DOC 55 **3887/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

7 mars 2024

PROJET DE LOI

modifiant la loi relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.)

Sommaire Pages

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

7 maart 2024

WETSONTWERP

tot wijziging van de wet betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E)

Inhoud Blz.

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 7 mars 2024.	*De regering heeft dit wetsontwerp op 7 maart 2024 ingediend.*
Le "bon à tirer" a été reçu à la Chambre le 11 mars 2024.	*De "goedkeuring tot drukken" werd op 11 maart 2024 door de Kamer ontvangen.*

N-VA	:	*Nieuw-Vlaamse Alliantie*
Ecolo-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 55e législature, suivi du numéro de base et numéro de suivi*	*DOC 55 0000/000*	*Parlementair document van de 55e 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 (beigekleurig papier)*

RÉSUMÉ

Le présent projet de loi a pour objectif de compléter la loi relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.) en insérant une nouvelle section qui clarifie la procédure de recours contre les décisions prises par l'U.N.E. sur les demandes d' autorisations de voyage.

Ces décisions pourront faire l'objet d'un recours en annulation devant le Conseil du contentieux des étrangers.

SAMENVATTING

Dit wetsontwerp heeft tot doel de wet betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E.) aan te vullen door een nieuwe afdeling in te voegen die de procedure voor een beroep tegen de beslissingen genomen door de E.N.E. over aanvragen tot reisautorisaties, verduidelijkt.

Deze beslissingen zullen het voorwerp kunnen uitmaken van een annulatieberoep bij de Raad voor Vreemdelingenbetwistingen.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS

EXPOSÉ GÉNÉRAL

Ce projet de loi vise à insérer dans la loi du… relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.), les dispositions relatives aux recours dont peuvent faire l'objet les décisions de l'U.N.E. relatives aux demandes d'autorisation de voyage. Ces dispositions relèvent en effet d'une matière visée à l'article 78 de la Constitution et doivent donc faire l'objet d'un projet de loi à part entière. Le choix d'une loi modificative s'est imposé en vue d'assurer aux personnes concernées un accès plus aisé aux informations relatives aux recours dont elles disposent. Cela leur évite en effet d'aller consulter une autre loi.

COMMENTAIRE DES ARTICLES

Article 3

L'article 3 du projet de loi prévoit l'insertion d'une nouvelle section dans la loi du XXX relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.) intitulée "Des recours contre les décisions de l'U.N.E.".

Article 4

Cet article insère les trois articles que comporte la nouvelle section créée par l'article 3.

Afin d'éviter tout doute sur la compétence du Conseil du contentieux des étrangers (ci-après "CCE"), l'article 26/1 le désigne expressément comme la juridiction habilitée à traiter les recours contre les décisions ETIAS relatives aux demandes d'autorisation de voyage. La question s'est en effet posée eu égard à la nature de l'autorisation de voyage et aux objectifs variés du Règlement ETIAS (voyez l'article 4). Les "décisions" sont définies à l'article 3, alinéa 2, 1°, de la loi relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.) et comprennent également les avis motivés

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

ALGEMENE TOELICHTING

Dit wetsontwerp heeft tot doel in de wet van… betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E.) de bepalingen op te nemen betreffende het beroep tegen de beslissingen van de E.N.E. betreffende aanvragen voor reisautorisaties. Deze bepalingen zijn namelijk een aangelegenheid die in artikel 78 van de Grondwet wordt bedoeld en moeten dus het voorwerp uitmaken van een geheel afzonderlijk wetsontwerp. De keuze voor een wijzigingswet was noodzakelijk om ervoor te zorgen dat de betrokken personen gemakkelijker toegang hebben tot informatie over de beroepsmogelijkheden waarover zij beschikken. Hierdoor moeten zij inderdaad geen andere wet gaan raadplegen.

TOELICHTING BIJ DE ARTIKELEN

Artikel 3

Artikel 3 van het wetsontwerp voorziet in de invoeging van een nieuwe afdeling in de wet van XXX betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E.) met als opschrift "Beroep tegen de beslissingen van de E.N.E.".

Artikel 4

Dit artikel voegt de drie artikelen in van de nieuwe afdeling die bij artikel 3 is gecreëerd.

Om elke twijfel over de bevoegdheid van de Raad voor Vreemdelingenbetwistingen (hierna "RVV") te vermijden, wijst artikel 26/1 haar uitdrukkelijk aan als de rechterlijke instantie die bevoegd is om beroepen tegen ETIAS-beslissingen betreffende aanvragen voor reisautorisaties, te behandelen. Deze vraag is inderdaad gerezen in het licht van de aard van de reisautorisatie en de verschillende doelstellingen van de ETIAS-Verordening (zie artikel 4). De "beslissingen" worden gedefinieerd in artikel 3, lid 2, 1°, van de wet betreffende de oprichting en de organisatie van de opdrachten van

rendus dans le cadre de la procédure de consultation visée à l'article 28 du Règlement ETIAS.

Elles ne concernent pas les décisions prises dans le cadre de l'article 64 du Règlement ETIAS en cas de refus d'une demande de modification ou d'effacement de données personnelles dans le système central ETIAS. Les recours possibles contre ces décisions spécifiques sont mentionnés à l'article 33 de la loi du XXX relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.).

Dans son Avis (point 11), l'APD a demandé de justifier le choix du recours en annulation devant le CCE. Il n'y a en fait pas eu de réel choix. Il a été tenu compte du fait que le recours en pleine juridiction devant le CCE est actuellement réservé aux décisions prises par le CGRA en matière d'asile. Pour toutes les autres décisions prises sur une demande d'entrée, de séjour ou d'établissement ou relatives à l'éloignement du territoire, seul un recours en annulation est possible. Une décision relative à une demande d'autorisation de voyage entre dans cette catégorie de décisions, notamment dans la mesure où disposer d'un ETIAS valable est une condition d'entrée sur le territoire. Les décisions relatives aux demandes de visas, qui sont largement similaires dans leurs effets, sont également susceptibles uniquement d'un recours en annulation. On imagine donc mal envisager un recours en pleine juridiction pour les décisions ETIAS qui n'est pas prévu pour les décisions VISA.

Les décisions ETIAS peuvent être prises par les deux sections de l'U.N.E., qui relèvent chacune d'un ministre différent: le ministre de l'Intérieur en ce qui concerne la section du Centre de crise national et le secrétaire d'État à l'asile et à la migration en ce qui concerne la section de l'Office des Étrangers. L'article 26/2 est calqué sur l'article 74/1 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, lequel vise à permettre au ministre compétent d'être représenté en audience dans le cadre de tout litige relatif à la loi sur les étrangers par un fonctionnaire désigné à cet effet, tant devant les juridictions nationales judiciaires ou administratives que devant les juridictions internationales. La compétence de représentation du fonctionnaire désigné à cet effet s'étend également à la rédaction, à l'introduction et à la signature des pièces de procédures. Il a semblé opportun de prévoir cette possibilité pour les deux sections de l'U.N.E.

de ETIAS Nationale Eenheid (E.N.E.) en omvatten ook de met redenen omklede adviezen die geleverd werden in het kader van de raadplegingsprocedure bedoeld in artikel 28 van de ETIAS-Verordening.

Zij hebben geen betrekking op de beslissingen genomen in het kader van artikel 64 van de ETIAS-Verordening in geval van weigering van een verzoek tot wijziging of verwijdering van persoonsgegevens in het centrale systeem van ETIAS. De beroepsmogelijkheden tegen deze specifieke beslissingen worden vermeld in artikel 33 van de wet van XXX betreffende de oprichting en de organisatie van de opdrachten van de nationale ETIAS-eenheid (E.N.E.).

In haar Advies (punt 11), heeft de GBA gevraagd om de keuze voor een annulatieberoep bij de RVV te rechtvaardigen. Er was in feite geen echte keuze. Er werd rekening gehouden met het feit dat het volledig gerechtelijk beroep voor de RVV momenteel voorbehouden is voor beslissingen genomen door het CGVS in asielzaken. Voor alle andere beslissingen genomen over een aanvraag tot toegang, tot verblijf of tot vestiging of met betrekking tot de verwijdering van het grondgebied, is enkel een annulatieberoep mogelijk. Een beslissing over een aanvraag voor een reisautorisatie valt binnen deze categorie van beslissingen, voornamelijk in de mate dat het beschikken over een geldige ETIAS een voorwaarde voor toegang tot het grondgebied is. De beslissingen met betrekking tot visumaanvragen, die in grote lijnen hetzelfde effect hebben, zijn eveneens enkel onderworpen aan een annulatieberoep. Het is daarom moeilijk voor te stellen dat voor ETIAS-beslissingen een volledig gerechtelijk beroep ingediend kan worden dat niet voorzien is voor visumbeslissingen.

ETIAS-beslissingen kunnen genomen worden door de twee secties van de E.N.E., die elk onder het gezag van een andere minister vallen: de minister van Binnenlandse Zaken voor de sectie van het Nationaal Crisiscentrum en de staatssecretaris voor asiel en migratie voor de sectie van de Dienst Vreemdelingenzaken. Het artikel 26/2 is geïnspireerd op artikel 74/1 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, dat ertoe strekt dat de bevoegde minister zich, zowel voor nationale rechterlijke of administratieve instanties als voor internationale instanties, in elk geschil met betrekking tot de vreemdelingenwet in rechte kan laten vertegenwoordigen door een ambtenaar die daartoe is aangewezen. De vertegenwoordigingsbevoegdheid van de daartoe aangewezen ambtenaar strekt zich ook uit tot het opstellen, inleiden en ondertekenen van procedurestukken. Het leek dienstig in deze mogelijkheid te voorzien voor de twee secties van de E.N.E.

L'article 26/3 prévoit que le service des litiges de chaque section de l'U.N.E. assurera la gestion des recours qui leur sont attribués en vertu de la loi.

Si le financement européen s'avère insuffisant, un financement national sera prévu pour la gestion des litiges.

La ministre de l'Intérieur,

Annelies Verlinden

Artikel 26/3 voorziet dat de dienst geschillen van elke sectie van de E.N.E. het beheer van beroepen zal verzekeren die haar door de wet zijn toegewezen.

Wanneer blijkt dat Europese financiering niet volstaat, zal nationale financiering voorzien worden voor het beheer van geschillen.

De minister van Binnenlandse Zaken,

Annelies Verlinden

AVANT-PROJET DE LOI

soumis à l'avis du Conseil d'État

Avant-projet de loi modifiant la loi relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.)

Art. 1er. La présente loi règle une matière visée à l'article 78 de la Constitution.

Art. 2. Dans le chapitre 6 de la loi du XXX relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.), il est inséré une section 1/1 intitulée "Des recours contre les décisions de l'U.N.E.".

Art 3. Dans la section 1/1, insérée par l'article 2, sont insérés les articles suivants:

"Art. 30/1. Les décisions prises par l'U.N.E. sont susceptibles de recours en annulation devant le Conseil du contentieux des étrangers, visé à l'article 39/1 de la loi du 15 décembre 1980.

Art. 30/2. La représentation de l'État peut être assurée dans toutes les contestations relatives à l'application de la présente loi par les ministres compétents ou leurs délégués.

Art. 30/3. Les services de litiges au sein de chaque section de l'U.N.E. assurent la gestion des recours qui leurs sont attribués conformément à l'article 7, 6°, et 26, § 2, point 3°."

