aanwijzen als een essentiële of belangrijke entiteit. Een entiteit of een bepaalde onderaannemer van een NIS-entiteit kan immers een kritieke dienst verlenen die rechtvaardigt dat zij of hij onderworpen is aan de bepalingen van de wet, ook al behoren haar of zijn activiteiten niet tot een van de sectoren opgenomen in de bijlagen bij de wet. De toepassing van dit artikel is beperkt tot bijzondere gevallen en houdt in dat, vóór de beslissing van het Strategisch Comité voor Inlichtingen en Veiligheid, overleg wordt gepleegd tussen de betrokken entiteit, de nationale cyberbeveiligingsautoriteit, de deelgebieden en de eventuele sectorale overheid."

Daaruit vloeit voort dat voorafgaand aan de beslissing van het Strategisch Comité voor Inlichtingen en Veiligheid "overleg [moet worden] gepleegd tussen de betrokken entiteit, de nationale cyberbeveiligingsautoriteit, de deelgebieden en de eventuele sectorale overheid".

De bepaling moet worden herzien zodat ze de aan de Koning verleende machtiging procedureel omkadert.

Artikel 21

Paragraaf 2, tweede lid, luidt als volgt:

"De doeleinden van voornoemde taken zijn:

1° onverminderd de bevoegdheden van de personen die de gerechtelijke politie uitoefenen, met name de procureurs des Konings, de federale procureur of de procureurs-generaal, het voorkomen, onderzoeken en opsporen van inbreuken die online of via een elektronisch communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten;

2° la prévention de menaces graves contre la sécurité publique;

3° l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information”.

La section de législation n'aperçoit cependant pas pourquoi le rappel des compétences des personnes exerçant la police judiciaire se limite à l'hypothèse envisagée au 1°.

Interrogé à ce sujet, le délégué du Premier ministre a répondu ce qui suit:

“L'ajout à l'article 21, § 2, alinéa 1^{er} ('sans préjudice des compétences des personnes exerçant la police judiciaire, notamment des procureurs du Roi, du procureur fédéral ou des procureurs généraux, ni des compétences des juges d'instruction') a été inséré au cours des discussions des textes afin de confirmer ce qui était une évidence: les missions de l'autorité nationale de cybersécurité (CCB) s'exercent sans préjudice des missions légales dévolues personnes exerçant la police judiciaire, notamment des procureurs du Roi, du procureur fédéral ou des procureurs généraux, ni des compétences des juges d'instruction.

Le cas échéant, cette mention pourrait accompagner l'ensemble de l'article 21 (lequel a pour vocation initiale d'habiliter l'autorité nationale de cybersécurité à accomplir certaines tâches”.

La précision relative aux compétences des personnes exerçant la police judiciaire figurera dès lors dans la phrase introductive de l'article à l'examen.

Article 23

Le commentaire de la disposition précise que

“[...] toutes les données collectées par le hacker éthique devraient être supprimées dans un délai raisonnable après le signalement. Si cela s'avère nécessaire de conserver ces données encore pendant un certain temps ou si une procédure judiciaire est en cours, le hacker éthique doit veiller à ce que ces données sont conservées en toute sécurité durant cette période”.

Le dispositif sera complété afin d'énoncer le régime relatif à la suppression des données collectées qui est évoqué dans le commentaire de l'article.

Article 26

Au paragraphe 1^{er}, il est prévu que la disposition ne porte pas préjudice à l'application de la loi du 11 décembre 1998 'relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé'.

2° het voorkomen van ernstige bedreigingen voor de openbare veiligheid;

3° het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten of informatiesystemen.”

Het is de afdeling Wetgeving evenwel niet duidelijk waarom de “bevoegdheden van de personen die de gerechtelijke politie uitoefenen” enkel worden gememoreerd in het geval dat in punt 1° wordt bedoeld.

Op die vraag heeft de gemachtigde van de eerste minister het volgende geantwoord:

“L'ajout à l'article 21, § 2, alinéa 1^{er} ('sans préjudice des compétences des personnes exerçant la police judiciaire, notamment des procureurs du Roi, du procureur fédéral ou des procureurs généraux, ni des compétences des juges d'instruction') a été inséré au cours des discussions des textes afin de confirmer ce qui était une évidence: les missions de l'autorité nationale de cybersécurité (CCB) s'exercent sans préjudice des missions légales dévolues personnes exerçant la police judiciaire, notamment des procureurs du Roi, du procureur fédéral ou des procureurs généraux, ni des compétences des juges d'instruction.

Le cas échéant, cette mention pourrait accompagner l'ensemble de l'article 21 (lequel a pour vocation initiale d'habiliter l'autorité nationale de cybersécurité à accomplir certaines tâches.”

De precisering in verband met de bevoegdheden van de personen die de gerechtelijke politie uitoefenen, dient dan ook te worden opgenomen in de inleidende zin van het voorliggende artikel.

Artikel 23

In de toelichting bij de bepaling wordt het volgende gesteld:

“Ook moeten alle door ethische hackers verzamelde gegevens binnen een redelijke termijn na de melding worden verwijderd. Indien het noodzakelijk is om deze gegevens nog enige tijd te bewaren of indien er een gerechtelijke procedure loopt, moeten ethische hackers ervoor zorgen dat deze gegevens in deze periode veilig worden bewaard.”

Het dispositief moet worden aangevuld zodat het melding maakt van de regeling inzake het verwijderen van de verzamelde gegevens, die ter sprake komt in de toelichting bij het artikel.

Artikel 26

In paragraaf 1 wordt gesteld dat de bepaling niet raakt aan de toepassing van de wet van 11 december 1998 'betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst'.

Or, il résulte déjà de l'article 5, § 2, que l'avant-projet est sans préjudice de la loi du 11 décembre 1998.

Le dispositif sera réexaminé et, le cas échéant, revu, afin de veiller à l'articulation des articles 5 et 26 et d'éviter les dispositifs redondants.

Article 29

Compte tenu de l'article 9, paragraphe 4, de la directive NIS2 que l'article 29 tend à transposer et à l'instar de ce que mentionne l'intitulé du chapitre 5 du titre 2 en projet, au paragraphe 1^{er}, première phrase, et dans la phrase introductive du paragraphe 2, les mots "plan national de réaction aux crises et incidents de cybersécurité" seront complétés par le mot "majeurs".

Article 30

Le paragraphe 1^{er} tend à transposer l'article 21, paragraphe 1, alinéa 1^{er}, de la directive NIS2.

Ce dernier prévoit que les États membres veillent à ce que "[l]es entités essentielles et importantes prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services". Or, le paragraphe 1^{er} ne fait mention que de "mesures appropriées et proportionnées" sans préciser qu'il s'agit de mesures "techniques, opérationnelles et organisationnelles" comme le prévoit la directive.

La disposition sera réexaminée et, le cas échéant, revue, afin d'assurer la transposition complète de la directive NIS2.

Article 44

Au paragraphe 1^{er}, le contenu de l'alinéa 2 figure déjà à l'article 39, alinéa 2, de l'avant-projet.

Le dispositif sera réexaminé et, le cas échéant, revu, afin de veiller à l'articulation des articles 39 et 44 et d'éviter les dispositifs redondants.

Article 59

1. À l'alinéa 1^{er}, 1°, de l'accord du délégué du Premier ministre, les mots "à l'article 11, § 5" seront remplacés par les mots "à l'article 12".

Dat het voorontwerp geen afbreuk doet aan de wet van 11 december 1998, blijkt echter al uit artikel 5, § 2.

Men dient het dispositief opnieuw te onderzoeken en in voorkomend geval te herzien, om te zorgen voor samenhang tussen de artikelen 5 en 26 en om overbodige bepalingen te vermijden.

Artikel 29

Gelet op artikel 9, lid 4, van de NIS 2-richtlijn dat bij artikel 29 wordt omgezet, en naar het voorbeeld van hetgeen wordt vermeld in het opschrift van het ontworpen hoofdstuk 5 van titel 2, dient men in paragraaf 1, eerste zin, en in de inleidende zin van paragraaf 2 het woord "grootschalige" in te voegen tussen de woorden "plan voor" en "cyberbeveiligingsincidenten".

Artikel 30

Paragraaf 1 strekt ertoe artikel 21, lid 1, eerste alinea, van de NIS 2-richtlijn om te zetten.

Die laatstgenoemde bepaling stelt het volgende: "De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken". Paragraaf 1 maakt evenwel alleen melding van "passende en evenredige maatregelen", zonder nader te stellen dat het gaat om "technische, operationele en organisatorische maatregelen" zoals bedoeld in de richtlijn.

Men dient de bepaling opnieuw te onderzoeken en in voorkomend geval te herzien, om te zorgen voor de volledige omzetting van de NIS 2-richtlijn.

Artikel 44

De inhoud van het tweede lid van paragraaf 1 staat reeds in artikel 39, tweede lid, van het voorontwerp.

Men dient het dispositief opnieuw te onderzoeken en in voorkomend geval te herzien, om te zorgen voor samenhang tussen de artikelen 39 en 44 en om overbodige bepalingen te vermijden.

Artikel 59

1. De gemachtigde van de eerste minister is het ermee eens dat de woorden "in artikel 11, § 5," in het eerste lid, 1°, moeten worden vervangen door de woorden "in artikel 12".

2. Selon l'alinéa 1^{er}, 3°, "[e]st puni d'une amende de 500 à 200.000 euros quiconque ne se conforme pas aux obligations de contrôle visées au présent titre". Le titre 4 auquel se réfère le dispositif englobe un grand nombre d'obligations.

Comme la section de législation l'a rappelé à diverses reprises, "[l]e droit de ne pas s'auto-incriminer, garanti par l'article 6 de la Convention européenne des droits de l'homme, fait toutefois obstacle à ce qu'une personne, 'pénalement accusée' au sens de cette disposition, puisse être sanctionnée pour avoir refusé de prêter son concours à l'établissement de sa propre culpabilité"⁶.

L'article 48, § 4, alinéa 1^{er}, 3°, de l'avant-projet prévoit que la personne auditionnée par le service de l'inspection a le droit de garder le silence et de ne pas contribuer à sa propre incrimination.

Il faut donc considérer que l'alinéa 1^{er}, 3°, est applicable sans préjudice de l'article 48, § 4, alinéa 1^{er}, 3°, de l'avant-projet.

Partant, et pour éviter toute méprise à ce sujet, mieux vaut ajouter au début de la disposition les mots "Sans préjudice de l'article 48, § 4, alinéa 1^{er}, 3°,".

Article 65

De l'accord du délégué du Premier ministre, les mots "visé à l'alinéa 1^{er}" seront remplacés par les mots "visé à l'article 64".

Article 79

Au 1°, les mots "l'autorité nationale de cybersécurité visée à l'article 8, 47°," seront remplacés par les mots "l'autorité nationale de cybersécurité visée à l'article 8, 46°,".

⁶ Avis 60.619/2 donné le 25 janvier 2017 sur un avant-projet devenu la loi du 2 octobre 2017 'réglementant la sécurité privée et particulière', *Doc. parl.*, Chambre, 2016-2017, n° 54-2388/001, p. 194. Voir aussi l'avis 63.296/4; l'avis 64.879/4 donné le 4 février 2019 sur un avant-projet devenu le décret du 2 mai 2019 'modifiant le Code wallon de l'Action sociale et de la Santé en ce qui concerne la prévention et la promotion de la santé', *Doc. parl.*, Parl. w., 2018-2019, n° 1332/1, pp. 25-35; et l'avis 70.306/2 donné le 23 novembre 2021 sur un avant-projet devenu la loi du 23 février 2022 'visant à mettre en œuvre le règlement (UE) 2020/1503 du parlement européen et du conseil du 7 octobre 2020 relatif aux prestataires européens de services de financement participatif pour les entrepreneurs, et modifiant le règlement (UE) 2017/1129 et la directive (UE) 2019/1937 et à transposer la directive (UE) 2021/338 du parlement européen et du conseil du 16 février 2021 modifiant la directive 2014/65/UE en ce qui concerne les obligations d'information, la gouvernance des produits et les limites de position, et les directives 2013/36/UE et (UE) 2019/878 en ce qui concerne leur application aux entreprises d'investissement, afin de soutenir la reprise à la suite de la crise liée à la COVID-19', *Doc. parl.*, Chambre, 2021-2022, n° 55-2400/001, pp. 84-98.

2. Volgens het eerste lid, 3°, wordt "eenieder die niet voldoet aan de in deze titel bedoelde toezichtverplichtingen (...) bestraft met een geldboete van 500 tot 200.000 euro". Titel 4, waarnaar het dispositief verwijst, omvat een groot aantal verplichtingen.

De afdeling Wetgeving heeft er al herhaaldelijk aan herinnerd dat "[h]et recht om zichzelf niet te beschuldigen, dat gewaarborgd is door artikel 6 van het Europees Verdrag voor de rechten van de mens, (...) er evenwel aan in de weg [staat] dat een persoon, 'tegen wie een vervolging is ingesteld', in de zin van deze bepaling, kan worden bestraft omdat hij geweigerd heeft zijn medewerking te verlenen bij het bewijzen van zijn eigen schuld".⁶

Artikel 48, § 4, eerste lid, 3°, van het voorontwerp bepaalt dat de persoon die door de inspectiedienst wordt verhoord, het recht heeft om te zwijgen en niet bij te dragen tot zijn eigen beschuldiging.

Het eerste lid, 3°, moet dus geacht worden van toepassing te zijn onverminderd artikel 48, § 4, eerste lid, 3°, van het voorontwerp.

Om elke misvatting in dat verband te vermijden, verdient het derhalve aanbeveling aan het begin van de bepaling de woorden "Onverminderd artikel 48, § 4, eerste lid, 3°," toe te voegen.

Artikel 65

De gemachtigde van de eerste minister is het ermee eens dat de woorden "bedoeld in het eerste lid" dienen te worden vervangen door de woorden "bedoeld in artikel 64".

Artikel 79

In de bepaling onder 1° dienen de woorden "de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 47°," te worden vervangen door de woorden "de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 46°,".

⁶ Advies 60.619/2 van 25 januari 2017 over een voorontwerp dat heeft geleid tot de wet van 2 oktober 2017 'tot regeling van de private en bijzondere veiligheid', *Parl. St.* Kamer 2016-17, nr. 54-2388/001, 194. Zie ook advies 63.296/4; advies 64.879/4 van 4 februari 2019 over een voorontwerp dat heeft geleid tot het decreet van 2 mei 2019 'tot wijziging van het Waalse Wetboek van Sociale Actie en Gezondheid wat betreft de preventie en de bevordering van de gezondheid', *Parl. St.* W.Parl 2018-19, nr. 1332/1, 25-35; en advies 70.306/2 van 23 november 2021 over een voorontwerp dat heeft geleid tot de wet van 23 februari 2022 'tot tenuitvoerlegging van verordening (EU) 2020/1503 van het Europees parlement en de raad van 7 oktober 2020 betreffende Europese crowdfundingdienstverleners voor bedrijven en tot wijziging van verordening (EU) 2017/1129 en richtlijn (EU) 2019/1937, en tot omzetting van richtlijn (EU) 2021/338 van het Europees parlement en de raad van 16 februari 2021 tot wijziging van richtlijn 2014/65/EU wat betreft informatievereisten, productgovernance en positiefmilieuen, en richtlijnen 2013/36/EU en (EU) 2019/878 wat betreft de toepassing daarvan op beleggingsondernemingen, om bij te dragen aan het herstel van de COVID-19-crisis (II)', *Parl. St.* Kamer 2021-22, nr. 55-2400/001, 84-98.

La même observation vaut pour le 2°.

Article 83

1. Aux 2° et 3°, les mots “au sens de l'article 8, 24°, de cette même loi” seront insérés après les mots “prestataires de services de confiance”.

2. Au 3°, les mots “comme autorité sectorielle et service d'inspection sectoriel pour” seront remplacés par les mots “comme autorité sectorielle au sens de l'article 8, 55°, de cette même loi et service d'inspection sectoriel au sens de l'article 44, § 1^{er}, alinéa 2, de cette même loi pour”.

Article 85

Dans l'article 2, 94°, en projet (article 85, 5°, de l'avant-projet), les mots “comme prévu dans la loi” seront remplacés par les mots “au sens de l'article 8, 24°, de la loi”.

Article 87

Dans l'article 107/4, § 6, en projet, les mots “dans le chapitre 2 de la loi NIS 2” seront remplacés par les mots “dans le titre 4, chapitre 2, de la loi du [XX XXXX XXXX] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique”.

Annexes

Conformément aux annexes I et II de la directive NIS2, l'intitulé complet des directives et règlements qui y figurent sera inséré dans les tableaux.

OBSERVATIONS FINALES

1. Les tableaux de correspondance, le cas échéant, lus en combinaison avec l'exposé des motifs et le commentaire des articles, doivent notamment permettre d'appréhender la mesure dans laquelle la directive NIS2 est correctement transposée.

Or, il apparaît que les tableaux qui ont été transmis à la section de législation sont, pour plusieurs dispositions de l'avant-projet, en défaut de satisfaire aux exigences de précision auxquelles pareils tableaux doivent se conformer.

2. Ainsi, dans les tableaux, les articles 84 et 87 de l'avant-projet ne constituent pas des dispositions nationales étrangères à la transposition de la directive NIS2, mais constituent au contraire des dispositions transposant cette directive.

3. En outre, il y a lieu, dans le premier tableau, d'indiquer:

– que l'article 3, § 1^{er}, alinéa 2, de l'avant-projet transpose l'article 2, paragraphe 1, alinéa 2, de la directive;

Dezelfde opmerking geldt voor de bepaling onder 2°.

Artikel 83

1. In de bepalingen onder 2° en 3° dienen de woorden “in de zin van artikel 8, 24°, van diezelfde wet” te worden ingevoegd na de woorden “verleners van vertrouwensdiensten”.

2. In de bepaling onder 3° dienen de woorden “als sectorale overheid en sectorale inspectiedienst voor” te worden vervangen door de woorden “als sectorale overheid in de zin van artikel 8, 55°, van diezelfde wet en sectorale inspectiedienst in de zin van artikel 44, § 1, tweede lid, van diezelfde wet, voor”.

Artikel 85

In het ontworpen artikel 2, 94° (artikel 85, 5°, van het voorontwerp) dienen de woorden “zoals bedoeld in de wet” te worden vervangen door de woorden “in de zin van artikel 8, 24°, van de wet”.

Artikel 87

In het ontworpen artikel 107/4, § 6, dienen de woorden “in hoofdstuk 2 van de NIS 2-wet” te worden vervangen door de woorden “in titel 4, hoofdstuk 2, van de wet van [XX XX XXXX] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid”.

Bijlagen

Overeenkomstig de bijlagen I en II van de NIS 2-richtlijn dient het volledige opschrift van de richtlijnen en verordeningen die daarin worden vermeld, in de tabellen te worden ingevoegd.

SLOTOPMERKINGEN

1. De concordantietabellen, in voorkomend geval gelezen in samenhang met de memorie van toelichting en de artikels-gewijze toelichting, moeten het onder meer mogelijk maken na te gaan in welke mate de NIS 2-richtlijn correct is omgezet.

Voor verschillende bepalingen van het voorontwerp blijken de tabellen die aan de afdeling Wetgeving zijn overgezonden, echter niet te beantwoorden aan de nauwkeurigheidsvereisten waaraan ze moeten voldoen.

2. In de tabellen vormen de artikelen 84 en 87 van het voorontwerp aldus geen nationale bepalingen die geen uitstaans hebben met de omzetting van de NIS 2-richtlijn, maar zijn ze integendeel wetsbepalingen tot omzetting van die richtlijn.

3. Voorts dient in de eerste tabel te worden aangegeven:

– dat artikel 3, § 1, tweede lid, van het voorontwerp artikel 2, lid 1, tweede alinea, van de richtlijn omzet;

– que l'article 4, § 4, de l'avant-projet transpose l'article 26, paragraphe 2, de la directive;

– que l'article 5, § 5, de l'avant-projet transpose l'article 2, paragraphe 8, de la directive;

– que l'article 20, 1°, de l'avant-projet transpose l'article 10, paragraphe 3, de la directive;

– que l'article 37, § 2, de l'avant-projet transpose l'article 23, paragraphe 7, de la directive;

– que l'article 37, § 3, de l'avant-projet transpose l'article 23, paragraphe 8, de la directive;

– que l'article 37, § 4, de l'avant-projet transpose l'article 23, paragraphe 9, de la directive;

– que l'article 37, § 5, de l'avant-projet transpose l'article 23, paragraphe 10, de la directive;

– que l'article 46, §§ 2 et 3, de l'avant-projet transpose l'article 37, paragraphe 1, de la directive;

– que l'article 48, § 7, alinéa 2, de l'avant-projet transpose l'article 35, paragraphe 3, de la directive.

4. Les principes de technique législative établis par la section de législation invitent les auteurs d'avant-projets, lors d'une transposition de directive, à établir des tableaux de transposition:

“191. Établissez deux tableaux de transposition.

191.1. Pour contrôler qu'une directive est transposée correctement et complètement, établissez un tableau de correspondance entre les (subdivisions des) articles de la directive et les (subdivisions des) articles de l'acte de transposition que vous rédigez. Mentionnez également dans ce tableau:

a) les (subdivisions des) articles de la directive qui ont éventuellement déjà été transposés, en correspondance avec les actes de droit interne et les (subdivisions des) articles qui ont procédé à cette transposition;

b) les (subdivisions des) articles de la directive qui doivent encore être transposés par une autre autorité.

191.2. Pour pouvoir lire chaque article de l'acte de transposition à la lumière des exigences de la directive, établissez aussi un tableau de correspondance entre les (subdivisions des) articles de l'acte de transposition et les (subdivisions des) articles de la directive”⁷.

⁷ Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires, www.raadvst-consetat.be, onglet “Technique législative”, recommandations n°s 191 à 191.2.

– dat artikel 4, § 4, van het voorontwerp artikel 26, lid 2, van de richtlijn omzet;

– dat artikel 5, § 5, van het voorontwerp artikel 2, lid 8, van de richtlijn omzet;

– dat artikel 20, 1°, van het voorontwerp artikel 10, lid 3, van de richtlijn omzet;

– dat artikel 37, § 2, van het voorontwerp artikel 23, lid 7, van de richtlijn omzet;

– dat artikel 37, § 3, van het voorontwerp artikel 23, lid 8, van de richtlijn omzet;

– dat artikel 37, § 4, van het voorontwerp artikel 23, lid 9, van de richtlijn omzet;

– dat artikel 37, § 5, van het voorontwerp artikel 23, lid 10, van de richtlijn omzet;

– dat artikel 46, §§ 2 en 3, van het voorontwerp artikel 37, lid 1, van de richtlijn omzet;

– dat artikel 48, § 7, tweede lid, van het voorontwerp artikel 35, lid 3, van de richtlijn omzet.

4. Volgens de beginselen van de wetgevingstechniek die de afdeling Wetgeving heeft opgesteld, wordt de stellers van voorontwerpen verzocht om bij de omzetting van richtlijnen omzettingstabellen op te maken:

“191. Maak twee omzettingstabellen op.

191.1. Om te controleren of een richtlijn correct en volledig wordt omgezet, maak een concordantietabel op met de (onderdelen van de) artikelen van de richtlijn en van de er mee overeenstemmende (onderdelen van de) artikelen van de door u opgestelde tekst die in de omzetting voorziet. Vermeld eveneens in deze tabel:

a) de artikelen van de richtlijn die eventueel reeds zijn omgezet, alsmede de overeenstemmende teksten van intern recht en de artikelen waarbij de richtlijn is omgezet;

b) de artikelen van de richtlijn die door een andere instantie nog moeten worden omgezet.

191.2. Om ieder artikel van de tekst die in de omzetting voorziet te kunnen lezen in het licht van de vereisten van de richtlijn, maak eveneens een concordantietabel op met de (onderdelen van de) artikelen van de tekst die in de omzetting voorziet en de (onderdelen van de) artikelen van de richtlijn.”⁷

⁷ Beginselen van de wetgevingstechniek – Handleiding voor het opstellen van wetgevende en reglementaire teksten, www.raadvst-consetat.be, tab “Wetgevingstechniek”, aanbevelingen 191 tot 191.2.

Il convient dès lors de prévoir un tableau reprenant les (subdivisions des) articles de la directive qui doivent encore être transposés par une autre autorité.

*

<i>Le greffier,</i>	<i>Le président,</i>
Charles-Henri VAN HOVE	Bernard BLERO

Er dient derhalve in een tabel te worden voorzien die opgeeft welke (onderdelen van de) artikelen van de richtlijn nog moeten worden omgezet door een andere instantie.

*

<i>De griffier,</i>	<i>De voorzitter,</i>
Charles-Henri VAN HOVE	Bernard BLERO

PROJET DE LOI

PHILIPPE,

ROI DES BELGES,

À tous, présents et à venir,

SALUT.

Sur la proposition du premier ministre et de la ministre de l'Intérieur,

NOUS AVONS ARRÊTÉ ET ARRÊTONS:

Le premier ministre et la ministre de l'Intérieur, sont chargés de présenter, en Notre nom, à la Chambre des représentants, le projet de loi dont la teneur suit:

TITRE 1^{ER}*Définitions et dispositions générales***CHAPITRE 1^{ER}****Objet et champ d'application****Section 1^{re}***Objet***Article 1^{er}**

La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2

La présente loi vise notamment à transposer la directive européenne (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148. Cette directive est dénommée ci-après la "directive NIS2".

WETSONTWERP

FILIP,

KONING DER BELGEN,

Aan allen die nu zijn en hierna wezen zullen,

ONZE GROET.

Op de voordracht van de eerste minister en de minister van Binnenlandse Zaken,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De eerste minister en de minister van Binnenlandse Zaken zijn ermee belast in Onze naam bij de Kamer van volksvertegenwoordigers het ontwerp van wet in te dienen waarvan de tekst hierna volgt:

TITEL 1*Definities en algemene bepalingen***HOOFDSTUK 1****Onderwerp en toepassingsgebied****Afdeling 1***Onderwerp***Artikel 1**

Deze wet regelt een materie als bedoeld in artikel 74 van de Grondwet.

Art. 2

Deze wet voorziet met name in de omzetting van de Europese Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148. Deze richtlijn wordt hierna de "NIS2-richtlijn" genoemd.

Section 2

Champ d'application

Art. 3

§ 1^{er}. Dans les limites de l'article 4 et sans préjudice de l'article 6, la présente loi s'applique aux entités publiques ou privées d'un type visé à l'annexe I ou II et qui constituent:

1° une entreprise moyenne en vertu de l'article 2 de l'annexe de la recommandation n° 2003/361/CE; ou

2° une entreprise qui dépasse les plafonds prévus au § 1^{er} du même article de cette annexe.

L'article 3, § 4, de l'annexe de la recommandation n° 2003/361/CE ne s'applique pas aux fins de la présente loi.

§ 2. Dans le cadre de l'application de l'article 6, paragraphe 2, de l'annexe de la recommandation n° 2003/361/CE, l'autorité nationale de cybersécurité tient compte du degré d'indépendance dont jouit une entité à l'égard de ses partenaires et de ses entreprises liées, en particulier en ce qui concerne les réseaux et les systèmes d'information qu'elle utilise pour fournir ses services et en ce qui concerne les services qu'elle fournit.

Sur base de l'alinéa 1^{er}, l'autorité nationale de cybersécurité considère qu'une telle entité ne constitue pas une entreprise moyenne en vertu de l'article 2 de l'annexe de la recommandation n° 2003/361/CE, ou ne dépasse pas les plafonds applicables à une entreprise moyenne prévus au paragraphe 1 dudit article, si, après prise en compte du degré d'indépendance de ladite entité, celle-ci n'aurait pas été considérée comme constituant une entreprise moyenne ou dépassant lesdits plafonds si seules ses propres données avaient été prises en compte.

Le Roi peut déterminer les critères sur base desquels le degré d'indépendance dont jouit une entité à l'égard de ses partenaires et de ses entreprises liées est évalué.

§ 3. Sans préjudice de l'article 6, la présente loi s'applique également aux entités d'un type visé à l'annexe I ou II, quelle que soit leur taille, dans un des cas suivants:

1° les services sont fournis par:

Afdeling 2

Toepassingsgebied

Art. 3

§ 1. Binnen de grenzen van artikel 4 en onverminderd artikel 6 is deze wet van toepassing op publieke of private entiteiten van een in bijlage I of II bedoelde soort die:

1° een middelgrote onderneming zijn krachtens artikel 2 van de bijlage bij Aanbeveling nr. 2003/361/EG; of

2° een onderneming die de plafonds overschrijdt zoals vastgesteld in lid 1 van hetzelfde artikel van deze bijlage.

Artikel 3, lid 4, van de bijlage bij Aanbeveling nr. 2003/361/EG geldt niet voor de toepassing van deze wet.

§ 2. In het kader van de toepassing van artikel 6, lid 2, van de bijlage bij Aanbeveling nr. 2003/361/EG houdt de nationale cyberbeveiligingsautoriteit rekening met de mate van onafhankelijkheid van een entiteit ten opzichte van haar partnerondernemingen of verbonden ondernemingen, meer bepaald wat de netwerk- en informatiesystemen betreft waarvan zij gebruikmaakt bij het verlenen van haar diensten en wat de diensten betreft die zij verleent.

Op basis van het eerste lid beschouwt de nationale cyberbeveiligingsautoriteit een dergelijke entiteit als een entiteit die niet wordt aangemerkt als een middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling nr. 2003/361/EG, noch de plafonds voor een middelgrote onderneming als bepaald in lid 1 van dat artikel overschrijdt, indien die entiteit, rekening houdend met de mate van onafhankelijkheid die zij geniet, niet als middelgrote onderneming zou worden aangemerkt of niet zou worden geacht die plafonds te overschrijden ingeval alleen rekening zou worden gehouden met haar eigen gegevens.

De Koning kan de criteria bepalen op basis waarvan de mate van onafhankelijkheid van een entiteit ten opzichte van haar partnerondernemingen of verbonden ondernemingen wordt beoordeeld.

§ 3. Onverminderd artikel 6 is deze wet ook van toepassing op entiteiten van een in bijlage I of II bedoelde soort, ongeacht hun omvang, in een van de volgende gevallen:

1° de diensten worden verleend door:

a) des fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public;

b) des prestataires de services de confiance;

c) des registres de noms de domaine de premier niveau et des fournisseurs de services de systèmes de noms de domaine;

2° l'entité est identifiée comme une entité essentielle ou importante conformément au chapitre 4 du présent titre;

3° l'entité est une entité de l'administration publique:

a) qui dépend de l'État fédéral;

b) qui dépend des entités fédérées, identifiée conformément à l'article 11, § 2;

c) qui est une zone de secours au sens de l'article 14 de la loi du 15 mai 2007 relative à la sécurité civile ou le Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale au sens de l'ordonnance du 19 juillet 1990 portant création d'un Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale.

§ 4. Sans préjudice de l'article 6, quelle que soit leur taille, la présente loi s'applique aux entités identifiées comme exploitants d'une infrastructure critique au sens de la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

§ 5. Quelle que soit leur taille, la présente loi s'applique aux entités fournissant des services d'enregistrement de noms de domaine.

§ 6. Après consultation des éventuelles autorités sectorielles concernées et de l'autorité nationale de cybersécurité, le Roi peut, par arrêté délibéré en Conseil des ministres, ajouter d'autres secteurs et/ou sous-secteurs à l'annexe I ou II ou élargir les secteurs et/ou sous-secteurs existants.

Art. 4

§ 1^{er}. La présente loi s'applique aux entités visées à l'article 3 qui sont établies en Belgique et qui fournissent leurs services ou exercent leurs activités au sein de l'Union européenne.

a) aanbieders van openbare elektronische-communicatienetwerken of van openbare elektronische-communicatiediensten;

b) verleners van vertrouwensdiensten;

c) registers voor topleveldomeinnamen en domeinnaamsysteem-dienstverleners;

2° de entiteit wordt geïdentificeerd als een essentiële of belangrijke entiteit overeenkomstig hoofdstuk 4 van deze titel;

3° de entiteit is een overheidsinstantie:

a) die van de Federale Staat afhangt;

b) die van de deelgebieden afhangt, geïdentificeerd overeenkomstig artikel 11, § 2;

c) die een hulpverleningszone is in de zin van artikel 14 van de wet van 15 mei 2007 betreffende de civiele veiligheid of de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp in de zin van de ordonnantie van 19 juli 1990 houdende oprichting van de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp.

§ 4. Onverminderd artikel 6 is deze wet van toepassing op entiteiten, ongeacht hun omvang, die worden geïdentificeerd als exploitanten van een kritieke infrastructuur als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

§ 5. Deze wet is van toepassing op entiteiten, ongeacht hun omvang, die domeinnaamregistratiediensten verlenen.

§ 6. Na raadpleging van de eventuele betrokken sectorale overheden en de nationale cyberbeveiligingsautoriteit kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, andere sectoren en/of deelsectoren toevoegen aan bijlage I of II of de bestaande sectoren en/of deelsectoren uitbreiden.

Art. 4

§ 1. Deze wet is van toepassing op de in artikel 3 bedoelde entiteiten die gevestigd zijn in België en die hun diensten verlenen of hun activiteiten verrichten in de Europese Unie.

§ 2. Par exception au paragraphe 1^{er}, la présente loi s'applique:

1° aux fournisseurs de réseaux de communications électroniques publics ou aux fournisseurs de services de communications électroniques accessibles au public, lorsqu'ils fournissent ces services en Belgique;

2° aux fournisseurs de services DNS, registres de noms de domaine de premier niveau, entités fournissant des services d'enregistrement de noms de domaine, fournisseurs de services d'informatique en nuage, fournisseurs de services de centres de données, fournisseurs de réseaux de diffusion de contenu, fournisseurs de services gérés, fournisseurs de services de sécurité gérés, ainsi qu'aux fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux, lorsqu'ils ont leur établissement principal en Belgique, conformément aux paragraphes 4 et 5.

§ 3. Si une entité visée au paragraphe 2, 2°, n'est pas établie dans l'Union européenne mais y fournit des services, elle désigne un représentant dans l'Union. Le représentant est établi dans l'un des États membres où les services sont fournis.

§ 4. Pour l'application de la présente loi, les entités visées au paragraphe 2, 2°, ont leur établissement principal en Belgique lorsqu'elles y prennent principalement les décisions liées aux mesures de gestion des risques de cybersécurité.

Si l'endroit où ces décisions sont prises ne peut être déterminé ou ne se trouve pas dans l'Union européenne, les entités visées au paragraphe 2, 2°, sont réputées avoir leur établissement principal en Belgique lorsqu'elles y conduisent leurs opérations de cybersécurité.

Si l'endroit où sont conduites ces opérations ne peut être déterminé, les entités visées au paragraphe 2, 2°, sont réputées avoir leur établissement principal en Belgique lorsque s'y trouve leur établissement avec le plus grand nombre d'employés.

§ 5. Les entités visées au paragraphe 2, 2°, sont réputées avoir leur établissement principal en Belgique, pour l'application de la présente loi, lorsqu'elles ne sont pas établies dans l'Union européenne mais qu'elles fournissent leurs services dans l'Union et que leur représentant dans l'Union européenne est établi en Belgique.

§ 6. La désignation d'un représentant par une entité visée au paragraphe 2, 2°, est sans préjudice d'actions en justice qui pourraient être intentées contre l'entité elle-même.

§ 2. In afwijking van paragraaf 1 is deze wet van toepassing op:

1° aanbieders van openbare elektronische-communicatienetwerken of aanbieders van openbare elektronische-communicatiediensten, wanneer zij deze diensten in België verlenen;

2° DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsook op aanbieders van online-marktplaatsen, onlinezoekmachines of platformen voor socialenetwerkdiensten, wanneer zij hun hoofdvestiging in België hebben, overeenkomstig de paragrafen 4 en 5.

§ 3. Indien een entiteit als bedoeld in paragraaf 2, 2°, niet in de Europese Unie is gevestigd, maar diensten in de Unie aanbiedt, wijst zij een vertegenwoordiger in de Unie aan. De vertegenwoordiger is gevestigd in een van de lidstaten waar de diensten worden verleend.

§ 4. Voor de toepassing van deze wet hebben de in paragraaf 2, 2°, bedoelde entiteiten hun hoofdvestiging in België wanneer zij er hoofdzakelijk de beslissingen nemen rond maatregelen voor het beheer van cyberbeveiligingsrisico's.

Indien de plaats waar deze beslissingen worden genomen niet kan worden bepaald of zich niet in de Europese Unie bevindt, worden de in paragraaf 2, 2°, bedoelde entiteiten geacht hun hoofdvestiging in België te hebben wanneer zij er hun cyberbeveiligingsactiviteiten uitvoeren.

Indien de plaats waar deze activiteiten plaatsvinden niet kan worden bepaald, worden de in paragraaf 2, 2°, bedoelde entiteiten geacht hun hoofdvestiging in België te hebben wanneer hun vestiging met het grootste aantal werknemers zich daar bevindt.

§ 5. Voor de toepassing van deze wet worden de in paragraaf 2, 2°, bedoelde entiteiten geacht hun hoofdvestiging in België te hebben, wanneer zij niet gevestigd zijn in de Europese Unie maar hun diensten verlenen in de Unie en hun vertegenwoordiger in de Europese Unie in België gevestigd is.

§ 6. De aanwijzing van een vertegenwoordiger door een entiteit als bedoeld in paragraaf 2, 2°, doet geen afbreuk aan juridische stappen die tegen de entiteit zelf kunnen worden ingesteld.

Art. 5

§ 1^{er}. La présente loi ne porte pas préjudice à l'application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ni aux dispositions légales et réglementaires qui complètent ou précisent ledit règlement ni à la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

§ 2. La présente loi est sans préjudice de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé et ne s'applique pas aux systèmes de communication et d'information approuvés pour utiliser des informations classifiées sous forme électronique conformément à la loi précitée.

§ 3. La présente loi est sans préjudice des règles applicables aux documents nucléaires, au sens de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire.

§ 4. Sous réserve des articles 8 et 38 ainsi que du titre 2, la présente loi ne s'applique pas:

1° aux services de renseignement et de sécurité visés à l'article 2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

2° à l'Organe de coordination pour l'analyse de la menace créé par l'article 5 de la loi du 10 juillet 2006 relative à l'analyse de la menace;

3° au Ministère de la Défense visé à l'article 1^{er} de l'arrêté royal du 2 décembre 2018 déterminant la structure générale du Ministère de la Défense et fixant les attributions de certaines autorités;

4° aux services de police et à l'inspection générale visés à l'article 2, 2° et 3°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux;

Art. 5

§ 1. Deze wet doet geen afbreuk aan de toepassing van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), aan de wettelijke en reglementaire bepalingen die deze verordening aanvullen of verduidelijken of aan de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

§ 2. Deze wet doet geen afbreuk aan de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst en is niet van toepassing op communicatie- en informatiesystemen die zijn goedgekeurd om geclassificeerde informatie in elektronische vorm te gebruiken overeenkomstig de bovengenoemde wet.

§ 3. Deze wet doet geen afbreuk aan de regels die van toepassing zijn op nucleaire documenten in de zin van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.

§ 4. Behoudens de artikelen 8 en 38 en titel 2 is deze wet niet van toepassing op:

1° de inlichtingen- en veiligheidsdiensten bedoeld in artikel 2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

2° het Coördinatieorgaan voor de dreigingsanalyse opgericht bij artikel 5 van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

3° het Ministerie van Landsverdediging bedoeld in artikel 1 van het koninklijk besluit van 2 december 2018 tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en tot vaststelling van de bevoegdheden van bepaalde autoriteiten;

4° de politiediensten en de algemene inspectie bedoeld in artikel 2, 2° en 3°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus;

5° aux autorités judiciaires, entendues comme les organes du pouvoir judiciaire, le Ministère public inclus;

6° au Service public fédéral Justice créé par l'arrêté royal du 23 mai 2001 portant création du Service public fédéral Justice, lorsqu'il gère des banques de données pour les autorités judiciaires visés au 5°;

7° aux réseaux et systèmes d'information des missions diplomatiques et consulaires belges dans des pays tiers à l'Union européenne;

8° aux établissements de classe I au sens de l'article 3.1 de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants.

Par dérogation à l'alinéa 1^{er}, 8°, la présente loi est applicable aux éléments d'une installation nucléaire destinée à la production industrielle d'électricité et qui servent au transport de l'électricité.

§ 5. Les dispositions du titre 3, du titre 4 et du titre 5 ne s'appliquent pas:

1° au NCCN;

2° à l'autorité nationale de cybersécurité visée à l'article 16.

§ 6. Les paragraphes 4 et 5 ne s'appliquent pas lorsqu'une de ces entités agit en tant que prestataire de services de confiance.

Art. 6

§ 1^{er}. Lorsqu'un instrument juridique sectoriel de l'Union européenne impose aux entités qui entrent dans le champ d'application de la présente loi d'adopter des mesures de gestion des risques en matière de cybersécurité ou de notifier des incidents significatifs et lorsque ces exigences ont un effet au moins équivalent à celui des obligations prévues par la présente loi, les dispositions pertinentes de la présente loi ne sont pas applicables à ces entités.

Lorsqu'un instrument juridique sectoriel de l'Union européenne visé à l'alinéa 1^{er} ne couvre pas l'ensemble des entités d'un secteur spécifique entrant dans le champ d'application de la présente loi, les dispositions pertinentes de la présente loi s'appliquent aux entités

5° de rechterlijke overheden, begrepen als de organen van de rechterlijke macht, met inbegrip van het Openbaar Ministerie;

6° de Federale Overheidsdienst Justitie opgericht bij het koninklijk besluit van 23 mei 2001 houdende oprichting van de Federale Overheidsdienst Justitie, wanneer deze databanken beheert voor de rechterlijke overheden bedoeld in 5°;

7° de netwerk- en informatiesystemen van diplomatieke en consulaire missies in landen buiten de Europese Unie;

8° de inrichtingen van klasse I als bedoeld in artikel 3.1 van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen.

In afwijking van het eerste lid, 8°, is deze wet van toepassing op de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van elektriciteit.

§ 5. De bepalingen van titel 3, 4 en 5 zijn niet van toepassing op:

1° het NCCN;

2° de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16.

§ 6. De paragrafen 4 en 5 zijn niet van toepassing wanneer een van deze entiteiten optreedt als verlener van vertrouwensdiensten.

Art. 6

§ 1. Indien een sectorspecifiek rechtsinstrument van de Europese Unie vereist dat entiteiten die tot het toepassingsgebied van deze wet behoren, maatregelen nemen voor het beheer van cyberbeveiligingsrisico's of significante incidenten melden en indien deze eisen ten minste gelijkwaardig zijn aan de in deze wet vastgestelde verplichtingen, zijn de relevante bepalingen van deze wet niet van toepassing op deze entiteiten.

Indien een in het eerste lid bedoeld sectorspecifiek rechtsinstrument van de Europese Unie niet op alle entiteiten in een specifieke sector die tot het toepassingsgebied van deze wet behoort, betrekking heeft, zijn de relevante bepalingen van deze wet van toepassing

non couvertes par cet instrument juridique sectoriel de l'Union européenne.

§ 2. Les exigences visées au paragraphe 1^{er}, alinéa 1^{er}, sont considérées comme ayant un effet équivalent aux obligations de la présente loi lorsque:

1° les mesures de gestion des risques en matière de cybersécurité ont un effet au moins équivalent à celui des mesures prévues à l'article 30; ou

2° l'instrument juridique sectoriel de l'Union européenne prévoit un accès immédiat, s'il y a lieu automatique et direct, aux notifications d'incidents pour le CSIRT national et lorsque les exigences relatives à la notification des incidents importants sont au moins équivalentes aux obligations prévues aux articles 34 à 37.

§ 3. Les dispositions du titre 3, du titre 4 et du titre 5 ne s'appliquent pas aux entités relevant des secteurs bancaire et infrastructures des marchés financiers au sens de l'annexe I qui tombent dans le champ d'application du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) n° 2016/1011, en ce compris l'activité de dépositaire central de titres exercée par la Banque nationale de Belgique.

§ 4. Les dispositions du titre 3, chapitre 1^{er}, du titre 4 et du titre 5 ne s'appliquent pas:

1° à la Banque nationale de Belgique, exception faite de son activité de dépositaire central de titres à laquelle s'applique le paragraphe 3;

2° aux établissements financiers soumis à la supervision de la Banque nationale de Belgique en vertu des articles 8 et 12bis de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique qui ne relèvent pas du paragraphe 3.

Art. 7

Le Roi peut, par arrêté délibéré en Conseil des ministres:

1° préciser les instruments juridiques sectoriels équivalents visés à l'article 6, § 1^{er}, alinéa 1^{er};

2° définir des règles particulières relatives à la coordination de l'échange d'informations, en ce compris

op de entiteiten waarop dit sectorspecifieke rechtsinstrument van de Europese Unie geen betrekking heeft.

§ 2. De in paragraaf 1, eerste lid, bedoelde eisen worden geacht gelijkwaardig te zijn aan de verplichtingen van deze wet wanneer:

1° de maatregelen voor het beheer van cyberbeveiligingsrisico's ten minste gelijkwaardig zijn aan de maatregelen bedoeld in artikel 30; of

2° het sectorspecifieke rechtsinstrument van de Europese Unie in onmiddellijke toegang voorziet, in voorkomend geval automatisch en rechtstreeks, tot de meldingen van incidenten voor het nationale CSIRT en wanneer de eisen voor het melden van significante incidenten ten minste gelijkwaardig zijn aan de verplichtingen bedoeld in de artikelen 34 tot 37.

§ 3. De bepalingen van titel 3, 4 en 5 zijn niet van toepassing op entiteiten die behoren tot de sectoren van het bankwezen en de infrastructuur voor de financiële markt in de zin van bijlage I die onder het toepassingsgebied vallen van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011, met inbegrip van de activiteit van centrale effectenbewaarinstitution vericht door de Nationale Bank van België.

§ 4. De bepalingen van titel 3, hoofdstuk 1, van titel 4 en van titel 5 zijn niet van toepassing:

1° op de Nationale Bank van België, met uitzondering van haar activiteit van centrale effectenbewaarinstitution waarop paragraaf 3 van toepassing is;

2° op financiële instellingen die onderworpen zijn aan het toezicht van de Nationale Bank van België krachtens de artikelen 8 en 12bis van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België en die niet onder paragraaf 3 vallen.

Art. 7

De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad:

1° de gelijkwaardige sectorspecifieke rechtsinstrumenten als bedoeld in artikel 6, § 1, eerste lid, nader bepalen;

2° bijzondere regels vaststellen met betrekking tot de coördinatie van de informatie-uitwisseling, met inbegrip

des exigences relatives à la notification des incidents importants, entre les entités visées à l'article 6, §§ 3 et 4, l'autorité sectorielle concernée, l'autorité nationale de cybersécurité et l'autorité chargée de la gestion des risques cyber.

CHAPITRE 2

Définitions

Art. 8

Pour l'application de la présente loi, il faut entendre par:

1° "réseau et système d'information":

a) un réseau de communications électroniques au sens de l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques;

b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation du processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel; ou

c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance;

2° "sécurité des réseaux et des systèmes d'information": la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à tout événement susceptible de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, ou des services que ces réseaux et systèmes d'information offrent ou rendent accessibles;

3° "cybersécurité": la cybersécurité au sens de l'article 2, 1), du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), ci-après le "règlement sur la cybersécurité";

van de eisen voor het melden van significante incidenten, tussen de entiteiten bedoeld in artikel 6, § 3 en § 4, de betrokken sectorale overheid, de nationale cyberbeveiligingsautoriteit en de autoriteit belast met het beheer van cyberrisico's.

HOOFDSTUK 2

Definities

Art. 8

Voor de toepassing van deze wet moet worden verstaan onder:

1° "netwerk- en informatiesysteem":

a) een elektronische-communicatienetwerk als bedoeld in artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

b) elk apparaat of elke groep van onderling verbonden of bij elkaar behorende apparaten, waarvan er een of meer, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische componenten van dat apparaat die met name de automatisering van het operationele proces, de controle op afstand of het verkrijgen van werkingsgegevens in real time mogelijk maken; of

c) digitale gegevens die worden opgeslagen, verwerkt, opgehaald of verzonden met behulp van de in punten a) en b) bedoelde elementen met het oog op de werking, het gebruik, de bescherming en het onderhoud ervan;

2° "beveiliging van netwerk- en informatiesystemen": het vermogen van netwerk- en informatiesystemen om op een bepaald niveau van betrouwbaarheid weerstand te bieden aan elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die door of via deze netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen;

3° "cyberbeveiliging": cyberbeveiliging als bedoeld in artikel 2, 1), van Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening), hierna de "cyberbeveiligingsverordening" genoemd;

4° “stratégie nationale en matière de cybersécurité”: le cadre cohérent fournissant des objectifs et des priorités stratégiques dans le domaine de la cybersécurité et de la gouvernance en vue de les réaliser en Belgique;

5° “incident”: un événement compromettant la disponibilité, l’authenticité, l’intégrité ou la confidentialité des données stockées, transmises ou faisant l’objet d’un traitement, ou des services que les réseaux et systèmes d’information offrent ou rendent accessibles;

6° “incident évité”: un événement qui aurait pu compromettre la disponibilité, l’authenticité, l’intégrité ou la confidentialité des données stockées, transmises ou faisant l’objet d’un traitement, ou des services que les réseaux et systèmes d’information offrent ou rendent accessibles, mais dont la réalisation a pu être empêchée ou ne s’est pas produite;

7° “incident de cybersécurité majeur”: un incident qui provoque des perturbations dépassant les capacités de réaction du seul État membre de l’Union européenne concerné ou qui a un impact significatif sur au moins deux États membres de l’Union européenne;

8° “traitement des incidents”: toutes les actions et procédures visant à prévenir, détecter, analyser et contenir un incident ou à y répondre et à y remédier;

9° “risque”: le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l’ampleur de cette perte ou de cette perturbation et de la probabilité qu’un tel incident se produise;

10° “cybermenace”: une cybermenace au sens de l’article 2, 8), du règlement sur la cybersécurité;

11° “cybermenace importante”: une cybermenace qui, compte tenu de ses caractéristiques techniques, peut être considérée comme susceptible d’avoir un impact grave sur les réseaux et les systèmes d’information d’une entité ou les utilisateurs des services de l’entité, en causant un dommage matériel, corporel ou moral considérable;

12° “produit TIC”: un produit TIC au sens de l’article 2, 12), du règlement sur la cybersécurité;

13° “service TIC”: un service TIC au sens de l’article 2, 13), du règlement sur la cybersécurité;

14° “processus TIC”: un processus TIC au sens de l’article 2, 14), du règlement sur la cybersécurité;

4° “nationale cyberbeveiligingsstrategie”: een samenhangend kader met strategische doelstellingen en prioriteiten op het vlak van cyberbeveiliging en governance om die doelstellingen en prioriteiten in België te verwezenlijken;

5° “incident”: een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt;

6° “bijna-incident”: een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar had kunnen brengen, maar die met succes is voorkomen of zich niet heeft voorgedaan;

7° “grootschalig cyberbeveiligingsincident”: een incident dat leidt tot een verstoringniveau dat te groot is om door een getroffen lidstaat van de Europese Unie alleen te worden verholpen of dat significante gevolgen heeft voor ten minste twee lidstaten van de Europese Unie;

8° “incidentenbehandeling”: alle acties en procedures die gericht zijn op het voorkomen, opsporen, analyseren en indammen van of het reageren op en het herstellen van een incident;

9° “risico”: de mogelijkheid van verlies of verstoring als gevolg van een incident, wat wordt uitgedrukt als een combinatie van de omvang van een dergelijk verlies of een dergelijke verstoring en de waarschijnlijkheid dat het incident zich voordoet;

10° “cyberdreiging”: een cyberdreiging als bedoeld in artikel 2, 8), van de cyberbeveiligingsverordening;

11° “significante cyberdreiging”: een cyberdreiging waarvan op basis van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerk- en informatiesystemen van een entiteit of de gebruikers van de diensten van de entiteit door het veroorzaken van aanzienlijke materiële of immateriële schade;

12° “ICT-product”: een ICT-product als bedoeld in artikel 2, 12), van de cyberbeveiligingsverordening;

13° “ICT-dienst”: een ICT-dienst als bedoeld in artikel 2, 13), van de cyberbeveiligingsverordening;

14° “ICT-proces”: een ICT-proces als bedoeld in artikel 2, 14), van de cyberbeveiligingsverordening;

15° “vulnérabilité”: une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace;

16° “norme”: une norme au sens de l’article 2, 1), du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil”;

17° “point d’échange internet”: une structure de réseau qui permet l’interconnexion de plus de deux réseaux indépendants (systèmes autonomes), essentiellement aux fins de faciliter l’échange de trafic internet, qui n’assure l’interconnexion que pour des systèmes autonomes et qui n’exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu’il ne modifie ou n’altère par ailleurs un tel trafic;

18° “système de nom de domaine” ou “DNS”: un système hiérarchique et distribué d’affectation de noms qui permet l’identification des services et des ressources internet, ce qui rend possible l’utilisation de services de routage et de connectivité internet par les dispositifs des utilisateurs finaux pour accéder à ces services et ressources;

19° “fournisseur de services DNS”: une entité qui fournit:

a) des services de résolution de noms de domaine récursifs accessibles au public destinés aux utilisateurs finaux de l’internet; ou

b) des services de résolution de noms de domaine faisant autorité pour une utilisation par des tiers, à l’exception des serveurs de noms de racines;

20° “registre de noms de domaine de premier niveau”: une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l’administration du domaine de premier niveau, y compris de l’enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l’exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par

15° “kwetsbaarheid”: een zwakheid, vatbaarheid of gebrek van ICT-producten of ICT-diensten die door een cyberdreiging kan worden uitgebuit;

16° “norm”: een norm als bedoeld in artikel 2, 1), van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad”;

17° “internetknooppunt”: een netwerkfaciliteit die de interconnectie van meer dan twee onafhankelijke netwerken (autonome systemen) mogelijk maakt, voornamelijk ter vergemakkelijking van de uitwisseling van internetverkeer, die alleen interconnectie voor autonome systemen biedt en die niet vereist dat het internetverkeer dat tussen een paar deelnemende autonome systemen verloopt, via een derde autonoom systeem verloopt, noch dat verkeer wijzigt of anderszins verstoort;

18° “domeinnaamsysteem” of “DNS”: een hiërarchisch gedistribueerd naamgevingssysteem dat het mogelijk maakt internetdiensten en -bronnen te identificeren, waardoor eindgebruikersapparaten in staat worden gesteld routing- en connectiviteitsdiensten op het internet te gebruiken om die diensten en bronnen te bereiken;

19° “DNS-dienstverlener”: een entiteit die de volgende diensten verleent:

a) openbare recursieve domeinnaamomzettingsdiensten voor interneteindgebruikers; of

b) gezaghebbende domeinnaamomzettingsdiensten voor gebruik door derden, met uitzondering van root-naamserver;

20° “register voor topleveldomeinnamen”: een entiteit waaraan een specifieke topleveldomeinnaam is gedelegeerd en die verantwoordelijk is voor het beheer van de topleveldomeinnaam, met inbegrip van de registratie van domeinnamen onder de topleveldomeinnaam en de technische exploitatie van de topleveldomeinnaam, met inbegrip van de exploitatie van de naamserver, het onderhoud van de databases en de verdeling van de zonebestanden van de topleveldomeinnaam over de naamserver, ongeacht of die activiteiten door de entiteit zelf worden uitgevoerd of worden uitbesteed, maar met

l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage;

21° "entité fournissant des services d'enregistrement de noms de domaine": un bureau d'enregistrement ou un agent agissant pour le compte de bureaux d'enregistrement, tel qu'un fournisseur ou revendeur de services d'anonymisation ou d'enregistrement fiduciaire;

22° "service numérique": un service au sens de l'article 1^{er}, § 1^{er}, b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information;

23° "service de confiance": un service de confiance au sens de l'article 3, 16., du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, ci-après le "règlement eIDAS";

24° "prestataire de service de confiance": un prestataire de services de confiance au sens de l'article 3, 19., du règlement eIDAS;

25° "service de confiance qualifié": un service de confiance qualifié au sens de l'article 3, 17., du règlement eIDAS;

26° "prestataire de services de confiance qualifiés": un prestataire de services de confiance qualifié au sens de l'article 3, 20., du règlement eIDAS;

27° "place de marché en ligne": une place de marché en ligne au sens de l'article I.8, 41°, du Code de droit économique;

28° "moteur de recherche en ligne": un moteur de recherche en ligne au sens de l'article 2, 5), du règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne;

29° "service d'informatique en nuage": un service numérique qui permet l'administration à la demande et l'accès large à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris lorsque ces ressources sont réparties à différents endroits;

uitzondering van situaties waarin topleveldomeinnamen uitsluitend voor eigen gebruik worden aangewend door een register;

21° "entiteit die domeinnaamregistratiediensten aanbiedt": een registrar of een agent die namens registrators optreedt, zoals een aanbieder van privacy- of proxy-registratiediensten of wederverkoper;

22° "digitale dienst": een dienst als bedoeld in artikel 1, lid 1, b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij;

23° "vertrouwensdienst": een vertrouwensdienst als bedoeld in artikel 3, 16., van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, hierna de "eIDAS-verordening" genoemd;

24° "verlener van vertrouwensdiensten": een verlener van vertrouwensdiensten als bedoeld in artikel 3, 19., van de eIDAS-verordening;

25° "gekwalficeerde vertrouwensdienst": een gekwalificeerde vertrouwensdienst als bedoeld in artikel 3, 17., van de eIDAS-verordening;

26° "gekwalficeerde verlener van vertrouwensdiensten": een gekwalificeerde verlener van vertrouwensdiensten als bedoeld in artikel 3, 20., van de eIDAS-verordening;

27° "onlinemarktplaats": een onlinemarktplaats als bedoeld in artikel I.8, 41°, van het Wetboek van economisch recht;

28° "onlinezoekmachine": een onlinezoekmachine als bedoeld in artikel 2, 5), van Verordening (EU) 2019/1150 van het Europees Parlement en de Raad van 20 juni 2019 ter bevordering van billijkheid en transparantie voor zakelijke gebruikers van onlinetussenhandelsdiensten;

29° "cloudcomputingdienst": een digitale dienst die administratie op aanvraag en brede toegang op afstand tot een schaalbare en elastische pool van deelbare computerbronnen mogelijk maakt, ook wanneer die bronnen over verschillende locaties verspreid zijn;

30° “service de centre de données”: un service qui englobe les structures, ou groupes de structures, dédiées à l’hébergement, l’interconnexion et l’exploitation centralisées des équipements informatiques et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l’ensemble des installations et infrastructures de distribution d’électricité et de contrôle environnemental;

31° “réseau de diffusion de contenu”: un réseau de serveurs géographiquement répartis visant à assurer la haute disponibilité, l’accessibilité ou la fourniture rapide de contenu et de services numériques aux utilisateurs d’internet pour le compte de fournisseurs de contenu et de services;

32° “plateforme de services de réseaux sociaux”: une plateforme qui permet aux utilisateurs finaux de se connecter, de partager, de découvrir et de communiquer entre eux sur plusieurs terminaux, notamment par conversations en ligne, publications, vidéos et recommandations;

33° “représentant”: une personne physique ou morale établie dans l’Union européenne qui est expressément désignée pour agir pour le compte d’un fournisseur de services DNS, d’un registre de noms de domaine de premier niveau, d’une entité fournissant des services d’enregistrement de noms de domaine, d’un fournisseur d’informatique en nuage, d’un fournisseur de services de centre de données, d’un fournisseur de réseau de diffusion de contenu, d’un fournisseur de services gérés, d’un fournisseur de services de sécurité gérés ou d’un fournisseur de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux non établi dans l’Union européenne, qui peut être contactée par l’autorité nationale de cybersécurité à la place de l’entité elle-même concernant les obligations incombant à ladite entité en vertu de la présente loi;

34° “entité de l’administration publique”: une autorité administrative visée à l’article 14, § 1^{er}, alinéa 1^{er}, des lois coordonnées sur le Conseil d’État qui satisfait aux critères suivants:

- a) elle n’a pas de caractère industriel ou commercial;
- b) elle n’exerce pas à titre principal une activité énumérée dans la colonne type d’entité d’un autre secteur ou sous-secteur de l’une des annexes de la loi;
- c) elle n’est pas une personne morale de droit privé.

35° “réseau de communications électroniques public”: un réseau public de communications électroniques au

30° “datacentrumdienst”: een dienst die structuren of groepen van structuren omvat die bestemd zijn voor de gecentraliseerde accommodatie, de interconnectie en de exploitatie van IT- en netwerkkapparatuur die diensten op het gebied van gegevensopslag, -verwerking en -transport aanbiedt, samen met alle faciliteiten en infrastructuur voor energiedistributie en omgevingscontrole;

31° “netwerk voor de levering van inhoud”: een netwerk van geografisch verspreide servers met het oog op een hoge beschikbaarheid, toegankelijkheid of snelle levering van digitale inhoud en diensten aan internetgebruikers ten behoeve van aanbieders van inhoud en diensten;

32° “platform voor socialenetwerkdiensten”: een platform dat eindgebruikers in staat stelt zich met elkaar te verbinden, te delen, te ontdekken en met elkaar te communiceren via meerdere apparaten, met name via chats, posts, video’s en aanbevelingen;

33° “vertegenwoordiger”: een in de Europese Unie gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om op te treden namens een DNS-dienstverlener, een register voor topleveldomeinnamen, een entiteit die domeinnaamregistratiediensten verleent, een aanbieder van cloudcomputingdiensten, een aanbieder van datacentrumdiensten, een aanbieder van een netwerk voor de levering van inhoud, een aanbieder van beheerde diensten, een aanbieder van beheerde beveiligingsdiensten, of een aanbieder van een onlinemarktplaats, van een onlinezoekmachine of van een platform voor socialenetwerkdiensten die niet in de Europese Unie is gevestigd, en die door de nationale cyberbeveiligingsautoriteit kan worden gecontacteerd in plaats van de entiteit zelf met betrekking tot de verplichtingen van die entiteit uit hoofde van deze wet;

34° “overheidsinstantie”: een administratieve overheid als bedoeld in artikel 14, § 1, eerste lid, van de gecoördineerde wetten op de Raad van State die aan de volgende criteria voldoet:

- a) zij is niet van industriële of commerciële aard;
- b) zij oefent niet hoofdzakelijk een activiteit uit, opgesomd in de kolom soort entiteit van een andere sector of deelsector van een van de bijlagen;
- c) zij is geen privaatrechtelijke rechtspersoon.

35° “openbaar elektronische-communicatienetwerk”: een openbaar elektronische-communicatienetwerk als

sens de l'article 2, 10°, de la loi du 13 juin 2005 relative aux communications électroniques;

36° "service de communications électroniques": un service de communications électroniques au sens de l'article 2, 5°, de la loi du 13 juin 2005 relative aux communications électroniques;

37° "entité": une personne physique ou morale constituée et reconnue comme telle en vertu du droit national de son lieu de constitution, et ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations;

38° "fournisseur de services gérés": une entité qui fournit des services liés à l'installation, à la gestion, à l'exploitation ou à l'entretien de produits, de réseaux, d'infrastructures ou d'applications TIC ou d'autres réseaux et systèmes d'information, par l'intermédiaire d'une assistance ou d'une administration active, soit dans les locaux des clients, soit à distance;

39° "fournisseur de services de sécurité gérés": un fournisseur de services gérés qui effectue ou fournit une assistance pour des activités liées à la gestion des risques en matière de cybersécurité;

40° "organisme de recherche": une entité dont l'objectif premier est de mener des activités de recherche appliquée ou de développement expérimental en vue d'exploiter les résultats de cette recherche à des fins commerciales, à l'exclusion des établissements d'enseignement;

41° "recommandation n° 2003/361/CE": la Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises;

42° "loi du 13 juin 2005": la loi du 13 juin 2005 relative aux communications électroniques;

43° "loi du 1^{er} juillet 2011": la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques;

44° "arrêté du 18 avril 1988": l'arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise;

45° "autorité nationale de cybersécurité": l'autorité visée à l'article 16;

46° "CSIRT national": le centre national de réponse aux incidents de sécurité informatique;

bedoeld in artikel 2, 10°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

36° "elektronische-communicatiedienst": een elektronische-communicatiedienst als bedoeld in artikel 2, 5°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

37° "entiteit": een natuurlijke of rechtspersoon die als zodanig is opgericht en erkend volgens het nationale recht van zijn vestigingsplaats, en die in eigen naam rechten kan uitoefenen en aan verplichtingen kan worden onderworpen;

38° "aanbieder van beheerde diensten": een entiteit die diensten verleent die verband houden met de installatie, het beheer, de exploitatie of het onderhoud van ICT-producten, -netwerken, -infrastructuur, -toepassingen of andere netwerk- en informatiesystemen, via bijstand of actieve administratie bij de klanten ter plaatse of op afstand;

39° "aanbieder van beheerde beveiligingsdiensten": een aanbieder van beheerde diensten die bijstand biedt of verleent voor activiteiten die verband houden met risicobeheer op het gebied van cyberbeveiliging;

40° "onderzoeksorganisatie": een entiteit die als hoofddoel heeft het verrichten van toegepast onderzoek of experimentele ontwikkeling met het oog op de exploitatie van de resultaten van dat onderzoek voor commerciële doeleinden, met uitsluiting van onderwijsinstellingen;

41° "Aanbeveling nr. 2003/361/EG": de Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen;

42° "wet van 13 juni 2005": de wet van 13 juni 2005 betreffende de elektronische communicatie;

43° "wet van 1 juli 2011": de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;

44° "koninklijk besluit van 18 april 1988": het koninklijk besluit van 18 april 1988 tot oprichting van het coördinatie- en Crisiscentrum van de regering;

45° "nationale cyberbeveiligingsautoriteit": de autoriteit bedoeld in artikel 16;

46° "nationaal CSIRT": het nationale computer security incident response team;

47° “ENISA”: l’Agence de l’Union européenne pour la cybersécurité instituée par le règlement sur la cybersécurité;

48° “NCCN”: le Centre institué par l’arrêté royal du 18 avril 1988;

49° “règlement (UE) 2016/679”: le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données);

50° “autorité de protection des données”: autorité de contrôle au sens de l’article 4, 21°, du règlement (UE) 2016/679;

51° “organisme national d’accréditation”: l’organisme visé à l’article 2, point 11, du règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l’accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, ci-après le “règlement (CE) n° 765/2008”;

52° “politique de sécurité des systèmes et réseaux d’information (“P.S.I.”)”: la politique consignée dans un document visé à l’article 30, reprenant les mesures de sécurité des réseaux et des systèmes d’information, à adopter par une entité essentielle ou importante;

53° “organisme d’évaluation de la conformité”: l’organisme visé à l’article 2, point 13, du règlement (CE) n° 765/2008;

54° “autorité sectorielle”: l’autorité visée à l’article 15, § 2;

55° “réseau des CSIRT”: le réseau des CSIRT nationaux institué par l’article 15 de la directive NIS2;

56° “groupe de coopération”: le groupe de coopération institué par l’article 14 de la directive NIS2;

57° “incident significatif”: tout incident ayant un impact significatif sur la fourniture de l’un des services fournis dans les secteurs ou sous-secteurs repris à l’annexe I et II de la loi et qui:

1° a causé ou est susceptible de causer une perturbation opérationnelle grave de l’un des services fournis dans les secteurs ou sous-secteurs repris à l’annexe I et II ou des pertes financières pour l’entité concernée; ou

47° “Enisa”: het Agentschap van de Europese Unie voor cyberbeveiliging opgericht bij de cyberbeveiligingsverordening;

48° “NCCN”: het Centrum opgericht door het koninklijk besluit van 18 april 1988;

49° “Verordening (EU) 2016/679”: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);

50° “gegevensbeschermingsautoriteit”: toezichthoudende autoriteit in de zin van artikel 4, 21°, van Verordening (EU) 2016/679;

51° “nationale accreditatie-instantie”: de instantie bedoeld in artikel 2, punt 11, van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93, hierna “Verordening (EG) nr. 765/2008”;

52° “beveiligingsbeleid voor de netwerk- en informatiesystemen (“I.B.B.”)”: het beleid vastgelegd in een document als bedoeld in artikel 30, met de te nemen maatregelen voor de beveiliging van netwerk- en informatiesystemen die een essentiële of belangrijke entiteit heeft genomen;

53° “conformiteitsbeoordelingsinstantie”: de instantie bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008;

54° “sectorale overheid”: de overheid bedoeld in artikel 15, § 2;

55° “CSIRT-netwerk”: het netwerk van nationale CSIRT’s opgericht bij artikel 15 van de NIS2-richtlijn;

56° “samenwerkingsgroep”: de samenwerkingsgroep opgericht bij artikel 14 van de NIS2-richtlijn;

57° “significant incident”: elk incident dat significante gevolgen heeft voor de verlening van een van de diensten in de sectoren of deelsectoren van de bijlagen I en II van de wet en dat:

1° een ernstige operationele verstoring van een van de diensten in de sectoren of deelsectoren van de bijlagen I en II of financiële verliezen voor de betrokken entiteit heeft veroorzaakt of kan veroorzaken; of

2° a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

58° "crise cyber": tout incident de cybersécurité qui, par sa nature ou ses conséquences:

1° menace les intérêts vitaux du pays ou les besoins essentiels de la population;

2° requiert des décisions urgentes;

3° demande une action coordonnée de plusieurs départements et organisations.

59° "Institut": l'Institut belge des services postaux et des télécommunications tel que visé à l'article 13 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.

CHAPITRE 3

Catégories d'entités

Art. 9

Sont des entités essentielles:

1° les entités d'un type visé à l'annexe I qui excèdent les plafonds applicables aux moyennes entreprises prévus à l'article 2, § 1^{er}, de l'annexe de la recommandation n° 2003/361/CE;

2° les prestataires de services de confiance qualifiés et les registres de noms de domaines de premier niveau ainsi que les fournisseurs de services DNS, quelle que soit leur taille;

3° les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public qui constituent au moins des moyennes entreprises, en vertu de l'article 2 de l'annexe de la recommandation n° 2003/361/CE;

4° les entités de l'administration publique qui dépendent de l'État fédéral;

5° les entités visées à l'article 3, § 4;

6° toute autre entité d'un type visé à l'annexe I ou II qui est identifiée comme entité essentielle conformément à l'article 11.

2° andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

58° "cybercrisis": elk cyberbeveiligingsincident dat wegens zijn aard of gevolgen:

1° de vitale belangen van het land of de essentiële behoeften van de bevolking bedreigt;

2° een dringende besluitvorming vereist;

3° en de gecoördineerde inzet van verscheidene departementen en organismen vergt.

59° "Instituut": het Belgisch Instituut voor postdiensten en telecommunicatie zoals bedoeld in artikel 13 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.

HOOFDSTUK 3

Categorieën van entiteiten

Art. 9

Zijn essentiële entiteiten:

1° de entiteiten van een in bijlage I bedoelde soort die de plafonds voor middelgrote ondernemingen overschrijden die zijn vastgesteld in artikel 2, lid 1, van de bijlage bij Aanbeveling nr. 2003/361/EG;

2° de gekwalificeerde verleners van vertrouwensdiensten en de registers voor topleveldomeinnamen, alsook de DNS-dienstverleners, ongeacht hun omvang;

3° de aanbieders van openbare elektronische-communicatienetwerken of van openbare elektronische-communicatiediensten die minstens in aanmerking komen als middelgrote ondernemingen uit hoofde van artikel 2 van de bijlage bij Aanbeveling nr. 2003/361/EG;

4° de overheidsinstanties die van de Federale Staat afhangen;

5° de entiteiten bedoeld in artikel 3, § 4;

6° alle andere entiteiten van een in bijlage I of II bedoelde soort die worden geïdentificeerd als essentiële entiteiten overeenkomstig artikel 11.

Art. 10

Sont des entités importantes:

1° les entités d'un type visé à l'annexe I ou II qui ne sont pas qualifiées d'entités essentielles sur la base de l'article 9;

2° les entités identifiées comme entités importantes conformément à l'article 11.

CHAPITRE 4

Identification

Art. 11

§ 1^{er}. Sans préjudice de l'article 6, d'initiative ou sur proposition de l'éventuelle autorité sectorielle concernée, l'autorité nationale de cybersécurité identifie une entité comme entité essentielle ou importante, quelle que soit sa taille, dans les cas suivants:

1° l'entité est le seul prestataire, en Belgique, d'au moins un service essentiel au maintien d'activités sociétales ou économiques critiques, notamment dans l'un des secteurs ou sous-secteurs repris aux annexes I et II de la loi;

2° une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique;

3° une perturbation du service fourni par l'entité pourrait induire un risque systémique important, en particulier pour les secteurs où une telle interruption pourrait avoir un impact transfrontière;

4° l'entité est critique en raison de son importance spécifique au niveau national ou régional pour le secteur ou le type de service en question, ou pour d'autres secteurs interdépendants, en Belgique.

§ 2. En ce qui concerne les entités qui dépendent des entités fédérées, l'autorité nationale de cybersécurité identifie les administrations publiques qui, à la suite d'une évaluation basée sur les risques, fournissent des services dont la perturbation pourrait avoir un impact important sur des activités sociétales ou économiques critiques.

§ 3. Dans le cadre de l'identification visée aux paragraphes 1^{er} et 2, l'autorité nationale de cybersécurité soumet préalablement un projet de décision à l'entité concernée et ensuite aux éventuelles entités fédérées

Art. 10

Zijn belangrijke entiteiten:

1° de entiteiten van een in bijlage I of II bedoelde soort die niet als essentiële entiteiten worden beschouwd op basis van artikel 9;

2° de entiteiten die worden geïdentificeerd als belangrijke entiteiten overeenkomstig artikel 11.

HOOFDSTUK 4

Identificatie

Art. 11

§ 1. Onverminderd artikel 6 identificeert de nationale cyberbeveiligingsautoriteit, op eigen initiatief of op voorstel van de eventuele betrokken sectorale overheid, een entiteit als een essentiële of belangrijke entiteit, ongeacht haar omvang, in de volgende gevallen:

1° de entiteit is de enige aanbieder, in België, van minstens één dienst die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten, met name in een van de sectoren of deelsectoren van de bijlagen I en II van de wet;

2° een verstoring van de door de entiteit verleende dienst kan aanzienlijke gevolgen hebben voor de openbare veiligheid, de openbare beveiliging of de volksgezondheid;

3° een verstoring van de door de entiteit verleende dienst kan een aanzienlijk systeemrisico met zich brengen, met name voor sectoren waar een dergelijke verstoring een grensoverschrijdende impact kan hebben;

4° de entiteit is kritiek vanwege het specifieke belang ervan op nationaal of regionaal niveau voor de specifieke sector of het specifieke type dienst, of voor andere onderling afhankelijke sectoren in België.

§ 2. Wat betreft de entiteiten die van de deelgebieden afhangen, identificeert de nationale cyberbeveiligingsautoriteit overheidsinstanties die, na een risicobeoordeling, diensten verlenen waarvan de verstoring aanzienlijke gevolgen kan hebben voor kritieke maatschappelijke of economische activiteiten.

§ 3. In het kader van de identificatie bedoeld in de paragrafen 1 en 2 legt de nationale cyberbeveiligingsautoriteit vooraf een ontwerpbeslissing voor aan de betrokken entiteit en vervolgens aan de eventuele betrokken

concernées et autorités sectorielles, qui rendent un avis non publié endéans les soixante jours.

En l'absence d'un avis rendu dans le délai visé à l'alinéa 1^{er}, il peut être passé outre à l'absence d'avis.

En cas d'avis défavorable d'une autorité sectorielle et si l'autorité nationale de cybersécurité souhaite maintenir son projet de décision, le projet de décision, accompagné de l'avis, est soumis au Comité stratégique du renseignement et de la sécurité, créé par l'arrêté royal du 22 décembre 2020 portant création du Conseil national de sécurité, du Comité stratégique du renseignement et de la sécurité et du Comité de coordination du renseignement et de la sécurité, qui rend un avis contraignant.

§ 4. L'autorité nationale de cybersécurité évalue et, le cas échéant, met à jour l'identification des entités essentielles et importantes au moins tous les deux ans, selon les modalités visées aux paragraphes 1^{er} à 3.

L'autorité nationale de cybersécurité adresse les identifications et actualisations des entités essentielles au NCCN et à l'éventuelle autorité sectorielle concernée.

L'autorité nationale de cybersécurité adresse les identifications et actualisations des entités importantes à l'éventuelle autorité sectorielle concernée.

§ 5. Dans les cas visés au paragraphe 1^{er}, le Roi peut, par arrêté délibéré en Conseil des ministres, désigner comme entité essentielle ou importante une entité qui ne fait pas partie des secteurs visés en annexe.

Art. 12

Dans le cadre de l'identification visée à l'article 11, l'entité concernée transmet toutes les informations utiles à son éventuelle identification, à la demande de l'autorité nationale de cybersécurité ou de l'autorité sectorielle.

CHAPITRE 5

Enregistrement des entités

Art. 13

§ 1^{er}. Dans les cinq mois suivant l'entrée en vigueur de la loi ou l'identification visée à l'article 11, les entités

deelgebieden en sectorale overheden, die binnen zestig dagen een niet-gepubliceerd advies uitbrengen.

Indien binnen de in het eerste lid bedoelde termijn geen advies is uitgebracht, kan worden voorbijgegaan aan het feit dat geen advies gegeven is.

In geval van een ongunstig advies van een sectorale overheid en indien de nationale cyberbeveiligingsautoriteit haar ontwerpbeslissing wenst te handhaven, wordt de ontwerpbeslissing samen met het advies voorgelegd aan het Strategisch Comité Inlichtingen en Veiligheid, opgericht bij het koninklijk besluit van 22 december 2020 tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité Inlichtingen en Veiligheid en het Coördinatiecomité Inlichtingen en Veiligheid die een bindend advies uitbrengen.

§ 4. De nationale cyberbeveiligingsautoriteit evalueert en actualiseert, in voorkomend geval, minstens om de twee jaar de identificatie van essentiële en belangrijke entiteiten volgens de modaliteiten bedoeld in de paragrafen 1 tot 3.

De nationale cyberbeveiligingsautoriteit stuurt de identificaties en actualiseringen van essentiële entiteiten naar het NCCN en naar de eventuele betrokken sectorale overheid.

De nationale cyberbeveiligingsautoriteit stuurt de identificaties en actualiseringen van belangrijke entiteiten naar de eventuele betrokken sectorale autoriteit.

§ 5. In de gevallen bedoeld in paragraaf 1 kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, een entiteit die geen deel uitmaakt van de in de bijlage bedoelde sectoren, aanwijzen als een essentiële of belangrijke entiteit.

Art. 12

In het kader van de identificatie bedoeld in artikel 11 bezorgt de betrokken entiteit op verzoek van de nationale cyberbeveiligingsautoriteit of de sectorale overheid, alle informatie die nuttig is voor haar eventuele identificatie.

HOOFDSTUK 5

Registratie van de entiteiten

Art. 13

§ 1. Binnen vijf maanden na de inwerkingtreding van de wet of de in artikel 11 bedoelde identificatie registreren

essentiellens, les entités importantes et les entités fournissant des services d'enregistrement de noms de domaine s'enregistrent auprès de l'autorité nationale de cybersécurité selon les modalités pratiques fixées par cette autorité et lui communiquent les informations suivantes:

1° leur dénomination ainsi que leur numéro d'enregistrement auprès de la Banque-carrefour des entreprises (BCE) ou un enregistrement équivalent dans l'Union européenne;

2° leur adresse et leurs coordonnées actualisées, y compris leur adresse de courrier électronique, leurs plages d'IP et leur numéro de téléphone;

3° le cas échéant, le secteur et le sous-secteur concernés visés à l'annexe I ou II; et

4° le cas échéant, une liste des États membres dans lesquels elles fournissent des services relevant du champ d'application de la présente loi.

Le Roi peut compléter cette liste d'informations.

§ 2. Par dérogation au paragraphe 1^{er}, alinéa 1^{er}, lorsque l'entité visée au paragraphe précité communique déjà à l'autorité sectorielle concernée certaines des informations visées au paragraphe précité, en vertu d'une obligation légale, l'entité complète auprès de cette autorité sectorielle ces informations.

L'entité visée au paragraphe 1^{er}, alinéa 1^{er}, communique les informations dans les cinq mois suivant l'entrée en vigueur de la loi, selon les modalités pratiques fixées par l'autorité précitée.

§ 3. Les entités visées au paragraphe 1^{er}, alinéa 1^{er}, communiquent sans tarder toute modification des informations qu'elles ont communiquées conformément au paragraphe 1^{er}, alinéa 1^{er}, et paragraphe 2, alinéa 1^{er}, et, en tout état de cause, dans un délai de deux semaines à compter de la date de la modification.

§ 4. L'autorité sectorielle concernée communique les informations collectées en vertu des paragraphes 2 et 3 à l'autorité nationale de cybersécurité.

L'autorité nationale de cybersécurité prend les mesures nécessaires pour que les autorités sectorielles puissent consulter, pour les secteurs qui les concernent, les données communiquées.

essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen zich bij de nationale cyberbeveiligingsautoriteit volgens de door deze autoriteit vastgestelde praktische modaliteiten en bezorgen haar de volgende informatie:

1° hun naam, alsook hun registratienummer bij de Kruispuntbank van Ondernemingen (KBO) of een gelijkwaardige registratie in de Europese Unie;

2° hun adres en hun actuele contactgegevens, waaronder hun e-mailadres, hun IP-bereiken en hun telefoonnummer;

3° indien van toepassing, de relevante sector en deelsector als bedoeld in bijlage I of II, en

4° indien van toepassing, een lijst van de lidstaten waar zij diensten verlenen die binnen het toepassingsgebied van deze wet vallen.

De Koning kan deze lijst met informatie aanvullen.

§ 2. In afwijking van paragraaf 1, eerste lid, vervolledigt de in voornoemde paragraaf bedoelde entiteit, wanneer zij krachtens een wettelijke verplichting al een deel van de in voornoemde paragraaf bedoelde informatie meedeelt aan de betrokken sectorale overheid, deze informatie bij deze sectorale overheid.

De in paragraaf 1, eerste lid, bedoelde entiteit bezorgt de informatie binnen vijf maanden na de inwerkingtreding van de wet, volgens de door voornoemde overheid vastgestelde praktische modaliteiten.

§ 3. De in paragraaf 1, eerste lid, bedoelde entiteiten bezorgen onmiddellijk elke wijziging in de bijzonderheden die zij op grond van paragraaf 1, eerste lid, en paragraaf 2, eerste lid, hebben ingediend, en in elk geval binnen twee weken na de datum van de wijziging.

§ 4. De betrokken sectorale overheid bezorgt de krachtens de paragrafen 2 en 3 verzamelde informatie aan de nationale cyberbeveiligingsautoriteit.

De nationale cyberbeveiligingsautoriteit neemt de nodige maatregelen om ervoor te zorgen dat de sectorale overheden de meegedeelde gegevens kunnen raadplegen voor de sectoren die hen aangaan.

Art. 14

§ 1^{er}. Dans les deux mois suivant l'entrée en vigueur de la loi, les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les entités qui fournissent des services d'enregistrement de noms de domaine, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux communiquent à l'autorité nationale de cybersécurité, selon les modalités visées à l'article 13, § 1^{er}, alinéa 1^{er}, au moins les informations suivantes:

1° leur nom;

2° leur secteur, sous-secteur et type d'entité concernés, visés à l'annexe I ou II, le cas échéant;

3° l'adresse de leur établissement principal et de leurs autres établissements légaux dans l'Union ou, s'ils ne sont pas établis dans l'Union, de leur représentant désigné conformément à l'article 4, § 3;

4° leurs coordonnées actualisées, y compris les adresses de courrier électronique et les numéros de téléphone et, le cas échéant, celles de leur représentant désigné conformément à l'article 4, § 3;

5° les États membres dans lesquels ils fournissent leurs services relevant du champ d'application de la présente loi; et

6° leurs plages d'IP.

§ 2. Les entités visées au paragraphe 1^{er} notifient à l'autorité nationale de cybersécurité toute modification des informations qu'elles ont communiquées en vertu du paragraphe 1^{er} sans tarder et, en tout état de cause, dans un délai de trois mois à compter de la date de la modification.

§ 3. Par dérogation au paragraphe 1^{er}, les données visées au même paragraphe, relatives aux prestataires de services de confiance qualifiés en Belgique, qui ont déjà été communiquées à l'organe de contrôle visé à l'article 17 du règlement eIDAS sont transmises par cet organe à l'autorité nationale de cybersécurité, selon les modalités fixées par le Roi.

Art. 14

§ 1. Binnen twee maanden na de inwerkingtreding van de wet verstrekken DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaam-registratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsmede aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor sociale netwerkdiensten de nationale cyberbeveiligingsautoriteit volgens de modaliteiten bedoeld in artikel 13, § 1, eerste lid, ten minste de volgende informatie:

1° hun naam;

2° hun relevante sector, deelsector en soort entiteit bedoeld in bijlage I of II, waar van toepassing;

3° het adres van hun hoofdvestiging en hun andere wettelijke vestigingen in de Unie of, indien deze niet in de Unie zijn gevestigd, van hun op grond van artikel 4, § 3, aangewezen vertegenwoordiger;

4° hun actuele contactgegevens, met inbegrip van e-mailadressen en telefoonnummers en, indien van toepassing, deze van hun op grond van artikel 4, § 3, aangewezen vertegenwoordiger;

5° de lidstaten waar ze hun diensten verlenen die tot het toepassingsgebied van deze wet behoren; en

6° hun IP-bereiken.

§ 2. De in paragraaf 1 bedoelde entiteiten stellen de nationale cyberbeveiligingsautoriteit onverwijld en in elk geval binnen drie maanden na de datum waarop de wijziging van kracht is geworden, in kennis van eventuele wijzigingen in de gegevens die zij op grond van paragraaf 1 hebben ingediend.

§ 3. In afwijking van paragraaf 1 worden de in diezelfde paragraaf bedoelde gegevens met betrekking tot gekwalificeerde verleners van vertrouwensdiensten in België, die al zijn verstrekt aan het in artikel 17 van de eIDAS-verordening bedoelde toezichthoudende orgaan, door dat orgaan doorgestuurd naar de nationale cyberbeveiligingsautoriteit, volgens de door de Koning vastgestelde modaliteiten.

TITRE 2

*Autorités compétentes et coopération au niveau national*CHAPITRE 1^{ER}**Autorités compétentes****Section 1^{re}***Désignation des autorités compétentes*

Art. 15

§ 1^{er}. Le Roi désigne l'autorité nationale de cybersécurité.

§ 2. Après avis de l'autorité nationale de cybersécurité, le Roi peut, par arrêté délibéré en Conseil des ministres, désigner une autorité sectorielle et, le cas échéant, un service d'inspection sectoriel chargé, pour un secteur ou sous-secteur spécifique, de la supervision de la mise en œuvre des mesures sectorielles ou sous-sectorielles supplémentaires de gestion des risques en matière de cybersécurité visées à l'article 33.

Dans le cadre de la désignation visée à l'alinéa 1^{er}, le Roi tient compte de l'identité des autorités sectorielles et services d'inspection sectoriels désignées dans le cadre de la loi du 1^{er} juillet 2011.

Le Roi peut, par arrêté délibéré en Conseil des ministres, créer des autorités sectorielles, composées de représentants de l'État fédéral, des Communautés et des Régions, conformément aux modalités prévues à l'article 92^{ter} de la loi spéciale du 8 août 1980 de réformes institutionnelles.

Par dérogation à l'alinéa 1^{er}, la loi désigne elle-même les autorités sectorielles et les services d'inspection créés et régies par la loi.

Section 2*L'autorité nationale de cybersécurité*

Art. 16

L'autorité nationale de cybersécurité est chargée du suivi et de la coordination de la mise en œuvre de la présente loi, de veiller à la mise en œuvre de la présente loi par les entités essentielles et importantes ainsi que de la gestion des crises cyber et incidents de cybersécurité conformément à l'article 18.

TITEL 2

Bevoegde autoriteiten en samenwerking op nationaal niveau

HOOFDSTUK 1

Bevoegde autoriteiten**Afdeling 1***Aanwijzing van de bevoegde autoriteiten*

Art. 15

§ 1. De Koning wijst de nationale cyberbeveiligingsautoriteit aan.

§ 2. Na advies van de nationale cyberbeveiligingsautoriteit kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, een sectorale overheid en, in voorkomend geval, een sectorale inspectiedienst aanwijzen die voor een specifieke sector of deelsector belast is met het toezicht op de uitvoering van de bijkomende sectorale of deelsectorale maatregelen voor het beheer van cyberbeveiligingsrisico's als bedoeld in artikel 33.

In het kader van de aanwijzing bedoeld in het eerste lid houdt de Koning rekening met de identiteit van de in het kader van de wet van 1 juli 2011 aangewezen sectorale overheden en sectorale inspectiediensten.

De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad, sectorale overheden oprichten, bestaande uit vertegenwoordigers van de Federale Staat, de Gemeenschappen en de Gewesten, overeenkomstig de modaliteiten bepaald in artikel 92^{ter} van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.

In afwijking van het eerste lid wijst de wet zelf de bij wet opgerichte en geregelde sectorale overheden en sectorale inspectiediensten aan.

Afdeling 2*De nationale cyberbeveiligingsautoriteit*

Art. 16

De nationale cyberbeveiligingsautoriteit is belast met de opvolging en coördinatie van de uitvoering van deze wet, het toezicht op de uitvoering ervan door de essentiële en belangrijke entiteiten, alsook met het beheer van cybercrises en cyberbeveiligingsincidenten overeenkomstig artikel 18.

À ce titre, l'autorité nationale de cybersécurité assure les tâches d'autorité compétente pour les entités essentielles et importantes, de CSIRT national, de point de contact national unique pour l'exécution de la présente loi et de représentation de la Belgique au sein du groupe de coopération, du réseau des CSIRT et du réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONE) visé à l'article 16 de la directive NIS2.

Sous-section 1^{re}

Tâches relatives au rôle d'autorité compétente chargée de la cybersécurité

Art. 17

Les tâches de l'autorité nationale de cybersécurité sont les suivantes:

1° assurer la coordination entre les autorités compétentes dans le cadre de l'application de la présente loi, ainsi qu'entre les différents services et autorités concernés par la cybersécurité en Belgique;

2° superviser, coordonner et veiller à la mise en œuvre de la stratégie nationale en matière de cybersécurité visée à l'article 28;

3° identifier des entités essentielles et importantes conformément à l'article 11;

4° superviser la mise en œuvre de la loi par les entités essentielles et importantes conformément au titre 4;

5° assurer la coordination entre les autorités publiques et le secteur privé ou le monde scientifique;

6° formuler des propositions pour l'adaptation du cadre légal et réglementaire en matière de cybersécurité;

7° élaborer, diffuser et veiller à la mise en œuvre des standards, directives et normes pour la cybersécurité des différents types de systèmes d'information;

8° coordonner la représentation belge aux forums internationaux sur la cybersécurité, le suivi des obligations internationales et la présentation du point de vue national en la matière;

9° servir de point de contact unique exerçant une fonction de liaison visant à assurer, dans le cadre de l'application de la présente loi, la coopération transfrontière des autorités belges avec les autorités compétentes

Daartoe vervult de nationale cyberbeveiligingsautoriteit de taken van bevoegde autoriteit voor essentiële en belangrijke entiteiten, van nationaal CSIRT, van centraal nationaal contactpunt voor de uitvoering van deze wet, en vertegenwoordigt zij België in de samenwerkingsgroep, het CSIRT-netwerk en het Europees netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONE) bedoeld in artikel 16 van de NIS2-richtlijn.

Onderafdeling 1

Taken met betrekking tot de rol van bevoegde autoriteit belast met cyberbeveiliging

Art. 17

De nationale cyberbeveiligingsautoriteit heeft de volgende taken:

1° het zorgen voor coördinatie tussen de bevoegde autoriteiten in het kader van de toepassing van deze wet, alsook tussen de verschillende diensten en autoriteiten die betrokken zijn bij cyberbeveiliging in België;

2° het opvolgen en coördineren van en toezien op de uitvoering van de nationale cyberbeveiligingsstrategie bedoeld in artikel 28;

3° het identificeren van de essentiële en belangrijke entiteiten overeenkomstig artikel 11;

4° het toezien op de uitvoering van de wet door de essentiële en belangrijke entiteiten overeenkomstig titel 4;

5° het zorgen voor coördinatie tussen de overheden en de particuliere sector of de wetenschappelijke wereld;

6° het formuleren van voorstellen tot aanpassing van het wettelijk en regelgevend kader op het vlak van cyberbeveiliging;

7° het opstellen, verspreiden en toezien op de uitvoering van standaarden, richtlijnen en normen voor de cyberbeveiliging van de verschillende soorten informatiesystemen;

8° het coördineren van de Belgische vertegenwoordiging in internationale fora voor cyberbeveiliging, van de opvolging van internationale verplichtingen en van voorstellen van het nationale standpunt op dit vlak;

9° het fungeren als centraal contactpunt dat een verbindingsfunctie vervult om, in het kader van de toepassing van deze wet, te zorgen voor grensoverschrijdende samenwerking van de Belgische autoriteiten

des autres États membres de l'Union européenne et, le cas échéant, avec la Commission et l'ENISA, ainsi qu'à garantir la coopération intersectorielle avec les autres autorités compétentes belges;

10° coordonner l'évaluation et la certification de la sécurité des systèmes d'information et de communication;

11° informer et sensibiliser les utilisateurs des systèmes d'information et de communication;

12° accorder des subventions pour des projets et activités relatifs à la cybersécurité, dans les limites de ses crédits budgétaires et selon les conditions établies par le Roi;

13° faciliter et encourager l'organisation de formations en matière de cybersécurité pour les membres du personnel des entités essentielles ou importantes;

14° établir une liste des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine. Par la suite, réexaminer cette liste et, le cas échéant, la mettre à jour régulièrement et au moins tous les deux ans.

Sous-section 2

Tâches relatives au rôle de gestion des crises cyber

Art. 18

Sans préjudice des articles 8 et 9 de la loi du 15 mai 2007 relative à la sécurité civile et de leurs arrêtés d'exécution et sans préjudice des compétences du NCCN, les tâches de l'autorité nationale de cybersécurité relatives au rôle de gestion des crises cyber sont les suivantes:

1° en collaboration avec le NCCN, recenser les capacités, les moyens et les procédures qui peuvent être déployés en cas de crise cyber;

2° superviser, en collaboration avec le NCCN, la rédaction, l'actualisation et l'opérationnalisation du plan national de réaction aux crises cyber et incidents de cybersécurité visé à l'article 29;

3° assurer le rôle de coordinateur dans la gestion des crises cyber et incidents de cybersécurité, le cas échéant conformément au plan visé au 2°.

met de bevoegde autoriteiten van andere lidstaten van de Europese Unie en in voorkomend geval met de Commissie en Enisa, alsmede om te zorgen voor sectoroverschrijdende samenwerking met andere bevoegde Belgische autoriteiten;

10° het coördineren van de evaluatie en certificering van de beveiliging van informatie- en communicatiesystemen;

11° het informeren en sensibiliseren van gebruikers van informatie- en communicatiesystemen;

12° het toekennen van subsidies voor projecten en activiteiten rond cyberbeveiliging, binnen de grenzen van haar begrotingskredieten en volgens de voorwaarden bepaald door de Koning;

13° het faciliteren en aanmoedigen van de organisatie van opleidingen rond cyberbeveiliging voor personeelsleden van essentiële of belangrijke entiteiten;

14° het opstellen van een lijst van essentiële en belangrijke entiteiten, alsook van entiteiten die domeinnaamregistratiediensten verlenen. Vervolgens het regelmatig en ten minste om de twee jaar evalueren en, in voorkomend geval, actualiseren van die lijst.

Onderafdeling 2

Taken met betrekking tot het cybercrisisbeheer

Art. 18

Onverminderd de artikelen 8 en 9 van de wet van 15 mei 2007 betreffende de civiele veiligheid en de uitvoeringsbesluiten ervan en onverminderd de bevoegdheden van het NCCN vervult de nationale cyberbeveiligingsautoriteit de volgende taken met betrekking tot het cybercrisisbeheer:

1° in samenwerking met het NCCN, het vaststellen van de capaciteiten, middelen en procedures die in geval van een cybercrisis kunnen worden ingezet;

2° het opvolgen van de opmaak, actualisering en operationalisering van het nationale plan voor cyberbeveiligingsincidenten en cybercrisisrespons bedoeld in artikel 29, in samenwerking met het NCCN;

3° het vervullen van de rol van coördinator bij het beheer van cybercrises en cyberbeveiligingsincidenten, in voorkomend geval overeenkomstig het in 2° bedoelde plan.

*Sous-section 3**Tâches et obligations
relatives au rôle de CSIRT national*

Art. 19

§ 1^{er}. Les tâches du CSIRT national, sont les suivantes:

1° surveiller et analyser les cybermenaces, les vulnérabilités et les incidents au niveau national et, sur demande, apporter une assistance aux entités essentielles et importantes concernées pour surveiller en temps réel ou quasi réel leurs réseaux et systèmes d'information;

2° activer le mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les cybermenaces, les vulnérabilités et les incidents auprès des entités essentielles et importantes concernées ainsi qu'auprès des autorités compétentes et des autres parties prenantes concernées, si possible en temps quasi réel;

3° réagir aux incidents et apporter une assistance aux entités essentielles et importantes concernées, le cas échéant;

4° rassembler et analyser des données forensiques, et assurer une analyse dynamique des risques et incidents et une appréciation de la situation en matière de cybersécurité;

5° réaliser, à la demande d'une entité essentielle ou importante, un scan proactif des réseaux et des systèmes d'information de l'entité concernée afin de détecter les vulnérabilités susceptibles d'avoir un impact important;

6° participer au réseau des CSIRT, coopérer de manière effective, efficace et sécurisée au sein de ce réseau et apporter une assistance mutuelle en fonction de ses capacités et de ses compétences aux autres membres du réseau des CSIRT à leur demande;

7° le cas échéant, agir en qualité de coordinateur aux fins du processus de divulgation coordonnée des vulnérabilités en vertu de l'article 22;

8° contribuer au déploiement d'outils sécurisés de partage d'informations;

9° procéder à un scan proactif et non intrusif des réseaux et systèmes d'information accessibles au public lorsque ce scan est effectué dans le but de détecter les réseaux et systèmes d'information vulnérables ou configurés de façon peu sûre et d'informer les entités

*Onderafdeling 3**Taken en voorschriften met betrekking tot de rol van
nationaal CSIRT*

Art. 19

§ 1. Het nationale CSIRT heeft de volgende taken:

1° het monitoren en analyseren van cyberdreigingen, kwetsbaarheden en incidenten op nationaal niveau, en, op verzoek, het verlenen van bijstand aan de betrokken essentiële en belangrijke entiteiten met betrekking tot het realtime of bijna-realtime monitoren van hun netwerk- en informatiesystemen;

2° het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie onder de betrokken essentiële en belangrijke entiteiten en aan de bevoegde autoriteiten en andere relevante belanghebbenden over cyberdreigingen, kwetsbaarheden en incidenten, in bijna-*realtime* indien mogelijk;

3° het reageren op incidenten en verlenen van bijstand aan de betrokken essentiële en belangrijke entiteiten, indien van toepassing;

4° het verzamelen en analyseren van forensische gegevens en het zorgen voor dynamische risico- en incidentenanalyse en situationeel bewustzijn met betrekking tot cyberbeveiliging;

5° op verzoek van een essentiële of belangrijke entiteit: het proactief scannen van de netwerk- en informatiesystemen van de betrokken entiteit om kwetsbaarheden met mogelijk significante gevolgen op te sporen;

6° het deelnemen aan het CSIRT-netwerk, het doeltreffend, efficiënt en veilig samenwerken in dit netwerk en, in overeenstemming met zijn capaciteiten en bevoegdheden, het verlenen van wederzijdse bijstand aan andere leden van dit netwerk op hun verzoek;

7° indien van toepassing, het optreden als coördinator ten behoeve van het in artikel 22 bedoelde proces van gecoördineerde bekendmaking van kwetsbaarheden;

8° het bijdragen aan de uitrol van veilige instrumenten voor het delen van informatie;

9° het proactief en niet-intrusief scannen van openbaar toegankelijke netwerk- en informatiesystemen als deze scan wordt uitgevoerd om kwetsbare of onveilig geconfigureerde netwerk- en informatiesystemen op te sporen en de betrokken entiteiten te informeren en deze

concernées et qu'il n'a pas d'effet négatif sur le fonctionnement des services des entités;

10° détecter, observer et analyser des problèmes de sécurité informatique;

11° établir des relations de coopération avec les acteurs concernés du secteur privé, en vue d'atteindre les objectifs de la présente loi;

12° faciliter la coopération visée au 11° en encourageant l'adoption et l'utilisation de pratiques, de systèmes de classification et de taxonomies communs ou normalisés en ce qui concerne:

a) les procédures de gestion des incidents;

b) la gestion de crise; et

c) la divulgation coordonnée des vulnérabilités en vertu de l'article 22;

13° coopérer et, le cas échéant, échanger des informations pertinentes conformément à l'article 27 avec les communautés visées au même article;

14° participer aux évaluations par les pairs organisées conformément à l'article 19 de la directive NIS2.

Après avis du CSIRT national, le Roi peut, par arrêté délibéré en Conseil des ministres, lui confier des tâches supplémentaires.

§ 2. Lorsqu'il exécute les tâches visées au paragraphe 1^{er}, le CSIRT national peut donner la priorité à certaines tâches sur la base d'une approche basée sur les risques.

Art. 20

Les obligations du CSIRT national sont les suivantes:

1° disposer d'une infrastructure de communication et d'information adaptée, sécurisée et résiliente lui permettant d'échanger des informations avec les entités essentielles et importantes et les autres parties prenantes;

2° veiller à un niveau élevé de disponibilité de ses canaux de communication en évitant les points uniques de défaillance et disposer de plusieurs moyens pour être contacté et contacter autrui à tout moment; spécifier

geen negatieve gevolgen heeft voor de werking van de diensten van de entiteiten;

10° het opsporen, observeren en analyseren van computerbeveiligingsproblemen;

11° het tot stand brengen van samenwerkingsrelaties met relevante belanghebbenden in de particuliere sector, teneinde de doelstellingen van deze wet te verwezenlijken;

12° het vergemakkelijken van de in punt 11° bedoelde samenwerking door de invoering en het gebruik te bevorderen van gemeenschappelijke of gestandaardiseerde praktijken, classificatieschema's en taxonomieën met betrekking tot:

a) procedures voor de incidentenbehandeling;

b) crisisbeheer; en

c) de gecoördineerde bekendmaking van kwetsbaarheden uit hoofde van artikel 22;

13° het samenwerken en in voorkomend geval uitwisselen van relevante informatie overeenkomstig artikel 27 met de in datzelfde artikel bedoelde gemeenschappen;

14° het deelnemen aan de overeenkomstig artikel 19 van de NIS2-richtlijn georganiseerde collegiale toetsingen.

Na advies van het nationale CSIRT kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, dit CSIRT bijkomende taken toevertrouwen.

§ 2. Bij de uitvoering van de in paragraaf 1 bedoelde taken kan het nationale CSIRT, op grond van een risico-gebaseerde benadering, prioriteit geven aan bepaalde taken.

Art. 20

De voorschriften voor het nationale CSIRT omvatten het volgende:

1° beschikken over een passende, veilige en weerbare communicatie- en informatie-infrastructuur waardoor informatie kan worden uitgewisseld met essentiële en belangrijke entiteiten en andere relevante belanghebbenden;

2° een hoge mate van beschikbaarheid van zijn communicatiekanalen garanderen door zwakke punten te voorkomen en te allen tijde te beschikken over diverse kanalen waarlangs ze gecontacteerd kunnen worden

clairement les canaux de communication et les faire connaître aux partenaires et collaborateurs;

3° disposer de locaux et de systèmes d'information se trouvant sur des sites sécurisés;

4° être doté d'un système approprié de gestion et de routage des demandes afin, notamment, de faciliter les transferts effectifs et efficaces;

5° garantir la confidentialité et la fiabilité de ses opérations;

6° être doté des effectifs adéquats afin de pouvoir garantir une disponibilité permanente de ses services et veiller à ce que son personnel reçoive une formation appropriée;

7° être doté de systèmes redondants et d'un espace de travail de secours pour assurer la continuité de ses services.

Art. 21

§ 1^{er}. Dans le cadre de l'exercice de ses compétences, le CSIRT national prend toutes les mesures adéquates afin de réaliser les objectifs définis aux articles 19 et 20. Ces mesures doivent être proportionnelles à ces objectifs, et respecter les principes d'objectivité, de transparence et de non-discrimination.

§ 2. Lorsque cela s'avère strictement nécessaire à la réalisation de ses tâches énumérées à l'article 19, § 1^{er}, 1° à 5°, le CSIRT national peut obtenir d'un opérateur visé à l'article 2, 11°, de la loi du 13 juin 2005, des données d'identification visées à l'article 2, alinéa 1^{er}, 5°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ou des métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi précitée du 13 juin 2005 conservées par celui-ci.

Sans porter atteinte aux, ou sans s'immiscer dans les compétences des personnes exerçant la police judiciaire ni des autorités judiciaires, les finalités poursuivies par les tâches précitées sont:

1° sans finalité à caractère pénal, la prévention, la recherche et la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave;

en contact met anderen kunnen opnemen; de communicatiekanalen duidelijk specificeren en meedelen aan de gebruikersgroep en de samenwerkingspartners;

3° beschikken over lokalen en informatiesystemen die zich op beveiligde locaties bevinden;

4° uitgerust zijn met een adequaat systeem voor het beheren en routeren van verzoeken met het oog op doeltreffende en efficiënte overdrachten;

5° de vertrouwelijkheid en betrouwbaarheid van zijn activiteiten waarborgen;

6° beschikken over voldoende personeel om te allen tijde de beschikbaarheid van zijn diensten te garanderen, en ervoor zorgen dat zijn personeel naar behoren wordt opgeleid;

7° uitgerust zijn met redundante systemen en reservevruimten om de continuïteit van zijn diensten te waarborgen.

Art. 21

§ 1. In het kader van de uitoefening van zijn bevoegdheden neemt het nationale CSIRT alle passende maatregelen om de in de artikelen 19 en 20 bepaalde doelstellingen te verwezenlijken. Deze maatregelen moeten evenredig zijn met die doelstellingen, en in overeenstemming met de beginselen van objectiviteit, transparantie en non-discriminatie.

§ 2. Indien dat strikt noodzakelijk is voor de uitvoering van zijn taken opgesomd in artikel 19, § 1, 1° tot 5°, kan het nationale CSIRT identificatiegegevens bedoeld in artikel 2, eerste lid, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector of elektronische-communicatiemetagegegevens als bedoeld in artikel 2, 93°, van de wet van 13 juni 2005 verkrijgen van een operator als bedoeld in artikel 2, 11°, van de voormelde wet van 13 juni 2005, die deze gegevens bewaart.

Zonder afbreuk te doen aan of zich in te mengen in de bevoegdheden van personen die de gerechtelijke politie uitoefenen en de gerechtelijke autoriteiten, worden met voornoemde taken de volgende doeleinden nagestreefd:

1° zonder strafrechtelijke finaliteit, het voorkomen, onderzoeken en opsporen van inbreuken die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten;

2° la prévention de menaces graves contre la sécurité publique;

3° l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information.

Le CSIRT national peut déterminer le délai endéans lequel l'opérateur répond à sa demande, en fonction de l'urgence de celle-ci.

§ 3. Lorsque le CSIRT national adresse à un opérateur une demande de données d'identification visées à l'article 2, alinéa 1^{er}, 5°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, cette demande est autorisée par le supérieur hiérarchique.

§ 4. Lorsque le CSIRT national adresse à un opérateur une demande de métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi du 13 juin 2005 autres que celles visées au paragraphe 3, cette demande fait l'objet d'un contrôle préalable par l'autorité de protection des données.

En cas de situation urgente dûment justifiée, le CSIRT national peut se passer du contrôle préalable visé à l'alinéa 1^{er} et solliciter directement les données. Cette demande est envoyée sans délai à l'autorité visée à l'alinéa 1^{er} pour permettre un contrôle ultérieur.

Lorsqu'à la suite du contrôle visé à l'alinéa 2, l'autorité de protection des données refuse de confirmer la validité de la demande de métadonnées de communications électroniques visée à l'alinéa 1^{er}, le CSIRT national le notifie sans délai à l'opérateur concerné et supprime les métadonnées reçues.

§ 5. Le directeur général du CSIRT national désigne expressément les personnes habilitées à traiter les données de communications électroniques visées au présent article.

§ 6. Le CSIRT national informe, dans la mesure du possible, les personnes physiques concernées de l'accès à leurs données de communications électroniques lorsque cela n'est plus susceptible de compromettre le bon déroulement de ses tâches ou d'une enquête en cours et lorsque ces personnes peuvent être identifiées.

§ 7. Sans préjudice des articles 28quinquies, § 1^{er}, et 57, § 1^{er}, du Code d'instruction criminelle, pour atteindre ces objectifs, le CSIRT national est autorisé à détenir, à divulguer, à diffuser ou à faire usage de toutes les

2° het voorkomen van ernstige bedreigingen voor de openbare veiligheid;

3° het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten of informatiesystemen.

Het nationale CSIRT kan bepalen binnen welke termijn de operator op zijn verzoek moet reageren, naargelang de dringendheid hiervan.

§ 3. Indien het nationale CSIRT een operator een verzoek om identificatiegegevens bedoeld in artikel 2, eerste lid, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector stuurt, wordt dat verzoek toegestaan door de hiërarchische meerdere.

§ 4. Indien het nationale CSIRT een operator een verzoek om elektronische-communicatiemetagegegevens als bedoeld in artikel 2, 93°, van de wet van 13 juni 2005 die geen in paragraaf 3 bedoelde gegevens zijn, stuurt, wordt dat verzoek vooraf gecontroleerd door de gegevensbeschermingsautoriteit.

In dringende en naar behoren met redenen omklede gevallen kan het nationale CSIRT optreden zonder de voorafgaande controle bedoeld in het eerste lid, en de gegevens rechtstreeks opvragen. Dit verzoek wordt onverwijld naar de in het eerste lid bedoelde overheid gestuurd om een latere controle mogelijk te maken.

Indien de gegevensbeschermingsautoriteit, na de in het tweede lid bedoelde controle, weigert de geldigheid van het in het eerste lid bedoelde verzoek om elektronische-communicatiemetagegegevens te bevestigen, stelt het nationale CSIRT de betrokken operator daarvan onverwijld in kennis en verwijdt het de ontvangen metagegegevens.

§ 5. De directeur-generaal van het nationale CSIRT wijst uitdrukkelijk de personen aan die gemachtigd zijn om de in dit artikel bedoelde elektronische-communicatiegegevens te verwerken.

§ 6. Het nationale CSIRT brengt de betrokken natuurlijke personen voor zover mogelijk op de hoogte van de toegang tot hun elektronische-communicatiegegevens als de uitvoering van zijn taken of van een lopend onderzoek hierdoor niet meer in het gedrang kan komen en als deze personen kunnen worden geïdentificeerd.

§ 7. Onverminderd de artikelen 28quinquies, § 1, en 57, § 1, van het Wetboek van strafvordering mag het nationale CSIRT, om die doelstellingen te verwezenlijken, alle beschikbare gegevens bezitten, onthullen of

informations disponibles, même si celles-ci sont issues d'un accès non autorisé à un système informatique par un tiers.

§ 8. Dans l'accomplissement de ses missions, le CSIRT national use de la prudence que l'on est en droit d'attendre d'une autorité publique, en veillant toujours en priorité à ne pas perturber le fonctionnement du système informatique et en prenant toutes précautions raisonnables afin qu'aucun dommage matériel ne soit causé au système informatique.

Le directeur général du CSIRT national veille, par l'adoption de procédures internes, au respect des conditions visées au présent article.

Art. 22

§ 1^{er}. Dans son rôle de coordinateur aux fins de la divulgation coordonnée des vulnérabilités, le CSIRT national fait office d'intermédiaire de confiance en facilitant, si nécessaire, les interactions entre la personne physique ou morale qui signale une potentielle vulnérabilité et le fabricant ou le fournisseur des produits TIC ou des services TIC potentiellement vulnérables, à la demande de l'une des deux parties.

Dans ce cadre, les tâches du CSIRT national consistent notamment à:

- 1° identifier et contacter les entités concernées;
- 2° apporter une assistance aux personnes physiques ou morales signalant une vulnérabilité; et
- 3° négocier des délais de divulgation et gérer les vulnérabilités qui touchent plusieurs entités.

§ 2. Toute personne physique ou morale peut signaler, même de manière anonyme lorsqu'elle le demande, au CSIRT national l'existence d'une potentielle vulnérabilité.

Le signalement est effectué par écrit, selon la procédure détaillée sur le site internet du CSIRT national.

Ce signalement est sans préjudice de l'application de la loi du 28 novembre 2022 sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé ou des dispositions légales sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur public.

verspreiden, of er enig gebruik van maken, zelfs als die gegevens voortkomen uit een ongerechtigde toegang tot een informaticasysteem door een derde.

§ 8. Het nationale CSIRT vervult zijn opdrachten met de nodige behoedzaamheid die verwacht mag worden van een overheid, waarbij er steeds bij voorrang voor wordt gezorgd dat de werking van het informaticasysteem niet wordt verstoord en alle redelijke voorzorgen worden genomen om te voorkomen dat het informaticasysteem materiële schade oploopt.

De directeur-generaal van het nationale CSIRT zorgt voor de naleving van de in dit artikel vermelde voorwaarden. Daartoe werkt hij interne procedures uit.

Art. 22

§ 1. In zijn rol van coördinator met het oog op een ge-coördineerde bekendmaking van kwetsbaarheden treedt het nationale CSIRT op als betrouwbare tussenpersoon en vergemakkelijkt het, waar nodig, de interactie tussen de natuurlijke of rechtspersoon die een mogelijke kwetsbaarheid meldt enerzijds en de fabrikant of aanbieder van de mogelijk kwetsbare ICT-producten of -diensten anderzijds, op verzoek van een van beide partijen.

In dat kader omvatten de taken van het nationale CSIRT met name:

- 1° het identificeren van en contact opnemen met de betrokken entiteiten;
- 2° het bijstaan van de natuurlijke of rechtspersonen die een kwetsbaarheid melden; en
- 3° het onderhandelen over tijdschema's voor de bekendmaking, en het beheren van kwetsbaarheden die van invloed zijn op meerdere entiteiten.

§ 2. Iedere natuurlijke of rechtspersoon kan, zelfs desgevraagd anoniem, aan het nationale CSIRT het bestaan van een mogelijke kwetsbaarheid melden.

De melding gebeurt schriftelijk, volgens de procedure die op de website van het nationale CSIRT beschreven is.

Deze melding doet geen afbreuk aan de toepassing van de wet van 28 november 2022 betreffende de bescherming van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de particuliere sector of van wettelijke bepalingen betreffende de bescherming van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de overheidssector.

§ 3. Le CSIRT national veille à ce que des mesures de suivi diligentes soient prises en ce qui concerne la vulnérabilité signalée et veille à l'anonymat de la personne physique ou morale signalant la vulnérabilité, pour autant que cette personne le demande et respecte les conditions visées à l'article 23.

Le CSIRT national préserve l'exhaustivité, l'intégrité, le stockage durable et la confidentialité des informations transmises au travers du signalement.

L'accès à ces informations est limité aux personnes habilitées par le directeur général du CSIRT national, sauf lorsque le partage de ces informations s'avère nécessaire à l'exécution des tâches énumérées au présent article.

§ 4. Tout en respectant les conditions énumérées à l'article 21, §§ 1^{er} et 4, le CSIRT national peut observer, étudier ou tester la sécurité d'un réseau et système d'information afin de déterminer l'existence d'une vulnérabilité potentielle ou de vérifier les méthodes utilisées par l'auteur de signalement.

§ 5. Lorsque la vulnérabilité signalée est susceptible d'avoir un impact significatif sur des entités dans plusieurs États membres, le CSIRT national coopère, le cas échéant, avec les autres CSIRT désignés comme coordinateurs au sein du réseau des CSIRT.

§ 6. Le directeur général du CSIRT national veille, par l'adoption de procédures internes, au respect des conditions visées au présent article.

Art. 23.

§ 1^{er}. Dans le cadre de la procédure visée à l'article 22, les auteurs de signalement ne commettent pas d'infraction aux articles 314^{bis}, 458, 550^{bis}, 550^{ter} du Code pénal et de l'article 145 de la loi du 13 juin 2005 à condition:

1° qu'ils aient agi sans intention frauduleuse, ni dessein de nuire;

2° qu'ils aient adressé une notification simplifiée qui reprend l'identification du système concerné et une description simple de la vulnérabilité potentielle, sans délai et au plus tard dans les 24 heures de la découverte d'une potentielle vulnérabilité, à l'organisation responsable du système et au CSIRT national;

3° qu'ils aient adressé une notification complète, sans délai et au plus tard dans les 72 heures de la découverte d'une potentielle vulnérabilité, à l'organisation responsable

§ 3. Het nationale CSIRT ziet erop toe dat de gemelde kwetsbaarheid zorgvuldig wordt opgevolgd en waarborgt de anonimiteit van de natuurlijke of rechtspersoon die de kwetsbaarheid meldt, voor zover deze persoon hierom verzoekt en de in artikel 23 bedoelde voorwaarden naleeft.

Het nationale CSIRT waarborgt de volledigheid, integriteit, duurzame opslag en geheimhouding van de informatie die via de melding wordt overgemaakt.

De toegang tot deze informatie wordt beperkt tot personen die daartoe door de directeur-generaal van het nationale CSIRT gemachtigd zijn, behalve indien het delen van deze informatie noodzakelijk is voor de uitvoering van de taken opgesomd in dit artikel.

§ 4. Met inachtneming van de voorwaarden opgesomd in artikel 21, §§ 1 en 4, kan het nationale CSIRT de beveiliging van een netwerk- en informatiesysteem observeren, onderzoeken en testen om te bepalen of er sprake is van een mogelijke kwetsbaarheid of om de door de melder gebruikte methoden na te gaan.

§ 5. Wanneer een gemelde kwetsbaarheid significante gevolgen kan hebben voor entiteiten in meer dan één lidstaat, werkt het nationale CSIRT, in voorkomend geval, samen met andere als coördinator aangewezen CSIRT's binnen het CSIRT-netwerk.

§ 6. De directeur-generaal van het nationale CSIRT zorgt voor de naleving van de in dit artikel vermelde voorwaarden. Daartoe werkt hij interne procedures uit.

Art. 23

§ 1. In het kader van de procedure bedoeld in artikel 22 plegen melders geen inbreuk op de artikelen 314^{bis}, 458, 550^{bis} en 550^{ter} van het Strafwetboek en op artikel 145 van de wet van 13 juni 2005, op voorwaarde dat:

1° zij zonder bedrieglijk opzet of het oogmerk om te schaden hebben gehandeld;

2° zij onverwijld en uiterlijk binnen 24 uur na de ontdekking van een mogelijke kwetsbaarheid een vereenvoudigde kennisgeving met de identificatie van het betrokken systeem en een eenvoudige beschrijving van de mogelijke kwetsbaarheid hebben gestuurd naar de organisatie die verantwoordelijk is voor het systeem en naar het nationale CSIRT;

3° zij onverwijld en uiterlijk binnen 72 uur na de ontdekking van een mogelijke kwetsbaarheid een volledige kennisgeving hebben gestuurd naar de organisatie die

du système, le cas échéant dans le respect des modalités de signalement établis par cette organisation, et au CSIRT national, conformément à la procédure prévue à l'article 22, § 2;

4° qu'ils n'aient pas agi au-delà de ce qui était nécessaire et proportionné pour vérifier l'existence d'une vulnérabilité et pour la rapporter;

5° qu'ils n'aient pas publiquement divulgué les informations relatives à la vulnérabilité découverte et aux systèmes vulnérables, sans l'accord du CSIRT national;

6° en ce qui concerne les réseaux et systèmes des organisations visées à l'article 5, §§ 4 et 5, et des organes judiciaires ainsi que les informations traitées par eux ou pour leur compte, qu'ils aient, avant la commission de ces actes, conclu un accord écrit avec le service compétent sur les modalités et la méthodologie à utiliser dans le cadre de la recherche de potentielles vulnérabilités.

§ 2. Lorsque des personnes signalent des informations sur une potentielle vulnérabilité dont ils ont eu connaissance dans leur contexte professionnel, elles ne sont pas considérées comme ayant enfreint leur obligation de secret professionnel et n'encourent aucune responsabilité d'aucune sorte concernant la transmission d'informations nécessaires pour signaler une potentielle vulnérabilité au CSIRT national.

§ 3. Toute autre responsabilité éventuelle des auteurs de signalement découlant d'actes ou d'omissions qui ne sont pas nécessaires à l'accomplissement de la procédure visée à l'article 22 et ne respectent pas les conditions du paragraphe 1^{er} continue d'être régie par le droit applicable.

Section 3

Les éventuelles autorités sectorielles

Art. 24

Sans préjudice des autres dispositions, l'autorité sectorielle peut:

1° organiser des exercices sectoriels, les coordonner ou y participer, pour ce qui concerne les mesures visées aux articles 30 et 33;

2° analyser et gérer les conséquences d'un incident pour le secteur;

responsable est pour het systeem, in voorkomend geval met inachtneming van de door deze organisatie vastgestelde meldingsmodaliteiten, en naar het nationale CSIRT, overeenkomstig de in artikel 22, § 2, bedoelde procedure;

4° zij niet verder zijn gegaan dan nodig en evenredig was om het bestaan van een kwetsbaarheid na te gaan en die te melden;

5° zij de informatie over de ontdekte kwetsbaarheid en de kwetsbare systemen niet openbaar hebben gemaakt zonder de toestemming van het nationale CSIRT;

6° zij, wat betreft de netwerken en systemen van de in artikel 5, §§ 4 en 5, bedoelde organisaties en van de rechterlijke instanties, en de informatie die door hen of namens hen wordt verwerkt, vóór het plegen van die daden een schriftelijke overeenkomst hebben gesloten met de bevoegde dienst over de te hanteren modaliteiten en methodologie in het kader van het onderzoek naar mogelijke kwetsbaarheden.

§ 2. Personen die informatie melden over een mogelijke kwetsbaarheid waarvan zij in het kader van hun beroep kennis hebben gekregen, worden niet geacht hun beroepsgeheim te hebben geschonden en kunnen op generlei wijze aansprakelijk worden gesteld voor de overdracht van informatie die noodzakelijk was om een mogelijke kwetsbaarheid aan het nationale CSIRT te melden.

§ 3. Voor elke andere mogelijke aansprakelijkheid van melders die voortvloeit uit handelingen of nalatigheden die niet noodzakelijk zijn voor de uitvoering van de in artikel 22 bedoelde procedure en die niet voldoen aan de voorwaarden van paragraaf 1, blijft het toepasselijke recht gelden.

Afdeling 3

De eventuele sectorale overheden

Art. 24

Onverminderd de andere bepalingen kan de sectorale overheid:

1° sectorale oefeningen organiseren, coördineren of eraan deelnemen, voor wat betreft de maatregelen bedoeld in de artikelen 30 en 33;

2° de gevolgen van een incident voor de sector analyseren en beheren;

3° participer aux travaux du groupe de coopération pour ce qui concerne les sujets qui touchent à ses compétences;

4° sensibiliser les entités relevant de son secteur.

CHAPITRE 2

Coopération au niveau national

Art. 25

§ 1^{er}. Les autorités visées au chapitre 1^{er} du présent titre coopèrent les unes avec les autres afin de respecter les obligations énoncées dans la présente loi.

§ 2. En fonction des besoins nécessaires à l'exécution de la présente loi, les autorités visées au paragraphe 1^{er} coopèrent également, au niveau national, avec le NCCN, les services administratifs de l'État, les autorités administratives, en ce compris les autorités nationales en vertu des règlements (CE) n° 300/2008 et n° 2018/1139, les organes de contrôle au titre du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, la Banque nationale de Belgique, l'Autorité des services et marchés financiers, l'Institut, les autorités compétentes en vertu de la loi du 1^{er} juillet 2011, les autorités judiciaires, les services de renseignement et de sécurité visés par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, les services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux et avec les autorités de protection des données.

§ 3. Les entités essentielles et importantes et les autorités visées au chapitre 1^{er} du présent titre collaborent en tout temps, par un échange adéquat d'informations concernant la sécurité des systèmes et réseaux d'informations.

§ 4. Les autorités visées au chapitre 1^{er} du présent titre et les autorités compétentes dans le cadre de la loi du 1^{er} juillet 2011 coopèrent et échangent régulièrement des informations sur le recensement des infrastructures critiques, les risques, les cybermenaces et les incidents, ainsi que sur les risques, menaces et incidents non cyber qui touchent les exploitants d'infrastructures recensées en tant qu'infrastructures critiques en vertu de la loi du

3° deelnemen aan de werkzaamheden van de samenwerkingsgroep voor de onderwerpen die betrekking hebben op haar bevoegdheden;

4° de entiteiten die onder haar sector vallen sensibiliseren.

HOOFDSTUK 2

Samenwerking op nationaal niveau

Art. 25

§ 1. De autoriteiten bedoeld in hoofdstuk 1 van deze titel werken samen om de in deze wet vastgestelde verplichtingen na te komen.

§ 2. Naargelang de behoeften die nodig zijn voor de uitvoering van deze wet werken de in paragraaf 1 bedoelde autoriteiten op nationaal niveau ook samen met het NCCN, de administratieve diensten van de Staat, de administratieve overheden, met inbegrip van de nationale autoriteiten krachtens Verordening (EG) nr. 300/2008 en nr. 2018/1139, de toezichthoudende organen uit hoofde van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, de Nationale Bank van België, de Autoriteit voor Financiële Diensten en Markten, het Instituut, de krachtens de wet van 1 juli 2011 bevoegde autoriteiten, de gerechtelijke overheden, de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, en de gegevensbeschermingsautoriteiten.

§ 3. De essentiële en belangrijke entiteiten en de autoriteiten bedoeld in hoofdstuk 1 van deze titel werken te allen tijde samen door een adequate uitwisseling van informatie over de beveiliging van netwerk- en informatiesystemen.

§ 4. De in hoofdstuk 1 van deze titel bedoelde autoriteiten en de in het kader van de wet van 1 juli 2011 bevoegde autoriteiten werken samen en wisselen regelmatig informatie uit inzake het als kritiek aanmerken van infrastructuur, over risico's, cyberdreigingen en incidenten, alsook over niet-cyberbepaalde risico's, -dreigingen en -incidenten die gevolgen hebben voor exploitanten van infrastructuur die uit hoofde van de wet van

1^{er} juillet 2011 et sur les mesures prises pour faire face à ces risques, menaces et incidents.

§ 5. Les autorités visées au chapitre 1^{er} du présent titre et les autorités compétentes en vertu du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 et de la loi du 13 juin 2005, échangent régulièrement des informations pertinentes, y compris en ce qui concerne les incidents et les cybermenaces concernés.

§ 6. L'autorité nationale de cybersécurité crée une plateforme de coordination et d'évaluation afin que les autorités visées à l'article 15 et le NCCN échangent de l'information et se coordonnent dans le cadre de l'exécution de la présente loi.

CHAPITRE 3

Confidentialité et échanges d'information

Art. 26

§ 1^{er}. Le présent article ne porte pas préjudice à l'application de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, de la loi du 11 avril 1994 relative à la publicité de l'administration ou d'autres dispositions légales garantissant la confidentialité des informations liées aux intérêts essentiels de la sécurité publique nationale.

§ 2. Toute personne qui est appelée à prêter son concours professionnel à l'évaluation de la conformité ou à la supervision est tenue au secret. Celui qui viole ce secret est puni des peines prévues à l'article 458 du Code pénal.

Les personnes dépositaires, par état ou par profession, des secrets qu'on leur confie sont autorisées à faire connaître ces secrets pour l'exécution de la présente loi.

1 juli 2011 als kritieke infrastructuur zijn aangemerkt, en over de maatregelen die in reactie op dergelijke risico's, dreigingen en incidenten zijn genomen.

§ 5. De in hoofdstuk 1 van deze titel bedoelde autoriteiten en de autoriteiten die bevoegd zijn krachtens Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 en de wet van 13 juni 2005, wisselen regelmatig relevante informatie uit, onder meer met betrekking tot relevante incidenten en cyberdreigingen.

§ 6. De nationale cyberbeveiligingsautoriteit richt een coördinatie- en evaluatieplatform op dat de in artikel 15 bedoelde autoriteiten en het NCCN toelaat informatie uit te wisselen en hun optreden in het kader van de uitvoering van deze wet op elkaar af te stemmen.

HOOFDSTUK 3

Vertrouwelijkheid en informatie-uitwisseling

Art. 26

§ 1. Dit artikel doet geen afbreuk aan de toepassing van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, de wet van 11 april 1994 betreffende de openbaarheid van bestuur of andere wettelijke bepalingen die de vertrouwelijkheid van informatie met betrekking tot de wezenlijke belangen van de nationale openbare veiligheid waarborgen.

§ 2. Eenieder die beroepshalve zijn medewerking dient te verlenen aan de conformiteitsbeoordeling of het toezicht is tot geheimhouding verplicht. Diegene die dit geheim schendt, wordt gestraft met de straffen bepaald in artikel 458 van het Strafwetboek.

Personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd, mogen deze geheimen bekendmaken voor de uitvoering van deze wet.

Ces personnes obtiennent l'accord des autorités visées à l'article 5, § 4, lorsque ces autorités sont concernées par le secret.

§ 3. Les autorités visées au chapitre 1^{er} du présent titre, les entités essentielles ou importantes, ou leurs sous-traitants, limitent l'accès aux informations dans le cadre de la présente loi aux personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec l'exécution de la présente loi.

§ 4. Les informations fournies aux autorités visées au chapitre 1^{er} du présent titre par les entités essentielles ou importantes, peuvent être échangées avec des autorités de l'Union européenne, avec des autorités belges ou étrangères, lorsque cet échange est nécessaire à l'application de dispositions légales.

Les informations échangées se limitent à ce qui est pertinent et sont proportionnées à l'objectif de cet échange, notamment dans le respect du règlement (UE) 2016/679. Cet échange d'informations préserve la confidentialité des informations concernées et protège la sécurité et les intérêts commerciaux des entités essentielles ou importantes.

Art. 27

§ 1^{er}. À titre volontaire, les entités relevant du champ d'application de la présente loi et, le cas échéant, les autres entités concernées ne relevant pas du champ d'application de la présente loi peuvent échanger, entre elles, au sein de communautés, des informations pertinentes en matière de cybersécurité, y compris des informations relatives aux cybermenaces, aux incidents évités, aux vulnérabilités, aux techniques et procédures, aux indicateurs de compromission, aux tactiques adverses, ainsi que des informations spécifiques sur les acteurs de la menace, des alertes de cybersécurité et des recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberattaques, lorsque ce partage d'informations:

1° vise à prévenir et à détecter les incidents, à y réagir, à s'en rétablir ou à atténuer leur impact;

2° renforce le niveau de cybersécurité, notamment en sensibilisant aux cybermenaces, en limitant ou en empêchant leur capacité de se propager, en soutenant une série de capacités de défense, en remédiant aux vulnérabilités et en les révélant, en mettant en œuvre des techniques de détection, d'endiguement et de prévention des menaces, des stratégies d'atténuation

Deze personen verkrijgen het akkoord van de autoriteiten bedoeld in artikel 5, § 4, wanneer deze autoriteiten bij het geheim betrokken zijn.

§ 3. De autoriteiten bedoeld in hoofdstuk 1 van deze titel en de essentiële of belangrijke entiteiten, of hun onderaannemers, beperken de toegang tot de informatie in het kader van deze wet tot de personen die ervan op de hoogte moeten zijn en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met de uitvoering van deze wet.

§ 4. De informatie die door essentiële of belangrijke entiteiten aan de autoriteiten bedoeld in hoofdstuk 1 van deze titel wordt bezorgd, mag worden uitgewisseld met autoriteiten van de Europese Unie, Belgische of buitenlandse autoriteiten, wanneer die uitwisseling noodzakelijk is voor de toepassing van wettelijke bepalingen.

De uitgewisselde informatie wordt beperkt tot hetgeen relevant is voor en evenredig is met het doel van die uitwisseling, met name overeenkomstig Verordening (EU) 2016/679. Bij die uitwisseling van informatie wordt de vertrouwelijkheid van de informatie gewaarborgd en worden de beveiligings- en commerciële belangen van essentiële of belangrijke entiteiten beschermd.

Art. 27

§ 1. Binnen het toepassingsgebied van deze wet vallende entiteiten en, indien van toepassing, andere entiteiten die niet binnen het toepassingsgebied van deze wet vallen, kunnen op vrijwillige basis onderling, binnen gemeenschappen, relevante informatie over cyberbeveiliging uitwisselen, met inbegrip van informatie over cyberdreigingen, bijna-incidenten, kwetsbaarheden, technieken en procedures, indicatoren voor aantasting, vijandige tactieken, dreigingsactorspecifieke informatie, cyberbeveiligingswaarschuwingen en aanbevelingen betreffende de configuratie van cyberbeveiligingsinstrumenten om cyberaanvallen te detecteren, wanneer dat uitwisselen van informatie:

1° beoogt incidenten te voorkomen, te detecteren, erop te reageren of ervan te herstellen of de gevolgen ervan te beperken;

2° het niveau van de cyberbeveiliging verhoogt, met name door de bewustwording met betrekking tot cyberdreigingen te vergroten, het vermogen van dergelijke dreigingen om zich te verspreiden te beperken of te belemmeren, een reeks verdedigingscapaciteiten, het herstel en openbaarmaking van kwetsbaarheden, het opsporen van dreigingen, beheersings- en preventietechnieken,

ou des étapes de réaction et de rétablissement, ou en encourageant la recherche collaborative en matière de cybermenaces entre les entités publiques et privées.

§ 2. L'échange d'informations visé au paragraphe 1^{er} est mis en œuvre au moyen d'accords de partage d'informations en matière de cybersécurité, compte tenu de la nature potentiellement sensible des informations partagées.

§ 3. L'autorité nationale de cybersécurité facilite la mise en place des accords de partage d'informations en matière de cybersécurité visés au paragraphe 2. Ces accords peuvent préciser les éléments opérationnels, y compris l'utilisation de plateformes TIC spécialisées et d'outils d'automatisation, le contenu et les conditions des accords de partage d'informations. L'autorité nationale de cybersécurité et les éventuelles autorités sectorielles peuvent imposer des conditions d'utilisation des informations qu'elles mettent à disposition des communautés visées au paragraphe 1^{er}.

§ 4. Les entités essentielles et importantes notifient à l'autorité nationale de cybersécurité leur participation aux accords de partage d'informations en matière de cybersécurité visés au paragraphe 2, lorsqu'elles concluent de tels accords ou, le cas échéant, lorsqu'elles se retirent de ces accords, une fois que le retrait prend effet.

CHAPITRE 4

Stratégie nationale en matière de cybersécurité

Art. 28

§ 1^{er}. Les ministres réunis en Conseil adoptent la stratégie nationale en matière de cybersécurité et la mettent à jour au moins tous les 5 ans, sur la base d'indicateurs de performance, après avis du Conseil national de sécurité, des autorités visées à l'article 15, du NCCN et, le cas échéant, des autorités de protection des données.

Cette stratégie définit les objectifs stratégiques, les ressources nécessaires pour atteindre ces objectifs, ainsi que les mesures politiques et réglementaires appropriées, en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir.

§ 2. La stratégie nationale en matière de cybersécurité comprend, entre autres:

bepenkingsstrategieën of respons- en herstelfasen te ondersteunen of gezamenlijk onderzoek naar cyberdreigingen door publieke en particuliere entiteiten te bevorderen.

§ 2. De informatie-uitwisseling bedoeld in paragraaf 1 wordt uitgevoerd door middel van informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging met betrekking tot de potentieel gevoelige aard van de uitgewisselde informatie.

§ 3. De nationale cyberbeveiligingsautoriteit faciliteert de vaststelling van de in paragraaf 2 bedoelde informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging. In dergelijke regelingen kunnen de operationele elementen, met inbegrip van het gebruik van specifieke ICT-platforms en automatiseringshulpmiddelen, de inhoud en de voorwaarden van de informatie-uitwisselingsregelingen worden gespecificeerd. De nationale cyberbeveiligingsautoriteit en de eventuele sectorale overheden kunnen voorwaarden opleggen aan het gebruik van de informatie die zij ter beschikking stellen van de gemeenschappen bedoeld in paragraaf 1.

§ 4. De essentiële en belangrijke entiteiten stellen de nationale cyberbeveiligingsautoriteit in kennis van hun deelname aan de in paragraaf 2 bedoelde informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging wanneer zij dergelijke regelingen aangaan, of, indien van toepassing, van hun terugtrekking uit dergelijke regelingen, zodra de terugtrekking van kracht wordt.

HOOFDSTUK 4

Nationale cyberbeveiligingsstrategie

Art. 28

§ 1. De in Raad vergaderde ministers keuren de nationale cyberbeveiligingsstrategie goed en werken deze minstens om de 5 jaar bij op basis van prestatie-indicatoren, na advies van de Nationale Veiligheidsraad, de in artikel 15 bedoelde autoriteiten, het NCCN en, in voorkomend geval, de gegevensbeschermingsautoriteiten.

Deze strategie bepaalt de strategische doelstellingen, de middelen die nodig zijn om die doelstellingen te behalen, en passende beleids- en regelgevingsmaatregelen, om een hoog niveau van cyberbeveiliging te bereiken en te handhaven.

§ 2. De nationale cyberbeveiligingsstrategie omvat onder meer:

1° les objectifs et les priorités de la stratégie nationale en matière de cybersécurité, couvrant en particulier les secteurs visés aux annexes I et II;

2° un cadre de gouvernance visant à atteindre les objectifs et les priorités visés au 1°, y compris les tâches et les responsabilités des autorités publiques et des autres acteurs concernés ainsi que les politiques visées au paragraphe 3;

3° un cadre de gouvernance précisant les rôles et les responsabilités des parties prenantes en Belgique, et sur lequel reposent la coopération et la coordination, en Belgique, entre les autorités visées au chapitre 1^{er} du présent titre ainsi que la coopération et la coordination entre ces autorités et les autorités compétentes en vertu d'instruments juridiques sectoriels de l'Union européenne;

4° un mécanisme visant à identifier les actifs pertinents et une évaluation des risques en Belgique;

5° un inventaire des mesures garantissant la préparation, la réaction et la récupération des services après incident, y compris la coopération entre les secteurs public et privé;

6° une liste des différents acteurs et autorités concernés par la mise en œuvre de la stratégie nationale en matière de cybersécurité;

7° un cadre politique visant une coordination renforcée entre les autorités visées au chapitre 1^{er} du présent titre et les autorités compétentes en vertu de la loi du 1^{er} juillet 2011 aux fins du partage d'informations relatives aux risques, aux menaces et aux incidents dans les domaines cyber et non cyber et de l'exercice des tâches de supervision, le cas échéant;

8° un plan comprenant les mesures nécessaires en vue d'améliorer le niveau général de sensibilisation des citoyens à la cybersécurité;

9° un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de cybersécurité;

10° un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de cybersécurité.

§ 3. Des politiques, parties intégrantes de la stratégie nationale en matière de cybersécurité, sont adoptées et portent sur les éléments suivants:

1° de doelstellingen en prioriteiten van de nationale cyberbeveiligingsstrategie, met name inzake de in de bijlagen I en II bedoelde sectoren;

2° een governancekader om de in punt 1° bedoelde doelstellingen en prioriteiten te verwezenlijken, met inbegrip van de taken en verantwoordelijkheden van de overheid en de andere belanghebbenden alsook van het in paragraaf 3 bedoelde beleid;

3° een governancekader dat de taken en verantwoordelijkheden van de belanghebbenden in België verduidelijkt, ter onderbouwing van de samenwerking en coördinatie, in België, tussen de autoriteiten bedoeld in hoofdstuk 1 van deze titel, alsook van de samenwerking en coördinatie tussen die autoriteiten en uit hoofde van sectorspecifieke rechtsinstrumenten van de Europese Unie bevoegde autoriteiten;

4° een mechanisme om relevante activa vast te stellen en een beoordeling van de risico's in België;

5° een inventarisatie van de maatregelen om te zorgen voor paraatheid, respons en herstel bij incidenten, met inbegrip van samenwerking tussen de publieke en de particuliere sector;

6° een lijst van de verschillende belanghebbenden en autoriteiten die betrokken zijn bij de uitvoering van de nationale cyberbeveiligingsstrategie;

7° een beleidskader voor versterkte coördinatie tussen de autoriteiten bedoeld in hoofdstuk 1 van deze titel en de uit hoofde van de wet van 1 juli 2011 bevoegde autoriteiten, met als doel het delen van informatie over risico's, cyberdreigingen en incidenten, alsook over niet-cyberdreigingen en -incidenten, en in voorkomend geval de uitoefening van toezichthoudende taken;

8° een plan, met inbegrip van de noodzakelijke maatregelen, om het algemene niveau van cyberbeveiligingsbewustzijn bij de burgers te verbeteren;

9° een overzicht van de onderwijs-, bewustmakings- en opleidingsprogramma's met betrekking tot de nationale cyberbeveiligingsstrategie;

10° een overzicht van de plannen voor onderzoek en ontwikkeling met betrekking tot de nationale cyberbeveiligingsstrategie.

§ 3. Er worden beleidsmaatregelen genomen die integraal deel uitmaken van de nationale cyberbeveiligingsstrategie:

1° la cybersécurité dans le cadre de la chaîne d'approvisionnement des produits et services TIC utilisés par des entités pour la fourniture de leurs services;

2° l'inclusion et la spécification d'exigences liées à la cybersécurité pour les produits et services TIC dans les marchés publics, y compris concernant la certification de cybersécurité, le chiffrement et l'utilisation de produits de cybersécurité en sources ouvertes;

3° la gestion des vulnérabilités, y compris la promotion et la facilitation de la divulgation coordonnée des vulnérabilités conformément à l'article 22;

4° le maintien de la disponibilité générale, de l'intégrité et de la confidentialité du noyau public de l'internet ouvert, y compris, le cas échéant, la cybersécurité des câbles de communication sous-marins;

5° la promotion du développement et de l'intégration de technologies avancées pertinentes visant à mettre en œuvre des mesures de pointe dans la gestion des risques en matière de cybersécurité;

6° la promotion et le développement de l'éducation et de la formation en matière de cybersécurité, des compétences en matière de cybersécurité, des initiatives de sensibilisation et de recherche et de développement en matière de cybersécurité, ainsi que des orientations sur les bonnes pratiques de cyberhygiène et les contrôles, à l'intention des citoyens, des parties prenantes et des entités;

7° le soutien aux institutions universitaires et de recherche visant à développer, améliorer et promouvoir le déploiement des outils de cybersécurité et à sécuriser les infrastructures de réseau;

8° la mise en place de procédures pertinentes et d'outils de partage d'informations appropriés visant à soutenir le partage volontaire d'informations sur la cybersécurité entre les entités;

9° le renforcement des valeurs de cyberrésilience et de cyberhygiène des petites et moyennes entreprises, en particulier celles qui sont exclues du champ d'application de la présente loi, en fournissant des orientations et un soutien facilement accessibles pour répondre à leurs besoins spécifiques;

10° la promotion d'une cyberprotection active.

1° inzake cyberbeveiliging in de toeleveringsketen voor ICT-producten en ICT-diensten die door entiteiten worden gebruikt voor het verlenen van hun diensten;

2° inzake het opnemen en specificeren van cyberbeveiligingsgerelateerde eisen voor ICT-producten en ICT-diensten bij overheidsopdrachten, onder meer met betrekking tot cyberbeveiligingscertificering, versleuteling en het gebruik van open-source-cyberbeveiligingsproducten;

3° voor het beheer van kwetsbaarheden, met inbegrip van de bevordering en vergemakkelijking van de gecoördineerde bekendmaking van kwetsbaarheden overeenkomstig artikel 22;

4° inzake het in stand houden van de algemene beschikbaarheid, integriteit en vertrouwelijkheid van de openbare kern van het open internet, in voorkomend geval met inbegrip van de cyberbeveiliging van onderzeese communicatiekabels;

5° voor het bevorderen van de ontwikkeling en integratie van relevante geavanceerde technologieën met het oog op de toepassing van geavanceerde risicobeheersmaatregelen op het gebied van cyberbeveiliging;

6° voor het bevorderen en ontwikkelen van onderwijs en opleiding op het gebied van cyberbeveiliging, cyberbeveiligingsvaardigheden, bewustmakings- en onderzoeks- en ontwikkelingsinitiatieven rond cyberbeveiliging, alsook van richtsnoeren voor goede praktijken en controles op het gebied van cyberhygiène, gericht op burgers, belanghebbenden en entiteiten;

7° voor het ondersteunen van academische en onderzoeksinstellingen bij de ontwikkeling, versterking en bevordering van de uitrol van instrumenten voor cyberbeveiliging en een veilige netwerkinfrastructuur;

8° met inbegrip van relevante procedures en passende instrumenten voor het delen van informatie, ter ondersteuning van het vrijwillig delen van cyberbeveiligingsinformatie tussen entiteiten;

9° voor het versterken van de digitale weerbaarheid en het basisniveau van cyberhygiène van kleine en middelgrote ondernemingen, met name die welke van het toepassingsgebied van deze wet zijn uitgesloten, door te voorzien in gemakkelijk toegankelijke richtsnoeren en bijstand voor hun specifieke behoeften;

10° voor het bevorderen van actieve cyberbescherming.

CHAPITRE 5

Le plan national de réaction aux crises cyber et incidents de cybersécurité

Art. 29

§ 1^{er}. Le Roi établit, par arrêté délibéré en Conseil des ministres, un plan national de réaction aux crises cyber et incidents de cybersécurité. Ce plan constitue un plan national au sens de l'article 9, § 2, de la loi du 15 mai 2007 relative à la sécurité civile.

§ 2. Sans préjudice des éléments devant être contenus dans les plans nationaux, le plan national de réaction aux crises cyber et incidents de cybersécurité contient au moins les éléments suivants:

1° les objectifs des mesures et activités nationales de préparation;

2° les tâches et responsabilités des autorités de gestion des crises cyber;

3° les procédures de gestion des crises cyber, y compris leur intégration dans le cadre national général de gestion des crises et les canaux d'échange d'informations;

4° les mesures de préparation nationales, y compris des exercices et des activités de formation;

5° les parties prenantes et les infrastructures des secteurs public et privé concernées;

6° les procédures et arrangements nationaux entre les autorités et les organismes nationaux compétents visant à garantir la participation et le soutien effectifs de la Belgique à la gestion coordonnée des crises cyber et incidents de cybersécurité au niveau de l'Union européenne.

HOOFDSTUK 5

Het nationale plan voor cyberbeveiligingsincidenten en cybercrisisrespons

Art. 29

§ 1. De Koning stelt, bij besluit vastgesteld na overleg in de Ministerraad, een nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons op. Dit plan is een nationaal plan als bedoeld in artikel 9, § 2, van de wet van 15 mei 2007 betreffende de civiele veiligheid.

§ 2. Onverminderd de elementen die moeten worden opgenomen in de nationale plannen, bevat het nationale plan voor cyberbeveiligingsincidenten en cybercrisisrespons ten minste:

1° de doelstellingen van de nationale paraatheidsmaatregelen en -activiteiten;

2° de taken en verantwoordelijkheden van de cybercrisisbeheerautoriteiten;

3° de cybercrisisbeheerprocedures, met inbegrip van de integratie ervan in het algemene nationale crisisbeheerkader en in de informatie-uitwisselingskanalen;

4° de nationale paraatheidsmaatregelen, met inbegrip van oefeningen en opleidingsactiviteiten;

5° de relevante publieke en particuliere belanghebbenden en betrokken infrastructuur;

6° de nationale procedures en regelingen tussen de betrokken nationale autoriteiten en instanties om de effectieve deelname van België aan het gecoördineerde beheer van cybercrises en cyberbeveiligingsincidenten op het niveau van de Europese Unie en de ondersteuning daarvan te waarborgen.

TITRE 3

Mesures de gestion des risques en matière de cybersécurité et obligations d'information

CHAPITRE 1

Mesures de gestion des risques en matière de cybersécurité

Art. 30

§ 1^{er}. Les entités essentielles et importantes prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services.

§ 2. Les mesures visées au paragraphe 1^{er} garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, en tenant compte de l'état des connaissances et, s'il y a lieu, des normes européennes et internationales applicables, ainsi que du coût de mise en œuvre. Lors de l'évaluation de la proportionnalité de ces mesures, il convient de tenir dûment compte du degré d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales et économiques.

§ 3. Les mesures visées au paragraphe 1^{er} sont fondées sur une approche "tous risques" qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents, et elles portent au moins sur:

1° les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information;

2° la gestion des incidents;

3° la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises;

4° la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs;

TITEL 3

Maatregelen voor het beheer van cyberbeveiligingsrisico's en rapportageverplichtingen

HOOFDSTUK 1

Maatregelen voor het beheer van cyberbeveiligingsrisico's

Art. 30

§ 1. De essentiële en belangrijke entiteiten nemen passende en evenredige technische, operationele en organisatorische maatregelen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die zij voor hun activiteiten of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken.

§ 2. Rekening houdend met de stand van de techniek en, indien van toepassing, de desbetreffende Europese en internationale normen, alsook met de uitvoeringskosten, zorgen de in paragraaf 1 bedoelde maatregelen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen. Bij de beoordeling van de evenredigheid van die maatregelen wordt naar behoren rekening gehouden met de mate waarin de entiteit aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen.

§ 3. De in paragraaf 1 bedoelde maatregelen zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen, en hebben ten minste betrekking op het volgende:

1° beleid inzake risicoanalyse en beveiliging van informatiesystemen;

2° incidentenbehandeling;

3° bedrijfscontinuïteit, zoals back-upbeheer, noodvoorzieningenplannen en crisisbeheer;

4° de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;

5° la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités;

6° des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité;

7° les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité;

8° des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement;

9° la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs;

10° l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins;

11° une politique de divulgation coordonnée des vulnérabilités.

§ 4. Lorsque les entités essentielles et importantes examinent lesquelles des mesures visées au paragraphe 3, 4°, sont appropriées, elles tiennent compte des vulnérabilités propres à chaque fournisseur et prestataire de services direct et de la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et prestataires de services, y compris de leurs procédures de développement sécurisé.

Ces mesures doivent être appropriées au regard des résultats des évaluations coordonnées au niveau de l'Union européenne des risques pour la sécurité des chaînes d'approvisionnement critiques.

§ 5. Chaque entité essentielle et importante effectue une analyse des risques fondée sur une approche "tous risques" qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents et élabore, sur la base de cette analyse, une P.S.I. reprenant au moins les aspects visés au paragraphe 3.

§ 6. Lorsqu'une entité essentielle ou importante constate qu'elle ne se conforme pas aux mesures prévues au paragraphe 3, elle prend, sans retard injustifié, toutes les mesures correctives nécessaires appropriées et proportionnées.

5° beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;

6° beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;

7° basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;

8° beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;

9° beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;

10° wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit;

11° een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden.

§ 4. Wanneer essentiële en belangrijke entiteiten nagaan welke maatregelen als bedoeld in paragraaf 3, 4°, passend zijn, houden zij rekening met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures.

Deze maatregelen moeten passend zijn in het licht van de resultaten van de op het niveau van de Europese Unie gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens.

§ 5. Iedere essentiële en belangrijke entiteit voert een risicoanalyse uit gebaseerd op een benadering die alle gevaren omvat en tot doel heeft de netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen en werkt, op basis daarvan, een I.B.B. uit dat minstens de in paragraaf 3 bedoelde aspecten bevat.

§ 6. Een essentiële of belangrijke entiteit die vaststelt dat zij niet voldoet aan de in paragraaf 3 bedoelde maatregelen, neemt onverwijld alle noodzakelijke, passende en evenredige corrigerende maatregelen.

Art. 31

§ 1^{er}. Les organes de direction des entités essentielles et importantes approuvent les mesures de gestion des risques en matière de cybersécurité que ces entités prennent afin de se conformer à l'article 30, supervisent leur mise en œuvre et sont responsables de la violation dudit article par ces entités.

Cet article est sans préjudice des règles en matière de responsabilité applicables aux institutions publiques, ainsi que de responsabilité des agents de la fonction publique et des responsables élus ou nommés.

§ 2. Les membres des organes de direction des entités essentielles et importantes suivent une formation pour que leurs connaissances et compétences soient suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité.

Art. 32

L'entité essentielle ou importante est responsable de l'analyse des risques effectuée ainsi que du choix et de la mise en œuvre des mesures visées à l'article 30, § 1^{er}.

Art. 33

Après consultation de l'autorité nationale de cybersécurité, de l'éventuelle autorité sectorielle concernée et des entités fédérées concernées, le Roi peut, par arrêté délibéré en Conseil des ministres, imposer des mesures supplémentaires de gestion des risques en matière de cybersécurité appropriées et proportionnées.

CHAPITRE 2

Notification d'incidents

Section 1^{re}*Notification obligatoire*

Art. 34

§ 1^{er}. Les entités essentielles et importantes notifient tout incident significatif sans retard injustifié au CSIRT national, selon les modalités établies dans un protocole conclu entre lui et le NCCN. Ces entités signalent, entre

Art. 31

§ 1. De bestuursorganen van essentiële en belangrijke entiteiten keuren de maatregelen voor het beheer van cyberbeveiligingsrisico's goed die deze entiteiten nemen om te voldoen aan artikel 30, zien toe op de uitvoering ervan en zijn aansprakelijk voor inbreuken door deze entiteiten op dat artikel.

Dit artikel doet geen afbreuk aan de aansprakelijkheidsregels die gelden voor overheidsinstanties, alsook voor ambtenaren en verkozen of benoemde mandatarissen.

§ 2. De leden van de bestuursorganen van essentiële en belangrijke entiteiten volgen een opleiding zodat ze over voldoende kennis en vaardigheden beschikken om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.

Art. 32

De essentiële of belangrijke entiteit is verantwoordelijk voor de uitgevoerde risicoanalyse, alsook voor de keuze en uitvoering van de maatregelen bedoeld in artikel 30, § 1.

Art. 33

Na raadpleging van de nationale cyberbeveiligingsautoriteit, de eventuele betrokken sectorale overheid en deelgebieden kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, passende en evenredige bijkomende maatregelen voor het beheer van cyberbeveiligingsrisico's opleggen.

HOOFDSTUK 2

Melding van incidenten

Afdeling 1

Verplichte melding

Art. 34

§ 1. De essentiële en belangrijke entiteiten melden elk significant incident onverwijld aan het nationale CSIRT, volgens de modaliteiten bepaald in een protocol gesloten tussen het nationale CSIRT en het NCCN. Deze entiteiten

autres, toute information permettant au CSIRT national de déterminer si l'incident a un impact transfrontière.

Le cas échéant, les entités concernées notifient, sans retard injustifié, aux destinataires de leurs services les incidents significatifs susceptibles de nuire à la fourniture des services relatifs aux secteurs ou sous-secteurs repris à l'annexe I et II.

Le CSIRT national communique immédiatement les notifications visées à l'alinéa 1^{er} aux éventuelles autorités sectorielles compétentes. Les notifications des entités essentielles sont également transmises au NCCN.

§ 2. Le cas échéant, les entités concernées communiquent, sans retard injustifié, aux destinataires de leurs services qui sont potentiellement affectés par une cybermenace importante toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace. Le cas échéant, les entités informent également ces destinataires de la cybermenace importante elle-même.

§ 3. Après consultation de l'autorité nationale de cybersécurité, des autorités sectorielles, du NCCN et des entités fédérées, le Roi peut déterminer, par arrêté délibéré en Conseil des ministres, des seuils précis de notification en fonction du degré d'impact ou d'urgence de l'incident.

§ 4. Le simple fait de notifier un incident n'accroît pas la responsabilité de l'entité qui est à l'origine de la notification.

Art. 35

§ 1^{er}. Aux fins de la notification visée à l'article 34, § 1^{er}, alinéa 1^{er}, les entités concernées soumettent au CSIRT national:

1° sans retard injustifié et en tout état de cause dans les vingt-quatre heures après avoir eu connaissance de l'incident significatif, une alerte précoce qui, le cas échéant, indique si l'on suspecte que l'incident significatif a été causé par des actes illicites ou malveillants ou s'il pourrait avoir un impact transfrontière;

2° sans retard injustifié et en tout état de cause dans les 72 heures après avoir eu connaissance de l'incident significatif, une notification d'incident qui, le cas échéant, met à jour les informations visées au 1° et fournit une évaluation initiale de l'incident significatif, y compris de

rapporter en outre toute information que le nationale CSIRT in staat stelt om eventuele grensoverschrijdende gevolgen van het incident te bepalen.

In voorkomend geval stellen de betrokken entiteiten de ontvangers van hun diensten onverwijld in kennis van significante incidenten die een nadelige invloed kunnen hebben op de verlening van de diensten betreffende de sectoren of deelsectoren van de bijlagen I en II.

Het nationale CSIRT bezorgt de in het eerste lid bedoelde meldingen onmiddellijk aan de eventuele bevoegde sectorale overheden. Meldingen van essentiële entiteiten worden ook doorgestuurd naar het NCCN.

§ 2. Indien van toepassing delen de betrokken entiteiten de ontvangers van hun diensten die mogelijkerwijs door een significante cyberdreiging worden getroffen, onverwijld mee welke maatregelen die ontvangers kunnen nemen in reactie op die dreiging. Indien nodig stellen de entiteiten die ontvangers ook in kennis van de significante cyberdreiging zelf.

§ 3. Na raadpleging van de nationale cyberbeveiligingsautoriteit, de sectorale overheden, het NCCN en de deelgebieden kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, precieze meldingsdrempels bepalen naargelang de impact of dringendheid van het incident.

§ 4. Een melding leidt niet tot blootstelling van de entiteit aan een verhoogde aansprakelijkheid.

Art. 35

§ 1. Voor de in artikel 34, § 1, eerste lid, bedoelde melding bezorgen de betrokken entiteiten het nationale CSIRT:

1° onverwijld en in elk geval binnen vierentwintig uur nadat zij kennis hebben gekregen van het significante incident, een vroegtijdige waarschuwing waarin, indien van toepassing, wordt aangegeven of het significante incident vermoedelijk door een onrechtmatige of kwaadwillige handeling is veroorzaakt, dan wel grensoverschrijdende gevolgen zou kunnen hebben;

2° onverwijld en in elk geval binnen 72 uur nadat zij kennis hebben gekregen van het significante incident, een incidentmelding met, indien van toepassing, een update van de in 1° bedoelde informatie, een initiële beoordeling van het significante incident, met inbegrip

sa gravité et de son impact, ainsi que des indicateurs de compromission, lorsqu'ils sont disponibles;

3° à la demande du CSIRT national ou de l'éventuelle autorité sectorielle concernée, un rapport intermédiaire sur les mises à jour pertinentes de la situation;

4° un rapport final au plus tard un mois après la présentation de la notification d'incident visée au 2°, comprenant les éléments suivants:

a) une description détaillée de l'incident, y compris de sa gravité et de son impact;

b) le type de menace ou la cause profonde qui a probablement déclenché l'incident;

c) les mesures d'atténuation appliquées et en cours;

d) le cas échéant, l'impact transfrontière de l'incident;

5° en cas d'incident en cours au moment de la présentation du rapport final visé au 4°, les entités concernées fournissent à ce moment-là un rapport d'avancement puis un rapport final dans un délai d'un mois à compter du traitement définitif de l'incident.

§ 2. Par dérogation au paragraphe 1^{er}, 2°, un prestataire de services de confiance notifie au CSIRT national les incidents significatifs qui ont un impact sur la fourniture de ses services de confiance, sans retard injustifié et en tout état de cause dans les vingt-quatre heures après avoir eu connaissance de l'incident significatif.

§ 3. Le CSIRT national communique, immédiatement, les notifications visées aux paragraphes 1^{er} et 2 aux éventuelles autorités sectorielles compétentes. Les notifications des entités essentielles sont également transmises au NCCN.

Art. 36

§ 1^{er} Le CSIRT national fournit, sans retard injustifié et si possible dans les vingt-quatre heures suivant la réception de l'alerte précoce visée à l'article 35, § 1^{er}, 1°, une réponse à l'entité émettrice de la notification, y compris un retour d'information initial sur l'incident significatif et, à la demande de l'entité, des orientations ou des conseils opérationnels sur la mise en œuvre d'éventuelles mesures d'atténuation.

van de ernst en de gevolgen ervan en, indien beschikbaar, de indicatoren voor aantasting;

3° op verzoek van het nationale CSIRT of van de eventuele betrokken sectorale overheid, een tussentijds verslag over relevante updates van de situatie;

4° uiterlijk één maand na de indiening van de in 2° bedoelde incidentmelding, een eindverslag waarin het volgende is opgenomen:

a) een gedetailleerde beschrijving van het incident, met inbegrip van de ernst en de gevolgen ervan;

b) het soort bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid;

c) toegepaste en lopende risicobeperkende maatregelen;

d) in voorkomend geval, de grensoverschrijdende gevolgen van het incident;

5° indien het incident nog aan de gang is op het moment dat het in 4° bedoelde eindverslag moet worden ingediend, dienen de betrokken entiteiten op dat moment een voortgangsverslag in, en binnen één maand nadat zij het incident definitief hebben afgehandeld, een eindverslag.

§ 2. In afwijking van paragraaf 1, 2°, meldt een verlener van vertrouwensdiensten significante incidenten die gevolgen hebben voor de verlening van zijn vertrouwensdiensten onverwijld, en in elk geval binnen vierentwintig uur nadat hij er kennis van heeft gekregen, aan het nationale CSIRT.

§ 3. Het nationale CSIRT bezorgt de in de paragrafen 1 en 2 bedoelde meldingen onmiddellijk aan de eventuele bevoegde sectorale overheden. Meldingen van essentiële entiteiten worden ook doorgestuurd naar het NCCN.

Art. 36

§ 1. Het nationale CSIRT verstrekt onverwijld en zo mogelijk binnen vierentwintig uur na ontvangst van de in artikel 35, § 1, bedoelde vroegtijdige waarschuwing een antwoord aan de meldende entiteit, met inbegrip van een eerste feedback over het significante incident en, op verzoek van de entiteit, richtsnoeren of operationeel advies voor de uitvoering van mogelijke risicobeperkende maatregelen.

§ 2. Le CSIRT national fournit un soutien technique supplémentaire si l'entité concernée le demande. Lorsqu'il y a lieu de suspecter que l'incident est de nature criminelle, le CSIRT national fournit également des orientations sur les modalités de notification de l'incident significatif aux autorités répressives.

Art. 37

§ 1^{er}. Lorsque c'est approprié, et notamment si l'incident significatif concerne deux États membres ou plus, le CSIRT national informe sans retard injustifié les autres États membres touchés et l'ENISA de l'incident significatif. Sont alors partagées des informations du type de celles reçues conformément à l'article 35. Ce faisant, le CSIRT national doit, dans le respect du droit de l'Union européenne ou du droit national, préserver la sécurité et les intérêts commerciaux de l'entité ainsi que la confidentialité des informations communiquées.

§ 2. Lorsque la sensibilisation du public est nécessaire pour prévenir un incident significatif ou pour faire face à un incident significatif en cours, ou lorsque la divulgation de l'incident significatif est par ailleurs dans l'intérêt public, le CSIRT national peut, après avoir consulté l'entité concernée, le NCCN, l'éventuelle autorité sectorielle concernée et le ministre concerné, informer le public de l'incident significatif ou exiger de l'entité qu'elle le fasse.

§ 3. À la demande de l'éventuelle autorité sectorielle concernée, l'autorité nationale de cybersécurité transmet les notifications reçues en vertu de l'article 34, § 1^{er}, alinéa 1^{er}, aux points de contact uniques des autres États membres touchés.

§ 4. L'autorité nationale de cybersécurité soumet tous les trois mois à l'ENISA un rapport de synthèse comprenant des données anonymisées et agrégées sur les incidents significatifs, les incidents, les cybermenaces et les incidents évités notifiés conformément à l'article 34, § 1^{er}, alinéa 1^{er}, et à l'article 38, § 1^{er}.

§ 5. Le CSIRT national fournit aux autorités compétentes en vertu de la loi du 1^{er} juillet 2011 des informations sur les incidents significatifs, les incidents, les cybermenaces et les incidents évités notifiés conformément à l'article 34, § 1^{er}, alinéa 1^{er}, et à l'article 38, § 1^{er}, par les exploitants d'infrastructures identifiées comme infrastructures critiques en vertu de la loi du 1^{er} juillet 2011.

§ 2. Het nationale CSIRT verleent aanvullende technische ondersteuning indien de betrokken entiteit daarom verzoekt. Wanneer wordt vermoed dat het significante incident van criminele aard is, geeft het nationale CSIRT ook richtsnoeren voor het melden van het significante incident aan de rechtshandavingsinstanties.

Art. 37

§ 1. In voorkomend geval, en met name wanneer het significante incident betrekking heeft op twee of meer lidstaten, stelt het nationale CSIRT de andere getroffen lidstaten en Enisa onverwijld in kennis van het significante incident. Die informatie omvat het soort informatie dat overeenkomstig artikel 35 is ontvangen. Daarbij beschermt het nationale CSIRT, overeenkomstig het Unie- of het nationale recht, de beveiligings- en commerciële belangen van de entiteit, alsook de vertrouwelijkheid van de verstrekte informatie.

§ 2. Wanneer publieke bewustmaking nodig is om een significant incident te voorkomen of een lopend incident aan te pakken, of wanneer de bekendmaking van het significante incident anderszins in het algemeen belang is, kan het nationale CSIRT, na raadpleging van de betrokken entiteit, het NCCN, de eventuele betrokken sectorale overheid en de betrokken minister, het publiek over het significante incident informeren of van de entiteit verlangen dat zij dit doet.

§ 3. De nationale cyberbeveiligingsautoriteit stuurt, op verzoek van de eventuele betrokken sectorale overheid, de op grond van artikel 34, § 1, eerste lid, ontvangen meldingen door naar de centrale contactpunten van de andere betrokken lidstaten.

§ 4. De nationale cyberbeveiligingsautoriteit dient om de drie maanden bij Enisa een samenvattend verslag in met geanonimiseerde en geaggregeerde gegevens over significante incidenten, incidenten, cyberdreigingen en bijna-incidenten die overeenkomstig artikel 34, § 1, eerste lid, en artikel 38, § 1, zijn gemeld.

§ 5. Het nationale CSIRT verstrekt de uit hoofde van de wet van 1 juli 2011 bevoegde autoriteiten informatie over significante incidenten, incidenten, cyberdreigingen en bijna-incidenten die overeenkomstig artikel 34, § 1, eerste lid, en artikel 38, § 1, zijn gemeld door exploitanten van infrastructuur die uit hoofde van de wet van 1 juli 2011 als kritieke infrastructuur zijn aangemerkt.

Section 2*Notification volontaire***Art. 38**

§ 1^{er}. Outre les obligations de notification prévues à l'article 34, peuvent être notifiés à titre volontaire au CSIRT national par:

1° les entités essentielles et importantes, les incidents, les cybermenaces et les incidents évités;

2° les entités autres que celles visées au 1°, indépendamment du fait qu'elles relèvent ou non du champ d'application de la présente loi, les incidents significatifs, les cybermenaces et les incidents évités.

§ 2. Les notifications volontaires visées au paragraphe 1^{er} sont traitées de la même manière que les notifications obligatoires visées à la section 1^{re} du présent chapitre.

Les notifications obligatoires peuvent néanmoins être traitées de manière prioritaire par rapport aux notifications volontaires.

Sans préjudice de la prévention et de la détection d'infractions pénales et des enquêtes et poursuites en la matière, un signalement volontaire n'a pas pour effet direct de lancer une inspection visée à l'article 44 ou d'imposer à l'entité ayant effectué la notification des obligations supplémentaires auxquelles elle n'aurait pas été soumise si elle n'avait pas transmis la notification.

TITRE 4*Supervision et sanctions***CHAPITRE 1^{ER}****Supervision****Section 1^{re}***Évaluation périodique de la conformité***Art. 39**

Les entités essentielles se soumettent à une évaluation périodique de la conformité de la mise en œuvre des mesures de gestion des risques en matière de cybersécurité visées à l'article 30, sur base des modalités et des cadres de référence déterminés par le Roi:

Afdeling 2*Vrijwillige melding***Art. 38**

§ 1. Naast de in artikel 34 bedoelde meldingsverplichtingen kunnen vrijwillig aan het nationale CSIRT worden gemeld door:

1° essentiële en belangrijke entiteiten: incidenten, cyberdreigingen en bijna-incidenten;

2° andere dan in 1° bedoelde entiteiten, ongeacht of zij tot het toepassingsgebied van deze wet behoren: significante incidenten, cyberdreigingen en bijna-incidenten.

§ 2. De in paragraaf 1 bedoelde vrijwillige meldingen worden op dezelfde wijze verwerkt als de verplichte meldingen bedoeld in afdeling 1 van dit hoofdstuk.

Er kan evenwel voorrang worden gegeven aan de verwerking van verplichte meldingen boven die van vrijwillige meldingen.

Onverminderd het voorkomen, opsporen, onderzoeken en vervolgen van misdrijven, mag een vrijwillige melding er niet direct toe leiden dat een inspectie volgens artikel 44 wordt opgestart of dat er bijkomende verplichtingen worden opgelegd aan de meldende entiteit waaraan zij niet zou zijn onderworpen indien zij de melding niet had ingediend.

TITEL 4*Toezicht en sancties***HOOFDSTUK 1****Toezicht****Afdeling 1***Regelmatige conformiteitsbeoordeling***Art. 39**

Essentiële entiteiten onderwerpen zich aan een regelmatige conformiteitsbeoordeling van de uitvoering van de maatregelen voor het beheer van cyberbeveiligingsrisico's bedoeld in artikel 30, op basis van de door de Koning bepaalde modaliteiten en referentiekaders:

1° Soit en choisissant une évaluation périodique de la conformité visée à l'article 40, sur base de l'un des cadres de référence déterminé par le Roi;

2° Soit en se soumettant à une inspection par l'autorité nationale de cybersécurité, sur base des modalités déterminées par le Roi.

Par dérogation à l'alinéa 1^{er}, et à la demande de l'autorité sectorielle concernée, les inspections visées à l'alinéa 1^{er}, 2°, sont effectuées de manière conjointe, sous la direction de l'autorité nationale de cybersécurité ou sont déléguées à l'éventuel service d'inspection concerné moyennant l'accord de l'autorité nationale de cybersécurité.

Lorsque le Roi détermine plusieurs cadres de référence, les entités essentielles choisissent le cadre de référence auquel ils se soumettent.

Art. 40

§ 1^{er}. L'évaluation périodique de la conformité visée à l'article 39, alinéa 1^{er}, 1°, est effectuée par un organisme d'évaluation de la conformité agréé par l'autorité nationale de cybersécurité selon les conditions fixées par le Roi.

Pour le contrôle des entités identifiées comme exploitants d'une infrastructure critique au sens de la loi du 1^{er} juillet 2011 et des entités de l'administration publique, l'organisme d'évaluation de la conformité ainsi que les personnes physiques qui évaluent la conformité disposent d'une habilitation de sécurité.

§ 2. Le service d'inspection de l'autorité nationale de cybersécurité peut à tout moment vérifier le respect des conditions d'agrément visées au paragraphe 1^{er} par les organismes d'évaluation de la conformité, conformément aux dispositions du présent chapitre.

Art. 41

Les entités importantes peuvent, de manière volontaire, se soumettre à une évaluation périodique de la conformité visée à l'article 39, alinéa 1^{er}, 1°, de la mise en œuvre des mesures de gestion des risques en matière de cybersécurité visées à l'article 30, § 3, sur base des modalités et des cadres de référence déterminés par le Roi.

1° ofwel opteren zij voor een in artikel 40 bedoelde regelmatige conformiteitsbeoordeling, op basis van een van de door de Koning bepaalde referentiekaders;

2° ofwel onderwerpen zij zich aan een inspectie door de nationale cyberbeveiligingsautoriteit, op basis van de door de Koning bepaalde nadere regels.

In afwijking van het eerste lid en op verzoek van de betrokken sectorale overheid worden de in het eerste lid, 2°, bedoelde inspecties gezamenlijk uitgevoerd, onder leiding van de nationale cyberbeveiligingsautoriteit of worden gedelegeerd aan de betrokken inspectiedienst mits akkoord van de nationale cyberbeveiligingsautoriteit.

Indien de Koning meerdere referentiekaders bepaalt, kiezen essentiële entiteiten aan welk referentiekader zij zich onderwerpen.

Art. 40

§ 1. De in artikel 39, eerste lid, 1°, bedoelde regelmatige conformiteitsbeoordeling wordt verricht door een conformiteitsbeoordelingsinstantie die erkend is door de nationale cyberbeveiligingsautoriteit volgens de door de Koning bepaalde voorwaarden.

Voor het toezicht op entiteiten die worden geïdentificeerd als exploitanten van een kritieke infrastructuur als bedoeld in de wet van 1 juli 2011 en overheidsinstanties beschikken de conformiteitsbeoordelingsinstantie en de natuurlijke personen die de conformiteit beoordelen over een veiligheidsmachtiging.

§ 2. De inspectiedienst van de nationale cyberbeveiligingsautoriteit kan op elk ogenblik nagaan of de conformiteitsbeoordelingsinstanties de in paragraaf 1 bedoelde erkenningsvoorwaarden naleven, overeenkomstig de bepalingen van dit hoofdstuk.

Art. 41

Belangrijke entiteiten kunnen zich vrijwillig onderwerpen aan een regelmatige conformiteitsbeoordeling als bedoeld in artikel 39, eerste lid, 1°, van de uitvoering van de maatregelen voor het beheer van cyberbeveiligingsrisico's bedoeld in artikel 30, § 3, op basis van de door de Koning bepaalde modaliteiten en referentiekaders.

Art. 42

Les entités essentielles et importantes qui se soumettent à une évaluation périodique de la conformité visée à l'article 39, alinéa 1^{er}, 1^o, respectivement conformément à l'article 39 et 41 sont, jusqu'à preuve du contraire, présumées respecter les obligations visées à l'article 30.

Art. 43

Une liste des organismes d'évaluation de la conformité agréés par l'autorité nationale de cybersécurité conformément à l'article 40 est disponible auprès de l'autorité nationale de cybersécurité, qui la tient à jour.

Section 2

Dispositions générales relatives au service d'inspection

Art. 44

§ 1^{er}. Le service d'inspection de l'autorité nationale de cybersécurité réalise des contrôles du respect par les entités essentielles et importantes des mesures de gestion des risques en matière de cybersécurité et des règles de notification des incidents.

Par dérogation à l'alinéa 1^{er}, et à la demande de l'autorité sectorielle concernée, ces contrôles sont effectués de manière conjointe, sous la direction de l'autorité nationale de cybersécurité, ou sont délégués à l'éventuel service d'inspection concerné moyennant l'accord de l'autorité nationale de cybersécurité.

L'autorité sectorielle ou le service d'inspection sectoriel compétent, ou, lorsqu'aucun service d'inspection sectoriel n'a été désigné par la loi ou par le Roi, le service d'inspection de l'autorité nationale de cybersécurité peut réaliser des contrôles du respect par les entités essentielles et importantes des mesures de gestion des risques en matière de cybersécurité sectorielles ou sous-sectorielles supplémentaires visées à l'article 33.

§ 2. Au moment de formuler une demande d'informations ou de preuves, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent mentionnent la finalité de la demande, les informations ou preuves précises demandées et le délai dans lequel celles-ci doivent être fournies.

Le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel

Art. 42

Essentiële en belangrijke entiteiten die zich aan een regelmatige conformiteitsbeoordeling als bedoeld in artikel 39, eerste lid, 1^o, onderwerpen, respectievelijk overeenkomstig artikel 39 en 41, worden tot bewijs van het tegendeel geacht de in artikel 30 bedoelde verplichtingen na te leven.

Art. 43

Een lijst van de conformiteitsbeoordelingsinstanties die overeenkomstig artikel 40 erkend zijn door de nationale cyberbeveiligingsautoriteit, is beschikbaar bij laatstgenoemde autoriteit, die ze actueel houdt.

Afdeling 2

Algemene bepalingen betreffende de inspectiedienst

Art. 44

§ 1. De inspectiedienst van de nationale cyberbeveiligingsautoriteit voert controles uit om na te gaan of de essentiële en belangrijke entiteiten de maatregelen voor het beheer van cyberbeveiligingsrisico's en de regels voor het melden van incidenten naleven.

In afwijking van het eerste lid en op verzoek van de betrokken sectorale overheid worden deze controles gezamenlijk uitgevoerd, onder leiding van de nationale cyberbeveiligingsautoriteit, of gedelegeerd aan de eventuele betrokken inspectiedienst mits akkoord van de nationale cyberbeveiligingsautoriteit.

De bevoegde sectorale overheid of sectorale inspectiedienst of, indien geen sectorale inspectiedienst is aangewezen door de wet of de Koning, de inspectiedienst van de nationale cyberbeveiligingsautoriteit kan controles uitvoeren om na te gaan of de essentiële en belangrijke entiteiten de bijkomende sectorale of deelsectorale maatregelen voor het beheer van cyberbeveiligingsrisico's bedoeld in artikel 33 naleven.

§ 2. Bij het formuleren van een verzoek om informatie of bewijzen vermelden de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst het doeleinde van het verzoek, de precieze informatie of bewijzen die worden gevraagd en de termijn waarbinnen deze moeten worden verstrekt.

De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid

service d'inspection sectoriel compétent peuvent faire appel à des experts.

§ 3. Le service d'inspection de l'autorité nationale de cybersécurité ainsi que les éventuels autorités sectorielles et services d'inspection sectoriels peuvent fixer des priorités en ce qui concerne les tâches de supervision visées au présent titre selon une approche basée sur les risques.

§ 4. Lorsqu'ils traitent des incidents donnant lieu à des violations de données à caractère personnel au sens de l'article 4, 12), du règlement (UE) 2016/679, le service d'inspection de l'autorité nationale de cybersécurité ainsi que les éventuels autorités sectorielles et services d'inspection sectoriels coopèrent étroitement avec les autorités de protection des données, sans préjudice de la compétence et des missions de ces dernières.

Art. 45

§ 1^{er}. Le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent informent les autorités compétentes en vertu de la loi du 1^{er} juillet 2011 lorsqu'ils exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'un exploitant d'une infrastructure définie comme critique en vertu de la loi du 1^{er} juillet 2011 respecte la présente loi. S'il y a lieu, les autorités compétentes en vertu de la loi du 1^{er} juillet 2011 peuvent demander au service d'inspection de l'autorité nationale de cybersécurité et à l'éventuelle autorité sectorielle ou à l'éventuel service d'inspection sectoriel compétent d'exercer leurs pouvoirs de supervision et d'exécution à l'égard d'un exploitant d'une infrastructure qui est définie comme infrastructure critique en vertu de la loi du 1^{er} juillet 2011.

§ 2. Le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent coopèrent avec les autorités compétentes pertinentes en vertu du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011. En particulier, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent informent le forum de supervision institué en vertu de l'article 32, paragraphe 1, dudit règlement lorsqu'ils exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'une entité essentielle ou

of sectorale inspectiedienst kunnen een beroep doen op experts.

§ 3. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele sectorale overheden en sectorale inspectiediensten kunnen prioriteit geven aan de in deze titel bedoelde toezichtstaken volgens een risicogebaseerde benadering.

§ 4. Bij de aanpak van incidenten die leiden tot inbreuken in verband met persoonsgegevens zoals gedefinieerd in artikel 4, punt 12, van Verordening (EU) 2016/679, werken de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele sectorale overheden en sectorale inspectiediensten nauw samen met de gegevensbeschermingsautoriteiten, onverminderd de bevoegdheid en taken van deze laatste.

Art. 45

§ 1. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst stellen de uit hoofde van de wet van 1 juli 2011 bevoegde autoriteiten in kennis wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat een exploitant van een infrastructuur die op grond van de wet van 1 juli 2011 als kritieke infrastructuur wordt aangemerkt, voldoet aan deze wet. In voorkomend geval kunnen de uit hoofde van de wet van 1 juli 2011 bevoegde autoriteiten de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst verzoeken hun toezichts- en handhavingsbevoegdheden uit te oefenen ten aanzien van een exploitant van een infrastructuur die is aangemerkt als kritieke infrastructuur uit hoofde van de wet van 1 juli 2011.

§ 2. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst werken samen met de relevante autoriteiten die bevoegd zijn uit hoofde van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst stellen met name het oversightforum dat is opgericht op grond van artikel 32, lid 1, van bovengenoemde verordening in kennis wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat

importante qui a été désignée comme étant un prestataire tiers critique de services TIC au titre de l'article 31 dudit règlement respecte la présente loi.

Art. 46

§ 1^{er}. Lorsque les réseaux et les systèmes d'information d'une entité sont situés en dehors du territoire belge, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent, en concertation avec l'autorité nationale de cybersécurité, peuvent solliciter la coopération et l'assistance des autorités de contrôle compétentes d'autres États membres.

Dans le cadre de la sollicitation visée à l'alinéa 1^{er}:

1° le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent peuvent demander aux autorités de contrôle compétentes d'autres États membres de prendre des mesures de supervision ou d'exécution;

2° le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent peuvent demander, de manière motivée, aux autorités de contrôle compétentes d'autres États membres une assistance mutuelle afin que les mesures de supervision ou d'exécution puissent être mises en œuvre de manière effective, efficace et cohérente.

L'assistance mutuelle visée à l'alinéa 2, 2°, peut porter sur des demandes d'informations et des mesures de contrôle, y compris des demandes de procéder à des inspections sur place, à des contrôles à distance ou à des audits de sécurité ciblés.

§ 2. De manière proportionnée à leurs ressources et pour autant que cela rentre dans le cadre de leurs compétences, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent coopèrent et apportent leur assistance aux autorités de contrôle compétentes en matière de cybersécurité d'autres États membres qui en font la demande, lorsque les réseaux et les systèmes d'information de l'entité concernée sont situés dans le territoire belge.

Dans le cadre de la demande visée à l'alinéa 1^{er}:

1° l'autorité nationale de cybersécurité centralise les informations et consultations en ce qui concerne

een essentiële of belangrijke entiteit die op grond van artikel 31 van bovengenoemde verordening als kritieke derde aanbieder van ICT-diensten is aangewezen, voldoet aan deze wet.

Art. 46

§ 1. Wanneer de netwerk- en informatiesystemen van een entiteit zich buiten het Belgische grondgebied bevinden, kunnen de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst, in overleg met de nationale cyberbeveiligingsautoriteit, de bevoegde toezichthoudende autoriteiten van andere lidstaten om samenwerking en bijstand verzoeken.

In het kader van het verzoek bedoeld in het eerste lid:

1° kunnen de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst de bevoegde toezichthoudende autoriteiten van andere lidstaten verzoeken om toezichts- of handhavingsmaatregelen te nemen;

2° kunnen de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst de bevoegde toezichthoudende autoriteiten van andere lidstaten gemotiveerd om wederzijdse bijstand verzoeken, zodat de toezichts- of handhavingsmaatregelen op een effectieve, efficiënte en consistente wijze kunnen worden uitgevoerd.

De wederzijdse bijstand bedoeld in het tweede lid, 2°, kan betrekking hebben op verzoeken om informatie en toezichtsmaatregelen, met inbegrip van verzoeken om inspecties ter plaatse, toezicht elders of gerichte beveiligingsaudits uit te voeren.

§ 2. In verhouding tot hun middelen en voor zover dit binnen hun bevoegdheden valt, werken de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst samen met de toezichthoudende autoriteiten bevoegd voor cyberbeveiliging van andere lidstaten en verlenen ze bijstand aan deze autoriteiten indien deze hierom verzoeken en de netwerk- en informatiesystemen van de betrokken entiteit zich op Belgisch grondgebied bevinden.

In het kader van het verzoek bedoeld in het eerste lid:

1° centraliseert de nationale cyberbeveiligingsautoriteit de informatie en raadplegingen met betrekking tot

les mesures de supervision et d'exécution prises par elle-même, par l'éventuelle autorité sectorielle et par l'éventuel service d'inspection sectoriel compétent et les communique aux autorités de contrôle compétentes en matière de cybersécurité d'autres États membres;

2° ladite demande peut porter sur des mesures de supervision ou d'exécution;

3° ladite demande peut, de manière motivée, porter sur une assistance mutuelle afin que les mesures de supervision ou d'exécution puissent être mises en œuvre de manière effective, efficace et cohérente.

L'assistance mutuelle visée à l'alinéa 2, 3°, peut porter sur des demandes d'informations et des mesures de contrôle, y compris des demandes de procéder à des inspections sur place, à des contrôles à distance ou à des audits de sécurité ciblés.

L'autorité à laquelle une demande d'assistance est adressée ne peut refuser cette demande que s'il est établi que ladite autorité n'est pas compétente pour fournir l'assistance demandée, que l'assistance demandée n'est pas proportionnée aux tâches de supervision de ladite autorité ou que la demande concerne des informations ou implique des activités dont la divulgation ou l'exercice seraient contraires aux intérêts essentiels de la sécurité nationale, la sécurité publique ou la défense de la Belgique. Avant de refuser une telle demande, ladite autorité consulte les autres autorités compétentes concernées ainsi que, à la demande de l'un des États membres concernés, la Commission et l'ENISA.

§ 3. D'un commun accord, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent peuvent mener à bien des actions communes de supervision entre elles et/ou avec les autorités de contrôle compétentes d'autres États membres.

§ 4. Le présent article n'est pas applicable aux missions diplomatiques et consulaires.

Art. 47

§ 1^{er}. Les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent sont dotés d'une carte de légitimation dont le modèle est fixé par le Roi.

§ 2. Les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité

de toezichts- en handhavingsmaatregelen die zichzelf of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst heeft genomen, en deelt deze mee aan de toezichthoudende autoriteiten bevoegd voor cyberbeveiliging van andere lidstaten;

2° dit verzoek kan betrekking hebben op toezichts- of handhavingsmaatregelen;

3° dit verzoek kan, indien het gemotiveerd wordt, betrekking hebben op wederzijdse bijstand, zodat de toezichts- of handhavingsmaatregelen op een effectieve, efficiënte en consistente wijze kunnen worden uitgevoerd.

De wederzijdse bijstand bedoeld in het tweede lid, 3°, kan betrekking hebben op verzoeken om informatie en toezichtsmaatregelen, met inbegrip van verzoeken om inspecties ter plaatse, toezicht elders of gerichte beveiligingsaudits uit te voeren.

De autoriteit waaraan een verzoek om bijstand is gericht, mag dat verzoek niet weigeren, tenzij wordt vastgesteld dat zij niet bevoegd is om de gevraagde bijstand te verlenen, de gevraagde bijstand niet in verhouding staat tot de toezichthoudende taken van deze autoriteit, of het verzoek betrekking heeft op informatie of activiteiten inhoudt die, indien ze openbaar zouden worden gemaakt of zouden worden uitgevoerd, in strijd zouden zijn met de wezenlijke belangen van de nationale veiligheid, de openbare veiligheid of de defensie van België. Alvorens een dergelijk verzoek af te wijzen, raadpleegt voornoemde autoriteit de andere betrokken bevoegde autoriteiten alsook, op verzoek van een van de betrokken lidstaten, de Commissie en Enisa.

§ 3. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst kunnen in onderlinge overeenstemming gezamenlijke toezichtsacties uitvoeren, en dit onderling en/of met de bevoegde toezichthoudende autoriteiten van andere lidstaten.

§ 4. Dit artikel is niet van toepassing op diplomatieke en consulaire missies.

Art. 47

§ 1. De leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst beschikken over een legitimatiekaart waarvan het model door de Koning wordt bepaald.

§ 2. De leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde

sectorielle ou de l'éventuel service d'inspection sectoriel compétent et les experts appelés à participer à l'inspection ne peuvent avoir un intérêt quelconque, direct ou indirect, dans les entreprises ou institutions qu'ils sont chargés de contrôler, susceptible de compromettre leur objectivité. Ils prêtent serment auprès du fonctionnaire dirigeant de leur service.

Les autorités visées à l'article 44, § 1^{er}, prennent les mesures nécessaires afin d'assurer l'indépendance des membres de leur personnel, de prévenir, d'identifier et de résoudre efficacement les conflits d'intérêts lors de l'exécution de leurs tâches.

La notion de conflit d'intérêts vise au moins les situations dans lesquelles un membre du personnel des autorités visées à l'article 44, § 1^{er}, a, directement ou indirectement, un intérêt financier, économique ou un autre intérêt personnel qui pourrait être perçu comme compromettant son impartialité et son indépendance dans le cadre de sa mission ou de ses fonctions.

§ 3. Les membres du personnel des autorités visées à l'article 44, § 1^{er}, ne reçoivent ni ne cherchent pas, dans les limites de leurs attributions, de façon directe ou indirecte, d'instructions de personne tierce.

Il leur est interdit d'être présents lors d'une délibération ou décision sur les dossiers pour lesquels ils ont un intérêt personnel ou direct ou pour lesquels leurs parents ou alliés jusqu'au troisième degré ont un intérêt personnel ou direct.

Le Roi peut également désigner d'autres situations comme étant des conflits d'intérêts.

Section 3

La supervision des entités par le service d'inspection

Art. 48

§ 1^{er}. Sans préjudice des attributions des officiers de police judiciaire visées à l'article 8 du Code d'instruction criminelle, les membres assermentés du service d'inspection de l'autorité nationale de cybersécurité et les membres assermentés de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent disposent, dans l'exercice de leur mission de supervision, des compétences de contrôle suivantes, tant dans le cadre de démarches administratives que dans le cadre de la constatation de violations de la présente loi:

sectorale overheid of sectorale inspectiedienst en de experten die deelnemen aan de inspectie, mogen geen enkel rechtstreeks of onrechtstreeks belang hebben in de ondernemingen of instellingen waarop zij toezicht dienen uit te oefenen, waardoor hun objectiviteit in het gedrang zou kunnen komen. Zij leggen de eed af bij de leidend ambtenaar van hun dienst.

De autoriteiten bedoeld in artikel 44, § 1, nemen de nodige maatregelen om, bij de uitvoering van hun taken, de onafhankelijkheid van hun personeelsleden te garanderen en om belangenconflicten doeltreffend te voorkomen, te identificeren en op te lossen.

Het begrip "belangenconflict" heeft minstens betrekking op situaties waarin een personeelslid van de autoriteiten bedoeld in artikel 44, § 1, rechtstreeks of onrechtstreeks financiële, economische of andere persoonlijke belangen heeft die geacht kunnen worden zijn onpartijdigheid en onafhankelijkheid in het kader van zijn opdracht of functie in het gedrang te brengen.

§ 3. De personeelsleden van de autoriteiten bedoeld in artikel 44, § 1, krijgen noch vragen binnen de grenzen van hun bevoegdheden op directe of indirecte wijze instructies van derden.

Het is hen verboden aanwezig te zijn bij een beraadslaging of besluit over dossiers waarin zij een persoonlijk of rechtstreeks belang hebben of waarin hun bloed- of aanverwanten tot en met de derde graad een persoonlijk of rechtstreeks belang hebben.

De Koning kan ook andere situaties benoemen als belangenconflicten.

Afdeling 3

Het door de inspectiedienst uitgeoefende toezicht op de entiteiten

Art. 48

§ 1. Onverminderd de bevoegdheden van de officieren van gerechtelijke politie bedoeld in artikel 8 van het Wetboek van strafvordering beschikken de beëdigde leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de beëdigde leden van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst bij de uitoefening van hun toezichtsopdracht over de volgende toezichtsbevoegdheden, en dit zowel in het kader van administratieve handelingen als in het kader van de vaststelling van inbreuken op deze wet:

1° demander l'accès à et obtenir une copie de tout document ou toute information nécessaire à l'exercice de leur mission de supervision, notamment les preuves de la mise en œuvre de politiques de cybersécurité, telles que les résultats des évaluations de la conformité ou des audits de sécurité et les éléments de preuve sous-jacents correspondants;

2° procéder, sur place ou à distance, à tout examen, contrôle et audition, y compris des contrôles aléatoires effectués par des professionnels formés;

3° soumettre les entités essentielles à des audits de sécurité réguliers et ciblés réalisés par un organisme indépendant, basés sur des évaluations des risques effectuées par le service d'inspection concerné ou l'entité contrôlée, ou sur d'autres informations disponibles relatives aux risques;

4° requérir toutes les informations qu'ils estiment nécessaires à l'évaluation des mesures de gestion des risques en matière de cybersécurité adoptées par l'entité concernée, notamment les politiques de cybersécurité consignées par écrit, du respect de l'obligation de soumettre des informations à l'autorité nationale de cybersécurité ou à l'éventuelle autorité sectorielle conformément au titre 1^{er} et de la mise en œuvre de la présente loi;

5° réaliser un audit *ad hoc*, notamment lorsqu'il est justifié en raison d'un incident significatif ou d'une violation de la présente loi;

6° effectuer des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération de l'entité concernée;

7° prendre l'identité des personnes qui se trouvent sur les lieux utilisés par l'entité et dont ils estiment l'audition nécessaire pour l'exercice de leur mission. À cet effet, ils peuvent exiger de ces personnes la présentation de documents officiels d'identification;

8° le cas échéant, demander l'assistance des services de la police fédérale ou locale dans le cadre de l'usage de la force;

9° solliciter des informations auprès des membres du personnel visés à l'article 9 de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, pour les besoins de l'exécution des dispositions de la présente loi;

1° toegang vragen tot alle documenten of informatie die nodig zijn voor de uitoefening van hun toezichtsoverdracht en hiervan een kopie verkrijgen, met name de bewijzen van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van conformiteitsbeoordelingen en van beveiligingsaudits en de respectieve onderliggende bewijzen;

2° overgaan, ter plaatse of elders, tot elk onderzoek, elke controle en elk verhoor, met inbegrip van steekproefsgewijze controles die worden uitgevoerd door daartoe opgeleide professionals;

3° essentiële entiteiten onderwerpen aan regelmatige en gerichte beveiligingsaudits die worden uitgevoerd door een onafhankelijke instantie, gebaseerd op door de betrokken inspectiedienst of de gecontroleerde entiteit verrichte risicobeoordelingen of op andere beschikbare risicogerelateerde informatie;

4° alle inlichtingen inwinnen die zij nodig achten voor de beoordeling van de door de betrokken entiteit genomen maatregelen voor het beheer van cyberbeveiligingsrisico's, met name betreffende het gedocumenteerde cyberbeveiligingsbeleid, de naleving van de verplichting om informatie in te dienen bij de nationale cyberbeveiligingsautoriteit of bij de eventuele sectorale overheid overeenkomstig titel 1 en de uitvoering van deze wet;

5° een ad-hocaudit uitvoeren, ook in gevallen waarin dat gerechtvaardigd is op grond van een significant incident of een inbreuk op deze wet;

6° beveiligingsscan uitvoeren op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria, indien nodig in samenwerking met de betrokken entiteit;

7° de identiteit opnemen van de personen die zich op de door de entiteit gebruikte plaatsen bevinden en van wie ze het verhoor nodig achten voor de uitoefening van hun opdracht. Daartoe kunnen ze van deze personen eisen dat ze officiële identificatiedocumenten voorleggen;

8° in voorkomend geval, de bijstand vragen van de federale of lokale politiediensten in het kader van het gebruik van geweld;

9° inlichtingen inwinnen bij de personeelsleden bedoeld in artikel 9 van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, voor de uitvoering van de bepalingen van deze wet;

10° pénétrer sans avertissement préalable, sur présentation de leur carte de légitimation, dans tous les lieux utilisés par l'entité; ils n'ont accès aux locaux habités que moyennant autorisation préalable délivrée par le juge d'instruction.

§ 2. Dans le cadre de l'inspection des entités importantes, les compétences de contrôle visées au paragraphe 1^{er} s'effectuent de manière *ex post*, sur base d'éléments de preuve, d'indications ou d'informations selon lesquels une entité importante ne respecterait pas la présente loi.

§ 3. Pour obtenir l'autorisation de pénétrer dans des locaux habités, les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent adressent une demande motivée au juge d'instruction. Cette demande contient au moins les données suivantes:

1° l'identification des espaces habités auxquels ils souhaitent avoir accès;

2° les manquements éventuels qui font l'objet du contrôle;

3° tous les documents et renseignements desquels il ressort que l'utilisation de ce moyen est nécessaire.

Le juge d'instruction décide dans un délai de quarante-huit heures maximum après réception de la demande. La décision du juge d'instruction est motivée. En l'absence de décision dans le délai prescrit, la visite des lieux est réputée être refusée. Le service d'inspection de l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent peut introduire un recours contre la décision de refus ou l'absence de décision devant la chambre des mises en accusation dans les quinze jours de la notification de la décision ou de l'expiration du délai.

Les visites sans autorisation de l'occupant dans des locaux habités se font entre cinq et vingt-et-une heures par au moins deux membres du service d'inspection agissant conjointement.

§ 4. Au début de toute audition, il est communiqué à la personne interrogée:

1° que ses déclarations peuvent être utilisées comme preuve en justice;

10° zonder voorafgaande verwittiging, op vertoon van hun legitimatiekaart, alle door de entiteit gebruikte plaatsen betreden; zij hebben slechts toegang tot bewoonde lokalen mits vooraf een machtiging is uitgereikt door de onderzoeksrechter.

§ 2. In het kader van de inspectie van belangrijke entiteiten worden de toezichtsbevoegdheden bedoeld in paragraaf 1 achteraf ("*ex post*") uitgeoefend op basis van bewijzen, aanwijzingen of informatie waaruit blijkt dat een belangrijke entiteit deze wet niet zou naleven.

§ 3. Om een machtiging tot betreding van bewoonde lokalen te bekomen, richten de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst een met redenen omkleed verzoek aan de onderzoeksrechter. Dit verzoek bevat minstens de volgende gegevens:

1° de identificatie van de bewoonde ruimten waartoe zij toegang wensen te hebben;

2° de eventuele inbreuken die het voorwerp zijn van het toezicht;

3° alle documenten en inlichtingen waaruit blijkt dat het gebruik van dit middel nodig is.

De onderzoeksrechter beslist binnen een termijn van maximum achtenveertig uur na ontvangst van het verzoek. De beslissing van de onderzoeksrechter is met redenen omkleed. Bij gebrek aan een beslissing binnen de voorgeschreven termijn wordt het plaatsbezoek geacht te zijn geweigerd. De inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst kan beroep instellen tegen de weigeringsbeslissing of het gebrek aan een beslissing bij de kamer van inbeschuldigingstelling binnen vijftien dagen na de kennisgeving van de beslissing of het verstrijken van de termijn.

Bezoeken aan bewoonde lokalen zonder toestemming van de bewoner gebeuren tussen vijf en eenentwintig uur door minstens twee leden van de inspectiedienst die samen optreden.

§ 4. Bij het begin van elk verhoor wordt aan de ondervraagde persoon meegedeeld:

1° dat zijn verklaringen voor een rechtbank als bewijs kunnen worden gebruikt;

2° qu'elle peut demander que toutes les questions qui lui sont posées et les réponses qu'elle donne soient actées dans les termes utilisés;

3° qu'elle a le droit de garder le silence et de ne pas contribuer à sa propre incrimination.

Toute personne interrogée peut utiliser les documents en sa possession, sans que cela puisse entraîner le report de l'audition. Elle peut, lors de l'audition ou ultérieurement, exiger que ces documents soient joints à l'audition.

L'audition mentionne avec précision l'heure à laquelle elle a pris cours, est éventuellement interrompue et reprise, et prend fin. Elle mentionne l'identité des personnes qui interviennent lors de l'audition ou lors d'une partie de celle-ci.

À la fin de l'audition, la personne interrogée a le droit de relire celle-ci ou de demander que lecture lui en soit faite. Elle peut demander à ce que ses déclarations soient corrigées ou complétées.

Les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent qui interrogent une personne l'informent qu'elle peut demander une copie du texte de son audition. Cette copie lui est délivrée gratuitement.

§ 5. Les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent peuvent consulter tous les supports d'information et les données qu'ils contiennent. Ils peuvent se faire produire sur place le système informatique et les données qu'il contient dont ils ont besoin pour leurs examens et constatations, et en prendre ou en demander gratuitement des extraits, des duplicatas ou des copies, sous une forme lisible et intelligible qu'ils ont demandée.

S'il n'est pas possible de prendre des copies sur place, les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent peuvent saisir, contre récépissé contenant un inventaire, le système informatique et les données qu'il contient.

§ 6. Pour étendre les recherches dans un système informatique ou une partie de celui-ci, entamées sur la base du paragraphe 5, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée, le service d'inspection de l'autorité nationale de cybersécurité ou

2° dat hij kan vragen dat alle vragen die hem worden gesteld en de antwoorden die hij geeft, worden genoteerd in de gebruikte bewoordingen;

3° dat hij het recht heeft om te zwijgen en niet bij te dragen tot zijn eigen beschuldiging.

Elke ondervraagde persoon mag de documenten in zijn bezit gebruiken, zonder dat daardoor het verhoor uitgesteld wordt. Hij mag tijdens het verhoor of later vragen om die documenten bij het verhoor te voegen.

Het verhoor vermeldt nauwkeurig het tijdstip waarop het wordt aangevat, eventueel onderbroken en hervat, alsook beëindigd. Het vermeldt de identiteit van de personen die tussenkomen tijdens het verhoor of een deel ervan.

Aan het einde van het verhoor heeft de ondervraagde persoon het recht om zijn verhoor te lezen of het te laten voorlezen. Hij mag zijn verklaringen laten verbeteren of er iets aan laten toevoegen.

De leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst die een persoon ondervragen, delen hem mee dat hij een kopie mag vragen van de tekst van zijn verhoor. Deze kopie wordt gratis verstrekt.

§ 5. De leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst mogen alle informatiedragers en de erin opgenomen gegevens raadplegen. Zij mogen zich ter plaatse het informaticasysteem en de erin opgenomen gegevens die zij nodig hebben voor hun onderzoeken en vaststellingen doen voorleggen en er kosteloos uittreksels, duplicaten of kopieën van nemen of vragen in een door hen gevraagde leesbare en verstaanbare vorm.

Indien het niet mogelijk is om ter plaatse kopieën te nemen, mogen de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst, tegen een ontvangstbewijs dat een inventaris bevat, het informaticasysteem en de erin opgenomen gegevens in beslag nemen.

§ 6. Om de zoekactie in een informaticasysteem of een deel hiervan die op basis van paragraaf 5 werd opgestart uit te breiden naar een informaticasysteem of een deel hiervan dat zich op een andere plaats bevindt dan die van de zoekactie, kan de inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele

l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent peut solliciter l'intervention d'un juge d'instruction.

§ 7. Lorsque le service d'inspection de l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent prend connaissance, dans le cadre de la supervision ou de l'exécution, du fait que la violation commise par une entité essentielle ou importante à l'égard des obligations énoncées aux articles 30 et 34 à 37 peut donner lieu à une violation de données à caractère personnel au sens de l'article 4, point 12, du règlement (UE) 2016/679, devant être notifiée en vertu de l'article 33 dudit règlement, ils en informent sans retard injustifié les autorités de protection des données.

Lorsque l'autorité de protection des données compétente est établie dans un autre État membre que la Belgique, le service d'inspection de l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent informe l'autorité de protection des données compétente établie en Belgique de la violation potentielle de données à caractère personnel visée à l'alinéa 1^{er}.

§ 8. Lors de l'exécution de leurs pouvoirs de contrôle visés au présent article, les membres assermentés des autorités visées à l'article 44, § 1^{er}, veillent à ce que les moyens qu'ils utilisent soient appropriés et nécessaires pour ledit contrôle.

Art. 49

§ 1^{er}. Après chaque inspection, les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent rédigent un rapport et en transmettent une copie à l'entité inspectée.

§ 2. L'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle se communiquent mutuellement leur rapport d'inspection.

Art. 50

§ 1^{er}. L'entité supervisée apporte son entière collaboration aux membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent dans l'exercice de leurs fonctions et notamment pour informer ceux-ci au mieux de toutes les mesures de sécurité existantes.

bevoegde sectorale overheid of sectorale inspectiedienst een onderzoeksrechter vragen om op te treden.

§ 7. Wanneer de inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst er bij toezicht of handhaving kennis van krijgen dat de inbreuk door een essentiële of belangrijke entiteit op de in de artikelen 30 en 34 tot 37 vastgestelde verplichtingen een inbreuk in verband met persoonsgegevens zoals gedefinieerd in artikel 4, punt 12, van Verordening (EU) 2016/679 kan inhouden, die op grond van artikel 33 van die verordening moet worden gemeld, stellen zij de gegevensbeschermingsautoriteiten daarvan onverwijld in kennis.

Wanneer de bevoegde gegevensbeschermingsautoriteit in een andere lidstaat dan België gevestigd is, stelt de inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst de in België gevestigde bevoegde gegevensbeschermingsautoriteit in kennis van de in het eerste lid bedoelde potentiële inbreuk in verband met persoonsgegevens.

§ 8. Bij de uitvoering van hun toezichtsbevoegdheden bedoeld in dit artikel zorgen de beëdigde leden van de autoriteiten bedoeld in artikel 44, § 1, ervoor dat de door hen gebruikte middelen passend en noodzakelijk zijn voor dit toezicht.

Art. 49

§ 1. Na elke inspectie stellen de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst een verslag op en bezorgen ze daarvan een kopie aan de geïnspecteerde entiteit.

§ 2. De nationale cyberbeveiligingsautoriteit en de eventuele sectorale overheid wisselen hun inspectieverslagen uit.

Art. 50

§ 1. De entiteit waarop toezicht wordt uitgeoefend, verleent haar volledige medewerking aan de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst bij de uitoefening van hun functie en met name om deze zo goed mogelijk te informeren over alle bestaande beveiligingsmaatregelen.

Si nécessaire, l'entité met à disposition des membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent le matériel nécessaire de manière à ce qu'ils remplissent les consignes de sécurité lors des inspections.

§ 2. Les coûts des inspections ne sont pas mis à charge des entités.

Par dérogation à l'alinéa précédent, le Roi peut déterminer, par secteur ou sous-secteur, par arrêté délibéré en Conseil des ministres et après avis de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle concernée, des rétributions relatives aux prestations d'inspections. Il en fixe les modalités de calcul et de paiement.

§ 3. Le fait pour quiconque d'empêcher ou d'entraver volontairement l'exécution d'un contrôle effectué par les membres du service d'inspection de l'autorité nationale de cybersécurité ou de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent, de refuser de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle, ou de communiquer sciemment des informations inexacts ou incomplètes est constaté dans un procès-verbal par les membres assermentés du service d'inspection de l'autorité nationale de cybersécurité ou de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent.

CHAPITRE 2

Les mesures et amendes administratives

Section 1^{re}

Procédure

Art. 51

§ 1^{er}. Lorsqu'un ou plusieurs manquements aux exigences imposées par la présente loi, ses arrêtés d'exécution ou les décisions administratives individuelles y afférentes sont observés, les faits peuvent être constatés dans un procès-verbal rédigé par les membres assermentés du service d'inspection de l'autorité nationale de cybersécurité, de l'éventuel service d'inspection sectoriel ou de l'éventuelle autorité sectorielle concernée, conformément à l'article 44, § 1^{er}

Moyennant l'accord de l'autorité nationale de cybersécurité, l'autorité sectorielle peut imposer à une entité

Indien nodig stelt de entiteit het nodige materiaal ter beschikking van de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst, zodat ze de veiligheidsvoorschriften kunnen naleven tijdens de inspecties.

§ 2. De kosten van de inspecties zijn niet ten laste van de entiteiten.

In afwijking van het vorige lid kan de Koning, voor elke sector of deelsector, bij besluit vastgesteld na overleg in de Ministerraad en na advies van de nationale cyberbeveiligingsautoriteit en van de eventuele betrokken sectorale overheid, retributies bepalen voor de inspectieprestaties. De Koning bepaalt de berekenings- en betalingsregels.

§ 3. Het feit dat iemand de uitvoering van een controle door de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst opzettelijk verhindert of belemmert, de informatie die hem gevraagd wordt naar aanleiding van deze controle weigert mee te delen, of bewust foutieve of onvolledige informatie verstrekt, wordt opgetekend in een proces-verbaal door de beëdigde leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst.

HOOFDSTUK 2

De administratieve maatregelen en geldboetes

Afdeling 1

Procedure

Art. 51

§ 1. Wanneer een of meer inbreuken op de eisen van deze wet, de uitvoeringsbesluiten ervan of de eraan verbonden individuele administratieve beslissingen worden vastgesteld, kunnen de feiten opgetekend worden in een proces-verbaal door de beëdigde leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit, van de eventuele sectorale inspectiedienst of van de eventuele betrokken sectorale overheid, overeenkomstig artikel 44, § 1.

Mits de nationale cyberbeveiligingsautoriteit akkoord gaat, kan de sectorale overheid administratieve

des mesures et amendes administratives visées à la section 2.

L'autorité nationale de cybersécurité informe l'autorité sectorielle concernée lorsqu'elle a l'intention d'imposer à une entité des mesures et amendes administratives visées aux articles 58 et 59.

Lorsque les autorités visées aux alinéas 1^{er} et 2 prennent connaissance, dans le cadre de leur mission de supervision, du fait qu'un manquement visé à l'alinéa 1^{er} ou 2, commis par une entité essentielle ou importante, peut donner lieu à une violation de données à caractère personnel au sens de l'article 4, 12), du règlement (UE) 2016/679, devant être notifiée en vertu de l'article 33 dudit règlement, elles en informent sans retard injustifié les autorités de protection des données compétentes.

§ 2. Sur la base du procès-verbal visé au paragraphe 1^{er} et, le cas échéant, des rapports pertinents visés à l'article 49, § 1^{er}, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente peut rédiger un projet de décision contenant au moins les références du procès-verbal qui constate l'infraction et qui relate les faits à propos desquels la procédure est entamée et une ou plusieurs mesures ou amendes administratives visées à l'article 58 et/ou 59 envisagées ainsi que le délai endéans lequel l'entité concernée exécuterait les mesures administratives.

Le délai visé à l'alinéa 1^{er} est déterminé en tenant compte des conditions de fonctionnement de l'entité et des mesures à mettre en œuvre.

§ 3. L'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente envoie le projet de décision visé au paragraphe 2 à l'entité concernée en exposant, en détail, les motifs relatifs aux mesures et/ou amendes administratives envisagées et lui fait part de son droit, dans les trente jours de la réception de cette information, de formuler par écrit ses moyens de défense ou de solliciter d'être d'entendu. L'information est présumée reçue par le contrevenant le sixième jour suivant l'envoi du projet de décision précité.

Par exception à l'alinéa 1^{er}, le projet de décision n'est pas envoyé au préalable à l'entité concernée dans des cas exceptionnels, dûment motivés, où cela entraverait une intervention immédiate pour prévenir un incident ou y répondre.

§ 4. Après que l'entité concernée a pu faire valoir ses moyens de défense, à la fin du délai visé au paragraphe 3,

maatregelen en geldboetes als bedoeld in afdeling 2 opleggen aan een entiteit.

De nationale cyberbeveiligingsautoriteit informeert de betrokken sectorale overheid wanneer zij overweegt om administratieve maatregelen en geldboetes als bedoeld in artikelen 58 en 59 op te leggen aan een entiteit.

Wanneer de autoriteiten bedoeld in het eerste en tweede lid er tijdens hun toezichtsovereenkomst kennis van krijgen dat een in het eerste of tweede lid bedoelde inbreuk door een essentiële of belangrijke entiteit een inbreuk in verband met persoonsgegevens zoals gedefinieerd in artikel 4, 12), van Verordening (EU) 2016/679 kan inhouden, die op grond van artikel 33 van die verordening moet worden gemeld, stellen zij de bevoegde gegevensbeschermingsautoriteiten daarvan onverwijld in kennis.

§ 2. Op basis van het in paragraaf 1 bedoelde proces-verbaal en, in voorkomend geval, van de relevante verslagen bedoeld in artikel 49, § 1, kan de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid een ontwerp van beslissing opstellen dat minstens de referenties van het proces-verbaal dat de inbreuk vaststelt en de feiten beschrijft die aanleiding hebben gegeven tot de procedure, en een of meer overwogen administratieve maatregelen of geldboetes als bedoeld in artikel 58 en/of 59 bevat, alsook de termijn waarbinnen de betrokken entiteit de administratieve maatregelen zou uitvoeren.

De in het eerste lid bedoelde termijn wordt bepaald rekening houdend met de werkingsomstandigheden van de entiteit en de te nemen maatregelen.

§ 3. De nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid verstuurt het in paragraaf 2 bedoelde ontwerp van beslissing naar de betrokken entiteit, met een gedetailleerde motivering voor de overwogen administratieve maatregelen en/of geldboetes, en laat haar weten dat zij het recht heeft om, binnen dertig dagen na ontvangst van deze informatie, haar verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. De informatie wordt geacht te zijn ontvangen door de overtreder de zesde dag na de verzending van voormeld ontwerp van beslissing.

In afwijking van het eerste lid wordt het ontwerp van beslissing niet vooraf naar de betrokken entiteit gestuurd in naar behoren gemotiveerde uitzonderlijke gevallen waarin een onmiddellijk optreden om een incident te voorkomen of erop te reageren anders zou worden belemmerd.

§ 4. Nadat de betrokken entiteit haar verweermiddelen heeft kunnen aanvoeren, op het einde van de termijn

alinéa 1^{er}, ou dans le cas visé au paragraphe 3, alinéa 2, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente maintient ou modifie le projet de décision visé au paragraphe 2, alinéa 1^{er} ou y renonce, en tenant compte de la catégorie d'entité à laquelle appartient l'entité concernée, des moyens de défense de cette dernière et des éléments visés à l'article 54.

Art. 52

§ 1^{er}. Lorsque les mesures d'exécution adoptées en vertu de l'article 58, 1^o à 4^o, et 6^o, sont inefficaces, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente peut fixer un délai dans lequel une entité essentielle est invitée à prendre les mesures nécessaires pour pallier les insuffisances ou satisfaire à ses exigences.

§ 2. Lorsqu'une entité essentielle ne se conforme pas à la ou aux mesures contenues dans la décision visée à l'article 51, § 4, l'autorité qui a pris cette décision constate les faits dans un procès-verbal.

§ 3. Sur la base du procès-verbal visé au paragraphe 2, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente rédige un projet de décision contenant au moins une ou plusieurs mesures ou amendes administratives visées aux articles 59 et/ou 60 envisagées.

§ 4. L'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente envoie le projet de décision visé au paragraphe 3 à l'entité concernée en exposant, en détail, les motifs relatifs aux mesures et/ou amendes administratives envisagées et lui fait part de son droit, dans les trente jours de la réception de cette information, de formuler par écrit ses moyens de défense ou de solliciter d'être entendu. L'information est présumée reçue par le contrevenant le sixième jour suivant l'envoi du projet de décision précité.

Par exception à l'alinéa 1^{er}, le projet de décision n'est pas envoyé au préalable à l'entité concernée dans des cas exceptionnels, dûment motivés, où cela entraverait une intervention immédiate pour prévenir un incident ou y répondre.

§ 5. Après que l'entité concernée ait pu faire valoir ses moyens de défense, à la fin du délai visé au paragraphe 4, alinéa 1^{er}, ou dans le cas visé au paragraphe 4, alinéa 2, l'autorité nationale de cybersécurité ou l'éventuelle autorité

bedoeld in paragraaf 3, eerste lid, of in het geval bedoeld in paragraaf 3, tweede lid, zal de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid het ontwerp van beslissing bedoeld in paragraaf 2, eerste lid, handhaven, wijzigen of ervan afzien, rekening houdend met de entiteitscategorie waartoe de betrokken entiteit behoort, de verweermiddelen van deze laatste en de in artikel 54 bedoelde elementen.

Art. 52

§ 1. Indien de op grond van artikel 58, 1^o tot 4^o, en 6^o, genomen handhavingsmaatregelen ondoeltreffend zijn, kan de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid een termijn vaststellen waarbinnen een essentiële entiteit wordt verzocht de noodzakelijke maatregelen te nemen om de tekortkomingen te verhelpen of aan haar eisen te voldoen.

§ 2. Indien een essentiële entiteit geen gevolg geeft aan de maatregel(en) vermeld in de beslissing bedoeld in artikel 51, § 4, stelt de autoriteit die deze beslissing heeft genomen de feiten vast in een proces-verbaal.

§ 3. Op basis van het in paragraaf 2 bedoelde proces-verbaal stelt de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid een ontwerp van beslissing op dat minstens een of meer overwogen administratieve maatregelen of geldboetes als bedoeld in de artikelen 59 en/of 60 bevat.

§ 4. De nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid verstuurt het in paragraaf 3 bedoelde ontwerp van beslissing naar de betrokken entiteit, met een gedetailleerde motivering voor de overwogen administratieve maatregelen en/of geldboetes, en laat haar weten dat zij het recht heeft om, binnen dertig dagen na ontvangst van deze informatie, haar verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. De informatie wordt geacht te zijn ontvangen door de overtreder de zesde dag na de verzending van voormeld ontwerp van beslissing.

In afwijking van het eerste lid wordt het ontwerp van beslissing niet vooraf naar de betrokken entiteit gestuurd in naar behoren gemotiveerde uitzonderlijke gevallen waarin een onmiddellijk optreden om een incident te voorkomen of erop te reageren anders zou worden belemmerd.

§ 5. Nadat de betrokken entiteit haar verweermiddelen heeft kunnen aanvoeren, op het einde van de termijn bedoeld in paragraaf 4, eerste lid, of in het geval bedoeld in paragraaf 4, tweede lid, zal de nationale

sectorielle compétente maintient ou modifie le projet de décision visé au paragraphe 3 ou y renonce en tenant compte des moyens de défense de l'entité concernée et des éléments visés à l'article 54.

Art. 53

Les procès-verbaux rédigés par les membres assermentés du service d'inspection font foi jusqu'à preuve du contraire.

Art. 54

§ 1^{er}. Lorsqu'elle prend toute mesure d'exécution dans le cadre des procédures visées aux articles 51 et 52, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente respecte les droits de la défense, tient compte des circonstances propres à chaque cas et, au minimum, tient dûment compte:

1° de la catégorie visée aux articles 9 et 10 à laquelle l'entité concernée appartient;

2° de la gravité de la violation et de l'importance des dispositions enfreintes, les faits suivants, entre autres, devant être considérés en tout état de cause comme graves:

- a) les violations répétées;
- b) le fait de ne pas notifier des incidents significatifs ou de ne pas y remédier;
- c) le fait de ne pas pallier les insuffisances à la suite d'instructions contraignantes des autorités compétentes;
- d) le fait d'entraver des audits ou des activités de contrôle ordonnées par le service d'inspection de l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent à la suite de la constatation d'une violation;
- e) la fourniture d'informations fausses ou manifestement inexactes relatives aux mesures de gestion des risques en matière de cybersécurité ou aux notifications d'incidents prévues au titre 3;

3° de la durée de la violation;

cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid het in paragraaf 3 bedoelde ontwerp van beslissing handhaven, wijzigen of ervan afzien, rekening houdend met de verweermiddelen van de betrokken entiteit en de in artikel 54 bedoelde elementen.

Art. 53

De processen-verbaal van de beëdigde leden van de inspectiedienst hebben bewijskracht tot het tegendeel is bewezen.

Art. 54

§ 1. Bij het nemen van handhavingsmaatregelen in het kader van de in de artikelen 51 en 52 bedoelde procedures eerbiedigt de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid de rechten van de verdediging, houdt zij rekening met de omstandigheden van elk afzonderlijk geval en houdt zij ten minste naar behoren rekening met:

1° de in de artikelen 9 en 10 bedoelde categorie waartoe de betrokken entiteit behoort;

2° de ernst van de inbreuk en het belang van de geschonden bepalingen, waarbij onder meer het volgende in ieder geval een ernstige inbreuk vormt:

- a) herhaalde inbreuken;
- b) het niet melden of niet verhelpen van significante incidenten;
- c) het niet verhelpen van tekortkomingen naar aanleiding van bindende aanwijzingen van de bevoegde autoriteiten;
- d) het belemmeren van audits of monitoringsactiviteiten waartoe de inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst opdracht heeft gegeven naar aanleiding van de vaststelling van een inbreuk;
- e) het verstrekken van valse of heel onnauwkeurige informatie met betrekking tot de maatregelen voor het beheer van cyberbeveiligingsrisico's of de in titel 3 bedoelde melding van incidenten;

3° de duur van de inbreuk;

4° de toute violation antérieure pertinente commise par l'entité concernée;

5° des dommages matériels, corporels ou moraux causés, y compris des pertes financières ou économiques, des effets sur d'autres services et du nombre d'utilisateurs touchés;

6° du fait que l'auteur de la violation a agi délibérément ou par négligence;

7° des mesures prises par l'entité pour prévenir ou atténuer les dommages matériels, corporels ou moraux;

8° de l'application de codes de conduite approuvés ou de mécanismes de certification approuvés;

9° du degré de coopération avec le service d'inspection de l'autorité nationale de cybersécurité ou avec l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent des personnes physiques ou morales tenues pour responsables.

§ 2. Lorsque les autorités de protection des données imposent une amende administrative en vertu de l'article 58, paragraphe 2, point i), du règlement (UE) 2016/679, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente n'impose pas d'amende administrative pour une violation découlant du même comportement que celui qui a fait l'objet d'une amende administrative au titre de l'article 58, paragraphe 2, point i), dudit règlement.

Art. 55

§ 1^{er}. Les décisions visées aux articles 51 et 52 sont notifiées par envoi recommandé au contrevenant.

§ 2. Les amendes administratives imposées par une décision visée à l'article 51 ou 52 doivent être acquittées dans les soixante jours qui suivent la réception de l'envoi recommandé visé au paragraphe 1^{er}.

Ce délai peut être augmenté en fonction du montant de l'amende administrative.

Le délai visé à l'alinéa 1^{er} est réputé commencer au plus tard six jours après l'envoi recommandé visé au paragraphe 1^{er}.

§ 3. Lorsqu'une décision visée à l'article 51 ou 52 impose une mesure administrative autre qu'une amende

4° eventuele relevante eerdere inbreuken door de betrokken entiteit;

5° elke veroorzaakte materiële of immateriële schade, met inbegrip van elke financiële of economische schade, gevolgen voor andere diensten en het aantal getroffen gebruikers;

6° opzet of nalatigheid van de pleger van de inbreuk;

7° door de entiteit genomen maatregelen om de materiële of immateriële schade te voorkomen of te beperken;

8° de naleving van goedgekeurde gedragscodes of goedgekeurde certificeringsmechanismen;

9° de mate waarin de aansprakelijk gestelde natuurlijke of rechtspersonen meewerken met de inspectiedienst van de nationale cyberbeveiligingsautoriteit of met de eventuele bevoegde sectorale overheid of sectorale inspectiedienst.

§ 2. Indien de gegevensbeschermingsautoriteiten een administratieve geldboete opleggen op grond van artikel 58, lid 2, punt i), van Verordening (EU) 2016/679, legt de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid geen geldboete op voor een inbreuk die voortvloeit uit dezelfde gedraging als die waarvoor een administratieve geldboete uit hoofde van artikel 58, lid 2, punt i), van die verordening is opgelegd.

Art. 55

§ 1. De in de artikelen 51 en 52 bedoelde beslissingen worden bij aangetekende zending ter kennis gebracht van de overtreder.

§ 2. De geldboetes die worden opgelegd door een in artikel 51 of 52 bedoelde beslissing, moeten worden betaald binnen de zestig dagen na ontvangst van de in paragraaf 1 bedoelde aangetekende zending.

Deze termijn kan verlengd worden in functie van het bedrag van de geldboete.

De in het eerste lid bedoelde termijn wordt geacht in te gaan uiterlijk zes dagen na de in paragraaf 1 bedoelde aangetekende zending.

§ 3. Wanneer een in artikel 51 of 52 bedoelde beslissing een andere administratieve maatregel dan

administrative, cette décision précise le délai endéans lequel la mesure doit être exécutée.

§ 4. L'autorité nationale de cybersécurité et, le cas échéant, l'éventuelle autorité sectorielle se communiquent mutuellement leur décision visée à l'article 51 ou 52.

Art. 56

§ 1^{er}. Lorsque l'entité concernée reste en défaut de payer l'amende administrative dans le délai imparti, la décision d'infliger une amende administrative a force exécutoire et l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente peut décerner une contrainte.

La contrainte est décernée par un représentant légal de l'autorité nationale de cybersécurité ou de l'éventuelle autorité sectorielle compétente ou par un membre du personnel habilité à cette fin.

§ 2. La contrainte est signifiée au contrevenant par exploit d'huissier de justice. La signification contient un commandement de payer dans les quarante-huit heures, à peine d'exécution par voie de saisie, de même qu'une justification comptable des sommes exigées ainsi que copie de l'exécutoire.

§ 3. Le contrevenant peut former opposition à la contrainte devant le juge des saisies.

L'opposition est motivée à peine de nullité. Elle est formée au moyen d'une citation de l'autorité nationale de cybersécurité ou de l'éventuelle autorité sectorielle compétente signifiée par exploit d'huissier dans les quinze jours à partir de la signification de la contrainte.

Les dispositions du chapitre VIII de la première partie du Code judiciaire sont applicables à ce délai, y compris les prorogations prévues à l'article 50, alinéa 2, et à l'article 55 de ce Code.

L'exercice de l'opposition à la contrainte suspend l'exécution de celle-ci, ainsi que la prescription des créances contenues dans la contrainte, jusqu'à ce qu'il ait été statué sur son bien-fondé. Les saisies déjà pratiquées antérieurement conservent leur caractère conservatoire.

§ 4. L'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente peut faire pratiquer la saisie conservatoire et exécuter la contrainte en usant

een administratieve geldboete oplegt, vermeldt deze beslissing de termijn waarbinnen de maatregel moet worden uitgevoerd.

§ 4. De nationale cyberbeveiligingsautoriteit en, desgevallend, de eventuele sectorale overheid wisselen hun in artikel 51 of 52 bedoelde beslissing uit.

Art. 56

§ 1. Als de betrokken entiteit de administratieve geldboete niet betaalt binnen de gestelde termijn, is de beslissing om een administratieve geldboete op te leggen uitvoerbaar en kan de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid een dwangbevel uitvaardigen.

Het dwangbevel wordt uitgevaardigd door een wettelijke vertegenwoordiger van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of door een daartoe gemachtigd personeelslid.

§ 2. Het dwangbevel wordt aan de overtreder bij gerechtsdeurwaarderexploot betekend. De betekening bevat een bevel om te betalen binnen achtenveertig uur op straffe van tenuitvoerlegging door beslag, alsook een boekhoudkundige verantwoording van de gevorderde bedragen en een afschrift van de uitvoerbaarverklaring.

§ 3. De overtreder kan tegen het dwangbevel verzet aantekenen bij de beslagrechter.

Het verzet is, op straffe van nietigheid, met redenen omkleed. Het moet worden ingediend door middel van een dagvaarding van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid bij deurwaardersexploot binnen vijftien dagen te rekenen vanaf de betekening van het dwangbevel.

De bepalingen van hoofdstuk VIII van het eerste deel van het Gerechtelijk Wetboek zijn van toepassing op deze termijn, met inbegrip van de verlengingen bepaald in artikel 50, tweede lid, en artikel 55 van dit Wetboek.

De uitoefening van verzet tegen het dwangbevel schorst de tenuitvoerlegging hiervan, alsook de verjaring van de schuldvorderingen opgenomen in het dwangbevel, tot uitspraak is gedaan over de gegrondheid ervan. De reeds eerder gelegde beslagen behouden hun bewarend karakter.

§ 4. De nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid mag bewarend beslag laten leggen en het dwangbevel uitvoeren met

des voies d'exécution prévues à la cinquième partie du Code judiciaire.

Les paiements partiels effectués en suite de la signification d'une contrainte ne font pas obstacle à la continuation des poursuites.

§ 5. Les frais de signification de la contrainte de même que les frais de l'exécution ou des mesures conservatoires sont à charge du contrevenant.

Ils sont déterminés suivant les règles établies pour les actes accomplis par les huissiers de justice en matière civile et commerciale.

Art. 57

Les faits sont prescrits trois ans après leur commission. La prescription n'est interrompue que par des actes d'enquête ou de poursuite par un service d'inspection. Ces actes font courir un nouveau délai d'égale durée, même à l'égard des personnes qui n'y sont pas impliquées.

Les mesures administratives ou les amendes administratives sont prescrites cinq ans à compter de la date à laquelle elles doivent être exécutées. Le délai de prescription est suspendu en cas d'un recours contre la décision administrative.

Section 2

Mesures et amendes administratives

Art. 58

Les mesures administratives suivantes peuvent être imposées aux entités sur la base de l'article 51:

1° émettre des avertissements concernant les violations de la présente loi par les entités concernées;

2° adopter des instructions contraignantes ou une injonction exigeant des entités concernées qu'elles remédient aux insuffisances constatées ou aux violations de la présente loi;

3° ordonner aux entités concernées de mettre un terme à un comportement qui viole la présente loi et de ne pas le réitérer;

4° ordonner aux entités concernées de garantir la conformité de leurs mesures de gestion des risques en matière de cybersécurité avec le titre 3 ou de respecter les obligations en matière de notification d'incidents

gebruikmaking van de middelen tot tenuitvoerlegging bepaald in het vijfde deel van het Gerechtelijk Wetboek.

De gedeeltelijke betalingen gedaan ingevolge de betekening van een dwangbevel verhinderen de voortzetting van de vervolging niet.

§ 5. De betekeningskosten van het dwangbevel evenals de kosten van tenuitvoerlegging of van bewarende maatregelen zijn ten laste van de overtreder.

Ze worden bepaald volgens de regels die gelden voor de akten van gerechtsdeurwaarders in burgerlijke zaken en handelszaken.

Art. 57

De feiten zijn drie jaar na het plegen verjaard. De verjaring wordt alleen gestuit door onderzoekshandelingen of door de vervolging een inspectiedienst. Deze handelingen doen een nieuwe periode van gelijke duur lopen, zelfs ten aanzien van personen die niet betrokken zijn.

De administratieve maatregelen of geldboetes verjaren vijf jaar na de datum waarop ze ten uitvoer moeten worden gelegd. De verjaringstermijn wordt geschorst in geval van beroep tegen de administratieve beslissing.

Afdeling 2

Administratieve maatregelen en geldboetes

Art. 58

De volgende administratieve maatregelen kunnen aan entiteiten worden opgelegd op basis van artikel 51:

1° waarschuwingen geven over inbreuken door de betrokken entiteiten op deze wet;

2° bindende aanwijzingen vaststellen of een bevel uitvaardigen waarin de betrokken entiteiten worden verplicht de vastgestelde tekortkomingen of de inbreuken op deze wet te verhelpen;

3° de betrokken entiteiten gelasten een einde te maken aan gedragingen die inbreuk maken op deze wet en af te zien van herhaling van die gedragingen;

4° de betrokken entiteiten gelasten er op een gespecificeerde wijze en binnen een gespecificeerde termijn voor te zorgen dat hun maatregelen voor het beheer van cyberbeveiligingsrisico's in overeenstemming zijn met

énoncées au même titre, de manière spécifique et dans un délai déterminé;

5° ordonner aux entités concernées d'informer les personnes physiques ou morales à l'égard desquelles elles fournissent des services ou exercent des activités susceptibles d'être affectées par une cybermenace importante de la nature de la menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace;

6° ordonner aux entités concernées de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable;

7° ordonner aux entités concernées de rendre publics les aspects de violations de la présente loi de manière spécifique;

8° lorsque l'entité concernée est une entité essentielle, désigner, pour une période déterminée, un responsable du contrôle ayant des tâches bien définies pour superviser le respect, par les entités concernées, des mesures de gestion des risques en matière de cybersécurité et de notification d'incidents visées au titre 3.

Lorsque l'entité concernée est une entité essentielle, les instructions contraignantes visées à l'alinéa 1^{er}, 2°, concernent également les mesures nécessaires pour éviter un incident ou y remédier, ainsi que les délais pour mettre en œuvre ces mesures et rendre compte de cette mise en œuvre.

Art. 59

Les amendes administratives suivantes peuvent être imposées aux entités sur la base de l'article 51 ou 52:

1° est puni d'une amende de 500 à 125.000 euros quiconque ne se conforme pas aux obligations d'information visées à l'article 12;

2° est punie d'une amende de 500 à 200.000 euros l'entité qui fait subir des conséquences négatives à une personne agissant pour son compte en raison de l'exécution, de bonne foi et dans le cadre de ses fonctions, des obligations découlant de la présente loi;

3° sans préjudice de l'article 48, § 4, alinéa 1^{er}, 3°, est puni d'une amende de 500 à 200.000 euros quiconque ne se conforme pas aux obligations de contrôle visées au présent titre;

titel 3 of te voldoen aan de verplichtingen inzake het melden van incidenten bedoeld in dezelfde titel;

5° de betrokken entiteiten gelasten de natuurlijke of rechtspersonen aan wie zij diensten verlenen of voor wie zij activiteiten uitvoeren die mogelijkerwijs door een significante cyberdreiging worden beïnvloed, in kennis te stellen van de aard van de dreiging en van alle mogelijke beschermings- of herstelmaatregelen die deze natuurlijke of rechtspersonen kunnen nemen als reactie op die dreiging;

6° de betrokken entiteiten gelasten de naar aanleiding van een beveiligingsaudit gedane aanbevelingen binnen een redelijke termijn uit te voeren;

7° de betrokken entiteiten gelasten aspecten van inbreuken op deze wet op een bepaalde manier openbaar te maken;

8° wanneer de betrokken entiteit een essentiële entiteit is, een controlefunctionaris aanwijzen die gedurende een bepaalde periode duidelijk omschreven taken heeft om erop toe te zien dat de betrokken entiteiten voldoen aan de maatregelen voor het beheer van cyberbeveiligingsrisico's en inzake het melden van incidenten bedoeld in titel 3.

Wanneer de betrokken entiteit een essentiële entiteit is, omvatten de bindende aanwijzingen bedoeld in het eerste lid, 2°, ook de maatregelen die nodig zijn om een incident te voorkomen of te verhelpen, alsmede uiterste termijnen voor de uitvoering van dergelijke maatregelen en voor verslaggeving over de uitvoering ervan.