VOORONTWERP VAN WET

onderworpen aan het advies van de Raad van State

Voorontwerp van wet tot wijziging van de wet betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E)

Art. 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

Art. 2. In hoofdstuk 6 van de wet van XXX betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E) wordt een afdeling 1/1 ingevoegd, met als titel "Beroep tegen de beslissingen van de E.N.E.".

Art. 3. In afdeling 1/1, ingevoegd door artikel 2, worden de volgende artikelen ingevoegd:

"Art. 30/1. Tegen de beslissingen genomen door de E.N.E. kan beroep tot nietigverklaring worden ingesteld bij de Raad voor Vreemdelingenbetwistingen, bedoeld in artikel 39/1 van de wet van 15 december 1980.

Art. 30/2. De Staat kan in alle geschillen met betrekking tot de toepassing van deze wet worden vertegenwoordigd door de bevoegde ministers of hun gemachtigden.

Art. 30/3. De diensten geschillen binnen elke sectie van de E.N.E. beheren de hen toegewezen beroepen overeenkomstig de artikelen 7, 6° en 26, § 2, punt 3°."

AVIS DU CONSEIL D'ÉTAT N° 73.820/2/V DU 21 AOUT 2023

Le 8 juin 2023, le Conseil d'État, section de législation, a été invité par la ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique à communiquer un avis dans un délai de trente jours, sur un avant-projet de loi 'modifiant la loi relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E)'.

L'avant-projet a été examiné par la deuxième chambre des vacations le 21 aout 2023. La chambre était composée de Martine Baguet, président de chambre, Bernard Blero et Christine Horevoets, conseillers d'État, Sébastien Van Drooghenbroeck, assesseur, et Anne-Catherine Van Geersdaele, greffier.

Le rapport a été présenté par Xavier Miny, auditeur adjoint.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Martine Baguet.

L'avis, dont le texte suit, a été donné le 21 aout 2023.

*

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 2°, 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 l'observation suivante.

‡ S'agissant d'un avant-projet de loi, on entend par "fondement juridique" la conformité aux normes supérieures.

ADVIES VAN DE RAAD VAN STATE NR. 73.820/2/V VAN 21 AUGUSTUS 2023

Op 8 juni 2023 is de Raad van State, afdeling Wetgeving, door de minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische Vernieuwing verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet 'tot wijziging van de wet betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E)'.

Het voorontwerp is door de tweede vakantiekamer onderzocht op 21 augustus 2023. De kamer was samengesteld uit Martine Baguet, kamervoorzitter, Bernard Blero en Christine Horevoets, staatsraden, Sébastien Van Drooghenbroeck, assessor, en Anne-Catherine Van Geersdaele, griffier.

Het verslag is uitgebracht door Xavier Miny, adjunct-auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Martine Baguet.

Het advies, waarvan de tekst hierna volgt, is gegeven op 21 augustus 2023.

*

Aangezien de adviesaanvraag is ingediend op basis van artikel 84, § 1, eerste lid, 2°, 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 opmerking.

‡ Aangezien het om een voorontwerp van wet gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere rechtsnormen verstaan.

Afin que l'article 1er de la loi "relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.)" sur laquelle la section de législation a donné ce jour l'avis n° 73.819/2/V (ci-près l'avant-projet n° 73.819/2/V), rende compte de sa nature, il convient que l'article 1er de l'avant-projet n° 73.819/2/V soit modifié par une nouvelle disposition insérée dans l'avant-projet à l'examen afin d'y mentionner que le chapitre 6, section 1/1, intitulée "Des recours contre les décisions de l'U.N.E." de l'avant-projet n° 73.819/2/V, règle une matière visée à l'article 78 de la Constitution[1].

Le greffier, *Le président,*

Anne-Catherine Van Geersdaele — Martine Baguet

Om duidelijkheid te scheppen over de strekking van artikel 1 van de wet "betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E.)" waarover de afdeling Wetgeving vandaag advies 73.819/2/V heeft uitgebracht (hierna: "voorontwerp 73.819/2/V"), dient artikel 1 van voorontwerp 73.819/2/V te worden gewijzigd bij een nieuwe bepaling, in te voegen in het voorliggende voorontwerp, zodat het vermeldt dat hoofdstuk 6, afdeling 1/1, van voorontwerp 73.819/2/V, met als opschrift "Beroep tegen de beslissingen van de E.N.E.", een aangelegenheid regelt als bedoeld in artikel 78 van de Grondwet.[1]

De griffier, *De voorzitter,*

Anne-Catherine Van Geersdaele — Martine Baguet

[1] Voir dans le même sens l'avis n° 53.021/4 donné le 22 avril 2013 sur un avantprojet devenu la loi du 30 aout 2013 'portant le Code ferroviaire', *Doc. parl.*, Chambre, 2012-2013, n° 2855/001, pp. 155-162 et la loi du 30 aout 2013 'insérant un titre 7/1 dans la loi du 30 aout 2013 portant le Code ferroviaire, en ce qui concerne les matières visées à l'article 77 de la Constitution', *Doc. parl.*, Chambre, 2012-2013, n° 2856/001, pp. 155-162.

[1] Zie in dezelfde zin advies 53.021/4 van 22 april 2013 over een voorontwerp dat heeft geleid tot de wet van 30 augustus 2013 'houdende de Spoorcodex', *Parl.St.* Kamer 2012-13, nr. 2855/001, 155-162, en tot de wet van 30 augustus 2013 'houdende invoeging van een titel 7/1 in de wet van 30 augustus 2013 houdende de Spoorcodex voor wat betreft de aangelegenheden als bedoeld in artikel 77 van de Grondwet', *Parl.St.* Kamer 2012-13, nr. 2856/001, 155-162.

PROJET DE LOI

PHILIPPE,

ROI DES BELGES,

À tous, présents et à venir,

SALUT.

Sur la proposition de la ministre de l'Intérieur,

NOUS AVONS ARRÊTÉ ET ARRÊTONS:

La ministre de l'Intérieur est chargée de présenter en notre nom aux Chambres législatives et de déposer à la Chambre des représentants le projet de loi dont la teneur suit:

CHAPITRE 1ER

Disposition générale

Article 1er

La présente loi règle une matière visée à l'article 78 de la Constitution.

CHAPITRE 2

Dispositions modificatives

Art. 2

L'article 1er de la loi du XXX relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.) est remplacé par ce qui suit:

"Art. 1er. La présente loi règle des matières visées aux articles 74 et 78 de la Constitution.".

Art. 3

Dans le chapitre 6 de la même loi, il est inséré une section 1/1 intitulée "Des recours contre les décisions de l'U.N.E.".

WETSONTWERP

FILIP,

KONING DER BELGEN,

Aan allen die nu zijn en hierna wezen zullen,

ONZE GROET.

Op de voordracht van de minister van Binnenlandse Zaken,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De minister van Binnenlandse Zaken is ermee belast in onze naam aan de Wetgevende Kamers voor te leggen en bij de Kamer van volksvertegenwoordigers het ontwerp van wet in te dienen waarvan de tekst hierna volgt:

HOOFDSTUK 1

Algemene bepaling

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

HOOFDSTUK 2

Wijzigingsbepalingen

Art. 2

Artikel 1 van de wet van XXX betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E) wordt vervangen als volgt:

"Art. 1. Deze wet regelt aangelegenheden als bedoeld in de artikelen 74 en 78 van de Grondwet.".

Art. 3

In hoofdstuk 6 van dezelfde wet wordt een afdeling 1/1 ingevoegd, met als opschrift "Beroep tegen de beslissingen van de E.N.E.".

Art. 4

Dans la section 1/1, insérée par l'article 3, sont insérés les articles suivants:

"Art. 26/1. Les décisions prises par l'U.N.E. sont susceptibles de recours en annulation devant le Conseil du contentieux des étrangers, visé à l'article 39/1 de la loi du 15 décembre 1980.

Art. 26/2. La représentation de l'État peut être assurée dans toutes les contestations relatives à l'application de la présente loi par les ministres compétents ou leurs délégués.

Art. 26/3. Les services de litiges au sein de chaque section de l'U.N.E. assurent la gestion des recours qui leurs sont attribués conformément aux articles 7, 7°, et 21, § 2, 3°.".

Donné à Bruxelles, le 6 mars 2024

PHILIPPE

Par le Roi:

La ministre de l'Intérieur,

Annelies Verlinden

Art. 4

In afdeling 1/1, ingevoegd door artikel 3, worden de volgende artikelen ingevoegd:

"Art. 26/1. Tegen de beslissingen genomen door de E.N.E. kan beroep tot nietigverklaring worden ingesteld bij de Raad voor Vreemdelingenbetwistingen, bedoeld in artikel 39/1 van de wet van 15 december 1980.

Art. 26/2. De Staat kan in alle geschillen met betrekking tot de toepassing van deze wet worden vertegenwoordigd door de bevoegde ministers of hun gemachtigden.

Art. 26/3. De diensten geschillen binnen elke sectie van de E.N.E. beheren de hen toegewezen beroepen overeenkomstig de artikelen 7, 7° en 21, § 2, 3°.".

Gegeven te Brussel, 6 maart 2024

FILIP

Van Koningswege:

De minister van Binnenlandse Zaken,

Annelies Verlinden

ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DA230019		10.07.2023

Objet : Avis relatif à l'avant-projet de loi relatif à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.) et à l'avant-projet de loi modifiant la loi relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.)

L'Organe de contrôle de l'information policière (ci-après le 'COC' ou 'l'Organe de contrôle').

Vu la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (M.B. du 5 septembre 2018, ci-après 'la LPD'), en particulier l'article 59 §1er, 2e alinéa, l'article 71 et le Titre VII, en particulier l'article 236.

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD').

Vu la loi du 5 août 1992 sur la fonction de police (ci-après 'la LFP').

Vu la *Law Enforcement Directive* 2016/680 du 27 avril 2016 (ci-après 'la *LED*').

Vu la loi du 25 décembre 2016 relative au traitement des données des passagers.

Vu la demande du 15 mai 2023 du ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique, reçue le 30 mai 2023.

Vu le rapport de Monsieur Ronny Saelens, membre-conseiller a.i. de l'Organe de contrôle.

Émet, le 10 juillet 2023, l'avis suivant.

I. Remarque préalable concernant la compétence de l'Organe de contrôle

1. À la lumière respectivement de l'application et de la transposition du Règlement 2016/679[1] et de la Directive 2016/680[2], le législateur a remanié en profondeur les tâches et missions de l'Organe de contrôle. L'article 4 §2, quatrième alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD') dispose qu'à l'égard des services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle. Cela signifie notamment que l'Organe de contrôle est compétent également lorsque des services de police traitent des données à caractère personnel qui ne relèvent pas des missions de police administrative et judiciaire, par exemple dans le cadre de finalités socioéconomiques ou de traitements relevant de la gestion des ressources humaines. L'Organe de contrôle doit être consulté lors de la préparation de la législation ou d'une mesure réglementaire ayant trait au traitement de données à caractère personnel par les services de police de la police intégrée (voir les articles 59 §1er, 2e alinéa et 236 §2 de la LPD, l'article 36.4 du RGPD et l'article 28.2 de la directive Police-Justice). L'Organe de contrôle a dans ce contexte pour mission d'examiner si l'activité de traitement projetée par les services de police est conforme aux dispositions du Titre 1er (pour les traitements non opérationnels)[3] et du Titre 2 (pour les traitements opérationnels) de la LPD[4]. De plus, le COC est aussi chargé d'émettre des avis d'initiative, comme prévu à l'article 236 §2 de la LPD, et est investi conformément à l'article 240 de la LPD d'une mission générale d'information à l'égard du grand public, des personnes concernées, des responsables du traitement et des sous-traitants dans le domaine du droit à la protection des données et à la protection de la vie privée.