Art. 59

De volgende administratieve geldboetes kunnen aan entiteiten worden opgelegd op basis van artikel 51 of 52:

1° eenieder die niet voldoet aan de in artikel 12 bedoelde rapportageverplichtingen wordt bestraft met een geldboete van 500 tot 125.000 euro;

2° een entiteit die een persoon die optreedt voor haar rekening nadelige gevolgen berokkent ingevolge de uitvoering, te goeder trouw en in het kader van zijn functie, van de verplichtingen die voortvloeien uit deze wet, wordt bestraft met een geldboete van 500 tot 200.000 euro;

3° onverminderd artikel 48, § 4, eerste lid, 3°, eenieder die niet voldoet aan de in deze titel bedoelde toezichtverplichtingen wordt bestraft met een geldboete van 500 tot 200.000 euro;

4° est punie d'une amende de 500 à 7.000.000 d'euros ou 1,4 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu, l'entité importante qui ne se conforme pas aux obligations relatives aux mesures de gestion des risques en matière de cybersécurité et/ou de notification d'incidents visées au titre 3;

5° est punie d'une amende de 500 à 10.000.000 d'euros ou 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu, l'entité essentielle qui ne se conforme pas aux obligations relatives aux mesures de gestion des risques en matière de cybersécurité et/ou de notification d'incidents visées au titre 3.

L'amende administrative est doublée en cas de récidive pour les mêmes faits dans un délai de trois ans.

Le concours de plusieurs manquements peut donner lieu à une amende administrative unique proportionnelle à la gravité de l'ensemble des faits.

Art. 60

Si les mesures demandées ne sont pas prises dans le délai imparti, les mesures administratives suivantes peuvent être imposées aux entités essentielles sur la base de l'article 52:

1° demander à l'autorité nationale de cybersécurité de suspendre temporairement une certification ou une autorisation concernant tout ou partie des services pertinents fournis ou des activités pertinentes menées par l'entité concernée;

2° interdire temporairement à toute personne physique exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal dans l'entité concernée d'exercer des responsabilités dirigeantes dans cette entité.

Les suspensions ou interdictions temporaires visées à l'alinéa 1^{er} sont uniquement appliquées jusqu'à ce que l'entité concernée ait pris les mesures nécessaires pour remédier aux insuffisances ou se conformer aux exigences de l'autorité compétente à l'origine de l'application de ces mesures d'exécution.

4° een belangrijke entiteit die niet voldoet aan de verplichtingen betreffende de maatregelen voor het beheer van cyberbeveiligingsrisico's en/of aan de rapportageverplichtingen bedoeld in titel 3, wordt bestraft met een geldboete van 500 tot 7.000.000 euro of van 1,4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de belangrijke entiteit behoort, afhankelijk van welk bedrag het hoogst is;

5° een essentiële entiteit die niet voldoet aan de verplichtingen betreffende de maatregelen voor het beheer van cyberbeveiligingsrisico's en/of aan de rapportageverplichtingen bedoeld in titel 3, wordt bestraft met een geldboete van 500 tot 10.000.000 euro of van 2 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de essentiële entiteit behoort, afhankelijk van welk bedrag het hoogst is.

De administratieve geldboete wordt verdubbeld in geval van herhaling van dezelfde feiten binnen een termijn van drie jaar.

De samenloop van meerdere inbreuken kan aanleiding geven tot één enkele administratieve geldboete die in verhouding staat tot de ernst van het geheel van de feiten.

Art. 60

Indien de gevraagde acties niet binnen de gestelde termijn worden ondernomen, kunnen aan essentiële entiteiten op grond van artikel 52 de volgende administratieve maatregelen worden opgelegd:

1° de nationale cyberbeveiligingsautoriteit verzoeken een certificering of vergunning tijdelijk op te schorten met betrekking tot alle of een deel van de relevante door de betrokken entiteit verleende diensten of verrichte activiteiten;

2° een natuurlijke persoon met leidinggevende verantwoordelijkheden op het niveau van de algemeen directeur of de wettelijke vertegenwoordiger in de betrokken entiteit tijdelijk verbieden leidinggevende functies in die entiteit uit te oefenen.

De in het eerste lid bedoelde tijdelijke opschortingen of verboden worden slechts toegepast tot de betrokken entiteit de maatregelen heeft genomen die nodig zijn om de tekortkomingen te verhelpen of te voldoen aan de vereisten van de bevoegde autoriteit die deze handavingsmaatregelen heeft opgelegd.

Art. 61

Toute personne physique responsable d'une entité essentielle ou importante ou agissant en qualité de représentant légal d'une entité essentielle ou importante sur la base du pouvoir de la représenter, de prendre des décisions en son nom ou d'exercer son contrôle a le pouvoir de veiller au respect, par l'entité, de la présente loi. Ces personnes sont responsables des manquements à leur devoir de veiller au respect de la présente loi.

Cet article est sans préjudice des règles en matière de responsabilité applicables aux institutions publiques, ainsi que de responsabilité des agents de la fonction publique et des responsables élus ou nommés.

TITRE 5

*Dispositions spécifiques
au secteur de l'administration publique*

Art. 62

Les mesures et amendes administratives visées aux articles 59 et 60 ne s'appliquent pas aux entités faisant partie du secteur de l'administration publique.

Art. 63

§ 1^{er}. Le Roi est habilité à désigner une autorité comme organisme d'évaluation de la conformité de tout ou partie des entités de l'administration publique.

§ 2. L'autorité visée au paragraphe 1^{er} est agréée par l'autorité nationale de cybersécurité, selon les modalités fixées par le Roi, afin d'effectuer l'évaluation périodique de la conformité visée à l'article 39, alinéa 1^{er}, 1^o.

L'agrément visée à l'alinéa 1^{er} porte sur un ou plusieurs des cadres de référence visés à l'article 39.

Art. 64

Le service d'inspection de l'autorité nationale de cybersécurité ou, le cas échéant, le service d'inspection sectoriel désigné par le Roi pour le secteur de l'administration publique exerce ses tâches de supervision en jouissant d'une indépendance opérationnelle vis-à-vis des entités de l'administration publique supervisées.

Art. 61

Elke natuurlijke persoon die verantwoordelijk is voor of optreedt als wettelijke vertegenwoordiger van een essentiële of een belangrijke entiteit op basis van de bevoegdheid om deze te vertegenwoordigen, de bevoegdheid om namens deze entiteit beslissingen te nemen of de bevoegdheid om controle uit te oefenen op deze entiteit, heeft de bevoegdheid om ervoor te zorgen dat deze entiteit deze wet nakomt. Deze personen zijn aansprakelijk voor het niet nakomen van hun verplichtingen om te zorgen voor de naleving van deze wet.

Dit artikel doet geen afbreuk aan de aansprakelijkheidsregels die gelden voor overheidsinstanties, alsook voor ambtenaren en verkozen of benoemde mandatarissen.

TITEL 5

*Specifieke bepalingen
voor de overheidssector*

Art. 62

De administratieve maatregelen en geldboetes bedoeld in de artikelen 59 en 60 zijn niet van toepassing op entiteiten die deel uitmaken van de overheidssector.

Art. 63

§ 1. De Koning wordt gemachtigd een autoriteit aan te wijzen als conformiteitsbeoordelingsinstantie voor alle of een deel van de overheidsinstanties.

§ 2. De in paragraaf 1 bedoelde autoriteit wordt erkend door de nationale cyberbeveiligingsautoriteit, volgens de door de Koning bepaalde modaliteiten, om de in artikel 39, eerste lid, 1^o, bedoelde regelmatige conformiteitsbeoordeling uit te voeren.

De in het eerste lid bedoelde erkenning heeft betrekking op een of meer van de in artikel 39 bedoelde referentiekaders.

Art. 64

De inspectiedienst van de nationale cyberbeveiligingsautoriteit of, in voorkomend geval, de sectorale inspectiedienst die door de Koning is aangewezen voor de overheidssector, is bij de uitvoering van zijn toezichthoudende taken operationeel onafhankelijk van de overheidsinstanties waarop hij toezicht houdt.

Art. 65

L'article 47 est applicable au service d'inspection visé à l'article 64.

TITRE 6

*Traitement des données à caractère personnel*CHAPITRE 1^{ER}**Principes relatifs au traitement**

Art. 66

Les définitions du règlement (UE) 2016/679 sont d'application pour le présent titre.

Art. 67

Les finalités pour lesquelles des traitements de données à caractère personnel sont effectués, sont les suivantes:

1° l'amélioration de la cybersécurité à travers la recherche d'un niveau accru de protection des réseaux et systèmes d'information, le renforcement des politiques de prévention et de sécurité, la prévention des incidents de sécurité et la défense contre les cybermenaces;

2° l'exécution des tâches de l'autorité nationale de cybersécurité, notamment l'identification des entités, l'information et la sensibilisation des utilisateurs des systèmes d'information et de communication, l'octroi de subventions, la coopération internationale entre l'autorité nationale de cybersécurité, des autorités compétentes des autres États membres, des forums internationaux de cybersécurité, l'ENISA et la Commission européenne;

3° la gestion des crises cyber et incidents de cybersécurité;

4° l'exécution des tâches du CSIRT national visées aux articles suivants:

- a) 19, § 1^{er};
- b) 21, § 2, al. 2, 1° à 3°;
- c) 22, § 2 à § 6;
- d) 37, § 1^{er} à § 3, et § 5;

Art. 65

Artikel 47 is van toepassing op de inspectiedienst bedoeld in artikel 64.

TITEL 6

Verwerking van persoonsgegevens

HOOFDSTUK 1

Beginselen betreffende de verwerking

Art. 66

De definities van Verordening (EU) 2016/679 zijn van toepassing op deze titel.

Art. 67

De verwerking van persoonsgegevens vindt plaats voor de volgende doeleinden:

1° de verbetering van de cyberbeveiliging dankzij een betere bescherming van de netwerk- en informatiesystemen, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsincidenten en de bescherming tegen cyberdreigingen;

2° de uitvoering van de taken van de nationale cyberbeveiligingsautoriteit, met name het identificeren van de entiteiten, het informeren en sensibiliseren van de gebruikers van informatie- en communicatiesystemen, het toekennen van subsidies, de internationale samenwerking tussen de nationale cyberbeveiligingsautoriteit, de bevoegde autoriteiten van andere lidstaten, internationale fora voor cyberbeveiliging, Enisa en de Europese Commissie;

3° het beheer van cybercrises en cyberbeveiligingsincidenten;

4° de uitvoering van de taken van het nationale CSIRT bedoeld in de volgende artikelen:

- a) 19, § 1;
- b) 21, § 2, tweede lid, 1° tot 3°;
- c) 22, §§ 2 tot 6;
- d) 37, §§ 1 tot 3, en § 5;

5° la coopération, notamment l'échange d'informations entre l'autorité nationale de cybersécurité, les éventuelles autorités sectorielles, le NCCN et les autorités compétentes dans le cadre de la loi du 1^{er} juillet 2011, ainsi que les autorités visées à l'article 25, § 2 dans le cadre de l'exécution de la présente loi et la loi du 1^{er} juillet 2011;

6° la coopération entre les entités essentielles et importantes et les autorités visées au titre 2, chapitre 1^{er};

7° le partage d'informations entre les autorités visées à l'article 25, § 5;

8° la continuité des services prestés par les entités importantes ou essentielles;

9° la notification d'incidents et d'incidents évités;

10° le contrôle et la supervision des entités essentielles et importantes, ainsi que la préparation, l'organisation, la gestion et le suivi de mesures et d'amendes administratives.

Art. 68

Les catégories de données à caractère personnel traitées par les responsables de traitement sont les suivantes:

1° pour la finalité visée à l'article 67, 1°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par les missions d'amélioration de la cybersécurité, de renforcement des politiques de prévention et de sécurité, de prévention des incidents de sécurité et de défense contre les cybermenaces visées à l'article 67, 1°;

2° pour la finalité visée à l'article 67, 2°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par l'exécution des tâches de l'autorité nationale de cybersécurité;

3° pour la finalité visée à l'article 67, 3°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par les crises cyber et incidents de cybersécurité;

4° pour la finalité visée à l'article 67, 4°: les données d'identification, de connexion, de localisation, de communications électroniques au sens de l'article 2, 91°, de

5° de samenwerking, met name de informatie-uitwisseling tussen de nationale cyberbeveiligingsautoriteit, de eventuele sectorale overheden, het NCCN en de autoriteiten die bevoegd zijn in het kader van de wet van 1 juli 2011, alsook de autoriteiten bedoeld in artikel 25, § 2, in het kader van de uitvoering van deze wet en de wet van 1 juli 2011;

6° de samenwerking tussen essentiële en belangrijke entiteiten en de autoriteiten bedoeld in titel 2, hoofdstuk 1;

7° het delen van informatie tussen de autoriteiten bedoeld in artikel 25, § 5;

8° de continuïteit van de dienstverlening door belangrijke of essentiële entiteiten;

9° het melden van incidenten en bijna-incidenten;

10° de controle van en het toezicht op essentiële en belangrijke entiteiten, alsook de voorbereiding, de organisatie, het beheer en de opvolging van administratieve maatregelen en geldboetes.

Art. 68

De verwerkingsverantwoordelijken verwerken de volgende categorieën van persoonsgegevens:

1° voor het doeleinde bedoeld in artikel 67, 1°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij de opdrachten rond de verbetering van de cyberbeveiliging, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsincidenten en de bescherming tegen cyberdreigingen bedoeld in artikel 67, 1°;

2° voor het doeleinde bedoeld in artikel 67, 2°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij de uitvoering van de taken van de nationale cyberbeveiligingsautoriteit;

3° voor het doeleinde bedoeld in artikel 67, 3°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij cybercrises en cyberbeveiligingsincidenten;

4° voor het doeleinde bedoeld in artikel 67, 4°: de identificatie-, verbindings-, locatie-, elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de

la loi du 13 juin 2005 et des métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi précitée du 13 juin 2005, des personnes concernées par l'exécution des tâches du CSIRT;

5° pour la finalité visée à l'article 67, 5°: les données d'identification des personnes concernées par la coopération dans le cadre de la loi du 1^{er} juillet 2011;

6° pour la finalité visée à l'article 67, 6°: les données d'identification des personnes concernées par la coopération;

7° pour la finalité visée à l'article 67, 7°: les données d'identification des personnes concernées par le partage d'informations;

8° pour la finalité visée à l'article 67, 8°: les données d'identification des personnes concernées par l'assurance d'une continuité des services;

9° pour la finalité visée à l'article 67, 9°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par l'exercice de notification;

10° pour la finalité visée à l'article 67, 10°: les données à caractère personnel nécessaires et pertinentes à l'exercice des missions de contrôle, de supervision et de sanction, des personnes concernées par ces contrôles, cette supervision ou ces sanctions.

Art. 69

Les catégories de personnes dont les données à caractère personnel sont susceptibles de faire l'objet de traitement sont les suivantes:

1° les personnes participant directement aux missions confiées à l'autorité nationale de cybersécurité en vertu du titre 2;

2° les personnes visées par les obligations qui incombent aux entités essentielles et importantes en vertu du titre 3;

3° les personnes impliquées dans un incident;

4° les personnes directement impliquées dans les exercices de supervision, de contrôle et de sanction, visés au titre 4.

wet van 13 juni 2005, en elektronische-communicatiemeetgegevens als bedoeld in artikel 2, 93°, van voornoemde wet van 13 juni 2005, van de personen die betrokken zijn bij de uitvoering van de taken van het CSIRT;

5° voor het doeleinde bedoeld in artikel 67, 5°: de identificatiegegevens van de personen die betrokken zijn bij de samenwerking in het kader van de wet van 1 juli 2011;

6° voor het doeleinde bedoeld in artikel 67, 6°: de identificatiegegevens van de personen die betrokken zijn bij de samenwerking;

7° voor het doeleinde bedoeld in artikel 67, 7°: de identificatiegegevens van de personen die betrokken zijn bij het delen van informatie;

8° voor het doeleinde bedoeld in artikel 67, 8°: de identificatiegegevens van de personen die betrokken zijn bij het waarborgen van de continuïteit van de dienstverlening;

9° voor het doeleinde bedoeld in artikel 67, 9°: de identificatie-, verbindings-, locatie- en elektronische-communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij de melding;

10° voor het doeleinde bedoeld in artikel 67, 10°: de persoonsgegevens die nodig en relevant zijn voor de uitoefening van de controle-, toezichts- en sanctieopdrachten, van de personen die betrokken zijn bij deze controles, dit toezicht of deze sancties.

Art. 69

De persoonsgegevens van de volgende categorieën van personen kunnen het voorwerp uitmaken van verwerkingen:

1° de personen die rechtstreeks deelnemen aan de opdrachten die krachtens titel 2 zijn toevertrouwd aan de nationale cyberbeveiligingsautoriteit;

2° de personen bedoeld in het kader van de verplichtingen voor essentiële en belangrijke entiteiten die voortvloeien uit titel 3;

3° de personen die betrokken zijn bij een incident;

4° de personen die rechtstreeks betrokken zijn bij het toezicht, de controle en de sancties bedoeld in titel 4.

Art. 70

Les entités suivantes sont responsables des traitements qu'elles effectuent pour la réalisation des finalités visées à l'article 67:

- 1° l'autorité nationale de cybersécurité;
- 2° le NCCN;
- 3° l'éventuelle autorité sectorielle;
- 4° l'éventuel service d'inspection sectoriel;
- 5° les entités essentielles et importantes;
- 6° les entités fournissant des services d'enregistrement de noms de domaine;
- 7° les autorités visées à l'article 23, § 1^{er}, 6°.

CHAPITRE 2

Durée de conservation

Art. 71

Les données à caractère personnel traitées dans le cadre des traitements visés par la présente loi en vue de réaliser les finalités prévues à l'article 67, sont conservées, sans préjudice de recours éventuels, par le responsable du traitement cinq ans après la fin du dernier traitement effectué et dix ans maximum après le premier traitement effectué.

CHAPITRE 3

Limitation des droits des personnes concernées

Art. 72

§ 1^{er}. En application de l'article 23.1, a), b), c), d), e), h), du règlement (UE) 2016/679, certaines obligations et droits prévus par ledit règlement sont limités ou exclus, conformément aux dispositions du présent chapitre. Ces limitations ou exclusions ne peuvent porter préjudice à l'essence des libertés et droits fondamentaux et doivent être appliquées dans la stricte mesure nécessaire au but poursuivi.

§ 2. Les articles 12 à 16, 18 et 19 dudit règlement ne sont pas applicables aux traitements de données à caractère personnel effectués par une autorité visée à

Art. 70

De volgende entiteiten zijn verantwoordelijk voor de verwerkingen die zij uitvoeren voor de verwezenlijking van de doeleinden bedoeld in artikel 67:

- 1° de nationale cyberbeveiligingsautoriteit;
- 2° het NCCN;
- 3° de eventuele sectorale overheid;
- 4° de eventuele sectorale inspectiedienst;
- 5° de essentiële en belangrijke entiteiten;
- 6° de entiteiten die domeinnaamregistratiediensten verlenen;
- 7° de autoriteiten bedoeld in artikel 23, § 1, 6°.

HOOFDSTUK 2

Bewaartermijn

Art. 71

De verwerkingsverantwoordelijke bewaart de persoonsgegevens die verwerkt worden in het kader van de in deze wet bedoelde verwerkingen om de doeleinden bedoeld in artikel 67 te realiseren, onverminderd eventuele beroepsprocedures, gedurende vijf jaar na afloop van de laatste verwerking en maximaal gedurende tien jaar na de eerste verwerking.

HOOFDSTUK 3

Beperking van de rechten van de betrokkenen

Art. 72

§ 1. Met toepassing van artikel 23.1, a), b), c), d), e), h), van Verordening (EU) 2016/679 worden sommige verplichtingen en rechten van deze verordening beperkt of uitgesloten, overeenkomstig de bepalingen van dit hoofdstuk. Deze beperkingen of uitsluitingen mogen geen afbreuk doen aan de wezenlijke inhoud van de grondrechten en fundamentele vrijheden en moeten worden toegepast voor zover dit strikt noodzakelijk is voor het nagestreefde doel.

§ 2. De artikelen 12 tot 16, 18 en 19 van voornoemde verordening zijn niet van toepassing op verwerkingen van persoonsgegevens die worden verricht door een

l'article 15 pour la finalité visée à l'article 67, 10°, dans la mesure où l'exercice des droits consacrés par ces articles nuirait aux besoins du contrôle, de la supervision ou des actes préparatoires à celui-ci.

§ 3. L'exemption vaut pour les catégories de données à caractère personnel visées à l'article 68, 10°. Cette exemption vaut également pour les actes préparatoires ou pour les procédures visant à l'application éventuelle d'une sanction administrative.

§ 4. L'exemption ne s'applique que pendant la période au cours de laquelle la personne concernée fait l'objet d'un contrôle, d'une supervision ou d'actes préparatoires à ceux-ci, dans la mesure où l'exercice des droits faisant l'objet de la dérogation visée au présent article nuirait aux besoins du contrôle, de la supervision ou des actes préparatoires à ceux-ci et, en tous les cas, ne s'applique que jusqu'à un an après le début d'un contrôle, d'une supervision ou d'actes préparatoires à ceux-ci.

La durée des actes préparatoires, visés à l'alinéa 1^{er}, pendant laquelle les articles visés au paragraphe 2 ne sont pas applicables, ne peut excéder un an à partir de la réception d'une demande relative à l'application d'un des droits consacrés par ces articles.

§ 5. Le responsable du traitement qui ne se conforme pas à toutes les dispositions du présent titre et en particulier de l'article 73, ne peut bénéficier de l'exemption.

Art. 73

§ 1^{er}. Le responsable du traitement concerné donne accès à la personne concernée à des informations limitées concernant le traitement de ses données à caractère personnel, pour autant que cette communication ne compromette pas la réalisation des objectifs de la présente loi et de manière telle que la personne concernée se trouve dans l'impossibilité de savoir si elle fait l'objet d'une enquête ou pas, et sans pouvoir en aucun cas rectifier, effacer, limiter, notifier, transmettre à un tiers des données à caractère personnel, ni cesser toute forme de traitement desdites données qui soit nécessaire dans le cadre défini ci-avant.

§ 2. La mesure de refus ou de limitation des droits consacrés par les articles visés à l'article 72, § 2, doit être levée:

1° pour les mesures justifiées par les obligations en matière de notification d'incidents, lors de la clôture du

autoriteit bedoeld in artikel 15 voor het doeleinde bedoeld in artikel 67, 10°, voor zover de uitoefening van de in deze artikelen vastgelegde rechten nadelig zou zijn voor de controle, het toezicht of de voorbereidende werkzaamheden ervan.

§ 3. De vrijstelling geldt voor de categorieën van persoonsgegevens bedoeld in artikel 68, 10°. Deze vrijstelling geldt ook voor voorbereidende werkzaamheden of procedures met het oog op de eventuele toepassing van een administratieve sanctie.

§ 4. De vrijstelling geldt enkel voor de periode tijdens dewelke de betrokkene onderworpen is aan een controle, toezicht of de voorbereidende werkzaamheden ervan, voor zover de uitoefening van de rechten die het voorwerp uitmaken van de in dit artikel bedoelde afwijking nadelig zou zijn voor de controle, het toezicht of de voorbereidende werkzaamheden ervan. In ieder geval geldt ze slechts maximaal één jaar na aanvang van een controle, toezicht of de voorbereidende werkzaamheden ervan.

De duur van de voorbereidende werkzaamheden bedoeld in het eerste lid, tijdens dewelke de in paragraaf 2 bedoelde artikelen niet van toepassing zijn, is beperkt tot maximaal één jaar na ontvangst van een verzoek betreffende de toepassing van een van de in deze artikelen vastgelegde rechten.

§ 5. De verwerkingsverantwoordelijke die niet voldoet aan alle bepalingen van deze titel en met name van artikel 73, kan geen gebruik maken van de vrijstelling.

Art. 73

§ 1. De betrokken verwerkingsverantwoordelijke verleent de betrokkene toegang tot beperkte informatie over de verwerking van zijn persoonsgegevens, voor zover deze kennisgeving de verwezenlijking van de doelstellingen van deze wet niet in het gedrang brengt. Hierbij moet het voor de betrokkene onmogelijk zijn om na te gaan of hij al dan niet het voorwerp uitmaakt van een onderzoek, en kan hij in geen geval persoonsgegevens rechtzetten, wissen, beperken, meedelen, of aan derden overdragen, noch enige vorm van verwerking van voormelde gegevens die in het bovenvermelde kader noodzakelijk is, stopzetten.

§ 2. De maatregel betreffende de weigering of beperking van de rechten die zijn vastgelegd in de artikelen bedoeld in artikel 72, § 2, moet worden opgeheven:

1° voor maatregelen die gerechtvaardigd zijn door de verplichtingen inzake het melden van incidenten, bij het

traitement d'un incident par les autorités visées aux articles 34 et 38;

2° pour les mesures justifiées par les obligations en vertu du titre 4, lors de la clôture du contrôle, de la supervision ou des actes préparatoires à ceux-ci effectués par le service d'inspection, ainsi que pendant la période durant laquelle l'éventuelle autorité sectorielle traite les pièces provenant du service d'inspection en vue d'exercer des poursuites;

3° au plus tard un an à partir de la réception de la demande introduite en application des articles visés à l'article 72, § 2, sauf si un contrôle ou une supervision sont en cours.

§ 3. Le responsable du traitement concerné lève également la mesure de refus ou de limitation des droits consacrés par les articles visés à l'article 72, § 2, dès qu'une telle mesure n'est plus nécessaire au respect d'une des finalités visées à l'article 67.

§ 4. Dans tous les cas d'application des paragraphes 2 et 3, le délégué à la protection des données informe par écrit la ou les personnes concernées de la levée de la mesure de refus ou de limitation.

CHAPITRE 4

Limitations aux obligations de notification des violations de données à caractère personnel

Art. 74

Le responsable du traitement concerné est dispensé de communiquer une violation de données à caractère personnel à une ou des personnes concernées bien déterminées, au sens de l'article 34 du règlement (UE) 2016/679, moyennant l'autorisation de l'autorité nationale de cybersécurité, pour autant que et dans la mesure où une telle notification individuelle risque de compromettre la réalisation des finalités visées à l'article 72, § 2.

afsluiten van de verwerking van een incident door de autoriteiten bedoeld in de artikelen 34 en 38;

2° voor maatregelen die gerechtvaardigd zijn door de verplichtingen krachtens titel 4, bij het afsluiten van de controle, het toezicht of de voorbereidende werkzaamheden ervan door de inspectiedienst, alsook in de periode tijdens dewelke de eventuele sectorale overheid de stukken verwerkt die afkomstig zijn van de inspectiedienst met het oog op vervolging;

3° uiterlijk één jaar na ontvangst van het verzoek dat is ingediend overeenkomstig de artikelen bedoeld in artikel 72, § 2, behalve indien een controle of toezicht loopt.

§ 3. De betrokken verwerkingsverantwoordelijke heft de maatregel betreffende de weigering of beperking van de rechten die zijn vastgelegd in de artikelen bedoeld in artikel 72, § 2, ook op zodra deze maatregel niet meer nodig is voor het nakomen van een van de doeleinden bedoeld in artikel 67.

§ 4. In alle toepassingsgevallen van de paragrafen 2 en 3 informeert de functionaris voor gegevensbescherming de betrokkene of betrokkenen schriftelijk dat de maatregel betreffende de weigering of beperking is opgeheven.

HOOFDSTUK 4

Beperkingen inzake de verplichte melding van inbreuken in verband met persoonsgegevens

Art. 74

De betrokken verwerkingsverantwoordelijke is vrijgesteld van het meedelen van een inbreuk in verband met persoonsgegevens aan een of meer welbepaalde betrokkenen, in de zin van artikel 34 van Verordening EU 2016/679, mits toestemming van de nationale cyberbeveiligingsautoriteit, voor zover deze individuele kennisgeving de verwezenlijking van de doeleinden bedoeld in artikel 72, § 2, in het gedrang zou brengen.

TITRE 7

*Dispositions finales*CHAPITRE 1^{ER}**Disposition transitoire**

Art. 75

Le Roi fixe les délais endéans lesquels les entités essentielles effectuent leurs premières évaluations périodiques de la conformité visées à l'article 39.

CHAPITRE 2

Dispositions modificatives**Section 1^{re}**

Modifications de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire

Art. 76

À l'article 1^{er} de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, modifié en dernier lieu par la loi du 19 décembre 2021, les mots “-la loi du 7 avril 2019”: la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;” sont remplacés par les mots “- la loi NIS2: la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;”.

Art. 77

Dans la section 1^{re} du chapitre III de la même loi, l'article 15^{ter}, inséré par la loi du 7 avril 2019, est remplacé par ce qui suit:

TITEL 7

Slotbepalingen

HOOFDSTUK 1

Overgangsbepaling

Art. 75

De Koning stelt de termijnen vast waarbinnen essentiële entiteiten hun eerste regelmatige conformiteitsbeoordelingen als bedoeld in artikel 39 uitvoeren.

HOOFDSTUK 2

Wijzigingsbepalingen**Afdeling 1**

Wijzigingen van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle

Art. 76

In artikel 1 van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, het laatst gewijzigd bij de wet van 19 december 2021, worden de woorden “- de wet van 7 april 2019”: de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;” vervangen door de woorden “- de NIS2-wet: de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;”.

Art. 77

In afdeling 1 van hoofdstuk III van dezelfde wet wordt artikel 15^{ter}, ingevoegd bij de wet van 7 april 2019, vervangen als volgt:

“Art. 15ter. L’Agence est désignée comme service d’inspection sectoriel, au sens de la loi NIS2, pour le secteur de l’énergie, en ce qui concerne les mesures supplémentaires de gestion des risques en matière de cybersécurité applicables aux éléments d’une installation nucléaire destinée à la production industrielle d’électricité et qui servent au transport de l’électricité.

Le Roi fixe les modalités pratiques des inspections, après avis de l’Agence.”

Section 2

Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique

Art. 78

À l’article 36/1 de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique, modifié en dernier lieu par la loi du 20 juillet 2022, le 28° est remplacé par ce qui suit:

“la loi NIS2”: la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique;”

Art. 79

À l’article 36/14 de la même loi, modifié en dernier lieu par la loi du 20 juillet 2022, les modifications suivantes sont apportées:

1° au paragraphe 1^{er}, 20°, les mots “à l’autorité visée à l’article 7, § 1^{er}, de la loi du 7 avril 2019” sont remplacés par les mots “à l’autorité nationale de cybersécurité visée à l’article 8, 45°, de la loi NIS2”;

2° au même paragraphe, 20° /1, les mots “à l’autorité visée à l’article 7, § 1^{er}, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique – loi NIS” sont remplacés par les mots “à l’autorité nationale de cybersécurité visée à l’article 8, 45°, de la loi NIS2 et au CSIRT national visé à l’article 8, 46°, de la même loi”;

3° au même paragraphe, 24°, les mots “aux autorités visées à l’article 7 de la loi du 7 avril 2019 pour les besoins de l’exécution des dispositions de la loi du 7 avril 2019” sont remplacés par les mots “aux autorités

“Art. 15ter. Het Agentschap wordt aangewezen als sectorale inspectiedienst in de zin van de NIS2-wet voor de sector energie, wat betreft de bijkomende maatregelen voor het beheer van cyberbeveiligingsrisico’s die van toepassing zijn op de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van elektriciteit.

De Koning bepaalt de praktische inspectiemodaliteiten, na advies van het Agentschap.”

Afdeling 2

Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België

Art. 78

In artikel 36/1 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, het laatst gewijzigd bij de wet van 20 juli 2022, wordt punt 28° vervangen als volgt:

“de NIS2-wet”: de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;”

Art. 79

In artikel 36/14 van dezelfde wet, het laatst gewijzigd bij de wet van 20 juli 2022, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, 20°, worden de woorden “aan de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019” vervangen door de woorden “aan de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 45°, van de NIS2-wet”;

2° in dezelfde paragraaf, 20° /1, worden de woorden “aan de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid – NIS-wet” vervangen door de woorden “aan de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 45°, van de NIS2-wet en aan het nationaal CSIRT bedoeld in artikel 8, 46°, van dezelfde wet”;

3° in dezelfde paragraaf, 24°, worden de woorden “aan de autoriteiten bedoeld in artikel 7 van de wet van 7 april 2019 voor de uitvoering van de bepalingen van de wet van 7 april 2019” vervangen door de woorden “aan

visées à l'article 15 de la loi NIS2 pour les besoins de l'exécution des dispositions de la loi NIS2".

Art. 80

L'article 36/47 de la même loi, inséré par la loi du 7 avril 2019, est remplacé par ce qui suit:

"Pour l'application de la loi NIS2, la Banque est désignée comme autorité sectorielle et service d'inspection sectoriel pour les entités du secteur des finances, à l'exception des opérateurs de plate-forme de négociation au sens de l'article 3, 6°, de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la directive 2014/65/UE.

Si elle le juge utile, la Banque partage le plus vite possible avec la BCE les informations pertinentes sur les notifications d'incident qu'elle reçoit en vertu de la loi NIS2 ou du Règlement 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011."

Section 3

Modification de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

Art. 81

À l'article 75, § 1^{er}, 15°, de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, modifié en dernier lieu par la loi du 20 juillet 2020, les mots "l'article 7 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique" sont remplacés par les mots "l'article 15 de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique".

de autoriteiten bedoeld in artikel 15 van de NIS2-wet voor de uitvoering van de bepalingen van de NIS2-wet".

Art. 80

Artikel 36/47 van dezelfde wet, ingevoegd bij de wet van 7 april 2019, wordt vervangen als volgt:

"Voor de toepassing van de NIS2-wet wordt de Bank aangewezen als sectorale overheid en sectorale inspectiedienst voor de entiteiten van de sector financiën, met uitzondering van de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU.

Wanneer zij dit nuttig acht, deelt de Bank zo snel mogelijk met de ECB relevante informatie over incidentmeldingen die zij ontvangt krachtens de NIS2-Wet of Verordening 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011."

Afdeling 3

Wijziging van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

Art. 81

In artikel 75, § 1, 15°, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, het laatst gewijzigd bij de wet van 20 juli 2020, worden de woorden "artikel 7 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid" vervangen door de woorden "artikel 15 van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid".

Section 4

Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges

Art. 82

À l'article 1^{er}/1 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, remplacé par la loi du 21 décembre 2021, le 1^o est remplacé par ce qui suit:

"1^o la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148;"

Art. 83

À l'article 14 de la même loi, modifié en dernier lieu par la loi du 20 juillet 2022, les modifications suivantes sont apportées:

1^o au paragraphe 1^{er}, les mots "loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique" sont remplacés par les mots "loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique";

2^o au même paragraphe, le 3^o, alinéa 1^{er}, h), est remplacé par ce qui suit:

"h) la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, pour ce qui concerne les tâches dévolues à l'autorité sectorielle et au service d'inspection sectoriel pour le secteur des infrastructures numériques, à l'exception des prestataires de services de confiance au sens de l'article 8, 24^o, de cette même loi;"

3^o au même paragraphe, le 3^o, alinéa 2, est remplacé par ce qui suit:

"Pour l'application de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut est désigné comme autorité sectorielle au sens de l'article 8, 54^o, de cette même loi

Afdeling 4

Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

Art. 82

In artikel 1/1 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, vervangen door de wet van 21 december 2021, wordt punt 1^o vervangen als volgt:

"1^o Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148;"

Art. 83

In artikel 14 van dezelfde wet, het laatst gewijzigd bij de wet van 20 juli 2022, worden de volgende wijzigingen aangebracht:

1^o in paragraaf 1 worden de woorden "wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid" vervangen door de woorden "wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid";

2^o in dezelfde paragraaf wordt punt 3^o, eerste lid, h), vervangen als volgt:

"h) de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, voor wat betreft de taken toegewezen aan de sectorale overheid en de sectorale inspectiedienst voor de sector digitaal infrastructuur, met uitzondering van de verleners van vertrouwensdiensten in de zin van artikel 8, 24^o, van dezelfde wet;"

3^o in dezelfde paragraaf wordt punt 3^o, tweede lid, vervangen als volgt:

"Voor de toepassing van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wordt het Instituut aangewezen als sectorale overheid in de zin van artikel 8,

et service d'inspection sectoriel au sens de l'article 44, § 1^{er}, alinéa 2, de cette même loi pour le secteur des infrastructures numériques, à l'exception des prestataires de services de confiance au sens de l'article 8, 24°, de cette même loi, et pour le secteur des services postaux et d'expédition."

Section 5

Modifications de la loi du 13 juin 2005 relative aux communications électroniques

Art. 84

À l'article 1^{er} de la loi du 13 juin 2005 relative aux communications électroniques, modifiée en dernier lieu par la loi du 30 août 2023, les modifications suivantes sont apportées:

1° à l'alinéa 2, à la fin du 6°, le point est remplacé par un point-virgule;

2° le même alinéa est complété par un 7°, rédigé comme suit:

"7° la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148."

Art. 85

À l'article 2 de la même loi, les modifications suivantes sont apportées:

1° le 48/1° est remplacé par ce qui suit:

"48/1° "registre de noms de domaine de premier niveau": une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration du domaine de premier niveau, y compris de l'enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage;

54° van dezelfde wet en als sectorale inspectiedienst in de zin van artikel 44, § 1, tweede lid, van dezelfde wet voor de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten in de zin van artikel 8, 24°, van dezelfde wet, en voor de sector post- en koeriersdiensten."

Afdeling 5

Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie

Art. 84

In artikel 1 van de wet van 13 juni 2005 betreffende de elektronische communicatie, het laatst gewijzigd bij de wet van 30 augustus 2023, worden de volgende wijzigingen aangebracht:

1° in het tweede lid, aan het einde van punt 6°, wordt het punt vervangen door een puntkomma;

2° hetzelfde lid wordt aangevuld met een bepaling onder 7°, luidende:

"7° Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148."

Art. 85

In artikel 2 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de bepaling onder 48/1° wordt vervangen als volgt:

"48/1° "register voor topleveldomeinnamen": een entiteit waaraan een specifieke topleveldomeinnaam is gedelegeerd en die verantwoordelijk is voor het beheer van de topleveldomeinnaam, met inbegrip van de registratie van domeinnamen onder de topleveldomeinnaam en de technische exploitatie van de topleveldomeinnaam, met inbegrip van de exploitatie van de naamsservers, het onderhoud van de databases en de verdeling van de zonebestanden van de topleveldomeinnaam over de naamsservers, ongeacht of die activiteiten door de entiteit zelf worden uitgevoerd of worden uitbesteed, maar met uitzondering van situaties waarin topleveldomeinnamen uitsluitend voor eigen gebruik worden aangewend door een register;

2° le 48/3° est inséré, rédigé comme suit:

“48/3° “entité fournissant des services d’enregistrement de noms de domaine”: un bureau d’enregistrement ou un agent agissant pour le compte de bureaux d’enregistrement, tel qu’un fournisseur ou revendeur de services d’anonymisation ou d’enregistrement fiduciaire;”

3° les 62/2° et 62/3° sont remplacés par ce qui suit:

“62/2° “réseau et système d’information”:

a) un réseau de communications électroniques au sens du 3°;

b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d’un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l’automatisation du processus opérationnel, le contrôle à distance, ou l’obtention de données de fonctionnement en temps réel; ou

c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance;

62/3° “sécurité des réseaux et des systèmes d’information”: la capacité des réseaux et des systèmes d’information de résister, à un niveau de confiance donné, à tout événement susceptible de compromettre la disponibilité, l’authenticité, l’intégrité ou la confidentialité de données stockées, transmises ou faisant l’objet d’un traitement, ou des services que ces réseaux et systèmes d’information offrent ou rendent accessibles;”

4° les 62/4° à 62/8° sont insérés, rédigés comme suit:

“62/4° “incident de sécurité”: un événement compromettant la disponibilité, l’authenticité, l’intégrité ou la confidentialité des données stockées, transmises ou faisant l’objet d’un traitement, ou des services que les réseaux et systèmes d’information offrent ou rendent accessibles;

62/5° “cybersécurité”: la cybersécurité au sens de l’article 2, point 1), du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l’ENISA (Agence de l’Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l’information et des communications,

2° de bepaling onder 48/3° is ingevoegd, luidende:

“48/3° “entiteit die domeinnaamregistratiediensten aanbiedt”: een registrar of een agent die namensregistrators optreedt, zoals een aanbieder van privacy- of proxy-registratiediensten of wederverkoper;”

3° de bepalingen onder 62/2° en 62/3° worden vervangen als volgt:

“62/2° “netwerk- en informatiesysteem”:

a) een elektronische-communicatienetwerk als bedoeld in 3°;

b) elk apparaat of elke groep van onderling verbonden of bij elkaar behorende apparaten, waarvan er een of meer, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische componenten van dat apparaat die met name de automatisering van het operationele proces, de controle op afstand of het verkrijgen van werkingsgegevens in real time mogelijk maken; of

c) digitale gegevens die worden opgeslagen, verwerkt, opgehaald of verzonden met behulp van de in de punten a) en b) bedoelde elementen met het oog op de werking, het gebruik, de bescherming en het onderhoud ervan;

62/3° “beveiliging van netwerk- en informatiesystemen”: het vermogen van netwerken informatiesystemen om op een bepaald niveau van betrouwbaarheid weerstand te bieden aan elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die door of via deze netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen;”

4° de bepalingen onder 62/4° tot 62/8° worden ingevoegd, luidende:

“62/4° “beveiligingsincident”: een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt;

62/5° “cyberbeveiliging”: cyberbeveiliging als bedoeld in artikel 2, 1), van Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie

et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité);

62/6° “traitement des incidents”: toutes les actions et procédures visant à prévenir, détecter, analyser et contenir un incident ou à y répondre et à y remédier;

62/7° “cybermenace”: une cybermenace au sens de l’article 2, point 8), du règlement (UE) 2019/881;

62/8° “cybermenace importante”: une cybermenace qui, compte tenu de ses caractéristiques techniques, peut être considérée comme susceptible d’avoir un impact grave sur les réseaux et les systèmes d’information d’une entité ou les utilisateurs des services de l’entité, en causant un dommage matériel, corporel ou moral considérable;

5° l’article est complété par un 94°, rédigé comme suit:

“94° “fournisseur d’infrastructure numérique”: une entité qui relève du secteur infrastructure numérique, à l’exception des prestataires de services de confiance, au sens de l’article 8, 24°, de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique.”

Art. 86

Dans l’article 6, 4°, de la même loi, les mots “réseaux et services” sont remplacés par les mots “réseaux et systèmes d’information”.

Art. 87

Dans l’article 105, paragraphe 2, 2°, de la même loi, les mots “ou comme opérateur de services essentiels au sens de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique” sont supprimés.

Art. 88

Dans la même loi, les articles 107/2 à 107/4 sont remplacés par ce qui suit:

“Art. 107/2. § 1^{er}. Sans préjudice des dispositions de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d’information

en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening);

62/6° “incidentenbehandeling”: alle acties en procedures die gericht zijn op het voorkomen, opsporen, analyseren en indammen van of het reageren op en het herstellen van een beveiligingsincident;

62/7° “cyberdreiging”: een cyberdreiging als bedoeld in artikel 2, 8), van de cyberbeveiligingsverordening;

62/8° “significante cyberdreiging”: een cyberdreiging waarvan op basis van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerk- en informatiesystemen van een entiteit of de gebruikers van de diensten van de entiteit door het veroorzaken van aanzienlijke materiële of immateriële schade;”

5° het artikel wordt aangevuld met een bepaling onder 94°, luidende:

“94° “aanbieder van digitale infrastructuur”: een entiteit die behoort tot de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten, in de zin van artikel 8, 24°, van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.”

Art. 86

In artikel 6, 4°, van dezelfde wet, worden de woorden “netwerken en diensten” vervangen door de woorden “netwerk- en informatiesystemen”.

Art. 87

In artikel 105, paragraaf 2, 2°, van dezelfde wet worden de woorden “of als aanbieder van essentiële diensten in de zin van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid” geschrapt.

Art. 88

In dezelfde wet worden de artikelen 107/2 tot 107/4 vervangen als volgt:

“Art. 107/2. § 1. Onverminderd de bepalingen van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen

d'intérêt général pour la sécurité publique, les fournisseurs d'infrastructure numérique analysent les risques pour la sécurité de leurs réseaux et systèmes d'information. L'Institut peut fixer les modalités de cette analyse des risques.

§ 2. Sans préjudice du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, ci-après dénommé "RGPD" et de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, ci-après dénommée la "loi du 30 juillet 2018", les opérateurs veillent pour le moins à:

1° garantir que seules des personnes habilitées à agir à des fins légalement autorisées puissent avoir accès aux données à caractère personnel qu'ils traitent;

2° protéger les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites; et

3° assurer la mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel.

L'Institut est habilité à vérifier les mesures prises par ces opérateurs ainsi qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient permettre d'atteindre.

§ 3. Les opérateurs prennent toutes les mesures nécessaires, y compris préventives, pour assurer la disponibilité la plus complète possible des services de communications vocales et des services d'accès à l'internet en cas de défaillance exceptionnelle des réseaux ou de force majeure.

Le Roi, sur proposition de l'Institut ou d'initiative, sur avis de celui-ci, peut préciser ces mesures.

§ 4. Les opérateurs offrent gratuitement à leurs abonnés, compte tenu des possibilités techniques, les services sécurisés adéquats, afin de permettre aux utilisateurs finaux d'éviter toute forme de communication électronique non souhaitée.

Art. 107/3. § 1^{er}. En cas de cybermenace importante, le fournisseur d'infrastructure numérique informe l'Institut de la cybermenace, de toute mesure de protection ou

van algemeen belang voor de openbare veiligheid analyseren de aanbieders van digitale infrastructuur de risico's voor de beveiliging van hun netwerk- en informatiesystemen. Het Instituut kan de nadere regels van deze risicoanalyse vaststellen.

§ 2. Onverminderd Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, hierna "AVG" genoemd, en de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, hierna de "wet van 30 juli 2018" genoemd, zorgen de operatoren ervoor dat in ieder geval:

1° wordt gewaarborgd dat alleen gemachtigd personeel voor wettelijk toegestane doeleinden toegang heeft tot de persoonsgegevens die ze verwerken;

2° opgeslagen of verzonden persoonsgegevens worden beschermd tegen onbedoelde of onwettige vernietiging, onbedoeld verlies of wijziging, en niet-toegestane of onwettige opslag, verwerking, toegang of vrijgave, en

3° een beveiligingsbeleid wordt ingevoerd met betrekking tot de verwerking van persoonsgegevens.

Het Instituut kan de door deze operatoren genomen maatregelen controleren en aanbevelingen formuleren over de beste praktijken betreffende het beveiligingspeil dat met deze maatregelen moet worden gehaald.

§ 3. De operatoren nemen alle noodzakelijke maatregelen, inclusief preventieve, om de beschikbaarheid van de spraakcommunicatiediensten en de internet-toegangsdiensten zo volledig mogelijk te waarborgen in geval van uitzonderlijke netwerkuitval of in geval van overmacht.

Op voorstel van het Instituut of op eigen initiatief, en na advies van het Instituut, kan de Koning deze maatregelen preciseren.

§ 4. De operatoren bieden hun abonnees kosteloos, rekening houdend met de stand van de techniek, de gepaste beveiligde diensten aan die de eindgebruikers in staat stellen ongewenste elektronische communicatie in alle vormen te verhinderen.

Art. 107/3. § 1. In geval van een significante cyberdreiging informeert de aanbieder van digitale infrastructuur het Instituut over de dreiging, over mogelijke

correctrice que ses utilisateurs peuvent prendre ainsi que des mesures qu'il a prises ou envisage de prendre.

L'Institut peut préciser les cas dans lesquels une information doit être notifiée ainsi que les modalités de cette communication.

§ 2. En cas de violation de données à caractère personnel, l'opérateur de services de communications électroniques avertit sans délai l'autorité de protection des données, qui en avertit sans délai l'Institut.

Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, l'opérateur de services de communications électroniques avertit également sans délai l'abonné ou le particulier concerné de la violation.

L'autorité de protection des données examine si l'opérateur se conforme à cette obligation et informe l'Institut lorsqu'elle estime que cela n'est pas le cas.

La notification d'une violation des données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si l'opérateur de services de communications électroniques a prouvé, à la satisfaction de l'Institut, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

Sans préjudice de l'obligation de l'opérateur de service de communications électroniques d'informer les abonnés et les particuliers concernés, si cet opérateur n'a pas déjà averti l'abonné ou le particulier de la violation de données à caractère personnel, l'Institut peut, à la demande de l'autorité de protection des données, après avoir examiné les effets potentiellement négatifs de cette violation, exiger qu'il s'exécute.

La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel.

beschermingsmaatregelen of oplossingen die de gebruikers kunnen toepassen, alsook over de maatregelen die hij heeft genomen of overweegt te nemen.

Het Instituut kan de gevallen preciseren waarin informatie moet worden verstrekt alsook de nadere regels voor die kennisgeving.

§ 2. In geval van inbreuk in verband met persoonsgegevens verwittigt de operator van elektronische-communicatiediensten onverwijld de gegevensbeschermingsautoriteit, die onverwijld het Instituut verwittigt.

Indien de inbreuk in verband met persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor de persoonsgegevens of persoonlijke levenssfeer van een abonnee of een individueel persoon, stelt de operator van elektronische-communicatiediensten onverwijld ook de betrokken abonnee of individuele persoon in kennis van de inbreuk.

De gegevensbeschermingsautoriteit gaat na of de operator deze verplichting nakomt en brengt het Instituut op de hoogte wanneer ze van oordeel is dat dit niet het geval is.

De kennisgeving van een inbreuk in verband met persoonsgegevens aan een betrokken abonnee of individuele persoon is niet vereist wanneer de operator van elektronische-communicatiediensten tot voldoening van het Instituut heeft aangetoond dat hij de gepaste technologische beschermingsmaatregelen heeft genomen en dat deze maatregelen werden toegepast op de data die bij de beveiligingsinbreuk betrokken waren. Dergelijke technologische beschermingsmaatregelen maken de gegevens onbegrijpelijk voor eenieder die geen recht op toegang daartoe heeft.

Onverminderd de verplichting van de operator van elektronische-communicatiediensten om de betrokken abonnees en individuele personen in kennis te stellen, indien deze operator de abonnee of individuele persoon niet reeds in kennis heeft gesteld van de inbreuk in verband met persoonsgegevens, kan het Instituut op verzoek van de gegevensbeschermingsautoriteit hem, na te hebben gezien of en welke ongunstige gevolgen uit de inbreuk voortvloeien, verzoeken dat te doen.

In de kennisgeving aan de abonnee of de individuele persoon worden ten minste de aard van de inbreuk in verband met persoonsgegevens, alsmede de contactpunten voor meer informatie vermeld, en worden er maatregelen aanbevolen om mogelijke negatieve gevolgen van de inbreuk in verband met persoonsgegevens te verlichten.

La notification faite à l'autorité de protection des données décrit en outre les conséquences de la violation de données à caractère personnel, et les mesures proposées ou prises par l'opérateur de services de communications électroniques pour y remédier.

§ 3. Sous réserve de mesures d'exécution techniques émanant de la Commission européenne conformément à l'article 4, point 5, de la directive 2002/58/CE, et après avis de l'autorité de protection des données, l'Institut peut adopter des lignes directrices et, le cas échéant, édicter des instructions précisant les circonstances dans lesquelles les opérateurs de services de communications électroniques sont tenus de notifier la violation de données à caractère personnel.

Sous réserve de mesures techniques d'application émanant de la Commission européenne conformément à l'article 4, point 5, de la directive 2002/58/CE, et après avis de l'Institut, l'autorité de protection des données peut adopter des lignes directrices et, le cas échéant, édicter des instructions précisant le format applicable à cette notification et sa procédure de transmission.

Les opérateurs de services de communications électroniques tiennent à jour un inventaire des violations de données à caractère personnel, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier, de sorte que l'autorité de protection des données et l'Institut puissent vérifier le respect des dispositions du paragraphe 2. Cet inventaire comprend uniquement les informations nécessaires à cette fin.

Art. 107/4. § 1^{er}. Le présent article s'applique sans préjudice des dispositions de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, notamment en ce qui concerne les pouvoirs de supervision accordés à l'autorité sectorielle ou au service d'inspection sectoriel.

§ 2. L'Institut peut donner des instructions contraignantes dans le cadre des articles 107/2, 107/3 ainsi que des articles 30 et 33 de la loi du [xx xxx xxxx] précitée à un fournisseur d'infrastructure numérique, y compris les mesures requises pour remédier à un incident de sécurité ou empêcher qu'un tel incident ne se produise lorsqu'une cybermenace importante a été identifiée, ainsi que les dates limites de mise en œuvre de ces instructions.

§ 3. Dans le cadre de la supervision des articles 107/2 et 107/3 ainsi que des articles 30 et 33 de la loi du [xx

De kennisgeving aan de gegevensbeschermingsautoriteit bevat bovendien een omschrijving van de gevolgen van de inbreuk in verband met persoonsgegevens en van de door de operator van elektronische-communicatiediensten voorgestelde of getroffen maatregelen om die inbreuk te verhelpen.

§ 3. Onder voorbehoud van technische uitvoeringsmaatregelen van de Europese Commissie overeenkomstig artikel 4, punt 5, van Richtlijn 2002/58/EG, en na advies van de gegevensbeschermingsautoriteit, kan het Instituut richtsnoeren aannemen en, waar nodig, instructies uitvaardigen betreffende de omstandigheden waarin de kennisgeving van de inbreuk in verband met persoonsgegevens door de operatoren van elektronische-communicatiediensten noodzakelijk is.

Onder voorbehoud van technische uitvoeringsmaatregelen van de Europese Commissie overeenkomstig artikel 4, punt 5, van Richtlijn 2002/58/EG, en na advies van het Instituut, kan de gegevensbeschermingsautoriteit richtsnoeren aannemen en, waar nodig, instructies uitvaardigen betreffende het voor deze kennisgeving toepasselijke formaat, alsmede de manier waarop de kennisgeving geschiedt.

De operatoren van elektronische-communicatiediensten houden een inventaris bij van inbreuken in verband met persoonsgegevens, onder meer met de feiten in verband met deze inbreuken, de gevolgen ervan en de herstelmaatregelen die zijn genomen, zodat de gegevensbeschermingsautoriteit en het Instituut kunnen nagaan of de bepalingen van paragraaf 2 werden nageleefd. Deze inventaris bevat uitsluitend de voor dit doel noodzakelijke gegevens.

Art. 107/4. § 1. Dit artikel is van toepassing onverminderd de bepalingen van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid met name voor wat betreft de toezichtsbevoegdheden verleend aan de sectorale overheid of de sectorale inspectiedienst.

§ 2. Het Instituut kan een aanbieder van digitale infrastructuur bindende instructies geven in het kader van artikelen 107/2 en 107/3 en van artikelen 30 en 33 van de bovengenoemd wet van [xx xxx xxxx], onder meer de maatregelen die nodig zijn om een beveiligingsincident op te lossen of te voorkomen wanneer een significante dreiging is vastgesteld, alsook het tijdschema voor de uitvoering van die instructies.

§ 3. In het kader van het toezicht op de artikelen 107/2 en 107/3 en van artikelen 30 en 33 van de wet

xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut peut soumettre le fournisseur d'infrastructure numérique à :

a) des inspections sur place et des contrôles à distance, y compris des contrôles aléatoires effectués par des professionnels formés;

b) des audits de sécurité réguliers et ciblés réalisés par un organisme indépendant ou par l'Institut;

c) des audits *ad hoc*;

d) des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération du fournisseur d'infrastructure numérique;

e) des demandes d'informations nécessaires à l'évaluation des mesures de gestion des risques en matière de cybersécurité adoptées par le fournisseur d'infrastructure numérique concerné;

f) des demandes d'accès à des données, à des documents et à toutes informations nécessaires à l'Institut pour l'accomplissement de ses tâches de supervision;

g) des demandes de preuves de la mise en oeuvre de politiques de cybersécurité, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants.

Les audits de sécurité ciblés visés au premier alinéa, point b), sont basés sur des évaluations des risques effectuées par l'Institut ou l'entité contrôlée, ou sur d'autres informations disponibles relatives aux risques.

Lorsque l'audit de sécurité visé à l'alinéa 1^{er}, point b) est effectué par un organisme indépendant, le fournisseur d'infrastructure numérique propose à l'Institut un ou plusieurs organismes pour accord. L'Institut donne son accord lorsque l'organisme indépendant est qualifié pour effectuer l'audit et est indépendant par rapport à le fournisseur d'infrastructure numérique. À défaut d'accord de l'Institut dans le délai qu'il a fixé lors de la demande, l'Institut désigne lui-même l'organisme indépendant. Ce dernier communique à l'Institut le rapport complet et les résultats de cet audit. Les coûts de l'audit sont à la charge du fournisseur d'infrastructure numérique, sauf lorsque l'Institut en décide autrement dans des cas dûment motivés.

van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, kan het Instituut de aanbieder van digitale infrastructuur onderwerpen aan:

a) inspecties ter plaatse en toezicht elders, met inbegrip van steekproefsgewijze controles, die worden uitgevoerd door daartoe opgeleide professionals;

b) regelmatige en gerichte beveiligingsaudits die worden uitgevoerd door het Instituut of door een onafhankelijke instantie;

c) ad-hocaudits;

d) beveiligingsscan op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria, indien nodig in samenwerking met de betrokken aanbieder van digitale infrastructuur;

e) verzoeken om informatie die nodig is om de door de betrokken aanbieder van digitale infrastructuur genomen maatregelen voor het beheer van cyberbeveiligingsrisico's;

f) verzoeken van alle gegevens, documenten en informatie die het Instituut nodig acht voor de uitoefening van haar toezichthoudende taken;

g) verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de respectieve onderliggende bewijzen.

De in het eerste lid, punt b), bedoelde gerichte beveiligingsaudits zijn gebaseerd op door het Instituut of de gecontroleerde entiteit verrichte risicobeoordelingen of op andere beschikbare risicogerelateerde informatie.

Wanneer de in het eerste lid, punt b) bedoelde beveiligingsaudit wordt uitgevoerd door een onafhankelijke instantie, dan stelt de aanbieder van digitale infrastructuur een of meer instanties ter goedkeuring aan het Instituut voor. Het Instituut geeft zijn akkoord wanneer de onafhankelijke instantie gekwalificeerd is om de audit uit te voeren en onafhankelijk is van de aanbieder van digitale infrastructuur. Bij uitblijven van een akkoord vanwege het Instituut binnen de termijn die het bij het verzoek heeft vastgesteld, wijst het Instituut zelf de onafhankelijke instantie aan. Deze laatste bezorgt aan het Instituut het volledige verslag en de resultaten van deze audit en de kosten van de audit zijn ten laste van de aanbieder van digitale infrastructuur, behalve in naar behoren gemoeteerde gevallen waarin het Instituut anders besluit.

Lorsqu'il exerce ses pouvoirs en vertu du paragraphe 1, point e), f) ou g), l'Institut précise la finalité de la demande et les informations exigées.

L'Institut peut fixer les modalités de la fourniture par le fournisseur d'infrastructure numérique des informations concernant l'analyse de risque.

À la demande de l'Institut, un fournisseur d'infrastructure numérique participe à un exercice relatif à la sécurité des réseaux et systèmes d'information ou organise un tel exercice.

À la demande de l'Institut et dans le cadre de la gestion des incidents de sécurité, un fournisseur d'infrastructure numérique communique à l'Institut un point de contact disponible en permanence.

§ 4. À la demande de l'Institut et pour enquêter sur un cas de non-conformité par rapport aux articles 30 et 33 de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ou à une mesure d'exécution ainsi que sur son effet sur la sécurité des réseaux et systèmes d'information, le fournisseur d'infrastructure numérique lui donne accès à tout élément de son réseau.

§ 5. Sans préjudice des compétences de l'autorité nationale de cybersécurité, l'Institut coordonne les initiatives relatives à la sécurité des réseaux publics de communications électroniques et des services de communications électroniques accessibles au public.

Il supervise la détection, l'observation et l'analyse des problèmes de sécurité, et peut fournir aux utilisateurs des informations en la matière.

§ 6. Le non-respect par un fournisseur d'infrastructure numérique du présent article ou d'une décision de l'Institut prise sur base du présent article peut faire l'objet des mesures ou amendes administratives visées dans le titre 4, chapitre 2 de la loi du [XX XXXX XXXX] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique."

Art. 89

À l'article 126/3, § 3, l), de la même loi, les mots "essentiels des fournisseurs de service essentiels désignés sur la base de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes

Bij de uitoefening van zijn bevoegdheden uit hoofde van lid 1, punt e), f) of g), vermeldt het Instituut het doel van het verzoek en de gevraagde informatie.

Het Instituut kan bepalen op welke wijze de aanbieder van digitale infrastructuur informatie over de risicoanalyse moet verstrekken.

Op verzoek van het Instituut neemt een aanbieder van digitale infrastructuur deel aan een oefening in verband met de beveiliging van de netwerk- en informatiesystemen of organiseert hij een dergelijke oefening.

Op verzoek van het Instituut en in het kader van het beheer van beveiligingsincidenten, deelt een aanbieder van digitale infrastructuur het Instituut een contactpersoon mee die steeds bereikbaar is.

§ 4. Op verzoek van het Instituut en om een onderzoek in te stellen naar een geval van niet-conformiteit met de artikelen 30 en 33 van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, of met een uitvoeringsmaatregel, alsook naar de gevolgen ervan voor de beveiliging van netwerk- en informatiesystemen, geeft de aanbieder van digitale infrastructuur het Instituut toegang tot alle elementen van zijn netwerk.

§ 5. Onverminderd de bevoegdheden van de nationale cyberbeveiligingsautoriteit coördineert het Instituut de initiatieven rond de beveiliging van openbare elektronische-communicatienetwerken en openbare elektronische-communicatiediensten.

Het ziet toe op het opsporen, observeren en analyseren van beveiligingsproblemen, en kan de gebruikers hierover informatie verstrekken.

§ 6. Indien een aanbieder van digitale infrastructuur dit artikel of een op grond van dit artikel genomen beslissing van het Instituut niet naleeft, kunnen de in titel 4, hoofdstuk 2, van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid van de NIS2-wet bedoelde administratieve maatregelen of geldboetes worden opgelegd."

Art. 89

In artikel 126/3, § 3, l), van dezelfde wet worden de woorden "essentiële diensten van aanbieders van essentiële diensten ondersteunen aangeduid op basis van de wet van 7 april 2019 tot vaststelling van een kader

d'information d'intérêt général pour la sécurité publique" sont remplacés par les mots "des entités essentielles au sens de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique".

Art. 90

À l'article 164/1 de la même loi, les modifications suivantes sont apportées:

1° les mots "bureau d'enregistrement de noms de domaine Internet du domaine de premier niveau" sont remplacés par les mots "registre de noms de domaine de premier niveau du domaine de premier niveau";

2° au 4°, les mots "bureau d'enregistrement des noms de domaine" sont remplacés par les mots "registre de noms de domaine de premier niveau".

3° au 4°, les mots "bureau d'enregistrement des noms de domaine Internet" sont remplacés par les mots "registre de noms de domaine de premier niveau";

4° au 5°, dans le texte en néerlandais, le mot "topniveaudomein" est remplacé par le mot "topleveldomein".

Art. 91

À l'article 164/2 de la même loi, les modifications suivantes sont apportées:

1° les mots "bureau d'enregistrement de noms de domaine Internet" sont chaque fois remplacés par les mots "registre de noms de domaine de premier niveau";

2° dans le texte en néerlandais, le mot "topniveaudomein" est à chaque fois remplacé par le mot "topleveldomein".

Art. 92

Dans le titre VI, chapitre 3, de la même loi, il est inséré un article 164/3, rédigé comme suit:

"Art. 164/3. § 1^{er}. Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine collectent les données d'enregistrement de noms de domaine et

voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid" vervangen door de woorden "diensten van essentiële entiteiten in de zin van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid".

Art. 90

In artikel 164/1 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de woorden "Internetdomeinnaamregistreerbureau van het topniveaudomein" worden vervangen door de woorden "register voor topleveldomeinnamen van het topleveldomein";

2° in de bepaling onder 4° wordt het woord "domeinnaamregistreerbureau" vervangen door de woorden "register voor topleveldomeinnamen";

3° in de bepaling onder 4° wordt het woord "Internetdomeinnaamregistreerbureau" vervangen door de woorden "register voor topleveldomeinnamen";

4° in de bepaling onder 5°, in de Nederlandse tekst, wordt het woord "topniveaudomein" vervangen door het woord "topleveldomein".

Art. 91

In artikel 164/2 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de woorden "Internetdomeinnaamregistreerbureau" worden vervangen door de woorden "register voor topleveldomeinnamen";

2° in de Nederlandse tekst wordt het woord "topniveaudomein" vervangen door het woord "topleveldomein".

Art. 92

In titel VI, hoofdstuk 3, van dezelfde wet, wordt een artikel 164/3 ingevoegd, luidende:

"Art. 164/3. § 1. Registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, verzamelen met de nodige zorgvuldigheid nauwkeurige en volledige domeinnaamregistratiegegevens en houden

les maintiennent exactes et complètes au sein d'une base de données spécialisée conformément au droit de l'Union en matière de protection des données à caractère personnel.

§ 2. Les données d'enregistrement de noms de domaine visées à l'alinéa 1^{er} contiennent les informations nécessaires pour identifier et contacter les titulaires des noms de domaine et les points de contact qui gèrent les noms de domaine relevant des domaines de premier niveau. Ces informations comprennent au moins les éléments suivants:

1° le nom de domaine;

2° la date d'enregistrement;

3° le nom du titulaire de nom de domaine, son adresse de courrier électronique et son numéro de téléphone;

4° l'adresse de courrier électronique et le numéro de téléphone permettant de contacter le point de contact qui gère le nom de domaine, si ces coordonnées sont différentes de celles du titulaire.

Après avis de l'Institut, le Roi peut ordonner aux fournisseurs et aux revendeurs de services d'anonymisation ou d'enregistrement fiduciaire de partager les données d'enregistrement de noms de domaine avec les bureaux d'enregistrement et en définir les modalités.

Le respect des obligations visées au présent article n'entraîne pas de répétition inutile de la collecte des données d'enregistrement de noms de domaine auprès de la personne concernée. À cet effet, les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine coopèrent entre eux.

Après avis de l'Institut, le Roi peut préciser les modalités de cette coopération.

§ 2. Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine mettent en place des politiques et des procédures, notamment des procédures de vérification, visant à garantir que les bases de données visées au paragraphe 1^{er}, alinéa 1^{er}, contiennent des informations exactes et complètes. Ces politiques et procédures sont mises à la disposition du public.

Si les données d'enregistrement de noms de domaine énumérées au paragraphe 1^{er}, alinéa 2, d'un nom de domaine sont incorrectes, inexactes ou incomplètes, les registres de noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms

deze bij in een speciale database overeenkomstig het Unierecht inzake de bescherming van persoonsgegevens.

§ 2. De domeinregistratiegegevens bedoeld in het eerste lid bevatten de noodzakelijke informatie om de houders van de domeinnamen en de contactpunten die de domeinnamen onder de topleveldomeinnamen beheren, te identificeren en te contacteren. Die informatie omvat ten minste:

1° de domeinnaam;

2° de registratiedatum;

3° de naam van de houder van de domeinnaam, zijn e-mailadres en zijn telefoonnummer van;

4° het e-mailadres en het telefoonnummer van het contactpunt dat de domeinnaam beheert, indien deze verschillen van die van de houder van de domeinnaam.

De Koning kan, na advies van het Instituut, aanbieders van privacy- of proxy-registratiediensten en wederverkopers gelasten de domeinnaamregistratiegegevens die ze hebben verzameld te delen met de registrators, en de modaliteiten daarvan bepalen.

De naleving van de in dit artikel vastgestelde verplichtingen mag er niet toe leiden dat domeinnaamregistratiegegevens tweemaal worden verzameld bij de betrokkene. Daartoe werken registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, met elkaar samen.

De Koning kan, na advies van het Instituut, de modaliteiten van deze samenwerking preciseren.

§ 2. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, beschikken over beleidslijnen en procedures, waaronder verificatieprocedures, om ervoor te zorgen dat de in paragraaf 1, eerste lid, bedoelde databases juiste en volledige informatie bevatten. Deze beleidslijnen en procedures worden openbaar gemaakt.

Wanneer de domeinnaamregistratiegegevens opgesomd in paragraaf 1, tweede lid, van een domeinnaam onjuist, onnauwkeurig of onvolledig zijn, blokkeren de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen onmiddellijk

de domaine bloquent immédiatement le fonctionnement de ce nom de domaine jusqu'à ce que le titulaire du nom de domaine corrige les données d'enregistrement pour qu'elles deviennent correctes, exactes et complètes.

Si le titulaire du nom de domaine ne le fait pas dans le délai fixé par le registre des noms de domaine de premier niveau ou par l'entité fournissant des services d'enregistrement de nom de domaine, le nom de domaine est annulé.

Le transfert d'un nom de domaine bloqué à une autre entité fournissant des services d'enregistrement de noms de domaine est interdit.

§ 3. Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine rendent publiques, sans retard injustifié après l'enregistrement d'un nom de domaine, les données d'enregistrement du nom de domaine qui ne sont pas des données à caractère personnel.

§ 4. Sur demande dûment motivée, les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine fournissent gratuitement les données énumérées au paragraphe 1^{er}, alinéa 2, aux demandeurs d'accès légitimes, sans retard injustifié et en tout état de cause dans un délai de 72 heures après réception de toute demande d'accès, ou 24 heures après réception de toute demande d'accès en cas d'urgence.

Les demandeurs d'accès légitimes comprennent toute personne physique ou morale qui formule une demande d'examen, de constatation, d'exercice ou de défense de dispositions pénales, civiles ou autres du droit de l'Union ou du droit belge.

Sont considérés comme demandeurs d'accès légitimes:

1° toute personne dans le cadre de violations des droits de propriété intellectuelle ou des droits voisins;

2° l'Institut;

3° le CCB;

4° le CSIRT national;

5° les services de police;

6° les autorités judiciaires;

7° les services de renseignement et de sécurité;

het functioneren van deze domeinnaam tot de houder van de domeinnaam de registratiegegevens corrigeert zodat deze juist, nauwkeurig en volledig worden.

Indien de houder van de domeinnaam nalaat om dit te doen binnen de termijn zoals bepaald door het register voor topleveldomeinnamen of door de entiteit die domeinnaamregistratiediensten verleent, wordt de domeinnaam geannuleerd.

De transfer van een geblokkeerde domeinnaam naar een andere entiteit die domeinnaamregistratiediensten verleent, is verboden.

§ 3. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, maken de domeinnaamregistratiegegevens die geen persoonsgegevens zijn, onverwijld openbaar na de registratie van een domeinnaam.

§ 4. Op naar behoren gemotiveerd verzoek, verschaffen de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, kosteloos, aan de legitieme toegangsvragende partijen, de gegevens opgesomd in paragraaf 1, tweede lid, onverwijld en in elk geval binnen 72 uur na ontvangst van het verzoek, of 24 uur na ontvangst van het verzoek ingeval van hoogdringendheid.

Legitieme toegangsvragende partijen omvatten elke natuurlijke of rechtspersoon die een verzoek indient voor het onderzoeken, vaststellen, uitoefenen of verdedigen van strafrechtelijke, burgerrechtelijke of andere bepalingen in het Unierecht of Belgisch recht.

Als legitieme toegangsvragende partij worden beschouwd:

1° elke persoon in het kader van inbreuken op intellectuele eigendomsrechten of naburige rechten;

2° het Instituut;

3° het CCB;

4° het nationale CSIRT;

5° de politiediensten;

6° de gerechtelijke overheden;

7° de inlichtingen-en veiligheidsdiensten;

8° le SPF Économie;

9° le SPF Finances.

Après avis de l'Institut, le Roi peut ajouter à cette liste des demandeurs d'accès légitimes supplémentaires.

Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine, offrent au demandeur la possibilité d'introduire aisément sa demande.

Il est question d'urgence si l'utilisation d'un nom de domaine peut conduire à des situations de danger de mort et/ou à des dommages irréparables.

Tout refus d'une demande dûment motivée est motivé.

Les politiques et procédures de divulgation de ces données sont rendues publiques.

Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine ne peuvent pas informer le titulaire d'un nom de domaine lorsqu'une demande visée à l'alinéa 1^{er} a été formulée.

§ 5. L'Institut peut donner des instructions contraignantes à un registre de noms de domaine de premier niveau ou à une entité fournissant des services d'enregistrement de noms de domaine, en vue du respect du présent article.

§ 6. Si un registre de noms de domaine de premier niveau ou une entité fournissant des services d'enregistrement de noms de domaine ne respecte pas le présent article, un arrêté royal adopté en vertu du présent article ou une instruction contraignante émise par l'Institut, l'Institut peut imposer les mesures ou amendes administratives visées au chapitre 2 de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique."

8° de FOD Economie;

9° de FOD Financiën.

De Koning kan, na advies van het Instituut, bijkomende legitieme toegangsvragende partijen aan deze lijst toevoegen.

De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, stellen de verzoeker in staat om gemakkelijk, zijn verzoek in te dienen.

Er is sprake van hoogdringendheid indien het gebruik van een domeinnaam kan leiden tot levensbedreigende situaties en/of onherstelbare schade.

Elke weigering van een naar behoren gemotiveerd verzoek wordt gemotiveerd.

Het beleid en de procedures met betrekking tot de bekendmaking van deze gegevens worden openbaar gemaakt.

De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, mogen de houder van een domeinnaam niet op de hoogte brengen wanneer een verzoek zoals bedoeld in het eerste lid werd ingediend.

§ 5. Het Instituut kan een register voor topleveldomeinnamen of een entiteit die domeinnaamregistratiediensten verleent bindende instructies geven met het oog op de naleving van dit artikel.

§ 6. Indien een register voor topleveldomeinnamen of een entiteit die domeinnaamregistratiediensten verleent dit artikel, een in uitvoering van dit artikel aangenomen koninklijk besluit of een bindende instructie van het Instituut niet naleeft, kan het Instituut de in hoofdstuk 2 van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid bedoelde administratieve maatregelen of geldboetes opleggen."

Section 6

Modifications de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la directive 2014/65/UE

Art. 93

À l'article 71 de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la directive 2014/65/UE, modifié par la loi du 7 avril 2019, les mots "et du titre 2 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique. Pour l'exécution des missions précitées concernant la loi du 7 avril 2019, la FSMA peut néanmoins charger un prestataire externe spécialisé de l'exécution de tâches déterminées de contrôle ou obtenir l'assistance d'un tel prestataire" sont supprimés.

Art. 94

L'article 79, § 4, de la même loi, inséré par la loi du 7 avril 2019, est abrogé.

CHAPITRE 3**Disposition abrogatoire****Art. 95**

La loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique est abrogée.

Afdeling 6

Wijzigingen van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU

Art. 93

In artikel 71 van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU, gewijzigd bij de wet van 7 april 2019, worden de woorden "en van titel 2 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid. Voor de uitvoering van de voormelde opdrachten betreffende de wet van 7 april 2019 kan de FSMA niettemin een gespecialiseerde externe dienstverlener belasten met de uitvoering van welbepaalde toezichtopdrachten of de bijstand van een dergelijke dienstverlener verkrijgen" geschrapt.

Art. 94

Artikel 79, § 4, van dezelfde wet, ingevoegd bij de wet van 7 april 2019, wordt opgeheven.

HOOFDSTUK 3**Opheffingsbepaling****Art. 95**

De wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid wordt opgeheven.

CHAPITRE 4

Entrée en vigueur

Art. 96

La présente loi entre en vigueur le 18 octobre 2024.

Donné à Bruxelles, le 3 mars 2024.

PHILIPPE

PAR LE ROI:

Le premier ministre,

Alexander De Croo

La ministre de l'Intérieur,

Annelies Verlinden

HOOFDSTUK 4

Inwerkingtreding

Art. 96

Deze wet treedt in werking op 18 oktober 2024.

Gegeven te Brussel, 3 maart 2024.

FILIP

VAN KONINGSWEGE:

De eerste minister,

Alexander De Croo

De minister van Binnenlandse Zaken,

Annelies Verlinden

Annexe I à la loi du ... établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique		
Annexe I – Secteurs hautement critiques		
Secteur	Sous-secteur	Type d'entité
1. Énergie	a) Électricité	- Entreprises d'électricité au sens de l'article 2, point 57), de la directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE, qui remplissent la fonction de «fourniture» au sens de l'article 2, point 12), de ladite directive
		- Gestionnaires de réseau de distribution au sens de l'article 2, point 29), de la directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE
		- Gestionnaires de réseau de transport au sens de l'article 2, point 35), de la directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE
		- Producteurs au sens de l'article 2, point 38), de la directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE
		- Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8), du règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité
		- Acteurs du marché au sens de l'article 2, point 25), du règlement (UE) 2019/943 fournissant des services d'agrégation, de participation active de la demande ou de stockage d'énergie au sens de l'article 2, points 18), 20) et 59), de la directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE
		- Exploitants d'un point de recharge qui sont responsables de la gestion et de l'exploitation d'un point de recharge, lequel fournit un service de recharge aux utilisateurs finals, y compris au nom et pour le compte d'un prestataire de services de mobilité

	b) Réseau de chaleur et de froid	- Opérateurs de réseaux de chaleur ou de réseaux de froid au sens de l'article 2, point 19), de la directive (UE) 2018/2001 du Parlement européen et du Conseil du 11 décembre 2018 relative à la promotion de l'utilisation de l'énergie produite à partir de sources renouvelables
	c) Pétrole	- Exploitants d'oléoducs
		- Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
		- Entités centrales de stockage au sens de l'article 2, point f), de la directive 2009/119/CE du Conseil du 14 septembre 2009 faisant obligation aux États membres de maintenir un niveau minimal de stocks de pétrole brut et/ou de produits pétroliers
	d) Gaz	- Entreprises de fourniture au sens de l'article 2, point 8, de la directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE
		- Gestionnaires de réseau de distribution au sens de l'article 2, point 6, de la directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE
		- Gestionnaires de réseau de transport au sens de l'article 2, point 4, de la directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE
		- Gestionnaires d'installation de stockage au sens de l'article 2, point 10, de la directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE
		- Gestionnaires d'installation de GNL au sens de l'article 2, point 12, de la directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE
		- Entreprises de gaz naturel au sens de l'article 2, point 1, de la directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE

		- Exploitants d'installations de raffinage et de traitement de gaz naturel
	e) Hydrogène	- Exploitants de systèmes de production, de stockage et de transport d'hydrogène
2. Transports	a) Transports aériens	- Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) no 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n° 2320/2002, utilisés à des fins commerciales
		- Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires, aéroports au sens de l'article 2, point 1), de ladite directive, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision n° 661/2010/UE, et entités exploitant les installations annexes se trouvant dans les aéroports
		- Services du contrôle de la circulation aérienne au sens de l'article 2, point 1), du règlement (CE) n° 549/2004 du Parlement européen et du Conseil du 10 mars 2004 fixant le cadre pour la réalisation du ciel unique européen
	b) Transports ferroviaires	- Gestionnaires de l'infrastructure au sens de l'article 3, point 2), de la directive 2012/34/UE du Parlement européen et du Conseil du 21 novembre 2012 établissant un espace ferroviaire unique européen
		- Entreprises ferroviaires au sens de l'article 3, point 1), de la directive 2012/34/UE du Parlement européen et du Conseil du 21 novembre 2012 établissant un espace ferroviaire unique européen, y compris les exploitants d'installation de service au sens de l'article 3, point 12), de ladite directive
	c) Transports par eau	- Sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret, telles qu'elles sont définies pour le domaine du transport maritime à l'annexe I du règlement (CE) n° 725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires, à l'exclusion des navires exploités à titre individuel par ces sociétés

		- Entités gestionnaires des ports au sens de l'article 3, point 1), de la directive 2005/65/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à l'amélioration de la sûreté des ports, y compris les installations portuaires au sens de l'article 2, point 11), du règlement (CE) n° 725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires, ainsi que les entités exploitant des infrastructures et des équipements à l'intérieur des ports - Exploitants de services de trafic maritime (STM) au sens de l'article 3, point o), de la directive 2002/59/CE du Parlement européen et du Conseil du 27 juin 2002 relative à la mise en place d'un système communautaire de suivi du trafic des navires et d'information, et abrogeant la directive 93/75/CEE du Conseil
	d) Transports routiers	- Autorités routières au sens de l'article 2, point 12), du règlement délégué (UE) 2015/962 de la Commission du 18 décembre 2014 complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne la mise à disposition, dans l'ensemble de l'Union, de services d'informations en temps réel sur la circulation, chargées du contrôle de la gestion de la circulation, à l'exclusion des entités publiques pour lesquelles la gestion de la circulation ou l'exploitation de systèmes de transport intelligents constituent une partie non essentielle de leur activité générale - Exploitants de systèmes de transport intelligents au sens de l'article 4, point 1), de la directive 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport
	3. Secteur bancaire	- Établissements de crédit au sens de l'article 4, point 1), du règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012
4. Infrastructures des marchés financiers		- Exploitants de plates-formes de négociation au sens de l'article 4, point 24), de la directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés

		d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE - Contreparties centrales au sens de l'article 2, point 1), du règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux
5. Santé		- Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers - Laboratoires de référence de l'Union européenne visés à l'article 15 du règlement (UE) 2022/2371 du Parlement européen et du Conseil du 23 novembre 2022 concernant les menaces transfrontières graves pour la santé et abrogeant la décision n° 1082/2013/UE - Entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1^{er}, point 2, de la directive 2001/83/CE du Parlement européen et du Conseil du 6 novembre 2001 instituant un code communautaire relatif aux médicaments à usage humain - Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de l'annexe I, section C, division 21 du Règlement (CE) n° 1893/2006 du Parlement européen et du Conseil du 20 décembre 2006 établissant la nomenclature statistique des activités économiques NACE Rév. 2 et modifiant le règlement (CEE) n° 3037/90 du Conseil ainsi que certains règlements (CE) relatifs à des domaines statistiques spécifiques - Entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique (liste des dispositifs médicaux critiques en cas d'urgence de santé publique) au sens de l'article 22 du règlement (UE) 2022/123 du Parlement européen et du Conseil du 25 janvier 2022 relatif à un rôle renforcé de l'Agence européenne des médicaments dans la préparation aux crises et la gestion de celles-ci en ce qui concerne les médicaments et les dispositifs médicaux
6. Eau potable		- Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) a), de la directive (UE) 2020/2184 du

		Parlement européen et du Conseil du 16 décembre 2020 relative à la qualité des eaux destinées à la consommation humaine, à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine constitue une partie non essentielle de leur activité générale de distribution d'autres produits et biens
7. Eaux usées		- Entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, les eaux ménagères usées ou les eaux industrielles usées au sens de l'article 2, points 1), 2) et 3), de la directive 91/271/CEE du Conseil, du 21 mai 1991, relative au traitement des eaux urbaines résiduaires, à l'exclusion des entreprises pour lesquelles la collecte, l'évacuation ou le traitement des eaux urbaines résiduaires, des eaux ménagères usées ou des eaux industrielles usées constituent une partie non essentielle de leur activité générale
8. Infrastructure numérique		- Fournisseurs de points d'échange internet
		- Fournisseurs de services DNS, à l'exclusion des opérateurs de serveurs racines de noms de domaine
		- Registres de noms de domaine de premier niveau
		- Fournisseurs de services d'informatique en nuage
		- Fournisseurs de services de centres de données
		- Fournisseurs de réseaux de diffusion de contenu
		- Prestataires de services de confiance
		- Fournisseurs de réseaux de communications électroniques publics
9. Gestion des services TIC (interentreprises)		- Fournisseurs de services gérés
		- Fournisseurs de services de sécurité gérés
10. Administration publique		- Entités de l'administration publique qui dépendent de l'État fédéral
		- Entités de l'administration publique qui dépendent des entités fédérées, identifiés conformément à l'article 11, § 2, de la loi
		- Les zones de secours au sens de l'article 14 de la loi du 15 mai 2007 relative à la sécurité civile ou le Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale créé par l'ordonnance du 19 juillet 1990 portant création d'un Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale

11. Espace		- Exploitants d'infrastructures terrestres, détenues, gérées et exploitées par des États membres ou par des parties privées, qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics

Vu pour être annexé à la loi du ... établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

Bruxelles, le 3 mars 2024

PHILIPPE

Par le Roi :

Le Premier Ministre,

A. DE CROO

La Ministre de l'Intérieur,

A. VERLINDEN

Annexe II à la loi du ... établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique		
Annexe II - Autres secteurs critiques		
Secteur	Sous-secteur	Type d'entité
1. Services postaux et d'expédition		- Prestataires de services postaux au sens de l'article 2, point 1 bis), de la directive 97/67/CE du Parlement Européen et du Conseil du 15 décembre 1997 concernant des règles communes pour le développement du marché intérieur des services postaux de la Communauté et l'amélioration de la qualité du service, y compris les prestataires de services d'expédition
2. Gestion des déchets		- Entreprises exécutant des opérations de gestion des déchets au sens de l'article 3, point 9), de la directive 2008/98/CE du Parlement européen et du Conseil du 19 novembre 2008 relative aux déchets et abrogeant certaines directives, à l'exclusion des entreprises pour lesquelles la gestion des déchets n'est pas la principale activité économique
3. Fabrication, production et distribution de produits chimiques		- Entreprises procédant à la fabrication de substances et à la distribution de substances ou de mélanges au sens de l'article 3, points 9 et 14, du règlement (CE) n° 1907/2006 du Parlement européen et du Conseil du 18 décembre 2006 concernant l'enregistrement, l'évaluation et l'autorisation des substances chimiques, ainsi que les restrictions applicables à ces substances (REACH), instituant une agence européenne des produits chimiques, modifiant la directive 1999/45/CE et abrogeant le règlement (CEE) n° 793/93 du Conseil et le règlement (CE) n° 1488/94 de la Commission ainsi que la directive 76/769/CEE du Conseil et les directives 91/155/CEE, 93/67/CEE, 93/105/CE et 2000/21/CE de la Commission et entreprises procédant à la production d'articles au sens de l'article 3, point 3), dudit règlement, à partir de substances ou de mélanges
4. Production, transformation et distribution des denrées alimentaires		- Entreprises du secteur alimentaire au sens de l'article 3, point 2), du règlement (CE) n° 178/2002 du Parlement européen et du Conseil du 28 janvier 2002 établissant les principes généraux et les prescriptions générales de la législation alimentaire, instituant l'Autorité européenne de sécurité des aliments et fixant des procédures relatives à la sécurité des denrées alimentaires qui exercent des activités de distribution en gros ainsi

		que de production et de transformation industrielles
5. Fabrication	a) Fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro	- Entités fabriquant des dispositifs médicaux au sens de l'article 2, point 1), du règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE et entités fabriquant des dispositifs médicaux de diagnostic in vitro au sens de l'article 2, point 2), du règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission, à l'exception des entités fabriquant des dispositifs médicaux mentionnés à l'annexe I, point 5, cinquième tiret, de la présente directive
	b) Fabrication de produits informatiques, électroniques et optiques	- Entreprises exerçant l'une des activités économiques visées à l'annexe I, section C, division 26 du Règlement (CE) n° 1893/2006 du Parlement européen et du Conseil du 20 décembre 2006 établissant la nomenclature statistique des activités économiques NACE Rév. 2 et modifiant le règlement (CEE) n° 3037/90 du Conseil ainsi que certains règlements (CE) relatifs à des domaines statistiques spécifiques
	c) Fabrication d'équipements électriques	- Entreprises exerçant l'une des activités économiques visées à l'annexe I, section C, division 27 du Règlement (CE) n° 1893/2006 du Parlement européen et du Conseil du 20 décembre 2006 établissant la nomenclature statistique des activités économiques NACE Rév. 2 et modifiant le règlement (CEE) n° 3037/90 du Conseil ainsi que certains règlements (CE) relatifs à des domaines statistiques spécifiques
	d) Fabrication de machines et équipements n.c.a.	- Entreprises exerçant l'une des activités économiques visées à l'annexe I, section C, division 28 du Règlement (CE) n° 1893/2006 du Parlement européen et du Conseil du 20 décembre 2006 établissant la nomenclature statistique des activités économiques NACE Rév. 2 et modifiant le règlement (CEE) n° 3037/90 du Conseil ainsi que certains règlements (CE) relatifs à des domaines statistiques spécifiques
	e) Construction de véhicules automobiles, remorques et semi-remorques	- Entreprises exerçant l'une des activités économiques visées à l'annexe I, section C, division 29 du Règlement (CE) n° 1893/2006 du Parlement européen et du Conseil du 20 décembre 2006 établissant la nomenclature statistique des

		activités économiques NACE Rév. 2 et modifiant le règlement (CEE) n° 3037/90 du Conseil ainsi que certains règlements (CE) relatifs à des domaines statistiques spécifiques
	f) Fabrication d'autres matériels de transport	- Entreprises exerçant l'une des activités économiques visées à l'annexe I, section C, division 30 du Règlement (CE) n° 1893/2006 du Parlement européen et du Conseil du 20 décembre 2006 établissant la nomenclature statistique des activités économiques NACE Rév. 2 et modifiant le règlement (CEE) n° 3037/90 du Conseil ainsi que certains règlements (CE) relatifs à des domaines statistiques spécifiques
6. Fournisseurs numériques		- Fournisseurs de places de marché en ligne
		- Fournisseurs de moteurs de recherche en ligne
		- Fournisseurs de plateformes de services de réseaux sociaux
7. Recherche		- Organismes de recherche

Vu pour être annexé à la loi du ... établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

Bruxelles, le 3 mars 2024

PHILIPPE

Par le Roi :

Le Premier Ministre,

A. DE CROO

La Ministre de l'Intérieur,

A. VERLINDEN

Bijlage I bij de wet van ... tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid		
Bijlage I - Zeer kritieke sectoren		
Sector	Deelsector	Soort entiteit
1. Energie	a) Elektriciteit	- Elektriciteitsbedrijven zoals gedefinieerd in artikel 2, punt 57, van Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU, die de functie verrichten van “levering” zoals gedefinieerd in artikel 2, punt 12, van die richtlijn
		- Distributiesysteembeheerders zoals gedefinieerd in artikel 2, punt 29, van Richtlijn (EU) 2019/944 van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU
		- Transmissiesysteembeheerders zoals gedefinieerd in artikel 2, punt 35, van Richtlijn (EU) 2019/944 van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU
		- Producenten zoals gedefinieerd in artikel 2, punt 38, van Richtlijn (EU) 2019/944 van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU
		- Benoemde elektriciteitsmarktbeheerders zoals gedefinieerd in artikel 2, punt 8, van Verordening (EU) 2019/943 van het Europees Parlement en de Raad
		- Marktdeelnemers zoals gedefinieerd in artikel 2, punt 25, van Verordening (EU) 2019/943 van het Europees Parlement en de Raad van 5 juni 2019 betreffende de interne markt voor elektriciteit, die aggregatie verrichten of vraagrespons- of energieopslagdiensten verstrekken zoals gedefinieerd in artikel 2, punten 18, 20 en 59, van Richtlijn (EU) 2019/944 van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU
		- Exploitanten van een laadpunt die verantwoordelijk zijn voor het beheer en de exploitatie van een laadpunt dat een laaddienst levert aan eindgebruikers, onder meer namens en

		voor rekening van een aanbieder van mobiliteitsdiensten
	b) Stadsverwarming en -koeling	- Exploitanten van stadsverwarming of stadskoeling zoals gedefinieerd in artikel 2, punt 19, van Richtlijn (EU) 2018/2001 van het Europees Parlement en de Raad van 11 december 2018 ter bevordering van het gebruik van energie uit hernieuwbare bronnen
	c) Aardolie	- Exploitanten van oliepijpleidingen - Exploitanten van voorzieningen voor de productie, raffinage en behandeling van olie, opslag en transport - Centrale entiteiten voor de voorraadvorming zoals gedefinieerd in artikel 2, punt f), van Richtlijn 2009/119/EG van de Raad van 14 september 2009 houdende verplichting voor de lidstaten om minimumvoorraden ruwe aardolie en/of aardolieproducten in opslag te houden
	d) Aardgas	- Leveringsbedrijven zoals gedefinieerd in artikel 2, punt 8, van Richtlijn 2009/73/EG van het Europees Parlement en de Raad van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor aardgas en tot intrekking van Richtlijn 2003/55/EG - Distributiesysteembeheerders zoals gedefinieerd in artikel 2, punt 6, van Richtlijn 2009/73/EG van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor aardgas en tot intrekking van Richtlijn 2003/55/EG - Transmissiesysteembeheerders zoals gedefinieerd in artikel 2, punt 4, van Richtlijn 2009/73/EG van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor aardgas en tot intrekking van Richtlijn 2003/55/EG - Opslagsysteembeheerders zoals gedefinieerd in artikel 2, punt 10, van Richtlijn 2009/73/EG van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor aardgas en tot intrekking van Richtlijn 2003/55/EG - LNG-systeembeheerders zoals gedefinieerd in artikel 2, punt 12, van Richtlijn 2009/73/EG van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor aardgas en tot intrekking van Richtlijn 2003/55/EG - Aardgasbedrijven zoals gedefinieerd in artikel 2, punt 1, van Richtlijn 2009/73/EG van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor aardgas en tot intrekking van Richtlijn 2003/55/EG

2. Vervoer		- Exploitanten van voorzieningen voor de raffinage en behandeling van aardgas
	e) Waterstof	- Exploitanten van voorzieningen voor de productie, opslag en transmissie van waterstof
	a) Lucht	- Luchtvaartmaatschappijen zoals gedefinieerd in artikel 3, punt 4, Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad van 11 maart 2008 inzake gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart en tot intrekking van Verordening (EG) nr. 2320/2002, die voor commerciële doeleinden worden gebruikt - Luchthavenbeheerders zoals gedefinieerd in artikel 2, punt 2, van Richtlijn 2009/12/EG van het Europees Parlement en de Raad van 11 maart 2009 inzake luchthavengelden, luchthavens als bedoeld in artikel 2, punt 1, van die richtlijn, met inbegrip van de kernluchthavens die in bijlage II, afdeling 2, bij Verordening (EU) 1315/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk en tot intrekking van Besluit nr. 661/2010/EU zijn opgenomen, alsook de entiteiten die bijbehorende installaties bedienen welke zich op luchthavens bevinden - Exploitanten op het gebied van verkeersbeheer en -controle die luchtverkeersleidingsdiensten zoals gedefinieerd in artikel 2, punt 1, van Verordening (EG) nr. 549/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot vaststelling van het kader voor de totstandbrenging van het gemeenschappelijke Europese luchtruim aanbieden
	b) Spoor	- Infrastructuurbeheerders zoals gedefinieerd in artikel 3, punt 2, van Richtlijn 2012/34/EU van het Europees Parlement en de Raad van 21 november 2012 tot instelling van één Europese spoorwegruimte - Spoorwegondernemingen zoals gedefinieerd in artikel 3, punt 1, van Richtlijn 2012/34/EU van 21 november 2012 tot instelling van één Europese spoorwegruimte, inclusief exploitanten van dienstvoorzieningen zoals gedefinieerd in artikel 3, punt 12, van die richtlijn
	c) Water	- Bedrijven voor vervoer over water (binnenvaart, kust- en zeevervoer) van passagiers en vracht, die in bijlage I bij Verordening (EG) nr. 725/2004 van het Europees Parlement en de Raad van 31 maart 2004 betreffende de verbetering van de beveiliging van schepen en havenfaciliteiten als

		bedrijven in maritiem vervoer worden gedefinieerd, met uitzondering van de door deze bedrijven geëxploiteerde individuele vaartuigen - Beheerders van havens zoals gedefinieerd in artikel 3, punt 1, van Richtlijn 2005/65/EG van het Europees Parlement en de Raad van 26 oktober 2005 betreffende het verhogen van de veiligheid van havens, inclusief hun havenfaciliteiten zoals gedefinieerd in artikel 2, punt 11, van Verordening (EG) nr. 725/2004 van het Europees Parlement en de Raad van 31 maart 2004 betreffende de verbetering van de beveiliging van schepen en havenfaciliteiten; alsook entiteiten die werken en uitrusting in havens beheren - Exploitanten van verkeersbegeleidingssystemen (VBS) zoals gedefinieerd in artikel 3, punt o), van Richtlijn 2002/59/EG van het Europees Parlement en de Raad van 27 juni 2002 betreffende de invoering van een communautair monitoring en informatiesysteem voor de zeescheepvaart en tot intrekking van Richtlijn 93/75/EEG van de Raad
	d) Weg	- Wegenautoriteiten zoals gedefinieerd in artikel 2, punt 12, van gedelegeerde Verordening (EU) 2015/962 van de Commissie van 18 december 2014 ter aanvulling van Richtlijn 2010/40/EU van het Europees Parlement en de Raad wat de verlening van EU-wijde realtimeverkeersinformatiediensten betreft die verantwoordelijk zijn voor het verkeersbeheer, met uitzondering van overheidsinstanties waarvoor verkeersbeheer of de exploitatie van intelligente vervoerssystemen slechts een niet-essentieel onderdeel van hun algemene activiteit is - Exploitanten van intelligente vervoerssystemen zoals gedefinieerd in artikel 4, punt 1, van Richtlijn 2010/40/EU van het Europees Parlement en de Raad van 7 juli 2010 betreffende het kader voor het invoeren van intelligente vervoerssystemen op het gebied van wegvervoer en voor interfaces met andere vervoerswijzen
3. Bankwezen		- Kredietinstellingen zoals gedefinieerd in artikel 4, punt 1, Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad van 26 juni 2013 betreffende prudentiële vereisten voor kredietinstellingen en beleggingsondernemingen en tot wijziging van Verordening (EU) nr. 648/2012
4. Infrastructuur voor de financiële markt		- Exploitanten van handelsplatformen zoals gedefinieerd in artikel 4, punt 24, van Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor

		financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU - Centrale tegenpartijen zoals gedefinieerd in artikel 2, punt 1, Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters
5. Gezondheidszorg		- Zorgaanbieders zoals gedefinieerd in artikel 3, punt g), van Richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg - EU-referentielaboratoria als bedoeld in artikel 15 van Verordening (EU) 2022/2371 van het Europees Parlement en de Raad van 23 november 2022 inzake ernstige grensoverschrijdende gezondheidsbedreigingen en tot intrekking van Besluit nr. 1082/2013/EU inzake ernstige grensoverschrijdende bedreigingen van de gezondheid - Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen zoals gedefinieerd in artikel 1, punt 2, van Richtlijn 2001/83/EG van het Europees Parlement en de Raad van 6 november 2001 tot vaststelling van een communautair wetboek betreffende geneesmiddelen voor menselijk gebruik - Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen als bedoeld in bijlage I, sectie C, afdeling 21, van Verordening (EG) nr. 1893/2006 van het Europees Parlement en de Raad van 20 december 2006 tot vaststelling van de statistische classificatie van economische activiteiten NACE Rev. 2 en tot wijziging van Verordening (EEG) nr. 3037/90 en enkele EG-verordeningen op specifieke statistische gebieden vervaardigen - Entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd ("de lijst van in een noodsituatie op het gebied van de volksgezondheid kritieke hulpmiddelen") in de zin van artikel 22 van Verordening (EU) 2022/123 van het Europees Parlement en de Raad van 25 januari 2022 betreffende een grotere rol van het Europees Geneesmiddelenbureau inzake crisisparaatheid en -beheersing op het gebied van geneesmiddelen en medische hulpmiddelen

6. Drinkwater		- Leveranciers en distributeurs van voor menselijke consumptie bestemd water zoals gedefinieerd in artikel 2, punt 1, a), van Richtlijn (EU) 2020/2184 van het Europees Parlement en de Raad van 16 december 2020 betreffende de kwaliteit van voor menselijke consumptie bestemd water, met uitzondering van distributeurs waarvoor de distributie van water voor menselijke consumptie een niet-essentieel deel is van hun algemene activiteit van distributie van andere waren en goederen die niet worden beschouwd als essentiële of belangrijke diensten
7. Afvalwater		- Ondernemingen die stedelijk afvalwater, huishoudelijk afvalwater of industrieel afvalwater zoals gedefinieerd in artikel 2, punten 1, 2 en 3, van Richtlijn 91/271/EEG van de Raad van 21 mei 1991 inzake de behandeling van stedelijk afvalwater opvangen, lozen of behandelen, met uitzondering van ondernemingen waarvoor het opvangen, lozen of behandelen van stedelijk afvalwater, huishoudelijk afvalwater of industrieel afvalwater een niet-essentieel onderdeel van hun algemene activiteit is
8. Digitale infrastructuur		- Aanbieders van internetknooppunten
		- DNS-dienstverleners, met uitzondering van exploitanten van root-naamservers
		- Registers voor topleveldomeinnamen
		- Aanbieders van cloudcomputingdiensten
		- Aanbieders van datacentrumdiensten
		- Aanbieders van netwerken voor de levering van inhoud
		- Verleners van vertrouwensdiensten
		- Aanbieders van openbare elektronische-communicatienetwerken
9. Beheer van ICT-diensten (business-to-business)		- Aanbieders van beheerde diensten
		- Aanbieders van beheerde beveiligingsdiensten
10. Overheid		- Overheidsinstanties die van de Federale Staat afhangen
		- Overheidsinstanties die van de deelgebieden afhangen, geïdentificeerd overeenkomstig artikel 11, § 2, van de wet
		- De hulpverleningszones in de zin van artikel 14 van de wet van 15 mei 2007 betreffende de civiele veiligheid of de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp opgericht door de ordonnantie van 19 juli 1990 houdende oprichting van de Brusselse

		Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp
11. Ruimtevaart		- Exploitanten van grondfaciliteiten die in het bezit zijn van of beheerd of geëxploiteerd worden door de lidstaten of door particuliere partijen en die de verlening van vanuit de ruimte opererende diensten ondersteunen, met uitzondering van aanbieders van openbare elektronische communicatienetwerken

Gezien om te worden gevoegd bij de wet van ... tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

Brussel, 3 maart 2024

FILIP

Van Koningswege:

De Eerste Minister,

A. DE CROO

De Minister van Binnenlandse Zaken,

A. VERLINDEN

Bijlage II bij de wet van ... tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid		
Bijlage II - Andere kritieke sectoren		
Sector	Deelsector	Soort entiteit
1. Post- en koeriersdiensten		- Aanbieders van postdiensten zoals gedefinieerd in artikel 2, punt 1 bis, van Richtlijn 97/67/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende gemeenschappelijke regels voor de ontwikkeling van de interne markt voor postdiensten in de Gemeenschap en de verbetering van de kwaliteit van de dienst, met inbegrip van aanbieders van koeriersdiensten
2. Afvalstoffenbeheer		- Ondernemingen die handelingen in het kader van afvalstoffenbeheer uitvoeren zoals gedefinieerd in artikel 3, punt 9, van Richtlijn 2008/98/EG van het Europees Parlement en de Raad van 19 november 2008 betreffende afvalstoffen en tot intrekking van een aantal richtlijnen, met uitzondering van ondernemingen waarvoor afvalstoffenbeheer niet de voornaamste economische activiteit is
3. Vervaardiging, productie en distributie van chemische stoffen		- Ondernemingen die stoffen vervaardigen en stoffen of mengsels distribueren als bedoeld in artikel 3, punten 9 en 14, van Verordening (EG) nr. 1907/2006 van het Europees Parlement en de Raad van 18 december 2006 inzake de registratie en beoordeling van en de autorisatie en beperkingen ten aanzien van chemische stoffen (REACH), tot oprichting van een Europees Agentschap voor chemische stoffen, houdende wijziging van Richtlijn 1999/45/EG en houdende intrekking van Verordening (EEG) nr. 793/93 van de Raad en Verordening (EG) nr. 1488/94 van de Commissie alsmede Richtlijn 76/769/EEG van de Raad en de Richtlijnen 91/155/EEG, 93/67/EEG, 93/105/EG en 2000/21/EG van de Commissie en ondernemingen die voorwerpen zoals gedefinieerd in artikel 3, punt 3, van die verordening produceren uit stoffen of mengsels
4. Productie, verwerking en distributie van levensmiddelen		- Levensmiddelenbedrijven zoals gedefinieerd in artikel 3, punt 2, Verordening (EG) nr. 178/2002 van het Europees Parlement en de Raad van 28 januari 2002 tot vaststelling van de algemene beginselen en voorschriften van de levensmiddelenwetgeving, tot oprichting van een Europese Autoriteit voor voedselveiligheid en tot vaststelling van procedures voor voedselveiligheidsaangelegenheden die zich

		bezighouden met groothandel en industriële productie en verwerking
5. Vervaardiging	a) Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek	- Entiteiten die medische hulpmiddelen zoals gedefinieerd in artikel 2, punt 1, van Verordening (EU) 2017/745 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen, tot wijziging van Richtlijn 2001/83/EG, Verordening (EG) nr. 178/2002 en Verordening (EG) nr. 1223/2009, en tot intrekking van Richtlijnen 90/385/EEG en 93/42/EEG van de Raad vervaardigen en entiteiten die medische hulpmiddelen voor in-vitrodiagnostiek zoals gedefinieerd in artikel 2, punt 2, van Verordening (EU) 2017/746 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen voor in-vitrodiagnostiek en tot intrekking van Richtlijn 98/79/EG en Besluit 2010/227/EU van de Commissie vervaardigen, met uitzondering van entiteiten die medische hulpmiddelen vervaardigen als bedoeld in bijlage I, punt 5, vijfde streepje, van deze richtlijn
	b) Vervaardiging van informaticaproducten en van elektronische en optische producten	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in bijlage I, sectie C, afdeling 26, van Verordening (EG) nr. 1893/2006 van het Europees Parlement en de Raad van 20 december 2006 tot vaststelling van de statistische classificatie van economische activiteiten NACE Rev. 2 en tot wijziging van Verordening (EEG) nr. 3037/90 en enkele EG-verordeningen op specifieke statistische gebieden
	c) Vervaardiging van elektrische apparatuur	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in bijlage I, sectie C, afdeling 27, van Verordening (EG) nr. 1893/2006 van het Europees Parlement en de Raad van 20 december 2006 tot vaststelling van de statistische classificatie van economische activiteiten NACE Rev. 2 en tot wijziging van Verordening (EEG) nr. 3037/90 en enkele EG-verordeningen op specifieke statistische gebieden
	d) Vervaardiging van machines, apparaten en werktuigen, n.e.g.	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in bijlage I, sectie C, afdeling 28, van Verordening (EG) nr. 1893/2006 van het Europees Parlement en de Raad van 20 december 2006 tot vaststelling van de statistische classificatie van economische activiteiten NACE Rev. 2 en tot wijziging van Verordening (EEG) nr. 3037/90 en enkele EG-verordeningen op specifieke statistische gebieden
	e) Vervaardiging van motorvoertuigen,	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in bijlage I, sectie C, afdeling 29, van Verordening (EG) nr. 1893/2006 van het

	aanhangers en opleggers	Europees Parlement en de Raad van 20 december 2006 tot vaststelling van de statistische classificatie van economische activiteiten NACE Rev. 2 en tot wijziging van Verordening (EEG) nr. 3037/90 en enkele EG-verordeningen op specifieke statistische gebieden
	f) Vervaardiging van andere transportmiddelen	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in bijlage I, sectie C, afdeling 30, van Verordening (EG) nr. 1893/2006 van het Europees Parlement en de Raad van 20 december 2006 tot vaststelling van de statistische classificatie van economische activiteiten NACE Rev. 2 en tot wijziging van Verordening (EEG) nr. 3037/90 en enkele EG-verordeningen op specifieke statistische gebieden
6. Digitale aanbieders		- Aanbieders van onlinemarktplaatsen
		- Aanbieders van onlinezoekmachines
		- Aanbieders van platforms voor socialenetwerkdiensten
7. Onderzoek		- Onderzoeksorganisaties

Gezien om te worden gevoegd bij de wet van ... tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

Brussel, 3 maart 2024

FILIP

Van Koningswege:

De Eerste Minister,

A. DE CROO

De Minister van Binnenlandse Zaken,

A. VERLINDEN

Tableau de correspondance loi NIS2-directive NIS2 / Concordantietabel NIS2-wet - richtlijn NIS2

	Projet de loi / Wetsontwerp	Directive (UE) 2022/2555 / Richtlijn (EU) 2022/2555
TITRE 1ER. - DÉFINITIONS ET DISPOSITIONS GÉNÉRALES		
TITEL 1. - DEFINITIES EN ALGEMENE BEPALINGEN		
Chapitre 1er. Objet et champ d'application		
Hoofdstuk 1. Onderwerp en toepassingsgebied		
Section 1re. Objet		
Afdeling 1. Onderwerp		
	Art. 1	(disposition nationale strictement précisant le fondement constitutionnel de la loi / louter nationale wetsbepaling om de grondwettelijke grondslag van de wet te preciseren)
	Art. 2	Art. 41.2
Section 2. Champ d'application		
Afdeling 2. Toepassingsgebied		
	Art. 3, § 1, al. 1	Art. 2.1, al. 1
	Art. 3, § 1, al. 2	Art. 2.1, al. 2
	Art. 3, § 2	(disposition nationale mettant en œuvre le considérant 16 de la directive NIS2 / nationale wetsbepaling om de overweging 16 van de richtlijn uit te voeren)
	Art. 3, § 3	Art. 2.2
	Art. 3, § 4	Art. 2.3
	Art. 3, § 5	Art. 2.4

	Art. 3, § 6	(disposition nationale / nationale wetsbepaling)
	Art. 4, § 1	Art. 26.1
	Art. 4, § 2	Art. 26.1
	Art. 4, § 3	Art. 26.3
	Art. 4, § 4	Art. 26.2; 26.3
	Art. 4, § 5	Art. 26.4
	Art. 5, § 1	Art. 2.12
	Art. 5, § 2	Art. 2.6
	Art. 5, § 3	Art. 2.6
	Art. 5, § 4	Art. 2.7
	Art. 5, § 5	Art. 2.8
	Art. 5, § 6	Art. 2.9
	Art. 6, § 1	Art. 4.1
	Art. 6, § 2	Art. 4.2
	Art. 6, § 3	(disposition nationale / nationale wetsbepaling)
	Art. 6, § 4	(disposition nationale / nationale wetsbepaling)
	Art. 7	(disposition nationale / nationale wetsbepaling)
	Art. 8, 1°	Art. 6, 1)
	Art. 8, 2°	Art. 6, 2)
	Art. 8, 3°	Art. 6, 3)
	Art. 8, 4°	Art. 6, 4)
	Art. 8, 5°	Art. 6, 6)
	Art. 8, 6°	Art. 6, 5)
	Art. 8, 7°	Art. 6, 7)
	Art. 8, 8°	Art. 6, 8)
	Art. 8, 9°	Art. 6, 9)
	Art. 8, 10°	Art. 6, 10)
	Art. 8, 11°	Art. 6, 11)

	Art. 8, 12°	Art. 6, 12)
	Art. 8, 13°	Art. 6, 13)
	Art. 8, 14°	Art. 6, 14)
	Art. 8, 15°	Art. 6, 15)
	Art. 8, 16°	Art. 6, 16)
	Art. 8, 17°	Art. 6, 18)
	Art. 8, 18°	Art. 6, 19)
	Art. 8, 19°	Art. 6, 20)
	Art. 8, 20°	Art. 6, 21)
	Art. 8, 21°	Art. 6, 22)
	Art. 8, 22°	Art. 6, 23)
	Art. 8, 23°	Art. 6, 24)
	Art. 8, 24°	Art. 6, 25)
	Art. 8, 25°	Art. 6, 26)
	Art. 8, 26°	Art. 6, 27)
	Art. 8, 27°	Art. 6, 28)
	Art. 8, 28°	Art. 6, 29)
	Art. 8, 29°	Art. 6, 30)
	Art. 8, 30°	Art. 6, 31)
	Art. 8, 31°	Art. 6, 32)
	Art. 8, 32°	Art. 6, 33)
	Art. 8, 33°	Art. 6, 34)
	Art. 8, 34°	Art. 6, 35)
	Art. 8, 35°	Art. 6, 36)
	Art. 8, 36°	Art. 6, 37)
	Art. 8, 37°	Art. 6, 38)
	Art. 8, 38°	Art. 6, 39)
	Art. 8, 39°	Art. 6, 40)
	Art. 8, 40°	Art. 6, 41)
	Art. 8, 41°	(disposition nationale / nationale wetsbepaling)

Art. 8, 42°	(disposition nationale / nationale wetsbepaling)
Art. 8, 43°	(disposition nationale / nationale wetsbepaling)
Art. 8, 44°	(disposition nationale / nationale wetsbepaling)
Art. 8, 45°	(disposition nationale / nationale wetsbepaling)
Art. 8, 46°	(disposition nationale / nationale wetsbepaling)
Art. 8, 47°	(disposition nationale / nationale wetsbepaling)
Art. 8, 48°	(disposition nationale / nationale wetsbepaling)
Art. 8, 49°	(disposition nationale / nationale wetsbepaling)
Art. 8, 50°	(disposition nationale / nationale wetsbepaling)
Art. 8, 51°	(disposition nationale / nationale wetsbepaling)
Art. 8, 52°	(disposition nationale / nationale wetsbepaling)
Art. 8, 53°	(disposition nationale / nationale wetsbepaling)
Art. 8, 54°	(disposition nationale / nationale wetsbepaling)
Art. 8, 55°	(disposition nationale / nationale wetsbepaling)
Art. 8, 56°	(disposition nationale / nationale wetsbepaling)
Art. 8, 57°	Art. 23.3
Art. 8, 58°	(disposition nationale / nationale wetsbepaling)

	Art. 8, 59°	(disposition nationale / nationale wetsbepaling)
Chapitre 3. Catégories d'entités		
Hoofdstuk 3. Categorieën van entiteiten		
	Art. 9, 1°	Art. 3.1, a)
	Art. 9, 2°	Art. 3.1, b)
	Art. 9, 3°	Art. 3.1, c)
	Art. 9, 4°	Art. 3.1, d)
	Art. 9, 5°	Art. 3.1, f)
	Art. 9, 6°	Art. 3.1, e)
	Art. 10	Art. 3.2
Chapitre 4. Identification		
Hoofdstuk 4. Identificatie		
	Art. 11, § 1	Art. 2.2, b) à e); 3.1, e)
	Art. 11, § 2,	Art. 2.2, f), ii)
	Art. 11, § 3	(disposition nationale / nationale wetsbepaling)
	Art. 11, § 4	Art. 3.3
	Art. 11, § 5	(disposition nationale / nationale wetsbepaling)
	Art. 12	(disposition nationale / nationale wetsbepaling)
Chapitre 5. Enregistrement des entités		
Hoofdstuk 5. Registratie van de entiteiten		
	Art. 13, § 1, al. 1	Art. 3.4, al. 1

	Art. 13, § 1, al. 2	(disposition nationale / nationale wetsbepaling)
	Art. 13, § 2	(disposition nationale / nationale wetsbepaling)
	Art. 13, § 3	Art. 3.4, al. 2
	Art. 13, § 4	(disposition nationale / nationale wetsbepaling)
	Art. 14, § 1	Art. 27.2
	Art. 14, § 2	Art. 27.3
	Art. 14, § 3	(disposition nationale / nationale wetsbepaling)
TITRE 2. AUTORITÉS COMPÉTENTES ET COOPÉRATION AU NIVEAU NATIONAL		
TITEL 2. BEVOEGDE AUTORITEITEN EN SAMENWERKING OP NATIONAAL NIVEAU		
Chapitre 1er. Autorités compétentes		
Hoofdstuk 1. Bevoegde autoriteiten		
Section 1re. Désignation des autorités compétentes		
Afdeling 1. Aanwijzing van de bevoegde autoriteiten		
	Art. 15, § 1	Art. 8.1; 8.2
	Art. 15, § 2	Art. 8.1; 8.2
Section 2. L'autorité nationale de cybersécurité		
Afdeling 2. De nationale cyberbeveiligingsautoriteit		
	Art. 16	Art. 8.1; 8.2; 8.3; 9.1; 10.1
Sous-section 1re. Tâches relatives au rôle d'autorité compétente chargée de la cybersécurité		
Onderafdeling 1. Taken met betrekking tot de rol van bevoegde autoriteit belast met cyberbeveiliging		
	Art. 17, 1°	Art. 8.2
	Art. 17, 2°	Art. 8.2
	Art. 17, 3°	Art. 8.2
	Art. 17, 4°	Art. 8.2
	Art. 17, 5°	(disposition nationale / nationale wetsbepaling)
	Art. 17, 6°	(disposition nationale / nationale wetsbepaling)

	Art. 17, 7°	(disposition nationale / nationale wetsbepaling)
	Art. 17, 8°	(disposition nationale / nationale wetsbepaling)
	Art. 17, 9°	Art. 8.3
	Art. 17, 10°	(disposition nationale / nationale wetsbepaling)
	Art. 17, 11°	(disposition nationale / nationale wetsbepaling)
	Art. 17, 12°	(disposition nationale / nationale wetsbepaling)
	Art. 17, 13°	(disposition nationale / nationale wetsbepaling)
Sous-section 2. Tâches relatives au rôle de gestion des crises cyber		
Onderafdeling 2. Taken met betrekking tot het cybercrisisbeheer	Art. 18, 1°	Art. 9.3
	Art. 18, 2°	Art. 9.1
	Art. 18, 3°	Art. 9.2
Sous-section 3. Tâches et obligations relatives au rôle de CSIRT national		
Onderafdeling 3. Taken en voorschriften met betrekking tot de rol van nationaal CSIRT		
	Art. 19, § 1, al. 1, 1°	Art. 11.3, al. 1, a)
	Art. 19, § 1, al. 1, 2°	Art. 11.3, al. 1, b)
	Art. 19, § 1, al. 1, 3°	Art. 11.3, al. 1, c)
	Art. 19, § 1, al. 1, 4°	Art. 11.3, al. 1, d)
	Art. 19, § 1, al. 1, 5°	Art. 11.3, al. 1, e)
	Art. 19, § 1, al. 1, 6°	Art. 10.6; 11.3, al. 1, f)
	Art. 19, § 1, al. 1, 7°	Art. 11.3, al. 1, g)
	Art. 19, § 1, al. 1, 8°	Art. 11.3, al. 1, h)
	Art. 19, § 1, al. 1, 9°	Art. 11.3, al. 2
	Art. 19, § 1, al. 1, 10°	(disposition nationale / nationale wetsbepaling)

	Art. 19, § 1, al. 1, 11°	Art. 11.4
	Art. 19, § 1, al. 1, 12°	Art. 11.5
	Art. 19, § 1, al. 1, 13°	Art. 10.4
	Art. 19, § 1, al. 1, 14°	Art. 10.5
	Art. 19, § 1, al. 2	(disposition nationale / nationale wetsbepaling)
	Art. 19, § 2	Art. 11.3, al. 3
	Art. 20, 1°	Art. 10.3
	Art. 20, 2°	Art. 11.1, al. 1, a)
	Art. 20, 3°	Art. 11.1, al. 1, b)
	Art. 20, 4°	Art. 11.1, al. 1, c)
	Art. 20, 5°	Art. 11.1, al. 1, d)
	Art. 20, 6°	Art. 11.1, al. 1, e)
	Art. 20, 7°	Art. 11.1, al. 1, f)
	Art. 21	(disposition nationale / nationale wetsbepaling)
	Art. 22, § 1	Art. 12.1, al. 1
	Art. 22, § 2	Art. 12.1, al. 2
	Art. 22, § 3	Art. 12.1, al. 2
	Art. 22, § 4	(disposition nationale / nationale wetsbepaling)
	Art. 22, § 5	Art. 12.1, al. 2
	Art. 22, § 6	(disposition nationale / nationale wetsbepaling)
	Art. 23	(disposition nationale / nationale wetsbepaling)
Section 3. Les éventuelles autorités sectorielles		
Afdeling 3. De eventuele sectorale overheden		
	Art. 24	(disposition nationale / nationale wetsbepaling)
Chapitre 2. Coopération au niveau national		
Hoofdstuk 2. Samenwerking op nationaal niveau		

	Art. 25, § 1	Art. 13.1
	Art. 25, § 2	Art. 13.4
	Art. 25, § 3	(disposition nationale / nationale wetsbepaling)
	Art. 25, § 4	Art. 13.5
	Art. 25, § 5	Art. 13.5
	Art. 25, § 6	(disposition nationale / nationale wetsbepaling)
Chapitre 3. Confidentialité et échanges d'information		
Hoofdstuk 3. Vertrouwelijkheid en informatie-uitwisseling		
	Art. 26, § 1	Art. 2.6
	Art. 26, § 2	(disposition nationale / nationale wetsbepaling)
	Art. 26, § 3	Art. 2.13
	Art. 26, § 4	Art. 2.13
	Art. 27, § 1	Art. 29.1; 29.2
	Art. 27, § 2	Art. 29.2
	Art. 27, § 3	Art. 29.3
	Art. 27, § 4	Art. 29.4
Chapitre 4. Stratégie nationale en matière de cybersécurité		
Hoofdstuk 4. Nationale cyberbeveiligingsstrategie		
	Art. 28, § 1	Art. 7.1
	Art. 28, § 2, 1°	Art. 7.1, a)
	Art. 28, § 2, 2°	Art. 7.1, b)
	Art. 28, § 2, 3°	Art. 7.1, c)
	Art. 28, § 2, 4°	Art. 7.1, d)
	Art. 28, § 2, 5°	Art. 7.1, e)
	Art. 28, § 2, 6°	Art. 7.1, f)
	Art. 28, § 2, 7°	Art. 7.1, g)
	Art. 28, § 2, 8°	Art. 7.1, h)
	Art. 28, § 2, 9°	(disposition nationale / nationale wetsbepaling)

	Art. 28, § 2, 10°	(disposition nationale / nationale wetsbepaling)
	Art. 28, § 3, 1°	Art. 7.2, a)
	Art. 28, § 3, 2°	Art. 7.2, b)
	Art. 28, § 3, 3°	Art. 7.2, c)
	Art. 28, § 3, 4°	Art. 7.2, d)
	Art. 28, § 3, 5°	Art. 7.2, e)
	Art. 28, § 3, 6°	Art. 7.2, f)
	Art. 28, § 3, 7°	Art. 7.2, g)
	Art. 28, § 3, 8°	Art. 7.2, h)
	Art. 28, § 3, 9°	Art. 7.2, i)
	Art. 28, § 3, 10°	Art. 7.2, j)
Chapitre 5. Le plan national de réaction aux crises et incidents de cybersécurité majeurs		
Hoofdstuk 5. Het nationale plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons		
	Art. 29, § 1	Art. 9.4
	Art. 29, § 2, 1°	Art. 9.4, a)
	Art. 29, § 2, 2°	Art. 9.4, b)
	Art. 29, § 2, 3°	Art. 9.4, c)
	Art. 29, § 2, 4°	Art. 9.4, d)
	Art. 29, § 2, 5°	Art. 9.4, e)
	Art. 29, § 2, 6°	Art. 9.4, f)
TITRE 3. – MESURES DE GESTION DES RISQUES EN MATIÈRE DE CYBERSÉCURITÉ ET OBLIGATIONS D'INFORMATION		
TITEL 3. - MAATREGELEN VOOR HET BEHEER VAN CYBERBEVEILIGINGSRISICO'S EN RAPPORTAGEVERPLICHTINGEN		
Chapitre 1. Mesures de gestion des risques en matière de cybersécurité		
Hoofdstuk 1. Maatregelen voor het beheer van cyberbeveiligingsrisico's		
	Art. 30, § 1	Art. 21.1, al. 1
	Art. 30, § 2	Art. 21.1, al. 2
	Art. 30, § 3, 1°	Art. 21.2, a)
	Art. 30, § 3, 2°	Art. 21.2, b)
	Art. 30, § 3, 3°	Art. 21.2, c)
	Art. 30, § 3, 4°	Art. 21.2, d)
	Art. 30, § 3, 5°	Art. 21.2, e)

	Art. 30, § 3, 6°	Art. 21.2, f)
	Art. 30, § 3, 7°	Art. 21.2, g)
	Art. 30, § 3, 8°	Art. 21.2, h)
	Art. 30, § 3, 9°	Art. 21.2, i)
	Art. 30, § 3, 10°	Art. 21.2, j)
	Art. 30, § 3, 11°	(disposition nationale / nationale wetsbepaling)
	Art. 30, § 4	Art. 21.3
	Art. 30, § 5	(disposition nationale / nationale wetsbepaling)
	Art. 30, § 6	Art. 21.4
	Art. 31, § 1, al. 1	Art. 20.1, al. 1
	Art. 31, § 1, al. 2	Art. 20.1, al. 2
	Art. 31, § 2	Art. 20.2
	Art. 32	(disposition nationale / nationale wetsbepaling)
	Art. 33	(disposition nationale / nationale wetsbepaling)
Chapitre 2. Notification d'incidents		
Hoofdstuk 2. Melding van incidenten		
	Art. 34, § 1, al. 1	Art. 23.1, al. 1
	Art. 34, § 1, al. 2	Art. 23.1, al. 1
	Art. 34, § 2	Art. 23.2
	Art. 34, § 3	(disposition nationale / nationale wetsbepaling)
	Art. 34, § 4	Art. 23.1, al. 1
	Art. 35, § 1, 1°	Art. 23.4, al. 1, a)
	Art. 35, § 1, 2°	Art. 23.4, al. 1, b)
	Art. 35, § 1, 3°	Art. 23.4, al. 1, c)
	Art. 35, § 1, 4°	Art. 23.4, al. 1, d)
	Art. 35, § 1, 5°	Art. 23.4, al. 1, e)

	Art. 35, § 2	Art. 23.4, al. 2
	Art. 35, § 3	(disposition nationale / nationale wetsbepaling)
	Art. 36, § 1	Art. 23.5
	Art. 36, § 2	Art. 23.5
	Art. 37, § 1	Art. 23.6
	Art. 37, § 2	Art. 23.7
	Art. 37, § 3	Art. 23.8
	Art. 37, § 4	Art. 23.9
	Art. 37, § 5	Art. 23.10
Section 2. Notification volontaire		
Afdeling 2. Vrijwillige melding		
	Art. 38, § 1	Art. 30.1
	Art. 38, § 2	Art. 30.2
TITRE 4. – SUPERVISION ET SANCTIONS		
TITRE 4. - TOEZICHT EN SANCTIES		
Chapitre 1er. Supervision		
Hoofdstuk 1. Toezicht		
Section 1re. Évaluation périodique de la conformité		
Afdeling 1. Regelmatige conformiteitsbeoordeling		
	Art. 39, al. 1	Art. 32.2, b)
	Art. 39, al. 2	(disposition nationale / nationale wetsbepaling)
	Art. 40, § 1, al. 1	Art. 32.2, b)
	Art. 40, § 1, al. 2	Art. 2.6
	Art. 40, § 2	(disposition nationale / nationale wetsbepaling)
	Art. 41	(disposition nationale / nationale wetsbepaling)
	Art. 42	(disposition nationale / nationale wetsbepaling)

	Art. 43	(disposition nationale / nationale wetsbepaling)
Section 2. Dispositions générales relatives au service d'inspection		
Afdeling 2. Algemene bepalingen betreffende de inspectiedienst		
	Art. 44, § 1	(disposition nationale / nationale wetsbepaling)
	Art. 44, § 2, al. 1	Art. 32.3; 33.3
	Art. 44, § 2, al. 2	(disposition nationale / nationale wetsbepaling)
	Art. 44, § 3	Art. 31.2
	Art. 44, § 4	Art. 31.3
	Art. 45, § 1	Art. 32.9
	Art. 45, § 2	Art. 32.10; 33.6
	Art. 46, § 1	Art. 37.1
	Art. 46, § 2	Art. 37.1
	Art. 46, § 3	Art. 37.1
	Art. 46, § 4	(disposition nationale / nationale wetsbepaling)
	Art. 47	(disposition nationale / nationale wetsbepaling)
Section 3. La supervision des entités par le service d'inspection		
Afdeling 3. Het door de inspectiedienst uitgeoefende toezicht op de entiteiten		
	Art. 48, § 1, 1°	Art. 32.2, f); g); 33.2, e); f)
	Art. 48, § 1, 2°	Art. 32.2, a); 33.2, a)
	Art. 48, § 1, 3°	Art. 32.2, b); 33.2, b)
	Art. 48, § 1, 4°	Art. 32.2, e); 33.2, d)
	Art. 48, § 1, 5°	Art. 32.2, c)
	Art. 48, § 1, 6°	Art. 32.2, d); 33.2, c)
	Art. 48, § 1, 7°	(disposition nationale / nationale wetsbepaling)
	Art. 48, § 1, 8°	(disposition nationale / nationale wetsbepaling)

	Art. 48, § 1, 9°	(disposition nationale / nationale wetsbepaling)
	Art. 48, § 1, 10°	(disposition nationale / nationale wetsbepaling)
	Art. 48, § 2	Art. 33.1
	Art. 48, § 3	(disposition nationale / nationale wetsbepaling)
	Art. 48, § 4	(disposition nationale / nationale wetsbepaling)
	Art. 48, § 5	(disposition nationale / nationale wetsbepaling)
	Art. 48, § 6	(disposition nationale / nationale wetsbepaling)
	Art. 48, § 7, al. 1	Art. 35.1
	Art. 48, § 7, al. 2	Art. 35.3
	Art. 48, § 8	(disposition nationale / nationale wetsbepaling)
	Art. 49	(disposition nationale / nationale wetsbepaling)
	Art. 50	(disposition nationale / nationale wetsbepaling)
Chapitre 2. Les mesures et amendes administratives		
Hoofdstuk 2. De administratieve maatregelen en geldboetes		
Section 1re. Procédure		
Afdeling 1. Procedure		
	Art. 51, § 1	Art. 32.8; 33.5; 35.1
	Art. 51, § 2	Art. 32.8; 33.5; 34.2
	Art. 51, § 3	Art. 32.8; 33.5
	Art. 51, § 4	(disposition nationale / nationale wetsbepaling)
	Art. 52, § 1	Art. 32.5
	Art. 52, § 2	Art. 32.8

	Art. 52, § 3	Art. 32.8; 34.2
	Art. 52, § 4	Art. 32.8
	Art. 52, § 5	(disposition nationale / nationale wetsbepaling)
	Art. 53	(disposition nationale / nationale wetsbepaling)
	Art. 54, § 1	Art. 32.7; 33.5; 34.3
	Art. 54, § 1, 1°	(disposition nationale / nationale wetsbepaling)
	Art. 54, § 1, 2°	Art. 32.7, a)
	Art. 54, § 1, 3°	Art. 32.7, b)
	Art. 54, § 1, 4°	Art. 32.7, c)
	Art. 54, § 1, 5°	Art. 32.7, d)
	Art. 54, § 1, 6°	Art. 32.7, e)
	Art. 54, § 1, 7°	Art. 32.7, f)
	Art. 54, § 1, 8°	Art. 32.7, g)
	Art. 54, § 1, 9°	Art. 32.7, h)
	Art. 54, § 2	Art. 35.2
	Art. 55	(disposition nationale / nationale wetsbepaling)
	Art. 56, § 1	Art. 34.6
	Art. 56, § 2	(disposition nationale / nationale wetsbepaling)
	Art. 56, § 3	(disposition nationale / nationale wetsbepaling)
	Art. 56, § 4	(disposition nationale / nationale wetsbepaling)
	Art. 56, § 5	(disposition nationale / nationale wetsbepaling)
	Art. 57	(disposition nationale / nationale wetsbepaling)
Section 2. Mesures et amendes administratives		

Afdeling 2. Administratieve maatregelen en geldboetes		
	Art. 58, al. 1, 1°	Art. 32.4, a); 33.4, a)
	Art. 58, al. 1, 2°	Art. 32.4, b); 33.4, b)
	Art. 58, al. 1, 3°	Art. 32.4, c); 33.4, c)
	Art. 58, al. 1, 4°	Art. 32.4, d); 33.4, d)
	Art. 58, al. 1, 5°	Art. 32.4, e); 33.4, e)
	Art. 58, al. 1, 6°	Art. 32.4, f); 33.4, f)
	Art. 58, al. 1, 7°	Art. 32.4, h); 33.4, g)
	Art. 58, al. 1, 8°	Art. 32.4, g); 33.4, h)
	Art. 58, al. 2	Art. 32.4, b)
	Art. 59	Art. 32.4, i); 32.5; 33.4, h)
	Art. 59, al. 1, 1°	(disposition nationale / nationale wetsbepaling)
	Art. 59, al. 1, 2°	(disposition nationale / nationale wetsbepaling)
	Art. 59, al. 1, 3°	(disposition nationale / nationale wetsbepaling)
	Art. 59, al. 1, 4°	Art. 34.5
	Art. 59, al. 1, 5°	Art. 34.4
	Art. 59, al. 2	(disposition nationale / nationale wetsbepaling)
	Art. 59, al. 3	(disposition nationale / nationale wetsbepaling)
	Art. 60, al. 1, 1°	Art. 32.5, al. 1, a)
	Art. 60, al. 1, 2°	Art. 32.5, al. 1, b)
	Art. 60, al. 2	Art. 32.5, al. 2
	Art. 61	Art. 32.6; 33.5
TITRE 5. – DISPOSITIONS SPÉCIFIQUES AU SECTEUR DE L'ADMINISTRATION PUBLIQUE		
TITEL 5. - SPECIFIEKE BEPALINGEN VOOR DE OVERHEIDSSECTOR		
	Art. 62	Art. 32.5, alinéa 3; 34.7
	Art. 63, § 1	(disposition nationale / nationale wetsbepaling)

	Art. 63, § 2	(disposition nationale / nationale wetsbepaling)
	Art. 64	Art. 31.4
	Art. 65	(disposition nationale / nationale wetsbepaling)
TITRE 6. - TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL		
TITEL 6. - VERWERKING VAN PERSOONSGEGEVENS		
Chapitre 1er. Principes relatifs au traitement		
Hoofdstuk 1. Beginselen betreffende de verwerking		
	Art. 66	(disposition nationale / nationale wetsbepaling)
	Art. 67	(disposition nationale / nationale wetsbepaling)
	Art. 68	(disposition nationale / nationale wetsbepaling)
	Art. 69	(disposition nationale / nationale wetsbepaling)
	Art. 70	(disposition nationale / nationale wetsbepaling)
Chapitre 2. Durée de conservation		
Hoofdstuk 2. Bewaartermijn		
	Art. 71	(disposition nationale / nationale wetsbepaling)
Chapitre 3. Limitation des droits des personnes concernées		
Hoofdstuk 3. Beperking van de rechten van de betrokkenen		
	Art. 72	(disposition nationale / nationale wetsbepaling)
	Art. 73	(disposition nationale / nationale wetsbepaling)
Chapitre 4. Limitations aux obligations de notification des violations de données à caractère personnel		

Hoofdstuk 5. Beperkingen inzake de verplichte melding van inbreuken in verband met persoonsgegevens			
	Art. 74		(disposition nationale / nationale wetsbepaling)
Titre 7. - Dispositions finales			
Titel 7. - Slotbepalingen			
Chapitre 1er. Dispositions transitoires			
Hoofdstuk 1. Overgangsbepalingen		Art. 75	(disposition nationale / nationale wetsbepaling)
Chapitre 2. Dispositions modificatives			
Hoofdstuk 2. Wijzigingsbepalingen			
Section 1re. Modifications de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire			
Afdeling 1. Wijzigingen van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle			
	Art. 76		(disposition nationale / nationale wetsbepaling)
	Art. 77		(disposition nationale / nationale wetsbepaling)
Section 2. Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique			
Afdeling 2. Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België			
	Art. 78		(disposition nationale / nationale wetsbepaling)
	Art. 79		(disposition nationale / nationale wetsbepaling)
	Art. 80		(disposition nationale / nationale wetsbepaling)
Section 3. Modification de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers			
Afdeling 3. Wijziging van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten			
	Art. 81		(disposition nationale / nationale wetsbepaling)
Section 4. Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges			

Afdeling 4. Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector		Art. 82	Art. 41.2
		Art. 83	(disposition nationale / nationale wetsbepaling)
Section 5. Modification de la loi du 13 juin 2005 relative aux communications électroniques			
Afdeling 5. Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie			
		Art. 84	Art. 41.2
		Art. 85, 1°	Art. 6, 21)
		Art. 85, 2°	Art. 6, 22)
		Art. 85, 3°	Art. 6, 1); 6, 2)
		Art. 85, 4°	Art. 6, 3); 6, 6); 6, 8); 6, 10); 6, 11)
		Art. 85, 5°	Art. 6, 25)
		Art. 86	(disposition nationale / nationale wetsbepaling)
		Art. 87	(disposition nationale / nationale wetsbepaling)
		Art. 88	Art. 21; 23.2
		Art. 89	(disposition nationale / nationale wetsbepaling)
		Art. 90	(disposition nationale / nationale wetsbepaling)
		Art. 91	(disposition nationale / nationale wetsbepaling)
		Art. 92	Art. 28
Section 6. Modifications de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE			
Afdeling 6. Wijzigingen van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU			
		Art. 93	(disposition nationale / nationale wetsbepaling)

	Art. 94	(disposition nationale / nationale wetsbepaling)
Chapitre 3. Disposition abrogatoire Hoofdstuk 3. Opheffingsbepaling		
	Art. 95	(disposition nationale / nationale wetsbepaling)
Chapitre 4. Entrée en vigueur Hoofdstuk 4. Inwerkingtreding		
	Art. 96	(disposition nationale / nationale wetsbepaling)
ANNEXE I SECTEURS HAUTEMENT CRITIQUES BIJLAGE I ZEER KRITIEKE SECTOREN		
ANNEXE II AUTRES SECTEURS CRITIQUES BIJLAGE II ANDERE KRITIEKE SECTOREN		

Tableau de correspondance directive NIS2 - loi NIS2 / Concordantietabel richtlijn NIS 2 - loi NIS2

	Directive 2022/2555 / Richtlijn 2022/2555	(UE) (EU)	Projet de loi / Wetsontwerp
CHAPITRE I DISPOSITIONS GENERALES HOOFDSTUK I ALGEMENE BEPALINGEN			
Objet Onderwerp		Art. 1.1	(ne doit pas être transposé / dient niet te worden omgezet) [Dispositions liminaires]
		Art. 1.2	(ne doit pas être transposé / dient niet te worden omgezet) [Dispositions liminaires]
Champ d'application Toepassingsgebied		Art. 2.1	Art. 3, § 1
		Art. 2.2	Art. 3, § 3
		Art. 2.3	Art. 3, § 4
		Art. 2.4	Art. 3, § 5
		Art. 2.5	Art. 5, § 6
		Art. 2.6	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres/choix]
		Art. 2.7	Art. 5, § 4
		Art. 2.8	Art. 5, § 5
		Art. 2.9	Art. 5, § 5
		Art. 2.10	(ne doit pas être transposé / dient niet te worden omgezet) [cf. BNB]

	Art. 2.11	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres/choix national]
	Art. 2.12	Art. 5, § 1
	Art. 2.13	Art. 26, § 3 & § 4
	Art. 2.14	(ne doit pas être transposé / dient niet te worden omgezet)
Entités essentielles et importantes Essentiële en belangrijke entiteiten	Art. 3.1	Art. 9
	Art. 3.2	Art. 10
	Art. 3.3	Art. 17, 14°
	Art. 3.4	Art. 13
	Art. 3.5	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]
	Art. 3.6	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]
	Art. 4.1	Art. 6, § 1
	Art. 4.2	Art. 6, § 2
	Art. 4.3	(ne doit pas être transposé / dient niet te worden omgezet)
Actes juridiques sectoriels de l'Union Sectorspecifieke rechtshandelingen van de Unie	Art. 5	(ne doit pas être transposé / dient niet te worden omgezet)

Définitions Definities	Art. 6	Art. 8 ; 85
CHAPITRE II CADRES COORDONNÉS EN MATIÈRE DE CYBERSECURITE HOOFDSTUK II GECOÖRDINEERDE KADERS OP HET GEBIED VAN CYBERBEVEILIGING		
Stratégie nationale en matière de cybersécurité Nationale cyberbeveiligingsstrategie	Art. 7.1	Art. 28, § 1 & § 2
	Art. 7.2	Art. 28, § 3
	Art. 7.3	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]
	Art. 7.4	Art. 28, § 1, al. 1
	Art. 8.1	Art. 15
Autorités compétentes et points de contact uniques Bevoegde autoriteiten en centrale contactpunten	Art. 8.2	Art. 15 ; 16
	Art. 8.3	Art. 16
	Art. 8.4	Art. 17, 9°
	Art. 8.5	(ne doit pas être transposé / dient niet te worden omgezet)
	Art. 8.6	(ne doit pas être transposé / dient niet te worden omgezet)
Cadres nationaux de gestion des crises cyber Nationale kaders voor cybercrisisbeheer	Art. 9.1	Art. 16, al. 2
	Art. 9.2	Art. 18, 3°
	Art. 9.3	Art. 18, 1°
	Art. 9.4	Art. 29
	Art. 9.5	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]
Centres de réponse aux incidents de sécurité informatique (CSIRT)	Art. 10.1	Art. 16, al. 2

Computer security incident response teams (CSIRT's)	Art. 10.2	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]
	Art. 10.3	Art. 19, § 1, al. 1, 8°, 20, 1°
	Art. 10.4	Art. 19, § 1, al. 1, 13°
	Art. 10.5	Art. 19, § 1, al. 1, 14°
	Art. 10.6	Art. 19, § 1, al. 1, 6°
	Art. 10.7	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]
	Art. 10.8	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]
Obligations, capacités techniques et tâches des CSIRT Eisen, technische capaciteiten en taken van de CSIRT's	Art. 10.9	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]
	Art. 10.10	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]
	Art. 11.1	Art. 20, 2° à 7°
	Art. 11.2	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]

		exclusivement les autorités des Etats membres]
	Art. 11.3	Art. 19, § 1, al. 1, 1° à 9 & § 2
	Art. 11.4	Art. 19, § 1, al. 1, 11°
	Art. 11.5	Art. 19, § 1, al. 1, 12°
Divulgateion coordonnée des vulnérabilités et base de données européenne des vulnérabilités Gecoördineerde bekendmaking van de kwetsbaarheden en een Europese kwetsbaarheidsdatabase	Art. 12.1	Art. 22, § 1 à § 3 & § 5
	Art. 12.2	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
Coopération au niveau national Samenwerking op nationaal niveau	Art. 13.1	Art. 25, § 1; 34, § 1, al. 3
	Art. 13.2	Art. 34, § 1, al. 1 et 3
	Art. 13.3	(ne doit pas être transposé / dient niet te worden omgezet)
	Art. 13.4	Art. 25, § 2
	Art. 13.5	Art. 25, § 4 & § 5
	Art. 13.6	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]
CHAPITRE III COOPÉRATION AU NIVEAU DE L'UNION ET AU NIVEAU INTERNATIONAL HOOFDSTUK III SAMENWERKING OP UNIE- EN INTERNATIONAAL NIVEAU		
Groupe de coopération Samenwerkingsgroep	Art. 14.1	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
	Art. 14.2	
	Art. 14.3	
	Art. 14.4	
	Art. 14.5	
	Art. 14.6	
	Art. 14.7	
	Art. 14.8	

Réseau des CSIRT CSIRT-netwerk	Art. 14.9	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
	Art. 15.1	
	Art. 15.2	
	Art. 15.3	
	Art. 15.4	
	Art. 15.5	
	Art. 15.6	
Le réseau européen pour la préparation et la gestion des crises cyber (EU-CyclONE) Het Europese netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONE)	Art. 16.1	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
	Art. 16.2	
	Art. 16.3	
	Art. 16.4	
	Art. 16.5	
	Art. 16.6	
	Art. 16.7	
Coopération internationale Internationale samenwerking	Art. 17	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
Rapport sur l'état de la cybersécurité dans l'Union Verslag over de stand van zaken op het gebied van de cyberbeveiliging in de Unie	Art. 18.1	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
	Art. 18.2	
	Art. 18.3	
Évaluations par les pairs Collegiale toetsingen	Art. 19.1	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
	Art. 19.2	
	Art. 19.3	
	Art. 19.4	
	Art. 19.5	
	Art. 19.6	
	Art. 19.7	
CHAPITRE IV MESURES DE GESTION DES RISQUES EN MATIÈRE DE CYBERSÉCURITÉ ET OBLIGATIONS D'INFORMATION	Art. 19.8	
	Art. 19.9	

HOOFDSTUK IV RISICOBEBEERSMAATREGELEN EN RAPPORTAGEVERPLICHTINGEN OP HET GEBIED VAN CYBERBEVEILIGING		
Gouvernance Governance	Art. 20.1	Art. 31, § 1
	Art. 20.2	Art. 31, § 2
Mesures de gestion des risques en matière de cybersécurité Maatregelen voor het beheer van cyberbeveiligingsrisico's	Art. 21.1	Art. 30, § 1 & § 2
	Art. 21.2	Art. 30, § 3
	Art. 21.3	Art. 30, § 4
	Art. 21.4	Art. 30, § 6
	Art. 21.5	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
		(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
Évaluations coordonnées au niveau de l'Union des risques pour la sécurité des chaînes d'approvisionnement critiques Op Unieniveau gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens	Art. 22.1	
	Art. 22.2	
Obligations d'information Rapportageverplichtingen	Art. 23.1	Art. 34, § 1 & § 6
	Art. 23.2	Art. 34, § 2
	Art. 23.3	Art. 8, 57°
	Art. 23.4	Art. 35
	Art. 23.5	Art. 36, § 1 & § 2
	Art. 23.6	Art. 37, § 1
	Art. 23.7	Art. 37, § 2
	Art. 23.8	Art. 37, § 3
	Art. 23.9	Art. 37, § 4
	Art. 23.10	Art. 37, § 5
	Art. 23.11	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
Recours aux schémas européens de certification de cybersécurité Gebruik van Europese cyberbeveiligingscertificeringsregelingen	Art. 24.1	(ne doit pas être transposé / dient niet te worden omgezet) [concernent

		exclusivement les autorités des Etats membres]
	Art. 24.2	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
	Art. 24.3	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
Normalisation Normalisatie	Art. 25.1	Art. 17, 7°
	Art. 25.2	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
CHAPITRE V COMPÉTENCE ET ENREGISTREMENT HOOFDSTUK V JURISDICTIE EN REGISTRATIE		
Compétence et territorialité Jurisdictie en territorialiteit	Art. 26.1	Art. 4, § 1 & § 2
	Art. 26.2	Art. 4, § 4
	Art. 26.3	Art. 4, § 3 & § 5
	Art. 26.4	Art. 4, § 6
	Art. 26.5	Art. 46, § 2, al. 3
Registre des entités Register van entiteiten	Art. 27.1	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
	Art. 27.2	Art. 14, § 1
	Art. 27.3	Art. 14, § 2
	Art. 27.4	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]

	Art. 27.5	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]
Base des données d'enregistrement des noms de domaine Database met domeinnaamregistratiegegevens	Art. 28.1	Art. 92
	Art. 28.2	Art. 92
	Art. 28.3	Art. 92
	Art. 28.4	Art. 92
	Art. 28.5	Art. 92
	Art. 28.6	Art. 92
CHAPITRE VI PARTAGE D'INFORMATIONS		
HOOFDSTUK VI INFORMATIE-UITWISSELING		
Accords de partage d'informations en matière de cybersécurité Informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging	Art. 29.1	Art. 27, § 1
	Art. 29.2	Art. 27, § 1 & § 2
	Art. 29.3	Art. 27, § 3
	Art. 29.4	Art. 27, § 4
	Art. 29.5	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
Notification volontaire d'informations pertinentes Vrijwillige melding van relevante informatie	Art. 30.1	Art. 38, § 1
	Art. 30.2	Art. 38, § 2
CHAPITRE VII SUPERVISION ET EXÉCUTION		
HOOFDSTUK VII TOEZICHT EN HANDHAVING		
Aspects généraux concernant la supervision et l'exécution Algemene aspecten van het toezicht en de handhaving	Art. 31.1	(ne doit pas être transposé / dient niet te worden omgezet)
	Art. 31.2	Art. 44, § 3
	Art. 31.3	Art. 44, § 4
	Art. 31.4	Art. 64

Mesures de supervision et d'exécution en ce qui concerne les entités essentielles Toezichts- en handhavingsmaatregelen met betrekking tot essentiële entiteiten	Art. 32.1	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]
	Art. 32.2	Art. 39; 40; 48, § 1
	Art. 32.3	Art. 44, § 2
	Art. 32.4	Art. 58; 59
	Art. 32.5	Art. 52; 59; 60; 62
	Art. 32.6	Art. 61
	Art. 32.7	Art. 54, § 1
	Art. 32.8	Art. 51; 52
	Art. 32.9	Art. 45, § 1
	Art. 32.10	Art. 45, § 2
Mesures de supervision et d'exécution en ce qui concerne les entités importantes Toezichts- en handhavingsmaatregelen met betrekking tot belangrijke entiteiten	Art. 33.1	Art. 48, § 2
	Art. 33.2	Art. 48, § 1
	Art. 33.3	Art. 44, § 2
	Art. 33.4	Art. 58; 59
	Art. 33.5	Art. 51; 54, § 1; 61
	Art. 33.6	Art. 45, § 2
Conditions générales pour imposer des amendes administratives à des entités essentielles et importantes Algemene voorwaarden voor het opleggen van administratieve geldboeten aan essentiële en belangrijke entiteiten	Art. 34.1	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]
	Art. 34.2	Art. 51, § 2; 52, § 3
	Art. 34.3	Art. 54, § 1
	Art. 34.4	Art. 59, 5°
	Art. 34.5	Art. 59, 4°
	Art. 34.6	Art. 56
	Art. 34.7	Art. 62

	Art. 34.8	(ne doit pas être transposé / dient niet te worden omgezet)
Infractions donnant lieu à une violation de données à caractère personnel Inbreuken die een inbreuk in verband met persoonsgegevens inhouden	Art. 35.1	Art. 48, § 7, al. 1
	Art. 35.2	Art. 54, § 2
	Art. 35.3	Art. 48, § 7, al. 2
Sanctions Sancties	Art. 36	(ne doit pas être transposé / dient niet te worden omgezet) [concernent exclusivement les autorités des Etats membres]
Assistance mutuelle	Art. 37.1	Art. 46, § 1 & § 2
Wederzijdse bijstand	Art. 37.2	Art. 46, § 3
CHAPITRE VIII ACTES DÉLÉGUÉS ET ACTES D'EXÉCUTION		
HOOFDSTUK VIII GEDELEGEERDE HANDELINGEN EN UITVOERINGSHANDELINGEN		
Exercice de la delegation Uitoefening van de bevoegdheidsdelegatie	Art. 38.1	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
	Art. 38.2	
	Art. 38.3	
	Art. 38.4	
	Art. 38.5	
	Art. 38.6	
Comité Comitéprocedure	Art. 39.1	(ne doit pas être transposé / dient niet te worden omgezet) [tâches institutions européennes]
	Art. 39.2	
	Art. 39.3	
CHAPITRE IX DISPOSITIONS FINALES		
HOOFDSTUK IX SLOTBEPALINGEN		
Réexamen Evaluatie	Art. 40	(ne doit pas être transposé / dient niet te worden omgezet)
Transposition Omzetting	Art. 41.1	(ne doit pas être transposé / dient niet te worden omgezet)

	Art. 41.2	Art. 2; 82
Modification du règlement (UE) no 910/2014 Wijziging van Verordening (EU) nr. 910/2014	Art. 42	(ne doit pas être transposé / dient niet te worden omgezet)
Modification de la directive (UE) 2018/1972 Wijziging van Richtlijn (EU) 2018/1972	Art. 43	(ne doit pas être transposé / dient niet te worden omgezet)
Abrogation Intrekking	Art. 44	(ne doit pas être transposé / dient niet te worden omgezet)
Entrée en vigueur Inwerkingtreding	Art. 45	(ne doit pas être transposé / dient niet te worden omgezet)
Destinataires Adressaten	Art. 46	(ne doit pas être transposé / dient niet te worden omgezet)
ANNEXE I SECTEURS HAUTEMENT CRITIQUES		
BIJLAGE I ZEER KRITIEKE SECTOREN		
ANNEXE II AUTRES SECTEURS CRITIQUES		
BIJLAGE II ANDERE KRITIEKE SECTOREN		

COORDINATION DES ARTICLES

TEXTE EN VIGUEUR

PROJET DE LOI

Loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire

Article 1^{er}

Pour l'application de la présente loi, et de ses mesures d'exécution, il y a lieu d'entendre par:

- rayonnements ionisants: rayonnements composés de photons ou de particules capables de déterminer la formation d'ions directement ou indirectement;

- substance radioactive: toute substance ou toute matière contenant un ou plusieurs radionucléides dont l'activité ou la concentration ne peut être négligée pour des raisons de radioprotection;

- autorités compétentes: les autorités désignées en vertu de la présente loi et de ses arrêtés d'exécution;

- règlement général: l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants;

- organisme de contrôle physique: organisme, qui, en vertu de l'article 29bis, est agréé pour effectuer des missions du service de contrôle physique;

- service de contrôle physique: le service qui, en vertu de l'article 28, est en charge du contrôle physique;

- l'Agence: l'établissement public créé par la présente loi pour le contrôle nucléaire;

- pratique: activité humaine susceptible d'accroître l'exposition de certains individus aux rayonnements ionisants provenant d'une source artificielle ou d'une source naturelle de rayonnement lorsque des radionucléides naturels sont traités en raison de leurs

Article 1^{er}

Pour l'application de la présente loi, et de ses mesures d'exécution, il y a lieu d'entendre par:

- rayonnements ionisants: rayonnements composés de photons ou de particules capables de déterminer la formation d'ions directement ou indirectement;

- substance radioactive: toute substance ou toute matière contenant un ou plusieurs radionucléides dont l'activité ou la concentration ne peut être négligée pour des raisons de radioprotection;

- autorités compétentes: les autorités désignées en vertu de la présente loi et de ses arrêtés d'exécution;

- règlement général: l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants;

- organisme de contrôle physique: organisme, qui, en vertu de l'article 29bis, est agréé pour effectuer des missions du service de contrôle physique;

- service de contrôle physique: le service qui, en vertu de l'article 28, est en charge du contrôle physique;

- l'Agence: l'établissement public créé par la présente loi pour le contrôle nucléaire;

- pratique: activité humaine susceptible d'accroître l'exposition de certains individus aux rayonnements ionisants provenant d'une source artificielle ou d'une source naturelle de rayonnement lorsque des radionucléides naturels sont traités en raison de leurs

TEXTE EN VIGUEUR

propriétés radioactives, fissiles ou fertiles, sauf dans le cas d'une exposition d'urgence;

- contrôle physique: l'ensemble des mesures, exécutées sous la responsabilité du détenteur de l'autorisation, dans le but de vérifier que la population, les travailleurs et l'environnement sont protégés de manière effective contre le danger des rayonnements ionisants, et que les risques associés sont gérés de manière effective à l'exception:

a) des mesures relatives à la surveillance de la santé des personnes professionnellement exposées aux rayonnements ionisants;

b) des mesures relatives à la surveillance de l'exposition médicale des personnes;

c) des mesures de protection physique;

d) des mesures de sécurité des substances radioactives;

- surveillance de la santé des travailleurs: la surveillance de l'ensemble des mesures garantissant la santé des travailleurs, prises en application de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail et prises sous la responsabilité d'un médecin agréé en vertu de la présente loi;

- détenteur d'autorisation: détenteur d'une autorisation délivrée en vertu de l'article 16 ou d'un agrément délivré en vertu de l'article 4;

- matières nucléaires: les produits fissiles spéciaux et les matières brutes suivantes:

a) les produits fissiles spéciaux sont le plutonium 239, l'uranium 233, l'uranium enrichi en uranium 235 ou 233; tout produit contenant un ou plusieurs des isotopes ci-dessus.

L'uranium enrichi en uranium 235 ou 233 est de l'uranium qui contient soit de l'uranium 235 soit de l'uranium 233, soit ces deux isotopes en quantité telle que le rapport entre la somme de ces deux isotopes et l'isotope 238 est supérieur

PROJET DE LOI

propriétés radioactives, fissiles ou fertiles, sauf dans le cas d'une exposition d'urgence;

- contrôle physique: l'ensemble des mesures, exécutées sous la responsabilité du détenteur de l'autorisation, dans le but de vérifier que la population, les travailleurs et l'environnement sont protégés de manière effective contre le danger des rayonnements ionisants, et que les risques associés sont gérés de manière effective à l'exception:

a) des mesures relatives à la surveillance de la santé des personnes professionnellement exposées aux rayonnements ionisants;

b) des mesures relatives à la surveillance de l'exposition médicale des personnes;

c) des mesures de protection physique;

d) des mesures de sécurité des substances radioactives;

- surveillance de la santé des travailleurs: la surveillance de l'ensemble des mesures garantissant la santé des travailleurs, prises en application de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail et prises sous la responsabilité d'un médecin agréé en vertu de la présente loi;

- détenteur d'autorisation: détenteur d'une autorisation délivrée en vertu de l'article 16 ou d'un agrément délivré en vertu de l'article 4;

- matières nucléaires: les produits fissiles spéciaux et les matières brutes suivantes:

a) les produits fissiles spéciaux sont le plutonium 239, l'uranium 233, l'uranium enrichi en uranium 235 ou 233; tout produit contenant un ou plusieurs des isotopes ci-dessus.

L'uranium enrichi en uranium 235 ou 233 est de l'uranium qui contient soit de l'uranium 235 soit de l'uranium 233, soit ces deux isotopes en quantité telle que le rapport entre la somme de ces deux isotopes et l'isotope 238 est supérieur

TEXTE EN VIGUEUR

au rapport entre l'isotope 235 et l'isotope 238 dans l'uranium naturel;

b) les matières brutes sont l'uranium contenant le mélange d'isotopes qui se trouve dans la nature, et l'uranium appauvri en uranium 235; le thorium; toutes les matières mentionnées ci-dessus sous forme de métal, d'alliage, de composés chimiques ou de concentrés;

- transport nucléaire national: le transport de matières nucléaires conditionnées en vue d'un envoi par tout moyen de transport lorsque celui-ci se déroule exclusivement à l'intérieur du territoire belge;

- transport nucléaire international: le transport de matières nucléaires conditionnées en vue d'un envoi par tout moyen de transport lorsqu'il doit franchir les frontières du territoire au départ d'une installation de l'expéditeur située dans l'Etat d'origine jusqu'à son arrivée dans une installation du destinataire sur le territoire de l'Etat de destination finale;

- mesures de protection physique: toute mesure administrative, organisationnelle et technique qui a pour objectif de protéger les matières nucléaires en cours de production, d'utilisation, d'entreposage ou de transport contre les risques de détention illicite et de vol comme de protéger les matières nucléaires en cours de production, d'utilisation, d'entreposage ainsi que les installations nucléaires et les transports nucléaires nationaux et internationaux contre les risques de sabotage. Lesdites mesures ont également pour objectif de protéger des actes précités les documents nucléaires;

- mesures de sécurité pour les substances radioactives: toute mesure administrative, organisationnelle et technique qui a pour objectif:

a) de protéger les substances radioactives autres que les matières nucléaires, en cours de production, d'utilisation, d'entreposage ou de transport contre les risques de détention illicite et de vol;

PROJET DE LOI

au rapport entre l'isotope 235 et l'isotope 238 dans l'uranium naturel;

b) les matières brutes sont l'uranium contenant le mélange d'isotopes qui se trouve dans la nature, et l'uranium appauvri en uranium 235; le thorium; toutes les matières mentionnées ci-dessus sous forme de métal, d'alliage, de composés chimiques ou de concentrés;

- transport nucléaire national: le transport de matières nucléaires conditionnées en vue d'un envoi par tout moyen de transport lorsque celui-ci se déroule exclusivement à l'intérieur du territoire belge;

- transport nucléaire international: le transport de matières nucléaires conditionnées en vue d'un envoi par tout moyen de transport lorsqu'il doit franchir les frontières du territoire au départ d'une installation de l'expéditeur située dans l'Etat d'origine jusqu'à son arrivée dans une installation du destinataire sur le territoire de l'Etat de destination finale;

- mesures de protection physique: toute mesure administrative, organisationnelle et technique qui a pour objectif de protéger les matières nucléaires en cours de production, d'utilisation, d'entreposage ou de transport contre les risques de détention illicite et de vol comme de protéger les matières nucléaires en cours de production, d'utilisation, d'entreposage ainsi que les installations nucléaires et les transports nucléaires nationaux et internationaux contre les risques de sabotage. Lesdites mesures ont également pour objectif de protéger des actes précités les documents nucléaires;

- mesures de sécurité pour les substances radioactives: toute mesure administrative, organisationnelle et technique qui a pour objectif:

a) de protéger les substances radioactives autres que les matières nucléaires, en cours de production, d'utilisation, d'entreposage ou de transport contre les risques de détention illicite et de vol;

TEXTE EN VIGUEUR

b) de protéger contre les risques de sabotage ou de toute utilisation malveillante:

1) les substances radioactives autres que les matières nucléaires et qui sont en cours de production, d'utilisation ou d'entreposage;

2) les établissements où ces substances sont produites, fabriquées, détenues ou utilisées ainsi que leur transport;

- mesures de sécurité pour les appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives: toute mesure administrative, organisationnelle et technique qui a pour objectif:

a) de protéger les dits appareils ou installations contre les risques de détention illicite et de vol;

b) de protéger contre les risques de sabotage ou de toute utilisation malveillante:

1) lesdits appareils ou installations, ainsi que le transport de ces appareils ou installations;

2) les établissements et lieux où se trouvent ces appareils et installations;

- sabotage: tout acte délibéré:

a) qui est dirigé contre:

1) des matières nucléaires en cours de production, d'utilisation, d'entreposage ou de transport;

2) des installations nucléaires;

3) des transports nucléaires nationaux ou internationaux;

4) des substances radioactives autres que les matières nucléaires et qui sont en cours de production, d'utilisation, d'entreposage ou de transport;

PROJET DE LOI

b) de protéger contre les risques de sabotage ou de toute utilisation malveillante:

1) les substances radioactives autres que les matières nucléaires et qui sont en cours de production, d'utilisation ou d'entreposage;

2) les établissements où ces substances sont produites, fabriquées, détenues ou utilisées ainsi que leur transport;

- mesures de sécurité pour les appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives: toute mesure administrative, organisationnelle et technique qui a pour objectif:

a) de protéger les dits appareils ou installations contre les risques de détention illicite et de vol;

b) de protéger contre les risques de sabotage ou de toute utilisation malveillante:

1) lesdits appareils ou installations, ainsi que le transport de ces appareils ou installations;

2) les établissements et lieux où se trouvent ces appareils et installations;

- sabotage: tout acte délibéré:

a) qui est dirigé contre:

1) des matières nucléaires en cours de production, d'utilisation, d'entreposage ou de transport;

2) des installations nucléaires;

3) des transports nucléaires nationaux ou internationaux;

4) des substances radioactives autres que les matières nucléaires et qui sont en cours de production, d'utilisation, d'entreposage ou de transport;

TEXTE EN VIGUEUR

5) des établissements ou parties d'établissements, où des substances radioactives sont produites, fabriquées, détenues ou utilisées;

6) des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives;

7) le transport des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives;

8) des établissements, parties d'établissement et lieux où se trouvent des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives;

Et

b) qui pourrait mettre directement ou indirectement en danger la santé et la sécurité du personnel, de la population et de l'environnement par une exposition aux radiations ou l'émission de substances radioactives;

- [...]

- réacteur de puissance : un réacteur nucléaire, conçu à des fins de production électrique, qui est ou a été autorisé en tant qu'établissement de classe I en application de la réglementation relative à la protection contre les rayonnements ionisants et pour lequel aucune autorisation de démantèlement n'a encore été délivrée.

- personne professionnellement exposée: chaque personne physique soumise, dans le cadre de ses activités professionnelles, à une exposition aux rayonnements ionisants susceptible d'entraîner le dépassement de l'une des limites de dose fixées pour les personnes du public;

- personne soumise à la surveillance dosimétrique: chaque personne physique qui exécute des activités de quelque nature que ce soit lors desquelles elle est soumise à une

PROJET DE LOI

5) des établissements ou parties d'établissements, où des substances radioactives sont produites, fabriquées, détenues ou utilisées;

6) des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives;

7) le transport des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives;

8) des établissements, parties d'établissement et lieux où se trouvent des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives;

Et

b) qui pourrait mettre directement ou indirectement en danger la santé et la sécurité du personnel, de la population et de l'environnement par une exposition aux radiations ou l'émission de substances radioactives;

- [...]

- réacteur de puissance : un réacteur nucléaire, conçu à des fins de production électrique, qui est ou a été autorisé en tant qu'établissement de classe I en application de la réglementation relative à la protection contre les rayonnements ionisants et pour lequel aucune autorisation de démantèlement n'a encore été délivrée.

- personne professionnellement exposée: chaque personne physique soumise, dans le cadre de ses activités professionnelles, à une exposition aux rayonnements ionisants susceptible d'entraîner le dépassement de l'une des limites de dose fixées pour les personnes du public;

- personne soumise à la surveillance dosimétrique: chaque personne physique qui exécute des activités de quelque nature que ce soit lors desquelles elle est soumise à une

TEXTE EN VIGUEUR

exposition aux rayonnements ionisants susceptible d'entraîner le dépassement de l'une des limites de dose fixées pour les personnes du public;

- exploitant: toute personne physique ou morale qui assume la responsabilité de l'établissement devant faire l'objet d'une autorisation ou d'une déclaration conformément aux dispositions découlant de l'article 17;

- entreprise extérieure: toute personne physique ou morale appelée à exécuter des activités de quelque nature que ce soit dans un établissement devant faire l'objet d'une autorisation ou d'une déclaration conformément aux dispositions découlant de l'article 17, au cours desquelles l'une des limites de dose fixées pour les personnes du public pourraient être dépassées, à l'exception de l'exploitant de cet établissement et des membres de son personnel;

- médecin agréé: le conseiller en prévention-médecin du travail travaillant dans un service interne ou externe pour la prévention et la protection au travail, compétent dans le domaine de la médecine du travail conformément aux dispositions de la loi du 4 août 1996 relative au bien-être des travailleurs dans la cadre de l'exécution de leur travail et à ses arrêtés d'exécution et qui, en outre, est agréé conformément aux mesures d'exécution prises en vertu des articles 3 et 19;

- travailleur extérieur: toute personne soumise à la surveillance dosimétrique qui exécute chez un exploitant une mission comportant un risque d'exposition, qu'elle soit employée à titre temporaire ou permanent par une entreprise extérieure, ou qu'elle preste ses services en qualité de travailleur indépendant;

- mission comportant un risque d'exposition: l'activité de quelque nature que ce soit prestée par un travailleur extérieur chez un exploitant au cours de laquelle l'une des limites de dose fixées pour les personnes du public pourrait être dépassée;

PROJET DE LOI

exposition aux rayonnements ionisants susceptible d'entraîner le dépassement de l'une des limites de dose fixées pour les personnes du public;

- exploitant: toute personne physique ou morale qui assume la responsabilité de l'établissement devant faire l'objet d'une autorisation ou d'une déclaration conformément aux dispositions découlant de l'article 17;

- entreprise extérieure: toute personne physique ou morale appelée à exécuter des activités de quelque nature que ce soit dans un établissement devant faire l'objet d'une autorisation ou d'une déclaration conformément aux dispositions découlant de l'article 17, au cours desquelles l'une des limites de dose fixées pour les personnes du public pourraient être dépassées, à l'exception de l'exploitant de cet établissement et des membres de son personnel;

- médecin agréé: le conseiller en prévention-médecin du travail travaillant dans un service interne ou externe pour la prévention et la protection au travail, compétent dans le domaine de la médecine du travail conformément aux dispositions de la loi du 4 août 1996 relative au bien-être des travailleurs dans la cadre de l'exécution de leur travail et à ses arrêtés d'exécution et qui, en outre, est agréé conformément aux mesures d'exécution prises en vertu des articles 3 et 19;

- travailleur extérieur: toute personne soumise à la surveillance dosimétrique qui exécute chez un exploitant une mission comportant un risque d'exposition, qu'elle soit employée à titre temporaire ou permanent par une entreprise extérieure, ou qu'elle preste ses services en qualité de travailleur indépendant;

- mission comportant un risque d'exposition: l'activité de quelque nature que ce soit prestée par un travailleur extérieur chez un exploitant au cours de laquelle l'une des limites de dose fixées pour les personnes du public pourrait être dépassée;

TEXTE EN VIGUEUR

- registre d'exposition: le système d'enregistrement centralisé des données dosimétriques des personnes soumises à la surveillance dosimétrique, visé à l'article 25/2;

- passeport radiologique: le document individuel établi pour les travailleurs extérieurs permettant d'assurer leur surveillance dosimétrique pendant les missions comportant un risque d'exposition qu'ils exécutent à l'étranger;

- professionnel des soins de santé: le responsable du traitement qui gère les données concernant la santé visées dans la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et désigné au sein de l'Agence;

- consultant en sécurité de l'information et protection de la vie privée: le consultant visé à l'article 4, § 5, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité sociale et désigné au sein de l'Agence;

- responsable du traitement: la personne visée dans la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, en l'occurrence l'Agence;

- unité d'implantation: le lieu d'activité, géographiquement identifiable par une adresse, où s'exerce au moins une activité de l'entreprise ou à partir duquel elle est exercée;

- travailleur: le travailleur visé à l'article 2, § 1er, alinéas 1er et 2, 1°, de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail;

- employeur: l'employeur visé à l'article 2, § 1er, alinéas 1er et 2, 2°, de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail;

PROJET DE LOI

- registre d'exposition: le système d'enregistrement centralisé des données dosimétriques des personnes soumises à la surveillance dosimétrique, visé à l'article 25/2;

- passeport radiologique: le document individuel établi pour les travailleurs extérieurs permettant d'assurer leur surveillance dosimétrique pendant les missions comportant un risque d'exposition qu'ils exécutent à l'étranger;

- professionnel des soins de santé: le responsable du traitement qui gère les données concernant la santé visées dans la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et désigné au sein de l'Agence;

- consultant en sécurité de l'information et protection de la vie privée: le consultant visé à l'article 4, § 5, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité sociale et désigné au sein de l'Agence;

- responsable du traitement: la personne visée dans la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, en l'occurrence l'Agence;

- unité d'implantation: le lieu d'activité, géographiquement identifiable par une adresse, où s'exerce au moins une activité de l'entreprise ou à partir duquel elle est exercée;

- travailleur: le travailleur visé à l'article 2, § 1er, alinéas 1er et 2, 1°, de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail;

- employeur: l'employeur visé à l'article 2, § 1er, alinéas 1er et 2, 2°, de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail;

TEXTE EN VIGUEUR

- surveillance dosimétrique: la surveillance dosimétrique telle que visée à l'article 30.6 du Règlement général;

- sources authentiques: le Registre national créé par la loi du 8 août 1983 organisant un Registre national des personnes physiques, la Banque-Carrefour des entreprises créée par la loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses dispositions, et les Registres de la Banque-Carrefour de la Sécurité sociale (Registre bis et Registre des radiés) créés par la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité sociale;

- données anonymes: les données qui ne peuvent être mises en relation avec une personne identifiée ou identifiable et qui ne sont, en conséquence, pas des données à caractère personnel;

- "la loi du 7 avril 2019": la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

- "délégué à la protection des données": le délégué désigné par l'Agence en application de l'article 37.1. a) du règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE;

- loi du 23 mars 2020: la loi du 23 mars 2020 visant à flouter les images d'établissements nucléaires et sensibles et à limiter la prise ou la diffusion de photographies aériennes de ces établissements dans l'intérêt de la sécurité publique.

Article 15ter

L'Agence est désignée comme service d'inspection, au sens de l'article 42 de la loi du 7

PROJET DE LOI

- surveillance dosimétrique: la surveillance dosimétrique telle que visée à l'article 30.6 du Règlement général;

- sources authentiques: le Registre national créé par la loi du 8 août 1983 organisant un Registre national des personnes physiques, la Banque-Carrefour des entreprises créée par la loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses dispositions, et les Registres de la Banque-Carrefour de la Sécurité sociale (Registre bis et Registre des radiés) créés par la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité sociale;

- données anonymes: les données qui ne peuvent être mises en relation avec une personne identifiée ou identifiable et qui ne sont, en conséquence, pas des données à caractère personnel;

- la loi NIS2 : la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

- "délégué à la protection des données": le délégué désigné par l'Agence en application de l'article 37.1. a) du règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE;

- loi du 23 mars 2020: la loi du 23 mars 2020 visant à flouter les images d'établissements nucléaires et sensibles et à limiter la prise ou la diffusion de photographies aériennes de ces établissements dans l'intérêt de la sécurité publique.

Article 15ter

L'Agence est désignée comme service d'inspection sectoriel, au sens de la loi NIS2,

TEXTE EN VIGUEUR

avril 2019 et est chargée du contrôle de l'application des dispositions de ladite loi et de ses arrêtés d'exécution par les opérateurs de services essentiels, identifiés en vertu de la loi susmentionnée, pour ce qui concerne les éléments d'une installation nucléaire destinée à la production industrielle d'électricité et qui servent au transport de l'électricité.

Le Roi fixe les modalités pratiques des inspections, après avis de l'Agence.

PROJET DE LOI

pour le secteur de l'énergie, en ce qui concerne les mesures supplémentaires de gestion des risques en matière de cybersécurité applicables aux éléments d'une installation nucléaire destinée à la production industrielle d'électricité et qui servent au transport de l'électricité.

Le Roi fixe les modalités pratiques des inspections, après avis de l'Agence.

Loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique**Article 36/1**

Définitions : pour l'application du présent chapitre et du chapitre IV/2, il y a lieu d'entendre par :

1° " la loi du 2 août 2002 " : la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers;

2° " instrument financier " : un instrument tel que défini à l'article 2, 1° de la loi du 2 août 2002;

3° " établissement de crédit " : tout établissement visé au Livre II et aux Titres Ier et II du Livre III de la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit [...];

4° "établissement de monnaie électronique" : tout établissement visé à l'article 2, 74° de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement;

5° " entreprise d'investissement ayant le statut de société de bourse " : toute entreprise d'investissement par la loi du 20 juillet 2022 relative au statut et au contrôle des sociétés de

Article 36/1

Définitions : pour l'application du présent chapitre et du chapitre IV/2, il y a lieu d'entendre par :

1° " la loi du 2 août 2002 " : la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers;

2° " instrument financier " : un instrument tel que défini à l'article 2, 1° de la loi du 2 août 2002;

3° " établissement de crédit " : tout établissement visé au Livre II et aux Titres Ier et II du Livre III de la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit [...];

4° "établissement de monnaie électronique" : tout établissement visé à l'article 2, 74° de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement;

5° " entreprise d'investissement ayant le statut de société de bourse " : toute entreprise d'investissement par la loi du 20 juillet 2022 relative au statut et au contrôle des sociétés de bourse et portant dispositions diverses agréées

TEXTE EN VIGUEUR

bourse et portant dispositions diverses agréée en qualité de société de bourse ou autorisée à prêter des services d'investissement qui, s'ils étaient prestés par une entreprise d'investissement belge, nécessiteraient l'obtention d'un agrément en tant que société de bourse;

6° "entreprise d'assurance ou de réassurance": toute entreprise visée à l'article 5, alinéa 1er, 1°, ou 2°, de la loi du 13 mars 2016. relative au statut et au contrôle des entreprises d'assurance ou de réassurance;

7° [...]

8° " société de cautionnement mutuel " : toute société visée à l'article 57 de la loi-programme du 10 février 1998 pour la promotion de l'entreprise indépendante;

9° "établissement de paiement" : tout établissement visé à l'article 2, 8° de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement;

10° " marché réglementé " : tout marché réglementé belge ou étranger;

11° " marché réglementé belge " : un système multilatéral, exploité et/ou géré par une entreprise de marché, qui assure ou facilite la rencontre - en son sein même et selon ses règles non discrétionnaires - de multiples intérêts acheteurs et vendeurs exprimés par des tiers pour des instruments financiers, d'une manière qui aboutisse à la conclusion de contrats portant sur des instruments financiers admis à la négociation dans le cadre de ses règles et/ou de ses systèmes, et qui est agréé et fonctionne

PROJET DE LOI

en qualité de société de bourse ou autorisée à prêter des services d'investissement qui, s'ils étaient prestés par une entreprise d'investissement belge, nécessiteraient l'obtention d'un agrément en tant que société de bourse;

6° "entreprise d'assurance ou de réassurance": toute entreprise visée à l'article 5, alinéa 1er, 1°, ou 2°, de la loi du 13 mars 2016. relative au statut et au contrôle des entreprises d'assurance ou de réassurance;

7° [...]

8° " société de cautionnement mutuel " : toute société visée à l'article 57 de la loi-programme du 10 février 1998 pour la promotion de l'entreprise indépendante;

9° "établissement de paiement" : tout établissement visé à l'article 2, 8° de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement;

10° " marché réglementé " : tout marché réglementé belge ou étranger;

11° " marché réglementé belge " : un système multilatéral, exploité et/ou géré par une entreprise de marché, qui assure ou facilite la rencontre - en son sein même et selon ses règles non discrétionnaires - de multiples intérêts acheteurs et vendeurs exprimés par des tiers pour des instruments financiers, d'une manière qui aboutisse à la conclusion de contrats portant sur des instruments financiers admis à la négociation dans le cadre de ses règles et/ou de ses systèmes, et qui est agréé et fonctionne régulièrement conformément aux dispositions du chapitre II de la loi du 2 août 2002;

TEXTE EN VIGUEUR

régulièrement conformément aux dispositions du chapitre II de la loi du 2 août 2002;

12° " marché réglementé étranger " : tout marché d'instruments financiers qui est organisé par une entreprise de marché dont l'Etat d'origine est un Etat membre de l'Espace économique européen autre que la Belgique et qui a été agréé dans cet Etat membre en qualité de marché réglementé en application du titre III de la Directive 2014/65/UE;

13° "contrepartie centrale" : une contrepartie centrale telle que définie à l'article 2, 1), du Règlement (UE) n° 648/2012 du Parlement Européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux;

14° [...]

15° " FSMA " : l'Autorité des services et marchés financiers, en allemand " Kommission für das Bank-, Finanz- und Versicherungswesen ";

16° "autorité compétente" : la Banque, la FSMA ou l'autorité désignée par chaque Etat membre en application de l'article 67 de la Directive 2014/65/UE, de l'article 22 du Règlement 648/2012 , de l'article 11 du Règlement 909/2014 ou de l'article 2, 21), et de l'article 12 du Règlement 2022/858, à moins que la Directive et les Règlements respectifs n'en disposent autrement;

17° "la Directive 2014/65/UE" : la Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE;

18° " CREFS " : le Comité des risques et établissements financiers systémiques.

19° " institution de retraite professionnelle " : l'établissement visé à l'article 2, 1°, de la loi du

PROJET DE LOI

12° " marché réglementé étranger " : tout marché d'instruments financiers qui est organisé par une entreprise de marché dont l'Etat d'origine est un Etat membre de l'Espace économique européen autre que la Belgique et qui a été agréé dans cet Etat membre en qualité de marché réglementé en application du titre III de la Directive 2014/65/UE;

13° "contrepartie centrale" : une contrepartie centrale telle que définie à l'article 2, 1), du Règlement (UE) n° 648/2012 du Parlement Européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux;

14° [...]

15° " FSMA " : l'Autorité des services et marchés financiers, en allemand " Kommission für das Bank-, Finanz- und Versicherungswesen ";

16° "autorité compétente" : la Banque, la FSMA ou l'autorité désignée par chaque Etat membre en application de l'article 67 de la Directive 2014/65/UE, de l'article 22 du Règlement 648/2012 , de l'article 11 du Règlement 909/2014 ou de l'article 2, 21), et de l'article 12 du Règlement 2022/858, à moins que la Directive et les Règlements respectifs n'en disposent autrement;

17° "la Directive 2014/65/UE" : la Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE;

18° " CREFS " : le Comité des risques et établissements financiers systémiques.

19° " institution de retraite professionnelle " : l'établissement visé à l'article 2, 1°, de la loi du

TEXTE EN VIGUEUR

27 octobre 2006 relative au contrôle des institutions de retraite professionnelle;

20° " l'Autorité bancaire européenne " : l'Autorité bancaire européenne instituée par le Règlement n° 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la Décision n° 716/2009/CE et abrogeant la Décision 2009/78/CE de la Commission;

21° " l'Autorité européenne des assurances et des pensions professionnelles " : l'Autorité européenne des assurances et des pensions professionnelles instituée par le Règlement n° 1094/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), modifiant la Décision n° 716/2009/CE et abrogeant la Décision 2009/79/CE de la Commission;

21°/1 " l'Autorité européenne des marchés financiers " : l'Autorité européenne des marchés financiers instituée par le Règlement 1095/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers), modifiant la Décision n° 716/2009/CE et abrogeant la Décision 2009/77/CE de la Commission.

22° "le Règlement 648/2012" : le Règlement (UE) n° 648/2012 du Parlement Européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux;

23° "contrepartie financière" : une contrepartie telle que définie à l'article 2, 8) du Règlement 648/2012 ou à l'article 3, 3) du Règlement 2015/2365;

PROJET DE LOI

27 octobre 2006 relative au contrôle des institutions de retraite professionnelle;

20° " l'Autorité bancaire européenne " : l'Autorité bancaire européenne instituée par le Règlement n° 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la Décision n° 716/2009/CE et abrogeant la Décision 2009/78/CE de la Commission;

21° " l'Autorité européenne des assurances et des pensions professionnelles " : l'Autorité européenne des assurances et des pensions professionnelles instituée par le Règlement n° 1094/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), modifiant la Décision n° 716/2009/CE et abrogeant la Décision 2009/79/CE de la Commission;

21°/1 " l'Autorité européenne des marchés financiers " : l'Autorité européenne des marchés financiers instituée par le Règlement 1095/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers), modifiant la Décision n° 716/2009/CE et abrogeant la Décision 2009/77/CE de la Commission.

22° "le Règlement 648/2012" : le Règlement (UE) n° 648/2012 du Parlement Européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux;

23° "contrepartie financière" : une contrepartie telle que définie à l'article 2, 8) du Règlement 648/2012 ou à l'article 3, 3) du Règlement 2015/2365;

TEXTE EN VIGUEUR

24° "contrepartie non financière" : une contrepartie telle que définie à l'article 2, 9) du Règlement 648/2012 ou à l'article 3, 4) du Règlement 2015/2365;

25° "dépositaire central de titres" : un dépositaire central de titres tel que défini à l'article 2, paragraphe 1er, 1) du Règlement 909/2014;

26° "le Règlement 909/2014" : le Règlement (UE) n° 909/2014 du Parlement européen et du Conseil du 23 juillet 2014 concernant l'amélioration du règlement de titres dans l'Union européenne et les dépositaires centraux de titres, et modifiant les directives 98/26/CE et 2014/65/UE ainsi que le Règlement (UE) n° 236/2012;

27° "le Règlement 2015/2365" : le Règlement (UE) 2015/2365 du Parlement européen et du Conseil du 25 novembre 2015 relatif à la transparence des opérations de financement sur titres et de la réutilisation et modifiant le règlement (UE) n° 648/2012.

28° "la loi du 7 avril 2019" : la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

29° "tribunal de l'insolvabilité" : le tribunal de l'insolvabilité visé à l'article I.22, 4°, du Code de droit économique;

30° "la loi du 18 septembre 2017" : la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces;

31° "Règlement MSU" : Règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en

PROJET DE LOI

24° "contrepartie non financière" : une contrepartie telle que définie à l'article 2, 9) du Règlement 648/2012 ou à l'article 3, 4) du Règlement 2015/2365;

25° "dépositaire central de titres" : un dépositaire central de titres tel que défini à l'article 2, paragraphe 1er, 1) du Règlement 909/2014;

26° "le Règlement 909/2014" : le Règlement (UE) n° 909/2014 du Parlement européen et du Conseil du 23 juillet 2014 concernant l'amélioration du règlement de titres dans l'Union européenne et les dépositaires centraux de titres, et modifiant les directives 98/26/CE et 2014/65/UE ainsi que le Règlement (UE) n° 236/2012;

27° "le Règlement 2015/2365" : le Règlement (UE) 2015/2365 du Parlement européen et du Conseil du 25 novembre 2015 relatif à la transparence des opérations de financement sur titres et de la réutilisation et modifiant le règlement (UE) n° 648/2012.

28° "la loi NIS2" : la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

29° "tribunal de l'insolvabilité" : le tribunal de l'insolvabilité visé à l'article I.22, 4°, du Code de droit économique;

30° "la loi du 18 septembre 2017" : la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces;

31° "Règlement MSU" : Règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit;

TEXTE EN VIGUEUR

matière de surveillance prudentielle des établissements de crédit;

32° "directive 2015/849" : la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission;

33° "Règlement 2021/23" : Règlement (UE) 2021/23 du Parlement européen et du Conseil du 16 décembre 2020 relatif à un cadre pour le redressement et la résolution des contreparties centrales et modifiant les règlements (UE) n° 1095/2010, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 806/2014, (UE) 2015/2365, ainsi que les directives 2002/47/CE, 2004/25/CE, 2007/36/CE, 2014/59/UE et (UE) 2017/1132 ;

34° "Règlement 2022/858" : Règlement (UE) 2022/858 du Parlement européen et du Conseil du 30 mai 2022 sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués, et modifiant les règlements (UE) n° 600/2014 et (UE) n° 909/2014 et la directive 2014/65/UE ;

35° "entité qui exploite un système de règlement DLT ou un système de négociation et de règlement DLT" : un dépositaire central de titres ou une entreprise d'investissement ou un opérateur de marché qui exploite un système de règlement DLT ou un système de négociation et de règlement DLT visés à l'article 97, 13° et 14°, de la loi du ... portant dispositions financières diverses.

Article 36/14

§ 1^{er}. Par dérogation à l'article 35, la Banque peut également communiquer des informations

PROJET DE LOI

32° "directive 2015/849" : la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission;

33° "Règlement 2021/23" : Règlement (UE) 2021/23 du Parlement européen et du Conseil du 16 décembre 2020 relatif à un cadre pour le redressement et la résolution des contreparties centrales et modifiant les règlements (UE) n° 1095/2010, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 806/2014, (UE) 2015/2365, ainsi que les directives 2002/47/CE, 2004/25/CE, 2007/36/CE, 2014/59/UE et (UE) 2017/1132 ;

34° "Règlement 2022/858" : Règlement (UE) 2022/858 du Parlement européen et du Conseil du 30 mai 2022 sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués, et modifiant les règlements (UE) n° 600/2014 et (UE) n° 909/2014 et la directive 2014/65/UE ;

35° "entité qui exploite un système de règlement DLT ou un système de négociation et de règlement DLT" : un dépositaire central de titres ou une entreprise d'investissement ou un opérateur de marché qui exploite un système de règlement DLT ou un système de négociation et de règlement DLT visés à l'article 97, 13° et 14°, de la loi du ... portant dispositions financières diverses.

Article 36/14

§ 1^{er}. Par dérogation à l'article 35, la Banque peut également communiquer des informations

TEXTE EN VIGUEUR

confidentielles reçues dans l'exercice de ses missions visées à l'article 36/2, § 1er :

1° à la Banque centrale européenne et aux autres banques centrales et organismes à vocation similaire en leur qualité d'autorités monétaires lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales respectives, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier, de même qu'à d'autres autorités publiques chargées de la surveillance des systèmes de paiement.

Lorsque survient une situation d'urgence, notamment une évolution défavorable des marchés financiers, susceptible de menacer la liquidité du marché et la stabilité du système financier dans un des Etats membres dans lequel des entités d'un groupe comprenant des établissements de crédit ou des entreprises d'investissement ont été agréées ou dans lequel sont établies des succursales d'importance significative au sens de l'article 3, 65° de la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit [...] la Banque peut transmettre des informations aux banques centrales du Système européen de banques centrales lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier.

En cas de situation d'urgence telle que visée ci-dessus, la Banque peut divulguer, dans tous les Etats membres concernés, des informations qui présentent un intérêt pour les départements d'administrations centrales responsables de la législation relative à la surveillance des établissements de crédit, des établissements financiers, des services d'investissement et des entreprises d'assurances;

PROJET DE LOI

confidentielles reçues dans l'exercice de ses missions visées à l'article 36/2, § 1er :

1° à la Banque centrale européenne et aux autres banques centrales et organismes à vocation similaire en leur qualité d'autorités monétaires lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales respectives, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier, de même qu'à d'autres autorités publiques chargées de la surveillance des systèmes de paiement.

Lorsque survient une situation d'urgence, notamment une évolution défavorable des marchés financiers, susceptible de menacer la liquidité du marché et la stabilité du système financier dans un des Etats membres dans lequel des entités d'un groupe comprenant des établissements de crédit ou des entreprises d'investissement ont été agréées ou dans lequel sont établies des succursales d'importance significative au sens de l'article 3, 65° de la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit [...] la Banque peut transmettre des informations aux banques centrales du Système européen de banques centrales lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier.

En cas de situation d'urgence telle que visée ci-dessus, la Banque peut divulguer, dans tous les Etats membres concernés, des informations qui présentent un intérêt pour les départements d'administrations centrales responsables de la législation relative à la surveillance des établissements de crédit, des établissements financiers, des services d'investissement et des entreprises d'assurances;

TEXTE EN VIGUEUR

2° dans les limites du droit de l'Union européenne, aux autorités compétentes de l'Union européenne et d'autres Etats membres de l'Espace économique européen qui exercent une ou plusieurs compétences comparables à celles visées aux articles 36/2 et 36/3 , y compris la Banque centrale européenne en ce qui concerne les missions qui lui sont confiées par le Règlement MSU;

2° /1 dans les limites du droit de l'Union européenne, aux autorités compétentes d'autres Etats membres de l'Espace économique européen qui exercent une ou plusieurs compétences de contrôle à l'égard des entités assujetties énumérées à l'article 2, paragraphe 1er, points 1) et 2) de la directive (UE) 2015/849, aux fins du respect de ladite directive et ce, pour l'exercice de la mission que cette directive leur confère;

3° dans le respect du droit de l'Union européenne, aux autorités compétentes d'Etats tiers qui exercent une ou plusieurs compétences comparables à celles visées aux articles 36/2 et 36/3 , en ce compris les autorités ayant des compétences de même nature que celles des autorités visées au 2° /1, et avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'informations;

4° à la FSMA;

5° aux organismes belges ou d'un autre Etat membre de l'Espace économique européen gérant un système de protection des dépôts, des investisseurs ou des assurances sur la vie et à l'organe chargé des dispositifs de financement pour la résolution;

6° aux contreparties centrales, aux organismes de liquidation d'instruments financiers ou aux dépositaires centraux de titres qui sont autorisés à assurer des services de compensation ou de liquidation de transactions sur instruments financiers effectuées sur un marché réglementé belge, dans la mesure où la Banque estime que la communication des informations en question

PROJET DE LOI

2° dans les limites du droit de l'Union européenne, aux autorités compétentes de l'Union européenne et d'autres Etats membres de l'Espace économique européen qui exercent une ou plusieurs compétences comparables à celles visées aux articles 36/2 et 36/3 , y compris la Banque centrale européenne en ce qui concerne les missions qui lui sont confiées par le Règlement MSU;

2° /1 dans les limites du droit de l'Union européenne, aux autorités compétentes d'autres Etats membres de l'Espace économique européen qui exercent une ou plusieurs compétences de contrôle à l'égard des entités assujetties énumérées à l'article 2, paragraphe 1er, points 1) et 2) de la directive (UE) 2015/849, aux fins du respect de ladite directive et ce, pour l'exercice de la mission que cette directive leur confère;

3° dans le respect du droit de l'Union européenne, aux autorités compétentes d'Etats tiers qui exercent une ou plusieurs compétences comparables à celles visées aux articles 36/2 et 36/3 , en ce compris les autorités ayant des compétences de même nature que celles des autorités visées au 2° /1, et avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'informations;

4° à la FSMA;

5° aux organismes belges ou d'un autre Etat membre de l'Espace économique européen gérant un système de protection des dépôts, des investisseurs ou des assurances sur la vie et à l'organe chargé des dispositifs de financement pour la résolution;

6° aux contreparties centrales, aux organismes de liquidation d'instruments financiers ou aux dépositaires centraux de titres qui sont autorisés à assurer des services de compensation ou de liquidation de transactions sur instruments financiers effectuées sur un marché réglementé belge, dans la mesure où la Banque estime que la communication des informations en question

TEXTE EN VIGUEUR

est nécessaire en vue de garantir le fonctionnement régulier de ces contreparties centrales, organismes de liquidation et dépositaires centraux de titres par rapport à des manquements, même potentiels, d'intervenants sur le marché concerné;

7° dans les limites du droit de l'Union européenne, aux entreprises de marché pour le bon fonctionnement, le contrôle et la surveillance des marchés que celles-ci organisent;

8° au cours de procédures civiles ou commerciales, aux autorités et mandataires de justice impliqués dans des procédures de faillite ou de réorganisation judiciaire ou des procédures collectives analogues concernant des établissements soumis au contrôle de la Banque, à l'exception des informations confidentielles concernant la participation de tiers à des tentatives de sauvetage antérieures à ces procédures;

9° aux commissaires et réviseurs d'entreprises et aux autres contrôleurs légaux des comptes des établissements soumis au contrôle de la Banque, d'autres établissements financiers belges ou d'établissements étrangers similaires;

10° aux séquestres, pour l'exercice de leur mission visée par les lois régissant les missions confiées à la Banque;

11° au Collège de supervision des réviseurs d'entreprises et aux autorités d'Etats membres ou de pays tiers investies de la surveillance des personnes chargées du contrôle légal des comptes annuels des établissements soumis au contrôle de la Banque;

12° dans les limites du droit de l'Union européenne, à l'Autorité belge de la concurrence;

13° [...]

14° à l'Administration générale de la Trésorerie du Service public fédéral Finances lorsqu'une

PROJET DE LOI

est nécessaire en vue de garantir le fonctionnement régulier de ces contreparties centrales, organismes de liquidation et dépositaires centraux de titres par rapport à des manquements, même potentiels, d'intervenants sur le marché concerné;

7° dans les limites du droit de l'Union européenne, aux entreprises de marché pour le bon fonctionnement, le contrôle et la surveillance des marchés que celles-ci organisent;

8° au cours de procédures civiles ou commerciales, aux autorités et mandataires de justice impliqués dans des procédures de faillite ou de réorganisation judiciaire ou des procédures collectives analogues concernant des établissements soumis au contrôle de la Banque, à l'exception des informations confidentielles concernant la participation de tiers à des tentatives de sauvetage antérieures à ces procédures;

9° aux commissaires et réviseurs d'entreprises et aux autres contrôleurs légaux des comptes des établissements soumis au contrôle de la Banque, d'autres établissements financiers belges ou d'établissements étrangers similaires;

10° aux séquestres, pour l'exercice de leur mission visée par les lois régissant les missions confiées à la Banque;

11° au Collège de supervision des réviseurs d'entreprises et aux autorités d'Etats membres ou de pays tiers investies de la surveillance des personnes chargées du contrôle légal des comptes annuels des établissements soumis au contrôle de la Banque;

12° dans les limites du droit de l'Union européenne, à l'Autorité belge de la concurrence;

13° [...]

14° à l'Administration générale de la Trésorerie du Service public fédéral Finances lorsqu'une

TEXTE EN VIGUEUR

telle communication est prévue par le droit de l'Union européenne ou par une disposition légale ou réglementaire en matière de sanctions financières (notamment les dispositions contraignantes relatives aux embargos financiers telles que définies à l'article 4, 6°, de la loi du 18 septembre 2017) ou lorsque l'Administration générale de la Trésorerie agit en qualité d'autorité de contrôle assurant le respect du règlement (CE) 2271/96 du Conseil du 22 novembre 1996 portant protection contre les effets de l'application extraterritoriale d'une législation adoptée par un pays tiers, ainsi que des actions fondées sur elle ou en découlant;

15° dans les limites du droit de l'Union européenne, aux actuaux indépendants des établissements exerçant, en vertu de la loi, une tâche de contrôle sur ces établissements ainsi qu'aux organes chargés de la surveillance de ces actuaux;

16° à Fedris;

17° dans les limites du droit de l'Union européenne, au Service Public Fédéral économie, en sa qualité d'autorité compétente pour assurer le contrôle des dispositions visées au livre VII, titres 1er à 3, titre 5, chapitre 1er, et titres 6 et 7 du Code de droit économique ainsi qu'aux agents commissionnés par le ministre qui dans le cadre de leur mission visée à l'article XV.2 du Code de droit économique sont compétents pour rechercher et constater les infractions aux dispositions de l'article XV.89 dudit Code ;

18° aux autorités relevant du droit d'Etats membres de l'Union européenne compétentes dans le domaine de la surveillance macroprudentielle ainsi qu'au Comité européen du risque systémique institué par le Règlement (UE) n° 1092/2010 du Parlement européen et du Conseil du 24 novembre 2010;

19° dans les limites des règlements et directives européens, à l'Autorité européenne des marchés financiers, à l'Autorité européenne des assurances et des pensions professionnelles et à l'Autorité bancaire européenne;

PROJET DE LOI

telle communication est prévue par le droit de l'Union européenne ou par une disposition légale ou réglementaire en matière de sanctions financières (notamment les dispositions contraignantes relatives aux embargos financiers telles que définies à l'article 4, 6°, de la loi du 18 septembre 2017) ou lorsque l'Administration générale de la Trésorerie agit en qualité d'autorité de contrôle assurant le respect du règlement (CE) 2271/96 du Conseil du 22 novembre 1996 portant protection contre les effets de l'application extraterritoriale d'une législation adoptée par un pays tiers, ainsi que des actions fondées sur elle ou en découlant;

15° dans les limites du droit de l'Union européenne, aux actuaux indépendants des établissements exerçant, en vertu de la loi, une tâche de contrôle sur ces établissements ainsi qu'aux organes chargés de la surveillance de ces actuaux;

16° à Fedris;

17° dans les limites du droit de l'Union européenne, au Service Public Fédéral économie, en sa qualité d'autorité compétente pour assurer le contrôle des dispositions visées au livre VII, titres 1er à 3, titre 5, chapitre 1er, et titres 6 et 7 du Code de droit économique ainsi qu'aux agents commissionnés par le ministre qui dans le cadre de leur mission visée à l'article XV.2 du Code de droit économique sont compétents pour rechercher et constater les infractions aux dispositions de l'article XV.89 dudit Code ;

18° aux autorités relevant du droit d'Etats membres de l'Union européenne compétentes dans le domaine de la surveillance macroprudentielle ainsi qu'au Comité européen du risque systémique institué par le Règlement (UE) n° 1092/2010 du Parlement européen et du Conseil du 24 novembre 2010;

19° dans les limites des règlements et directives européens, à l'Autorité européenne des marchés financiers, à l'Autorité européenne des assurances et des pensions professionnelles et à l'Autorité bancaire européenne;

TEXTE EN VIGUEUR

20° dans les limites du droit de l'Union européenne, au Centre gouvernemental de Coordination et de Crise du SPF Intérieur, à l'Organe de coordination pour l'analyse de la menace, institué par la loi du 10 juillet 2006 relative à l'analyse de la menace, à l'autorité visée à l'article 7, § 1er, de la loi du 7 avril 2019 et aux services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, dans la mesure où l'application de l'article 19 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques le requiert;

20° /1 dans les limites du droit de l'Union européenne, aux services de police et à l'autorité visée à l'article 7, § 1er, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique - loi NIS pour les besoins de l'exécution de l'article 53, § 2, de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement ;

20°/2 dans les limites du droit de l'Union européenne, à l'autorité visée à l'article 5, § 1er, de la loi du 20 juillet 2022 relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité, ou aux autorités désignées par le Roi en vertu de l'article 5, § 2, de la même loi;

21° à l'Office de contrôle des mutualités et des unions nationales de mutualités, pour l'exercice de ses missions légales visées à l'article 303, § 3, de la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance, en ce qui concerne les sociétés mutualistes visées à l'article 43bis, § 5, ou à l'article 70, §§ 6, 7 et 8, de la loi du 6 août 1990

PROJET DE LOI

20° dans les limites du droit de l'Union européenne, au Centre gouvernemental de Coordination et de Crise du SPF Intérieur, à l'Organe de coordination pour l'analyse de la menace, institué par la loi du 10 juillet 2006 relative à l'analyse de la menace, **à l'autorité nationale de cybersécurité visée à l'article 8, 45°, de la loi NIS2** et aux services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, dans la mesure où l'application de l'article 19 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques le requiert;

20° /1 dans les limites du droit de l'Union européenne, aux services de police et **à l'autorité nationale de cybersécurité visée à l'article 8, 45°, de la loi NIS2 et au CSIRT national visé à l'article 8, 46°, de la même loi** pour les besoins de l'exécution de l'article 53, § 2, de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement ;

20°/2 dans les limites du droit de l'Union européenne, à l'autorité visée à l'article 5, § 1er, de la loi du 20 juillet 2022 relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité, ou aux autorités désignées par le Roi en vertu de l'article 5, § 2, de la même loi;

21° à l'Office de contrôle des mutualités et des unions nationales de mutualités, pour l'exercice de ses missions légales visées à l'article 303, § 3, de la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance, en ce qui concerne les sociétés mutualistes visées à l'article 43bis, § 5, ou à l'article 70, §§ 6, 7 et 8, de la loi du 6 août 1990

TEXTE EN VIGUEUR

relative aux mutualités et aux unions nationales de mutualités et leurs opérations;

22° dans les limites du droit de l'Union européenne, aux autorités de résolution visées à l'article 3 de la Directive 2014/59/UE du Parlement européen et du Conseil du 15 mai 2014 établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement, aux autorités d'Etats tiers chargées de missions équivalentes à celles visées à l'article 12ter, § 1er avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'information, ainsi qu'aux ministères compétents des Etats membres de l'Espace économique européen lorsque cela s'avère nécessaire à la planification ou à la réalisation d'une action de résolution;

22° /1 dans les limites du droit de l'Union européenne, aux autorités de résolution visées à l'article 3 du Règlement 2021/23, aux autorités d'Etats tiers chargées de missions équivalentes à celles visées à l'article 12ter, § 1/1, avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'information, ainsi qu'aux ministères compétents des Etats membres de l'Espace économique européen lorsque cela s'avère nécessaire à la planification ou l'exécution d'une mesure de résolution ;

23° à toute personne exerçant une tâche, prévue par ou en vertu de la loi, qui participe ou contribue à l'exercice de la mission de contrôle de la Banque lorsque cette personne a été désignée par ou avec l'accord de la Banque et aux fins de cette tâche, telle notamment:

a) le surveillant de portefeuille visé à l'article 16 de l'Annexe III à la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit [...];

b) le gestionnaire de portefeuille visé à l'article 8 de l'Annexe III à la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit [...]; et

PROJET DE LOI

relative aux mutualités et aux unions nationales de mutualités et leurs opérations;

22° dans les limites du droit de l'Union européenne, aux autorités de résolution visées à l'article 3 de la Directive 2014/59/UE du Parlement européen et du Conseil du 15 mai 2014 établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement, aux autorités d'Etats tiers chargées de missions équivalentes à celles visées à l'article 12ter, § 1er avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'information, ainsi qu'aux ministères compétents des Etats membres de l'Espace économique européen lorsque cela s'avère nécessaire à la planification ou à la réalisation d'une action de résolution;

22° /1 dans les limites du droit de l'Union européenne, aux autorités de résolution visées à l'article 3 du Règlement 2021/23, aux autorités d'Etats tiers chargées de missions équivalentes à celles visées à l'article 12ter, § 1/1, avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'information, ainsi qu'aux ministères compétents des Etats membres de l'Espace économique européen lorsque cela s'avère nécessaire à la planification ou l'exécution d'une mesure de résolution ;

23° à toute personne exerçant une tâche, prévue par ou en vertu de la loi, qui participe ou contribue à l'exercice de la mission de contrôle de la Banque lorsque cette personne a été désignée par ou avec l'accord de la Banque et aux fins de cette tâche, telle notamment:

a) le surveillant de portefeuille visé à l'article 16 de l'Annexe III à la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit [...];

b) le gestionnaire de portefeuille visé à l'article 8 de l'Annexe III à la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit [...]; et

TEXTE EN VIGUEUR

c) le commissaire spécial et l'administrateur provisoire visés à l'article 236, § 1er, de la loi précitée du 25 avril 2014, à l'article 204, § 1er de la loi du 20 juillet 2022 relative au statut et au contrôle des sociétés de bourse et portant dispositions diverses, à l'article 517, § 1er, de la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance, l'article 117, § 1er, de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement, l'article 215, § 1er, de la loi précitée, l'article 48, alinéa 1er, de l'arrêté royal du 30 avril 1999 réglementant le statut et le contrôle des sociétés de cautionnement mutuel et l'article 36/30, § 1er, alinéa 2, et l'article 36/30/1, § 2 de la présente loi ;

24° dans les limites du droit de l'Union européenne, aux autorités visées à l'article 7 de la loi du 7 avril 2019 pour les besoins de l'exécution des dispositions de la loi du 7 avril 2019 et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques;

25° au Service Public Fédéral Economie, P.M.E., Classes moyennes et Energie dans l'exercice de sa mission visée à l'article 85, § 1er 5°, de la loi du 18 septembre 2017 à l'égard des entités visées à l'article 5, § 1er, 21°, de la même loi;

26° dans les limites du droit de l'Union européenne, aux cellules de renseignement financier visées à l'article 4, 15° de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces;

27° en cas de détérioration de la situation financière d'un établissement financier visé à l'article 36/2, au Ministère public ;

PROJET DE LOI

c) le commissaire spécial et l'administrateur provisoire visés à l'article 236, § 1er, de la loi précitée du 25 avril 2014, à l'article 204, § 1er de la loi du 20 juillet 2022 relative au statut et au contrôle des sociétés de bourse et portant dispositions diverses, à l'article 517, § 1er, de la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance, l'article 117, § 1er, de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement, l'article 215, § 1er, de la loi précitée, l'article 48, alinéa 1er, de l'arrêté royal du 30 avril 1999 réglementant le statut et le contrôle des sociétés de cautionnement mutuel et l'article 36/30, § 1er, alinéa 2, et l'article 36/30/1, § 2 de la présente loi ;

24° dans les limites du droit de l'Union européenne, **aux autorités visées à l'article 15 de la loi NIS2 pour les besoins de l'exécution des dispositions de la loi NIS2** et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques;

25° au Service Public Fédéral Economie, P.M.E., Classes moyennes et Energie dans l'exercice de sa mission visée à l'article 85, § 1er 5°, de la loi du 18 septembre 2017 à l'égard des entités visées à l'article 5, § 1er, 21°, de la même loi;

26° dans les limites du droit de l'Union européenne, aux cellules de renseignement financier visées à l'article 4, 15° de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces;

27° en cas de détérioration de la situation financière d'un établissement financier visé à l'article 36/2, au Ministère public ;

TEXTE EN VIGUEUR

28° dans les limites du droit de l'Union européenne, à la Commission européenne lorsque ces informations sont nécessaires à l'exercice des compétences de cette dernière.

§ 2. La Banque ne peut communiquer des informations confidentielles en vertu du paragraphe 1er qu'aux conditions suivantes :

1° les informations sont destinées à l'accomplissement des missions des autorités ou organismes qui en sont les destinataires, ce qui inclut la communication desdites informations à des tiers en application d'une obligation légale applicable à ces autorités ou organismes; dans les autres cas, la Banque peut autoriser, dans les limites du droit de l'Union européenne, les destinataires desdites informations à les divulguer à des tiers, moyennant l'accord préalable de la Banque et, le cas échéant, aux seules fins pour lesquelles la Banque a marqué son accord;

2° les informations ainsi communiquées à des autorités ou organismes étrangers sont couvertes dans leur chef par une obligation de secret professionnel équivalente à celui prévu à l'article 35; et

3° lorsque les informations concernées proviennent d'une autorité d'un autre Etat membre de l'Espace économique européen, elles ne peuvent être divulguées aux autorités ou organismes suivants qu'avec l'accord explicite de l'autorité communicante et, le cas échéant, aux seules fins pour lesquelles cette dernière a marqué son accord :

a) les autorités ou organismes visés aux paragraphes 1er, 5°, 6°, 8° et 11° ;

b) les autorités ou organismes d'Etats tiers visés aux paragraphes 1er, 3°, 5°, 8°, 9°, 11°, 18° et 22° ;

PROJET DE LOI

28° dans les limites du droit de l'Union européenne, à la Commission européenne lorsque ces informations sont nécessaires à l'exercice des compétences de cette dernière.

§ 2. La Banque ne peut communiquer des informations confidentielles en vertu du paragraphe 1er qu'aux conditions suivantes :

1° les informations sont destinées à l'accomplissement des missions des autorités ou organismes qui en sont les destinataires, ce qui inclut la communication desdites informations à des tiers en application d'une obligation légale applicable à ces autorités ou organismes; dans les autres cas, la Banque peut autoriser, dans les limites du droit de l'Union européenne, les destinataires desdites informations à les divulguer à des tiers, moyennant l'accord préalable de la Banque et, le cas échéant, aux seules fins pour lesquelles la Banque a marqué son accord;

2° les informations ainsi communiquées à des autorités ou organismes étrangers sont couvertes dans leur chef par une obligation de secret professionnel équivalente à celui prévu à l'article 35; et

3° lorsque les informations concernées proviennent d'une autorité d'un autre Etat membre de l'Espace économique européen, elles ne peuvent être divulguées aux autorités ou organismes suivants qu'avec l'accord explicite de l'autorité communicante et, le cas échéant, aux seules fins pour lesquelles cette dernière a marqué son accord :

a) les autorités ou organismes visés aux paragraphes 1er, 5°, 6°, 8° et 11° ;

b) les autorités ou organismes d'Etats tiers visés aux paragraphes 1er, 3°, 5°, 8°, 9°, 11°, 18° et 22° ;

TEXTE EN VIGUEUR

c) les autorités ou organismes d'Etats tiers exerçant des missions équivalentes à celles de la FSMA.

§ 3. Sans préjudice des dispositions plus sévères des lois particulières qui les régissent, les personnes, autorités et organismes de droit belge visés au paragraphe 1er sont tenus au secret professionnel prévu à l'article 35 quant aux informations confidentielles reçues de la Banque en application du paragraphe 1er.

§ 4. [...]

Article 36/47

Pour l'application de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, la Banque est désignée comme autorité sectorielle et service d'inspection pour les opérateurs du secteur des finances, à l'exception des opérateurs de plate-forme de négociation au sens de l'article 3, 6°, de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE.

Les articles 36/19 et 36/20 sont applicables.

La Commission des sanctions statue sur l'imposition des amendes administratives prévues à l'article 52 de la loi précitée du 7 avril 2019. Les articles 36/8 à 36/12/3 et l'article 36/21 sont applicables.

PROJET DE LOI

c) les autorités ou organismes d'Etats tiers exerçant des missions équivalentes à celles de la FSMA.

§ 3. Sans préjudice des dispositions plus sévères des lois particulières qui les régissent, les personnes, autorités et organismes de droit belge visés au paragraphe 1er sont tenus au secret professionnel prévu à l'article 35 quant aux informations confidentielles reçues de la Banque en application du paragraphe 1er.

§ 4. [...]

Article 36/47

Pour l'application de la loi NIS2, la Banque est désignée comme autorité sectorielle et service d'inspection sectoriel pour les entités du secteur des finances, à l'exception des opérateurs de plate-forme de négociation au sens de l'article 3, 6°, de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE.

Si elle le juge utile, la Banque partage le plus vite possible avec la BCE les informations pertinentes sur les notifications d'incident qu'elle reçoit en vertu de la loi NIS2 ou du Règlement 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.

[...]

TEXTE EN VIGUEUR

La Banque partage avec la BCE le plus vite [...] possible les informations pertinentes sur les notifications d'incident qu'elle reçoit en vertu de la loi du 7 avril 2019.

PROJET DE LOI**Loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers****Article 75**

§ 1^{er}. Par dérogation à l'article 74, alinéa 1er, et dans les limites du droit de l'Union européenne la FSMA peut communiquer des informations confidentielles :

1° à la Banque centrale européenne, à la Banque et aux autres banques centrales et organismes à vocation similaire en leur qualité d'autorités monétaires, ainsi qu'à d'autres autorités publiques chargées de la surveillance des systèmes de paiement et de règlement;

à la Banque centrale européenne, à la Banque et aux autres banques centrales et organismes à vocation similaire en leur qualité d'autorités monétaires lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales respectives, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier, de même qu'à d'autres autorités publiques chargées de la surveillance des systèmes de paiement.

Lorsque survient une situation d'urgence, notamment une évolution défavorable des marchés financiers, susceptible de menacer la liquidité du marché et la stabilité du système financier dans un des Etats membres dans lequel des entités d'un groupe comprenant des entreprises d'investissement ont été agréées ou dans lequel sont établies des succursales d'importance significative au sens de l'article 59, §§ 6 et 7, de la loi du 25 octobre 2016, la FSMA peut transmettre des informations aux banques centrales du Système européen de banques centrales lorsque ces informations sont pertinentes pour l'exercice de leurs missions

Article 75

§ 1^{er}. Par dérogation à l'article 74, alinéa 1er, et dans les limites du droit de l'Union européenne la FSMA peut communiquer des informations confidentielles :

1° à la Banque centrale européenne, à la Banque et aux autres banques centrales et organismes à vocation similaire en leur qualité d'autorités monétaires, ainsi qu'à d'autres autorités publiques chargées de la surveillance des systèmes de paiement et de règlement;

à la Banque centrale européenne, à la Banque et aux autres banques centrales et organismes à vocation similaire en leur qualité d'autorités monétaires lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales respectives, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier, de même qu'à d'autres autorités publiques chargées de la surveillance des systèmes de paiement.

Lorsque survient une situation d'urgence, notamment une évolution défavorable des marchés financiers, susceptible de menacer la liquidité du marché et la stabilité du système financier dans un des Etats membres dans lequel des entités d'un groupe comprenant des entreprises d'investissement ont été agréées ou dans lequel sont établies des succursales d'importance significative au sens de l'article 59, §§ 6 et 7, de la loi du 25 octobre 2016, la FSMA peut transmettre des informations aux banques centrales du Système européen de banques centrales lorsque ces informations sont pertinentes pour l'exercice de leurs missions

TEXTE EN VIGUEUR

légales, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier.

En cas de situation d'urgence telle que visée ci-dessus, la FSMA peut divulguer, dans tous les Etats membres concernés, des informations qui présentent un intérêt pour les départements d'administrations centrales responsables de la législation relative à la surveillance des établissements de crédit, des établissements financiers, des services d'investissement et des entreprises d'assurances;

1° bis à la Banque;, à la Banque centrale européenne en ce qui concerne les missions qui lui sont confiées par le Règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit et aux autres membres du SEBC;

2° à l'Agence Fédérale de la Dette;

3° aux autorités compétentes d'autres Etats membres de l'Espace économique européen qui exercent une ou plusieurs compétences comparables à celles visées à l'article 45;

4° aux autorités compétentes d'Etats tiers qui exercent une ou plusieurs compétences comparables à celles visées à l'article 45 et avec lesquels la FSMA a conclu un accord de coopération prévoyant un échange d'informations;

5° et aux autorités de régulation nationales visées à l'article 2, point 10, du règlement 1227/2011 et, pour ce qui est du règlement 596/2014, à la Commission européenne et aux autres autorités visées à l'article 25 de ce règlement;

PROJET DE LOI

légales, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier.

En cas de situation d'urgence telle que visée ci-dessus, la FSMA peut divulguer, dans tous les Etats membres concernés, des informations qui présentent un intérêt pour les départements d'administrations centrales responsables de la législation relative à la surveillance des établissements de crédit, des établissements financiers, des services d'investissement et des entreprises d'assurances;

1° bis à la Banque;, à la Banque centrale européenne en ce qui concerne les missions qui lui sont confiées par le Règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit et aux autres membres du SEBC;

2° à l'Agence Fédérale de la Dette;

3° aux autorités compétentes d'autres Etats membres de l'Espace économique européen qui exercent une ou plusieurs compétences comparables à celles visées à l'article 45;

4° aux autorités compétentes d'Etats tiers qui exercent une ou plusieurs compétences comparables à celles visées à l'article 45 et avec lesquels la FSMA a conclu un accord de coopération prévoyant un échange d'informations;

5° et aux autorités de régulation nationales visées à l'article 2, point 10, du règlement 1227/2011 et, pour ce qui est du règlement 596/2014, à la Commission européenne et aux autres autorités visées à l'article 25 de ce règlement;

TEXTE EN VIGUEUR

6° aux organismes belges ou d'un autre Etat membre de l'Espace économique européen gérant un système de protection des dépôts, des investisseurs ou des assurances sur la vie;

7° aux contreparties centrales ou aux dépositaires centraux de titres qui sont autorisés à assurer des services de compensation ou de règlement de transactions sur instruments financiers effectuées sur un marché organisé belge, dans la mesure où la FSMA estime que la communication des informations en question est nécessaire en vue de garantir le fonctionnement régulier de ces organismes par rapport à des manquements, même potentiels, d'intervenants sur le marché concerné;

8° aux opérateurs de marché pour le bon fonctionnement, le contrôle et la surveillance des marchés qu'ils organisent;

9° au cours de procédures civiles ou commerciales, aux autorités et mandataires de justice impliqués dans des procédures de faillite ou de réorganisation judiciaire ou des procédures collectives analogues concernant des entreprises soumises au contrôle de la FSMA ou dont les opérations sont soumises à son contrôle, à l'exception des informations confidentielles concernant la participation de tiers à des tentatives de sauvetage antérieures à ces procédures;

10° aux commissaires et réviseurs d'entreprises et aux autres contrôleurs légaux des comptes des entreprises soumises au contrôle de la FSMA, d'autres établissements financiers belges ou d'entreprises similaires étrangères;

11° aux séquestres, pour l'exercice de leur mission visée dans les lois régissant les missions confiées à la FSMA;

12° au Collège de supervision des réviseurs d'entreprises et aux autorités d'Etats membres ou de pays tiers investies de la surveillance des personnes chargées du contrôle légal des comptes annuels des entreprises soumises au contrôle de la FSMA;

PROJET DE LOI

6° aux organismes belges ou d'un autre Etat membre de l'Espace économique européen gérant un système de protection des dépôts, des investisseurs ou des assurances sur la vie;

7° aux contreparties centrales ou aux dépositaires centraux de titres qui sont autorisés à assurer des services de compensation ou de règlement de transactions sur instruments financiers effectuées sur un marché organisé belge, dans la mesure où la FSMA estime que la communication des informations en question est nécessaire en vue de garantir le fonctionnement régulier de ces organismes par rapport à des manquements, même potentiels, d'intervenants sur le marché concerné;

8° aux opérateurs de marché pour le bon fonctionnement, le contrôle et la surveillance des marchés qu'ils organisent;

9° au cours de procédures civiles ou commerciales, aux autorités et mandataires de justice impliqués dans des procédures de faillite ou de réorganisation judiciaire ou des procédures collectives analogues concernant des entreprises soumises au contrôle de la FSMA ou dont les opérations sont soumises à son contrôle, à l'exception des informations confidentielles concernant la participation de tiers à des tentatives de sauvetage antérieures à ces procédures;

10° aux commissaires et réviseurs d'entreprises et aux autres contrôleurs légaux des comptes des entreprises soumises au contrôle de la FSMA, d'autres établissements financiers belges ou d'entreprises similaires étrangères;

11° aux séquestres, pour l'exercice de leur mission visée dans les lois régissant les missions confiées à la FSMA;

12° au Collège de supervision des réviseurs d'entreprises et aux autorités d'Etats membres ou de pays tiers investies de la surveillance des personnes chargées du contrôle légal des comptes annuels des entreprises soumises au contrôle de la FSMA;

TEXTE EN VIGUEUR

13° au Service public fédéral Economie, PME, Classes moyennes et Energie pour le contrôle relatif au crédit à la consommation, et pour le contrôle relatif au crédit hypothécaire aux pratiques du marché et aux services de paiement, aux autorités compétentes d'autres Etats membres de l'Espace économique européen qui exercent une compétence comparable, ainsi qu'aux autorités compétentes d'Etats tiers qui exercent une compétence comparable et avec lesquelles la FSMA a conclu un accord de coopération prévoyant un échange d'informations;

14° à l'Autorité belge de la concurrence;

15° les autorités visées à l'article 7 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique pour les besoins de l'exécution des dispositions de cette loi et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ;

16° à l'Administration générale de la Trésorerie du Service fédéral Finances lorsqu'une telle communication est prévue par le droit de l'Union européenne ou par une disposition légale ou réglementaire en matière de sanctions financières (notamment les dispositions contraignantes relatives aux embargos financiers telles que définies à l'article 4, 6° de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces) ou lorsque l'Administration générale de la Trésorerie agit en qualité d'autorité de contrôle assurant le respect du règlement (CE) 2271/96 du Conseil du 22 novembre 1996 portant protection contre les effets de l'application extraterritoriale d'une législation adoptée par un pays tiers, ainsi que des actions fondées sur elle ou en découlant;

17° aux actuaires indépendants des entreprises exerçant, en vertu de la loi, une tâche de

PROJET DE LOI

13° au Service public fédéral Economie, PME, Classes moyennes et Energie pour le contrôle relatif au crédit à la consommation, et pour le contrôle relatif au crédit hypothécaire aux pratiques du marché et aux services de paiement, aux autorités compétentes d'autres Etats membres de l'Espace économique européen qui exercent une compétence comparable, ainsi qu'aux autorités compétentes d'Etats tiers qui exercent une compétence comparable et avec lesquelles la FSMA a conclu un accord de coopération prévoyant un échange d'informations;

14° à l'Autorité belge de la concurrence;

15° les autorités visées à l'**article 15 de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique** pour les besoins de l'exécution des dispositions de cette loi et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ;

16° à l'Administration générale de la Trésorerie du Service fédéral Finances lorsqu'une telle communication est prévue par le droit de l'Union européenne ou par une disposition légale ou réglementaire en matière de sanctions financières (notamment les dispositions contraignantes relatives aux embargos financiers telles que définies à l'article 4, 6° de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces) ou lorsque l'Administration générale de la Trésorerie agit en qualité d'autorité de contrôle assurant le respect du règlement (CE) 2271/96 du Conseil du 22 novembre 1996 portant protection contre les effets de l'application extraterritoriale d'une législation adoptée par un pays tiers, ainsi que des actions fondées sur elle ou en découlant;

17° aux actuaires indépendants des entreprises exerçant, en vertu de la loi, une tâche de

TEXTE EN VIGUEUR

contrôle sur ces entreprises ainsi qu'aux organes chargés de la surveillance de ces actuares;

18° à Fedris;

19° à l'OCM, en sa qualité d'autorité de contrôle des sociétés mutualistes visées aux articles 43bis, § 5, et 70, §§ 6 et 7, de la loi du 6 août 1990 relative aux mutualités et aux unions nationales de mutualités et des intermédiaires d'assurances visés à l'article 68 de la loi du 26 avril 2010 portant des dispositions diverses en matière d'organisation de l'assurance maladie complémentaire (I), ainsi que de leurs activités;

19° [...]

20° [...]

21° à l'ESMA, l'EIOPA et l'EBA et au Comité européen du risque systémique.

22° aux autorités investies de la surveillance des personnes exerçant des activités sur les marchés des quotas d'émission;

23° aux autorités investies de la surveillance des personnes exerçant des activités sur les marchés dérivés de matières premières agricoles;

24° à l'Autorité belge de protection des données;

24° /1 à la Cellule de traitement des informations financières, visée à l'article 76 de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces ; "

b) dans le 26° de la même loi, modifié pour la dernière fois par la loi du 23 février 2022, les mots "et aux personnes ayant introduit une réclamation auprès de la FSMA, en application de l'article 50 du Règlement 2019/1238, ainsi qu'aux fournisseurs et distributeurs de PEPP au sens du règlement précité" sont insérés entre les mots "ainsi qu'aux prestataires de services de financement participatif," et les mots "dans la mesure nécessaire";

PROJET DE LOI

contrôle sur ces entreprises ainsi qu'aux organes chargés de la surveillance de ces actuares;

18° à Fedris;

19° à l'OCM, en sa qualité d'autorité de contrôle des sociétés mutualistes visées aux articles 43bis, § 5, et 70, §§ 6 et 7, de la loi du 6 août 1990 relative aux mutualités et aux unions nationales de mutualités et des intermédiaires d'assurances visés à l'article 68 de la loi du 26 avril 2010 portant des dispositions diverses en matière d'organisation de l'assurance maladie complémentaire (I), ainsi que de leurs activités;

19° [...]

20° [...]

21° à l'ESMA, l'EIOPA et l'EBA et au Comité européen du risque systémique.

22° aux autorités investies de la surveillance des personnes exerçant des activités sur les marchés des quotas d'émission;

23° aux autorités investies de la surveillance des personnes exerçant des activités sur les marchés dérivés de matières premières agricoles;

24° à l'Autorité belge de protection des données;

24° /1 à la Cellule de traitement des informations financières, visée à l'article 76 de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces ; "

b) dans le 26° de la même loi, modifié pour la dernière fois par la loi du 23 février 2022, les mots "et aux personnes ayant introduit une réclamation auprès de la FSMA, en application de l'article 50 du Règlement 2019/1238, ainsi qu'aux fournisseurs et distributeurs de PEPP au sens du règlement précité" sont insérés entre les mots "ainsi qu'aux prestataires de services de financement participatif," et les mots "dans la mesure nécessaire";

TEXTE EN VIGUEUR

25° au cours de procédures de liquidation d'une institution de retraite professionnelle ou d'un régime de retraite au sens de la loi du 27 octobre 2006 relative au contrôle des institutions de retraite professionnelle, aux autorités et personnes impliquées dans ces procédures, ainsi qu'aux autorités chargées de la surveillance de ces autorités ou personnes;

26° aux personnes ayant introduit une réclamation auprès de la FSMA, en application de l'article 38 du règlement 2020/1503 du Parlement européen et du Conseil du 7 octobre 2020 relatif aux prestataires européens de services de financement participatif pour les entrepreneurs, et modifiant le règlement (UE) 2017/1129 et la directive (UE) 2019/1937, ainsi qu'aux prestataires de services de financement participatif, dans la mesure nécessaire pour le traitement de ladite réclamation;

27° à l'autorité visée à l'article 5, § 1er, de la loi du 20 juillet 2022 relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité ou aux autorités désignées par le Roi en vertu de l'article 5, § 2, de la même loi;

27° /1 à la Commission européenne, dans le cadre du contrôle des sociétés de gestion de portefeuille et de conseil en investissement conformément à l'article 45, § 1er, 2°, a), lorsque ces informations sont nécessaires à l'exercice de ses compétences.

§ 2. La FSMA ne peut communiquer des informations confidentielles en vertu du § 1er qu'à condition qu'elles soient destinées à l'accomplissement des missions des autorités ou organismes qui en sont les destinataires et que les informations soient dans leur chef couvertes par un devoir de secret professionnel équivalent à celui prévu à l'article 74. En outre, les informations suivantes ne peuvent être divulguées qu'avec l'accord explicite de l'autorité dont elles proviennent et, le cas

PROJET DE LOI

25° au cours de procédures de liquidation d'une institution de retraite professionnelle ou d'un régime de retraite au sens de la loi du 27 octobre 2006 relative au contrôle des institutions de retraite professionnelle, aux autorités et personnes impliquées dans ces procédures, ainsi qu'aux autorités chargées de la surveillance de ces autorités ou personnes;

26° aux personnes ayant introduit une réclamation auprès de la FSMA, en application de l'article 38 du règlement 2020/1503 du Parlement européen et du Conseil du 7 octobre 2020 relatif aux prestataires européens de services de financement participatif pour les entrepreneurs, et modifiant le règlement (UE) 2017/1129 et la directive (UE) 2019/1937, ainsi qu'aux prestataires de services de financement participatif, dans la mesure nécessaire pour le traitement de ladite réclamation;

27° à l'autorité visée à l'article 5, § 1er, de la loi du 20 juillet 2022 relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité ou aux autorités désignées par le Roi en vertu de l'article 5, § 2, de la même loi;

27° /1 à la Commission européenne, dans le cadre du contrôle des sociétés de gestion de portefeuille et de conseil en investissement conformément à l'article 45, § 1er, 2°, a), lorsque ces informations sont nécessaires à l'exercice de ses compétences.

§ 2. La FSMA ne peut communiquer des informations confidentielles en vertu du § 1er qu'à condition qu'elles soient destinées à l'accomplissement des missions des autorités ou organismes qui en sont les destinataires et que les informations soient dans leur chef couvertes par un devoir de secret professionnel équivalent à celui prévu à l'article 74. En outre, les informations suivantes ne peuvent être divulguées qu'avec l'accord explicite de l'autorité dont elles proviennent et, le cas

TEXTE EN VIGUEUR

échéant, aux seules fins pour lesquelles cette autorité a marqué son accord:

1° les informations provenant d'une autorité d'un autre Etat membre de l'Espace économique européen, dans les cas visés aux 7°, 9°, 10°, 12° et 17° du paragraphe 1er;

2° les informations provenant d'une autorité d'un autre Etat membre de l'Espace économique européen et divulguées aux autorités ou organismes d'Etat tiers dans les cas visés aux 4° et 13° du paragraphe 1er;

3° les informations divulguées par la FSMA dans le cadre de l'exercice de ses compétences visées à l'article 45, § 1er, alinéa 1er, 2°, g), provenant des autorités ou personnes visées aux 3°, 9°, 10°, 12° et 17°, dans les cas visés au 1bis°, au 13° et au 19° du paragraphe 1er. De même, les informations obtenues par la FSMA dans le cadre de vérifications sur place dans un autre Etat membre, effectuées dans le cadre de l'exercice de ses compétences visées à l'article 45, § 1er, alinéa 1er, 2°, g), ne peuvent être divulguées qu'avec l'accord explicite de l'autorité compétente de l'Etat membre où la vérification sur place a été effectuée et le cas échéant, aux seules fins pour lesquelles cette autorité a marqué son accord.

§ 3. La FSMA peut faire usage des informations confidentielles visées à l'article 74, alinéa 1er, ou reçues de la part des autorités et organismes visés au § 1er pour l'accomplissement de l'ensemble de ses missions légales.

§ 4. Sans préjudice des dispositions plus sévères des lois particulières qui les régissent, les autorités et organismes belges visés au § 1er sont tenus au secret professionnel prévu à l'article 74 quant aux informations confidentielles qu'ils reçoivent de la FSMA en application du § 1er.

§ 5. Le présent article s'applique sans préjudice de dispositions plus restrictives du droit de l'Union européenne en matière de secret

PROJET DE LOI

échéant, aux seules fins pour lesquelles cette autorité a marqué son accord:

1° les informations provenant d'une autorité d'un autre Etat membre de l'Espace économique européen, dans les cas visés aux 7°, 9°, 10°, 12° et 17° du paragraphe 1er;

2° les informations provenant d'une autorité d'un autre Etat membre de l'Espace économique européen et divulguées aux autorités ou organismes d'Etat tiers dans les cas visés aux 4° et 13° du paragraphe 1er;

3° les informations divulguées par la FSMA dans le cadre de l'exercice de ses compétences visées à l'article 45, § 1er, alinéa 1er, 2°, g), provenant des autorités ou personnes visées aux 3°, 9°, 10°, 12° et 17°, dans les cas visés au 1bis°, au 13° et au 19° du paragraphe 1er. De même, les informations obtenues par la FSMA dans le cadre de vérifications sur place dans un autre Etat membre, effectuées dans le cadre de l'exercice de ses compétences visées à l'article 45, § 1er, alinéa 1er, 2°, g), ne peuvent être divulguées qu'avec l'accord explicite de l'autorité compétente de l'Etat membre où la vérification sur place a été effectuée et le cas échéant, aux seules fins pour lesquelles cette autorité a marqué son accord.

§ 3. La FSMA peut faire usage des informations confidentielles visées à l'article 74, alinéa 1er, ou reçues de la part des autorités et organismes visés au § 1er pour l'accomplissement de l'ensemble de ses missions légales.

§ 4. Sans préjudice des dispositions plus sévères des lois particulières qui les régissent, les autorités et organismes belges visés au § 1er sont tenus au secret professionnel prévu à l'article 74 quant aux informations confidentielles qu'ils reçoivent de la FSMA en application du § 1er.

§ 5. Le présent article s'applique sans préjudice de dispositions plus restrictives du droit de l'Union européenne en matière de secret

TEXTE EN VIGUEUR

professionnel ou de lois particulières régissant les missions de la FSMA.

PROJET DE LOI

professionnel ou de lois particulières régissant les missions de la FSMA.

Loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges

Article 1^{er}/1

La présente loi transpose partiellement les directives suivantes :

1° la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union;

2° la directive (UE) 2018/1972 du Parlement Européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen.

Article 1^{er}/1

La présente loi transpose partiellement les directives suivantes :

1° la Directive européenne (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148;

2° la directive (UE) 2018/1972 du Parlement Européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen.