2. En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou judiciaire, l'Organe de contrôle émet dès lors des avis soit d'initiative, soit à la demande du Gouvernement ou de la Chambre des Représentants, d'une autorité administrative ou judiciaire ou d'un service de police, concernant toute matière ayant trait à la gestion de l'information policière telle que régie par la Section 12 du Chapitre 4 de la loi sur la fonction de police[5].

3. Par ailleurs, l'Organe de contrôle est également chargé, à l'égard des services de police, de l'inspection générale de la police fédérale et de la police locale (en abrégé 'AIG') visée dans la loi du

[1] 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 ou « RGPD »).
[2] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 *« relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil »* (ci-après dénommée « directive Police-Justice » ou *Law Enforcement Directive* (*LED*)).
[3] Article 4 §2, 4e alinéa de la LPD.
[4] Article 71 §1er, 3e alinéa de la LPD.
[5] Articles 59 §1er, 2e alinéa et 236 §2 de la LPD.

15 mai 2007 sur l'Inspection générale et de l'Unité d'information des passagers (ci-après dénommée en abrégé 'BELPIU') visée au Chapitre 7 de la loi du 25 décembre 2016, de la surveillance de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel tel que visé aux articles 44/1 à 44/11/14 de la loi sur la fonction de police, et/ou de toute autre mission qui lui est confiée en vertu ou par d'autres lois[6].

4. L'Organe de contrôle est compétent à l'égard du Service Contentieux de l'Administration générale des Douanes et Accises en ce qui concerne les réquisitions adressées par ce service à la BELPIU dans des matières fiscales, et ce en vertu de l'article 281 §4 de la loi générale *« sur les douanes et accises »* du 18 juillet 1977, telle que modifiée par la loi du 2 mai 2019 *« modifiant diverses dispositions relatives au traitement des données des passagers »*.

5. Enfin, l'Organe de contrôle est également chargé, dans le cadre de la législation sur la rétention des données et en vertu de l'article 126/3 §1er, 8e alinéa de la loi du 13 juin 2005 relative aux communications électroniques (ci-après 'la LCE'), telle que modifiée par 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 (*M.B.* du 8 août 2022), de la validation des statistiques relatives au nombre de faits punissables et au délai de conservation pour chaque arrondissement judiciaire et chaque zone de police, une matière dans le cadre de laquelle il exerce toutes les compétences qui lui ont été attribuées par le Titre 7 de la loi du 30 juillet 2018. Il est par ailleurs également chargé, en application de l'article 42 §3, 2e et 3e alinéas de la LFP, du contrôle des requêtes de la Cellule Personnes disparues de la police fédérale en vue de la consultation des données relatives aux communications électroniques impliquant la personne disparue.

6. L'Organe de contrôle est compétent pour rendre des avis sur les aspects ayant trait au traitement des informations et des données à caractère personnel et à la protection de la vie privée par le traitement de données à caractère personnel pour autant qu'il existe un rapport avec le fonctionnement opérationnel et non opérationnel des services de police et/ou avec le personnel de la police intégrée (ci-après 'la GPI[7]') et/ou pour autant que le projet de texte soumis pour avis ait un impact sur la gestion de l'information policière en général.

7. Par ailleurs, l'Organe de contrôle n'est pas seulement une autorité de protection des données, mais est aussi une autorité de contrôle qui est légalement chargée de contrôler la légalité, l'efficacité, l'efficience et l'économie de la gestion de l'information policière[8].

---

[6] Article 71 §1er, troisième alinéa *juncto* article 236 §3 de la LPD.
[7] Geïntegreerde politie – Police Intégrée.
[8] Rapport d'activité 2021, www.organedecontrole.be, voir les points 3 et 52 et plus spécifiquement le point 71 : *« Il serait cependant faux de s'imaginer que le COC se préoccupe seulement de la protection des données ; il porte aussi énormément d'attention à tous les autres aspects opérationnels de la gestion de l'information policière et des informations des autres services qu'il contrôle, s'agissant là de matières relevant également de sa compétence. »* ; article 71 §1er de la LPD.

II. Objet de la demande

8. La demande d'avis a trait d'une part à un avant-projet de loi *« relatif à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.) »* (ci-après 'l'avant-projet'), et d'autre part à l'avant-projet de loi *« modifiant la loi relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.) »* (ci-après 'l'avant-projet relatif au recours').

9. Les deux avant-projets ont trait à la mise en œuvre de certaines dispositions du Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 *« portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) n° 1077/2011, (UE) n° 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226 »* (ci-après 'le Règlement ETIAS'), qui oblige les États membres à créer une Unité nationale ETIAS opérationnelle effectuant des traitements.

10. En résumé, l'objectif du Règlement ETIAS consiste en un contrôle préalable des ressortissants de pays tiers exemptés de l'obligation de visa pour accéder au territoire européen. Dans ce contexte, il est créé au niveau européen une unité centrale ETIAS ainsi qu'un système d'information central ETIAS qui procède pour les demandes d'autorisations de voyage à une évaluation des risques sécuritaires, migratoires et sanitaires sur la base de laquelle les demandeurs peuvent se voir refuser l'accès au territoire européen.

11. Dans le cadre de ce processus d'évaluation, les données du demandeur sont comparées aux différentes banques de données (policières) européennes et nationales. À cette fin, chaque État membre crée en marge de l'unité centrale ETIAS à l'échelon européen une Unité nationale ETIAS (U.N.E.) qui a accès au système d'information central ETIAS. Sous certaines conditions, le système d'information ETIAS sera également accessible à des fins de maintien de l'ordre public, et donc en dehors du contexte d'une demande visant à obtenir une autorisation de voyage pour le territoire européen.

12. Le système d'information central ETIAS prévoit un processus de demande automatisé dans le cadre duquel les données mentionnées sur le formulaire de demande numérique peuvent générer un 'hit' lorsque le demandeur est connu ou signalé dans une banque de données de l'UE, à savoir le système d'information Schengen (SIS), le système d'information sur les visas (VIS), le système d'entrée/de sortie (EES), Eurodac ou les bases de données d'Interpol sur les documents de voyage associés aux notices (SLTD[9] et TDAWN[10])[11]. Les données du demandeur sont en outre comparées à une liste de surveillance ETIAS spécifique composée en fonction des indicateurs de risques sécuritaires,

[9] La base de données d'Interpol sur les documents de voyage volés ou perdus (considérant 23 du Règlement ETIAS).
[10] La base de données d'Interpol sur les documents de voyage associés aux notices (considérant 23 du Règlement ETIAS).
[11] Cf. le Règlement ETIAS.

migratoires et sanitaires[12]. La liste de surveillance ETIAS est établie pour constater les corrélations entre les données d'un dossier de demande et les informations relatives à des personnes soupçonnées d'avoir commis une infraction terroriste ou une autre infraction pénale grave ou d'y avoir participé, ou à des personnes pour lesquelles il existe des indices concrets ou des motifs raisonnables permettant de croire qu'elles commettront une infraction terroriste ou une autre infraction pénale grave. Les données de cette liste de surveillance sont introduites par Europol et par les États membres. Dans le cadre de ce traitement de données en vue d'une évaluation des risques sécuritaires induits par les demandeurs d'une autorisation de voyage, l'U.N.E. est également composée de membres détachés de la police intégrée (ci-après 'la GPI'[13]) et de l'Administration générale des Douanes et Accises (ci-après 'les Douanes').

13. Le COC limite dans le présent avis son analyse d'une part aux traitements policiers dans la mesure où les avant-projets ont ou peuvent avoir une influence directe ou indirecte sur le fonctionnement de la GPI dans le cadre plus large de la gestion de l'information policière, et d'autre part aux traitements effectués par les Douanes dans la mesure où ceux-ci relèvent de la compétence de surveillance de l'Organe de contrôle. Pour le reste, l'Organe de contrôle renvoie à l'avis de l'APD.

L'avis de l'Organe de contrôle n'a par conséquent pas trait à l'avant-projet relatif au recours, pour lequel il est intégralement fait référence à l'avis de l'APD.

III. Analyse de la demande

1. Remarques générales

14. Selon le Règlement ETIAS, la *LED* s'applique aux traitements dans le cadre du maintien de l'ordre public. Concrètement, il s'agit des traitements effectués par les membres détachés de la GPI qui traitent des données policières au sein de l'U.N.E. dans le cadre des finalités du Règlement ETIAS[14].

15. Cela signifie que pour autant que le Règlement ETIAS donne naissance à des compétences présentant un lien avec l'application de la *LED*, et donc du Titre 2 de la LPD et de la LFP, celles-ci doivent être réglementées dans l'avant-projet.

2. Remarques concrètes concernant l'avant-projet

16. L'article 56.2, 2e alinéa du Règlement ETIAS dispose que la *LED* s'applique aux traitements de données à caractère personnel effectués par (une section de) l'U.N.E. aux fins de la prévention ou de

[12] Dont il est également question dans le Règlement ETIAS.
[13] Geïntegreerde politie – Police Intégrée.
[14] Considérants 54 et 55 du Règlement ETIAS.

la détection des infractions terroristes ou d'autres infractions pénales graves, ou des enquêtes en la matière.
L'article 66 du Règlement ETIAS concerne les autorités de contrôle. L'article 66.2 et l'article 66.3 sont formulés comme suit :
« 2. Chaque État membre veille à ce que les dispositions législatives, réglementaires et administratives nationales qu'il a adoptées en application de la directive (UE) 2016/680 s'appliquent aussi à l'accès à ETIAS par ses autorités nationales conformément au chapitre X du présent règlement, y compris pour ce qui est des droits des personnes dont les données sont ainsi consultées. »
« 3. L'autorité de contrôle instituée conformément à l'article 41, paragraphe 1, de la directive (UE) 2016/680 contrôle la licéité de l'accès aux données à caractère personnel par les États membres conformément au chapitre X du présent règlement, y compris de la transmission des données à partir d'ETIAS et vers celui-ci. ».
L'Organe de contrôle doit par conséquent être considéré comme l'autorité de contrôle pour les traitements policiers dans le cadre de la mise en œuvre du Règlement ETIAS et de l'avant-projet.

17. La compétence de surveillance de l'Organe de contrôle est ainsi directement liée à l'article 18 de l'avant-projet, qui dispose que les données à caractère personnel transmises à partir du système d'information central ETIAS aux services de police ne peuvent pas être conservées pendant plus d'un mois dans l'environnement policier, à moins qu'elles ne revêtent un intérêt opérationnel (voir concrètement le point 21).

En d'autres termes, il en découle pour l'Organe de contrôle une première (nouvelle) mission de surveillance. Cependant, l'avant-projet ne fait pas explicitement mention de l'Organe de contrôle en ce qui concerne ces traitements policiers.

Par ailleurs, la GPI doit en vertu de l'article 34 du Règlement ETIAS apporter à l'échelon national son concours à l'établissement de la liste de surveillance ETIAS. Cette disposition est mise en œuvre par l'article 21 de l'avant-projet. La pertinence et l'exactitude des données à caractère personnel figurant sur la liste de surveillance devront en effet en partie reposer sur les données policières nationales dont la licéité (légalité, proportionnalité, exactitude) du traitement relève de toute évidence de l'application du Titre 2 de la LPD et de la LFP, et par conséquent aussi de la compétence de surveillance de l'Organe de contrôle. Bien que le Règlement ETIAS établisse la compétence de l'autorité de contrôle pour les traitements relevant de la *LED*, il est indiqué que l'auteur de l'avant-projet désigne explicitement l'Organe de contrôle de l'information policière dans l'avant-projet.

18. Un autre aspect rejoignant la remarque formulée au point 16 peut être déduit de l'article 34 de l'avant-projet. Cet article prévoit une adaptation de l'article 281 de la *« loi générale sur les douanes et accises »* coordonnée le 18 juillet 1977 (la 'loi sur les douanes') en vue de permettre au conseiller-général de l'administration en charge des contentieux d'accéder aux données à caractère personnel

du système d'information central ETIAS. Selon le même article de l'avant-projet, l'Organe de contrôle effectue un contrôle *a posteriori* de la légalité et de la proportionnalité de l'accès des Douanes aux données contenues dans le système d'information central ETIAS. L'article 281 §4 de la loi sur les douanes prévoit déjà un régime similaire pour l'accès des Douanes aux données des passagers figurant dans la banque de données des passagers (voir plus loin) et la mission de contrôle du COC à cet égard.

19. L'avant-projet crée donc une (seconde) nouvelle mission pour l'Organe de contrôle.

Pour commencer, il convient inévitablement de s'interroger sur les aspects de moyens et de capacité inhérents à l'attribution de nouvelles missions. En sa qualité d'institution parlementaire ayant droit à une dotation, l'Organe de contrôle part du principe qu'il obtiendra du parlement fédéral les moyens supplémentaires dont il a besoin pour s'acquitter des missions additionnelles qui lui sont confiées par l'avant-projet, et qu'il bénéficiera dans ce contexte du soutien nécessaire du ministre de l'Intérieur – le demandeur du présent avis – et du ministre des Finances compétent.

Ensuite, en ce qui concerne le contenu et l'efficacité, on peut se demander comment l'Organe de contrôle peut contrôler la licéité (la légalité et la proportionnalité) de l'accès (et donc des données ETIAS demandées) des Douanes au système d'information central ETIAS, dans l'hypothèse où l'Organe de contrôle n'est ou ne serait pas investi d'une compétence de surveillance à l'égard des données traitées et des traitements effectués dans le système d'information central ETIAS. À titre d'exemple *a contrario*, on peut renvoyer *mutatis mutandis* à la compétence de surveillance de l'Organe de contrôle à l'égard de la banque de données des passagers visée aux articles 8 et 9 de la loi PNR[15]. Cette loi investit l'Organe de contrôle d'une compétence de surveillance à l'égard de l'accès à la banque de données des passagers pour les traitements relevant de sa compétence de surveillance, par exemple à l'égard de l'accès aux données des passagers par les Douanes. Le COC a aussi logiquement un accès illimité à la banque de données des passagers susmentionnée en sa qualité d'autorité de contrôle (cf. article 26, 7, f) *juncto* article 71 §1er, 3e alinéa de la LPD) de la BELPIU (l'Unité d'information des passagers). Il subsiste toutefois à cet égard un manque de clarté quant à la portée de la compétence de surveillance de l'Organe de contrôle pour les traitements des Douanes tels que prévus dans l'avant-projet et à la nature de l'accès au système d'information central ETIAS dont le COC dispose en droit.

20. À la lumière de ce qui précède, l'Organe de contrôle demande donc de définir clairement dans l'avant-projet (1) d'une part la mission de surveillance de l'Organe de contrôle à l'égard des traitements du Titre 2 de la LPD, qui sont effectués par les services de police visés à l'article 6, 2°, a) et faisant partie de la section du Centre de Crise National visée au chapitre 4 de l'avant-projet, et (2) d'autre

[15] Loi du 25 décembre 2016 *« relative au traitement des données des passagers »*.

part la surveillance de la consultation des données ETIAS par les services de police et les Douanes (moyennant une réquisition de la part du conseiller-général de cette dernière administration) en vue de prévenir et de détecter les infractions terroristes ou autres, et de prévoir dans ce contexte pour l'Organe de contrôle un accès univoque et intégral au système d'information central ETIAS ainsi qu'à toutes les autres banques de données éventuelles qui seraient créées dans ce cadre par l'U.N.E. et aux traitements y afférents.

3. Convergence avec les dispositions de la LFP relatives à la gestion de l'information

21. Selon l'article 18 de l'avant-projet, les données à caractère personnel transmises à la police à des fins de maintien de l'ordre public sont *« effacées lorsque ladite enquête est clôturée »*. Pour toute clarté et sauf erreur du COC, il est question ici de l'utilisation des données à caractère personnel provenant du système d'information central ETIAS qui n'ont pas trait à l'évaluation dans le cadre d'une demande d'autorisation de voyage. La question qui se pose est de savoir si l'obligation, pour les services de police, d'effacer les données reçues lorsque l'enquête est clôturée est compatible avec les articles 44/5 et 44/9 de la LFP relatifs au délai de conservation des données policières dans les banques de données opérationnelles et avec le régime prévu pour l'archivage de ces données. L'Organe de contrôle prie l'auteur de l'avant-projet de réfléchir à cette zone de tension plausible entre l'avant-projet et les dispositions en question de la LFP relatives à la gestion de l'information et, le cas échéant, de supprimer la dernière partie de phrase de l'article 18 de l'avant-projet et de la remplacer par une référence aux articles de la LFP désignés ci-avant.

22. Pour le reste, l'Organe de contrôle n'a pas de remarques à formuler.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

prie le demandeur de tenir compte des remarques susmentionnées.

Avis approuvé par l'Organe de contrôle de l'information policière le 10 juillet 2023.

Pour l'Organe de contrôle,
Le Président a.i.,
Frank SCHUERMANS (SIGNÉ)

CONTROLEORGAAN OP DE POLITIONELE INFORMATIE

Uw referentie	Onze referentie	Bijlage(n)	Datum
	DA230019		10.07.2023

<u>Betreft</u>: Advies betreffende het voorontwerp van wet betreffende de oprichting en organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E) en het voorontwerp van wet tot wijziging van de wet betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E)

Het Controleorgaan op de politionele informatie (hierna afgekort 'COC' of 'Controleorgaan').

Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (BS, 5 september 2018, hierna afgekort als 'WGB') inzonderheid het artikel 59 §1, 2e lid, artikel 71 en Titel VII, inzonderheid artikel 236.

Gelet op de wet van 3 december 2017 tot oprichting van een Gegevensbeschermingsautoriteit (hierna afgekort 'WOG').

Gelet op de wet van 5 augustus 1992 op het politieambt (hierna 'WPA').

Gelet op de *Law Enforcement Directive* 2016/680 van 27 april 2016 (hierna *LED*).

Gelet op de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens.

Gelet op het verzoek van de Minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische Vernieuwing van 15 mei 2023, ontvangen op 30 mei 2023;

Gelet op het verslag van de heer Ronny Saelens, lid-raadsheer a.i. van het Controleorgaan.

Brengt op 10 juli 2023 het volgend advies uit.

I. <u>Voorafgaande opmerking nopens de bevoegdheid van het Controleorgaan</u>

1. In het licht van, respectievelijk, de toepassing en omzetting van de Verordening 2016/679[1] en de Richtlijn 2016/680[2] heeft de wetgever de taken en opdrachten van het Controleorgaan grondig

[1] 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 of 'AVG').

[2] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 "*betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad*" (hierna 'Richtlijn Politie en Justitie' of *Law Enforcement Directive* (*LED*)).

gewijzigd. Artikel 4 § 2, vierde lid, van de organieke wet van 3 december 2017 betreffende de oprichting van een Gegevensbeschermingsautoriteit (hierna afgekort 'WOG') bepaalt dat de competenties, taken en bevoegdheden als toezichthoudende autoriteit voorzien door de Verordening 2016/679 voor de politiediensten in de zin van artikel 2,2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie, gestructureerd op twee niveaus, worden uitgeoefend door het Controleorgaan. Het betekent onder meer dat het Controleorgaan ook bevoegd is wanneer politiediensten persoonsgegevens verwerken die buiten de opdrachten van bestuurlijke en gerechtelijke politie vallen, bijvoorbeeld in het kader van sociaaleconomische doeleinden of human ressources verwerkingen. Het Controleorgaan moet geraadpleegd worden bij de voorbereiding van wetgeving of een regelgevende maatregel die verband houdt met de verwerking van persoonsgegevens door de politiediensten van de geïntegreerde politie (zie artikel 59 §1, 2e lid en 236 §2 WGB, artikel 36.4 van de AVG en artikel 28.2 van de Richtlijn politie-justitie). Daarbij heeft het Controleorgaan de opdracht om te onderzoeken of de voorgenomen verwerkingsactiviteit door de politiediensten in overeenstemming is met de bepalingen van Titel 1 (voor de niet operationele verwerkingen)[3] en 2 (voor de operationele verwerkingen) van de WGB[4]. Daarnaast heeft het COC ook een ambtshalve adviesopdracht voorzien in artikel 236 §2 WGB en een algemene voorlichtingsopdracht van het brede publiek, betrokkenen, verwerkingsverantwoordelijken en verwerkers in de materie van het privacy – en gegevensbeschermingsrecht voorzien in artikel 240 WGB.

2. Wat betreft derhalve in het bijzonder de verwerkingsactiviteiten in kader van de opdrachten van bestuurlijke en/of gerechtelijke politie brengt het Controleorgaan advies uit, hetzij uit eigen beweging, hetzij op verzoek van de Regering of van de Kamer van volksvertegenwoordigers, van een bestuurlijke of gerechtelijke overheid of van een politiedienst, inzake iedere aangelegenheid die betrekking heeft op het politionele informatiebeheer zoals geregeld in Afdeling 12 van Hoofdstuk 4 van de wet op het politieambt[5].

3. Het Controleorgaan is, ten aanzien van de politiediensten, de Algemene Inspectie van de federale politie en lokale politie (afgekort 'AIG') zoals bedoeld in de wet van 15 mei 2007 op de Algemene Inspectie en de Passagiersinformatie-eenheid (hierna afgekort 'BELPIU') bedoeld in Hoofdstuk 7 van de wet van 25 december 2016 tevens belast met het toezicht op de toepassing van Titel 2 van de GBW en/of de verwerking van persoonsgegevens zoals bedoeld in de artikelen 44/1 tot 44/11/14 van de wet op het politieambt en/of elke andere opdracht die haar krachtens of door andere wetten wordt verleend[6].

---

[3] Artikel 4 §2, 4e lid WOG.

[4] Artikel 71 §1, 3e lid WGB.

[5] Artikelen 59 §1, 2e lid en 236 § 2 WGB.

[6] Artikel 71 §1, derde lid *juncto* 236 § 3 WGB.