Article 14

§ 1^{er}. Sans préjudice de ses compétences légales, les missions de l'Institut en ce qui concerne les réseaux de communications électroniques et les services de communications électroniques, équipement terminal équipement hertzien, en ce qui concerne le secteur des infrastructures numériques au sens de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en ce qui concerne les secteurs des communications électroniques et des infrastructures numériques au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, en ce qui concerne la lutte contre la diffusion des contenus à caractère terroriste en ligne au sens du règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, en ce qui concerne l'article XI.216/2, § 2, du Code de droit économique, et en ce qui concerne les services

Article 14

§ 1^{er}. Sans préjudice de ses compétences légales, les missions de l'Institut en ce qui concerne les réseaux de communications électroniques et les services de communications électroniques, équipement terminal équipement hertzien, en ce qui concerne le secteur des infrastructures numériques au sens de la **loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique**, en ce qui concerne les secteurs des communications électroniques et des infrastructures numériques au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, en ce qui concerne la lutte contre la diffusion des contenus à caractère terroriste en ligne au sens du règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, en ce qui concerne l'article XI.216/2, § 2, du Code de droit économique, et en ce qui concerne les

TEXTE EN VIGUEUR

postaux et les réseaux postaux publics tels que définis à l'article 2 de la loi du 26 janvier 2018 relative aux services postaux, sont les suivantes :

1° la formulation d'avis d'initiative, dans les cas prévus par les lois et arrêtés ou à la demande du ministre ou de la Chambre des représentants;

2° la prise de décisions administratives;

3° le contrôle du respect des normes suivantes et de leurs arrêtés d'exécution :

a) la loi du 13 juin 2005 relative aux communications électroniques ;

b) le Titre Ier, chapitre X et le Titre III de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques ;

c) la loi du 26 janvier 2018 relative aux services postaux à l'exception des articles 3, § 2, alinéa 5, 5, § 1er, 5/2, 5/3, 5/4, 5/5 et 10/1];

d) les articles 14, § 2, 2°, et 21, §§ 5 à 7, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges ;

e) les articles 4 et 4/1 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ;

f) la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ;

g) la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne les secteurs des communications électroniques et des infrastructures numériques ;

h) la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité

PROJET DE LOI

services postaux et les réseaux postaux publics tels que définis à l'article 2 de la loi du 26 janvier 2018 relative aux services postaux, sont les suivantes :

1° la formulation d'avis d'initiative, dans les cas prévus par les lois et arrêtés ou à la demande du ministre ou de la Chambre des représentants;

2° la prise de décisions administratives;

3° le contrôle du respect des normes suivantes et de leurs arrêtés d'exécution :

a) la loi du 13 juin 2005 relative aux communications électroniques ;

b) le Titre Ier, chapitre X et le Titre III de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques ;

c) la loi du 26 janvier 2018 relative aux services postaux à l'exception des articles 3, § 2, alinéa 5, 5, § 1er, 5/2, 5/3, 5/4, 5/5 et 10/1];

d) les articles 14, § 2, 2°, et 21, §§ 5 à 7, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges ;

e) les articles 4 et 4/1 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ;

f) la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ;

g) la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne les secteurs des communications électroniques et des infrastructures numériques ;

h) la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour

TEXTE EN VIGUEUR

publique, en ce qui concerne le secteur des infrastructures numériques ;

i) le Règlement (UE) 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la Directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques;

j) tout acte juridique contraignant en droit de l'Union européenne, qui attribue des missions à l'autorité réglementaire nationale dans le secteur des postes ou des communications électroniques;

k) toute décision contraignante adoptée par :

i) l'Institut ;

ii) les ministres sur base de l'article 105, § 6, alinéa 1er, de la loi du 13 juin 2005 relative aux communications électroniques ;

iii) la Commission européenne dans le secteur des communications électroniques ou dans le secteur postal;

l) le règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère antiterroriste en ligne, sans préjudice de tâches confiées à d'autres autorités compétentes en vertu de l'article 12, paragraphe 1er, a) et b), dudit règlement.

Pour l'application de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut est désigné comme autorité sectorielle et service d'inspection pour le secteur des infrastructures numériques. Le Roi peut fixer les modalités

PROJET DE LOI

la sécurité publique, pour ce qui concerne les tâches dévolues à l'autorité sectorielle et au service d'inspection sectoriel pour le secteur des infrastructures numériques, à l'exception des prestataires de services de confiance au sens de l'article 8, 24°, de cette même loi;

i) le Règlement (UE) 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la Directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques;

j) tout acte juridique contraignant en droit de l'Union européenne, qui attribue des missions à l'autorité réglementaire nationale dans le secteur des postes ou des communications électroniques;

k) toute décision contraignante adoptée par :

i) l'Institut ;

ii) les ministres sur base de l'article 105, § 6, alinéa 1er, de la loi du 13 juin 2005 relative aux communications électroniques ;

iii) la Commission européenne dans le secteur des communications électroniques ou dans le secteur postal;

l) le règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère antiterroriste en ligne, sans préjudice de tâches confiées à d'autres autorités compétentes en vertu de l'article 12, paragraphe 1er, a) et b), dudit règlement.

Pour l'application de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut est désigné comme autorité sectorielle au sens de l'article 8, 54°, de cette même loi et service d'inspection sectoriel au sens de l'article 44, § 1er, alinéa 2, de cette même loi pour le secteur

TEXTE EN VIGUEUR

pratiques des inspections pour ce secteur, après avis de l'Institut.

4° en cas de litige entre des fournisseurs de réseaux, de services ou d'équipements de communications électroniques ou en cas de litige entre des prestataires de services postaux, (ou en cas de litige entre les fournisseurs de services ou de réseaux de communications électroniques ou de fournisseurs de services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale,) la formulation de propositions tendant à concilier les parties dans le délai d'un mois. Le Roi fixe, sur avis de l'Institut, les modalités de cette procédure;

4° /1 en cas de litige entre fournisseurs de réseaux, de services ou d'équipements de communications électroniques ou en cas de litige entre des prestataires de services postaux, ou en cas de litige entre les fournisseurs de services ou de réseaux de communications électroniques ou de fournisseurs de services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ou en l'absence d'accord au sens de l'article XI.216/2, § 2, du Code de droit économique, la prise de décision administrative [sur base de l'article 4 ou 4/1 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges;

5° poser tous les actes utiles qui ont pour objet la préparation de l'application des directives européennes entrées en vigueur dans le secteur des postes et des télécommunications.

6° L'Institut est chargé de contrôler l'exécution de toutes les missions de service public qui sont attribuées par l'Etat dans le secteur postal et dans le secteur des communications

PROJET DE LOI

des infrastructures numériques, à l'exception des prestataires de services de confiance au sens de l'article 8, 24°, de cette même loi, et pour le secteur des services postaux et d'expédition.

4° en cas de litige entre des fournisseurs de réseaux, de services ou d'équipements de communications électroniques ou en cas de litige entre des prestataires de services postaux, (ou en cas de litige entre les fournisseurs de services ou de réseaux de communications électroniques ou de fournisseurs de services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale,) la formulation de propositions tendant à concilier les parties dans le délai d'un mois. Le Roi fixe, sur avis de l'Institut, les modalités de cette procédure;

4° /1 en cas de litige entre fournisseurs de réseaux, de services ou d'équipements de communications électroniques ou en cas de litige entre des prestataires de services postaux, ou en cas de litige entre les fournisseurs de services ou de réseaux de communications électroniques ou de fournisseurs de services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ou en l'absence d'accord au sens de l'article XI.216/2, § 2, du Code de droit économique, la prise de décision administrative [sur base de l'article 4 ou 4/1 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges;

5° poser tous les actes utiles qui ont pour objet la préparation de l'application des directives européennes entrées en vigueur dans le secteur des postes et des télécommunications.

6° L'Institut est chargé de contrôler l'exécution de toutes les missions de service public qui sont attribuées par l'Etat dans le secteur postal et dans le secteur des communications

TEXTE EN VIGUEUR

électroniques, sous réserve des missions de service publics attribué dans le cadre d'article 141, § 1er bis, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. L'Institut informe tant le Ministre en charge du Secteur postal que le Ministre en charge des Entreprises publiques de l'exécution du contrat de gestion;

7° l'exercice des missions de contrôle et de sanctions qui lui sont confiées par l'arrêté royal visant à exécuter l'article 5, § 2, de la loi du 20 juillet 2022 relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité.

§ 2. Dans le cadre de ses compétences, l'Institut :

1° peut organiser de manière non discriminatoire toute forme d'enquêtes et de consultations publiques ; il doit organiser de telles consultations publiques afin qu'il tienne compte des points de vue des utilisateurs finals, des consommateurs (y compris notamment, des consommateurs handicapés), des fabricants et des entreprises qui fournissent des réseaux et/ou des services de communications électroniques sur toute question relative à tous les droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, en particulier lorsqu'ils ont une incidence importante sur le marché; ces consultations garantissent que, lorsque l'Institut statue sur des questions relatives aux droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, les intérêts des consommateurs en matière de communications électroniques sont dûment pris en compte;

2° peut exiger, par demande motivée, de toute personne concernée toute information utile. L'Institut fixe le délai de communication des informations demandées;

PROJET DE LOI

électroniques, sous réserve des missions de service publics attribué dans le cadre d'article 141, § 1er bis, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. L'Institut informe tant le Ministre en charge du Secteur postal que le Ministre en charge des Entreprises publiques de l'exécution du contrat de gestion;

7° l'exercice des missions de contrôle et de sanctions qui lui sont confiées par l'arrêté royal visant à exécuter l'article 5, § 2, de la loi du 20 juillet 2022 relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité.

§ 2. Dans le cadre de ses compétences, l'Institut :

1° peut organiser de manière non discriminatoire toute forme d'enquêtes et de consultations publiques ; il doit organiser de telles consultations publiques afin qu'il tienne compte des points de vue des utilisateurs finals, des consommateurs (y compris notamment, des consommateurs handicapés), des fabricants et des entreprises qui fournissent des réseaux et/ou des services de communications électroniques sur toute question relative à tous les droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, en particulier lorsqu'ils ont une incidence importante sur le marché; ces consultations garantissent que, lorsque l'Institut statue sur des questions relatives aux droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, les intérêts des consommateurs en matière de communications électroniques sont dûment pris en compte;

2° peut exiger, par demande motivée, de toute personne concernée toute information utile. L'Institut fixe le délai de communication des informations demandées;

TEXTE EN VIGUEUR

3° coopère avec et communique de l'information à :

a) la Commission européenne , l'ENISA, l'Office et à l'ORECE; e) les autorités belges en charge de la concurrence;

b) les autorités de régulation étrangères en matière de services postaux et de télécommunications;

c) les autorités de régulation des autres secteurs économiques;

d) les services publics fédéraux en charge de la protection des consommateurs;

e) les autorités belges en charge de la concurrence;

Après consultation de ces autorités et de l'Institut et sur proposition conjointe du ministre de l'Economie et du ministre, le Roi peut fixer les modalités de la coopération, de la consultation et de l'échange d'informations entre ces instances et l'Institut;

f) les autorités régulatrices des Communautés et des Régions, selon les modalités convenues dans les accords de coopération avec ces niveaux de pouvoir;

g) les services publics qui ont une compétence en matière de sécurité publique, en ce compris la sécurité des réseaux et des systèmes d'information, ou de sécurité et protection civile, ou de défense civile, ou de planification de crise, ou de sécurité ou de protection du potentiel économique et scientifique du pays;

h) l'Autorité de protection des données;

i) le Service public fédéral chargé des statistiques et de l'information économique;

j) les ministres visés à l'article 105, § 1er, alinéa 3, 1°, de la loi du 13 juin 2005 relative aux communications électroniques et leur cabinet, pour la mise en oeuvre de cet article ;

PROJET DE LOI

3° coopère avec et communique de l'information à :

a) la Commission européenne , l'ENISA, l'Office et à l'ORECE; e) les autorités belges en charge de la concurrence;

b) les autorités de régulation étrangères en matière de services postaux et de télécommunications;

c) les autorités de régulation des autres secteurs économiques;

d) les services publics fédéraux en charge de la protection des consommateurs;

e) les autorités belges en charge de la concurrence;

Après consultation de ces autorités et de l'Institut et sur proposition conjointe du ministre de l'Economie et du ministre, le Roi peut fixer les modalités de la coopération, de la consultation et de l'échange d'informations entre ces instances et l'Institut;

f) les autorités régulatrices des Communautés et des Régions, selon les modalités convenues dans les accords de coopération avec ces niveaux de pouvoir;

g) les services publics qui ont une compétence en matière de sécurité publique, en ce compris la sécurité des réseaux et des systèmes d'information, ou de sécurité et protection civile, ou de défense civile, ou de planification de crise, ou de sécurité ou de protection du potentiel économique et scientifique du pays;

h) l'Autorité de protection des données;

i) le Service public fédéral chargé des statistiques et de l'information économique;

j) les ministres visés à l'article 105, § 1er, alinéa 3, 1°, de la loi du 13 juin 2005 relative aux communications électroniques et leur cabinet, pour la mise en oeuvre de cet article ;

TEXTE EN VIGUEUR**PROJET DE LOI**

k) le Parquet fédéral et les autorités compétentes des autres Etats membres visées au règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère antiterroriste en ligne;

k) les inspecteurs sociaux de la Direction générale Contrôle des lois sociales du Service public fédéral Emploi, Travail et Concertation sociale, les inspecteurs sociaux de l'Inspection de l'Office national de Sécurité sociale, et les inspecteurs sociaux de l'Inspection de l'Office national de l'Emploi et les inspecteurs sociaux de l'Institut national d'assurances sociales pour travailleurs indépendants;

l) les agents de la Direction générale de l'Inspection économique du Service public fédéral Economie, P.M.E., Classes moyennes et Energie;

4° apporte sa collaboration aux activités de la Commission mixte des télécommunications, créée par l'arrêté royal du 10 décembre 1957, modifié par l'arrêté royal du 24 septembre 1993;

5° l'Institut peut uniquement prendre des décisions relatives aux réseaux de communications électroniques pour lesquels les Communautés sont également compétentes, après l'entrée en vigueur d'un accord de coopération avec les Communautés portant sur l'exercice des compétences en matière de réseaux de communications électroniques.

6° peut procéder, en respectant les motifs de l'annulation et sans modifier l'étendue de son champ d'application, à la réfection d'une décision annulée par une autorité juridictionnelle lorsque, du fait de cette annulation, un ou plusieurs des objectifs visés à l'article 6 de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 35 de la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ne sont plus réalisés. L'Institut peut procéder à une même réfection lorsque la

k) le Parquet fédéral et les autorités compétentes des autres Etats membres visées au règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère antiterroriste en ligne;

k) les inspecteurs sociaux de la Direction générale Contrôle des lois sociales du Service public fédéral Emploi, Travail et Concertation sociale, les inspecteurs sociaux de l'Inspection de l'Office national de Sécurité sociale, et les inspecteurs sociaux de l'Inspection de l'Office national de l'Emploi et les inspecteurs sociaux de l'Institut national d'assurances sociales pour travailleurs indépendants;

l) les agents de la Direction générale de l'Inspection économique du Service public fédéral Economie, P.M.E., Classes moyennes et Energie;

4° apporte sa collaboration aux activités de la Commission mixte des télécommunications, créée par l'arrêté royal du 10 décembre 1957, modifié par l'arrêté royal du 24 septembre 1993;

5° l'Institut peut uniquement prendre des décisions relatives aux réseaux de communications électroniques pour lesquels les Communautés sont également compétentes, après l'entrée en vigueur d'un accord de coopération avec les Communautés portant sur l'exercice des compétences en matière de réseaux de communications électroniques.

6° peut procéder, en respectant les motifs de l'annulation et sans modifier l'étendue de son champ d'application, à la réfection d'une décision annulée par une autorité juridictionnelle lorsque, du fait de cette annulation, un ou plusieurs des objectifs visés à l'article 6 de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 35 de la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ne sont plus réalisés. L'Institut peut procéder à une même réfection lorsque la

TEXTE EN VIGUEUR

décision annulée concerne le secteur postal et qu'un ou plusieurs des objectifs suivants ne sont plus réalisés :

- veiller à la qualité et à la pérennité du service universel;
- veiller aux intérêts des utilisateurs des services postaux;
- contribuer au développement d'un marché intérieur des services postaux;
- promouvoir la concurrence dans le secteur postal;

7° peut, en sa qualité de service d'inspection, exiger à tout moment la communication du plan de sécurité de l'exploitant, en dérogation à l'article 25, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

§ 3. Dans le cadre de la coopération avec les autorités énumérées au point 3 du paragraphe précédent, les membres du Conseil et les membres du personnel de l'Institut peuvent communiquer à ces autorités des informations confidentielles dont ils ont connaissance dans l'exercice de leur fonction, dans la mesure où cette communication est nécessaire pour l'accomplissement des missions de ces autorités.

PROJET DE LOI

décision annulée concerne le secteur postal et qu'un ou plusieurs des objectifs suivants ne sont plus réalisés :

- veiller à la qualité et à la pérennité du service universel;
- veiller aux intérêts des utilisateurs des services postaux;
- contribuer au développement d'un marché intérieur des services postaux;
- promouvoir la concurrence dans le secteur postal;

7° peut, en sa qualité de service d'inspection, exiger à tout moment la communication du plan de sécurité de l'exploitant, en dérogation à l'article 25, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

§ 3. Dans le cadre de la coopération avec les autorités énumérées au point 3 du paragraphe précédent, les membres du Conseil et les membres du personnel de l'Institut peuvent communiquer à ces autorités des informations confidentielles dont ils ont connaissance dans l'exercice de leur fonction, dans la mesure où cette communication est nécessaire pour l'accomplissement des missions de ces autorités.

Loi du 13 juin 2005 relative aux communications électroniques**Article 1^{er}**

La présente loi règle une matière visée à l'article 78 de la Constitution.

La présente loi transpose partiellement les directives suivantes:

1° la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive "Vie privée et

Article 1^{er}

La présente loi règle une matière visée à l'article 78 de la Constitution.

La présente loi transpose partiellement les directives suivantes:

1° la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive "Vie privée et

TEXTE EN VIGUEUR

communications électroniques") (J.O.C.E. 31 juillet 2002, L 201/37);

2° la directive 2002/77/CE de la Commission du 16 septembre 2002 relative à la concurrence dans les marchés des réseaux et des services de communications électroniques (directive "Concurrence") (J.O.C.E. 17 septembre 2002, L 249/21);

3° la directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des Etats membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE;

4° la directive 2014/61/UE du Parlement européen et du Conseil du 15 mai 2014 relative à des mesures visant à réduire le coût du déploiement des réseaux de communications électroniques à haut débit;

5° la directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des Etats membres relatives à la fourniture de services de médias audiovisuels (directive "Services de médias audiovisuels"), compte tenu de l'évolution des réalités du marché;

6° la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen.

Article 2**PROJET DE LOI**

communications électroniques") (J.O.C.E. 31 juillet 2002, L 201/37);

2° la directive 2002/77/CE de la Commission du 16 septembre 2002 relative à la concurrence dans les marchés des réseaux et des services de communications électroniques (directive "Concurrence") (J.O.C.E. 17 septembre 2002, L 249/21);

3° la directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des Etats membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE;

4° la directive 2014/61/UE du Parlement européen et du Conseil du 15 mai 2014 relative à des mesures visant à réduire le coût du déploiement des réseaux de communications électroniques à haut débit;

5° la directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des Etats membres relatives à la fourniture de services de médias audiovisuels (directive "Services de médias audiovisuels"), compte tenu de l'évolution des réalités du marché;

6° la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen ;

7° Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148.

Article 2

TEXTE EN VIGUEUR

Pour l'application de la présente loi, il faut entendre par :

1° " Institut " : l'Institut belge des services postaux et des télécommunications tel que visé à l'article 13 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges;

2° " ministre " : les ministres ou secrétaire d'Etat qui sont compétents pour les matières relatives aux communications électroniques telles que visées dans la présente loi;

3° "réseau de communications électroniques": les systèmes de transmission, qu'ils soient ou non fondés sur une infrastructure permanente ou une capacité d'administration centralisée et, le cas échéant, les équipements de commutation ou de routage et les autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par la voie hertziennne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux fixes (avec commutation de circuits ou de paquets, y compris l'internet) et mobiles, les systèmes utilisant le réseau électrique, dans la mesure où ils sont utilisés pour la transmission de signaux autres que ceux de services de médias audiovisuels ou sonores;

3/1° "réseau à très haute capacité": soit un réseau de communications électroniques qui est entièrement composé d'éléments de fibre optique au moins jusqu'au point de distribution au lieu de desserte, soit un réseau de communications électroniques qui est capable d'offrir, dans des conditions d'heures de pointe habituelles, une performance du réseau comparable en termes de débit descendant et ascendant, de résilience, de paramètres liés aux erreurs, de latence et de gigue; la performance du réseau peut être jugée comparable indépendamment des variations de l'expérience de l'utilisateur final qui sont dues aux caractéristiques intrinsèquement différentes du support par lequel se fait la connexion ultime du réseau au point de terminaison du réseau;

PROJET DE LOI

Pour l'application de la présente loi, il faut entendre par :

1° " Institut " : l'Institut belge des services postaux et des télécommunications tel que visé à l'article 13 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges;

2° " ministre " : les ministres ou secrétaire d'Etat qui sont compétents pour les matières relatives aux communications électroniques telles que visées dans la présente loi;

3° "réseau de communications électroniques": les systèmes de transmission, qu'ils soient ou non fondés sur une infrastructure permanente ou une capacité d'administration centralisée et, le cas échéant, les équipements de commutation ou de routage et les autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par la voie hertziennne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux fixes (avec commutation de circuits ou de paquets, y compris l'internet) et mobiles, les systèmes utilisant le réseau électrique, dans la mesure où ils sont utilisés pour la transmission de signaux autres que ceux de services de médias audiovisuels ou sonores;

3/1° "réseau à très haute capacité": soit un réseau de communications électroniques qui est entièrement composé d'éléments de fibre optique au moins jusqu'au point de distribution au lieu de desserte, soit un réseau de communications électroniques qui est capable d'offrir, dans des conditions d'heures de pointe habituelles, une performance du réseau comparable en termes de débit descendant et ascendant, de résilience, de paramètres liés aux erreurs, de latence et de gigue; la performance du réseau peut être jugée comparable indépendamment des variations de l'expérience de l'utilisateur final qui sont dues aux caractéristiques intrinsèquement différentes du support par lequel se fait la connexion ultime du réseau au point de terminaison du réseau;

TEXTE EN VIGUEUR

4° " fourniture d'un réseau de communications électroniques " : la mise en place, l'exploitation, la surveillance ou la mise à disposition d'un réseau de communications électroniques;

5° "service de communications électroniques": le service fourni normalement contre rémunération via des réseaux de communications électroniques qui, à l'exception des services consistant à fournir des contenus transmis à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus et à l'exception des services de médias audiovisuels ou sonores, comprend les types de services suivants:

a) un service d'accès à l'internet;

b) un service de communications interpersonnelles; et

c) des services consistants entièrement ou principalement en la transmission de signaux, tels que les services de transmission utilisés pour la fourniture de services de machine à machine;

5/1° "service d'accès à l'internet": un service de communications électroniques accessibles au public, qui fournit un accès à l'internet et, partant, une connectivité entre la quasi-totalité des points terminaux de l'internet, quels que soient la technologie de réseau ou les équipements terminaux utilisés;

5/2° "service de communications interpersonnelles": un service normalement fourni contre rémunération qui permet l'échange interpersonnel et interactif direct d'informations via des réseaux de communications électroniques entre un nombre fini de personnes, par lequel les personnes qui amorcent la communication ou y participent en déterminent le ou les destinataires et qui ne comprend pas les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction

PROJET DE LOI

4° " fourniture d'un réseau de communications électroniques " : la mise en place, l'exploitation, la surveillance ou la mise à disposition d'un réseau de communications électroniques;

5° "service de communications électroniques": le service fourni normalement contre rémunération via des réseaux de communications électroniques qui, à l'exception des services consistant à fournir des contenus transmis à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus et à l'exception des services de médias audiovisuels ou sonores, comprend les types de services suivants:

a) un service d'accès à l'internet;

b) un service de communications interpersonnelles; et

c) des services consistants entièrement ou principalement en la transmission de signaux, tels que les services de transmission utilisés pour la fourniture de services de machine à machine;

5/1° "service d'accès à l'internet": un service de communications électroniques accessibles au public, qui fournit un accès à l'internet et, partant, une connectivité entre la quasi-totalité des points terminaux de l'internet, quels que soient la technologie de réseau ou les équipements terminaux utilisés;

5/2° "service de communications interpersonnelles": un service normalement fourni contre rémunération qui permet l'échange interpersonnel et interactif direct d'informations via des réseaux de communications électroniques entre un nombre fini de personnes, par lequel les personnes qui amorcent la communication ou y participent en déterminent le ou les destinataires et qui ne comprend pas les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction

TEXTE EN VIGUEUR

mineure accessoire intrinsèquement liée à un autre service;

5/3° "service de communications interpersonnelles fondé sur la numérotation": un service de communications interpersonnelles qui établit une connexion à des ressources de numérotation attribuées publiquement, c'est-à-dire un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation ou qui permet la communication avec un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation;

5/4° "service de communications interpersonnelles non fondé sur la numérotation": un service de communications interpersonnelles qui n'établit pas de connexion à des ressources de numérotation attribuées publiquement, c'est-à-dire un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation, ou qui ne permet pas la communication avec un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation;

5/5° "une fraude": un acte malhonnête fait dans l'intention de tromper en contrevenant à la loi, aux règlements ou au contrat et de se procurer ou de procurer à autrui un avantage illicite au préjudice de l'opérateur ou de l'utilisateur final, commis par le biais de l'utilisation d'un service de communications électroniques;

5/6° "utilisation malveillante du réseau ou du service": utilisation du réseau ou du service de communications électroniques afin d'importuner son correspondant ou de provoquer des dommages;

6° "donnée de trafic" : toute donnée traitée en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de la facturation de ce type de communication;

7° "informations relatives à la localisation de l'appelant": dans un réseau mobile public, les

PROJET DE LOI

mineure accessoire intrinsèquement liée à un autre service;

5/3° "service de communications interpersonnelles fondé sur la numérotation": un service de communications interpersonnelles qui établit une connexion à des ressources de numérotation attribuées publiquement, c'est-à-dire un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation ou qui permet la communication avec un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation;

5/4° "service de communications interpersonnelles non fondé sur la numérotation": un service de communications interpersonnelles qui n'établit pas de connexion à des ressources de numérotation attribuées publiquement, c'est-à-dire un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation, ou qui ne permet pas la communication avec un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation;

5/5° "une fraude": un acte malhonnête fait dans l'intention de tromper en contrevenant à la loi, aux règlements ou au contrat et de se procurer ou de procurer à autrui un avantage illicite au préjudice de l'opérateur ou de l'utilisateur final, commis par le biais de l'utilisation d'un service de communications électroniques;

5/6° "utilisation malveillante du réseau ou du service": utilisation du réseau ou du service de communications électroniques afin d'importuner son correspondant ou de provoquer des dommages;

6° "donnée de trafic" : toute donnée traitée en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de la facturation de ce type de communication;

7° "informations relatives à la localisation de l'appelant": dans un réseau mobile public, les

TEXTE EN VIGUEUR

données traitées qui proviennent de l'infrastructure de réseau ou de l'appareil mobile et qui indiquent la position géographique de l'équipement terminal mobile d'un utilisateur final et, dans un réseau fixe public, les données relatives à l'adresse physique du point de terminaison du réseau;

8° " service à données de trafic " : un service qui exige un traitement particulier des données de trafic allant au-delà de ce qui est strictement nécessaire pour la transmission ou la facturation de la communication;

9° " service à données de localisation " : un service qui exige un traitement particulier des données de localisation allant au-delà de ce qui est strictement nécessaire pour la transmission ou la facturation de la communication;

10° " réseau public de communications électroniques " : un réseau de communications électroniques utilisé entièrement ou principalement pour la fourniture de services de communications électroniques accessibles au public permettant la transmission d'informations entre les points de terminaison du réseau;

10/1° " réseau de communications électroniques à haut débit " : un réseau de communications électroniques pouvant fournir des services d'accès au haut débit à une vitesse supérieure ou égale à 30 Mbit/s;

11° "opérateur": une personne ou entreprise qui fournit un réseau public de communications électroniques ou un service de communications électroniques accessible au public;

11/1° "gestionnaire d'infrastructures passives" : un acteur économique qui, d'une part, fournit un service de production, de transport ou de distribution de gaz; d'électricité (y compris pour l'éclairage public) ou d'eau (y compris l'évacuation ou le traitement et l'assainissement des eaux usées, et les systèmes d'égouts); un service de chauffage; ou des services de transport (y compris les voies ferrées, les routes, les ports et les aéroports), et qui, d'autre part,

PROJET DE LOI

données traitées qui proviennent de l'infrastructure de réseau ou de l'appareil mobile et qui indiquent la position géographique de l'équipement terminal mobile d'un utilisateur final et, dans un réseau fixe public, les données relatives à l'adresse physique du point de terminaison du réseau;

8° " service à données de trafic " : un service qui exige un traitement particulier des données de trafic allant au-delà de ce qui est strictement nécessaire pour la transmission ou la facturation de la communication;

9° " service à données de localisation " : un service qui exige un traitement particulier des données de localisation allant au-delà de ce qui est strictement nécessaire pour la transmission ou la facturation de la communication;

10° " réseau public de communications électroniques " : un réseau de communications électroniques utilisé entièrement ou principalement pour la fourniture de services de communications électroniques accessibles au public permettant la transmission d'informations entre les points de terminaison du réseau;

10/1° " réseau de communications électroniques à haut débit " : un réseau de communications électroniques pouvant fournir des services d'accès au haut débit à une vitesse supérieure ou égale à 30 Mbit/s;

11° "opérateur": une personne ou entreprise qui fournit un réseau public de communications électroniques ou un service de communications électroniques accessible au public;

11/1° "gestionnaire d'infrastructures passives" : un acteur économique qui, d'une part, fournit un service de production, de transport ou de distribution de gaz; d'électricité (y compris pour l'éclairage public) ou d'eau (y compris l'évacuation ou le traitement et l'assainissement des eaux usées, et les systèmes d'égouts); un service de chauffage; ou des services de transport (y compris les voies ferrées, les routes, les ports et les aéroports), et qui, d'autre part,

TEXTE EN VIGUEUR

met à disposition des éléments de son réseau sans que ceux-ci deviennent eux-mêmes un élément actif d'un réseau de communications électroniques ;

11/2° "autorisation générale": un cadre juridique mis en place, qui garantit le droit de fournir des réseaux ou des services de communications électroniques et qui fixe les obligations propres au secteur pouvant s'appliquer à tous les types de réseaux et de services de communications électroniques ou à certains d'entre eux;

12° " utilisateur " : une personne physique ou morale qui utilise ou demande un service de communications électroniques accessible au public;

13° " utilisateur final " : un utilisateur qui ne fournit pas de réseau public de communications électroniques ou de services de communications électroniques accessibles au public;

14° " consommateur " : toute personne physique qui utilise ou demande un service de communications électroniques accessible au public à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale;

14/1° "microentreprise": entreprise ne dépassant pas la moyenne annuelle de 9 travailleurs mis au travail, calculée conformément à l'article 1:24 du Code des sociétés et associations;

14/2° "petite entreprise": entreprise ne dépassant pas la moyenne annuelle de 49 travailleurs mis au travail, calculée conformément à l'article 1:24 du Code des sociétés et associations;

14/3° "moyenne entreprise": entreprise ne dépassant pas la moyenne annuelle de 249 travailleurs mis au travail, calculée conformément à l'article 1:24 du Code des sociétés et associations;

PROJET DE LOI

met à disposition des éléments de son réseau sans que ceux-ci deviennent eux-mêmes un élément actif d'un réseau de communications électroniques ;

11/2° "autorisation générale": un cadre juridique mis en place, qui garantit le droit de fournir des réseaux ou des services de communications électroniques et qui fixe les obligations propres au secteur pouvant s'appliquer à tous les types de réseaux et de services de communications électroniques ou à certains d'entre eux;

12° " utilisateur " : une personne physique ou morale qui utilise ou demande un service de communications électroniques accessible au public;

13° " utilisateur final " : un utilisateur qui ne fournit pas de réseau public de communications électroniques ou de services de communications électroniques accessibles au public;

14° " consommateur " : toute personne physique qui utilise ou demande un service de communications électroniques accessible au public à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale;

14/1° "microentreprise": entreprise ne dépassant pas la moyenne annuelle de 9 travailleurs mis au travail, calculée conformément à l'article 1:24 du Code des sociétés et associations;

14/2° "petite entreprise": entreprise ne dépassant pas la moyenne annuelle de 49 travailleurs mis au travail, calculée conformément à l'article 1:24 du Code des sociétés et associations;

14/3° "moyenne entreprise": entreprise ne dépassant pas la moyenne annuelle de 249 travailleurs mis au travail, calculée conformément à l'article 1:24 du Code des sociétés et associations;

TEXTE EN VIGUEUR

14/4° "micro-organisation à but non lucratif": association sans but lucratif, association internationale sans but lucratif ou fondation ne dépassant pas la moyenne annuelle de 9 travailleurs mis au travail, calculée conformément à l'article 1:28 du Code des sociétés et associations;

14/5° "petite organisation à but non lucratif": association sans but lucratif, association internationale sans but lucratif ou fondation ne dépassant pas la moyenne annuelle de 49 travailleurs mis au travail, calculée conformément à l'article 1:28 du Code des sociétés et associations;

15° "abonné" : toute personne physique ou morale, autre qu'un opérateur, partie à un contrat avec un opérateur qui fournit des services de communications électroniques accessibles au public, pour la fourniture de tels services;

15/1° "abonné comptant un maximum de 9 travailleurs": abonné ne dépassant pas la moyenne annuelle de 9 travailleurs mis au travail calculée, selon le cas, conformément aux articles 1:24 ou 1:28 du Code des sociétés et associations;

16° "point de terminaison du réseau": point physique auquel un utilisateur final obtient l'accès à un réseau public de communications électroniques; dans le cas de réseaux utilisant la commutation et l'acheminement, le point de terminaison du réseau est identifié par une adresse réseau spécifique qui peut être rattachée au numéro ou au nom d'un utilisateur final;

16/1° "point d'accès" : un point physique, situé à l'intérieur ou à l'extérieur de l'immeuble, accessible aux opérateurs, qui permet le raccordement à l'infrastructure physique adaptée au haut débit à l'intérieur de l'immeuble ;

17° "ressources associées": les services associés, les infrastructures physiques et autres

PROJET DE LOI

14/4° "micro-organisation à but non lucratif": association sans but lucratif, association internationale sans but lucratif ou fondation ne dépassant pas la moyenne annuelle de 9 travailleurs mis au travail, calculée conformément à l'article 1:28 du Code des sociétés et associations;

14/5° "petite organisation à but non lucratif": association sans but lucratif, association internationale sans but lucratif ou fondation ne dépassant pas la moyenne annuelle de 49 travailleurs mis au travail, calculée conformément à l'article 1:28 du Code des sociétés et associations;

15° "abonné" : toute personne physique ou morale, autre qu'un opérateur, partie à un contrat avec un opérateur qui fournit des services de communications électroniques accessibles au public, pour la fourniture de tels services;

15/1° "abonné comptant un maximum de 9 travailleurs": abonné ne dépassant pas la moyenne annuelle de 9 travailleurs mis au travail calculée, selon le cas, conformément aux articles 1:24 ou 1:28 du Code des sociétés et associations;

16° "point de terminaison du réseau": point physique auquel un utilisateur final obtient l'accès à un réseau public de communications électroniques; dans le cas de réseaux utilisant la commutation et l'acheminement, le point de terminaison du réseau est identifié par une adresse réseau spécifique qui peut être rattachée au numéro ou au nom d'un utilisateur final;

16/1° "point d'accès" : un point physique, situé à l'intérieur ou à l'extérieur de l'immeuble, accessible aux opérateurs, qui permet le raccordement à l'infrastructure physique adaptée au haut débit à l'intérieur de l'immeuble ;

17° "ressources associées": les services associés, les infrastructures physiques et autres

TEXTE EN VIGUEUR

ressources ou éléments associés à un réseau de communications électroniques ou à un service de communications électroniques, qui permettent ou soutiennent la fourniture de services via ce réseau ou ce service ou en ont le potentiel, et comprennent, entre autres, les bâtiments ou accès aux bâtiments, le câblage des bâtiments, les antennes, tours et autres constructions de soutènement, les gaines, conduites, pylônes, regards de visite et armoires;

17/1° "service associé": un service associé à un réseau de communications électroniques ou à un service de communications électroniques, qui permet ou soutient la fourniture, l'autofourniture ou la fourniture automatisée de services via ce réseau ou ce service ou en a le potentiel, et comprend notamment la conversion du numéro d'appel ou des systèmes offrant des fonctionnalités équivalentes et les systèmes d'accès conditionnel et les guides électroniques de programmes, en abrégé "EPG", ainsi que d'autres services tels que ceux relatifs à l'identité, l'emplacement et l'occupation (à l'exception des services et systèmes qui sont exclusivement utilisés pour les services de médias audiovisuels ou sonores);

17/2° " infrastructure physique située à l'intérieur d'un immeuble " : tout élément d'un réseau, tels que les conduites, pylônes, gaines, chambres de tirage et regards, trous de visite, boîtiers, immeubles ou accès à des immeubles, installations liées aux antennes, tours et poteaux (hormis les câbles, y compris la fibre noire) ainsi que les installations situés au niveau des locaux de l'utilisateur final, y compris dans les éléments en copropriété, qui sont destinés à accueillir des éléments de réseaux d'accès filaires ou sans fil sans devenir eux-mêmes un élément actif du réseau, lorsque ces réseaux permettent de fournir des services de communications électroniques et de raccorder le point d'accès de l'immeuble au point de terminaison du réseau;

17/3° "nomadicité": caractéristique d'un service de communications électroniques qui permet à ce service d'être utilisé à partir de pratiquement

PROJET DE LOI

ressources ou éléments associés à un réseau de communications électroniques ou à un service de communications électroniques, qui permettent ou soutiennent la fourniture de services via ce réseau ou ce service ou en ont le potentiel, et comprennent, entre autres, les bâtiments ou accès aux bâtiments, le câblage des bâtiments, les antennes, tours et autres constructions de soutènement, les gaines, conduites, pylônes, regards de visite et armoires;

17/1° "service associé": un service associé à un réseau de communications électroniques ou à un service de communications électroniques, qui permet ou soutient la fourniture, l'autofourniture ou la fourniture automatisée de services via ce réseau ou ce service ou en a le potentiel, et comprend notamment la conversion du numéro d'appel ou des systèmes offrant des fonctionnalités équivalentes et les systèmes d'accès conditionnel et les guides électroniques de programmes, en abrégé "EPG", ainsi que d'autres services tels que ceux relatifs à l'identité, l'emplacement et l'occupation (à l'exception des services et systèmes qui sont exclusivement utilisés pour les services de médias audiovisuels ou sonores);

17/2° " infrastructure physique située à l'intérieur d'un immeuble " : tout élément d'un réseau, tels que les conduites, pylônes, gaines, chambres de tirage et regards, trous de visite, boîtiers, immeubles ou accès à des immeubles, installations liées aux antennes, tours et poteaux (hormis les câbles, y compris la fibre noire) ainsi que les installations situés au niveau des locaux de l'utilisateur final, y compris dans les éléments en copropriété, qui sont destinés à accueillir des éléments de réseaux d'accès filaires ou sans fil sans devenir eux-mêmes un élément actif du réseau, lorsque ces réseaux permettent de fournir des services de communications électroniques et de raccorder le point d'accès de l'immeuble au point de terminaison du réseau;

17/3° "nomadicité": caractéristique d'un service de communications électroniques qui permet à ce service d'être utilisé à partir de pratiquement

TEXTE EN VIGUEUR

n'importe quelle connexion à un réseau de communications électroniques;

18° accès " : la mise à la disposition d'un opérateur, dans des conditions bien définies et de manière exclusive ou non exclusive, de ressources et/ou de services en vue de la fourniture de services de communications électroniques, ou l'offre de services de la société de l'information. Cela couvre notamment : l'accès à des éléments de réseaux et à des ressources associées ce qui peut comprendre à la connexion des équipements par des moyens fixes ou non (cela comprend en particulier l'accès à la boucle locale ainsi qu'aux ressources et services nécessaires à la fourniture de services par la boucle locale); l'accès à l'infrastructure physique, y compris aux bâtiments, gaines et pylônes; l'accès aux systèmes logiciels pertinents, y compris aux systèmes d'assistance à l'exploitation; l'accès aux systèmes d'information ou aux bases de données pour la préparation de commandes, l'approvisionnement, la commande, les demandes de maintenance et de réparation et la facturation; l'accès à la conversion du numéro d'appel ou à des systèmes offrant des fonctionnalités équivalentes; l'accès aux réseaux fixes et mobiles, notamment pour l'itinérance; l'accès aux services de réseaux virtuels;

19° "interconnexion": un type particulier d'accès mis en oeuvre entre opérateurs de réseaux publics au moyen de la liaison physique et logique des réseaux publics de communications électroniques utilisés par la même entreprise ou une entreprise différente, afin de permettre aux utilisateurs d'une entreprise de communiquer avec les utilisateurs de la même entreprise ou d'une autre entreprise, ou d'accéder aux services fournis par une autre entreprise lorsque ces services sont fournis par les parties concernées ou par d'autres parties qui ont accès au réseau;

20° " interface " : un point de terminaison du réseau et/ou une interface radio, et les spécifications techniques y afférentes;

21° [...];

PROJET DE LOI

n'importe quelle connexion à un réseau de communications électroniques;

18° accès " : la mise à la disposition d'un opérateur, dans des conditions bien définies et de manière exclusive ou non exclusive, de ressources et/ou de services en vue de la fourniture de services de communications électroniques, ou l'offre de services de la société de l'information. Cela couvre notamment : l'accès à des éléments de réseaux et à des ressources associées ce qui peut comprendre à la connexion des équipements par des moyens fixes ou non (cela comprend en particulier l'accès à la boucle locale ainsi qu'aux ressources et services nécessaires à la fourniture de services par la boucle locale); l'accès à l'infrastructure physique, y compris aux bâtiments, gaines et pylônes; l'accès aux systèmes logiciels pertinents, y compris aux systèmes d'assistance à l'exploitation; l'accès aux systèmes d'information ou aux bases de données pour la préparation de commandes, l'approvisionnement, la commande, les demandes de maintenance et de réparation et la facturation; l'accès à la conversion du numéro d'appel ou à des systèmes offrant des fonctionnalités équivalentes; l'accès aux réseaux fixes et mobiles, notamment pour l'itinérance; l'accès aux services de réseaux virtuels;

19° "interconnexion": un type particulier d'accès mis en oeuvre entre opérateurs de réseaux publics au moyen de la liaison physique et logique des réseaux publics de communications électroniques utilisés par la même entreprise ou une entreprise différente, afin de permettre aux utilisateurs d'une entreprise de communiquer avec les utilisateurs de la même entreprise ou d'une autre entreprise, ou d'accéder aux services fournis par une autre entreprise lorsque ces services sont fournis par les parties concernées ou par d'autres parties qui ont accès au réseau;

20° " interface " : un point de terminaison du réseau et/ou une interface radio, et les spécifications techniques y afférentes;

21° [...];

TEXTE EN VIGUEUR

22° "service de communications vocales": un service de communications électroniques accessible au public permettant d'émettre et de recevoir, directement ou indirectement, des appels nationaux ou nationaux et internationaux, en composant un ou plusieurs numéros d'un plan national ou international de numérotation;

22/1° "appel " : une connexion établie au moyen d'un service de communications interpersonnelles accessible au public permettant une communication vocale bidirectionnelle;

22/2° "service de conversation totale": un service multimédia de conversation en temps réel assurant la transmission symétrique et bidirectionnelle en temps réel de vidéos animées, de texte en temps réel et de voix entre des utilisateurs situés dans deux lieux différents ou plus;

23° " boucle locale " : un canal physique utilisé par les signaux de communications électroniques et relie le point de terminaison du réseau à un répartiteur ou à toute autre installation équivalente du réseau public fixe de communications électroniques];

24° " sous-boucle locale " : partie d'une boucle locale qui relie le point de terminaison du réseau à un point de concentration ou à un point d'accès intermédiaire spécifié du réseau de communications électroniques public fixe;

25° " accès totalement dégroupé à la boucle locale " : la fourniture d'un accès à la boucle locale ou à la sous-boucle locale d'une entreprise désignée comme étant puissante sur un marché pertinent, autorisant l'usage de la pleine capacité des infrastructures des réseaux;

26° " accès à un débit binaire " : accès consistant en la fourniture d'une capacité de transport avec la commutation associée vers un utilisateur pour lequel l'interface chez l'utilisateur est définie par le fournisseur d'accès;

PROJET DE LOI

22° "service de communications vocales": un service de communications électroniques accessible au public permettant d'émettre et de recevoir, directement ou indirectement, des appels nationaux ou nationaux et internationaux, en composant un ou plusieurs numéros d'un plan national ou international de numérotation;

22/1° " appel " : une connexion établie au moyen d'un service de communications interpersonnelles accessible au public permettant une communication vocale bidirectionnelle;

22/2° "service de conversation totale": un service multimédia de conversation en temps réel assurant la transmission symétrique et bidirectionnelle en temps réel de vidéos animées, de texte en temps réel et de voix entre des utilisateurs situés dans deux lieux différents ou plus;

23° " boucle locale " : un canal physique utilisé par les signaux de communications électroniques et relie le point de terminaison du réseau à un répartiteur ou à toute autre installation équivalente du réseau public fixe de communications électroniques];

24° " sous-boucle locale " : partie d'une boucle locale qui relie le point de terminaison du réseau à un point de concentration ou à un point d'accès intermédiaire spécifié du réseau de communications électroniques public fixe;

25° " accès totalement dégroupé à la boucle locale " : la fourniture d'un accès à la boucle locale ou à la sous-boucle locale d'une entreprise désignée comme étant puissante sur un marché pertinent, autorisant l'usage de la pleine capacité des infrastructures des réseaux;

26° " accès à un débit binaire " : accès consistant en la fourniture d'une capacité de transport avec la commutation associée vers un utilisateur pour lequel l'interface chez l'utilisateur est définie par le fournisseur d'accès;

TEXTE EN VIGUEUR**PROJET DE LOI**

27° " accès partagé à la boucle locale " : la fourniture d'un accès à la boucle locale ou à la sous-boucle locale d'une entreprise désignée comme étant puissante sur un marché pertinent, autorisant l'usage d'une partie spécifiée de la capacité des infrastructures des réseaux telle qu'une partie de la fréquence ou l'équivalent;

28° " accès dégroupé à la boucle locale " : la fourniture d'un accès totalement dégroupé ou d'un accès partagé à la boucle locale n'impliquant pas de changement en ce qui concerne la propriété de la boucle locale;

29° " colocalisation " : la fourniture d'un espace et des ressources techniques nécessaires à l'hébergement et à la connexion, dans des conditions raisonnables, des équipements pertinents d'un opérateur dans le cadre d'une offre de référence;

29/1° " gaine " : enveloppe servant à faire passer et protéger des câbles optiques, téléphoniques et/ou coaxiaux, et/ou ressources de réseau;

30° " ligne louée " : service de communications électroniques consistant en la fourniture d'un système de communications offrant une capacité de transmission transparente entre les points de terminaison de réseaux, à l'exclusion de la commutation sur demande;

31° " ondes radioélectriques " : les ondes électromagnétiques se propageant dans l'espace sans guide artificiel, et dont la fréquence est inférieure à 3000 GHz;

32° [...]

33° " spectre radioélectrique " : l'ensemble des ondes radioélectriques;

33/1° "attribution du spectre radioélectrique": la désignation d'une bande du spectre radioélectrique donnée, aux fins de son utilisation par un ou plusieurs types de services de radiocommunications, le cas échéant, selon des conditions définies;

27° " accès partagé à la boucle locale " : la fourniture d'un accès à la boucle locale ou à la sous-boucle locale d'une entreprise désignée comme étant puissante sur un marché pertinent, autorisant l'usage d'une partie spécifiée de la capacité des infrastructures des réseaux telle qu'une partie de la fréquence ou l'équivalent;

28° " accès dégroupé à la boucle locale " : la fourniture d'un accès totalement dégroupé ou d'un accès partagé à la boucle locale n'impliquant pas de changement en ce qui concerne la propriété de la boucle locale;

29° " colocalisation " : la fourniture d'un espace et des ressources techniques nécessaires à l'hébergement et à la connexion, dans des conditions raisonnables, des équipements pertinents d'un opérateur dans le cadre d'une offre de référence;

29/1° " gaine " : enveloppe servant à faire passer et protéger des câbles optiques, téléphoniques et/ou coaxiaux, et/ou ressources de réseau;

30° " ligne louée " : service de communications électroniques consistant en la fourniture d'un système de communications offrant une capacité de transmission transparente entre les points de terminaison de réseaux, à l'exclusion de la commutation sur demande;

31° " ondes radioélectriques " : les ondes électromagnétiques se propageant dans l'espace sans guide artificiel, et dont la fréquence est inférieure à 3000 GHz;

32° [...]

33° " spectre radioélectrique " : l'ensemble des ondes radioélectriques;

33/1° "attribution du spectre radioélectrique": la désignation d'une bande du spectre radioélectrique donnée, aux fins de son utilisation par un ou plusieurs types de services de radiocommunications, le cas échéant, selon des conditions définies;

TEXTE EN VIGUEUR

33/2° "plan national d'attribution des fréquences": document contenant pour chaque bande du spectre radioélectrique, les informations relatives aux attributions du spectre radioélectrique et aux applications autorisées;

33/3° "spectre radioélectrique harmonisé": spectre radioélectrique dont les conditions harmonisées quant à sa disponibilité et son utilisation efficace ont été établies par la voie de mesures techniques d'application conformément à l'article 4 de la décision no 676/2002/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire pour la politique en matière de spectre radioélectrique dans la Communauté européenne, ci-après dénommée "décision spectre radioélectrique";

33/4° "utilisation partagée du spectre radioélectrique": l'accès par deux utilisateurs ou plus, en vue de leur utilisation, aux mêmes bandes du spectre radioélectrique dans le cadre d'un dispositif de partage défini, autorisé sur le fondement d'une autorisation générale, de droits d'utilisation du spectre radioélectrique ou d'une combinaison de ceux-ci, y compris des mécanismes de régulation tels que l'accès partagé sous licence destiné à faciliter l'utilisation partagée d'une bande du spectre radioélectrique, sous réserve d'un accord contraignant entre toutes les parties concernées, conformément aux règles de partage incluses dans leurs droits d'utilisation du spectre radioélectrique, afin de garantir à tous les utilisateurs des dispositifs de partage prévisibles et fiables, et sans préjudice de l'application du droit de la concurrence;

33/5° "droits d'utilisation du spectre radioélectrique": droits individuels d'utilisation du spectre radioélectrique utilisés entièrement ou partiellement pour la fourniture de réseaux publics de communications électroniques ou de services de communications électroniques accessibles au public;

PROJET DE LOI

33/2° "plan national d'attribution des fréquences": document contenant pour chaque bande du spectre radioélectrique, les informations relatives aux attributions du spectre radioélectrique et aux applications autorisées;

33/3° "spectre radioélectrique harmonisé": spectre radioélectrique dont les conditions harmonisées quant à sa disponibilité et son utilisation efficace ont été établies par la voie de mesures techniques d'application conformément à l'article 4 de la décision no 676/2002/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire pour la politique en matière de spectre radioélectrique dans la Communauté européenne, ci-après dénommée "décision spectre radioélectrique";

33/4° "utilisation partagée du spectre radioélectrique": l'accès par deux utilisateurs ou plus, en vue de leur utilisation, aux mêmes bandes du spectre radioélectrique dans le cadre d'un dispositif de partage défini, autorisé sur le fondement d'une autorisation générale, de droits d'utilisation du spectre radioélectrique ou d'une combinaison de ceux-ci, y compris des mécanismes de régulation tels que l'accès partagé sous licence destiné à faciliter l'utilisation partagée d'une bande du spectre radioélectrique, sous réserve d'un accord contraignant entre toutes les parties concernées, conformément aux règles de partage incluses dans leurs droits d'utilisation du spectre radioélectrique, afin de garantir à tous les utilisateurs des dispositifs de partage prévisibles et fiables, et sans préjudice de l'application du droit de la concurrence;

33/5° "droits d'utilisation du spectre radioélectrique": droits individuels d'utilisation du spectre radioélectrique utilisés entièrement ou partiellement pour la fourniture de réseaux publics de communications électroniques ou de services de communications électroniques accessibles au public;

TEXTE EN VIGUEUR

34° "radiocommunication": toute communication au moyen d'ondes radioélectriques à l'exclusion de la transmission exclusive de signaux de services de médias audiovisuels et sonores;

35° [...]

36° [...]

37° [...]

38° "station de radiocommunications": un équipement hertzien, le cas échéant complété des antennes, ainsi que de tous les composants nécessaires au fonctionnement de l'ensemble, qui émet ou reçoit intentionnellement des ondes radioélectriques à des fins de radiocommunication et/ou de radiorepérage;

38/1° "réseau de radiocommunications": ensemble formé par plusieurs stations de radiocommunications pouvant communiquer entre elles dans les limites d'une autorisation de radiocommunications privées ou d'un droit d'utilisation du spectre radioélectrique;

38/2° "autorisation de radiocommunications privées": autorisation de pouvoir utiliser une station ou un réseau de radiocommunications à d'autres fins que la fourniture de réseaux publics de communications électroniques ou de services de communications électroniques accessibles au public;

38/3° "station de radiodiffusion": un équipement hertzien, le cas échéant complété des antennes associées, ainsi que de tous les composants nécessaires au fonctionnement de l'ensemble, qui émet ou reçoit intentionnellement des ondes radioélectriques à des fins de fourniture de services de médias audiovisuels et sonores;

38/4° "brouillage": effet, sur la réception dans un système de radiocommunication, d'une énergie non désirée due à une émission, à un rayonnement ou à une induction (ou à une combinaison de ces émissions, rayonnements ou

PROJET DE LOI

34° "radiocommunication": toute communication au moyen d'ondes radioélectriques à l'exclusion de la transmission exclusive de signaux de services de médias audiovisuels et sonores;

35° [...]

36° [...]

37° [...]

38° "station de radiocommunications": un équipement hertzien, le cas échéant complété des antennes, ainsi que de tous les composants nécessaires au fonctionnement de l'ensemble, qui émet ou reçoit intentionnellement des ondes radioélectriques à des fins de radiocommunication et/ou de radiorepérage;

38/1° "réseau de radiocommunications": ensemble formé par plusieurs stations de radiocommunications pouvant communiquer entre elles dans les limites d'une autorisation de radiocommunications privées ou d'un droit d'utilisation du spectre radioélectrique;

38/2° "autorisation de radiocommunications privées": autorisation de pouvoir utiliser une station ou un réseau de radiocommunications à d'autres fins que la fourniture de réseaux publics de communications électroniques ou de services de communications électroniques accessibles au public;

38/3° "station de radiodiffusion": un équipement hertzien, le cas échéant complété des antennes associées, ainsi que de tous les composants nécessaires au fonctionnement de l'ensemble, qui émet ou reçoit intentionnellement des ondes radioélectriques à des fins de fourniture de services de médias audiovisuels et sonores;

38/4° "brouillage": effet, sur la réception dans un système de radiocommunication, d'une énergie non désirée due à une émission, à un rayonnement ou à une induction (ou à une combinaison de ces émissions, rayonnements ou

TEXTE EN VIGUEUR

inductions), se manifestant par une dégradation de la qualité de transmission, une déformation ou une perte de l'information que l'on aurait pu extraire en l'absence de cette énergie non désirée;

39° " brouillage préjudiciable " : le brouillage qui compromet le fonctionnement d'un service de radionavigation ou d'autres services de sécurité ou qui altère gravement, entrave ou interrompt de façon répétée le fonctionnement d'un service de radiocommunications, d'un service de fourniture de services de médias audiovisuels et sonores, ou d'un service de communications électroniques opérant conformément à la réglementation applicable;

40° " cryptographie " : l'ensemble des services mettant en oeuvre les principes, moyens et méthodes de transformation de données dans le but de cacher leur contenu sémantique, d'établir leur authenticité, d'empêcher que leur modification passe inaperçue, de prévenir leur répudiation et d'empêcher leur utilisation non autorisée;

41° "équipement terminal":

a) tout équipement qui est connecté directement ou indirectement à l'interface d'un réseau public de communications électroniques pour transmettre, traiter ou recevoir des informations; dans les deux cas, direct ou indirect, la connexion peut être établie par fil, fibre optique ou voie électromagnétique; une connexion est indirecte si un appareil est interposé entre l'équipement terminal et l'interface du réseau public ;

b) les équipements de stations terrestres de satellites;

42° "équipement hertzien" : un produit électrique ou électronique qui émet et/ou reçoit intentionnellement des ondes radioélectriques à des fins de radiocommunication , de fourniture de services de médias audiovisuels et sonores et/ou radiorepérage, ou un produit électrique ou électronique qui doit être complété d'un

PROJET DE LOI

inductions), se manifestant par une dégradation de la qualité de transmission, une déformation ou une perte de l'information que l'on aurait pu extraire en l'absence de cette énergie non désirée;

39° " brouillage préjudiciable " : le brouillage qui compromet le fonctionnement d'un service de radionavigation ou d'autres services de sécurité ou qui altère gravement, entrave ou interrompt de façon répétée le fonctionnement d'un service de radiocommunications, d'un service de fourniture de services de médias audiovisuels et sonores, ou d'un service de communications électroniques opérant conformément à la réglementation applicable;

40° " cryptographie " : l'ensemble des services mettant en oeuvre les principes, moyens et méthodes de transformation de données dans le but de cacher leur contenu sémantique, d'établir leur authenticité, d'empêcher que leur modification passe inaperçue, de prévenir leur répudiation et d'empêcher leur utilisation non autorisée;

41° "équipement terminal":

a) tout équipement qui est connecté directement ou indirectement à l'interface d'un réseau public de communications électroniques pour transmettre, traiter ou recevoir des informations; dans les deux cas, direct ou indirect, la connexion peut être établie par fil, fibre optique ou voie électromagnétique; une connexion est indirecte si un appareil est interposé entre l'équipement terminal et l'interface du réseau public ;

b) les équipements de stations terrestres de satellites;

42° "équipement hertzien" : un produit électrique ou électronique qui émet et/ou reçoit intentionnellement des ondes radioélectriques à des fins de radiocommunication , de fourniture de services de médias audiovisuels et sonores et/ou radiorepérage, ou un produit électrique ou électronique qui doit être complété d'un

TEXTE EN VIGUEUR

accessoire, tel qu'une antenne, pour émettre et/ou recevoir intentionnellement des ondes radioélectriques à des fins de radiocommunication, de fourniture de services de médias audiovisuels et sonores et/ou de radiorepérage;

43° " équipement " : tout produit qui est soit un équipement hertzien, soit un équipement terminal, soit les deux;

44° " spécification technique " : la définition des caractéristiques de tous les services de communications électroniques fournis via le point de terminaison du réseau ou l'interface radio;

45° " espace de numérotation " : l'ensemble des numéros, adresses et noms utilisés en vue d'identifier des opérateurs ou des utilisateurs;

46° " numéro géographique " : numéro du plan national de numérotation dont une partie de la structure numérique contient une signification géographique utilisée pour acheminer les appels vers le lieu physique du point de terminaison du réseau;

47° " numéro non géographique " : numéro du [10 plan national de numérotation]¹⁰ qui n'est pas un numéro géographique; il s'agit entre autres des numéros d'appel mobiles, des numéros d'appel gratuits pour les appelants et des numéros à taux majoré;

48° " portabilité des numéros " : facilité permettant aux abonnés de conserver leur numéro, quel que soit l'opérateur fournissant le service, dans une zone géographique déterminée dans le cas d'un numéro géographique et quel que soit l'endroit, dans le cas de numéros autres que géographiques; la facilité ne permet pas de conserver le numéro de téléphone national entre un opérateur de services téléphoniques accessibles au public en position déterminée et un opérateur de services téléphoniques accessibles au public sur un réseau de communications électroniques mobile;

PROJET DE LOI

accessoire, tel qu'une antenne, pour émettre et/ou recevoir intentionnellement des ondes radioélectriques à des fins de radiocommunication, de fourniture de services de médias audiovisuels et sonores et/ou de radiorepérage;

43° " équipement " : tout produit qui est soit un équipement hertzien, soit un équipement terminal, soit les deux;

44° " spécification technique " : la définition des caractéristiques de tous les services de communications électroniques fournis via le point de terminaison du réseau ou l'interface radio;

45° " espace de numérotation " : l'ensemble des numéros, adresses et noms utilisés en vue d'identifier des opérateurs ou des utilisateurs;

46° " numéro géographique " : numéro du plan national de numérotation dont une partie de la structure numérique contient une signification géographique utilisée pour acheminer les appels vers le lieu physique du point de terminaison du réseau;

47° " numéro non géographique " : numéro du [10 plan national de numérotation]¹⁰ qui n'est pas un numéro géographique; il s'agit entre autres des numéros d'appel mobiles, des numéros d'appel gratuits pour les appelants et des numéros à taux majoré;

48° " portabilité des numéros " : facilité permettant aux abonnés de conserver leur numéro, quel que soit l'opérateur fournissant le service, dans une zone géographique déterminée dans le cas d'un numéro géographique et quel que soit l'endroit, dans le cas de numéros autres que géographiques; la facilité ne permet pas de conserver le numéro de téléphone national entre un opérateur de services téléphoniques accessibles au public en position déterminée et un opérateur de services téléphoniques accessibles au public sur un réseau de communications électroniques mobile;

TEXTE EN VIGUEUR

48/1° " Bureau d'enregistrement de noms de domaine Internet " : une entité qui tient à jour un registre de noms de domaine et qui exploite un système de sorte que ces noms de domaine puissent être utilisés pour obtenir un accès à des adresses de protocole Internet ou d'autres informations via l'Internet;

48/2° " service universel " : un ensemble de services minimal défini à l'article 68 de qualité déterminée, disponible pour tous les utilisateurs quelle que soit leur situation géographique et compte tenu des conditions nationales spécifiques, d'un prix abordable;

49° " annuaire " : livre, liste ou fichier contenant principalement ou exclusivement des données concernant les abonnés d'un service téléphonique public et mis à la disposition du public en vue de permettre exclusivement ou principalement l'identification du numéro d'appel des utilisateurs finaux;

50° [...]

51° " antenne " : un composant d'un appareil ou d'une station radio destiné au rayonnement et/ou à la captation d'ondes radioélectriques;

PROJET DE LOI

48/1° « registre de noms de domaine de premier niveau » : une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration du domaine de premier niveau, y compris de l'enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage;

48/2° " service universel " : un ensemble de services minimal défini à l'article 68 de qualité déterminée, disponible pour tous les utilisateurs quelle que soit leur situation géographique et compte tenu des conditions nationales spécifiques, d'un prix abordable;

48/3° « entité fournissant des services d'enregistrement de noms de domaine » : un bureau d'enregistrement ou un agent agissant pour le compte de bureaux d'enregistrement, tel qu'un fournisseur ou revendeur de services d'anonymisation ou d'enregistrement fiduciaire;

49° " annuaire " : livre, liste ou fichier contenant principalement ou exclusivement des données concernant les abonnés d'un service téléphonique public et mis à la disposition du public en vue de permettre exclusivement ou principalement l'identification du numéro d'appel des utilisateurs finaux;

50° [...]

51° " antenne " : un composant d'un appareil ou d'une station radio destiné au rayonnement et/ou à la captation d'ondes radioélectriques;

TEXTE EN VIGUEUR

52° " station de base " : une station de radiocommunication d'un réseau de communications électroniques installée et utilisée en un lieu déterminé, et destinée à assurer la couverture radioélectrique d'une zone géographique donnée;

53° " support " : une structure sur laquelle peuvent être placées les antennes de stations de base;

54° " site d'antennes " : l'ensemble des constructions, comportant au moins un support, une antenne et des locaux pour les équipements électriques et électroniques, permettant l'installation et l'exploitation d'une ou plusieurs stations de base;

55° " itinérance nationale " : la faculté pour un opérateur de permettre à ses clients d'accéder dans le même pays aux services de base offerts par un autre opérateur de réseau mobile de communications;

56° " identification de la ligne " : numéro, signe ou ensemble de signes attribués à un abonné, à un utilisateur final, à un utilisateur ou à un terminal qui permet à celui-ci d'être joint par d'autres abonnés, [9 utilisateurs finaux]9 ou utilisateurs de réseaux publics de communications électroniques ou de services de communications électroniques accessibles au public;

57° " identification de l'appelant " : toute donnée, disponible directement ou indirectement, dans les réseaux et services d'un opérateur, qui détermine le numéro d'appel du terminal, le nom de l'utilisateur final et l'endroit où l'équipement terminal se situe au moment de l'appel;

58° " service d'urgence " : tout service public ou d'intérêt public visé à l'article 107, § 1er, alinéa 1er, ou fixé par le Roi conformément à l'article 107, § 1er, alinéa 2, 1° ;

59° " numéro d'urgence " : numéro d'appel d'un service d'urgence fixé conformément à la

PROJET DE LOI

52° " station de base " : une station de radiocommunication d'un réseau de communications électroniques installée et utilisée en un lieu déterminé, et destinée à assurer la couverture radioélectrique d'une zone géographique donnée;

53° " support " : une structure sur laquelle peuvent être placées les antennes de stations de base;

54° " site d'antennes " : l'ensemble des constructions, comportant au moins un support, une antenne et des locaux pour les équipements électriques et électroniques, permettant l'installation et l'exploitation d'une ou plusieurs stations de base;

55° " itinérance nationale " : la faculté pour un opérateur de permettre à ses clients d'accéder dans le même pays aux services de base offerts par un autre opérateur de réseau mobile de communications;

56° " identification de la ligne " : numéro, signe ou ensemble de signes attribués à un abonné, à un utilisateur final, à un utilisateur ou à un terminal qui permet à celui-ci d'être joint par d'autres abonnés, [9 utilisateurs finaux]9 ou utilisateurs de réseaux publics de communications électroniques ou de services de communications électroniques accessibles au public;

57° " identification de l'appelant " : toute donnée, disponible directement ou indirectement, dans les réseaux et services d'un opérateur, qui détermine le numéro d'appel du terminal, le nom de l'utilisateur final et l'endroit où l'équipement terminal se situe au moment de l'appel;

58° " service d'urgence " : tout service public ou d'intérêt public visé à l'article 107, § 1er, alinéa 1er, ou fixé par le Roi conformément à l'article 107, § 1er, alinéa 2, 1° ;

59° " numéro d'urgence " : numéro d'appel d'un service d'urgence fixé conformément à la

TEXTE EN VIGUEUR

procédure prévue à l'article [1 107, § 1er, alinéa 2, 2° de la présente loi;

60° "communication d'urgence": une communication effectuée au moyen de services de communications interpersonnelles, entre un utilisateur final et un PSAP, dont le but est de recevoir de l'aide d'urgence de la part de services d'urgence;

61° "PSAP" ("Public Safety Answering Point") ou "centre de gestion des appels d'urgence": un lieu physique où est réceptionnée initialement une communication d'urgence sous la responsabilité d'une autorité publique ou d'un organisme privé reconnu;

62° "zone d'activité d'un PSAP": zone géographique pour laquelle un PSAP gère toutes les communications d'urgence vers le service d'urgence, dénommée ci-après "zone d'activité";

62/1° "PSAP le plus approprié": un PSAP établi par les autorités compétentes pour prendre en charge les communications d'urgence provenant d'une certaine zone ou les communications d'urgence d'un certain type ;

62/2° "sécurité des réseaux et services": la capacité des réseaux et services de communications électroniques de résister, à un niveau de confiance donné, à toute action qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité de ces réseaux et services, de données stockées, transmises ou traitées ou des services connexes offerts par ces réseaux ou services de communications électroniques ou rendus accessibles via de tels réseaux ou services;

PROJET DE LOI

procédure prévue à l'article [1 107, § 1er, alinéa 2, 2° de la présente loi;

60° "communication d'urgence": une communication effectuée au moyen de services de communications interpersonnelles, entre un utilisateur final et un PSAP, dont le but est de recevoir de l'aide d'urgence de la part de services d'urgence;

61° "PSAP" ("Public Safety Answering Point") ou "centre de gestion des appels d'urgence": un lieu physique où est réceptionnée initialement une communication d'urgence sous la responsabilité d'une autorité publique ou d'un organisme privé reconnu;

62° "zone d'activité d'un PSAP": zone géographique pour laquelle un PSAP gère toutes les communications d'urgence vers le service d'urgence, dénommée ci-après "zone d'activité";

62/1° "PSAP le plus approprié": un PSAP établi par les autorités compétentes pour prendre en charge les communications d'urgence provenant d'une certaine zone ou les communications d'urgence d'un certain type ;

62/2° « réseau et système d'information » :

a) un réseau de communications électroniques au sens du 3°;

b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques,

TEXTE EN VIGUEUR

62/3° "incident de sécurité": tout événement ayant un effet négatif réel sur la sécurité des réseaux ou des services de communications électroniques;

PROJET DE LOI

électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation du processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel; ou

c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance;

62/3° « sécurité des réseaux et des systèmes d'information » : la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à tout événement susceptible de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, ou des services que ces réseaux et systèmes d'information offrent ou rendent accessibles;

62/4° « incident de sécurité » : un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles;

62/5° « cybersécurité » : la cybersécurité au sens de l'article 2, point 1), du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité);

62/6° « traitement des incidents » : toutes les actions et procédures visant à prévenir, détecter, analyser et contenir un incident ou à y répondre et à y remédier;

TEXTE EN VIGUEUR

PROJET DE LOI

62/7° « cybermenace » : une cybermenace au sens de l'article 2, point 8), du règlement (UE) 2019/881;

62/8° « cybermenace importante » : une cybermenace qui, compte tenu de ses caractéristiques techniques, peut être considérée comme susceptible d'avoir un impact grave sur les réseaux et les systèmes d'information d'une entité ou les utilisateurs des services de l'entité, en causant un dommage matériel, corporel ou moral considérable;

63° " réviseur agréé " : un réviseur d'entreprises inscrit au tableau de l'Institution des Réviseurs d'Entreprises;

63° " réviseur agréé " : un réviseur d'entreprises inscrit au tableau de l'Institution des Réviseurs d'Entreprises;

64° " hôpitaux " : les établissements de soins de santé visés à l'article 2 de la loi sur les hôpitaux, coordonnée le 7 août 1987;

64° " hôpitaux " : les établissements de soins de santé visés à l'article 2 de la loi sur les hôpitaux, coordonnée le 7 août 1987;

65° " écoles " : tout établissement d'enseignement primaire, secondaire ou supérieur appartenant au réseau d'une Communauté, d'une province, d'une commune ou à un réseau libre subventionné;

65° " écoles " : tout établissement d'enseignement primaire, secondaire ou supérieur appartenant au réseau d'une Communauté, d'une province, d'une commune ou à un réseau libre subventionné;

66° " bibliothèques publiques " : toute bibliothèque publique reconnue par l'Etat fédéral ou par une Communauté;

66° " bibliothèques publiques " : toute bibliothèque publique reconnue par l'Etat fédéral ou par une Communauté;

67° " bureau public de communications électroniques " : local ou dispositif accessible au public en vue de la mise à disposition temporaire contre rémunération, d'un équipement terminal permettant d'utiliser sur place un réseau ou un service de communications électroniques sans relation contractuelle avec le fournisseur du réseau ou du service.

67° " bureau public de communications électroniques " : local ou dispositif accessible au public en vue de la mise à disposition temporaire contre rémunération, d'un équipement terminal permettant d'utiliser sur place un réseau ou un service de communications électroniques sans relation contractuelle avec le fournisseur du réseau ou du service.

68° " violation de données à caractère personnel " : une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications

68° " violation de données à caractère personnel " : une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications

TEXTE EN VIGUEUR

électroniques accessibles au public dans la Communauté;

69° " ENISA " : Agence européenne chargée de la sécurité des réseaux et de l'information instituée par le Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information;

70° "ORECE": Organe des régulateurs européens des communications électroniques, en anglais "Body of European Regulators for Electronic Communications (BEREC)", institué par le Règlement (UE) n° 2018/1971 du Parlement européen et du Conseil du 11 décembre 2018 établissant l'Organe des régulateurs européens des communications électroniques (ORECE) et l'Agence de soutien à l'ORECE (Office ORECE) modifiant le règlement (UE) 2015/2120 et abrogeant le règlement (CE) n° 1211/200, ci-après dénommé "Règlement (UE) 2018/1971;

71° "Office": Agence de soutien à l'ORECE, instituée par le Règlement (UE) 2018/1971;

71/1° "RSPG": groupe pour la politique en matière de spectre radioélectrique, en anglais "Radio Spectrum Policy Group", institué par la décision de la Commission européenne du 11 juin 2019 instituant un groupe pour la politique en matière de spectre radioélectrique et abrogeant la décision 2002/622/CE;

72° " Utilisateur prioritaire " : utilisateur de réseaux ou de services de communications électroniques qui par les tâches qu'il exerce et ses activités a une fonction sociétale reconnue importante par les autorités et qui par un manque d'accès aux services ou réseaux de communications électroniques n'est plus en mesure d'exécuter de façon adéquate ses tâches ou activités, ce qui peut mener à une situation qui peut nuire à la sécurité publique, ou la sécurité civile et la protection civile, ou à la défense civile, ou à la planification de crise, ou à la sécurité ou à la protection du potentiel économique et scientifique du pays;

PROJET DE LOI

électroniques accessibles au public dans la Communauté;

69° " ENISA " : Agence européenne chargée de la sécurité des réseaux et de l'information instituée par le Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information;

70° "ORECE": Organe des régulateurs européens des communications électroniques, en anglais "Body of European Regulators for Electronic Communications (BEREC)", institué par le Règlement (UE) n° 2018/1971 du Parlement européen et du Conseil du 11 décembre 2018 établissant l'Organe des régulateurs européens des communications électroniques (ORECE) et l'Agence de soutien à l'ORECE (Office ORECE) modifiant le règlement (UE) 2015/2120 et abrogeant le règlement (CE) n° 1211/200, ci-après dénommé "Règlement (UE) 2018/1971;

71° "Office": Agence de soutien à l'ORECE, instituée par le Règlement (UE) 2018/1971;

71/1° "RSPG": groupe pour la politique en matière de spectre radioélectrique, en anglais "Radio Spectrum Policy Group", institué par la décision de la Commission européenne du 11 juin 2019 instituant un groupe pour la politique en matière de spectre radioélectrique et abrogeant la décision 2002/622/CE;

72° " Utilisateur prioritaire " : utilisateur de réseaux ou de services de communications électroniques qui par les tâches qu'il exerce et ses activités a une fonction sociétale reconnue importante par les autorités et qui par un manque d'accès aux services ou réseaux de communications électroniques n'est plus en mesure d'exécuter de façon adéquate ses tâches ou activités, ce qui peut mener à une situation qui peut nuire à la sécurité publique, ou la sécurité civile et la protection civile, ou à la défense civile, ou à la planification de crise, ou à la sécurité ou à la protection du potentiel économique et scientifique du pays;

TEXTE EN VIGUEUR

73° [...]

74° "appels infructueux": toute communication au cours de laquelle un appel a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau;

75° "radiorepérage" : la détermination de la position, de la vitesse et/ou d'autres caractéristiques d'un objet ou l'obtention d'informations relatives à ces paramètres, grâce aux propriétés de propagation des ondes radioélectriques;

76° "mise à disposition sur le marché" : toute fourniture d'équipements hertziens destinés à être distribués, consommés ou utilisés sur le marché de l'Union dans le cadre d'une activité commerciale, à titre onéreux ou gratuit;

77° "mise sur le marché" : la première mise à disposition d'équipements hertziens sur le marché de l'Union;

78° "mise en service" : la première utilisation des équipements hertziens au sein de l'Union par leur utilisateur final;

79° "fabricant" : toute personne physique ou morale qui fabrique des équipements hertziens ou fait concevoir ou fabriquer des équipements hertziens, et qui les commercialise sous son nom ou sa marque;

80° "importateur" : toute personne physique ou morale établie dans l'Union européenne qui met des équipements hertziens provenant d'un pays tiers sur le marché de l'Union européenne;

81° "distributeur" : toute personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fabricant ou l'importateur, qui met des équipements hertziens à disposition sur le marché;

82° "rappel" : toute mesure visant à obtenir le retour d'équipements hertziens déjà mis à la disposition de l'utilisateur final;

PROJET DE LOI

73° [...]

74° "appels infructueux": toute communication au cours de laquelle un appel a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau;

75° "radiorepérage" : la détermination de la position, de la vitesse et/ou d'autres caractéristiques d'un objet ou l'obtention d'informations relatives à ces paramètres, grâce aux propriétés de propagation des ondes radioélectriques;

76° "mise à disposition sur le marché" : toute fourniture d'équipements hertziens destinés à être distribués, consommés ou utilisés sur le marché de l'Union dans le cadre d'une activité commerciale, à titre onéreux ou gratuit;

77° "mise sur le marché" : la première mise à disposition d'équipements hertziens sur le marché de l'Union;

78° "mise en service" : la première utilisation des équipements hertziens au sein de l'Union par leur utilisateur final;

79° "fabricant" : toute personne physique ou morale qui fabrique des équipements hertziens ou fait concevoir ou fabriquer des équipements hertziens, et qui les commercialise sous son nom ou sa marque;

80° "importateur" : toute personne physique ou morale établie dans l'Union européenne qui met des équipements hertziens provenant d'un pays tiers sur le marché de l'Union européenne;

81° "distributeur" : toute personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fabricant ou l'importateur, qui met des équipements hertziens à disposition sur le marché;

82° "rappel" : toute mesure visant à obtenir le retour d'équipements hertziens déjà mis à la disposition de l'utilisateur final;

TEXTE EN VIGUEUR

83° "retrait" : toute mesure visant à empêcher la mise à disposition sur le marché d'équipements hertziens présents dans la chaîne d'approvisionnement;

84° "interface radio" : les spécifications relatives à l'utilisation réglementée du spectre radioélectrique;

85° "prestataire de services" : personne dont le service ou le contenu fourni via un réseau de communications électroniques est porté en compte par un opérateur à l'utilisateur final;

86° "opérateur facilitateur" : opérateur qui met à la disposition d'un prestataire de services des numéros ou d'autres moyens, de manière à permettre à ce dernier de faire percevoir, par voie de facturation par un opérateur ou par comptabilisation sur une carte prépayée d'un opérateur, une rémunération pour son service ou son contenu;

87° "infrastructure passive": tout élément d'un réseau de communications électroniques qui est destiné à accueillir d'autres éléments d'un autre réseau de communications électroniques sans devenir lui-même un élément actif de ce dernier réseau, tel que les conduites, pylônes, gaines, chambres de tirage et regards, trous de visite, boîtiers, immeubles ou accès à des immeubles, installations liées aux antennes, tours ou poteaux ;

88° "point d'information unique": le système d'information mis en place au sein de la plateforme de l'ASBL "KLIM - CICC (Federaal Kabels en leidingen Informatie Meldpunt - Point de Contact fédéral Information Câbles et Conduites);

89° "MNO": un opérateur qui offre des services de communications électroniques mobiles et qui dispose d'un réseau d'accès radioélectrique propre, ainsi que de tous les éléments utiles à l'exploitation du réseau ;

PROJET DE LOI

83° "retrait" : toute mesure visant à empêcher la mise à disposition sur le marché d'équipements hertziens présents dans la chaîne d'approvisionnement;

84° "interface radio" : les spécifications relatives à l'utilisation réglementée du spectre radioélectrique;

85° "prestataire de services" : personne dont le service ou le contenu fourni via un réseau de communications électroniques est porté en compte par un opérateur à l'utilisateur final;

86° "opérateur facilitateur" : opérateur qui met à la disposition d'un prestataire de services des numéros ou d'autres moyens, de manière à permettre à ce dernier de faire percevoir, par voie de facturation par un opérateur ou par comptabilisation sur une carte prépayée d'un opérateur, une rémunération pour son service ou son contenu;

87° "infrastructure passive": tout élément d'un réseau de communications électroniques qui est destiné à accueillir d'autres éléments d'un autre réseau de communications électroniques sans devenir lui-même un élément actif de ce dernier réseau, tel que les conduites, pylônes, gaines, chambres de tirage et regards, trous de visite, boîtiers, immeubles ou accès à des immeubles, installations liées aux antennes, tours ou poteaux ;

88° "point d'information unique": le système d'information mis en place au sein de la plateforme de l'ASBL "KLIM - CICC (Federaal Kabels en leidingen Informatie Meldpunt - Point de Contact fédéral Information Câbles et Conduites);

89° "MNO": un opérateur qui offre des services de communications électroniques mobiles et qui dispose d'un réseau d'accès radioélectrique propre, ainsi que de tous les éléments utiles à l'exploitation du réseau ;

TEXTE EN VIGUEUR

"90° "MVNO": un opérateur qui offre des services de communications électroniques mobiles sans être MNO;

91° "données de communications électroniques": le contenu et les métadonnées de communications électroniques;

92° "contenu de communications électroniques": le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son;

93° "métadonnées de communications électroniques": les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication.

Article 6

Dans l'accomplissement des tâches qui lui incombent en vertu de la présente loi, l'Institut:

1° promeut la connectivité et l'accès à des réseaux à très haute capacité, y compris des réseaux fixes, mobiles et sans fil, et la pénétration de tels réseaux;

2° promeut la concurrence dans la fourniture de réseaux de communications électroniques et de

PROJET DE LOI

"90° "MVNO": un opérateur qui offre des services de communications électroniques mobiles sans être MNO;

91° "données de communications électroniques": le contenu et les métadonnées de communications électroniques;

92° "contenu de communications électroniques": le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son;

93° "métadonnées de communications électroniques": les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication ;

94° « fournisseur d'infrastructure numérique » : une entité qui relève du secteur infrastructure numérique, à l'exception des prestataires de services de confiance, au sens de l'article 8, 24°, de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

Article 6

Dans l'accomplissement des tâches qui lui incombent en vertu de la présente loi, l'Institut:

1° promeut la connectivité et l'accès à des réseaux à très haute capacité, y compris des réseaux fixes, mobiles et sans fil, et la pénétration de tels réseaux;

2° promeut la concurrence dans la fourniture de réseaux de communications électroniques et de

TEXTE EN VIGUEUR

ressources associées, y compris une concurrence efficace fondée sur les infrastructures, et dans la fourniture de services de communications électroniques et de services associés;

3° contribue au développement du marché intérieur en éliminant les derniers obstacles à l'investissement dans les réseaux de communications électroniques, les services de communications électroniques, les ressources associées et les services associés et à la fourniture de ces réseaux, services et ressources, et en facilitant les conditions de convergence en faveur de cet investissement; en élaborant des règles communes et des approches régulatrices prévisibles; en favorisant l'utilisation efficace, efficiente et coordonnée du spectre radioélectrique, l'innovation ouverte, l'établissement et le développement de réseaux transeuropéens, la fourniture, la disponibilité et l'interopérabilité de services paneuropéens et la connectivité de bout en bout;

4° promeut les intérêts des citoyens, en assurant la connectivité et la disponibilité et la pénétration à grande échelle des réseaux à très haute capacité, y compris les réseaux fixes, mobiles et sans fil, et des services de communications électroniques; en offrant un maximum d'avantages en termes de choix, de prix et de qualité sur la base d'une concurrence effective; en préservant la sécurité des réseaux et services; en assurant un niveau commun élevé de protection des utilisateurs finaux grâce à la réglementation sectorielle nécessaire et en répondant aux besoins, tels que des prix abordables, de groupes sociaux particuliers, notamment les utilisateurs finaux handicapés, les utilisateurs finaux âgés et les utilisateurs finaux ayant des besoins sociaux particuliers, ainsi qu'en assurant un accès et un choix équivalents pour les utilisateurs finaux handicapés.

Article 105

§ 1^{er}. Dans le but de préserver les intérêts visés à l'article 3, § 1^{er}, de la loi du 11 décembre 1998 relative à la classification et aux habilitations,

PROJET DE LOI

ressources associées, y compris une concurrence efficace fondée sur les infrastructures, et dans la fourniture de services de communications électroniques et de services associés;

3° contribue au développement du marché intérieur en éliminant les derniers obstacles à l'investissement dans les réseaux de communications électroniques, les services de communications électroniques, les ressources associées et les services associés et à la fourniture de ces réseaux, services et ressources, et en facilitant les conditions de convergence en faveur de cet investissement; en élaborant des règles communes et des approches régulatrices prévisibles; en favorisant l'utilisation efficace, efficiente et coordonnée du spectre radioélectrique, l'innovation ouverte, l'établissement et le développement de réseaux transeuropéens, la fourniture, la disponibilité et l'interopérabilité de services paneuropéens et la connectivité de bout en bout;

4° promeut les intérêts des citoyens, en assurant la connectivité et la disponibilité et la pénétration à grande échelle des réseaux à très haute capacité, y compris les réseaux fixes, mobiles et sans fil, et des services de communications électroniques; en offrant un maximum d'avantages en termes de choix, de prix et de qualité sur la base d'une concurrence effective; en préservant la sécurité des **réseaux et systèmes d'information**; en assurant un niveau commun élevé de protection des utilisateurs finaux grâce à la réglementation sectorielle nécessaire et en répondant aux besoins, tels que des prix abordables, de groupes sociaux particuliers, notamment les utilisateurs finaux handicapés, les utilisateurs finaux âgés et les utilisateurs finaux ayant des besoins sociaux particuliers, ainsi qu'en assurant un accès et un choix équivalents pour les utilisateurs finaux handicapés.

Article 105

§ 1^{er}. Dans le but de préserver les intérêts visés à l'article 3, § 1^{er}, de la loi du 11 décembre 1998 relative à la classification et aux habilitations,

TEXTE EN VIGUEUR

attestations et avis de sécurité, les MNO obtiennent une autorisation établie de façon conjointe par les ministres concernés visés à l'alinéa 3, 1°, avant d'utiliser un élément de leur réseau 5G.

En tenant compte des intérêts visés à l'alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi peut prévoir que cette autorisation est également nécessaire avant que les MNO ne puissent bénéficier de services de fournisseurs qui consistent à intervenir ponctuellement dans la gestion de ce réseau, notamment en cas d'incident ou de modification majeure du réseau, ou à gérer ou superviser quotidiennement des éléments du réseau ou est également nécessaire avant qu'ils ne puissent bénéficier de certains de ces services.

Pour l'application du présent article, on entend par :

1° ministres concernés : le Premier ministre, le ministre des Télécommunications, le ministre de la Défense, le ministre de la Justice, le ministre de l'Intérieur et le ministre des Affaires étrangères ;

2° réseau 5G : un réseau de communications électroniques dont le réseau d'accès radioélectrique est basé sur une interface radio spécifiée dans la recommandation UIT-R M.2150 de l'Union internationale des télécommunications.

Les alinéas 1er et 2 ne sont pas d'application :

1° pour l'utilisation d'éléments passifs du réseau, à savoir des éléments qui ne sont pas alimentés par une source d'énergie ;

2° pour les points de terminaison pour autant qu'ils ne contiennent pas une partie radio basée sur une interface radio spécifiée dans la recommandation UIT-R M.2150 de l'Union internationale des télécommunications ;

3° pour les éléments de réseaux mobiles de quatrième génération et des générations

PROJET DE LOI

attestations et avis de sécurité, les MNO obtiennent une autorisation établie de façon conjointe par les ministres concernés visés à l'alinéa 3, 1°, avant d'utiliser un élément de leur réseau 5G.

En tenant compte des intérêts visés à l'alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi peut prévoir que cette autorisation est également nécessaire avant que les MNO ne puissent bénéficier de services de fournisseurs qui consistent à intervenir ponctuellement dans la gestion de ce réseau, notamment en cas d'incident ou de modification majeure du réseau, ou à gérer ou superviser quotidiennement des éléments du réseau ou est également nécessaire avant qu'ils ne puissent bénéficier de certains de ces services.

Pour l'application du présent article, on entend par :

1° ministres concernés : le Premier ministre, le ministre des Télécommunications, le ministre de la Défense, le ministre de la Justice, le ministre de l'Intérieur et le ministre des Affaires étrangères ;

2° réseau 5G : un réseau de communications électroniques dont le réseau d'accès radioélectrique est basé sur une interface radio spécifiée dans la recommandation UIT-R M.2150 de l'Union internationale des télécommunications.

Les alinéas 1er et 2 ne sont pas d'application :

1° pour l'utilisation d'éléments passifs du réseau, à savoir des éléments qui ne sont pas alimentés par une source d'énergie ;

2° pour les points de terminaison pour autant qu'ils ne contiennent pas une partie radio basée sur une interface radio spécifiée dans la recommandation UIT-R M.2150 de l'Union internationale des télécommunications ;

3° pour les éléments de réseaux mobiles de quatrième génération et des générations

TEXTE EN VIGUEUR

antérieures, pour autant qu'ils ne soient pas nécessaires à la fourniture d'un réseau 5G.

Si l'utilisation de l'élément de réseau ou le recours au fournisseur de services est déjà effectif à la date d'entrée en vigueur de l'arrêté royal visé au paragraphe 4, alinéa 1er, une autorisation de régularisation est demandée dans les deux mois qui suivent cette date.

§ 2. En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er, le Roi peut, par arrêté délibéré en Conseil des ministres :

1° étendre l'obligation d'obtenir les autorisations visées au paragraphe 1er à une ou plusieurs catégories de MVNO ;

2° étendre l'obligation d'obtenir les autorisations visées au paragraphe 1er à la société anonyme de droit public ASTRID, et aux exploitants d'un réseau privé de communications électroniques qui ont été désignés comme exploitant d'une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ou comme opérateur de services essentiels au sens de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ;

3° charger une ou plusieurs autorités de désigner par décision individuelle, lorsque c'est nécessaire pour préserver les intérêts visés au paragraphe 1er, alinéa 1er, les autres exploitants d'un réseau privé de communications électroniques soumis à l'obligation d'obtenir les autorisations visées au paragraphe 1er ;

4° préciser les hypothèses dans lesquelles une autorisation visée au paragraphe 1er, alinéa 1er, est nécessaire en cas de mise à jour d'un logiciel ou d'un dispositif matériel du réseau ;

§ 3. Le demandeur introduit son dossier auprès de l'Institut, selon les modalités qu'il fixe sur son site internet.

PROJET DE LOI

antérieures, pour autant qu'ils ne soient pas nécessaires à la fourniture d'un réseau 5G.

Si l'utilisation de l'élément de réseau ou le recours au fournisseur de services est déjà effectif à la date d'entrée en vigueur de l'arrêté royal visé au paragraphe 4, alinéa 1er, une autorisation de régularisation est demandée dans les deux mois qui suivent cette date.

§ 2. En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er, le Roi peut, par arrêté délibéré en Conseil des ministres :

1° étendre l'obligation d'obtenir les autorisations visées au paragraphe 1er à une ou plusieurs catégories de MVNO ;

2° étendre l'obligation d'obtenir les autorisations visées au paragraphe 1er à la société anonyme de droit public ASTRID, et aux exploitants d'un réseau privé de communications électroniques qui ont été désignés comme exploitant d'une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques [...]

3° charger une ou plusieurs autorités de désigner par décision individuelle, lorsque c'est nécessaire pour préserver les intérêts visés au paragraphe 1er, alinéa 1er, les autres exploitants d'un réseau privé de communications électroniques soumis à l'obligation d'obtenir les autorisations visées au paragraphe 1er ;

4° préciser les hypothèses dans lesquelles une autorisation visée au paragraphe 1er, alinéa 1er, est nécessaire en cas de mise à jour d'un logiciel ou d'un dispositif matériel du réseau ;

§ 3. Le demandeur introduit son dossier auprès de l'Institut, selon les modalités qu'il fixe sur son site internet.

TEXTE EN VIGUEUR

Le Roi fixe, par arrêté délibéré en Conseil des ministres, les modalités de traitement de la demande et la composition du dossier.

Les ministres concernés, l'Institut et les services de renseignement et de sécurité peuvent demander des informations ou des documents complémentaires au demandeur ou à toute personne pouvant contribuer utilement à leur information.

§ 4. Lorsqu'ils prennent leur décision après l'examen de la demande visée au paragraphe 1er, ou la revoient d'initiative en raison d'un nouvel élément de nature à remettre en cause leur décision, les ministres concernés mettent en oeuvre les restrictions et délais de mise en oeuvre fixés par le Roi, par arrêté délibéré en Conseil des ministres, concernant l'utilisation, sur le territoire national ou dans les zones sensibles de ce territoire, d'éléments de réseau ou de services de fournisseurs à haut risque.

Ces restrictions et ces délais de mise en oeuvre ne peuvent être fixés qu'en vue de garantir la protection des intérêts visés au paragraphe 1er, alinéa 1er.

Lorsqu'ils revoient leur décision d'initiative et lorsque c'est justifié, les ministres concernés fixent une date de mise en oeuvre de la nouvelle décision qui est postérieure aux délais fixés par l'arrêté royal visé à l'alinéa 1er et qui suit d'au moins cinq ans la date de sa notification.

Le profil de risque d'un fournisseur est évalué sur base des critères suivants :

1° la probabilité qu'il subisse une ingérence de la part d'un pays autre qu'un Etat membre de l'Union européenne, une telle ingérence pouvant être facilitée, sans s'y limiter, par la présence d'un ou de plusieurs des facteurs suivants :

a) un lien fort avec les autorités publiques du pays en question ;

PROJET DE LOI

Le Roi fixe, par arrêté délibéré en Conseil des ministres, les modalités de traitement de la demande et la composition du dossier.

Les ministres concernés, l'Institut et les services de renseignement et de sécurité peuvent demander des informations ou des documents complémentaires au demandeur ou à toute personne pouvant contribuer utilement à leur information.

§ 4. Lorsqu'ils prennent leur décision après l'examen de la demande visée au paragraphe 1er, ou la revoient d'initiative en raison d'un nouvel élément de nature à remettre en cause leur décision, les ministres concernés mettent en oeuvre les restrictions et délais de mise en oeuvre fixés par le Roi, par arrêté délibéré en Conseil des ministres, concernant l'utilisation, sur le territoire national ou dans les zones sensibles de ce territoire, d'éléments de réseau ou de services de fournisseurs à haut risque.

Ces restrictions et ces délais de mise en oeuvre ne peuvent être fixés qu'en vue de garantir la protection des intérêts visés au paragraphe 1er, alinéa 1er.

Lorsqu'ils revoient leur décision d'initiative et lorsque c'est justifié, les ministres concernés fixent une date de mise en oeuvre de la nouvelle décision qui est postérieure aux délais fixés par l'arrêté royal visé à l'alinéa 1er et qui suit d'au moins cinq ans la date de sa notification.

Le profil de risque d'un fournisseur est évalué sur base des critères suivants :

1° la probabilité qu'il subisse une ingérence de la part d'un pays autre qu'un Etat membre de l'Union européenne, une telle ingérence pouvant être facilitée, sans s'y limiter, par la présence d'un ou de plusieurs des facteurs suivants :

a) un lien fort avec les autorités publiques du pays en question ;

TEXTE EN VIGUEUR

b) la législation ou la situation au sein du pays en question, notamment lorsqu'il n'y a pas de contrôle démocratique ou législatif en place ou en l'absence de conventions de protection des données ou de sécurité entre l'Union européenne et le pays en question ;

c) les caractéristiques de la propriété d'entreprise du fournisseur ;

d) la capacité du pays en question à exercer toute forme de pression, y compris par rapport au lieu de fabrication des équipements ;

e) le fait que le pays d'où est originaire le fournisseur mène ou est associé à une politique cyber offensive ;

2° la capacité du fournisseur à garantir l'approvisionnement en termes de délai et de quantité ;

3° la qualité globale des produits ou services et les pratiques en matière de sécurité du fournisseur, y compris le degré de contrôle sur sa propre chaîne d'approvisionnement et la question de savoir si une hiérarchisation adéquate des priorités est donnée aux pratiques en matière de sécurité.

Le Roi peut, par arrêté délibéré en Conseil des ministres, compléter les critères visés à l'alinéa 4.

Un seul de ces critères peut justifier qu'un fournisseur soit qualifié comme étant à haut risque.

Le profil de risque d'un fournisseur est évalué sur la base d'un avis des services de renseignement et de sécurité en ce qui concerne le critère fixé à l'alinéa 4, 1°, et sur la base d'un avis de l'Institut en ce qui concerne les critères fixés à l'alinéa 4, 2° et 3°.

Les zones sensibles sont identifiées par le Roi, sur base d'un avis du Conseil national de sécurité, et ce, en tenant compte de la présence dans ces

PROJET DE LOI

b) la législation ou la situation au sein du pays en question, notamment lorsqu'il n'y a pas de contrôle démocratique ou législatif en place ou en l'absence de conventions de protection des données ou de sécurité entre l'Union européenne et le pays en question ;

c) les caractéristiques de la propriété d'entreprise du fournisseur ;

d) la capacité du pays en question à exercer toute forme de pression, y compris par rapport au lieu de fabrication des équipements ;

e) le fait que le pays d'où est originaire le fournisseur mène ou est associé à une politique cyber offensive ;

2° la capacité du fournisseur à garantir l'approvisionnement en termes de délai et de quantité ;

3° la qualité globale des produits ou services et les pratiques en matière de sécurité du fournisseur, y compris le degré de contrôle sur sa propre chaîne d'approvisionnement et la question de savoir si une hiérarchisation adéquate des priorités est donnée aux pratiques en matière de sécurité.

Le Roi peut, par arrêté délibéré en Conseil des ministres, compléter les critères visés à l'alinéa 4.

Un seul de ces critères peut justifier qu'un fournisseur soit qualifié comme étant à haut risque.

Le profil de risque d'un fournisseur est évalué sur la base d'un avis des services de renseignement et de sécurité en ce qui concerne le critère fixé à l'alinéa 4, 1°, et sur la base d'un avis de l'Institut en ce qui concerne les critères fixés à l'alinéa 4, 2° et 3°.

Les zones sensibles sont identifiées par le Roi, sur base d'un avis du Conseil national de sécurité, et ce, en tenant compte de la présence dans ces

TEXTE EN VIGUEUR

zones de sites liés aux intérêts visés au paragraphe 1er, alinéa 1er.

L'arrêté royal identifiant les zones sensibles est publié par voie de mention au Moniteur belge.

§ 5. Lorsque les ministres concernés entendent refuser l'autorisation, l'assortir de conditions ou revoir leur décision, le demandeur dispose de vingt-huit jours après avoir reçu le projet de décision pour présenter ses observations écrites.

La possibilité est offerte au demandeur d'être entendu. Il peut se faire accompagner par les conseils, techniques ou juridiques, de son choix.

Les ministres concernés peuvent se faire représenter par l'administration de leur choix. L'Institut et les services de renseignement et de sécurité peuvent participer à l'audition.

§ 6. Les ministres concernés prennent ensemble une seule décision. L'Institut pose tous les actes utiles en vue de sa préparation.

Dans le délai fixé par le Roi, qui commence à partir de l'introduction de la demande, le demandeur reçoit la décision des ministres qui octroie l'autorisation ou le projet de décision dans lequel ils refusent l'autorisation ou l'assortissent de conditions.

En cas d'audition ou d'observations écrites du demandeur, visées au paragraphe 5, les ministres prennent leur décision au plus tard dans le délai fixé par le Roi, qui commence à partir de la réception des observations écrites ou de la date de l'audition, la date la plus tardive étant retenue.

La demande d'informations ou de documents visée au paragraphe 3, alinéa 3, ou adressée au demandeur afin qu'il complète son dossier, suspend les délais fixés aux alinéas 2 et 3, jusqu'au jour où les informations ou documents demandés sont fournis.

PROJET DE LOI

zones de sites liés aux intérêts visés au paragraphe 1er, alinéa 1er.

L'arrêté royal identifiant les zones sensibles est publié par voie de mention au Moniteur belge.

§ 5. Lorsque les ministres concernés entendent refuser l'autorisation, l'assortir de conditions ou revoir leur décision, le demandeur dispose de vingt-huit jours après avoir reçu le projet de décision pour présenter ses observations écrites.

La possibilité est offerte au demandeur d'être entendu. Il peut se faire accompagner par les conseils, techniques ou juridiques, de son choix.

Les ministres concernés peuvent se faire représenter par l'administration de leur choix. L'Institut et les services de renseignement et de sécurité peuvent participer à l'audition.

§ 6. Les ministres concernés prennent ensemble une seule décision. L'Institut pose tous les actes utiles en vue de sa préparation.

Dans le délai fixé par le Roi, qui commence à partir de l'introduction de la demande, le demandeur reçoit la décision des ministres qui octroie l'autorisation ou le projet de décision dans lequel ils refusent l'autorisation ou l'assortissent de conditions.

En cas d'audition ou d'observations écrites du demandeur, visées au paragraphe 5, les ministres prennent leur décision au plus tard dans le délai fixé par le Roi, qui commence à partir de la réception des observations écrites ou de la date de l'audition, la date la plus tardive étant retenue.

La demande d'informations ou de documents visée au paragraphe 3, alinéa 3, ou adressée au demandeur afin qu'il complète son dossier, suspend les délais fixés aux alinéas 2 et 3, jusqu'au jour où les informations ou documents demandés sont fournis.

TEXTE EN VIGUEUR

Le défaut de décision ou de projet de décision visé à l'alinéa 2 dans le délai fixé en vertu de l'alinéa 2 ou de l'alinéa 3 équivaut à un refus.

§ 7. La personne qui obtient une copie de la liste des zones sensibles visée au paragraphe 4, alinéa 8, ne peut la transmettre qu'aux personnes qui ont besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission dans le cadre du déploiement et de l'exploitation du réseau 5G.

Est punie d'une amende pénale de 1000 euros à 100 000 euros : la personne qui divulgue des informations relatives à la liste visée à l'alinéa 1er à une personne qui n'est pas visée à cet alinéa.

Les personnes qui traitent une demande d'autorisation ou la révision d'une décision antérieure peuvent communiquer à des administrations publiques qu'elles consultent dans ce cadre des informations confidentielles lorsque c'est nécessaire pour l'accomplissement de la tâche qu'elles leur confient.

Les personnes et les administrations publiques visées à l'alinéa 3 ne peuvent pas communiquer à des tiers des informations confidentielles dont elles ont connaissance dans le cadre de l'application du présent article, hormis les exceptions prévues par la loi.

Ces informations confidentielles sont celles qui sont qualifiées comme telles par la personne qui les a fournies, sans préjudice de l'article 23, paragraphe 3, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.

La violation de l'interdiction visée à l'alinéa 4 sera punie par les peines prévues à l'article 458 du Code pénal ou l'une de ces peines.

§ 8. Lorsqu'un MNO offre en Belgique des services de communications électroniques à l'aide d'un réseau 5G, les infrastructures de ce réseau doivent se trouver sur le territoire des Etats membres de l'Union européenne. En

PROJET DE LOI

Le défaut de décision ou de projet de décision visé à l'alinéa 2 dans le délai fixé en vertu de l'alinéa 2 ou de l'alinéa 3 équivaut à un refus.

§ 7. La personne qui obtient une copie de la liste des zones sensibles visée au paragraphe 4, alinéa 8, ne peut la transmettre qu'aux personnes qui ont besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission dans le cadre du déploiement et de l'exploitation du réseau 5G.

Est punie d'une amende pénale de 1000 euros à 100 000 euros : la personne qui divulgue des informations relatives à la liste visée à l'alinéa 1er à une personne qui n'est pas visée à cet alinéa.

Les personnes qui traitent une demande d'autorisation ou la révision d'une décision antérieure peuvent communiquer à des administrations publiques qu'elles consultent dans ce cadre des informations confidentielles lorsque c'est nécessaire pour l'accomplissement de la tâche qu'elles leur confient.

Les personnes et les administrations publiques visées à l'alinéa 3 ne peuvent pas communiquer à des tiers des informations confidentielles dont elles ont connaissance dans le cadre de l'application du présent article, hormis les exceptions prévues par la loi.

Ces informations confidentielles sont celles qui sont qualifiées comme telles par la personne qui les a fournies, sans préjudice de l'article 23, paragraphe 3, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.

La violation de l'interdiction visée à l'alinéa 4 sera punie par les peines prévues à l'article 458 du Code pénal ou l'une de ces peines.

§ 8. Lorsqu'un MNO offre en Belgique des services de communications électroniques à l'aide d'un réseau 5G, les infrastructures de ce réseau doivent se trouver sur le territoire des Etats membres de l'Union européenne. En

TEXTE EN VIGUEUR

tenant compte des intérêts visés au paragraphe 1er, alinéa 1er, et par arrêté délibéré en Conseil des ministres, le Roi peut fixer les exigences qui découlent de cette obligation.

En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi impose aux MNO visés à l'alinéa 1er les règles nécessaires pour qu'ils effectuent les activités indispensables au fonctionnement, à la sécurité et à la continuité de leur réseau, qu'il détermine, au sein du territoire des Etats membres de l'Union européenne.

En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi peut étendre les règles et exigences visées aux alinéas 1er et 2 aux MVNO et exploitants d'un réseau privé de communications électroniques qui sont soumis aux autorisations visées au paragraphe 1er.

Article 107/2

§ 1^{er}. Les opérateurs analysent les risques pour la sécurité de leurs réseaux et services. L'Institut peut fixer les modalités de cette analyse de risque.

Les opérateurs prennent les mesures d'ordre technique et organisationnel adéquates et proportionnées, y compris le cas échéant le chiffrement, pour gérer ces risques de manière appropriée ainsi que pour prévenir et limiter l'impact des incidents de sécurité tant pour les utilisateurs que pour d'autres réseaux et services.

Compte tenu des possibilités techniques les plus récentes, ces mesures garantissent un niveau de sécurité adapté aux risques existants.

PROJET DE LOI

tenant compte des intérêts visés au paragraphe 1er, alinéa 1er, et par arrêté délibéré en Conseil des ministres, le Roi peut fixer les exigences qui découlent de cette obligation.

En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi impose aux MNO visés à l'alinéa 1er les règles nécessaires pour qu'ils effectuent les activités indispensables au fonctionnement, à la sécurité et à la continuité de leur réseau, qu'il détermine, au sein du territoire des Etats membres de l'Union européenne.

En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi peut étendre les règles et exigences visées aux alinéas 1er et 2 aux MVNO et exploitants d'un réseau privé de communications électroniques qui sont soumis aux autorisations visées au paragraphe 1er.

Article 107/2

§ 1^{er}. Sans préjudice des dispositions de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, les fournisseurs d'infrastructure numérique analysent les risques pour la sécurité de leurs réseaux et systèmes d'information. L'Institut peut fixer des modalités de cette analyse de risque.

[...]

[...]

TEXTE EN VIGUEUR

Le Roi, sur proposition de l'Institut ou d'initiative, [...] sur avis de l'Institut, peut préciser les mesures visées à l'alinéa 2, lorsque le risque visé à cet alinéa découle de l'organisation des opérateurs.

Sous réserve de l'alinéa 4 et après avis de [...] l'Institut, le Roi peut préciser les mesures visées à l'alinéa 2.

§ 2. Sans préjudice du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, ci-après dénommé "RGPD" et de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, ci-après dénommée "loi du 30 juillet 2018", les mesures prévues au paragraphe 1er que prennent les opérateurs de services de communications électroniques, lorsqu'elles concernent des données à caractère personnel, visent pour le moins:

1° garantir que seules des personnes habilitées à agir à des fins légalement autorisées puissent avoir accès aux données à caractère personnel;

2° protéger les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites; et

3° assurer la mise en oeuvre d'une politique de sécurité relative au traitement des données à caractère personnel.

L'Institut est habilité à vérifier les mesures prises par ces opérateurs ainsi qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient permettre d'atteindre.

PROJET DE LOI

§ 2. Sans préjudice du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, ci-après dénommé "RGPD" et de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, ci-après dénommée "loi du 30 juillet 2018", les opérateurs veillent pour le moins à:

1° garantir que seules des personnes habilitées à agir à des fins légalement autorisées puissent avoir accès aux données à caractère personnel qu'ils traitent;

2° protéger les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites; et

3° assurer la mise en oeuvre d'une politique de sécurité relative au traitement des données à caractère personnel.

L'Institut est habilité à vérifier les mesures prises par ces opérateurs ainsi qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient permettre d'atteindre.

TEXTE EN VIGUEUR

§ 3. Les opérateurs prennent toutes les mesures nécessaires, y compris préventives, pour assurer la disponibilité la plus complète possible des services de communications vocales et des services d'accès à l'internet en cas de défaillance exceptionnelle des réseaux ou de force majeure.

Le Roi, sur proposition de l'Institut ou d'initiative, sur avis de celui-ci, peut préciser ces mesures, lorsque le risque de défaillance ou de force majeure découle de l'organisation des opérateurs.

Sans préjudice de l'alinéa 2, le Roi peut, après avis de l'Institut, préciser ces mesures.

§ 4. Les opérateurs offrent gratuitement à leurs abonnés, compte tenu des possibilités techniques, les services sécurisés adéquats, afin de permettre aux utilisateurs finaux d'éviter toute forme de communication électronique non souhaitée.

Article 107/3

§ 1^{er}. En cas de menace particulière et importante d'incident de sécurité dans un réseau public de communications électroniques ou un service de communications électroniques accessibles au public, l'opérateur informe l'Institut de la menace, de toute mesure de protection ou correctrice que ses utilisateurs peuvent prendre ainsi que des mesures qu'il a prises ou envisage de prendre.

L'opérateur informe ensuite ses utilisateurs potentiellement concernés par une telle menace, de toute mesure de protection ou correctrice que ces derniers peuvent prendre et, le cas échéant, de la menace.

L'Institut peut préciser les cas dans lesquels une information doit être notifiée ainsi que les modalités de cette communication.

§ 2. Les opérateurs notifient sans délai à l'Institut tout incident de sécurité ayant eu un impact

PROJET DE LOI

§ 3. Les opérateurs prennent toutes les mesures nécessaires, y compris préventives, pour assurer la disponibilité la plus complète possible des services de communications vocales et des services d'accès à l'internet en cas de défaillance exceptionnelle des réseaux ou de force majeure.

Le Roi, sur proposition de l'Institut ou d'initiative, sur avis de celui-ci, peut préciser ces mesures.

[...]

§ 4. Les opérateurs offrent gratuitement à leurs abonnés, compte tenu des possibilités techniques, les services sécurisés adéquats, afin de permettre aux utilisateurs finaux d'éviter toute forme de communication électronique non souhaitée.

Article 107/3

§ 1^{er}. En cas de cybermenace importante, le fournisseur d'infrastructure numérique informe l'Institut de la cybermenace, de toute mesure de protection ou correctrice que ses utilisateurs peuvent prendre ainsi que des mesures qu'il a prises ou envisage de prendre.

[...]

L'Institut peut préciser les cas dans lesquels une information doit être notifiée ainsi que les modalités de cette communication.

§ 2. En cas de violation de données à caractère personnel, l'opérateur de services de communications électroniques avertit sans

TEXTE EN VIGUEUR

significatif sur le fonctionnement des réseaux ou des services.

Afin de déterminer l'ampleur de l'impact d'un incident de sécurité, il est tenu compte en particulier des paramètres suivants, lorsqu'ils sont disponibles:

1° le nombre d'utilisateurs touchés par l'incident de sécurité;

2° la durée de l'incident de sécurité;

3° l'étendue géographique de la zone touchée par l'incident de sécurité;

4° la mesure dans laquelle le fonctionnement du réseau ou du service est affecté;

PROJET DE LOI

délai l'Autorité de protection des données, qui en avertit sans délai l'Institut.

Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, l'opérateur de services de communications électroniques avertit également sans délai l'abonné ou le particulier concerné de la violation.

L'Autorité de protection des données examine si l'opérateur se conforme à cette obligation et informe l'Institut lorsqu'elle estime que cela n'est pas le cas.

La notification d'une violation des données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si l'opérateur de services de communications électroniques a prouvé, à la satisfaction de l'Institut, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

Sans préjudice de l'obligation de l'opérateur de service de communications électroniques d'informer les abonnés et les particuliers concernés, si cet opérateur n'a pas déjà averti l'abonné ou le particulier de la violation de données à caractère personnel, l'Institut peut, à la demande de l'Autorité de protection des données, après avoir examiné les effets potentiellement négatifs de cette violation, exiger qu'il s'exécute.

La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles

TEXTE EN VIGUEUR

5° l'ampleur de l'impact sur les activités économiques et sociétales.

L'Institut précise dans quels cas l'incident de sécurité a un impact significatif au sens de l'alinéa 1er ainsi que les modalités de la notification.

En cas d'incident de sécurité, l'Institut peut en informer les autorités réglementaires des communautés compétentes en matière de réseaux de communications électroniques, les autorités réglementaires nationales des autres Etats membres et l'ENISA. L'Institut peut en informer le public ou exiger des opérateurs qu'ils le fassent, dès lors qu'il constate qu'il est d'utilité publique de divulguer l'incident de sécurité.

Une fois par an, l'Institut soumet à la Commission européenne et à l'ENISA un rapport succinct sur les notifications reçues et l'action engagée conformément au présent paragraphe.

§ 3. En cas de violation de données à caractère personnel, l'opérateur de services de communications électroniques avertit sans délai l'Autorité de protection des données, qui en avertit sans délai l'Institut.

Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, l'opérateur de service de communications électroniques avertit également sans délai

PROJET DE LOI

de la violation de données à caractère personnel.

La notification faite à l'Autorité de protection des données décrit en outre les conséquences de la violation de données à caractère personnel, et les mesures proposées ou prises par l'opérateur de services de communications électroniques pour y remédier.

[...]

[...]

[...]

§ 3. Sous réserve de mesures d'exécution techniques émanant de la Commission européenne conformément à l'article 4, point 5, de la directive 2002/58/CE, et après avis de l'Autorité de protection des données, l'Institut peut adopter des lignes directrices et, le cas échéant, édicter des instructions précisant les circonstances dans lesquelles les opérateurs de services de communications électroniques sont tenus de notifier la violation de données à caractère personnel.

Sous réserve de mesures techniques d'application émanant de la Commission européenne conformément à l'article 4, point 5, de la directive 2002/58/CE, et après avis de l'Institut, l'Autorité de protection des données peut adopter des lignes directrices et, le cas échéant, édicter des instructions précisant le

TEXTE EN VIGUEUR

l'abonné ou le particulier concerné de la violation.

L'Autorité de protection des données examine si l'opérateur se conforme à cette obligation et informe l'Institut lorsqu'elle estime que cela n'est pas le cas.

La notification d'une violation des données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si l'opérateur de services de communications électroniques a prouvé, à la satisfaction de l'Institut, qu'il a mis en oeuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

Sans préjudice de l'obligation de l'opérateur de service de communications électroniques d'informer les abonnés et les particuliers concernés, si cet opérateur n'a pas déjà averti l'abonné ou le particulier de la violation de données à caractère personnel, l'Institut peut, à la demande de l'Autorité de protection des données, après avoir examiné les effets potentiellement négatifs de cette violation, exiger qu'il s'exécute.

La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel.

La notification faite à l'Autorité de protection des données décrit en outre les conséquences de la

PROJET DE LOI

format applicable à cette notification et sa procédure de transmission.

Les opérateurs de services de communications électroniques tiennent à jour un inventaire des violations de données à caractère personnel, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier, de sorte que l'Autorité de protection des données et l'Institut puissent vérifier le respect des dispositions du paragraphe 2. Cet inventaire comprend uniquement les informations nécessaires à cette fin.

[...]

[...]

[...]

[...]

TEXTE EN VIGUEUR

violation de données à caractère personnel, et les mesures proposées ou prises par l'opérateur de service de communications électroniques pour y remédier.

§ 4. Sous réserve de mesures d'exécution techniques émanant de la Commission européenne conformément à l'article 4, point 5, de la directive 2002/58/CE, et après avis de l'Autorité de protection des données, l'Institut peut adopter des lignes directrices et, le cas échéant, édicter des instructions précisant les circonstances dans lesquelles les opérateurs de services de communications électroniques sont tenus de notifier la violation de données à caractère personnel. [...]

Sous réserve de mesures techniques d'application émanant de la Commission européenne conformément à l'article 4, point 5, de la directive 2002/58/CE, et après avis de l'Institut, l'Autorité de protection des données peut adopter des lignes directrices et, le cas échéant, édicter des instructions précisant le format applicable à cette notification et sa procédure de transmission. [...]

Les opérateurs de services de communications électroniques tiennent à jour un inventaire des violations de données à caractère personnel, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier, de sorte que l'Autorité de protection des données et l'Institut puissent vérifier le respect des dispositions du paragraphe 3. Cet inventaire comprend uniquement les informations nécessaires à cette fin. [...]

Article 107/4

§ 1^{er}. En vue de l'application des articles 107/2, 107/3 et du présent article, l'Institut peut donner des instructions contraignantes à un opérateur, y compris les mesures requises pour remédier à un incident de sécurité ou empêcher qu'un tel incident ne se produise lorsqu'une menace importante a été identifiée, ainsi que les dates limites de mise en oeuvre de ces instructions.

PROJET DE LOI**Article 107/4**

§ 1^{er}. Le présent article s'applique sans préjudice des dispositions de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, notamment en ce qui concerne les pouvoirs de supervision accordés à l'autorité sectorielle ou au service d'inspection sectoriel.

TEXTE EN VIGUEUR

A la demande de l'Institut, un opérateur [...] participe à un exercice relatif à la sécurité des réseaux ou services ou organise un tel exercice.

A la demande de l'Institut et dans le cadre de la [...] gestion des incidents de sécurité, un opérateur lui communique un point de contact disponible en permanence.

§ 2. L'opérateur fournit à l'Institut, à sa demande, toutes les informations nécessaires pour évaluer la sécurité de ses réseaux et services, y compris les documents relatifs à sa politique de sécurité. L'Institut peut fixer les modalités à respecter pour la fourniture de ces informations.

A la demande de l'Institut, un opérateur se [...] soumet à un contrôle de sécurité effectué par l'Institut lui-même, par un organisme ou en partie par l'Institut et en partie par cet organisme. L'Institut fixe l'objet et les modalités du contrôle et, lorsque le contrôle est effectué par un organisme, le délai dans lequel il doit être effectué. Lorsque le contrôle est effectué par l'Institut, ce contrôle peut inclure des inspections sur place. Lorsque le contrôle est effectué par un organisme, l'opérateur propose à l'Institut un ou plusieurs organismes pour accord. L'Institut donne son accord lorsque l'organisme est qualifié pour effectuer le contrôle et est indépendant par rapport à l'opérateur. A défaut d'accord de l'Institut dans le délai qu'il a fixé lors de la demande, l'Institut désigne lui-même l'organisme. Ce dernier communique à l'Institut le rapport complet et les résultats de ce contrôle et le coût du contrôle est à la charge de l'opérateur.