4. Het Controleorgaan is ingevolge artikel 281, § 4, van de algemene wet van 18 juli 1977 "*inzake douane en accijnzen*", zoals gewijzigd door de wet van 2 mei 2019 "*tot wijziging van diverse bepalingen met betrekking tot de verwerking van persoonsgegevens*" ten aanzien van de Dienst Geschillen van de Algemene Administratie van Douane en Accijnzen bevoegd in het kader van de vorderingen gericht aan de BELPIU in fiscale materies.

5. Het COC is tot slot ook belast, in het kader van de dataretentie wetgeving, op grond van artikel 126/3 §1, 8e lid van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna afgekort 'WEC'), zoals gewijzigd door 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 (*BS* van 8 augustus 2022), met de validatie van de statistieken met betrekking tot het aantal strafbare feiten en de bewaringstermijn voor elk gerechtelijk arrondissement en elke politiezone in het kader waarvan het al zijn bevoegdheden uitoefent die hem zijn toegekend bij titel 7 van de wet van 30 juli 2018. Het is daarnaast ook nog belast, in toepassing van artikel 42 § 3, 2de en 3de lid WPA met de controle van de vorderingen van de Cel Vermiste Personen van de federale politie tot opvraging van de gegevens met betrekking tot de elektronische communicatie betreffende de vermiste persoon.

6. Het Controleorgaan is bevoegd om advies te verlenen over aspecten met betrekking tot de verwerking van informatie en persoonsgegevens en de bescherming van het privéleven door de verwerking van persoonsgegevens voor zover deze betrekking hebben op of in verband staan met de operationele en niet-operationele werking van de politiediensten en/of het personeel van de geïntegreerde politie (hierna 'GPI[7]') en/of voor zover de voor advies voorgelegde ontwerptekst een impact heeft op de politionele informatiehuishouding in het algemeen.

7. Het Controleorgaan is daarnaast niet enkel een gegevensbeschermingsautoriteit maar een toezichthouder die evenzeer wettelijk belast is met de legaliteit, efficiëntie, effectiviteit en economie van de politionele informatiehuishouding[8].

II. Voorwerp van de aanvraag

8. De adviesaanvraag heeft betrekking op een voorontwerp van wet "*betreffende de oprichting en organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E)* (hierna het 'voorontwerp'), enerzijds, en het voorontwerp van wet "*tot wijziging van de wet betreffende de oprichting en de*

[7] Geïntegreerde politie – Police Intégrée.
[8] Activiteitenverslag 2021, www.controleorgaan.be, randnummers 3, 52 en in het bijzonder 71: "*Het COC heeft echter allerminst alleen oog voor dataprotectie; het heeft evenzeer veel aandacht en is bevoegd voor alle andere operationele aspecten van de politionele informatiehuishouding*"; artikel 71 §1 WGB.

organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E)" (hierna het 'voorontwerp betreffende het beroep'), anderzijds.

9. Beide voorontwerpen hebben betrekking op de uitvoering van sommige bepalingen van de Verordening (EU) 2018/1240 van het Europees Parlement en de Raad van 12 september 2018 "*tot oprichting van een Europees reisinformatie- en -autorisatiesysteem (Etias) en tot wijziging van de Verordeningen (EU) nr. 1077/2011, (EU) nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 en (EU) 2017/2226*" (hierna 'ETIAS-Verordening') die de lidstaten verplicht om een operationele en verwerkende ETIAS Nationale Eenheid op te richten.

10. Kort gezegd bestaat de doelstelling van de ETIAS-Verordening in een voorafgaande controle van onderdanen van derde landen die zijn vrijgesteld van de visumplicht om het Europees grondgebied binnen te komen. In dat verband wordt op Europees niveau een centrale ETIAS-eenheid en een centraal ETIAS-informatiesysteem opgericht dat een evaluatie van de migratie-, gezondheids- en veiligheidsrisico's van de aanvragen voor reisautorisaties uitvoert op basis waarvan aanvragers de toegang tot het Europees grondgebied kunnen geweigerd worden.

11. In het kader van dit evaluatieproces worden de gegevens van de aanvrager vergeleken met de verschillende Europese en nationale (politionele) gegevensbanken. Daartoe wordt, naast een centrale ETIAS eenheid op Europees niveau, door iedere lidstaat een ETIAS nationale eenheid (E.N.E) opgericht die toegang heeft tot het centraal ETIAS-informatiesysteem. Het ETIAS-informatiesysteem zal onder voorwaarden ook toegankelijk zijn voor rechtshandhavingsdoeleinden, en dus buiten de context van de aanvraag van een persoon om een reisautorisatie voor het Europees grondgebied te verkrijgen.

12. Het centraal ETIAS-informatiesysteem voorziet in een geautomatiseerd aanvraagproces waarbij de gegevens die vermeld worden op het digitaal aanvraagformulier een 'hit' kunnen genereren wanneer de aanvrager gekend of gesignaleerd is in een EU-gegevensbank, met name het Schengeninformatiesysteem (SIS), het Visuminformatiesysteem (VIS), het inreis-uitreissysteem (EES), Eurodac, of de Interpolgegevensbanken voor reisdocumenten die verband houden met kennisgevingen (SLTD[9] en TDWAN[10])[11]. Daarnaast worden de gegevens van de aanvrager vergeleken met een specifieke ETIAS-observatielijst die gebaseerd zijn op risico-indicatoren inzake migratie, gezondheid en veiligheid[12]. De ETIAS-observatielijst wordt opgesteld om correlaties vast te stellen tussen gegevens in een aanvraagdossier en informatie over personen die worden verdacht van het plegen van of betrokkenheid bij een terroristisch misdrijf of een ander ernstig strafbaar feit ten aanzien van wie feitelijke aanwijzingen of redelijke vermoedens bestaan dat hij deze misdrijven zal plegen. De

[9] De Interpol gegevensbank met gestolen of verloren reisdocumenten (overweging 23 Etias-Verordening).

[10] De Interpol gegevensbank voor reisdocumenten die verband houden met kennisgevingen (overweging 23 Etias-Verordening).

[11] Geregeld in de ETIAS-Verordening.

[12] Eveneens geregeld in de ETIAS-Verordening.

gegevens in deze observatielijst worden opgenomen door Europol en door de lidstaten. In het kader van deze gegevensverwerking met op het oog op een evaluatie van de veiligheidsrisico's die verbonden zijn aan aanvragers voor een reisautorisatie wordt de E.N.E ook samengesteld uit gedetacheerde leden van de geïntegreerde politie (hierna ' de GPI[13]') en de Algemene Administratie van de Douane en de Accijnzen (Douane).

13. Het COC beperkt in dit advies zijn onderzoek tot de politionele verwerkingen in de mate dat de voorontwerpen rechtstreeks of onrechtstreeks een invloed (kunnen) hebben op het functioneren van de GPI in het ruimere kader van de politionele informatiehuishouding, enerzijds, en de verwerkingen door de Douane in zoverre deze onder de toezichtsbevoegdheid van het Controleorgaan vallen. Voor het overige verwijst het controleorgaan naar het advies van de GBA.

Bijgevolg heeft het advies van het Controleorgaan geen betrekking op het voorontwerp betreffende het beroep, waarvoor integraal naar het advies van de GBA wordt verwezen.

III. Analyse van de aanvraag

1. Algemene opmerkingen

14. Volgens de ETIAS-verordening is voor de verwerkingen in het kader van de rechtshandhaving de *LED* van toepassing. Dit raakt concreet aan de verwerkingen door de gedetacheerde leden van de GPI die in de E.N.E. in het kader van de doeleinden van de ETIAS-verordening politionele gegevens verwerken[14].

15. Het voorgaande betekent dat, voor zover uit de ETIAS-Verordening bevoegdheden voortvloeien die in verband staat met de toepassing van de *LED*, en dus titel 2 WGB en de WPA, deze in het voorontwerp moeten geregeld worden.

2. Concrete opmerkingen m.b.t. het voorontwerp

16. Artikel 56.2, 2de lid van de ETIAS-Verordening bepaalt dat op de verwerking van persoonsgegevens door de (sectie van de) E.N.E. met het oog op het voorkomen, opsporen of onderzoeken van terroristische misdrijven of van andere strafbare feiten de *LED* van toepassing is.
Artikel 66 van de ETIAS-Verordening handelt over de toezichthoudende autoriteiten. Artikel 66.2 en 66.3 luiden als volgt:

---

[13] Geïntegreerde politie – Police Intégrée.

[14] Overwegingen 54 en 55 ETIAS-Verordening.

"2. Elke lidstaat zorgt ervoor dat de wettelijke en bestuursrechtelijke bepalingen die overeenkomstig Richtlijn (EU) 2016/680 in het nationale recht zijn vastgesteld, ook gelden voor de toegang tot Etias voor zijn nationale autoriteiten in overeenstemming met hoofdstuk X van deze verordening, met betrekking tot de rechten van personen tot wier gegevens aldus toegang wordt verkregen".
De overeenkomstig artikel 41, lid 1, van de Richtlijn (EU) 2016/680 ingestelde toezichthoudende autoriteit oefent toezicht uit op de rechtmatigheid van de toegang tot persoonsgegevens door de lidstaten overeenkomstig hoofdstuk X van deze verordening met betrekking tot de rechten van de personen tot wier gegevens aldus toegang wordt verkregen".
Aldus is het Controleorgaan te beschouwen als de toezichthoudende autoriteit met betrekking tot de politionele verwerkingen in het kader van de uitvoering van de ETIAS-Verordening en het voorontwerp.

17. Zo staat de toezichtbevoegdheid van het Controleorgaan in rechtstreeks verband met artikel 18 van het voorontwerp dat bepaalt dat de persoonsgegevens die uit het centrale ETIAS-informatiesysteem aan, *in casu*, de politiediensten worden doorgegeven, niet langer dan een maand in de politieomgeving mogen worden bewaard, tenzij de persoonsgegevens een operationeel belang hebben (zie concreet randnummer 21).

Hieruit volgt m.a.w. dat voor het Controleorgaan een eerste (nieuwe) toezichthoudende opdracht wordt gecreëerd. In het voorontwerp wordt het Controleorgaan ten aanzien van deze politionele verwerkingen evenwel niet uitdrukkelijk vermeld.

Daarnaast moet de GPI op grond van artikel 34 van de ETIAS-Verordening op nationaal niveau meewerken bij het opstellen van de ETIAS-observatielijst. Deze wordt uitgevoerd in artikel 21 van het voorontwerp. De pertinentie en correctheid van de in de observatielijst opgenomen persoonsgegevens zullen immers mede gebaseerd zijn op de nationale politionele gegevens waarvan de rechtmatigheid (wettigheid, proportionaliteit, accuraatheid) van de verwerking evident onder de toepassing van titel 2 WGB en de WPA en bijgevolg ook onder de toezichtsbevoegdheid van het Controleorgaan valt. Hoewel de ETIAS-Verordening de bevoegdheid van de toezichthoudende autoriteit voor de *LED*-verwerkingen vastlegt, is het aangewezen dat de steller van het voorontwerp uitdrukkelijk het Controleorgaan op de politionele informatie in het voortonwerp aanduidt.

18. Een ander aspect dat in verband staat met de opmerking van randnummer 16 valt af te leiden uit artikel 34 van het voorontwerp. Dat artikel voorziet een aanpassing van artikel 281 van "*de algemene wet inzake douane en accijnzen*", gecoördineerd op 18 juli 1977 (Douanewet), waarbij aan de adviseur-generaal van het departement geschillen toegang wordt verleend tot de persoonsgegevens van het centrale ETIAS-informatiesysteem. Volgens hetzelfde artikel van het voorontwerp voert het Controleorgaan een *a posteriori*-controle uit met betrekking tot de wettigheid en de proportionaliteit van de toegang door de douane tot de gegevens in het centrale ETIAS-informatiesysteem. Artikel 281 § 4 van de Douanewet voorziet reeds in een gelijkluidende regeling voor de toegang door de Douane

tot de passagiersgegevens in de passagiersgegevensbank (zie hierna) en de controleopdracht van het COC daarop.

19. Het voorontwerp creëert aldus een (tweede) nieuwe en bijkomende opdracht voor het Controleorgaan.

Vooreerst stelt zich onvermijdelijk de vraag naar aspecten inzake middelen en capaciteit die de toewijzing van nieuwe opdrachten met zich brengt. Het Controleorgaan gaat er, als dotatiegerechtigde parlementaire instelling, vanuit dat het de noodzakelijke bijkomende middelen voor de in dit voorontwerp voorziene bijkomende opdrachten zal bekomen vanwege het federale parlement en daarvoor de nodige steun zal bekomen vanwege de advies verzoekende Minister van Binnenlandse Zaken (en de bevoegde Minister van Financiën).

Vervolgens, inhoudelijk en naar werkbaarheid toe, rijst de vraag hoe het Controleorgaan de rechtmatigheid (wettigheid en proportionaliteit) van de toegang (en dus de gevorderde ETIAS-gegevens) van de Douane tot het centrale ETIAS-informatiesysteem kan controleren, in de hypohese dat het Controleorgaan geen toezichtbevoegdheid heeft of zou hebben op de gegevens en verwerkingen die in het centrale ETIAS-informatiesysteem worden verwerkt. Er kan bij wijze van een *a contrario* voorbeeld, *mutatis mutandis*, verwezen worden naar de toezichtsbevoegdheid van het Controleorgaan op de passagiersgegevensbank, bedoeld in de artikelen 8 en 9 van de PNR-wet[15]. Deze wet voorziet in een toezichtsbevoegdheid van het Controleorgaan op de toegang tot de passagiersgegevensbank voor de verwerkingen die onder zijn de toezichtbevoegdheid vallen, zoals met betrekking tot de toegang tot de passagiersgegevens door de Douane. Het COC heeft logischerwijze ook een onbeperkte toegang tot voormelde passagiersgegevensbank als toezichthouder (cf. art. 26, 7, f) *juncto* art. 71 §1, 3e lid WGB) van de BELPIE (passagiersinformatie-eenheid). Het is evenwel onduidelijk wat op dat vlak de reikwijdte van de toezichtbevoegdheid van het Controleorgaan is voor de verwerkingen van de Douane zoals voorzien in het voorontwerp en welke toegang het COC in rechte heeft tot het centrale ETIAS-informatiesysteem.

20. In het licht van het voorgaande verzoekt het Controleorgaan dan ook om in het voorontwerp (1) duidelijk de toezichthoudende opdracht van het Controleorgaan voor de verwerkingen van titel 2 WGB, die uitgevoerd worden door de in artikel 6, 2°, a) bedoelde politiediensten en die deel uit maken van de sectie van het Nationaal Crisiscentrum, bedoeld in hoofdstuk 4 van het voorontwerp, enerzijds, en (2) het toezicht op de raadpleging van ETIAS-gegevens door de politiediensten en de Douane (middels de vordering van adviseur-generaal van deze laatste) met het oog op het voorkomen en opsporen van

[15] Wet van 25 december 2016 "*betreffende de verwerking van passagiersgegevens*".

terroristische misdrijven of andere misdrijven, anderzijds, vast te leggen en daarbij te voorzien in een eenduidige en volledige toegang voor het Controleorgaan tot het centrale ETIAS-informatiesysteem en alle andere mogelijke databanken die in dat kader door de E.N.E zouden worden opgericht en desbetreffende verwerkingen.

3. Convergentie met de bepalingen van het informatiebeheer van de WPA

21. Volgens artikel 18 van het voorontwerp worden de persoonsgegevens die aan de politie voor handhavingsdoeleinden worden doorgegeven "*gewist wanneer dit onderzoek is afgesloten*". Het gaat hier, behoudens een vergissing van het COC, voor alle duidelijkheid over het gebruik van persoonsgegevens uit het centrale ETIAS-informatiesysteem dat geen betrekking heeft op de evaluatie in het kader van de aanvraag van een reisautorisatie. De vraag is of de verplichting voor de politiediensten om de ontvangen gegevens te wissen wanneer het onderzoek is afgesloten, verenigbaar is met de artikelen 44/5 en 44/9 van de WPA wat betreft de bewaartermijn van de politionele gegevens in de operationele gegevensbanken en de regeling met betrekking tot het archiveren van deze gegevens. Het Controleorgaan verzoekt dat de steller van het voorontwerp dit plausibele spanningsveld tussen dit voorontwerp en de desbetreffende bepalingen van het informatiebeheer van de WPA te onderzoeken en, in voorkomend geval, in artikel 18 van het voorontwerp het laatste zinsdeel te schrappen en te vervangen door een verwijzing naar de hiervoor aangestipte artikelen van de WPA.

22. Voor het overige heeft het Controleorgaan een opmerkingen.

OM DEZE REDENEN,

Het Controleorgaan op de Politionele Informatie,

verzoekt de aanvrager rekening te houden met de hogervermelde opmerkingen.

Advies goedgekeurd door het Controleorgaan op de Politionele Informatie op 10 juli 2023.

Voor het Controleorgaan,
De Voorzitter a.i.,
Frank SCHUERMANS

Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 121/2023 du 18 juillet 2023

Objet:
Demande d'avis concernant un avant-projet de loi relatif à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.) (CO-A-2023-236)
Demande d'avis concernant un avant-projet de loi modifiant la loi relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.) (CO-A-2023-237)

Version originale

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent.e.s : Mesdames Cédrine Morlière, Nathalie Ragheno et Griet Verhenneman et Messieurs Yves-Alexandre de Montjoye et Bart Preneel;

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 »);

Vu les demandes d'avis de la ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique, Madame Annelies Verlinden (ci-après « la ministre » ou « le demandeur »), reçues le 8 juin 2023;

Émet, le 18 juillet 2023, l'avis suivant :

I. Objet et contexte de la demande d'avis

1. La ministre a introduit auprès de l'Autorité une demande d'avis concernant un avant-projet de loi *relatif à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.)* (CO-A-2023-236) (ci-après, « **le Projet** »), et une demande d'avis concernant un avant-projet de loi *modifiant la loi relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.)* (CO-A-2023-237) (ci-après, « **le Projet modificatif** »).

2. Ces projets exécutent certaines dispositions du Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 *portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) no 1077/2011, (UE) no 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226* (ci-après, « **le Règlement ETIAS** »). Ce dispositif, s'inscrivant dans un contexte normatif complexe, concerne les ressortissants d'Etats tiers qui, dispensés de l'obligation d'obtenir un visa, souhaitent voyager dans l'Union. A sa genèse, ETIAS est inspiré de l'ESTA américain, de l'AVE du canadien et de l'eVisitor australien.

3. Le Contrôleur Européen de la Protection des Données (ci-après, « **CEPD** ») a rendu un avis au sujet de la proposition de Règlement ETIAS auquel l'Autorité renvoie à titre informatif[1].

[1] Celui-ci a toutefois souligné « *qu'en l'absence d'une analyse d'impact relative à la protection des données, qui constitue une condition sine qua non essentielle, il est impossible de procéder à une évaluation exhaustive de la nécessité et de la proportionnalité de l'ETIAS tel qu'il est proposé actuellement* » **CEPD, avis 3/2017** *sur la proposition de règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)*, 6 mars 2017 (ci-après « **avis CEPD ETIAS** »). Ultérieurement, voir CEPD, avis sur l'AIPD de l'ETIAS, Dossier 2021-0640, disponible sur https://edps.europa.eu/system/files/2022-03/22_03_27_formal_consultation_etias_dpia_fr.pdf, dernièrement consulté le 05/07/2023.

II. Examen

4. L'examen des Projets est structuré comme suit :

5. **Sur le plan de la protection des données**, ETIAS se situe à la fois dans le champ d'application du **RGPD**, dans celui de la Directive **2016/680**[2] et dans celui du **Règlement 2018/1725**[3]. L'article 31 du Projet découpe le Projet selon les règles de protection des données belges applicables. Conformément à la LTD, l'Autorité rappelle qu'elle ne se prononce pas sur le traitement de données à caractère personnel par les autorités compétentes (dont les services de police) visées au titre 2 de la LTD, compétence relevant de l'Organe de Contrôle de l'information policière (ci-après, « **COC** »), ou par les services de renseignement et de sécurité visés au titre 3 de la LTD, pour lesquels le Comité permanent de contrôle des services de renseignement et de sécurité est compétent. Ces autorités ont été saisies par le demandeur dans leurs compétences respectives.

6. Le **Règlement ETIAS** lui-même contient une série de **dispositions spécifiquement relatives au traitement de données à caractère personnel et en particulier** : son article 13 (accès aux données conservées dans ETIAS) ; son Chapitre XI (articles 54 et 55) (conservation[4] et modification des données) ; son Chapitre XII (protection des données), dont l'article 56 ventile l'application du RGPD et de la Directive 2016/680, l'article 57 identifie un responsable du traitement des données et l'article 58 désigne un sous-traitant, l'article 59 vise la sécurité des traitements, l'article 60 concerne les incidents de sécurité, l'article 61 porte sur l'autocontrôle, l'article 62 exige des sanctions, l'article 63 a trait à la responsabilité (civile – droit à réparation), l'article 64 vise le droit d'accès, l'article 65 limite les communications de données à caractère personnel à des Etats tiers ou des entités privées, les articles 66 à 68 visent le contrôle par les autorités de contrôle et leur coopération, et les articles 69 et 70 prévoient la tenue de registres.

7. En résumé, les Projets soumis pour avis s'inscrivent entre autres dans des logiques institutionnelles (création de l'Unité nationale ETIAS belge, répartition des tâches, etc.) et procédurales (organisation des accès, organisation d'une voie de recours dans le Projet de modification, etc.).

8. Le Règlement ETIAS et le Projet impliquent clairement une **ingérence particulièrement importante** dans les droits et libertés des personnes concernées. En ce sens notamment : les

---

[2] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.*

[3] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE*.

Pour être exhaustif, dès lors qu'Europol est impliquée, encore convient-il d'évoquer le Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 *relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI*.

[4] Le dossier de demande est conservé pendant la durée de validité de l'autorisation de voyage ou pendant cinq ans à compter de la dernière décision de refus, d'annulation ou de révocation (sous réserve de suppression anticipée, voir l'article 54, 1., b), du Règlement ETIAS). Le demandeur peut également consentir à ce que son dossier demeure conserver afin de faciliter une nouvelle demande (article 54, 2., du Règlement ETIAS). Le dossier de demande est automatiquement effacé du système central ETIAS à l'expiration de la période de conservation.

traitements prévus sont à grande échelle[5], ils ont un impact direct sur la liberté des personnes concernées de se rendre dans l'Union[6], ils impliquent des données pouvant se révéler sensibles et présentant un risque de discrimination[7], ils entraînent d'une manière ou d'une autre, une certaine surveillance continue des personnes concernées[8], ils conduisent au croisement de plusieurs systèmes d'information répondant à des finalités distinctes[9], et ils reposent sur des traitements automatisés de données (un *screening*) également basés sur le profilage[10].