A la demande de l'Institut et pour enquêter sur [...] un cas de non-conformité par rapport aux articles 107/2, 107/3 ou au présent article ou à une mesure d'exécution ainsi que sur son effet sur la sécurité des réseaux et services, l'opérateur lui donne accès à tout élément de son réseau.

PROJET DE LOI

§ 2. L'Institut peut donner des instructions contraignantes dans le cadre des articles 107/2, 107/3 ainsi que des articles 30 et 33 de la loi du [xx xxx xxxx] précitée à un fournisseur d'infrastructure numérique, y compris les mesures requises pour remédier à un incident de sécurité ou empêcher qu'un tel incident ne se produise lorsqu'une cybermenace importante a été identifiée, ainsi que les dates limites de mise en œuvre de ces instructions.

TEXTE EN VIGUEUR

§ 3. Pour mettre en oeuvre les articles 107/2 et 107/3, l'Institut a le pouvoir d'obtenir l'assistance du "Centre de réponse aux incidents de sécurité informatique" visé à l'article 7, § 2°, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, pour les questions relevant des tâches de ce centre.

PROJET DE LOI

§ 3. Dans le cadre de la supervision des articles 107/2 et 107/3 ainsi que des articles 30 et 33 de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut peut soumettre le fournisseur d'infrastructure numérique à :

a) des inspections sur place et des contrôles à distance, y compris des contrôles aléatoires effectués par des professionnels formés;

b) des audits de sécurité réguliers et ciblés réalisés par un organisme indépendant ou par l'Institut;

c) des audits ad hoc;

d) des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération du fournisseur d'infrastructure numérique;

e) des demandes d'informations nécessaires à l'évaluation des mesures de gestion des risques en matière de cybersécurité adoptées par le fournisseur d'infrastructure numérique concerné;

f) des demandes d'accès à des données, à des documents et à toutes informations nécessaires à l'Institut pour l'accomplissement de ses tâches de supervision;

g) des demandes de preuves de la mise en oeuvre de politiques de cybersécurité, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants.

Les audits de sécurité ciblés visés au premier alinéa, point b), sont basés sur des évaluations des risques effectuées par l'Institut ou l'entité

TEXTE EN VIGUEUR**PROJET DE LOI**

contrôlée, ou sur d'autres informations disponibles relatives aux risques.

Lorsque l'audit de sécurité visé à l'alinéa 1er, point b) est effectué par un organisme indépendant, le fournisseur d'infrastructure numérique propose à l'Institut un ou plusieurs organismes pour accord. L'Institut donne son accord lorsque l'organisme indépendant est qualifié pour effectuer l'audit et est indépendant par rapport à le fournisseur d'infrastructure numérique. A défaut d'accord de l'Institut dans le délai qu'il a fixé lors de la demande, l'Institut désigne lui-même l'organisme indépendant. Ce dernier communique à l'Institut le rapport complet et les résultats de cet audit. Les coûts de l'audit sont à la charge de le fournisseur d'infrastructure numérique, sauf lorsque l'Institut en décide autrement dans des cas dûment motivés.

Lorsqu'il exerce ses pouvoirs en vertu du paragraphe 1, point e), f) ou g), l'Institut précise la finalité de la demande et les informations exigées.

L'Institut peut fixer les modalités de la fourniture par le fournisseur d'infrastructure numérique des informations concernant l'analyse de risque.

A la demande de l'Institut, un fournisseur d'infrastructure numérique participe à un exercice relatif à la sécurité des réseaux et systèmes d'information ou organise un tel exercice.

A la demande de l'Institut et dans le cadre de la gestion des incidents de sécurité, un fournisseur d'infrastructure numérique communique à l'Institut un point de contact disponible en permanence.

§ 4. L'Institut coordonne les initiatives relatives à la sécurité des réseaux publics de communications électroniques et des services de communications électroniques accessibles au public.

§ 4. A la demande de l'Institut et pour enquêter sur un cas de non-conformité par rapport aux articles 30 et 33 de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt

TEXTE EN VIGUEUR

Il supervise la détection, l'observation et l'analyse des problèmes de sécurité, et peut fournir aux utilisateurs des informations en la matière.

§ 5. Le Roi et l'Institut peuvent adapter la mise en oeuvre des articles 107/2, 107/3 et du présent article, selon le type d'opérateurs et selon différentes catégories au sein des réseaux et services.

Article 126/3

§ 1^{er}. Les données visées à l'article 126/2, § 2, sont conservées dans la zone géographique composée de

- arrondissements judiciaires dans lesquels au moins trois infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

PROJET DE LOI

général pour la sécurité publique ou à une mesure d'exécution ainsi que sur son effet sur la sécurité des réseaux et systèmes d'information, le fournisseur d'infrastructure numérique lui donne accès à tout élément de son réseau.

[...]

§ 5. Sans préjudice des compétences de l'autorité nationale de cybersécurité, l'Institut coordonne les initiatives relatives à la sécurité des réseaux publics de communications électroniques et des services de communications électroniques accessibles au public.

Il supervise la détection, l'observation et l'analyse des problèmes de sécurité, et peut fournir aux utilisateurs des informations en la matière.

§ 6. Le non-respect par un fournisseur d'infrastructure numérique du présent article ou d'une décision de l'Institut prise sur base du présent article peut faire l'objet des mesures ou amendes administratives visées dans le titre 4, chapitre 2 de la loi du [XX XXXX XXXX] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

Article 126/3

§ 1^{er}. Les données visées à l'article 126/2, § 2, sont conservées dans la zone géographique composée de

- arrondissements judiciaires dans lesquels au moins trois infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

TEXTE EN VIGUEUR

- zones de police dans lesquelles au moins trois infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours, et situées dans les arrondissements judiciaires dans lesquels pendant l'année calendrier qui précède celle en cours, moins de trois infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an sur une moyenne de trois années calendriers qui précèdent celle en cours ont été constatées.

Dans l'hypothèse visée à l'alinéa 1er, premier tiret, le délai de conservation des données visées à l'article 126/2, § 2, est de:

a) six mois, s'il y a trois ou quatre infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours

b) neuf mois, s'il y a cinq ou six infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

c) douze mois, s'il y a sept ou plus de sept infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.

Dans l'hypothèse visée à l'alinéa 1er, deuxième tiret, le délai de conservation des données visées à l'article 126/2, § 2, est de:

a) six mois, s'il y a trois ou quatre infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours ;

b) neuf mois, s'il y a cinq ou six infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées

PROJET DE LOI

- zones de police dans lesquelles au moins trois infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours, et situées dans les arrondissements judiciaires dans lesquels pendant l'année calendrier qui précède celle en cours, moins de trois infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an sur une moyenne de trois années calendriers qui précèdent celle en cours ont été constatées.

Dans l'hypothèse visée à l'alinéa 1er, premier tiret, le délai de conservation des données visées à l'article 126/2, § 2, est de:

a) six mois, s'il y a trois ou quatre infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

b) neuf mois, s'il y a cinq ou six infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

c) douze mois, s'il y a sept ou plus de sept infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.

Dans l'hypothèse visée à l'alinéa 1er, deuxième tiret, le délai de conservation des données visées à l'article 126/2, § 2, est de:

a) six mois, s'il y a trois ou quatre infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours ;

b) neuf mois, s'il y a cinq ou six infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées

TEXTE EN VIGUEUR

sur une moyenne des trois années calendriers qui précèdent celle en cours;

c) douze mois, s'il y a sept ou plus de sept infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.

Le nombre d'infractions ainsi déterminé est arrondi à l'unité supérieure ou inférieure, selon que le chiffre de la première décimale atteint ou non cinq.

Les statistiques relatives au nombre d'infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours sont issues de la Banque de données Nationale Générale visée à l'article 44/7 de la loi du 5 août 1992 sur la fonction de police.

Les périmètres des arrondissements judiciaires visés à l'alinéa 1er, premier tiret, sont fixés par l'article 4 de l'annexe au Code judiciaire.

Les périmètres des zones de police visées à l'alinéa 1er, deuxième tiret, sont ceux fixés à l'annexe de l'arrêté royal du 24 octobre 2001 portant la dénomination des zones de police.

La direction, visée à l'article 44/11 de la loi du 5 août 1992 sur la fonction de police, envoie les statistiques relatives au nombre d'infractions et la durée de conservation pour chaque arrondissement judiciaire et chaque zone de police à l'Organe de contrôle de l'information policière, qui, dans le mois, après que toutes les données nécessaires à cette fin lui aient été communiquées, procède à leur validation. L'Organe de contrôle peut exercer, aux fins de cette validation, toutes ses compétences octroyées par le titre 7 de la loi du 30 juillet 2018.

Les statistiques et les durées de conservation sont transmises par la direction visée à l'article 44/11 de la loi du 5 août 1992 sur la fonction de police au service désigné par le Roi, uniquement

PROJET DE LOI

sur une moyenne des trois années calendriers qui précèdent celle en cours;

c) douze mois, s'il y a sept ou plus de sept infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.

Le nombre d'infractions ainsi déterminé est arrondi à l'unité supérieure ou inférieure, selon que le chiffre de la première décimale atteint ou non cinq.

Les statistiques relatives au nombre d'infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours sont issues de la Banque de données Nationale Générale visée à l'article 44/7 de la loi du 5 août 1992 sur la fonction de police.

Les périmètres des arrondissements judiciaires visés à l'alinéa 1er, premier tiret, sont fixés par l'article 4 de l'annexe au Code judiciaire.

Les périmètres des zones de police visées à l'alinéa 1er, deuxième tiret, sont ceux fixés à l'annexe de l'arrêté royal du 24 octobre 2001 portant la dénomination des zones de police.

La direction, visée à l'article 44/11 de la loi du 5 août 1992 sur la fonction de police, envoie les statistiques relatives au nombre d'infractions et la durée de conservation pour chaque arrondissement judiciaire et chaque zone de police à l'Organe de contrôle de l'information policière, qui, dans le mois, après que toutes les données nécessaires à cette fin lui aient été communiquées, procède à leur validation. L'Organe de contrôle peut exercer, aux fins de cette validation, toutes ses compétences octroyées par le titre 7 de la loi du 30 juillet 2018.

Les statistiques et les durées de conservation sont transmises par la direction visée à l'article 44/11 de la loi du 5 août 1992 sur la fonction de police au service désigné par le Roi, uniquement

TEXTE EN VIGUEUR

après avoir été informé de leur validation par l'Organe de contrôle.

Sur proposition du service désigné par le Roi, chaque année, les ministres de la Justice et de l'Intérieur adoptent la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation de données ainsi que leur durée de conservation.

Après cette adoption, le service désigné par le Roi transmet la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation de données, ainsi que leur durée de conservation, aux opérateurs.

§ 2. Les données visées à l'article 126/2, § 2, sont conservées dans les zones géographiques déterminées par l'Organe de coordination pour l'analyse de la menace, dont le niveau de la menace, déterminé par l'évaluation visée à l'article 8, 1° et 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, est au moins de niveau 3, conformément à l'article 11 de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace, et, aussi longtemps que le niveau de la menace d'au moins niveau 3 perdure pour ces zones.

Si le niveau de la menace est au moins de niveau 3 et couvre l'ensemble du territoire, l'Organe de coordination pour l'analyse de la menace informe immédiatement le service désigné par le Roi afin que ce service prenne les mesures nécessaires pour informer les opérateurs et procéder à une conservation générale et indifférenciée des données visées à l'article 126/2, § 2, sur l'ensemble du territoire.

L'obligation de conservation visée à l'alinéa 2 est confirmée par arrêté royal, sur proposition conjointe du ministre de l'Intérieur et du ministre de la Justice. En l'absence de confirmation par arrêté royal, publié dans le mois de la décision visée à l'alinéa 2, la conservation de données prend fin et les opérateurs en sont avertis par le service désigné par le Roi le plus rapidement possible. Après

PROJET DE LOI

après avoir été informé de leur validation par l'Organe de contrôle.

Sur proposition du service désigné par le Roi, chaque année, les ministres de la Justice et de l'Intérieur adoptent la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation de données ainsi que leur durée de conservation.

Après cette adoption, le service désigné par le Roi transmet la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation de données, ainsi que leur durée de conservation, aux opérateurs.

§ 2. Les données visées à l'article 126/2, § 2, sont conservées dans les zones géographiques déterminées par l'Organe de coordination pour l'analyse de la menace, dont le niveau de la menace, déterminé par l'évaluation visée à l'article 8, 1° et 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, est au moins de niveau 3, conformément à l'article 11 de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace, et, aussi longtemps que le niveau de la menace d'au moins niveau 3 perdure pour ces zones.

Si le niveau de la menace est au moins de niveau 3 et couvre l'ensemble du territoire, l'Organe de coordination pour l'analyse de la menace informe immédiatement le service désigné par le Roi afin que ce service prenne les mesures nécessaires pour informer les opérateurs et procéder à une conservation générale et indifférenciée des données visées à l'article 126/2, § 2, sur l'ensemble du territoire.

L'obligation de conservation visée à l'alinéa 2 est confirmée par arrêté royal, sur proposition conjointe du ministre de l'Intérieur et du ministre de la Justice. En l'absence de confirmation par arrêté royal, publié dans le mois de la décision visée à l'alinéa 2, la conservation de données prend fin et les opérateurs en sont avertis par le service désigné par le Roi le plus rapidement possible. Après

TEXTE EN VIGUEUR

cette notification, les opérateurs suppriment les données qui ont déjà été conservées à cette fin.

§ 3. Les données visées à l'article 126/2, § 2, sont conservées dans les zones particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave, à savoir:

a) les installations portuaires, les ports et les zones de sûreté portuaire visées à l'article 2.5.2.2, 3° à 5°, du Code de la Navigation belge;

b) les gares au sens de l'article 2, 5°, de la loi du 27 avril 2018 sur la police des chemins de fer;

c) les stations de métro et de pré-métro;

d) les aéroports au sens de l'article 2, point 1), de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision n° 661/2010/UE, et les entités exploitant les installations annexes se trouvant dans les aéroports;

e) les bâtiments affectés à l'administration des douanes et accises;

f) les prisons au sens de l'article 2, 15°, de la loi de principes du 12 janvier 2005 concernant l'administration pénitentiaire ainsi que le statut juridique des détenus, les centres communautaires pour mineurs ayant commis un fait qualifié infraction, visés à l'article 606 du Code d'instruction criminelle, et les centres de psychiatrie légale, visés à l'article 3, 4°, c), de la loi du 5 mai 2014 relative à l'internement;

g) les armuriers et les stands de tir au sens de l'article 2, 1° et 19°, de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes;

PROJET DE LOI

cette notification, les opérateurs suppriment les données qui ont déjà été conservées à cette fin.

§ 3. Les données visées à l'article 126/2, § 2, sont conservées dans les zones particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave, à savoir:

a) les installations portuaires, les ports et les zones de sûreté portuaire visées à l'article 2.5.2.2, 3° à 5°, du Code de la Navigation belge;

b) les gares au sens de l'article 2, 5°, de la loi du 27 avril 2018 sur la police des chemins de fer;

c) les stations de métro et de pré-métro;

d) les aéroports au sens de l'article 2, point 1), de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision n° 661/2010/UE, et les entités exploitant les installations annexes se trouvant dans les aéroports;

e) les bâtiments affectés à l'administration des douanes et accises;

f) les prisons au sens de l'article 2, 15°, de la loi de principes du 12 janvier 2005 concernant l'administration pénitentiaire ainsi que le statut juridique des détenus, les centres communautaires pour mineurs ayant commis un fait qualifié infraction, visés à l'article 606 du Code d'instruction criminelle, et les centres de psychiatrie légale, visés à l'article 3, 4°, c), de la loi du 5 mai 2014 relative à l'internement;

g) les armuriers et les stands de tir au sens de l'article 2, 1° et 19°, de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes;

TEXTE EN VIGUEUR

h) les établissements visés à l'article 3.1.a), de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants;

i) les établissements visés à l'article 2, 1°, de l'accord de coopération du 16 février 2016 entre l'Etat fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses;

j) les communes dans lesquelles il y a un ou plusieurs éléments critiques du réseau ou une ou plusieurs infrastructures critiques, visés dans la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et ses arrêtés d'exécution; lorsque l'ensemble du réseau a été identifié comme infrastructure critique, seuls les éléments critiques du réseau sont pris en compte pour l'application du présent article;

k) le siège de la SA Astrid et les bâtiments où sont situés ses centres de données centraux et provinciaux ainsi que les bâtiments où sont situés les centres de données centraux et les noeuds de communication du système de communication et d'informations sécurisé et crypté visé à l'article 11, § 7, de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace;

l) les systèmes de réseau et d'information qui soutiennent la fourniture des services essentiels des fournisseurs de service essentiels désignés sur la base de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

m) le cas échéant, sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones particulièrement exposées à des menaces pour

PROJET DE LOI

h) les établissements visés à l'article 3.1.a), de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants;

i) les établissements visés à l'article 2, 1°, de l'accord de coopération du 16 février 2016 entre l'Etat fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses;

j) les communes dans lesquelles il y a un ou plusieurs éléments critiques du réseau ou une ou plusieurs infrastructures critiques, visés dans la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et ses arrêtés d'exécution; lorsque l'ensemble du réseau a été identifié comme infrastructure critique, seuls les éléments critiques du réseau sont pris en compte pour l'application du présent article;

k) le siège de la SA Astrid et les bâtiments où sont situés ses centres de données centraux et provinciaux ainsi que les bâtiments où sont situés les centres de données centraux et les noeuds de communication du système de communication et d'informations sécurisé et crypté visé à l'article 11, § 7, de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace;

l) les systèmes de réseau et d'information qui soutiennent la fourniture des services **des entités essentiels au sens de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;**

m) le cas échéant, sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones particulièrement exposées à des menaces pour

TEXTE EN VIGUEUR

la sécurité nationale ou à la commission d'actes de criminalité grave fixées par arrêté royal.

§ 4. Les données visées à l'article 126/2, § 2, sont conservées dans les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population, à savoir:

a) en matière d'ordre public, les zones neutres au sens de l'article 3 de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution, et les organes stratégiques ministériels;

b) pour ce qui concerne le potentiel scientifique et économique, les bâtiments affectés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé et repris sur une liste établie annuellement par la Sûreté de l'Etat et le Service général du Renseignement et de la Sécurité sur proposition du ministre de la Justice et du ministre de la Défense et approuvée par le Conseil national de sécurité;

c) pour le transport, les autoroutes et les parkings publics attenants;

d) pour ce qui concerne la souveraineté nationale et les institutions établies par la Constitution et les lois, les décrets ou les ordonnances:

i) les assemblées législatives visées à l'article 1er de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution;

ii) les maisons communales et les hôtels de ville;

iii) le palais royal;

iv) les domaines royaux;

v) les bâtiments affectés aux institutions visées au titre III, chapitres 5 à 7, de la Constitution;

PROJET DE LOI

la sécurité nationale ou à la commission d'actes de criminalité grave fixées par arrêté royal.

§ 4. Les données visées à l'article 126/2, § 2, sont conservées dans les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population, à savoir:

a) en matière d'ordre public, les zones neutres au sens de l'article 3 de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution, et les organes stratégiques ministériels;

b) pour ce qui concerne le potentiel scientifique et économique, les bâtiments affectés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé et repris sur une liste établie annuellement par la Sûreté de l'Etat et le Service général du Renseignement et de la Sécurité sur proposition du ministre de la Justice et du ministre de la Défense et approuvée par le Conseil national de sécurité;

c) pour le transport, les autoroutes et les parkings publics attenants;

d) pour ce qui concerne la souveraineté nationale et les institutions établies par la Constitution et les lois, les décrets ou les ordonnances:

i) les assemblées législatives visées à l'article 1er de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution;

ii) les maisons communales et les hôtels de ville;

iii) le palais royal;

iv) les domaines royaux;

v) les bâtiments affectés aux institutions visées au titre III, chapitres 5 à 7, de la Constitution;

TEXTE EN VIGUEUR

vi) les communes dans lesquelles se trouvent des domaines militaires;

vii) les bâtiments affectés à la police locale, à la police fédérale, ainsi qu'à la Sûreté de l'Etat;

e) pour ce qui concerne l'intégrité du territoire national, les communes frontalières;

f) pour ce qui concerne les intérêts économiques ou financiers importants, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale:

i) les hôpitaux visés à l'article 2 de la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soins;

ii) la Banque nationale de Belgique;

g) le cas échéant, et sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population fixées par arrêté royal.

§ 5. Les données visées à l'article 126/2, § 2, sont conservées dans les zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national, à savoir:

a) les ambassades et les représentations diplomatiques;

b) les bâtiments affectés à l'Union européenne;

c) les bâtiments et infrastructures affectés à l'OTAN;

d) les institutions de l'Espace économique européen;

e) les institutions des Nations Unies;

f) le cas échéant, et sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones où il y a une menace potentielle grave pour les intérêts des

PROJET DE LOI

vi) les communes dans lesquelles se trouvent des domaines militaires;

vii) les bâtiments affectés à la police locale, à la police fédérale, ainsi qu'à la Sûreté de l'Etat;

e) pour ce qui concerne l'intégrité du territoire national, les communes frontalières;

f) pour ce qui concerne les intérêts économiques ou financiers importants, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale:

i) les hôpitaux visés à l'article 2 de la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soins;

ii) la Banque nationale de Belgique;

g) le cas échéant, et sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population fixées par arrêté royal.

§ 5. Les données visées à l'article 126/2, § 2, sont conservées dans les zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national, à savoir:

a) les ambassades et les représentations diplomatiques;

b) les bâtiments affectés à l'Union européenne;

c) les bâtiments et infrastructures affectés à l'OTAN;

d) les institutions de l'Espace économique européen;

e) les institutions des Nations Unies;

f) le cas échéant, et sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones où il y a une menace potentielle grave pour les intérêts des

TEXTE EN VIGUEUR

institutions internationales établies sur le territoire national fixées par arrêté royal.

§ 6. Pour chaque catégorie de zone visée aux paragraphes 3 à 5, le Roi détermine l'étendue du périmètre de la zone.

Chaque autorité compétente dans l'une des matières visées aux paragraphes 3 à 5, transmet chaque année à la date déterminée par le Roi, uniquement au service désigné par le Roi, les informations nécessaires à la détermination concrète des zones géographiques.

Ces autorités informent sans délai uniquement ce service lorsqu'une zone géographique ne correspond plus au critère concerné afin qu'il soit mis fin le plus rapidement possible à l'obligation de conservation visée à l'article 126/1, § 1er, dans cette zone.

A l'exception de la liste des lieux visés au paragraphe 4, b), mise exclusivement à la disposition du Comité permanent R par les services de renseignement et de sécurité, le service désigné par le Roi tient à la disposition de l'Organe de contrôle de l'information policière et du Comité permanent R, chacun dans le cadre de ses compétences, la liste actualisée des zones visées aux paragraphes 3 à 5, où une conservation de données est obligatoire.

L'Organe de contrôle de l'information policière et le Comité permanent R peuvent, chacun dans le cadre de ses compétences, formuler des recommandations à l'égard de cette liste ou ordonner de manière motivée que certaines zones géographiques visées aux paragraphes 3 à 5 soient retirées de la liste.

Sur proposition du service désigné par le Roi, chaque année et lors de chaque modification visée à l'alinéa 5, le ministre de la Défense, le ministre de la Justice et le ministre de l'Intérieur adoptent la liste des zones géographiques soumises à l'obligation de conservation des données ainsi que leur durée de conservation.

PROJET DE LOI

institutions internationales établies sur le territoire national fixées par arrêté royal.

§ 6. Pour chaque catégorie de zone visée aux paragraphes 3 à 5, le Roi détermine l'étendue du périmètre de la zone.

Chaque autorité compétente dans l'une des matières visées aux paragraphes 3 à 5, transmet chaque année à la date déterminée par le Roi, uniquement au service désigné par le Roi, les informations nécessaires à la détermination concrète des zones géographiques.

Ces autorités informent sans délai uniquement ce service lorsqu'une zone géographique ne correspond plus au critère concerné afin qu'il soit mis fin le plus rapidement possible à l'obligation de conservation visée à l'article 126/1, § 1er, dans cette zone.

A l'exception de la liste des lieux visés au paragraphe 4, b), mise exclusivement à la disposition du Comité permanent R par les services de renseignement et de sécurité, le service désigné par le Roi tient à la disposition de l'Organe de contrôle de l'information policière et du Comité permanent R, chacun dans le cadre de ses compétences, la liste actualisée des zones visées aux paragraphes 3 à 5, où une conservation de données est obligatoire.

L'Organe de contrôle de l'information policière et le Comité permanent R peuvent, chacun dans le cadre de ses compétences, formuler des recommandations à l'égard de cette liste ou ordonner de manière motivée que certaines zones géographiques visées aux paragraphes 3 à 5 soient retirées de la liste.

Sur proposition du service désigné par le Roi, chaque année et lors de chaque modification visée à l'alinéa 5, le ministre de la Défense, le ministre de la Justice et le ministre de l'Intérieur adoptent la liste des zones géographiques soumises à l'obligation de conservation des données ainsi que leur durée de conservation.

TEXTE EN VIGUEUR

L'arrêté ministériel visé à l'alinéa 6 est publié par voie de mention au Moniteur belge.

Après cette approbation, le service désigné par le Roi transmet la liste des zones géographiques soumises à l'obligation de conservation des données, ainsi que leur durée de conservation, aux opérateurs.

Toute personne qui, du chef de sa fonction, a connaissance des données communiquées par les autorités compétentes au service désigné par le Roi ou de la liste des zones géographiques soumises à l'obligation de conservation des données, ou prête son concours à la mise en oeuvre du présent article, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Article 164/1

Le bureau d'enregistrement de noms de domaine Internet du domaine de premier niveau ".be " :

1° possède un lieu d'établissement et un siège d'exploitation permanents en Belgique, sans préjudice de la possibilité pour l'intéressé de dédoubler une partie de son infrastructure technique à l'étranger, dans le seul but d'améliorer la fiabilité du service;

2° se présente sous la forme d'un organisme sans but lucratif;

3° facture pour ses prestations une indemnité directement liée aux frais réellement encourus;

4° met, selon les modalités déterminées par l'Institut, gratuitement à la disposition de l'Institut les installations qu'il a prévues de sorte que le passage à un nouveau bureau d'enregistrement des noms de domaine puisse se faire de manière efficiente et efficace, sans interruption de service sérieuse. Ces installations comprennent au minimum un registre actualisé des noms de domaine et de toutes les informations afférentes des titulaires des noms de domaine selon la périodicité et les modalités

PROJET DE LOI

L'arrêté ministériel visé à l'alinéa 6 est publié par voie de mention au Moniteur belge.

Après cette approbation, le service désigné par le Roi transmet la liste des zones géographiques soumises à l'obligation de conservation des données, ainsi que leur durée de conservation, aux opérateurs.

Toute personne qui, du chef de sa fonction, a connaissance des données communiquées par les autorités compétentes au service désigné par le Roi ou de la liste des zones géographiques soumises à l'obligation de conservation des données, ou prête son concours à la mise en oeuvre du présent article, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Article 164/1

Le **registre de noms de domaine de premier niveau du domaine de premier niveau ".be " :**

1° possède un lieu d'établissement et un siège d'exploitation permanents en Belgique, sans préjudice de la possibilité pour l'intéressé de dédoubler une partie de son infrastructure technique à l'étranger, dans le seul but d'améliorer la fiabilité du service;

2° se présente sous la forme d'un organisme sans but lucratif;

3° facture pour ses prestations une indemnité directement liée aux frais réellement encourus;

4° met, selon les modalités déterminées par l'Institut, gratuitement à la disposition de l'Institut les installations qu'il a prévues de sorte que le passage à un nouveau **registre de noms de domaine de premier niveau** puisse se faire de manière efficiente et efficace, sans interruption de service sérieuse. Ces installations comprennent au minimum un registre actualisé des noms de domaine et de toutes les informations afférentes des titulaires des noms de domaine selon la périodicité et les modalités

TEXTE EN VIGUEUR

fixées par l'Institut sous une forme pouvant être utilisée immédiatement en cas d'échec sérieux du bureau d'enregistrement des noms de domaine Internet et afin de garantir la stabilité de l'Internet belge; et

5° organise, administre et gère le domaine de premier niveau ".be" dans l'intérêt général et selon les principes de qualité, d'efficacité, de fiabilité et d'accessibilité.

Article 164/2

En cas d'échec sérieux du bureau d'enregistrement de noms de domaine Internet du domaine de premier niveau ".be", l'Institut prend les mesures nécessaires dans l'intérêt de l'utilisateur final et de l'économie belge afin d'assurer la continuité et la stabilité de l'Internet belge.

Par échec sérieux du bureau d'enregistrement de noms de domaine Internet, l'on entend :

1° l'application de pratiques illégales ou malhonnêtes et qui compromettent la bonne réputation du domaine de premier niveau ".be" lié à la Belgique, ou

2° l'incapacité à assurer la disponibilité d'un nombre considérable de noms de domaine actifs du domaine de premier niveau ".be", ou

3° l'incapacité à exécuter les tâches d'un bureau d'enregistrement de noms de domaine Internet conformément à la définition de l'article 2, 48/1°, ou

4° le fait de ne pas remplir les conditions de l'article 164/1.

En cas d'urgence, l'Institut peut désigner immédiatement un nouveau bureau d'enregistrement de noms de domaine Internet du domaine de premier niveau ".be" à titre provisoire. Les coûts supportés par ce bureau d'enregistrement de noms de domaine Internet provisoire dans le cadre des tâches que l'Institut lui a confiées sont à charge de l'Institut et seront

PROJET DE LOI

fixées par l'Institut sous une forme pouvant être utilisée immédiatement en cas d'échec sérieux du **registre de noms de domaine de premier niveau** et afin de garantir la stabilité de l'Internet belge; et

5° organise, administre et gère le domaine de premier niveau ".be" dans l'intérêt général et selon les principes de qualité, d'efficacité, de fiabilité et d'accessibilité.

Article 164/2

En cas d'échec sérieux du **registre de noms de domaine de premier niveau** du domaine de premier niveau ".be", l'Institut prend les mesures nécessaires dans l'intérêt de l'utilisateur final et de l'économie belge afin d'assurer la continuité et la stabilité de l'Internet belge.

Par échec sérieux du **registre de noms de domaine de premier niveau**, l'on entend :

1° l'application de pratiques illégales ou malhonnêtes et qui compromettent la bonne réputation du domaine de premier niveau ".be" lié à la Belgique, ou

2° l'incapacité à assurer la disponibilité d'un nombre considérable de noms de domaine actifs du domaine de premier niveau ".be", ou

3° l'incapacité à exécuter les tâches d'un **registre de noms de domaine de premier niveau** conformément à la définition de l'article 2, 48/1°, ou

4° le fait de ne pas remplir les conditions de l'article 164/1.

En cas d'urgence, l'Institut peut désigner immédiatement un nouveau **registre de noms de domaine de premier niveau** du domaine de premier niveau ".be" à titre provisoire. Les coûts supportés par ce **registre de noms de domaine de premier niveau** provisoire dans le cadre des tâches que l'Institut lui a confiées sont à charge de l'Institut et seront récupérés par la suite

TEXTE EN VIGUEUR

recupérés par la suite auprès du bureau d'enregistrement de noms de domaine Internet finalement désigné.

Immédiatement après la désignation du bureau d'enregistrement de noms de domaine Internet provisoire ou lorsqu'une telle désignation n'est pas nécessaire, l'Institut lance un appel aux candidats dans le Moniteur belge et publie un cahier des charges comprenant les conditions minimales relatives à l'exécution de l'activité du bureau d'enregistrement de noms de domaine Internet du domaine de premier niveau ".be". La désignation du nouveau bureau d'enregistrement de noms de domaine Internet se fait sur la base d'une procédure objective, transparente et non-discriminatoire ainsi que de critères objectifs, transparents et non-discriminatoires.

L'entité qui est désignée comme bureau d'enregistrement de noms de domaine Internet du domaine de premier niveau ".be" est tenue de respecter les conditions minimales du cahier des charges et de respecter tous les engagements pris au cours de la procédure de sélection.

PROJET DE LOI

auprès du **registre de noms de domaine de premier niveau** finalement désigné.

Immédiatement après la désignation du **registre de noms de domaine de premier niveau** provisoire ou lorsqu'une telle désignation n'est pas nécessaire, l'Institut lance un appel aux candidats dans le Moniteur belge et publie un cahier des charges comprenant les conditions minimales relatives à l'exécution de l'activité du **registre de noms de domaine de premier niveau** du domaine de premier niveau ".be". La désignation du nouveau **registre de noms de domaine de premier niveau** se fait sur la base d'une procédure objective, transparente et non-discriminatoire ainsi que de critères objectifs, transparents et non-discriminatoires.

L'entité qui est désignée comme **registre de noms de domaine de premier niveau** du domaine de premier niveau ".be" est tenue de respecter les conditions minimales du cahier des charges et de respecter tous les engagements pris au cours de la procédure de sélection.

Article 164/3

§ 1^{er}. Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine collectent les données d'enregistrement de noms de domaine et les maintiennent exactes et complètes au sein d'une base de données spécialisée conformément au droit de l'Union en matière de protection des données à caractère personnel.

§ 2. Les données d'enregistrement de noms de domaine visées à l'alinéa 1^{er} contiennent les informations nécessaires pour identifier et contacter les titulaires des noms de domaine et les points de contact qui gèrent les noms de domaine relevant des domaines de premier niveau. Ces informations comprennent au moins les éléments suivants:

TEXTE EN VIGUEUR**PROJET DE LOI**

1° le nom de domaine;

2° la date d'enregistrement;

3° le nom du titulaire de nom de domaine, son adresse de courrier électronique et son numéro de téléphone;

4° l'adresse de courrier électronique et le numéro de téléphone permettant de contacter le point de contact qui gère le nom de domaine, si ces coordonnées sont différentes de celles du titulaire.

Après avis de l'Institut, le Roi peut ordonner aux fournisseurs et aux revendeurs de services d'anonymisation ou d'enregistrement fiduciaire de partager les données d'enregistrement de noms de domaine avec les bureaux d'enregistrement et en définir les modalités.

Le respect des obligations visées au présent article n'entraîne pas de répétition inutile de la collecte des données d'enregistrement de noms de domaine auprès de la personne concernée. A cet effet, les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine coopèrent entre eux.

Après avis de l'Institut, le Roi peut préciser les modalités de cette coopération.

§ 2. Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine mettent en place des politiques et des procédures, notamment des procédures de vérification, visant à garantir que les bases de données visées au paragraphe 1^{er}, alinéa 1^{er}, contiennent des informations exactes et complètes. Ces politiques et procédures sont mises à la disposition du public.

Si les données d'enregistrement de noms de domaine énumérées au paragraphe 1^{er}, alinéa 2, d'un nom de domaine sont incorrectes, inexactes ou incomplètes, les registres de noms

TEXTE EN VIGUEUR**PROJET DE LOI**

de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine bloquent immédiatement le fonctionnement de ce nom de domaine jusqu'à ce que le titulaire du nom de domaine corrige les données d'enregistrement pour qu'elles deviennent correctes, exactes et complètes.

Si le titulaire du nom de domaine ne le fait pas dans le délai fixé par le registre des noms de domaine de premier niveau ou par l'entité fournissant des services d'enregistrement de nom de domaine, le nom de domaine est annulé.

Le transfert d'un nom de domaine bloqué à une autre entité fournissant des services d'enregistrement de noms de domaine est interdit.

§ 3. Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine rendent publiques, sans retard injustifié après l'enregistrement d'un nom de domaine, les données d'enregistrement du nom de domaine qui ne sont pas des données à caractère personnel.

§ 4. Sur demande dûment motivée, les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine fournissent gratuitement les données énumérées au paragraphe 1^{er}, alinéa 2, aux demandeurs d'accès légitimes, sans retard injustifié et en tout état de cause dans un délai de 72 heures après réception de toute demande d'accès, ou 24 heures après réception de toute demande d'accès en cas d'urgence.

Les demandeurs d'accès légitimes comprennent toute personne physique ou morale qui formule une demande d'examen, de constatation, d'exercice ou de défense de dispositions pénales, civiles ou autres du droit de l'Union ou du droit belge.

TEXTE EN VIGUEUR**PROJET DE LOI**

Sont considérés comme demandeurs d'accès légitimes :

1° toute personne dans le cadre de violations des droits de propriété intellectuelle ou des droits voisins;

2° l'Institut;

3° le CCB;

4° le CSIRT national;

5° les services de police;

6° les autorités judiciaires;

7° les services de renseignement et de sécurité;

8° le SPF Économie;

9° le SPF Finances.

Après avis de l'Institut, le Roi peut ajouter à cette liste des demandeurs d'accès légitimes supplémentaires.

Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine, offrent au demandeur la possibilité d'introduire aisément sa demande.

Il est question d'urgence si l'utilisation d'un nom de domaine peut conduire à des situations de danger de mort et/ou à des dommages irréparables.

Tout refus d'une demande dûment motivée est motivé.

Les politiques et procédures de divulgation de ces données sont rendues publiques.

Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine ne peuvent pas informer le titulaire d'un nom de

TEXTE EN VIGUEUR**PROJET DE LOI**

domaine lorsqu'une demande visée à l'alinéa 1er a été formulée.

§ 5. L'Institut peut donner des instructions contraignantes à un registre de noms de domaine de premier niveau ou à une entité fournissant des services d'enregistrement de noms de domaine, en vue du respect du présent article.

§ 6. Si un registre de noms de domaine de premier niveau ou une entité fournissant des services d'enregistrement de noms de domaine ne respecte pas le présent article, un arrêté royal adopté en vertu du présent article ou une instruction contraignante émise par l'Institut, l'Institut peut imposer les mesures ou amendes administratives visées au chapitre 2 de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

Loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE

Article 71

La FSMA contrôle l'application des dispositions de la présente loi et des arrêtés et règlements pris pour son exécution ainsi que du Règlement 600/2014 et du titre 2 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique. Pour l'exécution des missions précitées concernant la loi du 7 avril 2019, la FSMA peut néanmoins charger un prestataire externe spécialisé de l'exécution de tâches déterminées de contrôle ou obtenir l'assistance d'un tel prestataire.

Article 79

§ 1^{er}. Lorsque la FSMA constate une infraction aux dispositions de la présente loi ou des arrêtés et règlements pris pour son exécution, ou du Règlement 600/2014, elle peut enjoindre à la personne responsable de l'infraction de remédier à la situation constatée dans le délai

Article 71

La FSMA contrôle l'application des dispositions de la présente loi et des arrêtés et règlements pris pour son exécution ainsi que du Règlement 600/2014 [...].

Article 79

§ 1^{er}. Lorsque la FSMA constate une infraction aux dispositions de la présente loi ou des arrêtés et règlements pris pour son exécution, ou du Règlement 600/2014, elle peut enjoindre à la personne responsable de l'infraction de remédier à la situation constatée dans le délai

TEXTE EN VIGUEUR

que la FSMA détermine et, le cas échéant, de s'abstenir de réitérer le comportement constitutif d'une infraction. La FSMA peut également enjoindre à toute personne physique ou morale ayant publié ou diffusé des informations fausses ou trompeuses de publier un communiqué rectificatif.

Sans préjudice des autres mesures prévues par la loi, si la personne à laquelle elle a adressé une injonction en application de l'alinéa 1er reste en défaut à l'expiration du délai qui lui a été imparti, la FSMA peut, la personne ayant pu faire valoir ses moyens:

1° rendre publique sa position quant aux constatations faites en vertu de l'alinéa 1er, en précisant l'identité de la personne responsable de la violation et la nature de celle-ci. Les frais de cette publication sont à charge de la personne concernée;

2° imposer le paiement d'une astreinte qui ne peut être, par jour calendrier de non-respect de l'injonction, supérieure à 50 000 euros, ni, au total, excéder 2 500 000 euros;

Dans les cas urgents, la FSMA peut prendre les mesures visées à l'alinéa 2, 1°, sans injonction préalable en application de l'alinéa 1er, la personne ayant pu faire valoir ses moyens. Dans le cas également où la personne responsable de l'infraction n'est pas clairement identifiable, la FSMA peut, sans injonction préalable, publier un avertissement indiquant, le cas échéant, la nature de l'infraction.

§ 2. Sans préjudice des autres mesures prévues par la loi, lorsque, conformément aux articles 70 à 72 de la loi du 2 août 2002, elle constate une infraction aux dispositions de la présente loi ou dans les arrêtés et règlements pris pour son exécution, ou du Règlement 600/2014, la FSMA peut infliger au contrevenant une amende administrative.

Une amende administrative peut également être imposée à un ou plusieurs membres de l'organe

PROJET DE LOI

que la FSMA détermine et, le cas échéant, de s'abstenir de réitérer le comportement constitutif d'une infraction. La FSMA peut également enjoindre à toute personne physique ou morale ayant publié ou diffusé des informations fausses ou trompeuses de publier un communiqué rectificatif.

Sans préjudice des autres mesures prévues par la loi, si la personne à laquelle elle a adressé une injonction en application de l'alinéa 1er reste en défaut à l'expiration du délai qui lui a été imparti, la FSMA peut, la personne ayant pu faire valoir ses moyens:

1° rendre publique sa position quant aux constatations faites en vertu de l'alinéa 1er, en précisant l'identité de la personne responsable de la violation et la nature de celle-ci. Les frais de cette publication sont à charge de la personne concernée;

2° imposer le paiement d'une astreinte qui ne peut être, par jour calendrier de non-respect de l'injonction, supérieure à 50 000 euros, ni, au total, excéder 2 500 000 euros;

Dans les cas urgents, la FSMA peut prendre les mesures visées à l'alinéa 2, 1°, sans injonction préalable en application de l'alinéa 1er, la personne ayant pu faire valoir ses moyens. Dans le cas également où la personne responsable de l'infraction n'est pas clairement identifiable, la FSMA peut, sans injonction préalable, publier un avertissement indiquant, le cas échéant, la nature de l'infraction.

§ 2. Sans préjudice des autres mesures prévues par la loi, lorsque, conformément aux articles 70 à 72 de la loi du 2 août 2002, elle constate une infraction aux dispositions de la présente loi ou dans les arrêtés et règlements pris pour son exécution, ou du Règlement 600/2014, la FSMA peut infliger au contrevenant une amende administrative.

Une amende administrative peut également être imposée à un ou plusieurs membres de l'organe

TEXTE EN VIGUEUR

d'administration et à toute personne chargée de la direction effective, ainsi que de toute autre personne physique, lorsque celle-ci est reconnue responsable de l'infraction.

§ 3. Le montant des amendes administratives visées au paragraphe 2 est déterminé comme suit:

1° dans le cas d'une personne morale, le montant de l'amende administrative ne peut être supérieur, pour le même fait ou pour le même ensemble de faits, à 5 000 000 euros, ou, si le montant obtenu par application de ce pourcentage est plus élevé, à dix pour cent du chiffre d'affaire annuel total de la personne morale tel qu'il ressort des derniers comptes disponibles établis par l'organe d'administration. Si la personne morale concernée ne réalise pas de chiffre d'affaires, il y a lieu d'entendre par "chiffre d'affaires annuel total" le type de revenus correspondant au chiffre d'affaires, soit conformément aux directives comptables européennes pertinentes, soit, si celles-ci ne sont pas applicables à la personne morale concernée, conformément au droit interne de l'Etat membre dans lequel la personne morale a son siège statutaire. Lorsque la personne morale est une entreprise mère ou une filiale de l'entreprise mère qui est tenue d'établir des comptes financiers consolidés, le chiffre d'affaires annuel total à prendre en considération est le chiffre d'affaires annuel total, tel qu'il ressort des derniers comptes consolidés disponibles approuvés par l'organe d'administration de l'entreprise mère ultime;

2° dans le cas d'une personne physique, le montant de l'amende administrative ne peut être supérieur, pour le même fait ou pour le même ensemble de faits, à 5 000 000 euros.

Nonobstant ce qui précède, lorsque la violation a procuré un profit au contrevenant ou a permis à ce dernier d'éviter une perte, ce maximum peut être porté au double du montant de ce profit ou de cette perte.

PROJET DE LOI

d'administration et à toute personne chargée de la direction effective, ainsi que de toute autre personne physique, lorsque celle-ci est reconnue responsable de l'infraction.

§ 3. Le montant des amendes administratives visées au paragraphe 2 est déterminé comme suit:

1° dans le cas d'une personne morale, le montant de l'amende administrative ne peut être supérieur, pour le même fait ou pour le même ensemble de faits, à 5 000 000 euros, ou, si le montant obtenu par application de ce pourcentage est plus élevé, à dix pour cent du chiffre d'affaire annuel total de la personne morale tel qu'il ressort des derniers comptes disponibles établis par l'organe d'administration. Si la personne morale concernée ne réalise pas de chiffre d'affaires, il y a lieu d'entendre par "chiffre d'affaires annuel total" le type de revenus correspondant au chiffre d'affaires, soit conformément aux directives comptables européennes pertinentes, soit, si celles-ci ne sont pas applicables à la personne morale concernée, conformément au droit interne de l'Etat membre dans lequel la personne morale a son siège statutaire. Lorsque la personne morale est une entreprise mère ou une filiale de l'entreprise mère qui est tenue d'établir des comptes financiers consolidés, le chiffre d'affaires annuel total à prendre en considération est le chiffre d'affaires annuel total, tel qu'il ressort des derniers comptes consolidés disponibles approuvés par l'organe d'administration de l'entreprise mère ultime;

2° dans le cas d'une personne physique, le montant de l'amende administrative ne peut être supérieur, pour le même fait ou pour le même ensemble de faits, à 5 000 000 euros.

Nonobstant ce qui précède, lorsque la violation a procuré un profit au contrevenant ou a permis à ce dernier d'éviter une perte, ce maximum peut être porté au double du montant de ce profit ou de cette perte.

TEXTE EN VIGUEUR

§ 4. En cas de violation des dispositions [...] applicables de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, la FSMA peut infliger les sanctions administratives prévues par l'article 52 de ladite loi.

PROJET DE LOI

COORDINATIE VAN DE ARTIKELEN

BESTAANDE TEKST

ONTWERP VAN WET

Wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle

Artikel 1

Voor de toepassing van deze wet en haar uitvoeringsmaatregelen wordt verstaan onder :

- ioniserende stralingen : stralingen samengesteld uit fotonen of deeltjes welke in staat zijn direct of indirect de vorming van ionen te veroorzaken;

- radioactieve stof : elke stof of elk materiaal die/dat één of meer radionucliden bevat waarvan de activiteit of de concentratie om redenen van stralingsbescherming niet mag worden verwaarloosd;

- bevoegde overheid : (de overheid aangewezen krachtens deze wet en krachtens haar uitvoeringsbesluiten);

- algemeen reglement : - algemeen reglement : het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;

- instelling voor fysische controle: instelling die krachtens artikel 29bis erkend is om opdrachten van de dienst voor fysische controle uit te voeren;

- dienst voor fysische controle : de dienst die krachtens artikel 28 belast is met de fysische controle;

- het Agentschap : de openbare instelling opgericht door deze wet voor de nucleaire controle;

- handeling : menselijke verrichting die een bijkomende blootstelling van bepaalde personen aan ioniserende stralingen met zich mee kan

Artikel 1

Voor de toepassing van deze wet en haar uitvoeringsmaatregelen wordt verstaan onder :

- ioniserende stralingen : stralingen samengesteld uit fotonen of deeltjes welke in staat zijn direct of indirect de vorming van ionen te veroorzaken;

- radioactieve stof : elke stof of elk materiaal die/dat één of meer radionucliden bevat waarvan de activiteit of de concentratie om redenen van stralingsbescherming niet mag worden verwaarloosd;

- bevoegde overheid : (de overheid aangewezen krachtens deze wet en krachtens haar uitvoeringsbesluiten);

- algemeen reglement : - algemeen reglement : het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;

- instelling voor fysische controle: instelling die krachtens artikel 29bis erkend is om opdrachten van de dienst voor fysische controle uit te voeren;

- dienst voor fysische controle : de dienst die krachtens artikel 28 belast is met de fysische controle;

- het Agentschap : de openbare instelling opgericht door deze wet voor de nucleaire controle;

- handeling : menselijke verrichting die een bijkomende blootstelling van bepaalde personen aan ioniserende stralingen met zich mee kan brengen; deze kunnen afkomstig zijn van een

BESTAANDE TEKST

brengen; deze kunnen afkomstig zijn van een kunstmatige of van een natuurlijke stralingsbron, wanneer de natuurlijke radionucliden worden bewerkt omwille van hun radioactieve, splijt- of kweekeigenschappen. Blootstelling bij een noodgeval is hier niet inbegrepen;

- fysische controle : het geheel van maatregelen, uitgevoerd onder de verantwoordelijkheid van de vergunninghouder, met als doel te verifiëren dat de bevolking, de werknemers en het leefmilieu op afdoende wijze worden beschermd tegen het gevaar van ioniserende stralingen en dat de veiligheidsrisico's op afdoende wijze worden beheerst, met uitzondering van :

a) de maatregelen betreffende het gezondheidstoezicht op beroepshalve aan ioniserende straling blootgestelde personen;

b) de maatregelen betreffende het toezicht op de medische blootstelling van personen;

c) de fysieke beveiligingsmaatregelen;

d) de beveiligingsmaatregelen voor radioactieve stoffen;

- gezondheidstoezicht op de werknemers : het toezicht op het geheel van maatregelen ter waarborging van de gezondheid van de werknemers, genomen met toepassing van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk en genomen onder de verantwoordelijkheid van een krachtens deze wet erkende arts;

- vergunninghouder : houder van een vergunning afgeleverd met toepassing van artikel 16 of van een erkenning afgeleverd met toepassing van artikel 4;

- kernmateriaal : de volgende bijzondere splijtbare producten en kerngrondstoffen :

ONTWERP VAN WET

kunstmatige of van een natuurlijke stralingsbron, wanneer de natuurlijke radionucliden worden bewerkt omwille van hun radioactieve, splijt- of kweekeigenschappen. Blootstelling bij een noodgeval is hier niet inbegrepen;

- fysische controle : het geheel van maatregelen, uitgevoerd onder de verantwoordelijkheid van de vergunninghouder, met als doel te verifiëren dat de bevolking, de werknemers en het leefmilieu op afdoende wijze worden beschermd tegen het gevaar van ioniserende stralingen en dat de veiligheidsrisico's op afdoende wijze worden beheerst, met uitzondering van :

a) de maatregelen betreffende het gezondheidstoezicht op beroepshalve aan ioniserende straling blootgestelde personen;

b) de maatregelen betreffende het toezicht op de medische blootstelling van personen;

c) de fysieke beveiligingsmaatregelen;

d) de beveiligingsmaatregelen voor radioactieve stoffen;

- gezondheidstoezicht op de werknemers : het toezicht op het geheel van maatregelen ter waarborging van de gezondheid van de werknemers, genomen met toepassing van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk en genomen onder de verantwoordelijkheid van een krachtens deze wet erkende arts;

- vergunninghouder : houder van een vergunning afgeleverd met toepassing van artikel 16 of van een erkenning afgeleverd met toepassing van artikel 4;

- kernmateriaal : de volgende bijzondere splijtbare producten en kerngrondstoffen :

BESTAANDE TEKST

a) de bijzondere splijtbare producten zijn plutonium 239, uranium 233, uranium verrijkt in uranium 235 of 233 : elk product dat één of meerdere van de hierboven vermelde isotopen bevat.

Uranium verrijkt in uranium 235 of 233 is uranium dat hetzij uranium 235 bevat hetzij uranium 233, dan wel deze beide isotopen in een zodanige hoeveelheid dat de verhouding tussen de som van beide isotopen en de isotoop 238 groter is dan de verhouding tussen de isotoop 235 en de isotoop 238 in natuurlijk uranium;

b) de kerngrondstoffen zijn het uranium dat een mengeling aan isotopen bevat die in de natuur voorkomen en uranium verarmd in uranium 235; thorium; de voornoemde materialen onder de vorm van metaal, legering, de chemische verbindingen of concentraten;

- nationaal nucleair vervoer : het vervoer, met om het even welk vervoermiddel, van kernmateriaal dat geconditioneerd is met het oog op een zending, wanneer dit uitsluitend binnen Belgisch grondgebied plaatsvindt;

- internationaal nucleair vervoer : het vervoer, met om het even welk vervoermiddel, van kernmateriaal, dat geconditioneerd is met het oog op een zending, dat de grenzen van het grondgebied moet overschrijden, te rekenen vanaf het vertrek uit de installatie van de expeditie in de Staat van oorsprong tot de aankomst in een installatie van de geadresseerde op het grondgebied van de Staat van eindbestemming;

- fysieke beveiligingsmaatregelen : alle administratieve, organisatorische en technische maatregelen met als doel het beschermen van kernmateriaal tijdens de productie, het gebruik, de opslag of het vervoer tegen de risico's van ongeoorloofd bezit en diefstal en het beschermen van kernmateriaal tijdens de productie, het gebruik, de opslag alsook de

ONTWERP VAN WET

a) de bijzondere splijtbare producten zijn plutonium 239, uranium 233, uranium verrijkt in uranium 235 of 233 : elk product dat één of meerdere van de hierboven vermelde isotopen bevat.

Uranium verrijkt in uranium 235 of 233 is uranium dat hetzij uranium 235 bevat hetzij uranium 233, dan wel deze beide isotopen in een zodanige hoeveelheid dat de verhouding tussen de som van beide isotopen en de isotoop 238 groter is dan de verhouding tussen de isotoop 235 en de isotoop 238 in natuurlijk uranium;

b) de kerngrondstoffen zijn het uranium dat een mengeling aan isotopen bevat die in de natuur voorkomen en uranium verarmd in uranium 235; thorium; de voornoemde materialen onder de vorm van metaal, legering, de chemische verbindingen of concentraten;

- nationaal nucleair vervoer : het vervoer, met om het even welk vervoermiddel, van kernmateriaal dat geconditioneerd is met het oog op een zending, wanneer dit uitsluitend binnen Belgisch grondgebied plaatsvindt;

- internationaal nucleair vervoer : het vervoer, met om het even welk vervoermiddel, van kernmateriaal, dat geconditioneerd is met het oog op een zending, dat de grenzen van het grondgebied moet overschrijden, te rekenen vanaf het vertrek uit de installatie van de expeditie in de Staat van oorsprong tot de aankomst in een installatie van de geadresseerde op het grondgebied van de Staat van eindbestemming;

- fysieke beveiligingsmaatregelen : alle administratieve, organisatorische en technische maatregelen met als doel het beschermen van kernmateriaal tijdens de productie, het gebruik, de opslag of het vervoer tegen de risico's van ongeoorloofd bezit en diefstal en het beschermen van kernmateriaal tijdens de productie, het gebruik, de opslag alsook de

BESTAANDE TEKST

nucleaire installaties, het nationaal en internationaal nucleair vervoer tegen de risico's van sabotage. De genoemde maatregelen hebben eveneens tot doel de nucleaire documenten te beschermen tegen voornoemde handelingen;

- beveiligingsmaatregelen voor radioactieve stoffen: alle administratieve, organisatorische en technische maatregelen, met als doel:

a) om de radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik, de opslag of het vervoer tegen de risico's van ongeoorloofd bezit en diefstal te beschermen;

b) om wat volgt tegen de risico's van sabotage of elk kwaadwillig gebruik te beschermen:

1) de radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik of de opslag ervan;

2) de inrichtingen waar deze stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt, alsook hun vervoer;

- beveiligingsmaatregelen voor toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is: alle administratieve, organisatorische en technische maatregelen met als doel:

a) om voormelde toestellen of installaties tegen de risico's van ongeoorloofd bezit en diefstal te beschermen;

b) om wat volgt tegen de risico's van sabotage of elk kwaadwillig gebruik te beschermen:

1) voornoemde toestellen of installaties, alsook het vervoer van deze toestellen of installaties;

2) de inrichtingen waar deze toestellen of installaties zich bevinden.

ONTWERP VAN WET

nucleaire installaties, het nationaal en internationaal nucleair vervoer tegen de risico's van sabotage. De genoemde maatregelen hebben eveneens tot doel de nucleaire documenten te beschermen tegen voornoemde handelingen;

- beveiligingsmaatregelen voor radioactieve stoffen: alle administratieve, organisatorische en technische maatregelen, met als doel:

a) om de radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik, de opslag of het vervoer tegen de risico's van ongeoorloofd bezit en diefstal te beschermen;

b) om wat volgt tegen de risico's van sabotage of elk kwaadwillig gebruik te beschermen:

1) de radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik of de opslag ervan;

2) de inrichtingen waar deze stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt, alsook hun vervoer;

- beveiligingsmaatregelen voor toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is: alle administratieve, organisatorische en technische maatregelen met als doel:

a) om voormelde toestellen of installaties tegen de risico's van ongeoorloofd bezit en diefstal te beschermen;

b) om wat volgt tegen de risico's van sabotage of elk kwaadwillig gebruik te beschermen:

1) voornoemde toestellen of installaties, alsook het vervoer van deze toestellen of installaties;

2) de inrichtingen waar deze toestellen of installaties zich bevinden.

BESTAANDE TEKST

- sabotage : alle opzettelijke handelingen:

a) die zijn gericht tegen:

1) kernmateriaal tijdens de productie, het gebruik, de opslag of het vervoer ervan;

2) nucleaire installaties;

3) het nationaal of internationaal nucleair vervoer;

4) radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik, de opslag of het vervoer ervan;

5) inrichtingen of delen van inrichtingen waar radioactieve stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt;

6) toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is;

7) het vervoer van toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is;

8) inrichtingen, delen van inrichtingen en plaatsen waar zich toestellen of installaties bevinden die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is;

en

b) die op rechtstreekse of onrechtstreekse wijze de gezondheid en veiligheid van het personeel, de bevolking en het milieu in gevaar kunnen brengen door een blootstelling aan straling, of de uitstoot van radioactieve stoffen;

- [...]

- vermogensreactor een kernreactor, ontworpen voor de productie van elektriciteit, die vergund is of werd als inrichting van klasse I met toepassing van de regelgeving inzake de

ONTWERP VAN WET

- sabotage : alle opzettelijke handelingen:

a) die zijn gericht tegen:

1) kernmateriaal tijdens de productie, het gebruik, de opslag of het vervoer ervan;

2) nucleaire installaties;

3) het nationaal of internationaal nucleair vervoer;

4) radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik, de opslag of het vervoer ervan;

5) inrichtingen of delen van inrichtingen waar radioactieve stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt;

6) toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is;

7) het vervoer van toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is;

8) inrichtingen, delen van inrichtingen en plaatsen waar zich toestellen of installaties bevinden die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is;

en

b) die op rechtstreekse of onrechtstreekse wijze de gezondheid en veiligheid van het personeel, de bevolking en het milieu in gevaar kunnen brengen door een blootstelling aan straling, of de uitstoot van radioactieve stoffen;

- [...]

- vermogensreactor een kernreactor, ontworpen voor de productie van elektriciteit, die vergund is of werd als inrichting van klasse I met toepassing van de regelgeving inzake de

BESTAANDE TEKST

bescherming tegen ioniserende stralingen en waarvoor nog geen ontmantelingsvergunning werd afgeleverd.

- beroepshalve blootgestelde persoon : iedere natuurlijke persoon die ingevolge zijn beroepsactiviteiten, een blootstelling aan ioniserende stralingen ondergaat die kan leiden tot de overschrijding van één van de dosislimieten vastgesteld voor de personen van het publiek;

- aan dosimetrisch toezicht onderworpen persoon : iedere natuurlijke persoon die activiteiten van ongeacht welke aard uitvoert waarbij hij/zij een blootstelling aan ioniserende stralingen ondergaat die kan leiden tot de overschrijding van één van de dosislimieten vastgesteld voor de personen van het publiek;

- exploitant : elke natuurlijke of rechtspersoon die verantwoordelijk is voor de inrichting onderhevig aan de vergunnings- of aangifteplicht overeenkomstig de bepalingen die voortvloeien uit artikel 17;

- externe onderneming : elke natuurlijke of rechtspersoon, die activiteiten van om het even welke aard verricht in een inrichting onderhevig aan de vergunnings- of aangifteplicht overeenkomstig de bepalingen die voortvloeien uit artikel 17, waarbij één van de dosislimieten vastgesteld voor de personen van het publiek zou kunnen overschreden worden, met uitzondering van de exploitant van die inrichting, en zijn personeelsleden;

- erkende geneesheer : de preventieadviseur-arbeidsarts werkzaam in een interne of externe dienst voor preventie en bescherming op het werk, deskundig op gebied van arbeidsgeneeskunde overeenkomstig de bepalingen van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk, en de uitvoeringsbesluiten ervan en die bovendien

ONTWERP VAN WET

bescherming tegen ioniserende stralingen en waarvoor nog geen ontmantelingsvergunning werd afgeleverd.

- beroepshalve blootgestelde persoon : iedere natuurlijke persoon die ingevolge zijn beroepsactiviteiten, een blootstelling aan ioniserende stralingen ondergaat die kan leiden tot de overschrijding van één van de dosislimieten vastgesteld voor de personen van het publiek;

- aan dosimetrisch toezicht onderworpen persoon : iedere natuurlijke persoon die activiteiten van ongeacht welke aard uitvoert waarbij hij/zij een blootstelling aan ioniserende stralingen ondergaat die kan leiden tot de overschrijding van één van de dosislimieten vastgesteld voor de personen van het publiek;

- exploitant : elke natuurlijke of rechtspersoon die verantwoordelijk is voor de inrichting onderhevig aan de vergunnings- of aangifteplicht overeenkomstig de bepalingen die voortvloeien uit artikel 17;

- externe onderneming : elke natuurlijke of rechtspersoon, die activiteiten van om het even welke aard verricht in een inrichting onderhevig aan de vergunnings- of aangifteplicht overeenkomstig de bepalingen die voortvloeien uit artikel 17, waarbij één van de dosislimieten vastgesteld voor de personen van het publiek zou kunnen overschreden worden, met uitzondering van de exploitant van die inrichting, en zijn personeelsleden;

- erkende geneesheer : de preventieadviseur-arbeidsarts werkzaam in een interne of externe dienst voor preventie en bescherming op het werk, deskundig op gebied van arbeidsgeneeskunde overeenkomstig de bepalingen van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk, en de uitvoeringsbesluiten ervan en die bovendien erkend is overeenkomstig de

BESTAANDE TEKST

erkend is overeenkomstig de uitvoeringsmaatregelen genomen op grond van de artikelen 3 en 19;

- externe werker : iedere aan dosimetrisch toezicht onderworpen persoon, die een opdracht met blootstellingsrisico uitvoert bij een exploitant, ongeacht of hij dit doet als tijdelijk of vast werknemer van een externe onderneming, of als zelfstandige;

- opdracht met blootstellingsrisico : de activiteit van ongeacht welke aard, van een externe werker bij een exploitant, waarbij één van de dosislimieten vastgesteld voor de personen van het publiek zou kunnen overschreden worden;

- blootstellingsregister : het gecentraliseerd registratiesysteem bedoeld in artikel 25/2, dat de dosimetriegegevens van aan dosimetrisch toezicht onderworpen personen bevat;

- stralingspaspoort : het individueel document opgesteld voor externe werkers, dat toelaat om hun dosimetrisch toezicht te verzekeren tijdens de opdrachten met blootstellingsrisico uitgevoerd in het buitenland;

- beroepsbeoefenaar in de gezondheidszorg : de verwerkingsverantwoordelijke die de gezondheidsgegevens zoals bedoeld in de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens beheert, aangesteld binnen het Agentschap;

- consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer : de consulent bedoeld in artikel 4, § 5, van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid, zoals aangewezen binnen het Agentschap;

- verantwoordelijke voor de verwerking : de persoon bedoeld in de wet van 30 juli 2018 betreffende de bescherming van de natuurlijke

ONTWERP VAN WET

uitvoeringsmaatregelen genomen op grond van de artikelen 3 en 19;

- externe werker : iedere aan dosimetrisch toezicht onderworpen persoon, die een opdracht met blootstellingsrisico uitvoert bij een exploitant, ongeacht of hij dit doet als tijdelijk of vast werknemer van een externe onderneming, of als zelfstandige;

- opdracht met blootstellingsrisico : de activiteit van ongeacht welke aard, van een externe werker bij een exploitant, waarbij één van de dosislimieten vastgesteld voor de personen van het publiek zou kunnen overschreden worden;

- blootstellingsregister : het gecentraliseerd registratiesysteem bedoeld in artikel 25/2, dat de dosimetriegegevens van aan dosimetrisch toezicht onderworpen personen bevat;

- stralingspaspoort : het individueel document opgesteld voor externe werkers, dat toelaat om hun dosimetrisch toezicht te verzekeren tijdens de opdrachten met blootstellingsrisico uitgevoerd in het buitenland;

- beroepsbeoefenaar in de gezondheidszorg : de verwerkingsverantwoordelijke die de gezondheidsgegevens zoals bedoeld in de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens beheert, aangesteld binnen het Agentschap;

- consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer : de consulent bedoeld in artikel 4, § 5, van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid, zoals aangewezen binnen het Agentschap;

- verantwoordelijke voor de verwerking : de persoon bedoeld in de wet van 30 juli 2018 betreffende de bescherming van de natuurlijke

BESTAANDE TEKST

personen met betrekking tot de verwerking van persoonsgegevens beheert, in casu het Agentschap;

- vestigingseenheid : een plaats die men geografisch gezien kan identificeren door een adres, waar ten minste een activiteit van de onderneming wordt uitgeoefend of waaruit de activiteit wordt uitgeoefend;

- werknemer : de werknemer bedoeld in artikel 2, § 1, eerste en tweede lid, 1°, van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk;

- werkgever : de werkgever bedoeld in artikel 2, § 1, eerste en tweede lid, 2°, van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk;

- dosimetrisch toezicht : het dosimetrisch toezicht zoals bedoeld in artikel 30.6 van het Algemeen reglement;

- authentieke bronnen : het Rijksregister opgericht bij de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, de Kruispuntbank der ondernemingen opgericht bij wet van 16 januari 2003 tot oprichting van een Kruispuntbank van Ondernemingen, tot modernisering van het handelsregister, tot oprichting van erkende ondernemingsloketten en houdende diverse bepalingen, en de Registers van de Kruispuntbank van de Sociale Zekerheid (Bis-register en Register van de geschrapten) opgericht bij wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid;

- anonieme gegevens : de gegevens die niet met een geïdentificeerd of identificeerbaar persoon in verband kunnen worden gebracht en derhalve geen persoonsgegevens zijn;

ONTWERP VAN WET

personen met betrekking tot de verwerking van persoonsgegevens beheert, in casu het Agentschap;

- vestigingseenheid : een plaats die men geografisch gezien kan identificeren door een adres, waar ten minste een activiteit van de onderneming wordt uitgeoefend of waaruit de activiteit wordt uitgeoefend;

- werknemer : de werknemer bedoeld in artikel 2, § 1, eerste en tweede lid, 1°, van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk;

- werkgever : de werkgever bedoeld in artikel 2, § 1, eerste en tweede lid, 2°, van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk;

- dosimetrisch toezicht : het dosimetrisch toezicht zoals bedoeld in artikel 30.6 van het Algemeen reglement;

- authentieke bronnen : het Rijksregister opgericht bij de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, de Kruispuntbank der ondernemingen opgericht bij wet van 16 januari 2003 tot oprichting van een Kruispuntbank van Ondernemingen, tot modernisering van het handelsregister, tot oprichting van erkende ondernemingsloketten en houdende diverse bepalingen, en de Registers van de Kruispuntbank van de Sociale Zekerheid (Bis-register en Register van de geschrapten) opgericht bij wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid;

- anonieme gegevens : de gegevens die niet met een geïdentificeerd of identificeerbaar persoon in verband kunnen worden gebracht en derhalve geen persoonsgegevens zijn;

BESTAANDE TEKST

- "de wet van 7 april 2019": de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

- 'functionaris voor gegevensbescherming' : de door het Agentschap aangewezen functionaris met toepassing van artikel 37,1, a) van verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van gegevensbescherming en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG;

- wet van 23 maart 2020: wet van 23 maart 2020 tot wazigmaking van de beelden van nucleaire installaties en kritieke inrichtingen, en tot inperking van het maken of verspreiden van luchtfoto's van die installaties en inrichtingen, in het belang van de openbare veiligheid.

Artikel 15ter

Het Agentschap wordt aangewezen als inspectiedienst, in de zin van artikel 42 van de wet van 7 april 2019, en is belast met het controleren van de toepassing van de bepalingen van deze wet en de uitvoeringsbesluiten ervan door de aanbieders van essentiële diensten, die krachtens bovengenoemde wet geïdentificeerd zijn, wat betreft de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit.

De Koning bepaalt de praktische inspectiemodaliteiten, na advies van het Agentschap.

Wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België

Artikel 36/1**ONTWERP VAN WET**

- **de NIS2-wet: de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;**

- 'functionaris voor gegevensbescherming' : de door het Agentschap aangewezen functionaris met toepassing van artikel 37,1, a) van verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van gegevensbescherming en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG;

- wet van 23 maart 2020: wet van 23 maart 2020 tot wazigmaking van de beelden van nucleaire installaties en kritieke inrichtingen, en tot inperking van het maken of verspreiden van luchtfoto's van die installaties en inrichtingen, in het belang van de openbare veiligheid.

Artikel 15ter

Het Agentschap wordt aangewezen als sectorale inspectiedienst in de zin van de NIS2-wet voor de sector energie, wat betreft de bijkomende maatregelen voor het beheer van cyberbeveiligingsrisico's die van toepassing zijn op de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit.

De Koning bepaalt de praktische inspectiemodaliteiten, na advies van het Agentschap.

Artikel 36/1

BESTAANDE TEKST

Definities: voor de toepassing van dit hoofdstuk en hoofdstuk IV/2 wordt verstaan onder:

1° "de wet van 2 augustus 2002 " : de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten;

2° "financieel instrument " : een instrument als gedefinieerd in artikel 2, 1° van de wet van 2 augustus 2002;

3° "kredietinstelling " : een instelling als bedoeld in Boek II en in de Titels I en II van Boek III van de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen;

4° "instelling voor elektronisch geld" : een instelling als bedoeld in artikel 2, 74° van de wet van 11 maart 2018 op het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen;

5° "beleggingsonderneming met het statuut van beursvennootschap " : een beleggingsonderneming als bedoeld in de wet van 20 juli 2022 op het statuut van en het toezicht op beursvennootschappen en houdende diverse bepalingen, die een vergunning heeft als beursvennootschap of beleggingsdiensten mag verlenen die, indien zij door een Belgische beleggingsonderneming zouden worden verleend, een vergunning als beursvennootschap zouden vereisen;

6° "verzekeringsonderneming of herverzekeringsonderneming": een onderneming als bedoeld in artikel 5, eerste lid, 1°, of 2°, van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen;

7° [...]

8° "maatschappij voor onderlinge borgstelling " : een maatschappij als bedoeld in artikel 57 van de programmawet van 10 februari 1998 tot

ONTWERP VAN WET

Definities: voor de toepassing van dit hoofdstuk en hoofdstuk IV/2 wordt verstaan onder:

1° "de wet van 2 augustus 2002 " : de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten;

2° "financieel instrument " : een instrument als gedefinieerd in artikel 2, 1° van de wet van 2 augustus 2002;

3° "kredietinstelling " : een instelling als bedoeld in Boek II en in de Titels I en II van Boek III van de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen;

4° "instelling voor elektronisch geld" : een instelling als bedoeld in artikel 2, 74° van de wet van 11 maart 2018 op het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen;

5° "beleggingsonderneming met het statuut van beursvennootschap " : een beleggingsonderneming als bedoeld in de wet van 20 juli 2022 op het statuut van en het toezicht op beursvennootschappen en houdende diverse bepalingen, die een vergunning heeft als beursvennootschap of beleggingsdiensten mag verlenen die, indien zij door een Belgische beleggingsonderneming zouden worden verleend, een vergunning als beursvennootschap zouden vereisen;

6° "verzekeringsonderneming of herverzekeringsonderneming": een onderneming als bedoeld in artikel 5, eerste lid, 1°, of 2°, van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen;

7° [...]

8° "maatschappij voor onderlinge borgstelling " : een maatschappij als bedoeld in artikel 57 van de programmawet van 10 februari 1998 tot

BESTAANDE TEKST

bevordering van het zelfstandig ondernemerschap;

9° "betalingsinstelling" : een instelling als bedoeld in artikel 2, 8° van de wet van 11 maart 2018 op het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen;

10° " gereguleerde markt " : een Belgische of buitenlandse gereguleerde markt;

11° " Belgische gereguleerde markt " : een door een marktonderneming geëxploiteerd en/of beheerd multilateraal systeem dat verschillende koop- en verkoopintenties van derden met betrekking tot financiële instrumenten - binnen dit systeem en volgens de niet-discretionaire regels van dit systeem - samenbrengt of het samenbrengen daarvan vergemakkelijkt op zodanige wijze dat er een overeenkomst uit voortvloeit met betrekking tot financiële instrumenten die volgens de regels en/of de systemen van de markt tot de handel zijn toegelaten, en waaraan vergunning is verleend en die regelmatig werkt, overeenkomstig het bepaalde in hoofdstuk II van de wet van 2 augustus 2002;

12° "buitenlandse gereguleerde markt " : een markt voor financiële instrumenten die is georganiseerd door een marktonderneming waarvan de Staat van herkomst een andere lidstaat van de Europese Economische Ruimte is dan België, en waaraan in deze lidstaat een vergunning als gereguleerde markt met toepassing van titel III van Richtlijn 2014/65/EU is verleend;

13° "centrale tegenpartij" : een centrale tegenpartij als gedefinieerd in artikel 2, punt 1), van Verordening (EU) Nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters;

ONTWERP VAN WET

bevordering van het zelfstandig ondernemerschap;

9° "betalingsinstelling" : een instelling als bedoeld in artikel 2, 8° van de wet van 11 maart 2018 op het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen;

10° " gereguleerde markt " : een Belgische of buitenlandse gereguleerde markt;

11° " Belgische gereguleerde markt " : een door een marktonderneming geëxploiteerd en/of beheerd multilateraal systeem dat verschillende koop- en verkoopintenties van derden met betrekking tot financiële instrumenten - binnen dit systeem en volgens de niet-discretionaire regels van dit systeem - samenbrengt of het samenbrengen daarvan vergemakkelijkt op zodanige wijze dat er een overeenkomst uit voortvloeit met betrekking tot financiële instrumenten die volgens de regels en/of de systemen van de markt tot de handel zijn toegelaten, en waaraan vergunning is verleend en die regelmatig werkt, overeenkomstig het bepaalde in hoofdstuk II van de wet van 2 augustus 2002;

12° "buitenlandse gereguleerde markt " : een markt voor financiële instrumenten die is georganiseerd door een marktonderneming waarvan de Staat van herkomst een andere lidstaat van de Europese Economische Ruimte is dan België, en waaraan in deze lidstaat een vergunning als gereguleerde markt met toepassing van titel III van Richtlijn 2014/65/EU is verleend;

13° "centrale tegenpartij" : een centrale tegenpartij als gedefinieerd in artikel 2, punt 1), van Verordening (EU) Nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters;

BESTAANDE TEKST

14° [...]

15° " FSMA ": de Autoriteit voor Financiële Diensten en Markten, in het Duits " Kommission für das Bank-, Finanz- und Versicherungswesen ";

16° "bevoegde autoriteit" : de Bank, de FSMA of de autoriteit die door elke lidstaat wordt aangewezen met toepassing van artikel 67 van Richtlijn 2014/65/EU, artikel 22 van Verordening 648/2012, artikel 11 van Verordening 909/2014 of artikel 2, 21), en artikel 12 van Verordening 2022/858, tenzij anders is bepaald in de Richtlijn en de respectieve verordeningen;

17° "Richtlijn 2014/65/EU" : Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU;

18° " CSRSFI " : het Comité voor systeemrisico's en systeemrelevante financiële instellingen.

19° " instelling voor bedrijfspensioenvoorziening " : een instelling als bedoeld in artikel 2, 1° van de wet van 27 oktober 2006 betreffende het toezicht op de instellingen voor bedrijfspensioenvoorziening.

20° "Europese Bankautoriteit" : de Europese Bankautoriteit opgericht bij Verordening nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie;

21° "Europese Autoriteit voor verzekeringen en bedrijfspensioenen" : de Europese Autoriteit voor verzekeringen en bedrijfspensioenen opgericht bij Verordening nr. 1094/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen), tot wijziging van Besluit nr.

ONTWERP VAN WET

14° [...]

15° " FSMA ": de Autoriteit voor Financiële Diensten en Markten, in het Duits " Kommission für das Bank-, Finanz- und Versicherungswesen ";

16° "bevoegde autoriteit" : de Bank, de FSMA of de autoriteit die door elke lidstaat wordt aangewezen met toepassing van artikel 67 van Richtlijn 2014/65/EU, artikel 22 van Verordening 648/2012, artikel 11 van Verordening 909/2014 of artikel 2, 21), en artikel 12 van Verordening 2022/858, tenzij anders is bepaald in de Richtlijn en de respectieve verordeningen;

17° "Richtlijn 2014/65/EU" : Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU;

18° " CSRSFI " : het Comité voor systeemrisico's en systeemrelevante financiële instellingen.

19° " instelling voor bedrijfspensioenvoorziening " : een instelling als bedoeld in artikel 2, 1° van de wet van 27 oktober 2006 betreffende het toezicht op de instellingen voor bedrijfspensioenvoorziening.

20° "Europese Bankautoriteit" : de Europese Bankautoriteit opgericht bij Verordening nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie;

21° "Europese Autoriteit voor verzekeringen en bedrijfspensioenen" : de Europese Autoriteit voor verzekeringen en bedrijfspensioenen opgericht bij Verordening nr. 1094/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen), tot wijziging van Besluit nr.

BESTAANDE TEKST

716/2009/EG en tot intrekking van Besluit 2009/79/EG van de Commissie;

21°/1 "Europese Autoriteit voor effecten en markten" : de Europese Autoriteit voor effecten en markten opgericht bij Verordening 1095/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/77/EG van de Commissie;

22° "Verordening 648/2012" : Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters;

23° "financiële tegenpartij" : een tegenpartij als gedefinieerd in artikel 2, punt 8), van Verordening 648/2012 of in artikel 3, punt 3), van Verordening 2015/2365;

24° "niet-financiële tegenpartij" : een tegenpartij als gedefinieerd in artikel 2, punt 9), van Verordening 648/2012 of in artikel 3, punt 4), van Verordening 2015/2365;

25° "centrale effectenbewaarinstantie" : een centrale effectenbewaarinstantie als omschreven in artikel 2, lid 1, punt 1), van Verordening 909/2014;

26° "Verordening 909/2014" : Verordening (EU) nr. 909/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de verbetering van de effectenafwikkeling in de Europese Unie, betreffende centrale effectenbewaarinstanties en tot wijziging van Richtlijnen 98/26/EG en 2014/65/EU en Verordening (EU) nr. 236/2012;

27° "Verordening 2015/2365" : Verordening (EU) 2015/2365 van het Europees Parlement en de Raad van 25 november 2015 betreffende de transparantie van effectenfinancieringstransacties en van hergebruik en tot wijziging van Verordening (EU) nr. 648/2012.

ONTWERP VAN WET

716/2009/EG en tot intrekking van Besluit 2009/79/EG van de Commissie;

21°/1 "Europese Autoriteit voor effecten en markten" : de Europese Autoriteit voor effecten en markten opgericht bij Verordening 1095/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/77/EG van de Commissie;

22° "Verordening 648/2012" : Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters;

23° "financiële tegenpartij" : een tegenpartij als gedefinieerd in artikel 2, punt 8), van Verordening 648/2012 of in artikel 3, punt 3), van Verordening 2015/2365;

24° "niet-financiële tegenpartij" : een tegenpartij als gedefinieerd in artikel 2, punt 9), van Verordening 648/2012 of in artikel 3, punt 4), van Verordening 2015/2365;

25° "centrale effectenbewaarinstantie" : een centrale effectenbewaarinstantie als omschreven in artikel 2, lid 1, punt 1), van Verordening 909/2014;

26° "Verordening 909/2014" : Verordening (EU) nr. 909/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de verbetering van de effectenafwikkeling in de Europese Unie, betreffende centrale effectenbewaarinstanties en tot wijziging van Richtlijnen 98/26/EG en 2014/65/EU en Verordening (EU) nr. 236/2012;

27° "Verordening 2015/2365" : Verordening (EU) 2015/2365 van het Europees Parlement en de Raad van 25 november 2015 betreffende de transparantie van effectenfinancieringstransacties en van hergebruik en tot wijziging van Verordening (EU) nr. 648/2012.

BESTAANDE TEKST

28° "de wet van 7 april 2019": de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

29° "insolventierechtbank": de insolventierechtbank als bedoeld in artikel I.22, 4°, van het Wetboek van economisch recht;

30° "wet van 18 september 2017": de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;

31° "Verordening GTM": Verordening (EU) nr. 1024/2013 van de Raad van 15 oktober 2013 waarbij aan de Europese Centrale Bank specifieke taken worden opgedragen betreffende het beleid inzake het prudentieel toezicht op kredietinstellingen;

32° "richtlijn 2015/849": richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van richtlijn 2005/60/EG van het Europees Parlement en de Raad en richtlijn 2006/70/EG van de Commissie;

33° "Verordening 2021/23": Verordening (EU) 2021/23 van het Europees Parlement en de Raad van 16 december 2020 betreffende een kader voor het herstel en de afwikkeling van centrale tegenpartijen en tot wijziging van de Verordeningen (EU) nr. 1095/2010, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 806/2014 en (EU) 2015/2365, en de Richtlijnen 2002/47/EG, 2004/25/EG, 2007/36/EG, 2014/59/EU en (EU) 2017/1132;

34° "Verordening 2022/858": Verordening (EU) 2022/858 van het Europees Parlement en de Raad van 30 mei 2022 betreffende een proefregeling voor marktinfrastucturen op basis

ONTWERP VAN WET

28° "de NIS2-wet": de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

29° "insolventierechtbank": de insolventierechtbank als bedoeld in artikel I.22, 4°, van het Wetboek van economisch recht;

30° "wet van 18 september 2017": de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;

31° "Verordening GTM": Verordening (EU) nr. 1024/2013 van de Raad van 15 oktober 2013 waarbij aan de Europese Centrale Bank specifieke taken worden opgedragen betreffende het beleid inzake het prudentieel toezicht op kredietinstellingen;

32° "richtlijn 2015/849": richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van richtlijn 2005/60/EG van het Europees Parlement en de Raad en richtlijn 2006/70/EG van de Commissie;

33° "Verordening 2021/23": Verordening (EU) 2021/23 van het Europees Parlement en de Raad van 16 december 2020 betreffende een kader voor het herstel en de afwikkeling van centrale tegenpartijen en tot wijziging van de Verordeningen (EU) nr. 1095/2010, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 806/2014 en (EU) 2015/2365, en de Richtlijnen 2002/47/EG, 2004/25/EG, 2007/36/EG, 2014/59/EU en (EU) 2017/1132;

34° "Verordening 2022/858": Verordening (EU) 2022/858 van het Europees Parlement en de Raad van 30 mei 2022 betreffende een proefregeling voor marktinfrastucturen op basis

BESTAANDE TEKST

van distributed ledger-technologie en tot wijziging van Verordeningen (EU) nr. 600/2014 en (EU) nr. 909/2014 en Richtlijn 2014/65/EU;

35° "entiteit die een DLT-afwikkelingssysteem of een DLT-handels- en afwikkelingssysteem exploiteert": een centrale effectenbewaarinstelling of een beleggingsonderneming of marktexploitant die een DLT-afwikkelingssysteem of een DLT-handels- en afwikkelingssysteem exploiteert als bedoeld in artikel 97, 13° en 14°, van de wet van ... houdende diverse financiële bepalingen.

Artikel 36/14

§ 1. In afwijking van artikel 35 mag de Bank tevens vertrouwelijke informatie meedelen die zij ontvangen heeft in het kader van de uitvoering van haar in artikel 36/2, § 1 bedoelde opdrachten:

1° aan de Europese Centrale Bank en aan de andere centrale banken en instellingen met een soortgelijke taak in hun hoedanigheid van monetaire autoriteit als deze gegevens van belang zijn voor de uitoefening van hun respectieve wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en afwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel, alsook aan andere overheidsinstanties die belast zijn met het toezicht op de betalingssystemen.

Wanneer zich een noodsituatie voordoet, waaronder ongunstige ontwikkelingen op de financiële markten, die de liquiditeit van de markt en de stabiliteit van het financiële stelsel kan ondermijnen in een van de lidstaten waar aan entiteiten van een groep met kredietinstellingen of beleggingsondernemingen vergunning is verleend of significante bijkantoren zijn gevestigd in de zin van artikel 3, 65° van de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen, kan de Bank gegevens verzenden aan centrale

ONTWERP VAN WET

van distributed ledger-technologie en tot wijziging van Verordeningen (EU) nr. 600/2014 en (EU) nr. 909/2014 en Richtlijn 2014/65/EU;

35° "entiteit die een DLT-afwikkelingssysteem of een DLT-handels- en afwikkelingssysteem exploiteert": een centrale effectenbewaarinstelling of een beleggingsonderneming of marktexploitant die een DLT-afwikkelingssysteem of een DLT-handels- en afwikkelingssysteem exploiteert als bedoeld in artikel 97, 13° en 14°, van de wet van ... houdende diverse financiële bepalingen.

Artikel 36/14

§ 1. In afwijking van artikel 35 mag de Bank tevens vertrouwelijke informatie meedelen die zij ontvangen heeft in het kader van de uitvoering van haar in artikel 36/2, § 1 bedoelde opdrachten:

1° aan de Europese Centrale Bank en aan de andere centrale banken en instellingen met een soortgelijke taak in hun hoedanigheid van monetaire autoriteit als deze gegevens van belang zijn voor de uitoefening van hun respectieve wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en afwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel, alsook aan andere overheidsinstanties die belast zijn met het toezicht op de betalingssystemen.

Wanneer zich een noodsituatie voordoet, waaronder ongunstige ontwikkelingen op de financiële markten, die de liquiditeit van de markt en de stabiliteit van het financiële stelsel kan ondermijnen in een van de lidstaten waar aan entiteiten van een groep met kredietinstellingen of beleggingsondernemingen vergunning is verleend of significante bijkantoren zijn gevestigd in de zin van artikel 3, 65° van de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen, kan de Bank gegevens verzenden aan centrale

BESTAANDE TEKST

banken van het Europees stelsel van centrale banken als deze gegevens van belang zijn voor de uitoefening van hun wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samen-hangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en effectenafwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel.

In een noodsituatie zoals hierboven bedoeld, kan de Bank gegevens meedelen die van belang zijn voor de centrale overheidsdiensten in alle betrokken lidstaten die bevoegd zijn voor de wetgeving inzake toezicht op de kredietinstellingen, financiële instellingen, beleggingsdiensten en verzekeringmaatschappijen;

2° binnen de grenzen van het recht van de Europese Unie, aan de bevoegde autoriteiten van de Europese Unie en van andere Lidstaten van de Europese Economische Ruimte die één of meerdere bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in de artikelen 36/2 en 36/3, met inbegrip van de Europese Centrale Bank voor wat betreft de taken die haar zijn opgedragen bij de GTM-verordening;

2° /1 binnen de grenzen van het recht van de Europese Unie, aan de bevoegde autoriteiten van andere lidstaten van de Europese Economische Ruimte die één of meerdere toezichtsbevoegdheden uitoefenen ten aanzien van de onderworpen entiteiten die worden opgesomd in artikel 2, lid 1, punten 1) en 2) van richtlijn (EU) 2015/849, met het oog op de naleving van die richtlijn en in het kader van de uitvoering van de opdracht die hen is opgedragen bij die richtlijn;

3° met inachtneming van het recht van de Europese Unie, aan de bevoegde autoriteiten van derde Staten die één of meerdere bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in de artikelen 36/2 en 36/3, met inbegrip van de autoriteiten die soortgelijke

ONTWERP VAN WET

banken van het Europees stelsel van centrale banken als deze gegevens van belang zijn voor de uitoefening van hun wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samen-hangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en effectenafwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel.

In een noodsituatie zoals hierboven bedoeld, kan de Bank gegevens meedelen die van belang zijn voor de centrale overheidsdiensten in alle betrokken lidstaten die bevoegd zijn voor de wetgeving inzake toezicht op de kredietinstellingen, financiële instellingen, beleggingsdiensten en verzekeringmaatschappijen;

2° binnen de grenzen van het recht van de Europese Unie, aan de bevoegde autoriteiten van de Europese Unie en van andere Lidstaten van de Europese Economische Ruimte die één of meerdere bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in de artikelen 36/2 en 36/3, met inbegrip van de Europese Centrale Bank voor wat betreft de taken die haar zijn opgedragen bij de GTM-verordening;

2° /1 binnen de grenzen van het recht van de Europese Unie, aan de bevoegde autoriteiten van andere lidstaten van de Europese Economische Ruimte die één of meerdere toezichtsbevoegdheden uitoefenen ten aanzien van de onderworpen entiteiten die worden opgesomd in artikel 2, lid 1, punten 1) en 2) van richtlijn (EU) 2015/849, met het oog op de naleving van die richtlijn en in het kader van de uitvoering van de opdracht die hen is opgedragen bij die richtlijn;

3° met inachtneming van het recht van de Europese Unie, aan de bevoegde autoriteiten van derde Staten die één of meerdere bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in de artikelen 36/2 en 36/3, met inbegrip van de autoriteiten die soortgelijke

BESTAANDE TEKST

bevoegdheden hebben als de in de bepaling onder 2° /1 bedoelde autoriteiten, en waarmee de Bank een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten;

4° aan de FSMA;

5° aan de Belgische instellingen of aan instellingen van een andere Lidstaat van de Europese Economische Ruimte die een beschermingsregeling voor deposito's, beleggers of levensverzekeringen beheren en aan het orgaan dat bevoegd is voor de financieringsregelingen voor de afwikkeling;

6° aan de centrale tegenpartijen de instellingen voor vereffening van financiële instrumenten of de centrale effectenbewaarinstellingen die gemachtigd zijn om verrekenings- of vereffeningdiensten te verstrekken voor transacties in financiële instrumenten verricht op een Belgische gereguleerde markt, als de Bank van oordeel is dat de mededeling van de betrokken informatie noodzakelijk is om de regelmatige werking van die centrale tegenpartijen, instellingen voor vereffening en centrale effectenbewaarinstellingen te vrijwaren voor tekortkomingen, zelfs potentiële, van marktdeelnemers op de betrokken markt;

7° binnen de grenzen van het recht van de Europese Unie, aan de marktondernemingen voor de goede werking van, de controle van en het toezicht op de markten die deze inrichten;

8° tijdens burgerrechtelijke of handelsrechtelijke procedures, aan de autoriteiten en gerechtelijke mandatarissen die betrokken zijn bij procedures van faillissement of gerechtelijke reorganisatie of bij analoge collectieve procedures betreffende instellingen die onder het toezicht van de Bank staan, met uitzondering van de vertrouwelijke informatie over het aandeel van derden in reddingspogingen vóór de betrokken procedures werden ingesteld;

9° aan de commissarissen, de bedrijfsrevisoren en de andere personen die belast zijn met de wettelijke controle van de rekeningen van de

ONTWERP VAN WET

bevoegdheden hebben als de in de bepaling onder 2° /1 bedoelde autoriteiten, en waarmee de Bank een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten;

4° aan de FSMA;

5° aan de Belgische instellingen of aan instellingen van een andere Lidstaat van de Europese Economische Ruimte die een beschermingsregeling voor deposito's, beleggers of levensverzekeringen beheren en aan het orgaan dat bevoegd is voor de financieringsregelingen voor de afwikkeling;

6° aan de centrale tegenpartijen de instellingen voor vereffening van financiële instrumenten of de centrale effectenbewaarinstellingen die gemachtigd zijn om verrekenings- of vereffeningdiensten te verstrekken voor transacties in financiële instrumenten verricht op een Belgische gereguleerde markt, als de Bank van oordeel is dat de mededeling van de betrokken informatie noodzakelijk is om de regelmatige werking van die centrale tegenpartijen, instellingen voor vereffening en centrale effectenbewaarinstellingen te vrijwaren voor tekortkomingen, zelfs potentiële, van marktdeelnemers op de betrokken markt;

7° binnen de grenzen van het recht van de Europese Unie, aan de marktondernemingen voor de goede werking van, de controle van en het toezicht op de markten die deze inrichten;

8° tijdens burgerrechtelijke of handelsrechtelijke procedures, aan de autoriteiten en gerechtelijke mandatarissen die betrokken zijn bij procedures van faillissement of gerechtelijke reorganisatie of bij analoge collectieve procedures betreffende instellingen die onder het toezicht van de Bank staan, met uitzondering van de vertrouwelijke informatie over het aandeel van derden in reddingspogingen vóór de betrokken procedures werden ingesteld;

9° aan de commissarissen, de bedrijfsrevisoren en de andere personen die belast zijn met de wettelijke controle van de rekeningen van de

BESTAANDE TEKST

instellingen die onder het toezicht van de Bank vallen, van de rekeningen van andere Belgische financiële instellingen of van soortgelijke buitenlandse instellingen;

10° aan de sekwesters, voor de uitoefening van hun opdracht als bedoeld in de wetten tot regeling van de opdrachten die aan de Bank zijn toevertrouwd;

11° aan het College van toezicht op de bedrijfsrevisoren en aan de autoriteiten van lidstaten of derde landen die toezicht houden op de personen die belast zijn met de wettelijke controle op de jaarrekening van de instellingen die onder het toezicht van de Bank staan;

12° binnen de grenzen van het recht van de Europese Unie, aan de Belgische mededingingsautoriteit;

13° [...]

14° aan de Algemene Administratie van de Thesaurie van de Federale Overheidsdienst Financiën, indien het recht van de Europese Unie of een wettelijke of reglementaire bepaling inzake financiële sancties (met name de bindende bepalingen betreffende financiële embargo's die in artikel 4, 6°, van de wet van 18 september 2017 zijn opgenomen) in de mededeling van vertrouwelijke informatie voorziet, of wanneer de Algemene Administratie van de Thesaurie optreedt als autoriteit die toezicht houdt op de naleving van Verordening (EG) nr. 2271/96 van de Raad van 22 november 1996 tot bescherming tegen de gevolgen van de extraterritoriale toepassing van rechtsregels uitgevaardigd door een derde land en daarop gebaseerde of daaruit voortvloeiende handelingen;

15° binnen de grenzen van het recht van de Europese Unie, aan de van de instellingen onafhankelijke actuarissen die krachtens de wet een opdracht vervullen waarbij ze controle uitoefenen op die instellingen, alsook aan de instanties die met het toezicht op die actuarissen zijn belast;

ONTWERP VAN WET

instellingen die onder het toezicht van de Bank vallen, van de rekeningen van andere Belgische financiële instellingen of van soortgelijke buitenlandse instellingen;

10° aan de sekwesters, voor de uitoefening van hun opdracht als bedoeld in de wetten tot regeling van de opdrachten die aan de Bank zijn toevertrouwd;

11° aan het College van toezicht op de bedrijfsrevisoren en aan de autoriteiten van lidstaten of derde landen die toezicht houden op de personen die belast zijn met de wettelijke controle op de jaarrekening van de instellingen die onder het toezicht van de Bank staan;

12° binnen de grenzen van het recht van de Europese Unie, aan de Belgische mededingingsautoriteit;

13° [...]

14° aan de Algemene Administratie van de Thesaurie van de Federale Overheidsdienst Financiën, indien het recht van de Europese Unie of een wettelijke of reglementaire bepaling inzake financiële sancties (met name de bindende bepalingen betreffende financiële embargo's die in artikel 4, 6°, van de wet van 18 september 2017 zijn opgenomen) in de mededeling van vertrouwelijke informatie voorziet, of wanneer de Algemene Administratie van de Thesaurie optreedt als autoriteit die toezicht houdt op de naleving van Verordening (EG) nr. 2271/96 van de Raad van 22 november 1996 tot bescherming tegen de gevolgen van de extraterritoriale toepassing van rechtsregels uitgevaardigd door een derde land en daarop gebaseerde of daaruit voortvloeiende handelingen;

15° binnen de grenzen van het recht van de Europese Unie, aan de van de instellingen onafhankelijke actuarissen die krachtens de wet een opdracht vervullen waarbij ze controle uitoefenen op die instellingen, alsook aan de instanties die met het toezicht op die actuarissen zijn belast;

BESTAANDE TEKST

16° aan Fedris;

17° binnen de grenzen van het recht van de Europese Unie, aan de Federale Overheidsdienst Economie, in zijn hoedanigheid van bevoegde autoriteit voor het toezicht op de naleving van de bepalingen van boek VII, titels 1 tot 3, titel 5, hoofdstuk 1, en titels 6 en 7 van het Wetboek van economisch recht, en aan de ambtenaren aangesteld door de minister die in het raam van hun opdracht bedoeld in artikel XV.2 van het Wetboek van economisch recht bevoegd zijn om de inbreuken op de bepalingen van artikel XV.89 van het voornoemde Wetboek op te sporen en vast te stellen;

18° aan de autoriteiten die onder het recht van lidstaten van de Europese Unie ressorteren en die bevoegd zijn op het vlak van macroprudentieel toezicht, evenals aan het Europees Comité voor Systeemrisico's, ingesteld bij Europese Verordening (EU) nr. 1092/2010 van het Europees Parlement en de Raad van 24 november 2010;

19° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de Europese Autoriteit voor effecten en markten, aan de Europese Autoriteit voor verzekeringen en bedrijfspensioenen en aan de Europese Bankautoriteit;

20° binnen de grenzen van het recht van de Europese Unie, aan het Coördinatie- en Crisiscentrum van de Regering van de FOD Binnenlandse Zaken, aan het Coördinatieorgaan voor de dreigingsanalyse, ingesteld door de wet van 10 juli 2006 betreffende de analyse van de dreiging, aan de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019 en aan de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, in de mate dat de toepassing van artikel 19 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur zulks vereist;

ONTWERP VAN WET

16° aan Fedris;

17° binnen de grenzen van het recht van de Europese Unie, aan de Federale Overheidsdienst Economie, in zijn hoedanigheid van bevoegde autoriteit voor het toezicht op de naleving van de bepalingen van boek VII, titels 1 tot 3, titel 5, hoofdstuk 1, en titels 6 en 7 van het Wetboek van economisch recht, en aan de ambtenaren aangesteld door de minister die in het raam van hun opdracht bedoeld in artikel XV.2 van het Wetboek van economisch recht bevoegd zijn om de inbreuken op de bepalingen van artikel XV.89 van het voornoemde Wetboek op te sporen en vast te stellen;

18° aan de autoriteiten die onder het recht van lidstaten van de Europese Unie ressorteren en die bevoegd zijn op het vlak van macroprudentieel toezicht, evenals aan het Europees Comité voor Systeemrisico's, ingesteld bij Europese Verordening (EU) nr. 1092/2010 van het Europees Parlement en de Raad van 24 november 2010;

19° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de Europese Autoriteit voor effecten en markten, aan de Europese Autoriteit voor verzekeringen en bedrijfspensioenen en aan de Europese Bankautoriteit;

20° binnen de grenzen van het recht van de Europese Unie, aan het Coördinatie- en Crisiscentrum van de Regering van de FOD Binnenlandse Zaken, aan het Coördinatieorgaan voor de dreigingsanalyse, ingesteld door de wet van 10 juli 2006 betreffende de analyse van de dreiging, **aan de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 45°, van de NIS2-wet** en aan de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, in de mate dat de toepassing van artikel 19 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur zulks vereist;

BESTAANDE TEKST

20° /1 binnen de grenzen van het recht van de Europese Unie, aan de politiediensten en aan de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid - NIS-wet ten behoeve van de tenuitvoerlegging van artikel 53, § 2, van de wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen;

20°/2 binnen de grenzen van het recht van de Europese Unie, aan de autoriteit bedoeld in artikel 5, § 1, van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit, of aan de door de Koning krachtens artikel 5, § 2, van dezelfde wet aangewezen overheden;

21° aan de Controledienst voor de ziekenfondsen en de landsbonden van ziekenfondsen, voor de uitoefening van zijn wettelijke opdrachten als bedoeld in artikel 303, § 3, van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen, met betrekking tot de maatschappijen van onderlinge bijstand als bedoeld in artikel 43bis, § 5 of artikel 70, §§ 6, 7 en 8 van de wet van 6 augustus 1990 betreffende de ziekenfondsen en de landsbonden van ziekenfondsen en hun verrichtingen;

22° binnen de grenzen van het recht van de Europese Unie, aan de afwikkelingsautoriteiten als bedoeld in artikel 3 van Richtlijn 2014/59/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende de totstandbrenging van een kader voor het herstel en de afwikkeling van kredietinstellingen en beleggingsondernemingen, aan de autoriteiten

ONTWERP VAN WET

20° /1 binnen de grenzen van het recht van de Europese Unie, aan de politiediensten en **aan de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 45°, van de NIS2-wet en aan het nationaal CSIRT bedoeld in artikel 8, 46°, van dezelfde wet** ten behoeve van de tenuitvoerlegging van artikel 53, § 2, van de wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen;

20°/2 binnen de grenzen van het recht van de Europese Unie, aan de autoriteit bedoeld in artikel 5, § 1, van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit, of aan de door de Koning krachtens artikel 5, § 2, van dezelfde wet aangewezen overheden;

21° aan de Controledienst voor de ziekenfondsen en de landsbonden van ziekenfondsen, voor de uitoefening van zijn wettelijke opdrachten als bedoeld in artikel 303, § 3, van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen, met betrekking tot de maatschappijen van onderlinge bijstand als bedoeld in artikel 43bis, § 5 of artikel 70, §§ 6, 7 en 8 van de wet van 6 augustus 1990 betreffende de ziekenfondsen en de landsbonden van ziekenfondsen en hun verrichtingen;

22° binnen de grenzen van het recht van de Europese Unie, aan de afwikkelingsautoriteiten als bedoeld in artikel 3 van Richtlijn 2014/59/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende de totstandbrenging van een kader voor het herstel en de afwikkeling van kredietinstellingen en beleggingsondernemingen, aan de autoriteiten

BESTAANDE TEKST

van derde Staten die belast zijn met taken die te vergelijken zijn met die als bedoeld in artikel 12ter, § 1, waarmee de Bank een samenwerkingsakkoord heeft gesloten waarin wordt voorzien in de uitwisseling van informatie, alsook aan de bevoegde ministeries van de lidstaten van de Europese Economische Ruimte, wanneer dit noodzakelijk is voor het plannen of uitvoeren van afwikkelingsmaatregel;

22° /1 binnen de grenzen van het recht van de Europese Unie, aan de afwikkelingsautoriteiten bedoeld in artikel 3 van Verordening 2021/23, aan de autoriteiten van derde Staten die belast zijn met taken die te vergelijken zijn met die bedoeld in artikel 12ter, § 1/1, waarmee de Bank een samenwerkingsakkoord heeft gesloten waarin wordt voorzien in de uitwisseling van informatie, alsook aan de bevoegde ministeries van de lidstaten van de Europese Economische Ruimte, wanneer dit noodzakelijk blijkt voor het plannen of uitvoeren van een afwikkelingsmaatregel;

23° aan eenieder die een taak uitvoert die door of krachtens de wet is vastgesteld en die deelneemt of bijdraagt aan de uitoefening van de toezichtopdracht van de Bank, wanneer die persoon door of met instemming van de Bank werd aangeduid voor die taak, zoals, met name:

a) de portefeuillesurveillant bedoeld in artikel 16 van Bijlage III bij de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen ;

b) de portefeuillebeheerder bedoeld in artikel 8 van Bijlage III bij de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen ; en

c) de speciaal commissaris en de voorlopige bestuurder als bedoeld in artikel 236, § 1 van de voornoemde wet van 25 april 2014, artikel 204, § 1 van de wet van 20 juli 2022 op het statuut van en het toezicht op beursvennootschappen en houdende diverse bepalingen, artikel 517, § 1 van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of

ONTWERP VAN WET

van derde Staten die belast zijn met taken die te vergelijken zijn met die als bedoeld in artikel 12ter, § 1, waarmee de Bank een samenwerkingsakkoord heeft gesloten waarin wordt voorzien in de uitwisseling van informatie, alsook aan de bevoegde ministeries van de lidstaten van de Europese Economische Ruimte, wanneer dit noodzakelijk is voor het plannen of uitvoeren van afwikkelingsmaatregel;

22° /1 binnen de grenzen van het recht van de Europese Unie, aan de afwikkelingsautoriteiten bedoeld in artikel 3 van Verordening 2021/23, aan de autoriteiten van derde Staten die belast zijn met taken die te vergelijken zijn met die bedoeld in artikel 12ter, § 1/1, waarmee de Bank een samenwerkingsakkoord heeft gesloten waarin wordt voorzien in de uitwisseling van informatie, alsook aan de bevoegde ministeries van de lidstaten van de Europese Economische Ruimte, wanneer dit noodzakelijk blijkt voor het plannen of uitvoeren van een afwikkelingsmaatregel;

23° aan eenieder die een taak uitvoert die door of krachtens de wet is vastgesteld en die deelneemt of bijdraagt aan de uitoefening van de toezichtopdracht van de Bank, wanneer die persoon door of met instemming van de Bank werd aangeduid voor die taak, zoals, met name:

a) de portefeuillesurveillant bedoeld in artikel 16 van Bijlage III bij de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen ;

b) de portefeuillebeheerder bedoeld in artikel 8 van Bijlage III bij de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen ; en

c) de speciaal commissaris en de voorlopige bestuurder als bedoeld in artikel 236, § 1 van de voornoemde wet van 25 april 2014, artikel 204, § 1 van de wet van 20 juli 2022 op het statuut van en het toezicht op beursvennootschappen en houdende diverse bepalingen, artikel 517, § 1 van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of

BESTAANDE TEKST

herverzekeringsondernemingen, de artikelen 117, § 1 en 215, § 1 van de wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen, artikel 48, eerste lid van het koninklijk besluit van 30 april 1999 betreffende het statuut en de controle der maatschappijen voor onderlinge borgstelling, en de artikelen 36/30, § 1, tweede lid en 36/30/1, § 2 van deze wet;

24° binnen de grenzen van het recht van de Europese Unie, aan de autoriteiten bedoeld in artikel 7 van de wet van 7 april 2019 voor de uitvoering van de bepalingen van de wet van 7 april 2019 en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur;

25° aan de Federale Overheidsdienst Economie, KMO, Middenstand en Energie, in het kader van de uitvoering van zijn opdracht bedoeld in artikel 85, § 1, 5°, van de wet van 18 september 2017 ten aanzien van de entiteiten bedoeld in artikel 5, § 1, 21°, van dezelfde wet;

26° binnen de grenzen van het recht van de Europese Unie, aan de financiële inlichtingeneenheden bedoeld in artikel 4, 15° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;

27° ingeval de financiële situatie van een financiële instelling als bedoeld in artikel 36/2 verslechtert, aan het openbaar ministerie;

28° binnen de grenzen van het recht van de Europese Unie, aan de Europese Commissie als deze gegevens nodig zijn voor de uitoefening van de bevoegdheden van deze laatste.

ONTWERP VAN WET

herverzekeringsondernemingen, de artikelen 117, § 1 en 215, § 1 van de wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen, artikel 48, eerste lid van het koninklijk besluit van 30 april 1999 betreffende het statuut en de controle der maatschappijen voor onderlinge borgstelling, en de artikelen 36/30, § 1, tweede lid en 36/30/1, § 2 van deze wet;

24° binnen de grenzen van het recht van de Europese Unie, **aan de autoriteiten bedoeld in artikel 15 van de NIS2-wet voor de uitvoering van de bepalingen van de NIS2-wet** voor de uitvoering van de bepalingen van de wet van 7 april 2019 en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur;

25° aan de Federale Overheidsdienst Economie, KMO, Middenstand en Energie, in het kader van de uitvoering van zijn opdracht bedoeld in artikel 85, § 1, 5°, van de wet van 18 september 2017 ten aanzien van de entiteiten bedoeld in artikel 5, § 1, 21°, van dezelfde wet;

26° binnen de grenzen van het recht van de Europese Unie, aan de financiële inlichtingeneenheden bedoeld in artikel 4, 15° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;

27° ingeval de financiële situatie van een financiële instelling als bedoeld in artikel 36/2 verslechtert, aan het openbaar ministerie;

28° binnen de grenzen van het recht van de Europese Unie, aan de Europese Commissie als deze gegevens nodig zijn voor de uitoefening van de bevoegdheden van deze laatste.

BESTAANDE TEKST

§ 2. De Bank mag enkel vertrouwelijke informatie krachtens paragraaf 1 meedelen op de volgende voorwaarden :

1° de autoriteiten of instellingen die de informatie ontvangen, gebruiken deze voor de uitvoering van hun opdrachten, met inbegrip van de mededeling van deze informatie aan derden ingevolge een wettelijke verplichting van deze autoriteiten of instellingen; in de andere gevallen kan de Bank toestaan, binnen de grenzen van het recht van de Europese Unie, dat de ontvangers van de informatie deze bekendmaken aan derden, mits de Bank daar voorafgaandelijk mee heeft ingestemd en, in voorkomend geval, mits de informatie alleen voor de door de Bank toegestane doeleinden bekendgemaakt wordt;

2° Wat de aldus aan hen meegedeelde informatie betreft, zijn deze buitenlandse autoriteiten of instellingen aan een beroepsgeheim gebonden dat gelijkwaardig is aan dat van artikel 35; en

3° indien de betrokken informatie afkomstig is van een autoriteit van een andere lidstaat van de Europese Economische Ruimte, mag zij enkel bekendgemaakt worden aan de volgende autoriteiten of instellingen mits de autoriteit die de informatie heeft verstrekt uitdrukkelijk akkoord gaat met deze bekendmaking, en, in voorkomend geval, mits de informatie alleen voor de door deze autoriteit toegestane doeleinden bekendgemaakt wordt :

a) de in paragraaf 1, 5°, 6°, 8° en 11°, bedoelde autoriteiten of instellingen;

b) de in paragraaf 1, 3°, 5°, 8°, 9°, 11°, 18° en 22°, bedoelde autoriteiten of instellingen van derde Staten;

c) autoriteiten of instellingen van derde Staten die opdrachten uitvoeren die gelijkwaardig zijn aan die van de FSMA.

ONTWERP VAN WET

§ 2. De Bank mag enkel vertrouwelijke informatie krachtens paragraaf 1 meedelen op de volgende voorwaarden :

1° de autoriteiten of instellingen die de informatie ontvangen, gebruiken deze voor de uitvoering van hun opdrachten, met inbegrip van de mededeling van deze informatie aan derden ingevolge een wettelijke verplichting van deze autoriteiten of instellingen; in de andere gevallen kan de Bank toestaan, binnen de grenzen van het recht van de Europese Unie, dat de ontvangers van de informatie deze bekendmaken aan derden, mits de Bank daar voorafgaandelijk mee heeft ingestemd en, in voorkomend geval, mits de informatie alleen voor de door de Bank toegestane doeleinden bekendgemaakt wordt;

2° Wat de aldus aan hen meegedeelde informatie betreft, zijn deze buitenlandse autoriteiten of instellingen aan een beroepsgeheim gebonden dat gelijkwaardig is aan dat van artikel 35; en

3° indien de betrokken informatie afkomstig is van een autoriteit van een andere lidstaat van de Europese Economische Ruimte, mag zij enkel bekendgemaakt worden aan de volgende autoriteiten of instellingen mits de autoriteit die de informatie heeft verstrekt uitdrukkelijk akkoord gaat met deze bekendmaking, en, in voorkomend geval, mits de informatie alleen voor de door deze autoriteit toegestane doeleinden bekendgemaakt wordt :

a) de in paragraaf 1, 5°, 6°, 8° en 11°, bedoelde autoriteiten of instellingen;

b) de in paragraaf 1, 3°, 5°, 8°, 9°, 11°, 18° en 22°, bedoelde autoriteiten of instellingen van derde Staten;

c) autoriteiten of instellingen van derde Staten die opdrachten uitvoeren die gelijkwaardig zijn aan die van de FSMA.

BESTAANDE TEKST

§ 3. Onverminderd de strengere bepalingen van de bijzondere wetten die op hen van toepassing zijn, zijn de in paragraaf 1 bedoelde Belgische personen, autoriteiten en instellingen, wat de vertrouwelijke informatie betreft die zij van de Bank ontvangen met toepassing van paragraaf 1, gebonden door het beroepsgeheim als bedoeld in artikel 35.

§ 4. [...]

Artikel 36/47

Voor de toepassing van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid wordt de Bank aangewezen als sectorale overheid en inspectiedienst voor de aanbieders van de sector financiën, met uitzondering van de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU.

De artikelen 36/19 en 36/20 zijn van toepassing.

De Sanctiecommissie oordeelt over het opleggen van de administratieve geldboetes bedoeld in artikel 52 van voormelde wet van 7 april 2019. De artikelen 36/8 tot 36/12/3 en artikel 36/21 zijn van toepassing.

De Bank deelt relevante informatie over incidentmeldingen die zij ontvangt krachtens de wet van 7 april 2019 zo snel mogelijk met de ECB.

ONTWERP VAN WET

§ 3. Onverminderd de strengere bepalingen van de bijzondere wetten die op hen van toepassing zijn, zijn de in paragraaf 1 bedoelde Belgische personen, autoriteiten en instellingen, wat de vertrouwelijke informatie betreft die zij van de Bank ontvangen met toepassing van paragraaf 1, gebonden door het beroepsgeheim als bedoeld in artikel 35.

§ 4. [...]

Artikel 36/47

Voor de toepassing van de NIS2-wet wordt de Bank aangewezen als sectorale overheid en sectorale inspectiedienst voor de entiteiten van de sector financiën, met uitzondering van de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU.

Wanneer zij dit nuttig acht, deelt de Bank zo snel mogelijk met de ECB relevante informatie over incidentmeldingen die zij ontvangt krachtens de NIS2-Wet of Verordening 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011.

[...]

[...]

BESTAANDE TEKST**ONTWERP VAN WET****Wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten****Artikel 75****Artikel 75**

§ 1. In afwijking van artikel 74, eerste lid, en binnen de grenzen van het recht van de Europese Unie mag de FSMA vertrouwelijke informatie meedelen :

§ 1. In afwijking van artikel 74, eerste lid, en binnen de grenzen van het recht van de Europese Unie mag de FSMA vertrouwelijke informatie meedelen :

1° aan de Europese Centrale Bank, aan de Bank en aan de andere centrale banken en instellingen met een gelijkaardige opdracht als monetaire overheid, alsook aan andere overheidsinstanties die belast zijn met het toezicht op de betalings- en afwikkelingssystemen;

1° aan de Europese Centrale Bank, aan de Bank en aan de andere centrale banken en instellingen met een gelijkaardige opdracht als monetaire overheid, alsook aan andere overheidsinstanties die belast zijn met het toezicht op de betalings- en afwikkelingssystemen;

aan de Europese Centrale Bank, aan de Bank en aan de andere centrale banken en instellingen met een soortgelijke taak in hun hoedanigheid van monetaire autoriteit als deze gegevens van belang zijn voor de uitoefening van hun respectieve wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en afwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel, alsook aan andere overheidsinstanties die belast zijn met het toezicht op de betalingssystemen.

aan de Europese Centrale Bank, aan de Bank en aan de andere centrale banken en instellingen met een soortgelijke taak in hun hoedanigheid van monetaire autoriteit als deze gegevens van belang zijn voor de uitoefening van hun respectieve wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en afwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel, alsook aan andere overheidsinstanties die belast zijn met het toezicht op de betalingssystemen.

Wanneer zich een noodsituatie voordoet, waaronder ongunstige ontwikkelingen op de financiële markten, die de liquiditeit van de markt en de stabiliteit van het financiële stelsel kan ondermijnen in een van de lidstaten waar aan entiteiten van een groep met beleggingsondernemingen vergunning is verleend of significante bijkantoren zijn gevestigd in de zin van artikel 59, §§ 6 en 7, van de wet van 25 oktober 2016, kan de FSMA gegevens verzenden aan centrale banken van het Europees stelsel van centrale banken als deze gegevens van belang zijn voor de uitoefening van hun wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide

Wanneer zich een noodsituatie voordoet, waaronder ongunstige ontwikkelingen op de financiële markten, die de liquiditeit van de markt en de stabiliteit van het financiële stelsel kan ondermijnen in een van de lidstaten waar aan entiteiten van een groep met beleggingsondernemingen vergunning is verleend of significante bijkantoren zijn gevestigd in de zin van artikel 59, §§ 6 en 7, van de wet van 25 oktober 2016, kan de FSMA gegevens verzenden aan centrale banken van het Europees stelsel van centrale banken als deze gegevens van belang zijn voor de uitoefening van hun wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide

BESTAANDE TEKST

middelen, de uitoefening van toezicht op betalings-, clearing- en effectenafwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel.

In een noodsituatie zoals hierboven bedoeld, kan de FSMA gegevens meedelen die van belang zijn voor de centrale overheidsdiensten in alle betrokken lidstaten die bevoegd zijn voor de wetgeving inzake toezicht op de kredietinstellingen, financiële instellingen, beleggingsdiensten en verzekeringsmaatschappijen;

1° bis aan de Bank , aan de Europese Centrale Bank met betrekking tot de taken die haar zijn opgedragen door Verordening (EU) nr. 1024/2013 van de Raad van 15 oktober 2013 waarbij aan de Europese Centrale Bank specifieke taken worden opgedragen betreffende het beleid inzake het prudentieel toezicht op kredietinstellingen, en aan de andere leden van het ESCB;

2° aan het Federaal Agentschap van de Schuld;

3° aan de bevoegde autoriteiten van andere Lidstaten van de Europese Economische Ruimte die één of meer bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in artikel 45;

4° aan de bevoegde autoriteiten van derde Staten die één of meer bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in artikel 45 en waarmee de FSMA een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten;

5° aan het Agentschap voor de samenwerking tussen energieregulators (ACER) en de nationale regulerende instanties bedoeld in artikel 2, punt 10, van Verordening 1227/2011, en, voor Verordening 596/2014, aan de Europese Commissie en de overige instanties bedoeld in artikel 25 van die verordening;

ONTWERP VAN WET

middelen, de uitoefening van toezicht op betalings-, clearing- en effectenafwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel.

In een noodsituatie zoals hierboven bedoeld, kan de FSMA gegevens meedelen die van belang zijn voor de centrale overheidsdiensten in alle betrokken lidstaten die bevoegd zijn voor de wetgeving inzake toezicht op de kredietinstellingen, financiële instellingen, beleggingsdiensten en verzekeringsmaatschappijen;

1° bis aan de Bank , aan de Europese Centrale Bank met betrekking tot de taken die haar zijn opgedragen door Verordening (EU) nr. 1024/2013 van de Raad van 15 oktober 2013 waarbij aan de Europese Centrale Bank specifieke taken worden opgedragen betreffende het beleid inzake het prudentieel toezicht op kredietinstellingen, en aan de andere leden van het ESCB;

2° aan het Federaal Agentschap van de Schuld;

3° aan de bevoegde autoriteiten van andere Lidstaten van de Europese Economische Ruimte die één of meer bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in artikel 45;

4° aan de bevoegde autoriteiten van derde Staten die één of meer bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in artikel 45 en waarmee de FSMA een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten;

5° aan het Agentschap voor de samenwerking tussen energieregulators (ACER) en de nationale regulerende instanties bedoeld in artikel 2, punt 10, van Verordening 1227/2011, en, voor Verordening 596/2014, aan de Europese Commissie en de overige instanties bedoeld in artikel 25 van die verordening;

BESTAANDE TEKST

6° aan de Belgische instellingen of aan instellingen van andere lidstaten van de Europese Economische Ruimte die een beschermingsregeling voor deposito's, beleggers of levensverzekeringen beheren;

7° aan de centrale tegenpartijen of de centrale effectenbewaarinstellingen die gemachtigd zijn om verrekenings- of afwikkelingsdiensten te verstrekken voor transacties in financiële instrumenten verricht op een Belgische georganiseerde markt, als de FSMA van oordeel is dat de mededeling van de betrokken informatie noodzakelijk is om de regelmatige werking van die instellingen te vrijwaren voor tekortkomingen, zelfs potentiële, van marktdeelnemers op de betrokken markt;

8° aan de marktexploitanten voor de goede werking van, de controle van en het toezicht op de markten die zij inrichten;

9° tijdens burgerrechtelijke of handelsrechtelijke procedures, aan de autoriteiten en gerechtelijke mandatarissen die betrokken zijn bij procedures van faillissement of gerechtelijke reorganisatie of bij analoge collectieve procedures betreffende ondernemingen die onder het toezicht van de FSMA staan of waarvan de verrichtingen onder haar toezicht staan, met uitzondering van de vertrouwelijke informatie over het aandeel van derden in pogingen om de instelling te redden vóór de betrokken procedures werden ingesteld;

10° aan de commissarissen, de bedrijfsrevisoren en de andere personen die belast zijn met de wettelijke controle van de rekeningen van de ondernemingen die onder het toezicht van de FSMA vallen, van de rekeningen van andere Belgische financiële instellingen of van gelijkaardige buitenlandse ondernemingen;

11° aan de sekwesters, voor de uitoefening van hun opdracht als bedoeld in de wetten tot regeling van de opdrachten die aan de FSMA zijn toevertrouwd;

ONTWERP VAN WET

6° aan de Belgische instellingen of aan instellingen van andere lidstaten van de Europese Economische Ruimte die een beschermingsregeling voor deposito's, beleggers of levensverzekeringen beheren;

7° aan de centrale tegenpartijen of de centrale effectenbewaarinstellingen die gemachtigd zijn om verrekenings- of afwikkelingsdiensten te verstrekken voor transacties in financiële instrumenten verricht op een Belgische georganiseerde markt, als de FSMA van oordeel is dat de mededeling van de betrokken informatie noodzakelijk is om de regelmatige werking van die instellingen te vrijwaren voor tekortkomingen, zelfs potentiële, van marktdeelnemers op de betrokken markt;

8° aan de marktexploitanten voor de goede werking van, de controle van en het toezicht op de markten die zij inrichten;

9° tijdens burgerrechtelijke of handelsrechtelijke procedures, aan de autoriteiten en gerechtelijke mandatarissen die betrokken zijn bij procedures van faillissement of gerechtelijke reorganisatie of bij analoge collectieve procedures betreffende ondernemingen die onder het toezicht van de FSMA staan of waarvan de verrichtingen onder haar toezicht staan, met uitzondering van de vertrouwelijke informatie over het aandeel van derden in pogingen om de instelling te redden vóór de betrokken procedures werden ingesteld;

10° aan de commissarissen, de bedrijfsrevisoren en de andere personen die belast zijn met de wettelijke controle van de rekeningen van de ondernemingen die onder het toezicht van de FSMA vallen, van de rekeningen van andere Belgische financiële instellingen of van gelijkaardige buitenlandse ondernemingen;

11° aan de sekwesters, voor de uitoefening van hun opdracht als bedoeld in de wetten tot regeling van de opdrachten die aan de FSMA zijn toevertrouwd;

BESTAANDE TEKST

12° aan het College van toezicht op de bedrijfsrevisoren en aan de autoriteiten van lidstaten of derde landen die toezicht houden op de personen die belast zijn met de wettelijke controle op de jaarrekening van de ondernemingen die onder het toezicht van de FSMA staan;

13° aan de Federale Overheidsdienst Economie; K.M.O., Middenstand en Energie in het kader van het toezicht op het consumentenkrediet, op het hypothecair krediet op de marktpraktijken en op de betalingsdiensten, aan de bevoegde autoriteiten van andere Lidstaten van de Europese Economische Ruimte die een vergelijkbare bevoegdheid uitoefenen, alsook aan de bevoegde autoriteiten van derde Staten die een vergelijkbare bevoegdheid uitoefenen en waarmee de FSMA een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten;

14° aan de Belgische Mededingingsautoriteit;

15° aan de autoriteiten bedoeld in artikel 7 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid voor de uitvoering van de bepalingen van deze wet en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;

16° aan de Algemene Administratie van de Thesaurie als een dergelijke mededeling is voorgeschreven door het recht van de Europese Unie of door een wettelijke of reglementaire bepaling over financiële sancties (met name de bindende bepalingen betreffende financiële embargo's als gedefinieerd in artikel 4, 6° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten) of als de Algemene Administratie van de Thesaurie optreedt in de hoedanigheid van toezichthouder die zorgt voor de naleving van Verordening (EG) nr. 2271/96 van de Raad van 22 november 1996 tot bescherming tegen de

ONTWERP VAN WET

12° aan het College van toezicht op de bedrijfsrevisoren en aan de autoriteiten van lidstaten of derde landen die toezicht houden op de personen die belast zijn met de wettelijke controle op de jaarrekening van de ondernemingen die onder het toezicht van de FSMA staan;

13° aan de Federale Overheidsdienst Economie; K.M.O., Middenstand en Energie in het kader van het toezicht op het consumentenkrediet, op het hypothecair krediet op de marktpraktijken en op de betalingsdiensten, aan de bevoegde autoriteiten van andere Lidstaten van de Europese Economische Ruimte die een vergelijkbare bevoegdheid uitoefenen, alsook aan de bevoegde autoriteiten van derde Staten die een vergelijkbare bevoegdheid uitoefenen en waarmee de FSMA een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten;

14° aan de Belgische Mededingingsautoriteit;

15° aan de autoriteiten bedoeld in **artikel 15 van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid** voor de uitvoering van de bepalingen van deze wet en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur;

16° aan de Algemene Administratie van de Thesaurie als een dergelijke mededeling is voorgeschreven door het recht van de Europese Unie of door een wettelijke of reglementaire bepaling over financiële sancties (met name de bindende bepalingen betreffende financiële embargo's als gedefinieerd in artikel 4, 6° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten) of als de Algemene Administratie van de Thesaurie optreedt in de hoedanigheid van toezichthouder die zorgt voor de naleving van Verordening (EG) nr. 2271/96 van de Raad van 22 november 1996 tot bescherming tegen de

BESTAANDE TEKST

gevolgen van de extraterritoriale toepassing van rechtsregels uitgevaardigd door een derde land en daarop gebaseerde of daaruit voortvloeiende handelingen;

17° aan de van de ondernemingen onafhankelijke actuarissen die krachtens de wet een opdracht vervullen waarbij zij controle uitoefenen op die ondernemingen, alsook aan de instanties die met het toezicht op die actuarissen zijn belast;

18° aan Fedris;

19° aan de CDZ in zijn hoedanigheid van toezichthouder op de maatschappijen van onderlinge bijstand als bedoeld in de artikelen 43bis, § 5, en 70, §§ 6 en 7, van de wet van 6 augustus 1990 betreffende de ziekenfondsen en de landsbonden van ziekenfondsen, en op de verzekeringstussenpersonen als bedoeld in artikel 68 van de wet van 26 april 2010 houdende diverse bepalingen inzake de organisatie van de aanvullende ziekteverzekering (I), alsook op hun activiteiten;

19° [...]

20° [...]

21° , aan de ESMA, de EIOPA en de EBA en aan het Europees Comité voor systeemrisico's.

22° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de autoriteiten die toezicht houden op personen die actief zijn op markten voor emissierechten;

23° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de autoriteiten die toezicht houden op personen die actief zijn op markten voor landbouwgrondstoffenderivaten.

24° aan de Belgische Gegevensbeschermingsautoriteit.

24° /1 aan de Cel voor financiële informatieverwerking bedoeld in artikel 76 van

ONTWERP VAN WET

gevolgen van de extraterritoriale toepassing van rechtsregels uitgevaardigd door een derde land en daarop gebaseerde of daaruit voortvloeiende handelingen;

17° aan de van de ondernemingen onafhankelijke actuarissen die krachtens de wet een opdracht vervullen waarbij zij controle uitoefenen op die ondernemingen, alsook aan de instanties die met het toezicht op die actuarissen zijn belast;

18° aan Fedris;

19° aan de CDZ in zijn hoedanigheid van toezichthouder op de maatschappijen van onderlinge bijstand als bedoeld in de artikelen 43bis, § 5, en 70, §§ 6 en 7, van de wet van 6 augustus 1990 betreffende de ziekenfondsen en de landsbonden van ziekenfondsen, en op de verzekeringstussenpersonen als bedoeld in artikel 68 van de wet van 26 april 2010 houdende diverse bepalingen inzake de organisatie van de aanvullende ziekteverzekering (I), alsook op hun activiteiten;

19° [...]

20° [...]

21° , aan de ESMA, de EIOPA en de EBA en aan het Europees Comité voor systeemrisico's.

22° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de autoriteiten die toezicht houden op personen die actief zijn op markten voor emissierechten;

23° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de autoriteiten die toezicht houden op personen die actief zijn op markten voor landbouwgrondstoffenderivaten.

24° aan de Belgische Gegevensbeschermingsautoriteit.

24° /1 aan de Cel voor financiële informatieverwerking bedoeld in artikel 76 van

BESTAANDE TEKST

de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;

25° tijdens procedures tot vereffening van een instelling voor bedrijfspensioenvoorziening of van een pensioenregeling in de zin van de wet van 27 oktober 2006 betreffende het toezicht op de instellingen voor bedrijfspensioenvoorziening, aan de autoriteiten en personen die betrokken zijn bij die procedures, alsook aan de autoriteiten die verantwoordelijk zijn voor het toezicht op die autoriteiten en personen;

26° aan de personen die bij de FSMA een klacht hebben ingediend met toepassing van artikel 38 van Verordening 2020/1503 van het Europees Parlement en de Raad van 7 oktober 2020 betreffende Europese crowdfundingdienstverleners voor bedrijven en tot wijziging van Verordening (EU) 2017/1129 en Richtlijn (EU) 2019/1937, alsook aan de crowdfundingdienstverleners, aan de personen die, met toepassing van artikel 50 van Verordening 2019/1238, een klacht bij de FSMA hebben ingediend, en aan de PEPP-aanbieders en -distributeurs in de zin van voornoemde Verordening voor zover nodig voor de behandeling van die klacht;

27° aan de autoriteit bedoeld in artikel 5, § 1, van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit of aan de door de Koning aangewezen overheden krachtens artikel 5, § 2, van dezelfde wet;

27° /1 aan de Europese Commissie, in het kader van het toezicht op de vennootschappen voor vermogensbeheer en beleggingsadvies conform artikel 45, § 1, 2°, a), wanneer die informatie noodzakelijk is voor de uitoefening van haar bevoegdheden.

ONTWERP VAN WET

de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;

25° tijdens procedures tot vereffening van een instelling voor bedrijfspensioenvoorziening of van een pensioenregeling in de zin van de wet van 27 oktober 2006 betreffende het toezicht op de instellingen voor bedrijfspensioenvoorziening, aan de autoriteiten en personen die betrokken zijn bij die procedures, alsook aan de autoriteiten die verantwoordelijk zijn voor het toezicht op die autoriteiten en personen;

26° aan de personen die bij de FSMA een klacht hebben ingediend met toepassing van artikel 38 van Verordening 2020/1503 van het Europees Parlement en de Raad van 7 oktober 2020 betreffende Europese crowdfundingdienstverleners voor bedrijven en tot wijziging van Verordening (EU) 2017/1129 en Richtlijn (EU) 2019/1937, alsook aan de crowdfundingdienstverleners, aan de personen die, met toepassing van artikel 50 van Verordening 2019/1238, een klacht bij de FSMA hebben ingediend, en aan de PEPP-aanbieders en -distributeurs in de zin van voornoemde Verordening voor zover nodig voor de behandeling van die klacht;

27° aan de autoriteit bedoeld in artikel 5, § 1, van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit of aan de door de Koning aangewezen overheden krachtens artikel 5, § 2, van dezelfde wet;

27° /1 aan de Europese Commissie, in het kader van het toezicht op de vennootschappen voor vermogensbeheer en beleggingsadvies conform artikel 45, § 1, 2°, a), wanneer die informatie noodzakelijk is voor de uitoefening van haar bevoegdheden.

BESTAANDE TEKST

§ 2. De FSMA mag enkel vertrouwelijke informatie overeenkomstig § 1 meedelen op voorwaarde dat de autoriteiten of instellingen die er de geadresseerde van zijn, die informatie gebruiken voor de uitvoering van hun opdrachten, en dat zij, wat die informatie betreft, aan een gelijkwaardig beroepsgeheim gebonden zijn als bedoeld in artikel 74. Bovendien mag de volgende informatie enkel met de uitdrukkelijke instemming van de autoriteit van wie ze afkomstig is worden doorgegeven en, in voorkomend geval, enkel voor de doeleinden waarmee die autoriteit heeft ingestemd:

1° de informatie afkomstig van een autoriteit van een andere lidstaat van de Europese Economische Ruimte, in de gevallen als bedoeld in 7°, 9°, 10°, 12°, en 17 van § 1;

2° de informatie afkomstig van een autoriteit van een andere lidstaat van de Europese Economische Ruimte en doorgegeven aan de autoriteiten of organismen van derde Staten in de gevallen als bedoeld in de bepalingen onder 4° en 13° van § 1;

3° de informatie doorgegeven door de FSMA in het kader van haar bevoegdheden, als bedoeld in artikel 45, § 1, eerste lid, 2°, g), afkomstig van autoriteiten en personen bedoeld in 3°, 9°, 10°, 12° en 17°, in de gevallen bedoeld in 1bis, 13° en 19° van paragraaf 1. Bovendien mag de FSMA informatie welke is verkregen naar aanleiding van een verificatie ter plaatse in een andere lidstaat in het kader van haar bevoegdheden als bedoeld in artikel 45, § 1, eerste lid, 2°, g),, alleen worden doorgegeven met de uitdrukkelijke instemming van de bevoegde autoriteit van de lidstaat waar de verificatie ter plaatse is verricht en, in voorkomend geval, enkel voor de doeleinden waarmee die autoriteit heeft ingestemd.

§ 3. De FSMA mag de vertrouwelijke informatie als bedoeld in artikel 74, eerste lid, of de vertrouwelijke informatie die zij van de in § 1 bedoelde autoriteiten en instellingen heeft

ONTWERP VAN WET

§ 2. De FSMA mag enkel vertrouwelijke informatie overeenkomstig § 1 meedelen op voorwaarde dat de autoriteiten of instellingen die er de geadresseerde van zijn, die informatie gebruiken voor de uitvoering van hun opdrachten, en dat zij, wat die informatie betreft, aan een gelijkwaardig beroepsgeheim gebonden zijn als bedoeld in artikel 74. Bovendien mag de volgende informatie enkel met de uitdrukkelijke instemming van de autoriteit van wie ze afkomstig is worden doorgegeven en, in voorkomend geval, enkel voor de doeleinden waarmee die autoriteit heeft ingestemd:

1° de informatie afkomstig van een autoriteit van een andere lidstaat van de Europese Economische Ruimte, in de gevallen als bedoeld in 7°, 9°, 10°, 12°, en 17 van § 1;

2° de informatie afkomstig van een autoriteit van een andere lidstaat van de Europese Economische Ruimte en doorgegeven aan de autoriteiten of organismen van derde Staten in de gevallen als bedoeld in de bepalingen onder 4° en 13° van § 1;

3° de informatie doorgegeven door de FSMA in het kader van haar bevoegdheden, als bedoeld in artikel 45, § 1, eerste lid, 2°, g), afkomstig van autoriteiten en personen bedoeld in 3°, 9°, 10°, 12° en 17°, in de gevallen bedoeld in 1bis, 13° en 19° van paragraaf 1. Bovendien mag de FSMA informatie welke is verkregen naar aanleiding van een verificatie ter plaatse in een andere lidstaat in het kader van haar bevoegdheden als bedoeld in artikel 45, § 1, eerste lid, 2°, g),, alleen worden doorgegeven met de uitdrukkelijke instemming van de bevoegde autoriteit van de lidstaat waar de verificatie ter plaatse is verricht en, in voorkomend geval, enkel voor de doeleinden waarmee die autoriteit heeft ingestemd.

§ 3. De FSMA mag de vertrouwelijke informatie als bedoeld in artikel 74, eerste lid, of de vertrouwelijke informatie die zij van de in § 1 bedoelde autoriteiten en instellingen heeft

BESTAANDE TEKST

ontvangen, gebruiken voor de uitvoering van al haar wettelijke opdrachten.

§ 4. Onverminderd de strengere bepalingen van de bijzondere wetten die op hen van toepassing zijn, zijn de in § 1 bedoelde Belgische autoriteiten en instellingen, wat de vertrouwelijke informatie betreft die zij van de FSMA ontvangen met toepassing van § 1, gebonden door het beroepsgeheim als bedoeld in artikel 74.

§ 5. Dit artikel is van toepassing onverminderd de meer restrictieve bepalingen van het recht van de Europese Unie inzake het beroepsgeheim of de bijzondere wetten waarin de opdracht van de FSMA is vastgelegd.

Wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

Artikel 1/1

Deze wet voorziet in de gedeeltelijke omzetting van volgende richtlijnen:

1° Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie;

2° Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie.

Artikel 14

§ 1. Onverminderd zijn wettelijke bevoegdheden, heeft het Instituut de volgende taken met betrekking tot elektronische communicatienetwerken en elektronische communicatiediensten, eindapparatuur, radioapparatuur, met betrekking tot de sector digitale infrastructuur in de zin van de wet van 7 april 2019 tot vaststelling van een kader voor

ONTWERP VAN WET

ontvangen, gebruiken voor de uitvoering van al haar wettelijke opdrachten.

§ 4. Onverminderd de strengere bepalingen van de bijzondere wetten die op hen van toepassing zijn, zijn de in § 1 bedoelde Belgische autoriteiten en instellingen, wat de vertrouwelijke informatie betreft die zij van de FSMA ontvangen met toepassing van § 1, gebonden door het beroepsgeheim als bedoeld in artikel 74.

§ 5. Dit artikel is van toepassing onverminderd de meer restrictieve bepalingen van het recht van de Europese Unie inzake het beroepsgeheim of de bijzondere wetten waarin de opdracht van de FSMA is vastgelegd.

Artikel 1/1

Deze wet voorziet in de gedeeltelijke omzetting van volgende richtlijnen:

1° Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148;

2° Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie.

Artikel 14

§ 1. Onverminderd zijn wettelijke bevoegdheden, heeft het Instituut de volgende taken met betrekking tot elektronische communicatienetwerken en elektronische communicatiediensten, eindapparatuur, radioapparatuur, met betrekking tot de sector digitale infrastructuur in de zin van de **wet van [xx xxxx xxxx] tot vaststelling van een kader**

BESTAANDE TEKST

de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met betrekking tot de sectoren elektronische communicatie en digitale infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur, met betrekking tot het tegengaan van de verspreiding van terroristische online-inhoud in de zin van de Verordening (EU) 2021/784 van het Europees Parlement en Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud, met betrekking tot artikel XI.216/2, § 2, van het Wetboek van economisch recht, en met betrekking tot postdiensten en openbare postnetwerken zoals gedefinieerd door artikel 2 van de wet van 26 januari 2018 betreffende de postdiensten:

1° het formuleren van adviezen op eigen initiatief, in de gevallen waarin de wetten en besluiten erin voorzien of op verzoek van de minister of van de Kamer van volksvertegenwoordigers;

2° het nemen van administratieve beslissingen;

3° het toezicht op de naleving van de volgende normen en van de uitvoeringsbesluiten ervan:

a) de wet van 13 juni 2005 betreffende de elektronische communicatie;

b) Titel I, hoofdstuk X, en Titel III van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;

c) de wet van 26 januari 2018 betreffende de postdiensten met uitzondering van de artikelen 3, § 2, vijfde lid, 5, § 1, 5/2, 5/3, 5/4, 5/5 en 10/1;

d) de artikelen 14, § 2, 2°, 15 en 21, §§ 5 tot en met 7, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;

ONTWERP VAN WET

voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met betrekking tot de sectoren elektronische communicatie en digitale infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur, met betrekking tot het tegengaan van de verspreiding van terroristische online-inhoud in de zin van de Verordening (EU) 2021/784 van het Europees Parlement en Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud, met betrekking tot artikel XI.216/2, § 2, van het Wetboek van economisch recht, en met betrekking tot postdiensten en openbare postnetwerken zoals gedefinieerd door artikel 2 van de wet van 26 januari 2018 betreffende de postdiensten:

1° het formuleren van adviezen op eigen initiatief, in de gevallen waarin de wetten en besluiten erin voorzien of op verzoek van de minister of van de Kamer van volksvertegenwoordigers;

2° het nemen van administratieve beslissingen;

3° het toezicht op de naleving van de volgende normen en van de uitvoeringsbesluiten ervan:

a) de wet van 13 juni 2005 betreffende de elektronische communicatie;

b) Titel I, hoofdstuk X, en Titel III van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;

c) de wet van 26 januari 2018 betreffende de postdiensten met uitzondering van de artikelen 3, § 2, vijfde lid, 5, § 1, 5/2, 5/3, 5/4, 5/5 en 10/1;

d) de artikelen 14, § 2, 2°, 15 en 21, §§ 5 tot en met 7, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;

BESTAANDE TEKST

e) de artikelen 4 en 4/1 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;

f) de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad;

g) de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, wat de sectoren elektronische communicatie en digitale infrastructuur betreft;

h) de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met betrekking tot de sector digitale infrastructuur;

i) de Verordening (EU) 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie;

j) elke bindende rechtshandeling in het Europese Unierecht, die opdrachten toewijst aan de nationale regelgevende instantie in de sector van de post of elektronische communicatie;

k) elk bindend besluit aangenomen door:

i) het Instituut;

ii) de ministers op basis van artikel 105, § 6, eerste lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

ONTWERP VAN WET

e) de artikelen 4 en 4/1 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;

f) de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad;

g) de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur, wat de sectoren elektronische communicatie en digitale infrastructuur betreft;

h) de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, voor wat betreft de taken toegewezen aan de sectorale overheid en de sectorale inspectiedienst voor de sector digitaal infrastructuur, met uitzondering van de verleners van vertrouwensdiensten in de zin van artikel 8, 24° van dezelfde wet;

i) de Verordening (EU) 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie;

j) elke bindende rechtshandeling in het Europese Unierecht, die opdrachten toewijst aan de nationale regelgevende instantie in de sector van de post of elektronische communicatie;

k) elk bindend besluit aangenomen door:

i) het Instituut;

ii) de ministers op basis van artikel 105, § 6, eerste lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

BESTAANDE TEKST

iii) de Europese Commissie in de sector van de elektronische communicatie of in de postsector;

l) de Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud, onverminderd de taken die aan andere bevoegde autoriteiten zijn toevertrouwd krachtens artikel 12, lid 1, a) en b), van die verordening.

Voor de toepassing van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wordt het Instituut aangewezen als sectorale overheid en inspectiedienst voor de sector digitale infrastructuur. De Koning kan de praktische inspectiemodaliteiten voor deze sector bepalen, na advies van het Instituut.

4° in geval van een geschil tussen aanbieders van elektronische-communicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, (of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten,) het formuleren van voorstellen om de partijen te verzoenen binnen de termijn van één maand. De Koning legt de nadere regels van die procedure vast op advies van het Instituut;

4° /1 in geval van geschil tussen aanbieders van elektronische-communicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten of in het geval van het uitblijven van akkoord in de zin van artikel

ONTWERP VAN WET

iii) de Europese Commissie in de sector van de elektronische communicatie of in de postsector;

l) de Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud, onverminderd de taken die aan andere bevoegde autoriteiten zijn toevertrouwd krachtens artikel 12, lid 1, a) en b), van die verordening.

Voor de toepassing van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wordt het Instituut aangewezen als sectorale overheid in de zin van artikel 8, 54° van dezelfde wet en de sectorale inspectiedienst in de zin van artikel 44, § 1, tweede lid, van dezelfde wet voor de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten in de zin van artikel 8, 24°, van dezelfde wet, en voor de sector post- en koeriersdiensten.

4° in geval van een geschil tussen aanbieders van elektronische-communicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, (of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten,) het formuleren van voorstellen om de partijen te verzoenen binnen de termijn van één maand. De Koning legt de nadere regels van die procedure vast op advies van het Instituut;

4° /1 in geval van geschil tussen aanbieders van elektronische-communicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten of in het geval van het uitblijven van akkoord in de zin van artikel

BESTAANDE TEKST

XI.216/2, § 2, van het Wetboek van economisch recht, het nemen van een administratieve beslissing op basis van artikel 4 of 4/1 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;

5° het stellen van alle nuttige daden die als doel hebben de voorbereiding van de toepassing van inwerking getreden Europese richtlijnen in de sectoren post en telecommunicatie.

6° Het Instituut houdt toezicht op de uitvoering van de opdrachten van openbare dienst die door de Staat uitbesteed worden in de postsector en in de sector van de elektronische communicatie, onder voorbehoud van de opdrachten van openbare dienst toegekend in het kader van artikel 141, § 1bis, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven]². Het Instituut informeert zowel de Minister bevoegd voor de Postsector als de minister bevoegd voor Overheidsbedrijven over de uitvoering van het beheerscontract;

7° het uitoefenen van de toezichts- en sanctieopdrachten uit die hem zijn toevertrouwd bij het koninklijk besluit dat voorziet in de uitvoering van artikel 5, § 2, van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit.

§ 2. In het kader van zijn bevoegdheden :

1° kan het Instituut op een niet discriminerende wijze alle onderzoeken en openbare raadplegingen organiseren; het moet dergelijke openbare raadplegingen organiseren zodat het rekening houdt met de standpunten van de eindgebruikers, consumenten (met inbegrip van met name consumenten met een handicap), fabrikanten en ondernemingen die

ONTWERP VAN WET

XI.216/2, § 2, van het Wetboek van economisch recht, het nemen van een administratieve beslissing op basis van artikel 4 of 4/1 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;

5° het stellen van alle nuttige daden die als doel hebben de voorbereiding van de toepassing van inwerking getreden Europese richtlijnen in de sectoren post en telecommunicatie.

6° Het Instituut houdt toezicht op de uitvoering van de opdrachten van openbare dienst die door de Staat uitbesteed worden in de postsector en in de sector van de elektronische communicatie, onder voorbehoud van de opdrachten van openbare dienst toegekend in het kader van artikel 141, § 1bis, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven]². Het Instituut informeert zowel de Minister bevoegd voor de Postsector als de minister bevoegd voor Overheidsbedrijven over de uitvoering van het beheerscontract;

7° het uitoefenen van de toezichts- en sanctieopdrachten uit die hem zijn toevertrouwd bij het koninklijk besluit dat voorziet in de uitvoering van artikel 5, § 2, van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit.

§ 2. In het kader van zijn bevoegdheden :

1° kan het Instituut op een niet discriminerende wijze alle onderzoeken en openbare raadplegingen organiseren; het moet dergelijke openbare raadplegingen organiseren zodat het rekening houdt met de standpunten van de eindgebruikers, consumenten (met inbegrip van met name consumenten met een handicap), fabrikanten en ondernemingen die

BESTAANDE TEKST

elektronische-communicatienetwerken en/of -diensten aanbieden over aangelegenheden die verband houden met alle eindgebruikers- en consumentenrechten met betrekking tot openbare elektronische-communicatiediensten, met name wanneer zij een belangrijke invloed hebben op de markt; deze raadplegingen waarborgen dat bij de besluitvorming van het Instituut inzake vraagstukken die verband houden met de rechten van eindgebruikers en consumenten wat openbare elektronische-communicatiediensten betreft het op passende wijze rekening houdt met de belangen van de consumenten op het gebied van elektronische communicatie;

2° kan het Instituut van elke betrokken persoon op gemotiveerde wijze alle nuttige informatie opvragen. Het Instituut bepaalt de termijn waarbinnen de inlichtingen moeten worden meegedeeld;

3° werkt het Instituut samen met en verstrekt het informatie aan :

a) de Europese Commissie, ENISA, het Bureau en aan Berec;

b) de buitenlandse regulerende instanties voor postdiensten en telecommunicatie;

c) de regulerende instanties in de overige economische sectoren;

d) de federale overheidsdiensten die belast zijn met consumentenbescherming;

e) de Belgische instanties die belast zijn met mededinging.

De Koning kan, na raadpleging van deze instanties en van het Instituut en op gezamenlijk voorstel van de minister die bevoegd is voor Economie en van de minister de nadere regels vastleggen inzake samenwerking, raadpleging en uitwisseling van informatie tussen deze instanties en het Instituut;

ONTWERP VAN WET

elektronische-communicatienetwerken en/of -diensten aanbieden over aangelegenheden die verband houden met alle eindgebruikers- en consumentenrechten met betrekking tot openbare elektronische-communicatiediensten, met name wanneer zij een belangrijke invloed hebben op de markt; deze raadplegingen waarborgen dat bij de besluitvorming van het Instituut inzake vraagstukken die verband houden met de rechten van eindgebruikers en consumenten wat openbare elektronische-communicatiediensten betreft het op passende wijze rekening houdt met de belangen van de consumenten op het gebied van elektronische communicatie;

2° kan het Instituut van elke betrokken persoon op gemotiveerde wijze alle nuttige informatie opvragen. Het Instituut bepaalt de termijn waarbinnen de inlichtingen moeten worden meegedeeld;

3° werkt het Instituut samen met en verstrekt het informatie aan :

a) de Europese Commissie, ENISA, het Bureau en aan Berec;

b) de buitenlandse regulerende instanties voor postdiensten en telecommunicatie;

c) de regulerende instanties in de overige economische sectoren;

d) de federale overheidsdiensten die belast zijn met consumentenbescherming;

e) de Belgische instanties die belast zijn met mededinging.

De Koning kan, na raadpleging van deze instanties en van het Instituut en op gezamenlijk voorstel van de minister die bevoegd is voor Economie en van de minister de nadere regels vastleggen inzake samenwerking, raadpleging en uitwisseling van informatie tussen deze instanties en het Instituut;

BESTAANDE TEKST

f) de regulerende instanties van Gemeenschappen en Gewesten en dit volgens de nadere regels die werden afgesproken in samenwerkingsakkoorden met deze beleidsniveaus;

g) de openbare diensten die bevoegd zijn op het stuk van openbare veiligheid, met inbegrip van de beveiliging van netwerk- en informatiesystemen, of civiele veiligheid en bescherming, of civiele verdediging, of crisisplanning, of veiligheid of bescherming van het economische en wetenschappelijke potentieel van het land;

h) de Gegevensbeschermingsautoriteit;

i) de federale overheidsdienst die belast is met statistiek en economische informatie;

j) de ministers bedoeld in artikel 105, § 1, derde lid, 1°, van de wet van 13 juni 2005 betreffende de elektronische communicatie en hun kabinet, voor de uitvoering van dit artikel;

k) het federaal parket en de bevoegde autoriteiten van de andere lidstaten bedoeld in Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud;

k) de sociaal inspecteurs van de Algemene Directie Toezicht op de Sociale Wetten van de Federale Overheidsdienst Werkgelegenheid, Arbeid en Sociaal Overleg, de sociaal inspecteurs van de Rijksdienst voor Sociale Zekerheid, en de sociaal inspecteurs van de Rijksdienst voor Arbeidsvoorziening en de sociaal inspecteurs van het Rijksinstituut voor de sociale verzekeringen der zelfstandigen;

l) de ambtenaren van de Algemene Directie Economische Inspectie van de Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie;

4° verleent het Instituut zijn medewerking aan de gemengde Commissie voor

ONTWERP VAN WET

f) de regulerende instanties van Gemeenschappen en Gewesten en dit volgens de nadere regels die werden afgesproken in samenwerkingsakkoorden met deze beleidsniveaus;

g) de openbare diensten die bevoegd zijn op het stuk van openbare veiligheid, met inbegrip van de beveiliging van netwerk- en informatiesystemen, of civiele veiligheid en bescherming, of civiele verdediging, of crisisplanning, of veiligheid of bescherming van het economische en wetenschappelijke potentieel van het land;

h) de Gegevensbeschermingsautoriteit;

i) de federale overheidsdienst die belast is met statistiek en economische informatie;

j) de ministers bedoeld in artikel 105, § 1, derde lid, 1°, van de wet van 13 juni 2005 betreffende de elektronische communicatie en hun kabinet, voor de uitvoering van dit artikel;

k) het federaal parket en de bevoegde autoriteiten van de andere lidstaten bedoeld in Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud;

k) de sociaal inspecteurs van de Algemene Directie Toezicht op de Sociale Wetten van de Federale Overheidsdienst Werkgelegenheid, Arbeid en Sociaal Overleg, de sociaal inspecteurs van de Rijksdienst voor Sociale Zekerheid, en de sociaal inspecteurs van de Rijksdienst voor Arbeidsvoorziening en de sociaal inspecteurs van het Rijksinstituut voor de sociale verzekeringen der zelfstandigen;

l) de ambtenaren van de Algemene Directie Economische Inspectie van de Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie;

4° verleent het Instituut zijn medewerking aan de gemengde Commissie voor

BESTAANDE TEKST

telecommunicatie, opgericht bij het koninklijk besluit van 10 december 1957 en gewijzigd bij het koninklijk besluit van 24 september 1993;

5° kan het Instituut enkel besluiten nemen met betrekking tot die elektronische communicatienetwerken waarvoor de gemeenschappen eveneens bevoegd zijn nadat er omtrent de uitoefening van bevoegdheden met betrekking tot deze elektronische communicatienetwerken een samenwerkingsakkoord met de Gemeenschappen in werking is getreden.

6° mag het Instituut, mits de redenen voor de nietigverklaring worden geëerbiedigd en de omvang van het toepassingsgebied niet wordt gewijzigd, overgaan tot de vervanging van een door een rechterlijke autoriteit vernietigd besluit wanneer, wegens die nietigverklaring, één of meer doelstellingen beoogd in artikel 6 van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 35 van de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad niet langer worden gehaald. Het Instituut kan in een dergelijke vervanging tevens voorzien wanneer het vernietigde besluit betrekking heeft op de postsector en één of meer van de volgende doelstellingen niet langer worden gehaald :

- waken over de kwaliteit en het voortbestaan van de universele dienst;
- waken over de belangen van de gebruikers van postdiensten;
- bijdragen tot de ontwikkeling van een interne markt voor postdiensten;
- het bevorderen van de concurrentie in de postsector;

7° kan, in de hoedanigheid van inspectiedienst, de mededeling van het beveiligingsplan van de exploitant eisen op elk moment, in afwijking van artikel 25, § 2, van de wet van 1 juli 2011

ONTWERP VAN WET

telecommunicatie, opgericht bij het koninklijk besluit van 10 december 1957 en gewijzigd bij het koninklijk besluit van 24 september 1993;

5° kan het Instituut enkel besluiten nemen met betrekking tot die elektronische communicatienetwerken waarvoor de gemeenschappen eveneens bevoegd zijn nadat er omtrent de uitoefening van bevoegdheden met betrekking tot deze elektronische communicatienetwerken een samenwerkingsakkoord met de Gemeenschappen in werking is getreden.

6° mag het Instituut, mits de redenen voor de nietigverklaring worden geëerbiedigd en de omvang van het toepassingsgebied niet wordt gewijzigd, overgaan tot de vervanging van een door een rechterlijke autoriteit vernietigd besluit wanneer, wegens die nietigverklaring, één of meer doelstellingen beoogd in artikel 6 van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 35 van de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad niet langer worden gehaald. Het Instituut kan in een dergelijke vervanging tevens voorzien wanneer het vernietigde besluit betrekking heeft op de postsector en één of meer van de volgende doelstellingen niet langer worden gehaald :

- waken over de kwaliteit en het voortbestaan van de universele dienst;
- waken over de belangen van de gebruikers van postdiensten;
- bijdragen tot de ontwikkeling van een interne markt voor postdiensten;
- het bevorderen van de concurrentie in de postsector;

7° kan, in de hoedanigheid van inspectiedienst, de mededeling van het beveiligingsplan van de exploitant eisen op elk moment, in afwijking van artikel 25, § 2, van de wet van 1 juli 2011

BESTAANDE TEKST

betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

§ 3. In het kader van de samenwerking met de in de vorige paragraaf onder punt 3 opgesomde instanties kunnen de leden van de Raad en de leden van het personeel van het Instituut vertrouwelijke informatie waarvan ze kennis hebben in het kader van de uitvoering van hun functie, meedelen aan deze instanties, voor zover deze mededeling noodzakelijk is voor de uitvoering van de opdrachten van deze autoriteiten.

ONTWERP VAN WET

betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

§ 3. In het kader van de samenwerking met de in de vorige paragraaf onder punt 3 opgesomde instanties kunnen de leden van de Raad en de leden van het personeel van het Instituut vertrouwelijke informatie waarvan ze kennis hebben in het kader van de uitvoering van hun functie, meedelen aan deze instanties, voor zover deze mededeling noodzakelijk is voor de uitvoering van de opdrachten van deze autoriteiten.

Wet van 13 juni 2005 betreffende de elektronische communicatie**Artikel 1**

Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

Deze wet voorziet in de gedeeltelijke omzetting van volgende richtlijnen:

1° Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische-communicatie ("Privacy- en elektronische communicatierichtlijn") (PbEG 31 juli 2002, L 201/37);

2° Richtlijn 2002/77/EG van de Commissie van 16 september 2002 betreffende de mededinging op de markten voor elektronische-communicatienetwerken en -diensten ("Mededingingsrichtlijn") (PbEG 17 september 2002, L 249/21);

3° Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG;

4° Richtlijn 2014/61/EU van het Europees Parlement en de Raad van 15 mei 2014 inzake

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

Deze wet voorziet in de gedeeltelijke omzetting van volgende richtlijnen:

1° Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische-communicatie ("Privacy- en elektronische communicatierichtlijn") (PbEG 31 juli 2002, L 201/37);

2° Richtlijn 2002/77/EG van de Commissie van 16 september 2002 betreffende de mededinging op de markten voor elektronische-communicatienetwerken en -diensten ("Mededingingsrichtlijn") (PbEG 17 september 2002, L 249/21);

3° Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG;

4° Richtlijn 2014/61/EU van het Europees Parlement en de Raad van 15 mei 2014 inzake

BESTAANDE TEKST

maatregelen ter verlaging van de kosten van de aanleg van elektronische communicatienetwerken met hoge snelheid;

5° Richtlijn (EU) 2018/1808 van het Europees Parlement en de Raad van 14 november 2018 tot wijziging van Richtlijn 2010/13/EU betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten (richtlijn "audiovisuele mediadiensten") in het licht van een veranderende marktsituatie;

6° Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie.

ONTWERP VAN WET

maatregelen ter verlaging van de kosten van de aanleg van elektronische communicatienetwerken met hoge snelheid;

5° Richtlijn (EU) 2018/1808 van het Europees Parlement en de Raad van 14 november 2018 tot wijziging van Richtlijn 2010/13/EU betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten (richtlijn "audiovisuele mediadiensten") in het licht van een veranderende marktsituatie;

6° Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie;

7° Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148.

Artikel 2

Voor de toepassing van deze wet wordt verstaan onder :

1° " Instituut " : Het Belgisch Instituut voor postdiensten en telecommunicatie zoals bedoeld in artikel 13 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;

2° " minister " : de ministers of staatssecretaris die bevoegd zijn voor de aangelegenheden die de elektronische communicatie betreffen als bedoeld in deze wet;

3° "elektronische-communicatienetwerk": de transmissiesystemen, al dan niet gebaseerd op een permanente infrastructuur of gecentraliseerde beheercapaciteit, en in voorkomend geval de schakel- of

Artikel 2

Voor de toepassing van deze wet wordt verstaan onder :

1° " Instituut " : Het Belgisch Instituut voor postdiensten en telecommunicatie zoals bedoeld in artikel 13 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;

2° " minister " : de ministers of staatssecretaris die bevoegd zijn voor de aangelegenheden die de elektronische communicatie betreffen als bedoeld in deze wet;

3° "elektronische-communicatienetwerk": de transmissiesystemen, al dan niet gebaseerd op een permanente infrastructuur of gecentraliseerde beheercapaciteit, en in voorkomend geval de schakel- of

BESTAANDE TEKST

routeringsapparatuur en andere middelen, waaronder netwerk-elementen die niet actief zijn, die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen waaronder satellietnetwerken, vaste (circuit- en pakketgeschakelde, met inbegrip van internet) en mobiele netwerken, elektriciteitsnetten voor zover deze voor overdracht van andere signalen dan die voor audiovisuele en auditieve mediadiensten worden gebruikt;

3/1° "netwerk met zeer hoge capaciteit": hetzij een netwerk voor elektronische communicatie dat ten minste tot aan het distributiepunt volledig uit optische-vezelelementen bestaat, hetzij een elektronischecommunicatienetwerk dat, in gebruikelijke piekomstandigheden, in staat is om soortgelijke netwerkprestaties te bieden wat betreft downlink- en uplinkbandbreedte, veerkrachtigheid van het netwerk, parameters met betrekking tot fouten, latentietijden en de veranderingen daarin; de netwerkprestaties kunnen ook als vergelijkbaar worden beschouwd als de eindgebruiker een andere gebruikservaring heeft vanwege de inherent verschillende kenmerken van het medium dat op het netwerk wordt aangesloten;

4° "aanbieden van een elektronischecommunicatienetwerk": het bouwen, exploiteren, toezicht houden op of beschikbaar stellen van een elektronisch communicatienetwerk;

5° "elektronische-communicatiedienst": een gewoonlijk tegen vergoeding via elektronischecommunicatienetwerken aangeboden dienst, die, met uitzondering van diensten waarbij met behulp van elektronischecommunicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd en met uitzondering van audiovisuele en auditieve mediadiensten, de volgende soorten diensten omvat:

a) internettoegangsdienst;

ONTWERP VAN WET

routeringsapparatuur en andere middelen, waaronder netwerk-elementen die niet actief zijn, die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen waaronder satellietnetwerken, vaste (circuit- en pakketgeschakelde, met inbegrip van internet) en mobiele netwerken, elektriciteitsnetten voor zover deze voor overdracht van andere signalen dan die voor audiovisuele en auditieve mediadiensten worden gebruikt;

3/1° "netwerk met zeer hoge capaciteit": hetzij een netwerk voor elektronische communicatie dat ten minste tot aan het distributiepunt volledig uit optische-vezelelementen bestaat, hetzij een elektronischecommunicatienetwerk dat, in gebruikelijke piekomstandigheden, in staat is om soortgelijke netwerkprestaties te bieden wat betreft downlink- en uplinkbandbreedte, veerkrachtigheid van het netwerk, parameters met betrekking tot fouten, latentietijden en de veranderingen daarin; de netwerkprestaties kunnen ook als vergelijkbaar worden beschouwd als de eindgebruiker een andere gebruikservaring heeft vanwege de inherent verschillende kenmerken van het medium dat op het netwerk wordt aangesloten;

4° "aanbieden van een elektronischecommunicatienetwerk": het bouwen, exploiteren, toezicht houden op of beschikbaar stellen van een elektronisch communicatienetwerk;

5° "elektronische-communicatiedienst": een gewoonlijk tegen vergoeding via elektronischecommunicatienetwerken aangeboden dienst, die, met uitzondering van diensten waarbij met behulp van elektronischecommunicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd en met uitzondering van audiovisuele en auditieve mediadiensten, de volgende soorten diensten omvat:

a) internettoegangsdienst;

BESTAANDE TEKST

b) interpersoonlijke communicatiedienst; en

c) diensten die geheel of hoofdzakelijk bestaan in het overbrengen van signalen zoals transmissiediensten die voor het verlenen van intermachinale diensten worden gebruikt;

5/1° "internettoegangsdienst": een voor het publiek beschikbare elektronische-communicatiedienst die toegang tot het internet biedt en derhalve connectiviteit met vrijwel alle eindpunten van het internet, ongeacht de gebruikte netwerktechnologie en eindapparatuur;

5/2° "interpersoonlijke communicatiedienst": een gewoonlijk tegen vergoeding aangeboden dienst die directe persoonlijke en interactieve uitwisseling van informatie via elektronische-communicatienetwerken tussen een eindig aantal personen mogelijk maakt, waarbij de personen die de communicatie starten of eraan deelnemen, bepalen welke de ontvangers zijn, en die geen diensten omvat die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst;

5/3° "nummergebaseerde interpersoonlijke communicatiedienst": een interpersoonlijke communicatiedienst die verbinding maakt met openbaar toegewezen nummervoorraden, namelijk een nummer of een aantal nummers in nationale of internationale nummerplannen, of die communicatie mogelijk maakt met een nummer of een aantal nummers in nationale of internationale nummerplannen;

5/4° "nummeronafhankelijke interpersoonlijke communicatiedienst": een interpersoonlijke communicatiedienst die geen verbinding maakt met openbaar toegewezen nummervoorraden, namelijk een nummer of een aantal nummers in nationale of internationale nummerplannen, of die geen communicatie mogelijk maakt met een nummer of een aantal nummers in nationale of internationale nummerplannen;

ONTWERP VAN WET

b) interpersoonlijke communicatiedienst; en

c) diensten die geheel of hoofdzakelijk bestaan in het overbrengen van signalen zoals transmissiediensten die voor het verlenen van intermachinale diensten worden gebruikt;

5/1° "internettoegangsdienst": een voor het publiek beschikbare elektronische-communicatiedienst die toegang tot het internet biedt en derhalve connectiviteit met vrijwel alle eindpunten van het internet, ongeacht de gebruikte netwerktechnologie en eindapparatuur;

5/2° "interpersoonlijke communicatiedienst": een gewoonlijk tegen vergoeding aangeboden dienst die directe persoonlijke en interactieve uitwisseling van informatie via elektronische-communicatienetwerken tussen een eindig aantal personen mogelijk maakt, waarbij de personen die de communicatie starten of eraan deelnemen, bepalen welke de ontvangers zijn, en die geen diensten omvat die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst;

5/3° "nummergebaseerde interpersoonlijke communicatiedienst": een interpersoonlijke communicatiedienst die verbinding maakt met openbaar toegewezen nummervoorraden, namelijk een nummer of een aantal nummers in nationale of internationale nummerplannen, of die communicatie mogelijk maakt met een nummer of een aantal nummers in nationale of internationale nummerplannen;

5/4° "nummeronafhankelijke interpersoonlijke communicatiedienst": een interpersoonlijke communicatiedienst die geen verbinding maakt met openbaar toegewezen nummervoorraden, namelijk een nummer of een aantal nummers in nationale of internationale nummerplannen, of die geen communicatie mogelijk maakt met een nummer of een aantal nummers in nationale of internationale nummerplannen;

BESTAANDE TEKST

5/5° "fraude": een oneerlijke daad gepleegd met de bedoeling om te misleiden, indruisend tegen de wet, de reglementen of een contract, om voor zichzelf of iemand anders een onrechtmatig voordeel te verkrijgen, ten nadele van de operator of eindgebruiker, via het gebruik van een elektronische-communicatiedienst;

5/6° "kwaadwillig gebruik van het netwerk of van de dienst": gebruik van het elektronische-communicatienetwerk of van de elektronische-communicatiedienst om overlast te veroorzaken aan zijn correspondent of om schade te berokkenen;

6° " verkeersgegevens " : gegeven dat wordt verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor het factureren van een dergelijke communicatie;

7° "informatie over de locatie van de oproeper": in een openbaar mobiel netwerk, de verwerkte gegevens, afkomstig van netwerkinfrastructuur of van handsets, waaruit de geografische positie van de mobiele eindapparatuur van een eindgebruiker blijkt en, in een openbaar vast netwerk, de gegevens over het fysieke adres van het netwerkaansluitpunt;

8° " dienst met verkeersgegevens " : een dienst die een bijzondere behandeling van de verkeersgegevens vereist die verder gaat dan wat strikt noodzakelijk is voor het versturen of aanrekenen van de communicatie;

9° " dienst met locatiegegevens " : een dienst die een bijzondere behandeling van de locatiegegevens vereist die verder gaat dan wat strikt noodzakelijk is voor het versturen of aanrekenen van de communicatie;

10° " openbaar elektronische-communicatienetwerk " : een elektronische-communicatienetwerk dat geheel of hoofdzakelijk wordt gebruikt om voor het publiek beschikbare elektronische-communicatiediensten aan te bieden ter

ONTWERP VAN WET

5/5° "fraude": een oneerlijke daad gepleegd met de bedoeling om te misleiden, indruisend tegen de wet, de reglementen of een contract, om voor zichzelf of iemand anders een onrechtmatig voordeel te verkrijgen, ten nadele van de operator of eindgebruiker, via het gebruik van een elektronische-communicatiedienst;

5/6° "kwaadwillig gebruik van het netwerk of van de dienst": gebruik van het elektronische-communicatienetwerk of van de elektronische-communicatiedienst om overlast te veroorzaken aan zijn correspondent of om schade te berokkenen;

6° " verkeersgegevens " : gegeven dat wordt verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor het factureren van een dergelijke communicatie;

7° "informatie over de locatie van de oproeper": in een openbaar mobiel netwerk, de verwerkte gegevens, afkomstig van netwerkinfrastructuur of van handsets, waaruit de geografische positie van de mobiele eindapparatuur van een eindgebruiker blijkt en, in een openbaar vast netwerk, de gegevens over het fysieke adres van het netwerkaansluitpunt;

8° " dienst met verkeersgegevens " : een dienst die een bijzondere behandeling van de verkeersgegevens vereist die verder gaat dan wat strikt noodzakelijk is voor het versturen of aanrekenen van de communicatie;

9° " dienst met locatiegegevens " : een dienst die een bijzondere behandeling van de locatiegegevens vereist die verder gaat dan wat strikt noodzakelijk is voor het versturen of aanrekenen van de communicatie;

10° " openbaar elektronische-communicatienetwerk " : een elektronische-communicatienetwerk dat geheel of hoofdzakelijk wordt gebruikt om voor het publiek beschikbare elektronische-communicatiediensten aan te bieden ter

BESTAANDE TEKST

ondersteuning van de overdracht van informatie tussen netwerkaansluitpunten;

10/1° "elektronische-communicatienetwerk met hoge snelheid" : een elektronische-communicatienetwerk dat breedbandtoegangsdiens ten kan leveren met snelheden van minstens 30 Mbps;

11° "operator": persoon of onderneming die een openbaar elektronische-communicatienetwerk of een voor het publiek beschikbare elektronische-communicatiedienst aanbiedt;

11/1° "beheerder van passieve infrastructu ren": een economische speler die, enerzijds, een dienst levert van productie, transport of distributie van gas, van elektriciteit (straatverlichting inbegrepen) of van water (de verwijdering of verwerking en zuivering van afval- en rioolwater, en drainagesystemen inbegrepen); van verwarming; of die transportdiensten verstrekt (met inbegrip van spoorwegen, wegen, havens en luchthavens), en die anderzijds elementen van zijn netwerk ter beschikking stelt zonder dat deze zelf actieve elementen van een elektronische-communicatienetwerk worden;

11/2° "algemene machtiging": regelgeving waarbij rechten worden verleend voor het aanbieden van elektronische-communicatienetwerken of -diensten en specifieke sectorgebonden verplichtingen worden vastgesteld die kunnen gelden voor alle of voor specifieke soorten elektronische-communicatienetwerken en -diensten;

12° " gebruiker " : een natuurlijke of rechtspersoon die gebruik maakt van of verzoekt om een voor het publiek beschikbare elektronische-communicatiedienst;

13° " eindgebruiker " : een gebruiker die geen openbaar elektronische-communicatienetwerk of voor het publiek beschikbare elektronische-communicatiediensten aanbiedt;

ONTWERP VAN WET

ondersteuning van de overdracht van informatie tussen netwerkaansluitpunten;

10/1° "elektronische-communicatienetwerk met hoge snelheid" : een elektronische-communicatienetwerk dat breedbandtoegangsdiens ten kan leveren met snelheden van minstens 30 Mbps;

11° "operator": persoon of onderneming die een openbaar elektronische-communicatienetwerk of een voor het publiek beschikbare elektronische-communicatiedienst aanbiedt;

11/1° "beheerder van passieve infrastructu ren": een economische speler die, enerzijds, een dienst levert van productie, transport of distributie van gas, van elektriciteit (straatverlichting inbegrepen) of van water (de verwijdering of verwerking en zuivering van afval- en rioolwater, en drainagesystemen inbegrepen); van verwarming; of die transportdiensten verstrekt (met inbegrip van spoorwegen, wegen, havens en luchthavens), en die anderzijds elementen van zijn netwerk ter beschikking stelt zonder dat deze zelf actieve elementen van een elektronische-communicatienetwerk worden;

11/2° "algemene machtiging": regelgeving waarbij rechten worden verleend voor het aanbieden van elektronische-communicatienetwerken of -diensten en specifieke sectorgebonden verplichtingen worden vastgesteld die kunnen gelden voor alle of voor specifieke soorten elektronische-communicatienetwerken en -diensten;

12° " gebruiker " : een natuurlijke of rechtspersoon die gebruik maakt van of verzoekt om een voor het publiek beschikbare elektronische-communicatiedienst;

13° " eindgebruiker " : een gebruiker die geen openbaar elektronische-communicatienetwerk of voor het publiek beschikbare elektronische-communicatiediensten aanbiedt;

BESTAANDE TEKST

14° "consument" : een natuurlijke persoon die gebruik maakt van of verzoekt om een voor het publiek beschikbare elektronische-communicatiedienst voor andere doeleinden dan deze in het kader van zijn bedrijfs- of beroepsdoeleinden;

14/1° "micro-onderneming": onderneming die het jaargemiddelde van 9 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:24 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;

14/2° "kleine onderneming": onderneming die het jaargemiddelde van 49 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:24 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;

14/3° "middelgrote onderneming": onderneming die het jaargemiddelde van 249 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:24 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;

14/4° "micro-organisatie zonder winstoogmerk": vereniging zonder winstoogmerk, internationale vereniging zonder winstoogmerk of stichting die het jaargemiddelde van 9 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:28 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;

14/5° "kleine organisatie zonder winstoogmerk": vereniging zonder winstoogmerk, internationale vereniging zonder winstoogmerk of stichting die het jaargemiddelde van 49 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:28 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;

15° "abonnee" : een natuurlijke of rechtspersoon die geen operator is en die partij is bij een overeenkomst met een operator, die voor het publiek beschikbare elektronische-communicatiediensten aanbiedt voor de levering van die diensten;

ONTWERP VAN WET

14° "consument" : een natuurlijke persoon die gebruik maakt van of verzoekt om een voor het publiek beschikbare elektronische-communicatiedienst voor andere doeleinden dan deze in het kader van zijn bedrijfs- of beroepsdoeleinden;

14/1° "micro-onderneming": onderneming die het jaargemiddelde van 9 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:24 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;

14/2° "kleine onderneming": onderneming die het jaargemiddelde van 49 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:24 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;

14/3° "middelgrote onderneming": onderneming die het jaargemiddelde van 249 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:24 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;

14/4° "micro-organisatie zonder winstoogmerk": vereniging zonder winstoogmerk, internationale vereniging zonder winstoogmerk of stichting die het jaargemiddelde van 9 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:28 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;

14/5° "kleine organisatie zonder winstoogmerk": vereniging zonder winstoogmerk, internationale vereniging zonder winstoogmerk of stichting die het jaargemiddelde van 49 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:28 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;

15° "abonnee" : een natuurlijke of rechtspersoon die geen operator is en die partij is bij een overeenkomst met een operator, die voor het publiek beschikbare elektronische-communicatiediensten aanbiedt voor de levering van die diensten;

BESTAANDE TEKST

15/1° "abonnee met maximum 9 werknemers": abonnee die het jaargemiddelde van 9 tewerkgestelde werknemers, berekend overeenkomstig, naar gelang het geval, artikel 1:24 of 1:28 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;

16° "netwerkaansluitpunt": het fysieke punt waarop een eindgebruiker de toegang tot een openbaar elektronische-communicatienetwerk wordt geboden; in het geval van netwerken met schakelings- of routeringsfuncties wordt het netwerkaansluitpunt bepaald door middel van een specifiek netwerkadres dat met een nummer of naam van een eindgebruiker kan zijn verbonden;

16/1° "toegangspunt" : een in of buiten het gebouw gelegen fysiek punt dat toegankelijk is voor operatoren, waar het netwerk kan worden aangesloten op de voor hoge snelheid bestemde fysieke binnenhuisinfrastructuur;

17° "bijbehorende faciliteiten": de bij een elektronische-communicatienetwerk of een elektronische-communicatiedienst behorende diensten, fysieke infrastructuur en andere faciliteiten of elementen die het aanbieden van diensten via dat netwerk of dienst mogelijk maken of ondersteunen of het potentieel hiertoe bezitten en onder meer gebouwen of toegangen tot gebouwen, bekabeling van gebouwen, antennes, torens en andere ondersteunende constructies, kabelgoten, kabelbuizen, masten, mangaten en straatkasten omvatten;

17/1° "bijbehorende dienst": een bij een elektronische-communicatienetwerk of een elektronische-communicatiedienst behorende dienst die het aanbieden, het zelf verstrekken of het geautomatiseerd aanbieden van diensten via dat netwerk of dienst mogelijk maakt of ondersteunt of het potentieel hiertoe bezit en onder meer nummervertaalsystemen of systemen met soortgelijke functies en voorwaardelijke-toegangssystemen en elektronische programmagidsen, kort "EPG's",

ONTWERP VAN WET

15/1° "abonnee met maximum 9 werknemers": abonnee die het jaargemiddelde van 9 tewerkgestelde werknemers, berekend overeenkomstig, naar gelang het geval, artikel 1:24 of 1:28 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;

16° "netwerkaansluitpunt": het fysieke punt waarop een eindgebruiker de toegang tot een openbaar elektronische-communicatienetwerk wordt geboden; in het geval van netwerken met schakelings- of routeringsfuncties wordt het netwerkaansluitpunt bepaald door middel van een specifiek netwerkadres dat met een nummer of naam van een eindgebruiker kan zijn verbonden;

16/1° "toegangspunt" : een in of buiten het gebouw gelegen fysiek punt dat toegankelijk is voor operatoren, waar het netwerk kan worden aangesloten op de voor hoge snelheid bestemde fysieke binnenhuisinfrastructuur;

17° "bijbehorende faciliteiten": de bij een elektronische-communicatienetwerk of een elektronische-communicatiedienst behorende diensten, fysieke infrastructuur en andere faciliteiten of elementen die het aanbieden van diensten via dat netwerk of dienst mogelijk maken of ondersteunen of het potentieel hiertoe bezitten en onder meer gebouwen of toegangen tot gebouwen, bekabeling van gebouwen, antennes, torens en andere ondersteunende constructies, kabelgoten, kabelbuizen, masten, mangaten en straatkasten omvatten;

17/1° "bijbehorende dienst": een bij een elektronische-communicatienetwerk of een elektronische-communicatiedienst behorende dienst die het aanbieden, het zelf verstrekken of het geautomatiseerd aanbieden van diensten via dat netwerk of dienst mogelijk maakt of ondersteunt of het potentieel hiertoe bezit en onder meer nummervertaalsystemen of systemen met soortgelijke functies en voorwaardelijke-toegangssystemen en elektronische programmagidsen, kort "EPG's",

BESTAANDE TEKST

alsmede andere diensten zoals identiteit, locatie en presentie-informatiediensten omvat (met uitzondering van diensten en systemen die uitsluitend worden gebruikt voor audiovisuele of auditieve mediadiensten);

17/2° "fysieke binnenhuisinfrastructuur" : elk element van een netwerk, zoals buizen, masten, kabelgoten, inspectieputten, mangaten, straatkasten, gebouwen of ingangen in gebouwen, antenne-installaties, torens en palen (buiten kabels, met inbegrip van ongebruikte glasvezels (dark fibre)), alsook installaties op de locatie van de eindgebruiker, met inbegrip van elementen die gemeenschappelijk eigendom zijn, die bestemd zijn om elementen van vaste of draadloze toegangsnetwerken onder te brengen zonder dat ze zelf een actief element van het netwerk worden, voor zover die netwerken elektronische-communicatiediensten kunnen leveren en het toegangspunt van het gebouw kunnen aansluiten op het aansluitpunt van het netwerk;

17/3° "nomadiciteit": eigenschap van een elektronische-communicatiedienst waardoor deze dienst gebruikt kan worden vanuit potentieel om het even welke aansluiting op een elektronische-communicatienetwerk;

18° "toegang" : het beschikbaar stellen aan een operator van faciliteiten en/of diensten onder uitdrukkelijke voorwaarden, hetzij op exclusieve hetzij op niet-exclusieve basis, met het oog op het aanbieden van elektronische-communicatiediensten of het aanbieden van diensten van de informatiemaatschappij. Deze term omvat met name toegang tot netwerkelementen en verwante faciliteiten waarbij eventueel apparatuur kan worden verbonden met vaste of niet-vaste middelen (dit houdt met name toegang in tot het aansluitnet en tot faciliteiten en diensten die noodzakelijk zijn om diensten te kunnen aanbieden via het aansluitnet); toegang tot materiële infrastructuur waaronder gebouwen, kabelgoten en masten; toegang tot relevante programmatuursystemen waaronder operationele ondersteuningssystemen; toegang

ONTWERP VAN WET

alsmede andere diensten zoals identiteit, locatie en presentie-informatiediensten omvat (met uitzondering van diensten en systemen die uitsluitend worden gebruikt voor audiovisuele of auditieve mediadiensten);

17/2° "fysieke binnenhuisinfrastructuur" : elk element van een netwerk, zoals buizen, masten, kabelgoten, inspectieputten, mangaten, straatkasten, gebouwen of ingangen in gebouwen, antenne-installaties, torens en palen (buiten kabels, met inbegrip van ongebruikte glasvezels (dark fibre)), alsook installaties op de locatie van de eindgebruiker, met inbegrip van elementen die gemeenschappelijk eigendom zijn, die bestemd zijn om elementen van vaste of draadloze toegangsnetwerken onder te brengen zonder dat ze zelf een actief element van het netwerk worden, voor zover die netwerken elektronische-communicatiediensten kunnen leveren en het toegangspunt van het gebouw kunnen aansluiten op het aansluitpunt van het netwerk;

17/3° "nomadiciteit": eigenschap van een elektronische-communicatiedienst waardoor deze dienst gebruikt kan worden vanuit potentieel om het even welke aansluiting op een elektronische-communicatienetwerk;

18° "toegang" : het beschikbaar stellen aan een operator van faciliteiten en/of diensten onder uitdrukkelijke voorwaarden, hetzij op exclusieve hetzij op niet-exclusieve basis, met het oog op het aanbieden van elektronische-communicatiediensten of het aanbieden van diensten van de informatiemaatschappij. Deze term omvat met name toegang tot netwerkelementen en verwante faciliteiten waarbij eventueel apparatuur kan worden verbonden met vaste of niet-vaste middelen (dit houdt met name toegang in tot het aansluitnet en tot faciliteiten en diensten die noodzakelijk zijn om diensten te kunnen aanbieden via het aansluitnet); toegang tot materiële infrastructuur waaronder gebouwen, kabelgoten en masten; toegang tot relevante programmatuursystemen waaronder operationele ondersteuningssystemen; toegang

BESTAANDE TEKST

tot informatiesystemen of databases voor reservering, levering, bestelling, onderhouds- en herstelverzoeken en facturering; toegang tot nummervertaling of systemen met vergelijkbare functionaliteit; toegang tot vaste en mobiele netwerken, met name voor roaming; toegang tot virtuele netwerkdiensten;

19° "interconnectie": een specifiek type toegang dat tussen operatoren van openbare netwerken wordt gerealiseerd door het fysiek en logisch verbinden van openbare elektronische-communicatienetwerken die door dezelfde of een andere onderneming worden gebruikt om het de gebruikers van een onderneming mogelijk te maken te communiceren met die van dezelfde of van een andere onderneming of toegang te hebben tot diensten die door een andere onderneming worden aangeboden, wanneer die diensten worden aangeboden door de betrokken partijen of andere partijen die toegang hebben tot het netwerk;

20° "interface" : een netwerkaansluitpunt en/of een radio-interface en de bijhorende technische specificaties;

21° [...];

22° "spraakcommunicatiedienst": een voor het publiek beschikbare elektronische-communicatiedienst voor direct of indirect uitgaande en binnenkomende nationale of internationale gesprekken, met behulp van een nummer of een aantal nummers in een nationaal of internationaal nummerplan;

22/1° oproep " : door middel van een voor het publiek beschikbare interpersoonlijke communicatiedienst tot stand gebrachte verbinding die tweewegspraak-communicatie mogelijk maakt;

22/2° "dienst voor totale conversatie": een multimediale dienst voor in werkelijke tijd conversatie die bidirectionele symmetrische in werkelijke tijd overdracht van videofilm, realtime tekst en stem tussen gebruikers in twee of meer locaties biedt;

ONTWERP VAN WET

tot informatiesystemen of databases voor reservering, levering, bestelling, onderhouds- en herstelverzoeken en facturering; toegang tot nummervertaling of systemen met vergelijkbare functionaliteit; toegang tot vaste en mobiele netwerken, met name voor roaming; toegang tot virtuele netwerkdiensten;

19° "interconnectie": een specifiek type toegang dat tussen operatoren van openbare netwerken wordt gerealiseerd door het fysiek en logisch verbinden van openbare elektronische-communicatienetwerken die door dezelfde of een andere onderneming worden gebruikt om het de gebruikers van een onderneming mogelijk te maken te communiceren met die van dezelfde of van een andere onderneming of toegang te hebben tot diensten die door een andere onderneming worden aangeboden, wanneer die diensten worden aangeboden door de betrokken partijen of andere partijen die toegang hebben tot het netwerk;

20° "interface" : een netwerkaansluitpunt en/of een radio-interface en de bijhorende technische specificaties;

21° [...];

22° "spraakcommunicatiedienst": een voor het publiek beschikbare elektronische-communicatiedienst voor direct of indirect uitgaande en binnenkomende nationale of internationale gesprekken, met behulp van een nummer of een aantal nummers in een nationaal of internationaal nummerplan;

22/1° oproep " : door middel van een voor het publiek beschikbare interpersoonlijke communicatiedienst tot stand gebrachte verbinding die tweewegspraak-communicatie mogelijk maakt;

22/2° "dienst voor totale conversatie": een multimediale dienst voor in werkelijke tijd conversatie die bidirectionele symmetrische in werkelijke tijd overdracht van videofilm, realtime tekst en stem tussen gebruikers in twee of meer locaties biedt;

BESTAANDE TEKST

23° " aansluitnetwerk " : een fysiek pad dat door elektronische-communicatiesignalen wordt gebruikt en het netwerkaansluitpunt verbindt met een verdeler of een soortgelijke voorziening in het vaste voor het publiek beschikbare elektronische-communicatienetwerk;

24° subnetwerk " : gedeelte van een aansluitnetwerk dat het netwerkaansluitpunt verbindt met een concentratiepunt of een ander bepaald tussenliggend aansluitpunt gelegen in het vaste openbare elektronische-communicatienetwerk;

25° " volledig ontbundelde toegang tot het aansluitnetwerk " : het verlenen van toegang tot het aansluitnetwerk of het subnetwerk van een onderneming met aanmerkelijke marktmacht op een relevante markt, waarbij toestemming wordt verleend voor het gebruik van de volledige capaciteit van netwerkinfrastructuur;

26° " toegang tot binair debiet " : toegang die bestaat uit het verlenen van transportcapaciteit met de bijbehorende schakeling naar een gebruiker waarbij de toegangsleverancier de interface bij de gebruiker vastlegt;

27° " gedeelde toegang tot het aansluitnetwerk " : het verlenen van toegang tot het aansluitnetwerk of het subnetwerk van een onderneming met aanmerkelijke marktmacht op een relevante markt, waarbij toestemming wordt verleend voor het gebruik van een gespecificeerd deel van de capaciteit van de netwerkinfrastructuur, zoals een deel van de frequentie of iets gelijkwaardigs;

28° " ontbundelde toegang tot het aansluitnetwerk " : het verlenen van volledig ontbundelde toegang of gedeelde toegang tot het aansluitnetwerk, wat geen verandering behelst in de eigendom van het aansluitnetwerk;

29° " co-locatie " : het leveren van fysieke ruimte en technische faciliteiten, nodig om het installeren en aansluiten van apparatuur van een

ONTWERP VAN WET

23° " aansluitnetwerk " : een fysiek pad dat door elektronische-communicatiesignalen wordt gebruikt en het netwerkaansluitpunt verbindt met een verdeler of een soortgelijke voorziening in het vaste voor het publiek beschikbare elektronische-communicatienetwerk;

24° subnetwerk " : gedeelte van een aansluitnetwerk dat het netwerkaansluitpunt verbindt met een concentratiepunt of een ander bepaald tussenliggend aansluitpunt gelegen in het vaste openbare elektronische-communicatienetwerk;

25° " volledig ontbundelde toegang tot het aansluitnetwerk " : het verlenen van toegang tot het aansluitnetwerk of het subnetwerk van een onderneming met aanmerkelijke marktmacht op een relevante markt, waarbij toestemming wordt verleend voor het gebruik van de volledige capaciteit van netwerkinfrastructuur;

26° " toegang tot binair debiet " : toegang die bestaat uit het verlenen van transportcapaciteit met de bijbehorende schakeling naar een gebruiker waarbij de toegangsleverancier de interface bij de gebruiker vastlegt;

27° " gedeelde toegang tot het aansluitnetwerk " : het verlenen van toegang tot het aansluitnetwerk of het subnetwerk van een onderneming met aanmerkelijke marktmacht op een relevante markt, waarbij toestemming wordt verleend voor het gebruik van een gespecificeerd deel van de capaciteit van de netwerkinfrastructuur, zoals een deel van de frequentie of iets gelijkwaardigs;

28° " ontbundelde toegang tot het aansluitnetwerk " : het verlenen van volledig ontbundelde toegang of gedeelde toegang tot het aansluitnetwerk, wat geen verandering behelst in de eigendom van het aansluitnetwerk;

29° " co-locatie " : het leveren van fysieke ruimte en technische faciliteiten, nodig om het installeren en aansluiten van apparatuur van een

BESTAANDE TEKST

operator onder redelijke voorwaarden mogelijk te maken in het kader van een referentieaanbod;

29/1° " kabelgoot " : omhulsel dat dient om glasvezel-, telefoon- en/of coaxkabels en/of netwerkfaciliteiten te laten passeren en te beschermen;

30° " huurlijn " : elektronische-communicatiedienst bestaande uit de levering van communicatiefaciliteiten met behulp waarvan transparante transmissiecapaciteit tussen netwerkaansluitpunten wordt geboden, met uitzondering van de schakeling op aanvraag;

31° " radiogolven " : elektromagnetische golven die zich in de ruimte voortplanten zonder kunstmatige geleider, en waarvan de frequentie onder 3000 GHz ligt;

32° [...];

33° " radiospectrum " : het geheel van de radiogolven;

33/1° "radiospectrumtoewijzing": de aanwijzing van een specifieke radiospectrumband voor gebruik door een of meer soorten radiocommunicatiediensten, in voorkomend geval onder duidelijk omschreven voorwaarden;

33/2° "nationaal frequentietoewijzingsplan": document dat voor elke band van het radiospectrum de informatie bevat in verband met de toewijzingen van het radiospectrum en de toegestane toepassingen;

33/3° "geharmoniseerd radiospectrum": radiospectrum waarvoor geharmoniseerde voorwaarden in verband met de beschikbaarheid en het doelmatig gebruik ervan zijn vastgesteld door middel van technische uitvoeringsmaatregelen overeenkomstig artikel 4 van Beschikking nr. 676/2002/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een regelgevingskader voor het radio-spectrumbeleid in de Europese Gemeenschap, hierna te noemen "Radiospectrumbeschikking";

ONTWERP VAN WET

operator onder redelijke voorwaarden mogelijk te maken in het kader van een referentieaanbod;

29/1° " kabelgoot " : omhulsel dat dient om glasvezel-, telefoon- en/of coaxkabels en/of netwerkfaciliteiten te laten passeren en te beschermen;

30° " huurlijn " : elektronische-communicatiedienst bestaande uit de levering van communicatiefaciliteiten met behulp waarvan transparante transmissiecapaciteit tussen netwerkaansluitpunten wordt geboden, met uitzondering van de schakeling op aanvraag;

31° " radiogolven " : elektromagnetische golven die zich in de ruimte voortplanten zonder kunstmatige geleider, en waarvan de frequentie onder 3000 GHz ligt;

32° [...];

33° " radiospectrum " : het geheel van de radiogolven;

33/1° "radiospectrumtoewijzing": de aanwijzing van een specifieke radiospectrumband voor gebruik door een of meer soorten radiocommunicatiediensten, in voorkomend geval onder duidelijk omschreven voorwaarden;

33/2° "nationaal frequentietoewijzingsplan": document dat voor elke band van het radiospectrum de informatie bevat in verband met de toewijzingen van het radiospectrum en de toegestane toepassingen;

33/3° "geharmoniseerd radiospectrum": radiospectrum waarvoor geharmoniseerde voorwaarden in verband met de beschikbaarheid en het doelmatig gebruik ervan zijn vastgesteld door middel van technische uitvoeringsmaatregelen overeenkomstig artikel 4 van Beschikking nr. 676/2002/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een regelgevingskader voor het radio-spectrumbeleid in de Europese Gemeenschap, hierna te noemen "Radiospectrumbeschikking";

BESTAANDE TEKST

33/4° "gedeeld gebruik van radiospectrum": toegang door twee of meer gebruikers om gebruik te maken van dezelfde radiospectrumbanden in het kader van een bepaalde regeling inzake gedeeld gebruik, toegestaan op basis van een algemene machtiging, gebruiksrechten voor radiospectrum of een combinatie daarvan, met inbegrip van regelgevingsbenaderingen, zoals vergunningsplichtige gedeelde toegang, die als doel hebben het gedeeld gebruik van een radiospectrumband te vergemakkelijken, en onderworpen aan een bindende overeenkomst tussen alle betrokken partijen, overeenkomstig de regels inzake gedeeld gebruik die zijn opgenomen in hun gebruiksrechten voor radiospectrum, zodat aan alle gebruikers voorspelbare en betrouwbare regelingen inzake delen kunnen worden gewaarborgd, en zonder afbreuk te doen aan de toepassing van het mededingingsrecht;

33/5° "gebruiksrechten voor radiospectrum": individuele gebruiksrechten voor radiospectrum die geheel of gedeeltelijk gebruikt worden voor het aanbieden van openbare elektronische-communicatienetwerken of voor het publiek beschikbare elektronische-communicatiediensten;

34° "radiocommunicatie": communicatie door middel van radiogolven, met uitsluiting van de exclusieve transmissie van signalen van audiovisuele en auditieve mediadiensten;

35° [...];

36° [...];

37° [...];

38° "radiostation": radioapparatuur, eventueel aangevuld met antennes alsook alle onderdelen die nodig zijn om het geheel te laten functioneren, dat doelbewust radiogolven uitzendt of ontvangt ten behoeve van radiocommunicatie of radiodeterminatie;

ONTWERP VAN WET

33/4° "gedeeld gebruik van radiospectrum": toegang door twee of meer gebruikers om gebruik te maken van dezelfde radiospectrumbanden in het kader van een bepaalde regeling inzake gedeeld gebruik, toegestaan op basis van een algemene machtiging, gebruiksrechten voor radiospectrum of een combinatie daarvan, met inbegrip van regelgevingsbenaderingen, zoals vergunningsplichtige gedeelde toegang, die als doel hebben het gedeeld gebruik van een radiospectrumband te vergemakkelijken, en onderworpen aan een bindende overeenkomst tussen alle betrokken partijen, overeenkomstig de regels inzake gedeeld gebruik die zijn opgenomen in hun gebruiksrechten voor radiospectrum, zodat aan alle gebruikers voorspelbare en betrouwbare regelingen inzake delen kunnen worden gewaarborgd, en zonder afbreuk te doen aan de toepassing van het mededingingsrecht;

33/5° "gebruiksrechten voor radiospectrum": individuele gebruiksrechten voor radiospectrum die geheel of gedeeltelijk gebruikt worden voor het aanbieden van openbare elektronische-communicatienetwerken of voor het publiek beschikbare elektronische-communicatiediensten;

34° "radiocommunicatie": communicatie door middel van radiogolven, met uitsluiting van de exclusieve transmissie van signalen van audiovisuele en auditieve mediadiensten;

35° [...];

36° [...];

37° [...];

38° "radiostation": radioapparatuur, eventueel aangevuld met antennes alsook alle onderdelen die nodig zijn om het geheel te laten functioneren, dat doelbewust radiogolven uitzendt of ontvangt ten behoeve van radiocommunicatie of radiodeterminatie;

BESTAANDE TEKST

38/1° "radionet": het geheel samengesteld uit verscheidene radiostations die met elkaar in verbinding mogen treden binnen de grenzen van een vergunning voor private radiocommunicatie of een gebruiksrecht voor radiospectrum;

38/2° "vergunning voor private radiocommunicatie": vergunning om een radiostation of een radionetwerk te mogen gebruiken voor andere doeleinden dan het aanbieden van openbare elektronische-communicatienetwerken of voor het publiek beschikbare elektronische-communicatiediensten;

38/3° "omroepstation": radioapparatuur, eventueel aangevuld met de bijbehorende antennes alsook alle onderdelen die nodig zijn om het geheel te laten functioneren, dat doelbewust radiogolven uitzendt of ontvangt ten behoeve van het aanbieden van audiovisuele en auditieve mediadiensten;

38/4° "storing": effect op de ontvangst in een radiocommunicatiesysteem van een niet-gewenste energie, te wijten aan een uitzending, aan een straling of aan een inductie (of aan een combinatie van die uitzendingen, stralingen of inducties), dat zich manifesteert door een verslechtering van de transmissiekwiteit, een vervorming of een verlies van informatie die men had kunnen verkrijgen indien die niet-gewenste energie er niet was geweest;

39° "schadelijke storing": storing die het functioneren van een radionavigatiedienst of van andere veiligheidsdiensten in gevaar brengt, of die een overeenkomstig de van toepassing zijnde voorschriften werkende radiocommunicatiedienst, dienst voor de verstrekking van audiovisuele en auditieve mediadiensten of elektronische-communicatiedienst ernstig verslechtert, hindert of herhaaldelijk onderbreekt;

40° "versleuteling": alle diensten die de beginselen, middelen en methodes voor de omzetting van gegevens aanwenden met de bedoeling de semantische inhoud ervan te

ONTWERP VAN WET

38/1° "radionet": het geheel samengesteld uit verscheidene radiostations die met elkaar in verbinding mogen treden binnen de grenzen van een vergunning voor private radiocommunicatie of een gebruiksrecht voor radiospectrum;

38/2° "vergunning voor private radiocommunicatie": vergunning om een radiostation of een radionetwerk te mogen gebruiken voor andere doeleinden dan het aanbieden van openbare elektronische-communicatienetwerken of voor het publiek beschikbare elektronische-communicatiediensten;

38/3° "omroepstation": radioapparatuur, eventueel aangevuld met de bijbehorende antennes alsook alle onderdelen die nodig zijn om het geheel te laten functioneren, dat doelbewust radiogolven uitzendt of ontvangt ten behoeve van het aanbieden van audiovisuele en auditieve mediadiensten;

38/4° "storing": effect op de ontvangst in een radiocommunicatiesysteem van een niet-gewenste energie, te wijten aan een uitzending, aan een straling of aan een inductie (of aan een combinatie van die uitzendingen, stralingen of inducties), dat zich manifesteert door een verslechtering van de transmissiekwiteit, een vervorming of een verlies van informatie die men had kunnen verkrijgen indien die niet-gewenste energie er niet was geweest;

39° "schadelijke storing": storing die het functioneren van een radionavigatiedienst of van andere veiligheidsdiensten in gevaar brengt, of die een overeenkomstig de van toepassing zijnde voorschriften werkende radiocommunicatiedienst, dienst voor de verstrekking van audiovisuele en auditieve mediadiensten of elektronische-communicatiedienst ernstig verslechtert, hindert of herhaaldelijk onderbreekt;

40° "versleuteling": alle diensten die de beginselen, middelen en methodes voor de omzetting van gegevens aanwenden met de bedoeling de semantische inhoud ervan te

BESTAANDE TEKST

verbergen, de authenticiteit ervan vast te stellen, te verhinderen dat zij onopgemerkt worden gewijzigd, te verhinderen dat zij worden verworpen en te verhinderen dat zij zonder toestemming worden gebruikt;

41° "eindapparatuur":

a) de apparaten die voor overbrenging, verwerking of ontvangst van informatie direct of indirect op de interface van een openbaar elektronische-communicatienetwerk zijn aangesloten; in beide gevallen, direct of indirect, kan de aansluiting geschieden per draad, per optische vezel of via elektromagnetische golven; een aansluiting is indirect wanneer een apparaat geplaatst is tussen de eindapparatuur en de interface van het net;

b) satellietgrondstationapparatuur;

42° "radioapparatuur" : elektrisch of elektronisch product dat doelbewust radiogolven uitzendt en/of ontvangt ten behoeve van radiocommunicatie, verstrekking, van audiovisuele en auditieve mediadiensten of radiodeterminatie, of elektrisch of elektronisch product dat moet worden aangevuld met een accessoire, zoals een antenne, om doelbewust radiogolven uit te zenden of ontvangen ten behoeve van radiocommunicatie, verstrekking van audiovisuele en auditieve mediadiensten en/of radiodeterminatie;

43° " apparatuur " : alle producten die als radioapparatuur of als eindapparatuur, of als beide fungeren;

44° " technische specificatie " : de omschrijving van de kenmerken van alle elektronische-communicatiediensten die via het netwerkaansluitpunt of de radiointerface verstrekt worden;

45° " nummeringsruimte " : het geheel van nummers, adressen en namen die aangewend worden om operatoren of gebruikers te identificeren;

ONTWERP VAN WET

verbergen, de authenticiteit ervan vast te stellen, te verhinderen dat zij onopgemerkt worden gewijzigd, te verhinderen dat zij worden verworpen en te verhinderen dat zij zonder toestemming worden gebruikt;

41° "eindapparatuur":

a) de apparaten die voor overbrenging, verwerking of ontvangst van informatie direct of indirect op de interface van een openbaar elektronische-communicatienetwerk zijn aangesloten; in beide gevallen, direct of indirect, kan de aansluiting geschieden per draad, per optische vezel of via elektromagnetische golven; een aansluiting is indirect wanneer een apparaat geplaatst is tussen de eindapparatuur en de interface van het net;

b) satellietgrondstationapparatuur;

42° "radioapparatuur" : elektrisch of elektronisch product dat doelbewust radiogolven uitzendt en/of ontvangt ten behoeve van radiocommunicatie, verstrekking, van audiovisuele en auditieve mediadiensten of radiodeterminatie, of elektrisch of elektronisch product dat moet worden aangevuld met een accessoire, zoals een antenne, om doelbewust radiogolven uit te zenden of ontvangen ten behoeve van radiocommunicatie, verstrekking van audiovisuele en auditieve mediadiensten en/of radiodeterminatie;

43° " apparatuur " : alle producten die als radioapparatuur of als eindapparatuur, of als beide fungeren;

44° " technische specificatie " : de omschrijving van de kenmerken van alle elektronische-communicatiediensten die via het netwerkaansluitpunt of de radiointerface verstrekt worden;

45° " nummeringsruimte " : het geheel van nummers, adressen en namen die aangewend worden om operatoren of gebruikers te identificeren;

BESTAANDE TEKST

46 " geografisch nummer " : een nummer van het nationale nummerplan waarvan een deel van de cijferstructuur een geografische betekenis heeft die wordt gebruikt voor het routeren van gesprekken naar de fysieke locatie van het netwerkaansluitpunt;

47° " niet-geografisch nummer " : een nummer van het nationale nummerplan dat geen geografisch nummer is; het betreft hier onder meer nummers voor mobiele oproepen, nummers die gratis zijn voor de oproepers en betaalnummers;

48° " nummeroverdraagbaarheid " : de faciliteit die het de abonnees ... mogelijk maakt hun nummer te behouden, ongeacht de operator die de dienst levert, binnen een welbepaald geografisch gebied in geval van een geografisch nummer en op ongeacht welke locatie in geval van andere dan geografische nummers; de faciliteit omvat niet de mogelijkheid om het nationale telefoonnummer te behouden tussen een operator van voor het publiek beschikbare telefoondiensten aangeboden op een vaste locatie en een operator van openbare telefoondiensten aangeboden op een mobiel elektronisch communicatienetwerk;

48/1° " Internetdomeinnaamregistreerbureau " : een entiteit die een register van domeinnamen bijhoudt en die een systeem uitbaat zodat deze domeinnamen kunnen worden gebruikt om toegang te krijgen tot Internet- protocol-adressen of andere informatie via het Internet;

48/2° " universele dienst " : het minimumpakket van diensten als gedefinieerd in artikel 68 van

ONTWERP VAN WET

46 " geografisch nummer " : een nummer van het nationale nummerplan waarvan een deel van de cijferstructuur een geografische betekenis heeft die wordt gebruikt voor het routeren van gesprekken naar de fysieke locatie van het netwerkaansluitpunt;

47° " niet-geografisch nummer " : een nummer van het nationale nummerplan dat geen geografisch nummer is; het betreft hier onder meer nummers voor mobiele oproepen, nummers die gratis zijn voor de oproepers en betaalnummers;

48° " nummeroverdraagbaarheid " : de faciliteit die het de abonnees ... mogelijk maakt hun nummer te behouden, ongeacht de operator die de dienst levert, binnen een welbepaald geografisch gebied in geval van een geografisch nummer en op ongeacht welke locatie in geval van andere dan geografische nummers; de faciliteit omvat niet de mogelijkheid om het nationale telefoonnummer te behouden tussen een operator van voor het publiek beschikbare telefoondiensten aangeboden op een vaste locatie en een operator van openbare telefoondiensten aangeboden op een mobiel elektronisch communicatienetwerk;

48/1° "register voor topleveldomeinnamen": een entiteit waaraan een specifieke topleveldomeinnaam is gedelegeerd en die verantwoordelijk is voor het beheer van de topleveldomeinnaam, met inbegrip van de registratie van domeinnamen onder de topleveldomeinnaam en de technische exploitatie van de topleveldomeinnaam, met inbegrip van de exploitatie van de naamsservers, het onderhoud van de databases en de verdeling van de zonebestanden van de topleveldomeinnaam over de naamsservers, ongeacht of die activiteiten door de entiteit zelf worden uitgevoerd of worden uitbesteed, maar met uitzondering van situaties waarin topleveldomeinnamen uitsluitend voor eigen gebruik worden aangewend door een register;

48/2° " universele dienst " : het minimumpakket van diensten als gedefinieerd in artikel 68 van

BESTAANDE TEKST

een bepaalde kwaliteit dat voor alle gebruikers, ongeacht hun geografische locatie, beschikbaar is voor een in het licht van specifieke nationale omstandigheden betaalbare prijs;

ONTWERP VAN WET

een bepaalde kwaliteit dat voor alle gebruikers, ongeacht hun geografische locatie, beschikbaar is voor een in het licht van specifieke nationale omstandigheden betaalbare prijs;

48/3° "entiteit die domeinnaamregistratiediensten aanbiedt": een registrator of een agent die namens registrators optreedt, zoals een aanbieder van privacy- of proxy-registratiediensten of wederverkoper;

49° " telefoongids " : boek, lijst of bestand dat of die hoofdzakelijk of uitsluitend gegevens bevat over de abonnees van een openbare telefoondienst en die beschikbaar wordt gesteld voor het publiek om uitsluitend of hoofdzakelijk de oproepnummers van de eindgebruikers te kunnen identificeren;

49° " telefoongids " : boek, lijst of bestand dat of die hoofdzakelijk of uitsluitend gegevens bevat over de abonnees van een openbare telefoondienst en die beschikbaar wordt gesteld voor het publiek om uitsluitend of hoofdzakelijk de oproepnummers van de eindgebruikers te kunnen identificeren;

50° [...]

50° [...]

51° " antenne " : een onderdeel van een apparaat of radiostation voor het uitstralen en/of opvangen van radiogolven;

51° " antenne " : een onderdeel van een apparaat of radiostation voor het uitstralen en/of opvangen van radiogolven;

52° " basisstation " : een radiostation van een elektronische-communicatienetwerk opgesteld en gebruikt op een bepaalde plaats en bestemd voor radiodekking van een gegeven geografische zone;

52° " basisstation " : een radiostation van een elektronische-communicatienetwerk opgesteld en gebruikt op een bepaalde plaats en bestemd voor radiodekking van een gegeven geografische zone;

53° " steun " : structuur waarop antennes van basisstations kunnen worden geplaatst;

53° " steun " : structuur waarop antennes van basisstations kunnen worden geplaatst;

54° " antennesite " : geheel van constructies dat ten minste één steun, één antenne en lokalen omvat voor de elektrische en elektronische apparatuur, dat de installatie en de exploitatie van een of meer basisstations mogelijk maakt;

54° " antennesite " : geheel van constructies dat ten minste één steun, één antenne en lokalen omvat voor de elektrische en elektronische apparatuur, dat de installatie en de exploitatie van een of meer basisstations mogelijk maakt;

55° " nationale raming " : de mogelijkheid voor een operator om zijn klanten in staat te stellen in hetzelfde land toegang te krijgen tot de basisdiensten die verstrekt worden door een andere operator van een mobiel communicatienetwerk;

55° " nationale raming " : de mogelijkheid voor een operator om zijn klanten in staat te stellen in hetzelfde land toegang te krijgen tot de basisdiensten die verstrekt worden door een andere operator van een mobiel communicatienetwerk;

BESTAANDE TEKST

56° " identificatie van de lijn " : nummer, teken of geheel van tekens dat aan een abonnee, eindgebruiker, gebruiker of eindapparaat is toegewezen, waarmee deze door andere abonnees, eindgebruikers of gebruikers van voor het publiek beschikbare elektronische-communicatienetwerken of -diensten kan worden bereikt;

57° " identificatie van de oproeper " : elk gegeven, rechtstreeks of onrechtstreeks beschikbaar, in de netwerken en diensten van een operator, dat het oproepnummer van het eindapparaat, de naam van de eindgebruiker en de plaats waar de eindapparatuur zich bevindt op het ogenblik van de oproep bepaalt;

58° " nooddienst " : elke overheidsdienst of dienst van openbaar nut zoals gevisieerd in artikel 107, § 1, eerste lid, of vastgesteld door de Koning overeenkomstig artikel 107, § 1, tweede lid, 1°;

59° " noodnummer " : oproepnummer van een nooddienst, bepaald overeenkomstig de procedure in artikel 107, § 1, tweede lid, 2° van deze wet;

60° "noodcommunicatie": communicatie door middel van interpersoonlijke communicatiediensten tussen een eindgebruiker en een PSAP met het doel noodhulp te ontvangen van hulpdiensten;

61° "PSAP" ("Public Safety Answering Point") of "centrale voor het beheer van noodoproepen": de fysieke locatie waar noodcommunicatie initieel wordt ontvangen onder de verantwoordelijkheid van een openbare instantie of een erkende private organisatie;

62° "werkingsgebied van een PSAP": geografisch gebied waarvoor een PSAP alle noodcommunicatie naar de nooddienst beheert, hierna "werkingsgebied" genoemd;

62/1° "meest geschikte PSAP": een PSAP die door de bevoegde instanties is opgericht om

ONTWERP VAN WET

56° " identificatie van de lijn " : nummer, teken of geheel van tekens dat aan een abonnee, eindgebruiker, gebruiker of eindapparaat is toegewezen, waarmee deze door andere abonnees, eindgebruikers of gebruikers van voor het publiek beschikbare elektronische-communicatienetwerken of -diensten kan worden bereikt;

57° " identificatie van de oproeper " : elk gegeven, rechtstreeks of onrechtstreeks beschikbaar, in de netwerken en diensten van een operator, dat het oproepnummer van het eindapparaat, de naam van de eindgebruiker en de plaats waar de eindapparatuur zich bevindt op het ogenblik van de oproep bepaalt;

58° " nooddienst " : elke overheidsdienst of dienst van openbaar nut zoals gevisieerd in artikel 107, § 1, eerste lid, of vastgesteld door de Koning overeenkomstig artikel 107, § 1, tweede lid, 1°;

59° " noodnummer " : oproepnummer van een nooddienst, bepaald overeenkomstig de procedure in artikel 107, § 1, tweede lid, 2° van deze wet;

60° "noodcommunicatie": communicatie door middel van interpersoonlijke communicatiediensten tussen een eindgebruiker en een PSAP met het doel noodhulp te ontvangen van hulpdiensten;

61° "PSAP" ("Public Safety Answering Point") of "centrale voor het beheer van noodoproepen": de fysieke locatie waar noodcommunicatie initieel wordt ontvangen onder de verantwoordelijkheid van een openbare instantie of een erkende private organisatie;

62° "werkingsgebied van een PSAP": geografisch gebied waarvoor een PSAP alle noodcommunicatie naar de nooddienst beheert, hierna "werkingsgebied" genoemd;

62/1° "meest geschikte PSAP": een PSAP die door de bevoegde instanties is opgericht om

BESTAANDE TEKST

noodcommunicatie uit een bepaald gebied of van een bepaald type te behandelen;

62/2° "beveiliging van netwerken en diensten": het vermogen van elektronische-communicatienetwerken en -diensten om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van die netwerken en diensten, van de opgeslagen, verzonden of verwerkte gegevens of van de daaraan gerelateerde diensten die via die elektronische-communicatienetwerken en -diensten worden aangeboden, in gevaar brengen;

62/3° "beveiligingsincident": een gebeurtenis met een daadwerkelijk schadelijk effect op de beveiliging van elektronische-communicatienetwerken of -diensten;

ONTWERP VAN WET

noodcommunicatie uit een bepaald gebied of van een bepaald type te behandelen;

62/2° "netwerk- en informatiesysteem":

a) een elektronische-communicatienetwerk als bedoeld in 3°;

b) elk apparaat of elke groep van onderling verbonden of bij elkaar behorende apparaten, waarvan er een of meer, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische componenten van dat apparaat die met name de automatisering van het operationele proces, de controle op afstand of het verkrijgen van werkingsgegevens in real time mogelijk maken; of

c) digitale gegevens die worden opgeslagen, verwerkt, opgehaald of verzonden met behulp van de in punten a) en b) bedoelde elementen met het oog op de werking, het gebruik, de bescherming en het onderhoud ervan;

62/3° "beveiliging van netwerk- en informatiesystemen": het vermogen van netwerken informatiesystemen om op een bepaald niveau van betrouwbaarheid weerstand te bieden aan elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die door of via deze netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen;

BESTAANDE TEKST**ONTWERP VAN WET**

62/4° “beveiligingsincident”: een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt;

62/5° “cyberbeveiliging”: cyberbeveiliging als bedoeld in artikel 2, 1), van Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening);

62/6° “incidentenbehandeling”: alle acties en procedures die gericht zijn op het voorkomen, opsporen, analyseren en indammen van of het reageren op en het herstellen van een beveiligingsincident;

62/7° “cyberdreiging”: een cyberdreiging als bedoeld in artikel 2, 8), van de cyberbeveiligingsverordening;

62/8° “significante cyberdreiging”: een cyberdreiging waarvan op basis van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerk- en informatiesystemen van een entiteit of de gebruikers van de diensten van de entiteit door het veroorzaken van aanzienlijke materiële of immateriële schade;

63° " erkend revisor " : bedrijfsrevisor ingeschreven op de rol van het Instituut voor Bedrijfsrevisoren;

63° " erkend revisor " : bedrijfsrevisor ingeschreven op de rol van het Instituut voor Bedrijfsrevisoren;

64° " ziekenhuizen " : de instellingen voor gezondheidszorg zoals bepaald in artikel 2 van de wet op de ziekenhuizen, gecoördineerd op 7 augustus 1987;

64° " ziekenhuizen " : de instellingen voor gezondheidszorg zoals bepaald in artikel 2 van de wet op de ziekenhuizen, gecoördineerd op 7 augustus 1987;

BESTAANDE TEKST

65° " scholen " : alle instellingen van het lager, secundair of hoger onderwijs die behoren tot het net van een Gemeenschap, van een provincie, van een gemeente of tot een vrij gesubsidieerd net;

66° " openbare bibliotheken " : elke bibliotheek erkend door de federale Staat of door een Gemeenschap;

67° " openbaar bureau voor elektronische communicatie " : voor het publiek toegankelijke ruimte of inrichting voor de tijdelijke beschikbaarstelling van eindapparatuur waarmee tegen betaling een elektronische-communicatienetwerk of -dienst ter plaatse kan worden gebruikt zonder contractuele betrekking met de leverancier van het netwerk of de dienst.

68° " inbreuk in verband met persoonsgegevens " : een inbreuk op de beveiliging die resulteert in een accidentele of onwettige vernietiging, verlies, wijziging, niet-geautoriseerde vrijgave van of toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een voor het publiek beschikbare elektronische-communicatiedienst in de Gemeenschap;

69° " ENISA " : Europees Agentschap voor netwerk- en informatiebeveiliging opgericht door Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging;

70° "Berec": Orgaan van Europese regelgevende instanties voor elektronische communicatie, in het Engels "Body of European Regulators for Electronic Communications (Berec)", opgericht door Verordening (EU) 2018/1971 van het Europees Parlement en de Raad van 11 december 2018 tot instelling van het Orgaan van Europese regulerende instanties voor elektronische communicatie (Berec) en het Bureau voor ondersteuning van Berec (Berec-Bureau), tot wijziging van Verordening (EU) 2015/2120 en tot intrekking van Verordening

ONTWERP VAN WET

65° " scholen " : alle instellingen van het lager, secundair of hoger onderwijs die behoren tot het net van een Gemeenschap, van een provincie, van een gemeente of tot een vrij gesubsidieerd net;

66° " openbare bibliotheken " : elke bibliotheek erkend door de federale Staat of door een Gemeenschap;

67° " openbaar bureau voor elektronische communicatie " : voor het publiek toegankelijke ruimte of inrichting voor de tijdelijke beschikbaarstelling van eindapparatuur waarmee tegen betaling een elektronische-communicatienetwerk of -dienst ter plaatse kan worden gebruikt zonder contractuele betrekking met de leverancier van het netwerk of de dienst.

68° " inbreuk in verband met persoonsgegevens " : een inbreuk op de beveiliging die resulteert in een accidentele of onwettige vernietiging, verlies, wijziging, niet-geautoriseerde vrijgave van of toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een voor het publiek beschikbare elektronische-communicatiedienst in de Gemeenschap;

69° " ENISA " : Europees Agentschap voor netwerk- en informatiebeveiliging opgericht door Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging;

70° "Berec": Orgaan van Europese regelgevende instanties voor elektronische communicatie, in het Engels "Body of European Regulators for Electronic Communications (Berec)", opgericht door Verordening (EU) 2018/1971 van het Europees Parlement en de Raad van 11 december 2018 tot instelling van het Orgaan van Europese regulerende instanties voor elektronische communicatie (Berec) en het Bureau voor ondersteuning van Berec (Berec-Bureau), tot wijziging van Verordening (EU) 2015/2120 en tot intrekking van Verordening

BESTAANDE TEKST

(EG) nr. 1211/2009, hierna "Verordening (EU) 2018/1971" genoemd;

71° "Bureau": Bureau voor ondersteuning van Berec, ingesteld door de Verordening (EU) 2018/1971;

71/1° "RSPG": Beleidsgroep radiospectrum, in het Engels "Radio Spectrum Policy Group", opgericht bij besluit van de Europese Commissie van 11 juni 2019 tot oprichting van de Beleidsgroep radiospectrum en tot intrekking van Besluit 2002/622/EG;

72° "Prioritair gebruiker" : gebruiker van elektronische-communicatiediensten of -netwerken die door de taken die hij uitoefent of zijn activiteiten een door de overheden erkende belangrijke maatschappelijke functie heeft en die door een gebrek aan toegang tot elektronische-communicatiediensten of -netwerken niet meer in staat is zijn taken of activiteiten adequaat uit te voeren wat tot een toestand kan leiden die de openbare veiligheid, of de civiele veiligheid en de civiele bescherming, of de civiele verdediging, of de crisisplanning, of de veiligheid of de bescherming van het economische en wetenschappelijke potentieel van het land, kan schaden;

73° [...]

74° "oproep poging zonder resultaat": iedere communicatie waarbij een oproep wel werd doorgezonden, maar onbeantwoord is gebleven of door de netwerkbeheerder is beantwoord;

75° "radiodeterminatie" : het vaststellen van de positie, snelheid en/of andere kenmerken van een object of het verkrijgen van informatie over deze parameters door middel van de voortplantingseigenschappen van radiogolven;

76° "op de markt aanbieden" : het in het kader van een handelsactiviteit, al dan niet tegen betaling, verstrekken van radioapparatuur met het oog op distributie, consumptie of gebruik op de markt van de Unie;

ONTWERP VAN WET

(EG) nr. 1211/2009, hierna "Verordening (EU) 2018/1971" genoemd;

71° "Bureau": Bureau voor ondersteuning van Berec, ingesteld door de Verordening (EU) 2018/1971;

71/1° "RSPG": Beleidsgroep radiospectrum, in het Engels "Radio Spectrum Policy Group", opgericht bij besluit van de Europese Commissie van 11 juni 2019 tot oprichting van de Beleidsgroep radiospectrum en tot intrekking van Besluit 2002/622/EG;

72° "Prioritair gebruiker" : gebruiker van elektronische-communicatiediensten of -netwerken die door de taken die hij uitoefent of zijn activiteiten een door de overheden erkende belangrijke maatschappelijke functie heeft en die door een gebrek aan toegang tot elektronische-communicatiediensten of -netwerken niet meer in staat is zijn taken of activiteiten adequaat uit te voeren wat tot een toestand kan leiden die de openbare veiligheid, of de civiele veiligheid en de civiele bescherming, of de civiele verdediging, of de crisisplanning, of de veiligheid of de bescherming van het economische en wetenschappelijke potentieel van het land, kan schaden;

73° [...]

74° "oproep poging zonder resultaat": iedere communicatie waarbij een oproep wel werd doorgezonden, maar onbeantwoord is gebleven of door de netwerkbeheerder is beantwoord;

75° "radiodeterminatie" : het vaststellen van de positie, snelheid en/of andere kenmerken van een object of het verkrijgen van informatie over deze parameters door middel van de voortplantingseigenschappen van radiogolven;

76° "op de markt aanbieden" : het in het kader van een handelsactiviteit, al dan niet tegen betaling, verstrekken van radioapparatuur met het oog op distributie, consumptie of gebruik op de markt van de Unie;

BESTAANDE TEKST

77° "in de handel brengen" : het voor het eerst in de Unie op de markt aanbieden van radioapparatuur;

78° "ingebruikneming" : het eerste gebruik van radioapparatuur in de Unie door de eindgebruiker ervan;

79° "fabrikant" : natuurlijke of rechtspersoon die radioapparatuur vervaardigt of laat ontwerpen of vervaardigen, en deze apparatuur onder zijn naam of merknaam verhandelt;

80° "invoerder" : in de Europese Unie gevestigde natuurlijke of rechtspersoon die radioapparatuur uit een derde land in de Europese Unie in de handel brengt;

81° "distributeur" : natuurlijke of rechtspersoon in de toeleveringsketen, verschillend van de fabrikant of de invoerder, die radioapparatuur op de markt aanbiedt;

82° "terugroepen" : maatregel waarmee wordt beoogd radioapparatuur te doen terugkeren die al aan de eindgebruiker ter beschikking is gesteld;

83° "uit de handel nemen" : maatregel waarmee wordt beoogd te voorkomen dat radioapparatuur die zich in de toeleveringsketen bevindt, op de markt wordt aangeboden;

84° "radio-interface" : specificatie van het gereguleerd gebruik van het radiospectrum;

85° "dienstenaanbieder" : persoon wiens dienst of inhoud geleverd via een elektronische-communicatienetwerk door een operator aan de eindgebruiker in rekening wordt gebracht;

86° "faciliterende operator" : operator die nummers of andere middelen ter beschikking stelt van een dienstenaanbieder, zodat deze een vergoeding voor zijn dienst of inhoud kan laten invorderen via facturatie door een operator of aanrekening op een voorafbetaalde kaart van een operator;

ONTWERP VAN WET

77° "in de handel brengen" : het voor het eerst in de Unie op de markt aanbieden van radioapparatuur;

78° "ingebruikneming" : het eerste gebruik van radioapparatuur in de Unie door de eindgebruiker ervan;

79° "fabrikant" : natuurlijke of rechtspersoon die radioapparatuur vervaardigt of laat ontwerpen of vervaardigen, en deze apparatuur onder zijn naam of merknaam verhandelt;

80° "invoerder" : in de Europese Unie gevestigde natuurlijke of rechtspersoon die radioapparatuur uit een derde land in de Europese Unie in de handel brengt;

81° "distributeur" : natuurlijke of rechtspersoon in de toeleveringsketen, verschillend van de fabrikant of de invoerder, die radioapparatuur op de markt aanbiedt;

82° "terugroepen" : maatregel waarmee wordt beoogd radioapparatuur te doen terugkeren die al aan de eindgebruiker ter beschikking is gesteld;

83° "uit de handel nemen" : maatregel waarmee wordt beoogd te voorkomen dat radioapparatuur die zich in de toeleveringsketen bevindt, op de markt wordt aangeboden;

84° "radio-interface" : specificatie van het gereguleerd gebruik van het radiospectrum;

85° "dienstenaanbieder" : persoon wiens dienst of inhoud geleverd via een elektronische-communicatienetwerk door een operator aan de eindgebruiker in rekening wordt gebracht;

86° "faciliterende operator" : operator die nummers of andere middelen ter beschikking stelt van een dienstenaanbieder, zodat deze een vergoeding voor zijn dienst of inhoud kan laten invorderen via facturatie door een operator of aanrekening op een voorafbetaalde kaart van een operator;

BESTAANDE TEKST

87° "passieve infrastructuur": elk element van een elektronische-communicatienetwerk dat bedoeld is om er andere elementen van een ander elektronische-communicatienetwerk in onder te brengen zonder dat het zelf een actief element van dat laatste netwerk wordt, zoals buizen, masten, kabelgoten, inspectieputten, mangaten, straatkasten, gebouwen of ingangen in gebouwen, antenne-installaties, torens of palen;

88° "centraal informatiepunt": het informatiesysteem ingevoerd binnen het platform van de vzw "KLIM-CICC (Federaal Kabels en Leidingen Informatie Meldpunt - Point de Contact fédéral Information Câbles et Conduites);

89° "MNO": een operator die mobiele elektronische-communicatiediensten aanbiedt en die beschikt over een eigen radiotoegangsnetwerk, alsook over alle nuttige elementen voor de exploitatie van het netwerk;

90° "MVNO": een operator die mobiele elektronische-communicatiediensten aanbiedt zonder MNO te zijn;

91° "elektronische-communicatiegegevens": de inhoud en de metagegevens van elektronische communicatie;

92° "inhoud van elektronische communicatie": de inhoud die wordt uitgewisseld door middel van elektronische-communicatiediensten, met name tekst, spraak, video, beelden en geluid;

93° "elektronische-communicatiemetagegevens": de gegevens die worden verwerkt in een elektronische-communicatienetwerk met het oog op de transmissie, de distributie of de uitwisseling van de inhoud van elektronische communicatie, met inbegrip van gegevens waarmee een communicatie kan worden getraceerd en de bron en de bestemming van de communicatie kunnen worden bepaald, alsmede gegevens betreffende de locatie van de apparatuur die in het kader van het aanbieden van elektronische-

ONTWERP VAN WET

87° "passieve infrastructuur": elk element van een elektronische-communicatienetwerk dat bedoeld is om er andere elementen van een ander elektronische-communicatienetwerk in onder te brengen zonder dat het zelf een actief element van dat laatste netwerk wordt, zoals buizen, masten, kabelgoten, inspectieputten, mangaten, straatkasten, gebouwen of ingangen in gebouwen, antenne-installaties, torens of palen;

88° "centraal informatiepunt": het informatiesysteem ingevoerd binnen het platform van de vzw "KLIM-CICC (Federaal Kabels en Leidingen Informatie Meldpunt - Point de Contact fédéral Information Câbles et Conduites);

89° "MNO": een operator die mobiele elektronische-communicatiediensten aanbiedt en die beschikt over een eigen radiotoegangsnetwerk, alsook over alle nuttige elementen voor de exploitatie van het netwerk;

90° "MVNO": een operator die mobiele elektronische-communicatiediensten aanbiedt zonder MNO te zijn;

91° "elektronische-communicatiegegevens": de inhoud en de metagegevens van elektronische communicatie;

92° "inhoud van elektronische communicatie": de inhoud die wordt uitgewisseld door middel van elektronische-communicatiediensten, met name tekst, spraak, video, beelden en geluid;

93° "elektronische-communicatiemetagegevens": de gegevens die worden verwerkt in een elektronische-communicatienetwerk met het oog op de transmissie, de distributie of de uitwisseling van de inhoud van elektronische communicatie, met inbegrip van gegevens waarmee een communicatie kan worden getraceerd en de bron en de bestemming van de communicatie kunnen worden bepaald, alsmede gegevens betreffende de locatie van de apparatuur die in het kader van het aanbieden van elektronische-

BESTAANDE TEKST

communicatiediensten zijn gegenereerd, en de datum, het tijdstip, de duur en de aard van de communicatie.

ONTWERP VAN WET

communicatiediensten zijn gegenereerd, en de datum, het tijdstip, de duur en de aard van de communicatie.

94° “aanbieder van digitale infrastructuur”: een entiteit die behoort tot de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten, in de zin van artikel 8, 24° van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

Artikel 6

Bij de uitvoering van de taken die aan het Instituut krachtens deze wet zijn opgelegd:

1° bevordert het Instituut de connectiviteit met en de toegang tot, alsmede de benutting van netwerken met een zeer hoge capaciteit, met inbegrip van vaste, mobiele en draadloze netwerken;

2° bevordert het Instituut de mededinging bij het aanbieden van elektronische-communicatienetwerken en bijbehorende faciliteiten, met inbegrip van efficiënte concurrentie op basis van infrastructuur, en bij het aanbieden van elektronische-communicatiediensten en bijbehorende diensten;

3° draagt het Instituut bij tot de ontwikkeling van de interne markt, door het opheffen van resterende belemmeringen voor, en het bevorderen van convergerende voorwaarden voor, investeringen in en het aanbieden van elektronische-communicatienetwerken, elektronische-communicatiediensten, bijbehorende faciliteiten en bijbehorende diensten; door het ontwikkelen van gemeenschappelijke regels en voorspelbare regelgeving; en door het bevorderen van doeltreffend, efficiënt en gecoördineerd gebruik van het radiospectrum, open innovatie, het opzetten en ontwikkelen van trans-Europese netwerken, de verstrekking, de beschikbaarheid

Artikel 6

Bij de uitvoering van de taken die aan het Instituut krachtens deze wet zijn opgelegd:

1° bevordert het Instituut de connectiviteit met en de toegang tot, alsmede de benutting van netwerken met een zeer hoge capaciteit, met inbegrip van vaste, mobiele en draadloze netwerken;

2° bevordert het Instituut de mededinging bij het aanbieden van elektronische-communicatienetwerken en bijbehorende faciliteiten, met inbegrip van efficiënte concurrentie op basis van infrastructuur, en bij het aanbieden van elektronische-communicatiediensten en bijbehorende diensten;

3° draagt het Instituut bij tot de ontwikkeling van de interne markt, door het opheffen van resterende belemmeringen voor, en het bevorderen van convergerende voorwaarden voor, investeringen in en het aanbieden van elektronische-communicatienetwerken, elektronische-communicatiediensten, bijbehorende faciliteiten en bijbehorende diensten; door het ontwikkelen van gemeenschappelijke regels en voorspelbare regelgeving; en door het bevorderen van doeltreffend, efficiënt en gecoördineerd gebruik van het radiospectrum, open innovatie, het opzetten en ontwikkelen van trans-Europese netwerken, de verstrekking, de beschikbaarheid

BESTAANDE TEKST

en de interoperabiliteit van pan-Europese diensten, en eind-tot-eind connectiviteit;

4° bevordert het Instituut de belangen van de burgers, door te zorgen voor connectiviteit met, en ruime beschikbaarheid en benutting van, netwerken met een zeer hoge capaciteit, waaronder vaste, mobiele en draadloze netwerken, en van elektronische communicatiediensten; door erop toe te zien dat op basis van daadwerkelijke mededinging optimaal kan worden geprofiteerd wat betreft keuze, prijs en kwaliteit; door de beveiliging van netwerken en diensten te handhaven; door een hoog gemeenschappelijk beschermingsniveau voor eindgebruikers te waarborgen via de nodige sectorspecifieke regels; en door aandacht te schenken aan de behoeften, zoals betaalbare prijzen, van specifieke maatschappelijke groeperingen, met name eindgebruikers met een handicap, oudere eindgebruikers en eindgebruikers met speciale sociale behoeften, evenals keuzevrijheid en gelijkwaardige toegang voor eindgebruikers met een handicap.

Artikel 105

§ 1. Om de belangen te vrijwaren waarvan sprake in artikel 3, § 1, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen moeten de MNO's een machtiging krijgen die gezamenlijk is opgesteld door de betrokken ministers beoogd in het derde lid, 1°, alvorens een element van hun 5G-netwerk te gebruiken.

Rekening houdende met de in het eerste lid bedoelde belangen en bij besluit vastgesteld na overleg in de Ministerraad, kan de Koning bepalen dat deze machtiging ook noodzakelijk is voordat de MNO's diensten van aanbieders kunnen genieten die erin bestaan gericht tussenbeide te komen in het beheer van dat netwerk, met name in geval van een incident of grote wijziging van het netwerk, of dagelijks elementen van het netwerk te beheren of te

ONTWERP VAN WET

en de interoperabiliteit van pan-Europese diensten, en eind-tot-eind connectiviteit;

4° bevordert het Instituut de belangen van de burgers, door te zorgen voor connectiviteit met, en ruime beschikbaarheid en benutting van, netwerken met een zeer hoge capaciteit, waaronder vaste, mobiele en draadloze netwerken, en van elektronische communicatiediensten; door erop toe te zien dat op basis van daadwerkelijke mededinging optimaal kan worden geprofiteerd wat betreft keuze, prijs en kwaliteit; door de beveiliging van **netwerken- en informatiesystemen** te handhaven; door een hoog gemeenschappelijk beschermingsniveau voor eindgebruikers te waarborgen via de nodige sectorspecifieke regels; en door aandacht te schenken aan de behoeften, zoals betaalbare prijzen, van specifieke maatschappelijke groeperingen, met name eindgebruikers met een handicap, oudere eindgebruikers en eindgebruikers met speciale sociale behoeften, evenals keuzevrijheid en gelijkwaardige toegang voor eindgebruikers met een handicap.