II.1. ETIAS, SES FINALITÉS ET LES RÈGLES DE PROTECTION DES DONNÉES APPLICABLES

9. Le Règlement ETIAS crée un système européen d'information et d'autorisation concernant les voyages (ci-après, « **ETIAS** », pour « *European Travel Information and Authorisation System* »[11]). Lorsqu'il entrera en vigueur, les nationaux d'une soixantaine de pays tiers[12] ne devant pas disposer de visa pour entrer dans trente pays européens[13], devront obtenir une autorisation de voyage via ETIAS, accessible à partir d'un site Internet et d'une application mobile, et délivrée au terme d'un *screening* automatisé organisé par le Règlement et reposant en partie, sur les Etats membres.

[5] Voir les considérants nos 9-10.

[6] Voir notamment les considérants nos 9-13.

[7] Voir notamment le considérant n° 50.

[8] Voir les considérants nos 79-81.

[9] Notamment, au considérant n° 15 de son avis, le CEPD « *souhaite insister sur le fait que, bien qu'il existe des interactions entre la migration et la sécurité intérieure, il s'agit de deux domaines de l'ordre public différents dont les objectifs et les acteurs principaux sont distincts* ». Voir également les considérants nos 35 et s.

[10] Voir les considérants nos 35 et s.

[11] Voir https://travel-europe.europa.eu/etias/what-etias_en, dernièrement consulté le 27/06/2023.

[12] Voir https://travel-europe.europa.eu/etias/who-should-apply_en#who-needs-an-etias-travel-authorisation,

dernièrement consulté le 27/06/2023. L'article 2 du Règlement ETIAS définit les catégories de ressortissants de pays tiers auxquelles il s'applique et auxquelles il ne s'applique pas.

[13] Soit les 27 Etats Membres, la Suisse, le Lichtenstein et la Norvège,

voir https://travel-europe.europa.eu/etias/who-should-apply_en#ETIAS-countries, dernièrement consulté le 27/06/2023.

10. Le Règlement ETIAS[14] fixe dans le détail le cadre normatif de fonctionnement d'ETIAS (et du système d'information ETIAS[15]) de telle sorte qu'en la matière, la **marge de manœuvre de l'Etat belge est réduite**. Au niveau européen, ETIAS est développé et géré techniquement par l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (ci-après, « **eu-LISA** »)[16]. L'**unité centrale ETIAS** (soit une entité administrative) est quant à elle créée au sein de **l'Agence européenne de garde-frontières et de garde-côtes**[17]. Cette dernière Agence et eu-LISA se voient en outre attribuer par le Règlement ETIAS des responsabilités de responsable du traitement[18].

11. Dans le contexte du *screening* et des autorisations de voyage, les **unités nationales ETIAS** (ci-après, « **U.N.E.** »)[19] sont sollicitées dans certaines hypothèses, lorsque le *screening* automatisé nécessite un

[14] Confiant également à la Commission le pouvoir d'adopter des actes délégués et d'exécution. Peuvent être cités les textes suivants. Voir notamment :

Décision déléguée (UE) 2019/969 de la Commission du 22 février 2019 *relative à l'outil permettant aux demandeurs de donner ou de retirer leur consentement à la conservation de leur dossier de demande pour une période supplémentaire, en application de l'article 54, paragraphe 2, du règlement (UE) 2018/1240 du Parlement européen et du Conseil* ;

Décision d'exécution (UE) 2021/627 de la Commission du 15 avril 2021 *établissant des règles relatives à la tenue des registres et à l'accès à ceux-ci dans le système européen d'information et d'autorisation concernant les voyages (ETIAS) conformément au règlement (UE) 2018/1240 du Parlement européen et du Conseil* ;

Règlement délégué (UE) 2021/916 de la Commission du 12 mars 2021 *complétant le règlement (UE) 2018/1240 du Parlement européen et du Conseil portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) en ce qui concerne la liste préétablie de groupes d'emplois utilisée dans le formulaire de demande* ;

Décision d'exécution (UE) 2021/1028 de la Commission du 21 juin 2021 *portant adoption de mesures d'application du règlement (UE) 2018/1240 du Parlement européen et du Conseil en ce qui concerne la modification, l'effacement et l'effacement anticipé des données ainsi que l'accès à ces dernières dans le système central ETIAS* ;

Règlement d'exécution (UE) 2022/1380 de la Commission du 8 août 2022 *établissant les règles et conditions applicables aux interrogations de vérification lancées par les transporteurs, les dispositions relatives à la protection et à la sécurité des données pour le dispositif d'authentification des transporteurs, ainsi que les procédures de secours en cas d'impossibilité technique et abrogeant le règlement d'exécution (UE) 2021/1217* ;

Décision d'exécution (UE) 2022/102 de la Commission du 25 janvier 2022 *établissant des formulaires de refus, d'annulation ou de révocation d'une autorisation de voyage*, ci-après, la « **décision d'exécution 2022/102** » ;

Décision déléguée (UE) 2022/1612 de la Commission du 16 février 2022 *précisant le contenu et la forme de la liste préétablie d'options devant être utilisée aux fins d'une demande d'informations ou de documents supplémentaires conformément à l'article 27, paragraphe 3, du règlement (UE) 2018/1240 du Parlement européen et du Conseil* ;

Commission Delegated Decision of 10.12.2020 *supplementing Regulation (EU) 2018/1240 of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) as regards flagging* ;

Commission Delegated Decision of 23.11.2021 *on further defining security, illegal immigration or high epidemic risk*, C(2021) 4981 final ;

Commission Delegated Decision of 27.3.2023 *supplementing Regulation (EU) 2018/1240 of the European Parliament and of the Council, as regards specifying the conditions for the correspondence between the data present in a record, alert or file of the other EU information systems consulted and an ETIAS application file,* C(2023) 950 final ;

[15] Voir les articles 5 et 6 du Règlement ETIAS qui définissent ce qu'est ETIAS ainsi que l'architecture technique du système d'information ETIAS. Notamment, ETIAS comprend « *une interface uniforme nationale (**IUN**) dans chaque État membre, basée sur des spécifications techniques communes et identiques pour tous les États membres, qui permet au système central ETIAS de se connecter de manière sécurisée aux infrastructures frontalières nationales et aux points d'accès centraux des États membres visés à l'article 50, paragraphe 2* » (gras ajouté par l'Autorité) (article 6, 2., b), du Règlement ETIAS).

[16] Voir l'article 6 du Règlement ETIAS. Voir encore les responsabilités définies aux articles 73 et 74 du Règlement ETIAS.

[17] Voir l'article 7 du Règlement ETIAS. Voir encore les responsabilités définies à l'article 75 du Règlement ETIAS.

[18] Voir l'article 57 du Règlement ETIAS. Voir les considérants nos 102 et s.

[19] Article 8 du Règlement ETIAS.

traitement « manuel »[20]. Le Projet crée l'U.N.E belge **au sein du Centre de Crise National** (ci-après, « **CCN** »)[21].

12. ETIAS poursuit plusieurs objectifs[22] qui peuvent être regroupés, en simplifiant, sous trois grands groupes de finalités, dont les deux premiers retiendront l'essentiel des commentaires émis dans le présent avis.

II.1.1. <u>Finalité prévention de risques</u>

13. Tout d'abord, ETIAS à pour objectif de prévenir certains risques liés à l'entrée des personnes concernées sur le territoire européen : un risque en matière de **SÉCURITÉ**[23] ; un risque en matière **d'IMMIGRATION ILLÉGALE**[24] ; et un **RISQUE ÉPIDÉMIQUE ÉLEVÉ**[25]. Il s'agit d'une finalité de prévention de risques.

14. Le **RGPD** s'applique aux traitements par les **unités nationales ETIAS** « *qui **<u>évaluent</u>** les demandes* »[26] (gras ajouté et souligné par l'Autorité) d'autorisation de voyage des personnes concernées.

15. Cependant, « [l]*orsque le traitement de données à caractère personnel par les unités nationales ETIAS est effectué par les **autorités compétentes** qui **<u>évaluent</u>** les demandes aux fins de la **prévention** ou de la détection des **infractions terroristes ou d'autres infractions pénales graves**, ou des enquêtes en la matière, la **directive (UE) 2016/680** s'applique* »[27] (gras ajouté et souligné par l'Autorité).

16. « *Lorsque l'Unité nationale ETIAS **<u>décide</u>** de délivrer, de refuser, de révoquer ou d'annuler une autorisation de voyage* » (gras ajouté et souligné par l'Autorité), le **RGPD** s'applique[28].

---

[20] L'article 76 du Règlement ETIAS détermine des responsabilités incombant aux Etats membres.

[21] Article 4 du Projet.

[22] L'article 4 du Règlement ETIAS définit plus précisément les objectifs du Règlement.

[23] Défini à l'article 3, 1., 6., du Règlement ETIAS, comme « *un risque de menace pour l'ordre public, la sécurité intérieure ou les relations internationales de l'un des Etats membres* ».

[24] Défini à l'article 3, 1., 7., du Règlement ETIAS, comme « *le risque qu'un ressortissant de pays tiers ne remplisse as les conditions d'entrée et de séjour énoncées à l'article 6 du Règlement (UE) 2016/399* ».

[25] Défini à l'article 3, 1., 8., du Règlement ETIAS, comme « *toute maladie à potentiel épidémique au sens de la définition qu'en donne le règlement sanitaire internationale de l'Organisation mondiale de la santé (OMS) ou le Centre européen de prévention et de contrôle des maladies (ECDC), et d'autres maladies infectieuses ou parasitaires contagieuses, pour autant qu'elles fassent l'objet de dispositions de protection applicables aux ressortissants des Etats membres* ».

[26] Article 56, 2., al. 1er, du RGPD.

[27] Article 56, 2., al. 2, du RGPD.

[28] Article 56, 2., al. 3, du RGPD.

17. Et s'agissant de **l'autorité de contrôle**, le Règlement prévoit de manière générale que chaque Etat membre « *veille à ce que l'autorité de contrôle instituée conformément à l'article 51, paragraphe 1, du règlement (UE) 2016/679 contrôle en toute indépendance la licéité du traitement des données à caractère personnel effectué par l'État membre concerné en vertu du présent règlement, y compris de leur transmission à partir d'ETIAS et vers celui-ci* » (souligné par l'Autorité)[29]. Le Règlement ETIAS ne se réfère à l'autorité de contrôle visée à l'article 41 de la Directive 2016/680 que dans son article 65 (relatif à la communication des données à des pays tiers[30]) et concernant l'utilisation d'ETIAS à des fins répressives[31]. Autrement dit, **l'Autorité en conclut que l'Autorité de contrôle désignée en exécution du RGPD devrait également être compétente à l'égard de l'évaluation de risques, bien que cette évaluation soit soumise à la Directive 2016/680[32]**.

18. Le Projet alloue les compétences, dans la finalité de prévention des risques poursuivie par ETIAS, entre deux sections différentes de l'U.N.E. belge[33] :

- La **section de l'Office des Etrangers** (ci-après, « **Section OE** »)[34], qui est compétente à l'égard des risques d'immigration illégale ;

- Et la **section du Centre National de Crise** (ci-après, « **Section CCN** »)[35], qui est compétente pour les autres risques (à savoir, le risque de sécurité et le risque épidémique élevé)[36].