Artikel 105

§ 1. Om de belangen te vrijwaren waarvan sprake in artikel 3, § 1, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen moeten de MNO's een machtiging krijgen die gezamenlijk is opgesteld door de betrokken ministers beoogd in het derde lid, 1°, alvorens een element van hun 5G-netwerk te gebruiken.

Rekening houdende met de in het eerste lid bedoelde belangen en bij besluit vastgesteld na overleg in de Ministerraad, kan de Koning bepalen dat deze machtiging ook noodzakelijk is voordat de MNO's diensten van aanbieders kunnen genieten die erin bestaan gericht tussenbeide te komen in het beheer van dat netwerk, met name in geval van een incident of grote wijziging van het netwerk, of dagelijks elementen van het netwerk te beheren of te

BESTAANDE TEKST

superviseren, of ook noodzakelijk is voordat ze bepaalde van deze diensten kunnen genieten.

Voor de toepassing van dit artikel wordt verstaan onder:

1° betrokken ministers: de Eerste minister, de minister van Telecommunicatie, de minister van Defensie, de minister van Justitie, de minister van Binnenlandse Zaken en de minister van Buitenlandse Zaken;

2° 5G-netwerk: een elektronische-communicatienetwerk waarvan het radiotoegangsnetwerk gebaseerd is op een radio-interface die gespecificeerd is in de ITU-R-aanbeveling M.2150 van de Internationale Telecommunicatie Unie.

Het eerste en het tweede lid zijn niet van toepassing:

1° voor het gebruik van passieve elementen van het netwerk, namelijk elementen die niet door een energiebron worden gevoed;

2° voor de netwerkaansluitpunten voor zover ze geen radiogedeelte bevatten dat gebaseerd is op een radio-interface die gespecificeerd is in de ITU-R-aanbeveling M.2150 van de Internationale Telecommunicatie Unie;

3° voor de elementen van mobiele netwerken van de vierde generatie en vroegere generaties, op voorwaarde dat ze niet noodzakelijk zijn voor het aanbieden van een 5G-netwerk.

Indien het gebruik van het netwerkelement of het beroep op de dienstenaanbieder reeds bestaat op de datum van inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 4, eerste lid, wordt een machtiging tot regularisatie gevraagd in de twee maanden die volgen op die datum.

§ 2. Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad:

ONTWERP VAN WET

superviseren, of ook noodzakelijk is voordat ze bepaalde van deze diensten kunnen genieten.

Voor de toepassing van dit artikel wordt verstaan onder:

1° betrokken ministers: de Eerste minister, de minister van Telecommunicatie, de minister van Defensie, de minister van Justitie, de minister van Binnenlandse Zaken en de minister van Buitenlandse Zaken;

2° 5G-netwerk: een elektronische-communicatienetwerk waarvan het radiotoegangsnetwerk gebaseerd is op een radio-interface die gespecificeerd is in de ITU-R-aanbeveling M.2150 van de Internationale Telecommunicatie Unie.

Het eerste en het tweede lid zijn niet van toepassing:

1° voor het gebruik van passieve elementen van het netwerk, namelijk elementen die niet door een energiebron worden gevoed;

2° voor de netwerkaansluitpunten voor zover ze geen radiogedeelte bevatten dat gebaseerd is op een radio-interface die gespecificeerd is in de ITU-R-aanbeveling M.2150 van de Internationale Telecommunicatie Unie;

3° voor de elementen van mobiele netwerken van de vierde generatie en vroegere generaties, op voorwaarde dat ze niet noodzakelijk zijn voor het aanbieden van een 5G-netwerk.

Indien het gebruik van het netwerkelement of het beroep op de dienstenaanbieder reeds bestaat op de datum van inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 4, eerste lid, wordt een machtiging tot regularisatie gevraagd in de twee maanden die volgen op die datum.

§ 2. Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad:

BESTAANDE TEKST

1° de verplichting om de machtigingen bedoeld in paragraaf 1 te krijgen, uitbreiden naar één of meer categorieën van MVNO's;

2° de verplichting om de machtigingen bedoeld in paragraaf 1 te krijgen, uitbreiden naar de naamloze vennootschap van publiek recht ASTRID en naar de exploitanten van een privaat elektronische-communicatienetwerk die aangewezen zijn als exploitant van een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren of als aanbieder van essentiële diensten in de zin van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

3° een of meer autoriteiten opdragen om via individuele beslissing, wanneer dat noodzakelijk is om de in paragraaf 1, eerste lid bedoelde belangen te vrijwaren, de andere exploitanten van een privaat elektronische-communicatienetwerk aan te wijzen die onderworpen zijn aan de verplichting om de in paragraaf 1 bedoelde machtigingen te krijgen;

4° de hypothesen preciseren waarin een machtiging zoals bedoeld in paragraaf 1, eerste lid, noodzakelijk is in geval van een update van software of hardware van het netwerk;

§ 3. De verzoeker dient zijn dossier in bij het Instituut, volgens de nadere regels die het op zijn website bepaalt.

De Koning stelt, bij een besluit vastgesteld na overleg in de Ministerraad, de nadere regels voor de behandeling van het verzoek en de samenstelling van het dossier vast.

De betrokken ministers, het Instituut en de inlichtingen- en veiligheidsdiensten kunnen informatie of aanvullende documenten vragen aan de verzoeker of aan iedere persoon die op nuttige wijze kan bijdragen tot hun informatie.

ONTWERP VAN WET

1° de verplichting om de machtigingen bedoeld in paragraaf 1 te krijgen, uitbreiden naar één of meer categorieën van MVNO's;

2° de verplichting om de machtigingen bedoeld in paragraaf 1 te krijgen, uitbreiden naar de naamloze vennootschap van publiek recht ASTRID en naar de exploitanten van een privaat elektronische-communicatienetwerk die aangewezen zijn als exploitant van een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren [...];

3° een of meer autoriteiten opdragen om via individuele beslissing, wanneer dat noodzakelijk is om de in paragraaf 1, eerste lid bedoelde belangen te vrijwaren, de andere exploitanten van een privaat elektronische-communicatienetwerk aan te wijzen die onderworpen zijn aan de verplichting om de in paragraaf 1 bedoelde machtigingen te krijgen;

4° de hypothesen preciseren waarin een machtiging zoals bedoeld in paragraaf 1, eerste lid, noodzakelijk is in geval van een update van software of hardware van het netwerk;

§ 3. De verzoeker dient zijn dossier in bij het Instituut, volgens de nadere regels die het op zijn website bepaalt.

De Koning stelt, bij een besluit vastgesteld na overleg in de Ministerraad, de nadere regels voor de behandeling van het verzoek en de samenstelling van het dossier vast.

De betrokken ministers, het Instituut en de inlichtingen- en veiligheidsdiensten kunnen informatie of aanvullende documenten vragen aan de verzoeker of aan iedere persoon die op nuttige wijze kan bijdragen tot hun informatie.

BESTAANDE TEKST

§ 4. Wanneer ze hun beslissing nemen na het onderzoek van het in paragraaf 1 bedoelde verzoek of deze op eigen initiatief herzien wegens een nieuw element dat hun beslissing ter discussie stelt, leggen de betrokken ministers de beperkingen en toepassingstermijnen ten uitvoer die vastgesteld zijn door de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, betreffende het gebruik, op het nationale grondgebied of in de gevoelige zones van dit grondgebied, van netwerkelementen of van diensten van leveranciers die een hoog risico vormen.

Die beperkingen en toepassingstermijnen mogen enkel vastgesteld worden om de bescherming van de belangen bedoeld in paragraaf 1, eerste lid, te garanderen.

Wanneer ze op eigen initiatief hun beslissing herzien en wanneer dat gerechtvaardigd is, leggen de betrokken ministers een datum van uitvoering van de nieuwe beslissing vast die later komt dan de termijnen die vastgesteld zijn bij het in het eerste lid bedoelde koninklijk besluit en die minstens vijf jaar na de datum van de kennisgeving ervan valt.

Het risicoprofiel van een leverancier wordt beoordeeld op basis van de volgende criteria:

1° de kans dat hij inmenging ondervindt vanwege een land dat geen lidstaat is van de Europese Unie, waarbij een dergelijke inmenging gefaciliteerd kan worden, zonder zich daartoe te beperken, door de aanwezigheid van één of meer van de volgende factoren:

a) een sterke link met de overheidsinstanties van het land in kwestie;

b) de wetgeving van of de situatie in het land in kwestie, met name wanneer er geen democratische of wetgevende controle voorhanden is of bij afwezigheid van overeenkomsten over gegevensbescherming of beveiliging tussen de Europese Unie en het land in kwestie;

ONTWERP VAN WET

§ 4. Wanneer ze hun beslissing nemen na het onderzoek van het in paragraaf 1 bedoelde verzoek of deze op eigen initiatief herzien wegens een nieuw element dat hun beslissing ter discussie stelt, leggen de betrokken ministers de beperkingen en toepassingstermijnen ten uitvoer die vastgesteld zijn door de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, betreffende het gebruik, op het nationale grondgebied of in de gevoelige zones van dit grondgebied, van netwerkelementen of van diensten van leveranciers die een hoog risico vormen.

Die beperkingen en toepassingstermijnen mogen enkel vastgesteld worden om de bescherming van de belangen bedoeld in paragraaf 1, eerste lid, te garanderen.

Wanneer ze op eigen initiatief hun beslissing herzien en wanneer dat gerechtvaardigd is, leggen de betrokken ministers een datum van uitvoering van de nieuwe beslissing vast die later komt dan de termijnen die vastgesteld zijn bij het in het eerste lid bedoelde koninklijk besluit en die minstens vijf jaar na de datum van de kennisgeving ervan valt.

Het risicoprofiel van een leverancier wordt beoordeeld op basis van de volgende criteria:

1° de kans dat hij inmenging ondervindt vanwege een land dat geen lidstaat is van de Europese Unie, waarbij een dergelijke inmenging gefaciliteerd kan worden, zonder zich daartoe te beperken, door de aanwezigheid van één of meer van de volgende factoren:

a) een sterke link met de overheidsinstanties van het land in kwestie;

b) de wetgeving van of de situatie in het land in kwestie, met name wanneer er geen democratische of wetgevende controle voorhanden is of bij afwezigheid van overeenkomsten over gegevensbescherming of beveiliging tussen de Europese Unie en het land in kwestie;

BESTAANDE TEKST

c) de karakteristieken van de eigendom van de onderneming van de leverancier;

d) het vermogen van het land in kwestie om enige vorm van pressie uit te oefenen, inclusief wat betreft de plaats van vervaardiging van de apparatuur;

e) het feit dat het land waaruit de leverancier afkomstig is, een offensief cyberbeleid voert of daarbij betrokken is;

2° het vermogen van de leverancier om de bevoorrading te garanderen in termen van tijd en hoeveelheid;

3° de algemene kwaliteit van de producten of diensten en de praktijken inzake beveiliging van de leverancier, met inbegrip van de mate van controle over zijn eigen bevoorradingsketen en de vraag of een gepaste hiërarchische indeling van de prioriteiten wordt gegeven aan de praktijken inzake beveiliging.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, de in het vierde lid beoogde criteria aanvullen.

Slechts één van deze criteria kan reeds rechtvaardigen dat een aanbieder wordt aangeduid als een hoog risico vormend.

Het risicoprofiel van een leverancier wordt geëvalueerd op basis van een advies van de inlichtingen- en veiligheidsdiensten voor wat betreft het criterium vastgesteld in het vierde lid, 1°, en op basis van een advies van het Instituut voor wat betreft de criteria vastgesteld in het vierde lid, 2° en 3°.

De gevoelige zones worden geïdentificeerd door de Koning, op basis van een advies van de Nationale Veiligheidsraad en dit rekening houdend met de aanwezigheid in deze zones van sites gelieerd aan de belangen bedoeld in paragraaf 1, eerste lid.

ONTWERP VAN WET

c) de karakteristieken van de eigendom van de onderneming van de leverancier;

d) het vermogen van het land in kwestie om enige vorm van pressie uit te oefenen, inclusief wat betreft de plaats van vervaardiging van de apparatuur;

e) het feit dat het land waaruit de leverancier afkomstig is, een offensief cyberbeleid voert of daarbij betrokken is;

2° het vermogen van de leverancier om de bevoorrading te garanderen in termen van tijd en hoeveelheid;

3° de algemene kwaliteit van de producten of diensten en de praktijken inzake beveiliging van de leverancier, met inbegrip van de mate van controle over zijn eigen bevoorradingsketen en de vraag of een gepaste hiërarchische indeling van de prioriteiten wordt gegeven aan de praktijken inzake beveiliging.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, de in het vierde lid beoogde criteria aanvullen.

Slechts één van deze criteria kan reeds rechtvaardigen dat een aanbieder wordt aangeduid als een hoog risico vormend.

Het risicoprofiel van een leverancier wordt geëvalueerd op basis van een advies van de inlichtingen- en veiligheidsdiensten voor wat betreft het criterium vastgesteld in het vierde lid, 1°, en op basis van een advies van het Instituut voor wat betreft de criteria vastgesteld in het vierde lid, 2° en 3°.

De gevoelige zones worden geïdentificeerd door de Koning, op basis van een advies van de Nationale Veiligheidsraad en dit rekening houdend met de aanwezigheid in deze zones van sites gelieerd aan de belangen bedoeld in paragraaf 1, eerste lid.

BESTAANDE TEKST

Het koninklijk besluit dat de gevoelige zones identificeert, wordt bekendgemaakt via vermelding in het Belgisch Staatsblad.

§ 5. Wanneer de betrokken ministers van plan zijn de machtiging te weigeren, daar voorwaarden aan te koppelen of hun beslissing te herzien, beschikt de verzoeker, na de ontwerpbeslissing te hebben ontvangen, over achtentwintig dagen tijd om zijn schriftelijke opmerkingen voor te leggen.

De verzoeker wordt de kans geboden om te worden gehoord. Hij mag zich laten vergezellen door de technische of juridische raadgevers van zijn keuze.

De betrokken ministers kunnen zich laten vertegenwoordigen door het bestuur van hun keuze. Het Instituut en de inlichtingen- en veiligheidsdiensten kunnen aan de hoorzitting deelnemen.

§ 6. De betrokken ministers nemen samen één beslissing. Het Instituut stelt alle nuttige daden met het oog op de voorbereiding ervan.

Binnen de door de Koning vastgestelde termijn, die ingaat vanaf de indiening van het verzoek, ontvangt de verzoeker ofwel de beslissing van de ministers waarin de machtiging wordt verleend, ofwel de ontwerpbeslissing waarin ze de machtiging weigeren of voorwaarden daaraan koppelen.

In geval van een hoorzitting of van schriftelijke opmerkingen van de verzoeker, waarvan sprake in paragraaf 5, nemen de ministers hun beslissing uiterlijk binnen de termijn die door de Koning is vastgesteld en die ingaat vanaf de ontvangst van de schriftelijke opmerkingen of vanaf de datum van de hoorzitting, waarbij de datum die het laatst komt in aanmerking wordt genomen.

Het verzoek om inlichtingen of om documenten, waarvan sprake in paragraaf 3, derde lid, of dat gericht is aan de verzoeker om zijn dossier te vervolledigen, schorst de termijnen die

ONTWERP VAN WET

Het koninklijk besluit dat de gevoelige zones identificeert, wordt bekendgemaakt via vermelding in het Belgisch Staatsblad.

§ 5. Wanneer de betrokken ministers van plan zijn de machtiging te weigeren, daar voorwaarden aan te koppelen of hun beslissing te herzien, beschikt de verzoeker, na de ontwerpbeslissing te hebben ontvangen, over achtentwintig dagen tijd om zijn schriftelijke opmerkingen voor te leggen.

De verzoeker wordt de kans geboden om te worden gehoord. Hij mag zich laten vergezellen door de technische of juridische raadgevers van zijn keuze.

De betrokken ministers kunnen zich laten vertegenwoordigen door het bestuur van hun keuze. Het Instituut en de inlichtingen- en veiligheidsdiensten kunnen aan de hoorzitting deelnemen.

§ 6. De betrokken ministers nemen samen één beslissing. Het Instituut stelt alle nuttige daden met het oog op de voorbereiding ervan.

Binnen de door de Koning vastgestelde termijn, die ingaat vanaf de indiening van het verzoek, ontvangt de verzoeker ofwel de beslissing van de ministers waarin de machtiging wordt verleend, ofwel de ontwerpbeslissing waarin ze de machtiging weigeren of voorwaarden daaraan koppelen.

In geval van een hoorzitting of van schriftelijke opmerkingen van de verzoeker, waarvan sprake in paragraaf 5, nemen de ministers hun beslissing uiterlijk binnen de termijn die door de Koning is vastgesteld en die ingaat vanaf de ontvangst van de schriftelijke opmerkingen of vanaf de datum van de hoorzitting, waarbij de datum die het laatst komt in aanmerking wordt genomen.

Het verzoek om inlichtingen of om documenten, waarvan sprake in paragraaf 3, derde lid, of dat gericht is aan de verzoeker om zijn dossier te vervolledigen, schorst de termijnen die

BESTAANDE TEKST

vastgesteld zijn in het tweede en het derde lid, tot de dag waarop de gevraagde inlichtingen of documenten worden verstrekt.

Het uitblijven van een beslissing of ontwerpbeslissing bedoeld in het tweede lid binnen de krachtens het tweede of het derde lid vastgestelde termijn staat gelijk aan een weigering.

§ 7. De persoon die een kopie krijgt van de in paragraaf 4, achtste lid, bedoelde lijst van de gevoelige zones, mag die maar verzenden aan de personen die daar kennis van moeten hebben en die daar toegang toe moeten hebben om hun functies of opdracht in het kader van de uitrol en de exploitatie van het 5G-netwerk uit te voeren.

Wordt bestraft met een strafrechtelijke boete van 1000 euro tot 100 000 euro: de persoon die informatie onthult in verband met de in het eerste lid bedoelde lijst aan een persoon die in dat lid niet is beoogd.

Personen die een verzoek om machtiging of de herziening van een vroegere beslissing behandelen, mogen aan openbare besturen die zij in dat kader raadplegen vertrouwelijke informatie meedelen wanneer dat nodig is voor het vervullen van de taak die zij aan hen toevertrouwen.

De in het derde lid bedoelde personen en openbare besturen mogen derden geen vertrouwelijke informatie meedelen waarvan zij kennis hebben in het kader van de toepassing van dit artikel, buiten de in de wet bepaalde uitzonderingen.

Deze vertrouwelijke informatie is die welke als zodanig wordt aangeduid door de persoon die ze heeft verstrekt, onverminderd artikel 23, paragraaf 3, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.

De schending van het in het vierde lid bedoelde verbod wordt bestraft met de straffen die zijn

ONTWERP VAN WET

vastgesteld zijn in het tweede en het derde lid, tot de dag waarop de gevraagde inlichtingen of documenten worden verstrekt.

Het uitblijven van een beslissing of ontwerpbeslissing bedoeld in het tweede lid binnen de krachtens het tweede of het derde lid vastgestelde termijn staat gelijk aan een weigering.

§ 7. De persoon die een kopie krijgt van de in paragraaf 4, achtste lid, bedoelde lijst van de gevoelige zones, mag die maar verzenden aan de personen die daar kennis van moeten hebben en die daar toegang toe moeten hebben om hun functies of opdracht in het kader van de uitrol en de exploitatie van het 5G-netwerk uit te voeren.

Wordt bestraft met een strafrechtelijke boete van 1000 euro tot 100 000 euro: de persoon die informatie onthult in verband met de in het eerste lid bedoelde lijst aan een persoon die in dat lid niet is beoogd.

Personen die een verzoek om machtiging of de herziening van een vroegere beslissing behandelen, mogen aan openbare besturen die zij in dat kader raadplegen vertrouwelijke informatie meedelen wanneer dat nodig is voor het vervullen van de taak die zij aan hen toevertrouwen.

De in het derde lid bedoelde personen en openbare besturen mogen derden geen vertrouwelijke informatie meedelen waarvan zij kennis hebben in het kader van de toepassing van dit artikel, buiten de in de wet bepaalde uitzonderingen.

Deze vertrouwelijke informatie is die welke als zodanig wordt aangeduid door de persoon die ze heeft verstrekt, onverminderd artikel 23, paragraaf 3, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.

De schending van het in het vierde lid bedoelde verbod wordt bestraft met de straffen die zijn

BESTAANDE TEKST

bepaald in artikel 458 van het Strafwetboek of met één van die straffen.

§ 8. Wanneer een MNO in België elektronische-communicatiediensten aanbiedt met behulp van een 5G-netwerk, moeten de infrastructuur van dat netwerk zich bevinden op het grondgebied van de lidstaten van de Europese Unie. Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, kan de Koning de eisen vaststellen die uit die verplichting voortvloeien.

Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, legt de Koning de in het eerste lid bedoelde MNO's de noodzakelijke regels op opdat zij de activiteiten die absoluut noodzakelijk zijn voor de werking, de veiligheid en de continuïteit van hun netwerk, die Hij bepaalt, uitoefenen binnen het grondgebied van de lidstaten van de Europese Unie.

Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, kan de Koning de regels en eisen bedoeld in het eerste en tweede lid uitbreiden naar de MVNO's en exploitanten van een privaat elektronische-communicatienetwerk die onderworpen zijn aan de machtigingen bedoeld in paragraaf 1.

Artikel 107/2

§ 1. De operatoren analyseren de risico's voor de veiligheid van hun netwerken en diensten. Het Instituut kan de nadere regels van deze risicoanalyse vaststellen.

De operatoren nemen de passende en evenredige technische en organisatorische

ONTWERP VAN WET

bepaald in artikel 458 van het Strafwetboek of met één van die straffen.

§ 8. Wanneer een MNO in België elektronische-communicatiediensten aanbiedt met behulp van een 5G-netwerk, moeten de infrastructuur van dat netwerk zich bevinden op het grondgebied van de lidstaten van de Europese Unie. Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, kan de Koning de eisen vaststellen die uit die verplichting voortvloeien.

Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, legt de Koning de in het eerste lid bedoelde MNO's de noodzakelijke regels op opdat zij de activiteiten die absoluut noodzakelijk zijn voor de werking, de veiligheid en de continuïteit van hun netwerk, die Hij bepaalt, uitoefenen binnen het grondgebied van de lidstaten van de Europese Unie.

Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, kan de Koning de regels en eisen bedoeld in het eerste en tweede lid uitbreiden naar de MVNO's en exploitanten van een privaat elektronische-communicatienetwerk die onderworpen zijn aan de machtigingen bedoeld in paragraaf 1.

Artikel 107/2

§ 1. Onverminderd de bepalingen van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid analyseren de aanbieders van digitale infrastructuur de risico's voor de beveiliging van hun netwerk- en informatiesystemen. Het Instituut kan de nadere regels van deze risicoanalyse vaststellen.

[...]

BESTAANDE TEKST

maatregelen, waaronder in voorkomend geval versleuteling, om deze risico's goed te beheersen, alsook om de impact van beveiligingsincidenten op gebruikers en op andere netwerken en diensten zo laag mogelijk te houden.

Deze maatregelen zorgen, gezien de stand van de techniek, voor een veiligheidsniveau dat is afgestemd op de risico's die zich voordoen. [...]

De Koning, op voorstel van het Instituut of op eigen initiatief, na advies van het Instituut, kan de in het tweede lid bedoelde maatregelen preciseren, wanneer het in dat lid bedoelde risico voortvloeit uit de organisatie van de operatoren. [...]

Onder voorbehoud van het vierde lid en na advies van het Instituut kan de Koning de maatregelen verduidelijken waarvan sprake in het tweede lid. [...]

§ 2. Onverminderd de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, hierna te noemen "AVG" en de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, hierna te noemen "wet van 30 juli 2018", zorgen de in de eerste paragraaf bedoelde maatregelen die genomen worden door de operatoren van elektronische-communicatiediensten, wanneer het persoonsgegevens betreft, ervoor dat in ieder geval:

1° wordt gewaarborgd dat alleen gemachtigd personeel voor wettelijk toegestane doeleinden toegang heeft tot de persoonsgegevens;

2° opgeslagen of verzonden persoonsgegevens worden beschermd tegen onbedoelde of

ONTWERP VAN WET

§ 2. Onverminderd Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, hierna "AVG" genoemd, en de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, hierna "wet van 30 juli 2018" genoemd, zorgen de operatoren ervoor dat in ieder geval:

1° wordt gewaarborgd dat alleen gemachtigd personeel voor wettelijk toegestane doeleinden toegang heeft tot de persoonsgegevens die ze verwerken;

2° opgeslagen of verzonden persoonsgegevens worden beschermd tegen onbedoelde of

BESTAANDE TEKST

onwettige vernietiging, onbedoeld verlies of wijziging, en niet-toegestane of onwettige opslag, verwerking, toegang of vrijgave; en

3° een beveiligingsbeleid wordt ingevoerd met betrekking tot de verwerking van persoonsgegevens.

Het Instituut kan de door deze operatoren genomen maatregelen controleren en aanbevelingen formuleren over de beste praktijken betreffende het beveiligingspeil dat met deze maatregelen moet worden gehaald.

§ 3. De operatoren nemen alle noodzakelijke maatregelen, inclusief preventieve, om de beschikbaarheid van de spraakcommunicatiediensten en van de internettoegangsdiensten zo volledig mogelijk te waarborgen in geval van uitzonderlijke netwerkuitval of in geval van overmacht.

De Koning, op voorstel van het Instituut of op eigen initiatief, na advies van het Instituut, kan deze maatregelen preciseren wanneer het risico voor uitval of van overmacht voortvloeit uit de organisatie van de operatoren.

Onverminderd het tweede lid kan de Koning na advies van het Instituut deze maatregelen verduidelijken.

§ 4. De operatoren bieden hun abonnees kosteloos, rekening houdend met de stand van de techniek, de gepaste beveiligde diensten aan die de eindgebruikers in staat stellen ongewenste elektronische communicatie in alle vormen te verhinderen.

Artikel 107/3

§ 1. In geval van een specifieke en significante dreiging van een beveiligingsincident voor het publiek beschikbare elektronische-communicatienetwerken of voor het publiek beschikbare elektronische-communicatiediensten, informeert de operator het Instituut over de dreiging, over mogelijke beschermingsmaatregel of oplossing die de

ONTWERP VAN WET

onwettige vernietiging, onbedoeld verlies of wijziging, en niet-toegestane of onwettige opslag, verwerking, toegang of vrijgave, en

3° een beveiligingsbeleid wordt ingevoerd met betrekking tot de verwerking van persoonsgegevens.

Het Instituut kan de door deze operatoren genomen maatregelen controleren en aanbevelingen formuleren over de beste praktijken betreffende het beveiligingspeil dat met deze maatregelen moet worden gehaald.

§ 3. De operatoren nemen alle noodzakelijke maatregelen, inclusief preventieve, om de beschikbaarheid van de spraakcommunicatiediensten en de internettoegangsdiensten zo volledig mogelijk te waarborgen in geval van uitzonderlijke netwerkuitval of in geval van overmacht.

Op voorstel van het Instituut of op eigen initiatief, en na advies van het Instituut, kan de Koning deze maatregelen preciseren.

[...]

§ 4. De operatoren bieden hun abonnees kosteloos, rekening houdend met de stand van de techniek, de gepaste beveiligde diensten aan die de eindgebruikers in staat stellen ongewenste elektronische communicatie in alle vormen te verhinderen.

Artikel 107/3

§ 1. In geval van een significante cyberdreiging informeert de aanbieder van digitale infrastructuur het Instituut over de dreiging, over mogelijke beschermingsmaatregelen of oplossingen die de gebruikers kunnen toepassen, alsook over de maatregelen die hij heeft genomen of overweegt te nemen.

BESTAANDE TEKST

gebruikers kunnen toepassen, alsook over de maatregelen die hij genomen heeft of overweegt te nemen.

De operator informeert vervolgens zijn gebruikers die gevolgen van die dreiging kunnen ondervinden, over mogelijke beschermingsmaatregelen of oplossingen die de gebruikers kunnen toepassen en waar passend ook over de dreiging zelf.

Het Instituut kan de gevallen preciseren waarin informatie moet worden verstrekt alsook de praktische regels voor die notificatie.

§ 2. De operatoren stellen het Instituut onverwijld in kennis van elk beveiligingsincident dat een belangrijke impact heeft gehad op de werking van netwerken of diensten.

Om te bepalen of een beveiligingsincident een belangrijke impact heeft, wordt, voor zover beschikbaar, met name met de volgende parameters rekening gehouden:

1° het aantal gebruikers dat gevolgen ondervindt van het beveiligingsincident;

2° de duur van het beveiligingsincident;

ONTWERP VAN WET

[...]

Het Instituut kan de gevallen preciseren waarin informatie moet worden verstrekt alsook de nadere regels voor die kennisgeving.

§ 2. In geval van inbreuk in verband met persoonsgegevens verwittigt de operator van elektronische-communicatiediensten onverwijld de Gegevensbeschermingsautoriteit, die onverwijld het Instituut verwittigt.

Indien de inbreuk in verband met persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor de persoonsgegevens of persoonlijke levenssfeer van een abonnee of een individueel persoon, stelt de operator van elektronische-communicatiediensten onverwijld ook de betrokken abonnee of individuele persoon in kennis van de inbreuk.

De Gegevensbeschermingsautoriteit gaat na of de operator deze verplichting nakomt en brengt het Instituut op de hoogte wanneer ze van oordeel is dat dit niet het geval is.

De kennisgeving van een inbreuk in verband met persoonsgegevens aan een betrokken abonnee of individuele persoon is niet vereist wanneer de operator van elektronische-communicatiediensten tot voldoening van het Instituut heeft aangetoond dat hij de gepaste technologische beschermingsmaatregelen heeft genomen en dat deze maatregelen werden toegepast op de data die bij de beveiligingsinbreuk betrokken waren. Dergelijke technologische beschermingsmaatregelen maken de gegevens

BESTAANDE TEKST

3° de geografische spreiding van het door het beveiligingsincident getroffen gebied;

4° de mate waarin het functioneren van het netwerk of de dienst wordt aangetast;

5° de omvang van de impact op de economische en maatschappelijke activiteiten.

Het Instituut preciseert in welke gevallen het beveiligingsincident een belangrijke impact heeft in de zin van het eerste lid, alsook de nadere regels voor de kennisgeving.

In geval van een beveiligingsincident kan het Instituut de regelgevende gemeenschapsinstanties die bevoegd zijn op het stuk van elektronische-communicatienetwerken, de nationale regelgevende instanties in andere lidstaten en ENISA hiervan op de hoogte brengen. Het Instituut kan het publiek hiervan op de hoogte brengen of eisen dat de operatoren dit doen,

ONTWERP VAN WET

onbegrijpelijk voor eenieder die geen recht op toegang daartoe heeft.

Onverminderd de verplichting van de operator van elektronische-communicatiediensten om de betrokken abonnees en individuele personen in kennis te stellen, indien deze operator de abonnee of individuele persoon niet reeds in kennis heeft gesteld van de inbreuk in verband met persoonsgegevens, kan het Instituut op verzoek van de Gegevensbeschermingsautoriteit hem, na te hebben gezien of en welke ongunstige gevolgen uit de inbreuk voortvloeien, verzoeken dat te doen.

In de kennisgeving aan de abonnee of de individuele persoon worden ten minste de aard van de inbreuk in verband met persoonsgegevens, alsmede de contactpunten voor meer informatie vermeld, en worden er maatregelen aanbevolen om mogelijke negatieve gevolgen van de inbreuk in verband met persoonsgegevens te verlichten.

De kennisgeving aan de Gegevensbeschermingsautoriteit bevat bovendien een omschrijving van de gevolgen van de inbreuk in verband met persoonsgegevens en van de door de operator van elektronische-communicatiediensten voorgestelde of getroffen maatregelen om die inbreuk te verhelpen.

[...]

[...]

BESTAANDE TEKST

indien het de bekendmaking van het beveiligingsincident van algemeen belang acht.

Eenmaal per jaar dient het Instituut bij de Europese Commissie en ENISA een beknopt verslag in over de kennisgevingen die het heeft ontvangen en de maatregelen die overeenkomstig de bepalingen in deze paragraaf zijn genomen. [...]

§ 3. In geval van inbreuk in verband met persoonsgegevens verwittigt de operator van elektronische-communicatiediensten onverwijld de Gegevensbeschermingsautoriteit, die onverwijld het Instituut daarvan verwittigt.

Indien de inbreuk in verband met persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor de persoonsgegevens of persoonlijke levenssfeer van een abonnee of een individueel persoon stelt de operator van elektronische-communicatiediensten ook de abonnee of de individuele persoon in kwestie onverwijld van de inbreuk in kennis.

De Gegevensbeschermingsautoriteit onderzoekt of de operator deze verplichting nakomt en brengt het Instituut op de hoogte wanneer ze van oordeel is dat dit niet het geval is.

Kennisgeving van een betrokken abonnee of individuele persoon van een inbreuk in verband met persoonsgegevens is niet vereist wanneer [...]

ONTWERP VAN WET

§ 3. Onder voorbehoud van technische uitvoeringsmaatregelen van de Europese Commissie overeenkomstig artikel 4, punt 5, van Richtlijn 2002/58/EG, en na advies van de Gegevensbeschermingsautoriteit, kan het Instituut richtsnoeren aannemen en, waar nodig, instructies uitvaardigen betreffende de omstandigheden waarin de kennisgeving van de inbreuk in verband met persoonsgegevens door de operatoren van elektronische-communicatiediensten noodzakelijk is.

Onder voorbehoud van technische uitvoeringsmaatregelen van de Europese Commissie overeenkomstig artikel 4, punt 5, van Richtlijn 2002/58/EG, en na advies van het Instituut, kan de Gegevensbeschermingsautoriteit richtsnoeren aannemen en, waar nodig, instructies uitvaardigen betreffende het voor deze kennisgeving toepasselijke formaat, alsmede de manier waarop de kennisgeving geschiedt.

De operatoren van elektronische-communicatiediensten houden een inventaris bij van inbreuken in verband met persoonsgegevens, onder meer met de feiten in verband met deze inbreuken, de gevolgen ervan en de herstelmaatregelen die zijn genomen, zodat de Gegevensbeschermingsautoriteit en het Instituut kunnen nagaan of de bepalingen van paragraaf 2 werden nageleefd. Deze inventaris bevat uitsluitend de voor dit doel noodzakelijke gegevens.

BESTAANDE TEKST

de operator van elektronische-communicatiediensten tot voldoening van het Instituut heeft aangetoond dat hij de gepaste technologische beschermingsmaatregelen heeft genomen en dat deze maatregelen werden toegepast op de data die bij de beveiligingsinbreuk betrokken waren. Dergelijke technologische beschermingsmaatregelen maken de gegevens onbegrijpelijk voor eenieder die geen recht op toegang daartoe heeft.

Onverminderd de verplichting van de operator [...] van elektronische-communicatiediensten om de betrokken abonnees en de individuele personen in kwestie in kennis te stellen, indien deze operator de abonnee of individuele persoon niet reeds in kennis heeft gesteld van de inbreuk in verband met persoonsgegevens, kan het Instituut op verzoek van de Gegevensbeschermingsautoriteit hem, na te hebben gezien of en welke ongunstige gevolgen uit de inbreuk voortvloeien, verzoeken dat te doen.

In de kennisgeving aan de abonnee of de individuele persoon worden ten minste de aard van de inbreuk in verband met persoonsgegevens, alsmede de contactpunten voor meer informatie vermeld, en worden er maatregelen aanbevolen om mogelijke negatieve gevolgen van de inbreuk in verband met persoonsgegevens te verlichten.

De kennisgeving aan de [...] Gegevensbeschermingsautoriteit bevat bovendien een omschrijving van de gevolgen van de inbreuk in verband met persoonsgegevens en van de door de operator van elektronische-communicatiediensten voorgestelde of getroffen maatregelen om die inbreuk te verhelpen.

§ 4. Onder voorbehoud van technische [...] uitvoeringsmaatregelen afkomstig van de Europese Commissie overeenkomstig artikel 4, punt 5, van Richtlijn 2002/58/EG en na advies van de Gegevensbeschermingsautoriteit, kan het Instituut richtsnoeren aannemen en, waar nodig, instructies uitvaardigen betreffende de

ONTWERP VAN WET

BESTAANDE TEKST

omstandigheden waarin de kennisgeving van de inbreuk in verband met persoonsgegevens door de operatoren van elektronische-communicatiediensten noodzakelijk is.

Onder voorbehoud van technische [...] uitvoeringsmaatregelen afkomstig van de Europese Commissie conform artikel 4, punt 5, van Richtlijn 2002/58/EG, en na advies van het Instituut, kan de Gegevensbeschermingsautoriteit richtsnoeren aannemen en, desgevallend, instructies uitvaardigen die het format bepalen voor deze kennisgeving en de procedure van overbrenging.

De operatoren van elektronische-communicatiediensten houden een inventaris [...] bij van inbreuken op persoonsgegevens, onder meer met de feiten in verband met deze inbreuken, de gevolgen ervan en de herstelmaatregelen die zijn genomen, zodat de Gegevensbeschermingsautoriteit en het Instituut kunnen nagaan of de bepalingen van paragraaf 3 werden nageleefd. Deze inventaris bevat uitsluitend de voor dit doel noodzakelijke gegevens.

Artikel 107/4

§ 1. Met het oog op de uitvoering van de artikelen 107/2, 107/3 en van dit artikel kan het Instituut een operator bindende instructies geven, onder meer de maatregelen die nodig zijn om een beveiligingsincident op te lossen of te voorkomen wanneer een significante dreiging is vastgesteld, alsook het tijdschema voor de uitvoering van die instructies.

Op verzoek van het Instituut neemt een operator [...] deel aan een oefening in verband met de veiligheid van de netwerken of diensten of organiseert hij een dergelijke oefening.

Op verzoek van het Instituut en in het kader van [...] het beheer van veiligheidsincidenten, deelt een operator het een contactpersoon mee die steeds bereikbaar is.

ONTWERP VAN WET**Artikel 107/4**

§ 1. Dit artikel is van toepassing onverminderd de bepalingen van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid met name voor wat betreft de toezichtsbevoegdheden verleend aan de sectorale overheid of de sectorale inspectiedienst.

BESTAANDE TEKST

§ 2. De operator verschaft het Instituut, op zijn verzoek, alle informatie die nodig is om de veiligheid van zijn netwerken en diensten te beoordelen, met inbegrip van gedocumenteerde beveiligingsmaatregelen. Het Instituut kan de in acht te nemen nadere bepalingen voor de verstrekking van deze informatie vastleggen.

Op verzoek van het Instituut onderwerpt een operator zich aan een veiligheidscontrole uitgevoerd door het Instituut zelf, door een instantie of deels door het Instituut en deels door die instantie. Het Instituut stelt het voorwerp en de nadere regels van de controle vast, alsook de termijn waarbinnen die controle moet worden uitgevoerd, wanneer deze door een instantie wordt verricht. Wanneer de controle wordt uitgevoerd door het Instituut, kan deze controle inspecties ter plaatse omvatten. Wanneer de controle wordt uitgevoerd door een instantie, dan stelt de operator een of meer instanties ter goedkeuring aan het Instituut voor. Het Instituut geeft zijn akkoord wanneer de instantie gekwalificeerd is om de controle uit te voeren en onafhankelijk is van de operator. Bij uitblijven van een akkoord vanwege het Instituut binnen de termijn die het bij het verzoek heeft vastgesteld, wijst het Instituut zelf de instantie aan. Deze laatste bezorgt aan het Instituut het volledige verslag en de resultaten van deze controle en de kosten van de controle zijn ten laste van de operator.

Op verzoek van het Instituut en om een onderzoek in te stellen naar een geval van niet-conformiteit met de artikelen 107/2, 107/3 of dit artikel of met een uitvoeringsmaatregel, alsook naar het gevolg ervan voor de veiligheid van de netwerken en diensten, geeft de operator toegang tot elk element van zijn netwerk aan het Instituut.

§ 3. Ter uitvoering van de artikelen 107/2 en 107/3 heeft het Instituut de bevoegdheid om de hulp in te roepen van het "Computer Security Incident Response Team", bedoeld in artikel 7, §

ONTWERP VAN WET

§ 2. Het Instituut kan een aanbieder van digitale infrastructuur bindende instructies geven in het kader van artikelen 107/2 en 107/3 en van artikelen 30 en 33 van de bovengenoemd wet van [xx xxx xxxx], onder meer de maatregelen die nodig zijn om een beveiligingsincident op te lossen of te voorkomen wanneer een significante dreiging is vastgesteld, alsook het tijdschema voor de uitvoering van die instructies.

[...]

[...]

§ 3. In het kader van het toezicht op de artikelen 107/2 en 107/3 en van artikelen 30 en 33 van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en

BESTAANDE TEKST

2, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met betrekking tot kwesties die vallen onder de taken van dat team.

ONTWERP VAN WET

informatiesystemen van algemeen belang voor de openbare veiligheid, kan het Instituut de aanbieder van digitale infrastructuur onderwerpen aan:

a) inspecties ter plaatse en toezicht elders, met inbegrip van steekproefsgewijze controles, die worden uitgevoerd door daartoe opgeleide professionals;

b) regelmatige en gerichte beveiligingsaudits die worden uitgevoerd door het Instituut of door een onafhankelijke instantie;

c) ad-hoc audits;

d) beveiligingsscan op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobedoelingscriteria, indien nodig in samenwerking met de betrokken aanbieder van digitale infrastructuur;

e) verzoeken om informatie die nodig is om de door de betrokken aanbieder van digitale infrastructuur genomen maatregelen voor het beheer van cyberbeveiligingsrisico's

f) verzoeken van alle gegevens, documenten en informatie die het Instituut nodig acht voor de uitoefening van haar toezichthoudende taken;

g) verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de respectieve onderliggende bewijzen.

De in het eerste lid, punt b), bedoelde gerichte beveiligingsaudits zijn gebaseerd op door het Instituut of de gecontroleerde entiteit verrichte risicobedoelingen of op andere beschikbare risicogerelateerde informatie.

Wanneer de in het eerste lid, punt b) bedoelde beveiligingsaudit wordt uitgevoerd door een onafhankelijke instantie, dan stelt de aanbieder van digitale infrastructuur een of meer instanties ter goedkeuring aan het Instituut

BESTAANDE TEKST

§ 4. Het Instituut coördineert de initiatieven betreffende de veiligheid van de openbare elektronische-communicatienetwerken en openbare elektronische-communicatiediensten.

ONTWERP VAN WET

voor. Het Instituut geeft zijn akkoord wanneer de onafhankelijke instantie gekwalificeerd is om de audit uit te voeren en onafhankelijk is van de aanbieder van digitale infrastructuur. Bij uitblijven van een akkoord vanwege het Instituut binnen de termijn die het bij het verzoek heeft vastgesteld, wijst het Instituut zelf de onafhankelijke instantie aan. Deze laatste bezorgt aan het Instituut het volledige verslag en de resultaten van deze audit en de kosten van de audit zijn ten laste van de aanbieder van digitale infrastructuur, behalve in naar behoren gemotiveerde gevallen waarin het Instituut anders besluit.

Bij de uitoefening van zijn bevoegdheden uit hoofde van lid 1, punt e), f) of g), vermeldt het Instituut het doel van het verzoek en de gevraagde informatie.

Het Instituut kan bepalen op welke wijze de aanbieder van digitale infrastructuur informatie over de risicoanalyse moet verstrekken.

Op verzoek van het Instituut neemt een aanbieder van digitale infrastructuur deel aan een oefening in verband met de beveiliging van de netwerk- en informatiesystemen of organiseert hij een dergelijke oefening.

Op verzoek van het Instituut en in het kader van het beheer van beveiligingsincidenten, deelt een aanbieder van digitale infrastructuur het Instituut een contactpersoon mee die steeds bereikbaar is.

§ 4. Op verzoek van het Instituut en om een onderzoek in te stellen naar een geval van niet-conformiteit met artikelen 30 en 33 van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, of met een uitvoeringsmaatregel, alsook naar de gevolgen ervan voor de beveiliging van netwerk- en informatiesystemen, geeft de aanbieder van digitale infrastructuur het Instituut toegang tot alle elementen van zijn netwerk.

BESTAANDE TEKST

Het houdt toezicht op het opsporen, het observeren en het analyseren van de veiligheidsproblemen en kan informatie daarover aan de gebruikers verstrekken.

§ 5. De Koning en het Instituut kunnen de uitvoering van de artikelen 107/2, 107/3 en van het huidige artikel aanpassen naargelang van het type van operator en volgens verschillende categorieën binnen de netwerken en diensten.

ONTWERP VAN WET

[...]

§ 5. Onverminderd de bevoegdheden van de nationale cyberbeveiligingsautoriteit coördineert het Instituut de initiatieven rond de beveiliging van openbare elektronische-communicatienetwerken en openbare elektronische-communicatiediensten.

Het ziet toe op het opsporen, observeren en analyseren van beveiligingsproblemen, en kan de gebruikers hierover informatie verstrekken.

§ 6. Indien een aanbieder van digitale infrastructuur dit artikel of een op grond van dit artikel genomen beslissing van het Instituut niet naleeft, kunnen de in titel 4, hoofdstuk 2, van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid van de NIS2-wet bedoelde administratieve maatregelen of geldboetes worden opgelegd.

Artikel 126/3

§ 1. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones bestaande uit:

- de gerechtelijke arrondissementen waar minstens drie strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren;
- de politiezones waar minstens drie strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren, en die deel uitmaken van een gerechtelijk arrondissement waar, in het kalenderjaar voorafgaand aan het lopende kalenderjaar

Artikel 126/3

§ 1. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones bestaande uit:

- de gerechtelijke arrondissementen waar minstens drie strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren;
- de politiezones waar minstens drie strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren, en die deel uitmaken van een gerechtelijk arrondissement waar, in het kalenderjaar voorafgaand aan het lopende kalenderjaar

BESTAANDE TEKST

minder dan drie strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren.

In het geval bedoeld in het eerste lid, eerste streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in artikel 126/2, § 2:

a) zes maanden, indien er drie of vier strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

b) negen maanden, indien er vijf of zes strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

c) twaalf maanden, indien er zeven of meer dan zeven strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren.

In het geval bedoeld in het eerste lid, tweede streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in artikel 126/2, § 2:

a) zes maanden, indien er drie of vier strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

b) negen maanden, indien er vijf of zes strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

c) twaalf maanden, indien er zeven of meer dan zeven strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners

ONTWERP VAN WET

minder dan drie strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren.

In het geval bedoeld in het eerste lid, eerste streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in artikel 126/2, § 2:

a) zes maanden, indien er drie of vier strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

b) negen maanden, indien er vijf of zes strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

c) twaalf maanden, indien er zeven of meer dan zeven strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren.

In het geval bedoeld in het eerste lid, tweede streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in artikel 126/2, § 2:

a) zes maanden, indien er drie of vier strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

b) negen maanden, indien er vijf of zes strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

c) twaalf maanden, indien er zeven of meer dan zeven strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners

BESTAANDE TEKST

vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren.

Het aldus vastgestelde aantal strafbare feiten wordt naar boven of naar beneden afgerond op het dichtstbijzijnde gehele getal, al naargelang het eerste cijfer achter de komma al dan niet vijf bereikt.

De statistieken betreffende het aantal strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld over een gemiddelde van de drie voorbije kalenderjaren zijn afkomstig uit de Algemene Nationale Gegevensbank zoals bedoeld in artikel 44/7 van de wet van 5 augustus 1992 op het politieambt.

De grenzen van de gerechtelijke arrondissementen bedoeld in het eerste lid, eerste streepje, zijn vastgesteld in artikel 4 van de bijlage bij het Gerechtelijk Wetboek.

De grenzen van de politiezones bedoeld in het eerste lid, tweede streepje, zijn die welke zijn vermeld in de bijlage bij het koninklijk besluit van 24 oktober 2001 houdende de benaming van de politiezones.

De directie, bedoeld in artikel 44/11 van de wet van 5 augustus 1992 op het politieambt, stuurt de statistieken met betrekking tot het aantal strafbare feiten en de bewaringstermijn voor elk gerechtelijk arrondissement en elke politieke zone naar het Controleorgaan op de politieke informatie, dat binnen een maand na ontvangst van alle daartoe vereiste gegevens, deze valideert. Het Controleorgaan kan, met het oog op deze validatie, al de bevoegdheden uitoefenen die hem zijn toegekend bij titel 7 van de wet van 30 juli 2018.

De statistieken en de bewaringstermijnen worden door de directie bedoeld in artikel 44/11 van de wet van 5 augustus 1992 op het politieambt aan de door de Koning aangewezen dienst toegezonden, enkel nadat deze op de hoogte is gebracht van hun validatie door het Controleorgaan.

ONTWERP VAN WET

vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren.

Het aldus vastgestelde aantal strafbare feiten wordt naar boven of naar beneden afgerond op het dichtstbijzijnde gehele getal, al naargelang het eerste cijfer achter de komma al dan niet vijf bereikt.

De statistieken betreffende het aantal strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld over een gemiddelde van de drie voorbije kalenderjaren zijn afkomstig uit de Algemene Nationale Gegevensbank zoals bedoeld in artikel 44/7 van de wet van 5 augustus 1992 op het politieambt.

De grenzen van de gerechtelijke arrondissementen bedoeld in het eerste lid, eerste streepje, zijn vastgesteld in artikel 4 van de bijlage bij het Gerechtelijk Wetboek.

De grenzen van de politiezones bedoeld in het eerste lid, tweede streepje, zijn die welke zijn vermeld in de bijlage bij het koninklijk besluit van 24 oktober 2001 houdende de benaming van de politiezones.

De directie, bedoeld in artikel 44/11 van de wet van 5 augustus 1992 op het politieambt, stuurt de statistieken met betrekking tot het aantal strafbare feiten en de bewaringstermijn voor elk gerechtelijk arrondissement en elke politieke zone naar het Controleorgaan op de politieke informatie, dat binnen een maand na ontvangst van alle daartoe vereiste gegevens, deze valideert. Het Controleorgaan kan, met het oog op deze validatie, al de bevoegdheden uitoefenen die hem zijn toegekend bij titel 7 van de wet van 30 juli 2018.

De statistieken en de bewaringstermijnen worden door de directie bedoeld in artikel 44/11 van de wet van 5 augustus 1992 op het politieambt aan de door de Koning aangewezen dienst toegezonden, enkel nadat deze op de hoogte is gebracht van hun validatie door het Controleorgaan.

BESTAANDE TEKST

Op voorstel van de door de Koning aangewezen dienst stellen de ministers van Justitie en van Binnenlandse Zaken jaarlijks de lijst vast van de gerechtelijke arrondissementen en de politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn.

Na deze vaststelling, zendt de door de Koning aangewezen dienst de lijst van de gerechtelijke arrondissementen en politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn, naar de operatoren.

§ 2. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones die bepaald worden door het Coördinatieorgaan voor de Dreigingsanalyse, waar het dreigingsniveau, vastgesteld op basis van de evaluatie bedoeld in artikel 8, 1° en 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging, ten minste niveau 3 bedraagt, overeenkomstig artikel 11 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging, en zolang het dreigingsniveau van tenminste niveau 3 blijft bestaan voor deze zones.

Wanneer het dreigingsniveau ten minste niveau 3 bedraagt en deze het hele grondgebied bestrijkt, deelt het Coördinatieorgaan voor de Dreigingsanalyse dit onmiddellijk mee aan de dienst aangewezen door de Koning, zodat deze dienst de nodige maatregelen kan nemen om de operatoren in te lichten en tot een algemene en ongedifferentieerde bewaring van de gegevens bedoeld in artikel 126/2, § 2, over te gaan voor het gehele grondgebied.

De bewaarplicht bedoeld in het tweede lid wordt bevestigd bij koninklijk besluit, op gezamenlijk voorstel van de minister van Binnenlandse Zaken en de minister van Justitie. Bij ontstentenis van bevestiging bij koninklijk besluit, bekendgemaakt binnen de maand na de in het tweede lid bedoelde beslissing, wordt de

ONTWERP VAN WET

Op voorstel van de door de Koning aangewezen dienst stellen de ministers van Justitie en van Binnenlandse Zaken jaarlijks de lijst vast van de gerechtelijke arrondissementen en de politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn.

Na deze vaststelling, zendt de door de Koning aangewezen dienst de lijst van de gerechtelijke arrondissementen en politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn, naar de operatoren.

§ 2. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones die bepaald worden door het Coördinatieorgaan voor de Dreigingsanalyse, waar het dreigingsniveau, vastgesteld op basis van de evaluatie bedoeld in artikel 8, 1° en 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging, ten minste niveau 3 bedraagt, overeenkomstig artikel 11 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging, en zolang het dreigingsniveau van tenminste niveau 3 blijft bestaan voor deze zones.

Wanneer het dreigingsniveau ten minste niveau 3 bedraagt en deze het hele grondgebied bestrijkt, deelt het Coördinatieorgaan voor de Dreigingsanalyse dit onmiddellijk mee aan de dienst aangewezen door de Koning, zodat deze dienst de nodige maatregelen kan nemen om de operatoren in te lichten en tot een algemene en ongedifferentieerde bewaring van de gegevens bedoeld in artikel 126/2, § 2, over te gaan voor het gehele grondgebied.

De bewaarplicht bedoeld in het tweede lid wordt bevestigd bij koninklijk besluit, op gezamenlijk voorstel van de minister van Binnenlandse Zaken en de minister van Justitie. Bij ontstentenis van bevestiging bij koninklijk besluit, bekendgemaakt binnen de maand na de in het tweede lid bedoelde beslissing, wordt de

BESTAANDE TEKST

gegevensbewaring opgeheven en worden de operatoren daarvan zo spoedig mogelijk in kennis gesteld door de dienst aangewezen door de Koning. Na deze kennisgeving vernietigen de operatoren de tot dan toe en voor dit doel bewaarde gegevens.

§ 3. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, met name:

a) de havenfaciliteiten, de havens en de havenbeveiligingszones bedoeld in artikel 2.5.2.2, 3° tot 5°, van het Belgisch Scheepvaartwetboek;

b) de spoorwegstations in de zin van artikel 2, 5°, van de wet van 27 april 1981 op de politie van de spoorwegen;

c) de metro- en de pre-metrostations;

d) de luchthavens in de zin van artikel 2, punt 1), van Richtlijn 2009/12/EG van het Europees Parlement en de Raad van 11 maart 2009 inzake luchthavengelden, met inbegrip van de luchthavens die tot het kernnetwerk behoren, opgesomd in bijlage II, afdeling 2, van Verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk en tot intrekking van Besluit nr. 661/2010/EU, alsook de entiteiten die de bijbehorende installaties bedienen welke zich op de luchthavens bevinden;

e) de gebouwen bestemd voor de administratie van douane en accijnzen;

f) de gevangenen in de zin van artikel 2, 15°, van de basiswet van 12 januari 2005 betreffende het gevangeniswezen en de rechtspositie van de gedetineerden, de gemeenschapscentra voor minderjarigen die een als misdrijf omschreven feit hebben gepleegd, bedoeld in artikel 606 van het Wetboek van strafvordering, en de

ONTWERP VAN WET

gegevensbewaring opgeheven en worden de operatoren daarvan zo spoedig mogelijk in kennis gesteld door de dienst aangewezen door de Koning. Na deze kennisgeving vernietigen de operatoren de tot dan toe en voor dit doel bewaarde gegevens.

§ 3. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, met name:

a) de havenfaciliteiten, de havens en de havenbeveiligingszones bedoeld in artikel 2.5.2.2, 3° tot 5°, van het Belgisch Scheepvaartwetboek;

b) de spoorwegstations in de zin van artikel 2, 5°, van de wet van 27 april 1981 op de politie van de spoorwegen;

c) de metro- en de pre-metrostations;

d) de luchthavens in de zin van artikel 2, punt 1), van Richtlijn 2009/12/EG van het Europees Parlement en de Raad van 11 maart 2009 inzake luchthavengelden, met inbegrip van de luchthavens die tot het kernnetwerk behoren, opgesomd in bijlage II, afdeling 2, van Verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk en tot intrekking van Besluit nr. 661/2010/EU, alsook de entiteiten die de bijbehorende installaties bedienen welke zich op de luchthavens bevinden;

e) de gebouwen bestemd voor de administratie van douane en accijnzen;

f) de gevangenen in de zin van artikel 2, 15°, van de basiswet van 12 januari 2005 betreffende het gevangeniswezen en de rechtspositie van de gedetineerden, de gemeenschapscentra voor minderjarigen die een als misdrijf omschreven feit hebben gepleegd, bedoeld in artikel 606 van het Wetboek van strafvordering, en de

BESTAANDE TEKST

forensisch psychiatrische centra, bedoeld in artikel 3, 4°, c), van de wet van 5 mei 2014 betreffende de internering;

g) de wapenhandelaars en schietstanden zoals bedoeld in artikel 2, 1° en 19°, van de wet van 8 juni 2006 houdende regeling van economische en individuele activiteiten met wapens;

h) de inrichtingen bedoeld in artikel 3.1.a), van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;

i) de inrichtingen bedoeld in artikel 2, 1°, van het samenwerkingsakkoord van 16 februari 2016 tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken;

j) de gemeenten waar zich een of meerdere kritieke netwerkelementen of een of meerdere kritieke infrastructuren bevinden als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur en de uitvoeringsbesluiten ervan; indien het gehele netwerk als kritieke infrastructuur is aangemerkt, worden voor de toepassing van dit artikel alleen de kritieke netwerkelementen in aanmerking genomen;

k) de zetel van de NV Astrid en de gebouwen waarin haar centrale en provinciale datacentra zijn ondergebracht, alsmede de gebouwen waarin zich de centrale datacentra en de communicatieknooppunten van het beveiligde en gecodeerde communicatie- en informatiesysteem bevinden bedoeld in artikel 11, § 7, van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

l) de netwerk- en informatiesystemen die de verlening van essentiële diensten van aanbieders van essentiële diensten ondersteunen aangeduid op basis van de wet

ONTWERP VAN WET

forensisch psychiatrische centra, bedoeld in artikel 3, 4°, c), van de wet van 5 mei 2014 betreffende de internering;

g) de wapenhandelaars en schietstanden zoals bedoeld in artikel 2, 1° en 19°, van de wet van 8 juni 2006 houdende regeling van economische en individuele activiteiten met wapens;

h) de inrichtingen bedoeld in artikel 3.1.a), van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;

i) de inrichtingen bedoeld in artikel 2, 1°, van het samenwerkingsakkoord van 16 februari 2016 tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken;

j) de gemeenten waar zich een of meerdere kritieke netwerkelementen of een of meerdere kritieke infrastructuur bevinden als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur en de uitvoeringsbesluiten ervan; indien het gehele netwerk als kritieke infrastructuur is aangemerkt, worden voor de toepassing van dit artikel alleen de kritieke netwerkelementen in aanmerking genomen;

k) de zetel van de NV Astrid en de gebouwen waarin haar centrale en provinciale datacentra zijn ondergebracht, alsmede de gebouwen waarin zich de centrale datacentra en de communicatieknooppunten van het beveiligde en gecodeerde communicatie- en informatiesysteem bevinden bedoeld in artikel 11, § 7, van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

l) de netwerk- en informatiesystemen die de verlening van **diensten van essentiële entiteiten in de zin van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de**

BESTAANDE TEKST

van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

m) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, vastgesteld bij koninklijk besluit.

§ 4. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking, dit wil zeggen:

a) voor de openbare orde, de neutrale zones bedoeld in artikel 3 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten, en de ministeriële beleidscellen;

b) voor het wetenschappelijk en economisch potentieel, de gebouwen bestemd voor rechtspersonen waarvan het economisch en/of wetenschappelijk potentieel beschermd moet worden en die zijn opgenomen in een lijst die jaarlijks door de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid wordt opgesteld op voorstel van de minister van Justitie en de minister van Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad;

c) voor het transport, de autosnelwegen en de bijhorende openbare parkeerterreinen;

d) voor de nationale soevereiniteit en de instellingen opgericht door de Grondwet en de wetten, decreten of ordonnanties:

i) de wetgevende vergaderingen bedoeld in artikel 1 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten;

ONTWERP VAN WET

cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

m) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, vastgesteld bij koninklijk besluit.

§ 4. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking, dit wil zeggen:

a) voor de openbare orde, de neutrale zones bedoeld in artikel 3 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten, en de ministeriële beleidscellen;

b) voor het wetenschappelijk en economisch potentieel, de gebouwen bestemd voor rechtspersonen waarvan het economisch en/of wetenschappelijk potentieel beschermd moet worden en die zijn opgenomen in een lijst die jaarlijks door de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid wordt opgesteld op voorstel van de minister van Justitie en de minister van Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad;

c) voor het transport, de autosnelwegen en de bijhorende openbare parkeerterreinen;

d) voor de nationale soevereiniteit en de instellingen opgericht door de Grondwet en de wetten, decreten of ordonnanties:

i) de wetgevende vergaderingen bedoeld in artikel 1 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten;

BESTAANDE TEKST

- ii) de gemeentehuizen en de stadhuizen;
- iii) het koninklijk paleis;
- iv) de koninklijke domeinen;
- v) de gebouwen toegewezen aan de instellingen bedoeld in titel III, hoofdstukken 5 tot 7 van de Grondwet;
- vi) de gemeenten waar zich militaire domeinen bevinden;
- vii) de gebouwen bestemd voor de lokale en de federale politie, alsook voor de Veiligheid van de Staat;
- e) voor de integriteit van het nationaal grondgebied, de grensgemeenten;
- f) voor de belangrijke economische of financiële belangen, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid;
- i) de ziekenhuizen bedoeld in artikel 2 van de gecoördineerde wet van 10 juli 2008 op de ziekenhuizen en andere verzorgingsinrichtingen;
- ii) de Nationale Bank van België;
- g) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking vastgesteld bij koninklijk besluit.
- § 5. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen, dit wil zeggen:
- a) de ambassades en diplomatieke vertegenwoordigingen;

ONTWERP VAN WET

- ii) de gemeentehuizen en de stadhuizen;
- iii) het koninklijk paleis;
- iv) de koninklijke domeinen;
- v) de gebouwen toegewezen aan de instellingen bedoeld in titel III, hoofdstukken 5 tot 7 van de Grondwet;
- vi) de gemeenten waar zich militaire domeinen bevinden;
- vii) de gebouwen bestemd voor de lokale en de federale politie, alsook voor de Veiligheid van de Staat;
- e) voor de integriteit van het nationaal grondgebied, de grensgemeenten;
- f) voor de belangrijke economische of financiële belangen, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid;
- i) de ziekenhuizen bedoeld in artikel 2 van de gecoördineerde wet van 10 juli 2008 op de ziekenhuizen en andere verzorgingsinrichtingen;
- ii) de Nationale Bank van België;
- g) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking vastgesteld bij koninklijk besluit.
- § 5. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen, dit wil zeggen:
- a) de ambassades en diplomatieke vertegenwoordigingen;

BESTAANDE TEKST

b) de gebouwen bestemd voor de Europese Unie;

c) de gebouwen en de infrastructuur bestemd voor de NAVO;

d) de instellingen van de Europese Economische Ruimte;

e) de instellingen van de Verenigde Naties;

f) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen vastgesteld bij koninklijk besluit.

§ 6. Voor elke categorie van zone bedoeld in de paragrafen 3 tot 5, bepaalt de Koning de omvang van de perimeter van de zone.

Elke autoriteit die bevoegd is voor een van de aangelegenheden bedoeld in de paragrafen 3 tot 5, deelt jaarlijks op de door de Koning vastgestelde datum alleen aan de door de Koning aangewezen dienst de gegevens mee die nodig zijn voor de concrete vaststelling van de geografische zones.

Wanneer een geografische zone niet langer aan het bedoeld criterium voldoet, stellen deze autoriteiten alleen deze dienst daarvan onverwijld in kennis, zodat de verplichting tot bewaring bedoeld artikel 126/1, § 1, in deze zone zo spoedig mogelijk kan worden beëindigd.

Met uitzondering van de in paragraaf 4, b), bedoelde lijst van plaatsen, die door de inlichtingen- en veiligheidsdiensten exclusief ter beschikking van het Vast Comité I wordt gesteld, stelt de door de Koning aangewezen dienst de bijgewerkte lijst van zones bedoeld in de paragrafen 3 tot 5 waar de gegevensbewaring verplicht is, ter beschikking van het Controleorgaan op de politieke informatie en van het Vast Comité I, elk binnen het kader van hun bevoegdheden.

ONTWERP VAN WET

b) de gebouwen bestemd voor de Europese Unie;

c) de gebouwen en de infrastructuur bestemd voor de NAVO;

d) de instellingen van de Europese Economische Ruimte;

e) de instellingen van de Verenigde Naties;

f) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen vastgesteld bij koninklijk besluit.

§ 6. Voor elke categorie van zone bedoeld in de paragrafen 3 tot 5, bepaalt de Koning de omvang van de perimeter van de zone.

Elke autoriteit die bevoegd is voor een van de aangelegenheden bedoeld in de paragrafen 3 tot 5, deelt jaarlijks op de door de Koning vastgestelde datum alleen aan de door de Koning aangewezen dienst de gegevens mee die nodig zijn voor de concrete vaststelling van de geografische zones.

Wanneer een geografische zone niet langer aan het bedoeld criterium voldoet, stellen deze autoriteiten alleen deze dienst daarvan onverwijld in kennis, zodat de verplichting tot bewaring bedoeld artikel 126/1, § 1, in deze zone zo spoedig mogelijk kan worden beëindigd.

Met uitzondering van de in paragraaf 4, b), bedoelde lijst van plaatsen, die door de inlichtingen- en veiligheidsdiensten exclusief ter beschikking van het Vast Comité I wordt gesteld, stelt de door de Koning aangewezen dienst de bijgewerkte lijst van zones bedoeld in de paragrafen 3 tot 5 waar de gegevensbewaring verplicht is, ter beschikking van het Controleorgaan op de politieke informatie en van het Vast Comité I, elk binnen het kader van hun bevoegdheden.

BESTAANDE TEKST

Het Controleorgaan op de politionele informatie en het Vast Comité I kunnen, elk binnen het kader van hun bevoegdheden, aanbevelingen doen met betrekking tot deze lijst of het met redenen omklede bevel geven dat bepaalde geografische zones bedoeld in de paragrafen 3 tot 5, van de lijst geschrapt worden.

Op voorstel van de door de Koning aangewezen dienst stellen de minister van Defensie, de minister van Justitie, en de minister van Binnenlandse Zaken jaarlijks en bij elke wijziging bedoeld in het vijfde lid de lijst vast van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn.

Het ministeriële besluit bedoeld in het zesde lid wordt bekendgemaakt via vermelding in het Belgisch Staatsblad.

Na deze goedkeuring, zendt de door de Koning aangewezen dienst de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn, naar de operatoren.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de gegevens die door de bevoegde autoriteiten aan de door de Koning aangewezen dienst worden meegedeeld of van de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, of zijn medewerking verleent aan de uitvoering van dit artikel, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Artikel 164/1

Het Internetdomeinnaamregistreerbureau van het topniveaudomein ".be" :

1° heeft een permanente vestigingsplaats en exploitatiezetel in België, onverminderd de mogelijkheid voor de betrokkene om een gedeelte van zijn technische infrastructuur in het buitenland onder te brengen, met als enig doel

ONTWERP VAN WET

Het Controleorgaan op de politionele informatie en het Vast Comité I kunnen, elk binnen het kader van hun bevoegdheden, aanbevelingen doen met betrekking tot deze lijst of het met redenen omklede bevel geven dat bepaalde geografische zones bedoeld in de paragrafen 3 tot 5, van de lijst geschrapt worden.

Op voorstel van de door de Koning aangewezen dienst stellen de minister van Defensie, de minister van Justitie, en de minister van Binnenlandse Zaken jaarlijks en bij elke wijziging bedoeld in het vijfde lid de lijst vast van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn.

Het ministeriële besluit bedoeld in het zesde lid wordt bekendgemaakt via vermelding in het Belgisch Staatsblad.

Na deze goedkeuring, zendt de door de Koning aangewezen dienst de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn, naar de operatoren.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de gegevens die door de bevoegde autoriteiten aan de door de Koning aangewezen dienst worden meegedeeld of van de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, of zijn medewerking verleent aan de uitvoering van dit artikel, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Artikel 164/1

Het **register voor topleveldomeinnamen van het topleveldomein ".be"** :

1° heeft een permanente vestigingsplaats en exploitatiezetel in België, onverminderd de mogelijkheid voor de betrokkene om een gedeelte van zijn technische infrastructuur in het buitenland onder te brengen, met als enig doel

BESTAANDE TEKST

de betrouwbaarheid van de dienstverlening te verhogen;

2° heeft de vorm van een instelling zonder winstoogmerk;

3° brengt voor zijn prestaties een vergoeding in rekening die direct gerelateerd is aan de daadwerkelijk gemaakte kosten;

4° stelt, volgens de nadere regels bepaald door het Instituut, kosteloos de voorzieningen zoals vastgelegd door het Instituut beschikbaar aan het Instituut zodat zonder ernstige onderbreking van de dienstverlening de overgang naar een nieuw domeinnaamregistreerbureau op een efficiënte en doelmatige wijze kan plaatsvinden. Deze voorzieningen bevatten minimaal een geactualiseerd register van domeinnamen en alle bijbehorende informatie van de houders van domeinnamen volgens de periodiciteit en de nadere regels bepaald door het Instituut in een vorm die onmiddellijk kan worden gebruikt om in geval van ernstig falen van het Internetdomeinnaamregistreerbureau de continuïteit en de stabiliteit van het Belgische Internet te vrijwaren; en

5° organiseert, bestuurt en beheert het topniveaudomein ".be" in het algemeen belang en op basis van de beginselen van kwaliteit, efficiëntie, betrouwbaarheid en toegankelijkheid.

ONTWERP VAN WET

de betrouwbaarheid van de dienstverlening te verhogen;

2° heeft de vorm van een instelling zonder winstoogmerk;

3° brengt voor zijn prestaties een vergoeding in rekening die direct gerelateerd is aan de daadwerkelijk gemaakte kosten;

4° stelt, volgens de nadere regels bepaald door het Instituut, kosteloos de voorzieningen zoals vastgelegd door het Instituut beschikbaar aan het Instituut zodat zonder ernstige onderbreking van de dienstverlening de overgang naar een nieuw **register voor topleveldomeinnamen** op een efficiënte en doelmatige wijze kan plaatsvinden. Deze voorzieningen bevatten minimaal een geactualiseerd register van domeinnamen en alle bijbehorende informatie van de houders van domeinnamen volgens de periodiciteit en de nadere regels bepaald door het Instituut in een vorm die onmiddellijk kan worden gebruikt om in geval van ernstig falen van het **register voor topleveldomeinnamen** de continuïteit en de stabiliteit van het Belgische Internet te vrijwaren; en

5° organiseert, bestuurt en beheert het **topleveldomein** ".be" in het algemeen belang en op basis van de beginselen van kwaliteit, efficiëntie, betrouwbaarheid en toegankelijkheid.

Artikel 164/2

In geval van ernstig falen van het Internetdomeinnaamregistreerbureau van het topniveaudomein ".be" neemt het Instituut in het belang van de eindgebruiker en de Belgische economie de nodige maatregelen om de continuïteit en de stabiliteit van het Belgische Internet te vrijwaren.

Onder ernstig falen van het Internetdomeinnaamregistreerbureau wordt verstaan :

Artikel 164/2

In geval van ernstig falen van het **register voor topleveldomeinnamen** van het **topleveldomein** ".be" neemt het Instituut in het belang van de eindgebruiker en de Belgische economie de nodige maatregelen om de continuïteit en de stabiliteit van het Belgische Internet te vrijwaren.

Onder ernstig falen van het **register voor topleveldomeinnamen** wordt verstaan :

BESTAANDE TEKST

1° het hanteren van praktijken die illegaal of oneerlijk zijn en die de goede reputatie van het aan België gerelateerde topniveaudomein ".be" in het gedrang brengen, of

2° het onvermogen om de bereikbaarheid van een aanzienlijk aantal actieve domeinnamen van het topniveaudomein ".be" te verzekeren, of

3° het onvermogen om de taken van een Internet domeinnaamregistreerbureau, overeenkomstig de definitie van artikel 2, 48/1°, uit te voeren, of

4° het nalaten te voldoen aan de voorwaarden van artikel 164/1.

In geval van hoogdringendheid kan het Instituut onmiddellijk op voorlopige basis een nieuw Internetdomeinnaamregistreerbureau van het topniveaudomein ".be" aanwijzen. De kosten die dit tijdelijke Internetdomeinnaamregistreerbureau draagt in het kader van de door het Instituut opgedragen taken komen ten laste van het Instituut en worden achteraf gerecupereerd van het uiteindelijk aangewezen Internet domeinnaamregistreerbureau.

Onmiddellijk na het aanwijzen van het tijdelijke Internetdomeinnaamregistreerbureau of als een dergelijke aanwijzing niet nodig is, lanceert het Instituut een oproep tot kandidaten in het Belgisch Staatsblad en publiceert het een bestek, dat de minimale voorwaarden voor het uitvoeren van de activiteit van het Internetdomeinnaam-registreerbureau van het topniveaudomein ".be" bevat. De aanwijzing van het nieuwe Internetdomeinnaamregistreerbureau gebeurt op basis van een objectieve, transparante en niet-discriminerende procedure en objectieve, transparante en niet-discriminerende criteria.

De entiteit die aangewezen wordt als Internetdomeinnaamregistreerbureau van het topniveaudomein ".be" is gehouden tot het naleven van de minimale voorwaarden van het bestek en tot het naleven van alle verbintenissen

ONTWERP VAN WET

1° het hanteren van praktijken die illegaal of oneerlijk zijn en die de goede reputatie van het aan België gerelateerde **topleveldomein** ".be" in het gedrang brengen, of

2° het onvermogen om de bereikbaarheid van een aanzienlijk aantal actieve domeinnamen van het **topleveldomein** ".be" te verzekeren, of

3° het onvermogen om de taken van een **register voor topleveldomeinnamen**, overeenkomstig de definitie van artikel 2, 48/1°, uit te voeren, of

4° het nalaten te voldoen aan de voorwaarden van artikel 164/1.

In geval van hoogdringendheid kan het Instituut onmiddellijk op voorlopige basis een nieuw **register voor topleveldomeinnamen** van het **topleveldomein** ".be" aanwijzen. De kosten die dit tijdelijke **register voor topleveldomeinnamen** draagt in het kader van de door het Instituut opgedragen taken komen ten laste van het Instituut en worden achteraf gerecupereerd van het uiteindelijk aangewezen **register voor topleveldomeinnamen**.

Onmiddellijk na het aanwijzen van het tijdelijke **register voor topleveldomeinnamen** of als een dergelijke aanwijzing niet nodig is, lanceert het Instituut een oproep tot kandidaten in het Belgisch Staatsblad en publiceert het een bestek, dat de minimale voorwaarden voor het uitvoeren van de activiteit van het **register voor topleveldomeinnamen** van het **topleveldomein** ".be" bevat. De aanwijzing van het nieuwe **register voor topleveldomeinnamen** gebeurt op basis van een objectieve, transparante en niet-discriminerende procedure en objectieve, transparante en niet-discriminerende criteria.

De entiteit die aangewezen wordt als **register voor topleveldomeinnamen** van het **topleveldomein** ".be" is gehouden tot het naleven van de minimale voorwaarden van het bestek en tot het naleven van alle verbintenissen

BESTAANDE TEKST

die in de loop van de selectieprocedure zijn aangegaan.

ONTWERP VAN WET

die in de loop van de selectieprocedure zijn aangegaan.

Artikel 164/3

§ 1. Registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, verzamelen met de nodige zorgvuldigheid nauwkeurige en volledige domeinnaamregistratiegegevens en houden deze bij in een speciale database overeenkomstig het Unierecht inzake de bescherming van persoonsgegevens.

De domeinregistratiegegevens bedoeld in lid 1 bevatten de noodzakelijke informatie om de houders van de domeinnamen en de contactpunten die de domeinnamen onder de topleveldomeinnamen beheren, te identificeren en te contacteren. Die informatie omvat ten minste:

1° de domeinnaam;

2° de registratiedatum;

3° de naam van de houder van de domeinnaam, zijn e-mailadres en zijn telefoonnummer van;

4° het e-mailadres en het telefoonnummer van het contactpunt dat de domeinnaam beheert, indien deze verschillen van die van de houder van de domeinnaam.

De Koning kan, na advies van het Instituut, aanbieders van privacy- of proxy-registratiediensten en wederverkopers gelasten de domeinnaamregistratiegegevens die ze hebben verzameld te delen met de registrators, en de modaliteiten daarvan bepalen.

De naleving van de in dit artikel vastgestelde verplichtingen mag er niet toe leiden dat domeinnaamregistratiegegevens tweemaal worden verzameld bij de betrokkene. Daartoe werken registers voor topleveldomeinnamen en entiteiten die

BESTAANDE TEKST**ONTWERP VAN WET**

domeinnaamregistratiediensten verlenen, met elkaar samen.

De Koning kan, na advies van het Instituut, de modaliteiten van deze samenwerking preciseren.

§ 2. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, beschikken over beleidslijnen en procedures, waaronder verificatieprocedures, om ervoor te zorgen dat de in paragraaf 1, eerste lid, bedoelde databases juiste en volledige informatie bevatten. Deze beleidslijnen en procedures worden openbaar gemaakt.

Wanneer de domeinnaamregistratiegegevens opgesomd in paragraaf 1, tweede lid, van een domeinnaam onjuist, onnauwkeurig of onvolledig zijn, blokkeren de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen onmiddellijk het functioneren van deze domeinnaam tot de houder van de domeinnaam de registratiegegevens corrigeert zodat deze juist, nauwkeurig en volledig worden.

Indien de houder van de domeinnaam nalaat om dit te doen binnen de termijn zoals bepaald door het register voor topleveldomeinnamen of door de entiteit die domeinnaamregistratiediensten verleent, wordt de domeinnaam geannuleerd.

De transfer van een geblokkeerde domeinnaam naar een andere entiteit die domeinnaamregistratiediensten verleent, is verboden.

§ 3. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, maken de domeinnaamregistratiegegevens die geen persoonsgegevens zijn, onverwijld openbaar na de registratie van een domeinnaam.

BESTAANDE TEKST**ONTWERP VAN WET**

§ 4. Op naar behoren gemotiveerd verzoek, verschaffen de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, kosteloos, aan de legitieme toegangvragende partijen, de gegevens opgesomd in paragraaf 1, tweede lid, onverwijld en in elk geval binnen 72 uur na ontvangst van het verzoek, of 24 uur na ontvangst van het verzoek ingeval van hoogdringendheid.

Legitieme toegangvragende partijen omvatten elke natuurlijke of rechtspersoon die een verzoek indient voor het onderzoeken, vaststellen, uitoefenen of verdedigen van strafrechtelijke, burgerrechtelijke of andere bepalingen in het Unierecht of Belgisch recht.

Als legitieme toegangvragende partij worden beschouwd:

1° elke persoon in het kader van inbreuken op intellectuele eigendomsrechten of naburige rechten;

2° het Instituut;

3° het CCB;

4° het nationale CSIRT;

5° de politiediensten;

6° de gerechtelijke overheden;

7° de inlichtingen-en veiligheidsdiensten;

8° de FOD Economie;

9° de FOD Financiën.

De Koning kan, na advies van het Instituut, bijkomende legitieme toegangvragende partijen aan deze lijst toevoegen .

De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, stellen de verzoeker in staat om gemakkelijk, , zijn verzoek in te dienen.

BESTAANDE TEKST**ONTWERP VAN WET**

Er is sprake van hoogdringendheid indien het gebruik van een domeinnaam kan leiden tot levensbedreigende situaties en/of onherstelbare schade.

Elke weigering van een naar behoren gemotiveerd verzoek wordt gemotiveerd.

Het beleid en de procedures met betrekking tot de bekendmaking van deze gegevens worden openbaar gemaakt.

De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, mogen de houder van een domeinnaam niet op de hoogte brengen wanneer een verzoek zoals bedoeld in het eerste lid werd ingediend.

§ 5. Het Instituut kan een register voor topleveldomeinnamen of een entiteit die domeinnaamregistratiediensten verleent bindende instructies geven, met het oog op de naleving van dit artikel

§ 6. Indien een register voor topleveldomeinnamen of een entiteit die domeinnaamregistratiediensten verleent dit artikel, een in uitvoering van dit artikel aangenomen koninklijk besluit of een bindende instructie van het Instituut niet naleeft, kan het Instituut de in hoofdstuk 2 van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid bedoelde administratieve maatregelen of geldboetes opleggen."

Wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU

Artikel 71**Artikel 71**

De FSMA ziet toe op de toepassing van de bepalingen van deze wet en de besluiten en reglementen genomen ter uitvoering ervan, alsook van Verordening 600/2014 en van titel 2

De FSMA ziet toe op de toepassing van de bepalingen van deze wet en de besluiten en reglementen genomen ter uitvoering ervan, alsook van Verordening 600/2014 [...].

BESTAANDE TEKST

van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid. Voor de uitvoering van de voormelde opdrachten betreffende de wet van 7 april 2019 kan de FSMA niettemin een gespecialiseerde externe dienstverlener belasten met de uitvoering van welbepaalde toezichtopdrachten of de bijstand van een dergelijke dienstverlener verkrijgen.

Artikel 79

§ 1. Wanneer de FSMA een inbreuk vaststelt op de bepalingen van deze wet of de besluiten en reglementen genomen ter uitvoering ervan, of van Verordening 600/2014, kan zij de voor de inbreuk verantwoordelijke persoon bevelen om, binnen de termijn die zij bepaalt, de vastgestelde toestand te verhelpen alsook, desgevallend, om af te zien van herhaling van de gedraging die een inbreuk vormt. De FSMA kan ook elke natuurlijke of rechtspersoon die onjuiste of misleidende informatie heeft gepubliceerd of verspreid, bevelen om een rechtzetting te publiceren.

Onverminderd de overige maatregelen bepaald door de wet, kan de FSMA, indien de persoon tot wie zij een bevel heeft gericht met toepassing van het eerste lid, in gebreke blijft bij afloop van de hem opgelegde termijn, en op voorwaarde dat die persoon zijn middelen heeft kunnen laten gelden:

1° haar standpunt over de krachtens het eerste lid gedane vaststellingen openbaar maken, waarbij zij de identiteit van diegene die verantwoordelijk is voor de overtreding, en de aard van de overtreding verduidelijkt. Deze openbaarmaking gebeurt op kosten van de betrokken persoon;

2° de betaling van een dwangsom opleggen die per kalenderdag dat het bevel niet wordt nageleefd niet meer mag bedragen dan 50 000 euro, noch in het totaal 2 500 000 euro mag overschrijden;

ONTWERP VAN WET**Artikel 79**

§ 1. Wanneer de FSMA een inbreuk vaststelt op de bepalingen van deze wet of de besluiten en reglementen genomen ter uitvoering ervan, of van Verordening 600/2014, kan zij de voor de inbreuk verantwoordelijke persoon bevelen om, binnen de termijn die zij bepaalt, de vastgestelde toestand te verhelpen alsook, desgevallend, om af te zien van herhaling van de gedraging die een inbreuk vormt. De FSMA kan ook elke natuurlijke of rechtspersoon die onjuiste of misleidende informatie heeft gepubliceerd of verspreid, bevelen om een rechtzetting te publiceren.

Onverminderd de overige maatregelen bepaald door de wet, kan de FSMA, indien de persoon tot wie zij een bevel heeft gericht met toepassing van het eerste lid, in gebreke blijft bij afloop van de hem opgelegde termijn, en op voorwaarde dat die persoon zijn middelen heeft kunnen laten gelden:

1° haar standpunt over de krachtens het eerste lid gedane vaststellingen openbaar maken, waarbij zij de identiteit van diegene die verantwoordelijk is voor de overtreding, en de aard van de overtreding verduidelijkt. Deze openbaarmaking gebeurt op kosten van de betrokken persoon;

2° de betaling van een dwangsom opleggen die per kalenderdag dat het bevel niet wordt nageleefd niet meer mag bedragen dan 50 000 euro, noch in het totaal 2 500 000 euro mag overschrijden;

BESTAANDE TEKST

In spoedeisende gevallen kan de FSMA de maatregelen bedoeld in het tweede lid, 1°, nemen zonder voorafgaand bevel met toepassing van het eerste lid, mits de persoon zijn middelen heeft kunnen laten gelden. Ook wanneer er geen duidelijk identificeerbare voor de inbreuk verantwoordelijke persoon is, kan de FSMA zonder voorafgaand bevel een waarschuwing bekendmaken waarin desgevallend de aard van de inbreuk wordt genoemd.

§ 2. Onverminderd de overige maatregelen bepaald door de wet, kan de FSMA, indien zij overeenkomstig de artikelen 70 tot 72 van de wet van 2 augustus 2002 een inbreuk vaststelt op de bepalingen bedoeld in dit hoofdstuk of de besluiten of reglementen genomen ter uitvoering ervan, of van Verordening 600/2014, aan de overtreder een administratieve geldboete opleggen.

Een administratieve geldboete kan ook worden opgelegd aan één of meer leden van het bestuursorgaan en aan elke persoon die instaat voor de effectieve leiding, alsook aan elke andere natuurlijke persoon die verantwoordelijk wordt geacht voor de inbreuk.

§ 3. Het bedrag van de in paragraaf 2 bedoelde administratieve geldboetes wordt als volgt bepaald:

1° wanneer het een rechtspersoon betreft, mag de administratieve geldboete, voor hetzelfde feit of geheel van feiten, niet meer bedragen dan 5 000 000 euro, of, indien dit hoger is, tien procent van de totale jaaromzet van die rechtspersoon volgens de recentste jaarrekening die door het bestuursorgaan is opgesteld. Indien de betrokken rechtspersoon geen omzet realiseert, wordt onder "totale jaaromzet" begrepen de met omzet corresponderende soort inkomsten, hetzij overeenkomstig de toepasselijke Europese jaarrekeningenrichtlijnen hetzij, indien die niet van toepassing zijn op de betrokken rechtspersoon, overeenkomstig het nationale recht van de lidstaat waar de rechtspersoon gevestigd is. Indien de rechtspersoon een

ONTWERP VAN WET

In spoedeisende gevallen kan de FSMA de maatregelen bedoeld in het tweede lid, 1°, nemen zonder voorafgaand bevel met toepassing van het eerste lid, mits de persoon zijn middelen heeft kunnen laten gelden. Ook wanneer er geen duidelijk identificeerbare voor de inbreuk verantwoordelijke persoon is, kan de FSMA zonder voorafgaand bevel een waarschuwing bekendmaken waarin desgevallend de aard van de inbreuk wordt genoemd.

§ 2. Onverminderd de overige maatregelen bepaald door de wet, kan de FSMA, indien zij overeenkomstig de artikelen 70 tot 72 van de wet van 2 augustus 2002 een inbreuk vaststelt op de bepalingen bedoeld in dit hoofdstuk of de besluiten of reglementen genomen ter uitvoering ervan, of van Verordening 600/2014, aan de overtreder een administratieve geldboete opleggen.

Een administratieve geldboete kan ook worden opgelegd aan één of meer leden van het bestuursorgaan en aan elke persoon die instaat voor de effectieve leiding, alsook aan elke andere natuurlijke persoon die verantwoordelijk wordt geacht voor de inbreuk.

§ 3. Het bedrag van de in paragraaf 2 bedoelde administratieve geldboetes wordt als volgt bepaald:

1° wanneer het een rechtspersoon betreft, mag de administratieve geldboete, voor hetzelfde feit of geheel van feiten, niet meer bedragen dan 5 000 000 euro, of, indien dit hoger is, tien procent van de totale jaaromzet van die rechtspersoon volgens de recentste jaarrekening die door het bestuursorgaan is opgesteld. Indien de betrokken rechtspersoon geen omzet realiseert, wordt onder "totale jaaromzet" begrepen de met omzet corresponderende soort inkomsten, hetzij overeenkomstig de toepasselijke Europese jaarrekeningenrichtlijnen hetzij, indien die niet van toepassing zijn op de betrokken rechtspersoon, overeenkomstig het nationale recht van de lidstaat waar de rechtspersoon gevestigd is. Indien de rechtspersoon een

BESTAANDE TEKST

moederonderneming is of een dochteronderneming van de moederonderneming die een geconsolideerde jaarrekening moet opstellen, is de in aanmerking te nemen totale jaaromzet gelijk aan de totale jaaromzet, volgens de laatst beschikbare geconsolideerde jaarrekening als goedgekeurd door het bestuursorgaan van de uiteindelijke moederonderneming;

2° wanneer het een natuurlijk persoon betreft, mag de administratieve geldboete, voor hetzelfde feit of geheel van feiten, niet meer bedragen dan 5 000 000 euro.

Wanneer de overtreding de overtreder winst heeft opgeleverd of ervoor heeft gezorgd dat een verlies kon worden vermeden, mag dit maximum, ongeacht wat voorafgaat, tot het dubbele van die winst of dat verlies worden verhoogd.

§ 4. In geval van schending van de toepasselijke bepalingen van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid kan de FSMA de in artikel 52 van voormelde wet bepaalde administratieve sancties opleggen.

ONTWERP VAN WET

moederonderneming is of een dochteronderneming van de moederonderneming die een geconsolideerde jaarrekening moet opstellen, is de in aanmerking te nemen totale jaaromzet gelijk aan de totale jaaromzet, volgens de laatst beschikbare geconsolideerde jaarrekening als goedgekeurd door het bestuursorgaan van de uiteindelijke moederonderneming;

2° wanneer het een natuurlijk persoon betreft, mag de administratieve geldboete, voor hetzelfde feit of geheel van feiten, niet meer bedragen dan 5 000 000 euro.

Wanneer de overtreding de overtreder winst heeft opgeleverd of ervoor heeft gezorgd dat een verlies kon worden vermeden, mag dit maximum, ongeacht wat voorafgaat, tot het dubbele van die winst of dat verlies worden verhoogd.

[...]



Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis standard n° 65/2023 du 24 mars 2023
Version mise à jour en séance du 29 septembre 2023

Objet: Avis standard relatif à la rédaction des textes normatifs

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent.e.s : Mesdames Cédrine Morlière, Nathalie Raghenon et Griet Verhenneman et Messieurs Yves-Alexandre de Montjoye, Bart Preneel et Gert Vermeulen;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après « LCA »);

Vu l'article 25, alinéa 3, de la LCA selon lequel les décisions du Centre de Connaissances sont adoptées à la majorité des voix ;

Vu le règlement (UE) 2016/679 *du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après « RGPD »);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD »);

émet, le 24 mars 2023, l'avis standard suivant :

I. PORTÉE ET CONTEXTE DU PRÉSENT AVIS

1. Compte tenu du nombre exceptionnellement élevé de demandes d'avis dont l'Autorité est saisie et faute de disposer de moyens humains suffisants, l'Autorité n'est momentanément pas en mesure de procéder à un examen de toutes les demandes d'avis qu'elle reçoit. Lorsque le demandeur n'indique pas que le projet soumis pourrait occasionner des risques élevés pour les droits et libertés des personnes concernées et lorsque les réponses fournies par celui-ci dans le formulaire ne permettent pas non plus de déduire que de tels risques existeraient, l'Autorité peut décider de se référer au présent avis standard relatif à la rédaction des textes normatif¹.
2. Cet avis général rappelle les exigences principales auxquelles toute norme qui encadre des traitements de données à caractère personnel doit répondre. Il demeure par conséquent valable dans toutes les hypothèses de rédaction de textes normatifs. Il incombe à l'auteur d'un projet de norme de veiller à ce que celui-ci réponde effectivement aux exigences de qualité de la loi qui s'imposent en vertu du RGPD, lu en combinaison avec la Constitution, la Charte des droits fondamentaux de l'Union européenne et la Convention européenne des droits de l'homme (ci-après « la CEDH »).

II. RÉDACTION DES TEXTES NORMATIFS ET PROTECTION DES DONNÉES

A. Quant à l'exigence de nécessité et proportionnalité des traitements de données qui sont encadrés par le projet

3. L'Autorité rappelle que tout traitement de données à caractère personnel constitue une ingérence dans le droit au respect de la vie privée et le droit à la protection des données à caractère personnel. Une telle ingérence n'est admissible que pour autant qu'elle soit nécessaire et proportionnée à l'objectif légitime poursuivi.
4. Pour rappel, un traitement de données à caractère personnel est considéré comme étant nécessaire s'il constitue la mesure la moins attentatoire pour atteindre l'objectif légitime qu'il poursuit. L'auteur d'un texte normatif doit dès lors s'assurer qu'il n'y a pas d'autres mesures moins

¹ L'Autorité doit procéder à des choix stratégiques, compte tenu de ses missions en vertu du RGPD, des moyens dont elle dispose et des principes figurant dans le RGPD (comme le principe de l'approche basée sur les risques et le principe de 'responsabilité'). C'est la raison pour laquelle elle analyse d'abord les demandes d'avis, qui lui sont soumises en vertu de l'article 23 de la LCA et/ou de l'article 36.4 du RGPD, uniquement sur la base du formulaire.

Ce n'est que dans les cas où les réponses fournies dans le formulaire contiennent des indices sérieux que le projet de texte normatif implique un risque élevé que l'Autorité procède systématiquement à une analyse du projet de texte normatif proprement dit et émet concrètement un avis.

Dans les autres cas, et compte-tenu du flux de dossiers, l'Autorité ne procède pas à une analyse du texte du projet de texte normatif et communique les présentes lignes directrices générales. Il appartient au demandeur de s'assurer concrètement que le projet qu'il rédige répond effectivement aux exigences de qualité de la loi qui s'imposent en vertu du RGPD, de la Constitution, de la Charte des droits fondamentaux et de la CEDH.

attentatoires aux droits et libertés des personnes concernées qui permettent d'atteindre l'objectif poursuivi. Il faut donc que le traitement de données envisagé permette effectivement d'atteindre l'objectif poursuivi (critère d'efficacité), mais également qu'il constitue la mesure la moins intrusive dans les droits et libertés des personnes concernées (critère de nécessité au sens strict). Concrètement, cela signifie que s'il est possible d'atteindre l'objectif recherché au moyen d'une mesure moins intrusive pour le droit au respect de la vie privée ou le droit à la protection des données à caractère personnel, le traitement de données initialement envisagé ne pourra pas être mis en place.

5. Si la nécessité du traitement de données à caractère personnel est établie, il faut encore que l'auteur du texte normatif s'assure que celui-ci est bien proportionné (au sens strict) à l'objectif qu'il poursuit, c'est-à-dire qu'il faut qu'il existe un juste équilibre entre les différents intérêts en présence, droits et libertés des personnes concernées. En d'autres termes, il faut qu'il y ait un équilibre entre l'ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel et l'objectif que poursuit – et permet effectivement d'atteindre – ce traitement. Les avantages qui découlent du traitement de données en question doivent donc être plus importants que les inconvénients qu'il génère pour les personnes concernées (critère de proportionnalité au sens strict).
6. L'Autorité attire l'attention des auteurs de textes normatifs sur l'obligation de s'assurer que les traitements de données à caractère personnel encadrés par leurs projets ou qui seront mis en place en exécution de ceux-ci s'avèrent effectivement nécessaires et proportionnés à l'objectif poursuivi.

B. Quant à l'exigence de prévisibilité des traitements de données à caractère personnel

7. En outre, l'Autorité rappelle que chaque traitement de données à caractère personnel doit disposer d'une base juridique ou de légitimité figurant à l'article 6.1 du RGPD. Les traitements de données qui sont instaurés par une mesure normative sont presque toujours basés sur l'article 6.1, point c) ou e) du RGPD².
8. En vertu de l'article 22 de la Constitution, de l'article 8 de la CEDH et de l'article 6.3 du RGPD, de tels traitements doivent être prévus par une réglementation claire et précise, dont l'application doit

² Article 6.1 du RGPD : "Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : (...)

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; (...)

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; (...)"

être prévisible pour les personnes concernées³. En d'autres termes, la réglementation qui encadre ou dont la mise en œuvre implique des traitements de données doit répondre aux exigences de prévisibilité et de précision, de telle sorte qu'à sa lecture, les personnes concernées peuvent entrevoir clairement les traitements qui seront faits de leurs données et les circonstances dans lesquelles ces traitements sont autorisés.

9. Toutefois, cela ne signifie pas que chaque traitement de données doit être encadré par une norme *spécifique* régissant explicitement l'ensemble des sujets de protection des données dans son contexte. En effet, dans certains cas, la prévisibilité d'un traitement de données à caractère personnel qui est nécessaire à l'exécution d'une mission d'intérêt public pourra être assurée par la norme qui attribue cette mission au responsable du traitement et le RGPD (le cas échéant lus en combinaison avec d'autres normes également d'application).
10. La question se pose dès lors de savoir quand et dans quelle mesure un encadrement normatif *spécifique* est nécessaire. S'il n'y a pas de règle absolue ou de formule mathématique permettant de déterminer avec certitude quand il y a lieu de prévoir une norme spécifique pour assurer l'encadrement d'un traitement de données à caractère personnel nécessaire à l'exécution d'une mission d'intérêt public, et ce, en vue d'en assurer la prévisibilité, l'Autorité donne ci-dessous des indications à ce propos.
11. L'article 6.2 du RGPD prévoit que « *les États membres peuvent maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement pour ce qui est du traitement dans le but de respecter le paragraphe 1, points c) et e), en déterminant plus précisément les exigences spécifiques applicables au traitement ainsi que d'autres mesures visant à garantir un traitement licite et loyal, y compris dans d'autres situations particulières de traitement comme le prévoit le chapitre IX* ».
12. Le considérant 10 du RGPD, qui est relatif à l'article 6.2 du RGPD, précise que « *parallèlement à la législation générale et horizontale relative à la protection des données mettant en œuvre la directive 95/46/CE, il existe, dans les États membres, plusieurs législations sectorielles spécifiques dans des domaines qui requièrent des dispositions plus précises. Le présent règlement laisse aussi aux États membres une marge de manœuvre pour préciser des règles, y compris en ce qui concerne le traitement de catégories particulières de données à caractère personnel. A cet égard, le présent règlement n'exclut pas que le droit des États membres précise les circonstances des situations particulières de traitement y compris en fixant de manière plus précise les conditions dans lesquelles le traitement de données à caractère personnel est licite* » (c'est l'Autorité qui souligne).

³ Voir également le considérant 41 du RGPD.

13. De plus, le RGPD renvoie également, à plusieurs reprises, au droit national, que ce soit pour exiger un encadrement spécifique pour certains traitements de données à caractère personnel ou pour imposer l'adoption de mesures appropriées et spécifiques pour sauvegarder les droits fondamentaux et les intérêts des personnes concernées⁴.
14. L'Autorité identifie, notamment, trois situations dans lesquelles une norme nationale doit encadrer spécifiquement des traitements de données à caractère personnel :
 - lorsqu'il est n'est pas suffisant de renvoyer au libellé de **la norme attribuant une mission de service public pour assurer** la prévisibilité du traitement ; et/ou lorsqu'il y a lieu de **prévoir des garanties spécifiques** pour préserver les droits et libertés des personnes concernées ;
 - lorsqu'il est nécessaire de créer un traitement obligatoire de données à caractère personnel au sens de l'article art. 6.1.c RGPD. À ce propos, l'Autorité relève que la norme qui impose l'obligation légale doit, d'une part, spécifier la finalité concrète pour laquelle le traitement de données obligatoire doit être réalisé et, d'autre part, être claire et précise, de telle sorte que le responsable du traitement ne doit, en principe, pas avoir de marge d'appréciation quant à la façon de réaliser le traitement de données à caractère personnel nécessaire au respect de son obligation légale⁵.
 - lorsque le RGPD ou la LTD impose l'adoption d'une telle norme spécifique d'encadrement de traitement de données à caractère personnel, par exemple, pour prévoir des mesures spécifiques de sauvegarde pour les droits et libertés des personnes concernées. Ainsi par exemple, le RGPD impose une telle norme spécifique dans deux hypothèses, à savoir (1) lorsqu'il est envisagé d'encadrer des traitements portant sur des catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD (données relatives à l'origine raciale, données relatives à la santé, ...), ou encore au sens de l'article 10 du RGPD (données relatives à des condamnations, ...) et lorsqu'il est envisagé de prévoir dans ce cadre des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts des personnes concernées ou encore (2) lorsqu'il y a lieu de concilier dans une norme

⁴ C'est le cas, par exemple, pour les traitements portant sur des catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD (données relatives à l'origine raciale, données relatives à la santé, ...) qui sont nécessaires à l'exécution des obligations des responsables du traitement en matière de droit du travail ou encore des traitements portant sur ces données qui sont nécessaires pour des motifs d'intérêt public important.

⁵ Groupe de travail « Article 29 », *Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*, p. 22. L'Autorité rappelle qu'en tout état de cause, malgré une telle absence de marge d'appréciation, il incombe toujours au responsable du traitement de veiller à la conformité du traitement concerné à l'obligation en cause ainsi qu'au RGPD.

législative le droit d'accès du public aux documents officiels et le droit à la protection des données à caractère personnel (art. 86 RGDP).

15. Dans ce contexte, même si tout traitement de données à caractère personnel constitue une ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel, chacun de ces traitements (et donc toute ingérence dans le droit à la vie privée) ne doit, par conséquent, pas nécessairement être *spécifiquement* encadré par une norme de droit interne (comme par exemple, un chapitre spécifique consacré aux traitements de données à caractère personnel).
16. Pour ce qui est des traitements de données nécessaires à l'exécution d'une mission d'intérêt public, l'Autorité relève que, pour autant que les missions de service public (qui nécessitent la réalisation de traitement de données à caractère personnel) soient décrites et délimitées par le législateur de manière telle que les finalités de ces traitements puissent être considérées comme déterminées et explicites, et hormis les circonstances spécifiques décrites au § 14, il n'est pas systematiquement nécessaire d'encadrer *spécifiquement* ces traitements de données. En effet, sous cette condition, le RGPD peut, dans certains cas, suffire à encadrer lesdits traitements de données, notamment en l'absence de risque spécifique pour les droits et libertés des personnes concernées.
17. L'Autorité invite donc l'auteur d'un texte normatif à s'assurer que son projet répond bien à l'exigence de prévisibilité, de telle sorte qu'à sa lecture, éventuellement combinée à la lecture du cadre normatif pertinent, les personnes concernées soient en mesure d'entrevoir clairement les traitements qui seront faits de leurs données et les circonstances dans lesquelles ces traitements sont autorisés.

Pour le Centre de Connaissances,
Cédrine Morlière - Directrice du Centre de Connaissances



Autorité de protection des données
Gegevensbeschermingsautoriteit

Standaardadvies 65/2023 van 24 maart 2023

Bijgewerkte versie – zitting van 29 september 2023

Betreft: Standaardadvies betreffende de redactie van normatieve teksten

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit"),
aanwezig: de dames Cédrine Morlière, Nathalie Raghenon en Griet Verhenneman, en de heren Yves-Alexandre de Montjoye, Bart Preneel en Gert Vermeulen;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, met name de artikelen 23 en 26 (hierna "WOG");

Gelet op artikel 25, lid 3, WOG volgens hetwelk de beslissingen van het Kenniscentrum bij meerderheid van stemmen worden aangenomen;

Gelet op Verordening (EU) 2016/679 *van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Brengt op 24 maart 2023 het volgende standaardadvies uit.

I. TOEPASSINGSGEBIED EN CONTEXT VAN DIT ADVIES

1. Gezien het uitzonderlijk grote aantal adviesaanvragen dat momenteel bij de Autoriteit wordt ingediend en bij gebrek aan voldoende personele middelen, is de Autoriteit niet in staat om alle adviesaanvragen die zij ontvangt, te behandelen. Wanneer de aanvrager niet aangeeft dat het voorgelegde ontwerp aanleiding kan geven tot hoge risico's voor de rechten en vrijheden van de betrokkenen, en wanneer uit zijn antwoorden in het formulier ook niet kan worden afgeleid dat dergelijke risico's aanwezig zijn, kan de Autoriteit beslissen om te verwijzen naar voorliggend standaardadvies betreffende de redactie van normatieve teksten¹.
2. In dit algemene advies wordt gewezen op de belangrijkste eisen waaraan elke norm die de verwerking van persoonsgegevens regelt, moet voldoen. Het blijft dus geldig bij elke redactie van normatieve teksten. Het is de verantwoordelijkheid van de auteur van een ontwerpnorm om ervoor te zorgen dat deze daadwerkelijk voldoet aan de kwaliteitseisen van een wet, opgelegd op grond van de AVG en gelezen in samenhang met de Grondwet, het Handvest van de grondrechten van de Europese Unie en het Europees Verdrag tot bescherming van de rechten van de mens (hierna "het EVRM").

II. REDACTIE VAN NORMATIEVE TEKSTEN EN GEGEVENSBESCHERMING

A. Wat betreft de vereiste van noodzakelijkheid en evenredigheid van de gegevensverwerkingen die door het ontwerp worden geregeld

3. De Autoriteit herinnert eraan dat elke verwerking van persoonsgegevens een inmenging vormt in het recht op eerbiediging van de persoonlijke levenssfeer en het recht op bescherming van persoonsgegevens van de betrokkenen. Een dergelijke inmenging is enkel toelaatbaar als zij noodzakelijk is en evenredig met het nagestreefde gerechtvaardigde doel.
4. Ter herinnering: de verwerking van persoonsgegevens wordt als noodzakelijk beschouwd als zij de minst ingrijpende maatregel vormt om het ermee nagestreefde gerechtvaardigde doel te

¹ De Autoriteit dient strategische keuzes te maken, rekening houdend met de nieuwe taken die haar krachtens de AVG zijn opgelegd, de middelen waarover zij beschikt en de beginselen die in de AVG zijn vervat (zoals het beginsel van de risico-gebaseerde benadering en het beginsel van de 'verantwoordingsplicht'). Daarom onderzoekt zij de adviesaanvragen die haar op grond van artikel 23 van de WOG en/of artikel 36, lid 4, van de AVG worden voorgelegd eerst uitsluitend op basis van het formulier.

Alleen in gevallen waarin de antwoorden in het formulier ernstige aanwijzingen bevatten dat het ontwerp van normatieve tekst een hoog risico inhoudt, gaat de Autoriteit over tot een systematische analyse van het ontwerp van normatieve tekst zelf en brengt zij een concreet advies uit.

In de andere gevallen en gezien de toevloed aan dossiers, gaat de Autoriteit niet over tot een analyse van de tekst van het ontwerp van normatieve tekst en geeft zij voorliggende algemene richtlijnen. Het is aan de aanvrager om er in de praktijk voor te zorgen dat het ontwerp dat hij redigeert, daadwerkelijk voldoet aan de kwaliteitsvereisten van de wet die door de AVG, de Grondwet, het Handvest van de grondrechten en het EVRM, worden opgelegd.

bereiken. De auteur van een normatieve tekst moet daarom nagaan of er geen andere maatregelen zijn die minder ingrijpend zijn voor de rechten en vrijheden van de betrokkenen, en waarmee het nagestreefde doel kan worden bereikt. De beoogde gegevensverwerking moet dus toelaten het nagestreefde doel te bereiken (criterium van doeltreffendheid), maar moet tevens de maatregel zijn die het minst ingrijpt in de rechten en vrijheden van de betrokkenen (criterium van noodzakelijkheid in strikte zin). Concreet betekent dit dat als het mogelijk is het beoogde doel te bereiken met een maatregel die minder ingrijpt in het recht op eerbiediging van de persoonlijke levenssfeer of het recht op bescherming van persoonsgegevens, de oorspronkelijk beoogde gegevensverwerking niet ingevoerd mag worden.

5. Wanneer de noodzaak van de verwerking van persoonsgegevens vaststaat, moet de auteur van de normatieve tekst er zich nog van vergewissen dat de verwerking evenredig is (in strikte zin) met het beoogde doel, d.w.z. dat er een juist evenwicht moet worden gevonden tussen de verschillende belangen die op het spel staan en de rechten en vrijheden van de betrokkenen. Met andere woorden, er moet een evenwicht zijn tussen de inmenging in het recht op eerbiediging van de persoonlijke levenssfeer en op bescherming van persoonsgegevens, en het doel dat met die verwerking wordt beoogt en dat daadwerkelijk kan worden bereikt. De voordelen die voortvloeien uit de gegevensverwerking in kwestie moeten dus opwegen tegen de nadelen ervan voor de betrokkenen (criterium van evenredigheid in strikte zin).
6. De Autoriteit vestigt de aandacht van de auteurs van normatieve teksten op de verplichting ervoor te zorgen dat de verwerkingen van persoonsgegevens die door het ontwerp worden geregeld of in uitvoering daarvan zullen worden geregeld, werkelijk noodzakelijk zijn en evenredig met het nagestreefde doel.

B. Wat betreft de vereiste van voorspelbaarheid van de verwerking van persoonsgegevens

7. Verder herinnert de Autoriteit eraan dat elke verwerking van persoonsgegevens een rechtsgrond of een rechtmatigheidsgrond moet hebben, zoals bepaald in artikel 6, lid 1, van de AVG. Gegevensverwerkingen die bij een normatieve maatregel zijn ingevoerd, zijn bijna altijd gebaseerd op artikel 6, lid 1, punt c) of e), van de AVG².

²Artikel 6, lid 1, van de AVG: "De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan: (...)

c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust; (...)

e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen; (...)"

8. Krachtens artikel 22 van de Grondwet, artikel 8 van het EVRM en artikel 6, lid 3, van de AVG, moet voor dergelijke verwerkingen duidelijke en nauwkeurige regelgeving gelden, waarvan de toepassing voor de betrokkenen voorzienbaar moet zijn³. Met andere woorden, de regelgeving die de gegevensverwerking regelt of waarvan de toepassing een gegevensverwerking met zich meebrengt, moet voldoen aan de vereisten van voorspelbaarheid en nauwkeurigheid, zodat bij lezing ervan, de betrokkenen duidelijk kunnen begrijpen welke verwerkingen met hun gegevens zullen worden verricht en onder welke omstandigheden deze verwerkingen zijn toegestaan.
9. Dit betekent echter niet dat voor elke gegevensverwerking een *specifieke* norm moet gelden die uitdrukkelijk alle gegevensbeschermingskwesties in de betrokken context regelt. In bepaalde gevallen kan de voorspelbaarheid van een verwerking van persoonsgegevens die noodzakelijk is voor de vervulling van een taak van algemeen belang immers worden gewaarborgd door de norm die deze taak toekent aan de verwerkingsverantwoordelijke, en de AVG (in voorkomend geval gelezen in combinatie met andere normen die eveneens van toepassing zijn).
10. De vraag rijst dan wanneer en in welke mate een *specifiek* normatief kader noodzakelijk is. Aangezien er geen absolute regel of mathematische formule is om met zekerheid te bepalen wanneer moet worden voorzien in een specifieke norm om een verwerking van persoonsgegevens te regelen die noodzakelijk is voor de vervulling van een taak van algemeen belang, met het oog op de voorspelbaarheid ervan, geeft de Autoriteit hieronder richtsnoeren in dit verband.
11. Artikel 6, lid 2, van de AVG bepaalt: *"De lidstaten kunnen specifiekere bepalingen handhaven of invoeren ter aanpassing van de manier waarop de regels van deze verordening met betrekking tot de verwerking met het oog op de naleving van lid 1, punten c) en e), worden toegepast; hiertoe kunnen zij een nadere omschrijving geven van specifieke voorschriften voor de verwerking en andere maatregelen om een rechtmatige en behoorlijke verwerking te waarborgen, ook voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX."*
12. Overweging 10 van de AVG, die betrekking heeft op artikel 6, lid 2, van de AVG, bepaalt: *"In samenhang met de algemene en horizontale wetgeving inzake gegevensbescherming ter uitvoering van Richtlijn 95/46/EG beschikken de lidstaten over verscheidene sectorgebonden wetten op gebieden waar behoefte is aan meer specifieke bepalingen. Deze verordening biedt de lidstaten ook ruimte om eigen regels voor de toepassing vast te stellen, onder meer wat de verwerking van bijzondere persoonsgegevenscategorieën ("gevoelige gegevens") betreft. In zoverre staat deze verordening niet in de weg aan lidstatelijk recht waarin specifieke situaties op het gebied van gegevensverwerking nader worden omschreven, meer bepaald door nauwkeuriger*

³ Zie ook overweging 41 van de AVG.

*te bepalen in welke gevallen verwerking van persoonsgegevens rechtmatig geschiedt".
(onderstreept door de Autoriteit)*

13. Bovendien verwijst de AVG ook meermaals naar het nationale recht, hetzij om een specifiek kader voor bepaalde verwerkingen van persoonsgegevens te eisen, hetzij om het treffen van passende en specifieke maatregelen ter bescherming van de grondrechten en de belangen van de betrokkenen, op te leggen.⁴
14. De Autoriteit stelt met name drie situaties vast waarin een nationale norm de verwerking van persoonsgegevens specifiek moet regelen:
 - wanneer het niet voldoende is om te verwijzen naar de formulering van **de norm waarbij de publieke taak wordt toegekend** om de voorspelbaarheid van de verwerking te **waarborgen**, en wanneer moet worden **voorzien in specifieke waarborgen** om de rechten en vrijheden van de betrokkenen te beschermen;
 - wanneer het noodzakelijk is om een verplichte verwerking van persoonsgegevens in te stellen in de zin van artikel 6, lid 1, punt c), van de AVG. In dat verband wijst de Autoriteit erop dat de norm die de wettelijke verplichting oplegt, enerzijds het concrete doel moet preciseren waarvoor de verplichte gegevensverwerking moet worden uitgevoerd, en anderzijds duidelijk en nauwkeurig moet zijn, zodat de verwerkingsverantwoordelijke in principe geen beoordelingsmarge heeft met betrekking tot de manier waarop de verwerking van persoonsgegevens die nodig is om aan zijn wettelijke verplichting te voldoen, wordt uitgevoerd⁵.
 - wanneer de AVG of de WVG de vaststelling van een dergelijke specifieke norm voor de verwerking van persoonsgegevens oplegt, om bijvoorbeeld te voorzien in specifieke beschermingsmaatregelen voor de rechten en vrijheden van de betrokkenen. Zo legt de AVG een dergelijke specifieke norm op in twee gevallen, namelijk (1) wanneer wordt overwogen de verwerking van bijzondere categorieën van persoonsgegevens in de zin van artikel 9 van de AVG (gegevens over raciale afkomst, gegevens over gezondheid, ...) of in de zin van artikel 10 van de AVG (gegevens betreffende veroordelingen, enz.) te regelen en wanneer in dit verband wordt overwogen te voorzien in passende en specifieke maatregelen om de grondrechten en de belangen van de betrokkenen te vrijwaren, of (2) wanneer in een wettelijke norm het recht van toegang van het publiek tot officiële documenten in overeenstemming moet worden gebracht met het recht op bescherming van persoonsgegevens (artikel 86 van de AVG).

Advies 65/2023 - 6/7

⁴ Dat is bijvoorbeeld het geval voor verwerkingen betreffende bijzondere categorieën van persoonsgegevens in de zin van artikel 9 van de AVG (gegevens over ras, gegevens over de gezondheid,...) die nodig zijn voor de uitvoering van de verplichtingen van verwerkingsverantwoordelijken op het gebied van arbeidsrecht, of voor verwerkingen betreffende deze gegevens die nodig zijn om redenen van zwaarwegend algemeen belang.

⁵ Groep Artikel 29, *advies 06/2014 van over het begrip "gerechtvaardigd belang van de voor de verwerking verantwoordelijke" in artikel 7 van Richtlijn 95/46/EG*, blz. 22. De Autoriteit herinnert eraan dat, ondanks een dergelijk gebrek aan beoordelingsmarge, het hoe dan ook aan de verwerkingsverantwoordelijke is om ervoor te zorgen dat de betrokken verwerking in overeenstemming is met de verplichting in kwestie en met de AVG.

15. In deze context, ook al vormt elke verwerking van persoonsgegevens een inmenging in het recht op eerbiediging van de persoonlijke levenssfeer en op bescherming van persoonsgegevens, toch moet niet elke verwerking (en dus elke inmenging in het recht op privacy) noodzakelijkerwijs specifiek geregeld worden door een norm van nationaal recht (zoals bijvoorbeeld een specifiek hoofdstuk dat aan de verwerking van persoonsgegevens is gewijd).
16. Wat betreft gegevensverwerkingen die noodzakelijk zijn voor de vervulling van een taak van algemeen belang, merkt de Autoriteit op dat, voor zover de publieke taken (waarvoor de verwerking van persoonsgegevens nodig is) door de wetgever op zodanige wijze zijn omschreven en afgebakend dat de doeleinden van deze verwerkingen als welbepaald en uitdrukkelijk kunnen worden beschouwd, en afgezien van de specifieke omstandigheden beschreven in § 14, het niet systematisch nodig is om een *specifiek* kader voor *deze* gegevensverwerkingen te bieden. Onder deze voorwaarde kan de AVG immers in bepaalde gevallen volstaan om de genoemde gegevensverwerkingen te regelen, met name wanneer er geen specifiek risico voor de rechten en vrijheden van de betrokkenen bestaat.
17. De Autoriteit verzoekt de auteur van de normatieve tekst derhalve om ervoor te zorgen dat zijn ontwerp voldoet aan de vereiste van voorspelbaarheid, zodat bij de lezing ervan, eventueel in combinatie met de lezing van het relevante normatieve kader, de betrokkenen duidelijk kunnen begrijpen welke verwerkingen met hun gegevens zullen worden uitgevoerd en onder welke omstandigheden deze verwerkingen zijn toegestaan.

Voor het Kenniscentrum,
(get.) Cédrine Morlière - Directeur