19. Compte-tenu de ce qui vient d'être précisé, l'article 31, § 2, du Projet peut prévoir l'application du titre 2 de la LTD à « *l'évaluation des risques sécuritaires* », **pour autant que l'Autorité de Protection des Données sera l'autorité de contrôle compétente dans ce contexte**, **sauf pour ce qui concerne la compétence du COC à l'égard des services de police**, dès lors que celui-ci a aussi été désigné comme autorité de contrôle en exécution du RGPD[37].

---

[29] Article 66, 1., du Règlement ETIAS.

[30] Voir à ce sujet, les considérants nos 116-117.

[31] Considérants nos 28 et s.

[32] Ce qui peut être mis en perspective avec la possibilité ouverte aux Etats membres, par l'article 41, 3., de la Directive 2016/680, de désigner une autorité de contrôle instituée au titre du RGPD, comme autorité de contrôle dans le cadre de cette directive.

[33] Il s'agit plus exactement du traitement des « *réponses positives* », voir les considérants nos 42-58 à ce sujet. Article 5, § 1er, du Projet.

[34] L'article 26 du Projet détermine sa composition.

[35] Les articles 6 à 10 du Projet détermine sa composition et son fonctionnement.

[36] Celle-ci comporte un officier de liaison de l'Office des Etranger, article 6, 3°, du Projet, qui est sous l'autorité du fonctionnaire dirigeant de la Section O.E. de l'U.N.E. Sa mission est définie à l'article 30 du Projet.

[37] L'article 4, § 2, al. 4, de la LCA, prévoit que :

« *A l'égard des services de police au sens de l'article 2,2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle de l'information policière visé à l'article 44/6, § 1er, de la loi du 5 août 1992 sur la fonction de police* ».

20. Il convient encore de souligner que s'inscrit dans la finalité de la prévention des risques, l'établissement de la **liste de surveillance ETIAS**[38]. Il s'agit d'une liste comportant des informations introduites par Europol ou par les Etats Membres[39], sur la base d'informations relatives à des **infractions terroristes ou à d'autres infractions pénales graves** – sont visées des personnes soupçonnées[40]. Cette liste sera l'objet d'un traitement automatisé dans le cadre du *screening* mis en place en vertu du Règlement ETIAS[41].

21. **A ce sujet, l'article 21 du Projet doit être adapté en ce qu'il se réfère aux finalités répressives d'ETIAS plutôt qu'à la finalité de prévention du risque de sécurité**. Si le Règlement ETIAS n'est pas limpide à ce propos[42], l'Autorité est d'avis que le demandeur pourrait considérer de manière générale que la contribution à la liste de surveillance ETIAS participe à l'évaluation des demandes au regard du risque de sécurité et partant, peut être soumise aux règles transposant la Directive 2016/680[43], étant entendu que comme cela vient d'être souligné, l'Autorité de Protection des Données est l'autorité de contrôle visée par le Règlement ETIAS, sauf pour les services de police. Autrement dit, **l'article 21 du Projet peut prévoir l'application du titre 2 de la LTD « *aux fins de la gestion de la liste de surveillance ETIAS* » pour autant que l'Autorité de Protection des Données soit l'autorité de contrôle compétente, sauf pour les services de police**.

22. Enfin, si l'Autorité n'est en principe pas compétente en droit positif belge pour se prononcer sur les règles qui régissent les traitements de données dont sont responsables les **services de renseignements et de sécurité**, force est de constater que le Projet entend intégrer ces services au dispositif du Règlement ETIAS, en leur attribuant une compétence de procéder à l'évaluation des demandes au regard du risque de sécurité. **Sans adaptation du droit belge, l'Autorité de Protection des Données serait compétente, sur la base de sa compétence résiduaire[44], à l'égard des membres détachés des services de renseignement et de sécurité dans le cadre de l'analyse de risques** à réaliser (en exécution des règles de protection des données du titre 2 de la LTD).

---

[38] Voir l'article 20, 4., du Règlement ETIAS.

[39] Article 34, 3., du Règlement ETIAS. Les articles 34, 3., et 35, du Règlement ETIAS déterminent les **responsabilités des Etats membres** (et d'Europol) en la matière.

[40] Voir l'article 34, 2., du Règlement ETIAS et la note de bas de page n° 52. L'article 34, 4., du Règlement ETIAS précise les données reprises dans la liste (le nom, les autres noms tels que les éventuels pseudonymes, l'adresse électronique, l'adresse IP, les prénoms, la nationalité, etc.).

[41] Voir le considérant nos 45 et s.

[42] L'article 56, 2., ne vise pas directement la contribution à la liste de surveillance.

[43] Voir l'article 31, § 2, du Projet, rendant applicable le titre 2 de la LTD.

[44] Voir l'article 4, § 2, al. 2, de la LCA.

23. **A ce sujet, l'Autorité doute que le Règlement ETIAS permette de soumettre une partie des traitements de données qu'il encadre à une autorité de contrôle qui ne serait pas désignée en exécution du RGPD ou en transposition de la Directive 2016/680**, soit une autorité ne relevant pas de la sphère d'application du droit européen. Le Projet entend permettre l'intervention des services de renseignements et de sécurité dans les matières relevant des autorités compétentes au sens du titre 2 de la LTD et de la Directive 2016/680 – soit une finalité *autre* que celle justifiant leur exclusion du droit européen en général[45]. Or l'article 42 du Projet qui insère un nouveau sous-titre 5*bis* intitulé « *De la protection des personnes physiques à l'égard de certains traitements de données à caractère personnel par la section du Centre de Crise National de l'Unité nationale ETIAS* » au titre 3 de la LTD, attribue une compétence au Comité permanent R visé à l'article 95 de la LTD, une autorité qui n'est pas désignée en droit belge en vertu des règles européennes de protection des données précitées.

24. Dans ces conditions, **l'Autorité semble pouvoir conclure qu'il découle juridiquement de ce qui précède** (notamment au sujet de l'autorité de contrôle désignée par le Règlement ETIAS[46]) **que l'Autorité de Protection des Données doit être désignée comme autorité de contrôle** en la matière (évaluation des risques, y compris la liste de surveillance ETIAS) – sans préjudice des commentaires ultérieurs concernant les finalités poursuivies par les services de renseignement et de sécurité[47]. Et ceci, **à moins que le législateur belge**, à la manière dont il a procédé pour les services de police, **ne désigne le Comité R comme autorité compétente belge en exécution du RGPD, pour les services de renseignements et de sécurité** (compétence relevant à ce jour, de l'Autorité de Protection des Données)**, lorsque leurs traitements de données relèvent du RGPD[48]**.

25. Les **règles auxquelles seraient soumis les services de renseignements et de sécurité dans ce domaine en vertu du Projet posent également question**. Selon l'article 184/2 en projet de la LTD (tel qu'introduit par l'article 42 du Projet), celui-ci s'applique « *au traitement de données à caractère personnel effectué par les détachés de la* [VSSE] *et du* [SGRS] *au sein de la section du Centre de Crise National de l'U.N.E.* » dans le cadre des finalités visées à l'article 14, § 1er, 3°, du Projet, à savoir la consultation d'ETIAS *à des fins répressives*. L'Autorité observe d'emblée que l'article 31, § 3, du Projet et l'article 184/2 de la LTD en Projet doivent être reformulés afin que soient également

[45] Le Projet entend même aller plus loin, de manière contestable, voir les considérants nos 95 et s.

[46] Voir le considérant n° 17.

[47] Voir les considérants nos 95-97.

[48] Pour rappel bien entendu, l'article 73 de la LTD dispose que : « *Le présent sous-titre s'applique à tout traitement de données à caractère personnel par les services de renseignement et de sécurité et leurs sous-traitants effectués dans le cadre des missions desdits services visés aux articles 7 et 11 de la loi du 30 novembre 1998 ainsi que par ou en vertu de lois particulières* ». En substance, dans l'exercice de leurs missions relevant de la sécurité nationale, les services de renseignements et de sécurité sont soumis à des règles de protection des données belges ne découlant pas du droit de l'Union européenne. Et dans ce cadre, le Comité R est l'autorité de contrôle compétente, conformément à l'article 95 de la LTD.

encadrées sans aucun doute les activités de traitement par les membres détachés des services de renseignements et de sécurité *lorsqu'ils réalisent des évaluations de risques* pour la Section CCN.

26. Mais plus fondamentalement, compte-tenu de ce qui vient d'être évoqué[49] et de l'article 66, 2., du Règlement ETIAS[50], l'Autorité est d'avis que **ce serait en principe le titre 2 de la LTD qui devrait s'appliquer *mutatis mutandis,* et non un autre titre prévoyant des règles *sui generis* réduites concernant le traitement des données à caractère personnel**. Il se dégage clairement du Règlement ETIAS que les traitements de données réalisés en exécution de celui-ci doivent soit être conformes au RGPD soit à la Directive 2016/680. S'agissant de l'évaluation du risque de sécurité, c'est cette dernière qui s'applique conformément à l'article 56, 2., al. 2, du Règlement ETIAS.

27. **En conclusion, les développements précédents peuvent être synthétisés comme suit, s'agissant des services de renseignements et de sécurité.** Si l'Etat belge entend étendre le dispositif européen ETIAS à ses services de renseignements et de sécurité lorsque ceux-ci agissent dans le cadre des finalités de ce dernier, il doit soumettre ceux-ci, à ces fins, aux règles européennes de protection des données applicables, dès lors que dans ce cas, ils agissent comme des autorités compétentes au sens de la Directive 2016/680. D'une part, dès lors que l'évaluation du risque (y compris la contribution à la liste de surveillance) est soumise à la Directive 2016/680 lorsqu'elle est effectuée par les autorités compétentes, l'activité des services de renseignement en la matière doit être soumise *mutatis mutandis* aux règles de droit belge transposant cette directive (titre 2 de la LTD). S'agissant de l'autorité de contrôle compétente, d'autre part, le Règlement ETIAS exigeant qu'il s'agisse de l'autorité désignée en exécution du RGPD, cela ne peut être, pour ces services, que l'Autorité de Protection des Données. A moins que le législateur belge, à la manière dont il a procédé pour les services de police, ne désigne le Comité R comme autorité compétente belge en exécution du RGPD pour les services de renseignements et de sécurité, lorsque leurs traitements de données relèvent du RGPD[51].

II.1.2. <u>Fins répressives</u>

28. Comme cela a été annoncé, ETIAS contribue à la prévention, à la détection et aux enquêtes concernant des infractions terroristes ou d'autres infractions pénales graves, soit les « **FINS RÉPRESSIVES** » d'ETIAS[52].

[49] Considérants nos 22-23.

[50] Voir le considérant n° 29.

[51] Voir la note de bas de page n° 48.

[52] Voir le Chapitre X du Règlement ETIAS (articles 50 et s.). Voir les considérants nos 84 et s.

29. Les traitements de données réalisés dans ce contexte sont soumis à la **directive 2016/680**[53]. Chaque Etat membre doit veiller à « *ce que les dispositions législatives, réglementaires et administratives nationales qu'il a adoptées en application de la directive (UE) 2016/680 s'appliquent aussi à l'accès à ETIAS par ses autorités nationales conformément au chapitre X du présent règlement, y compris pour ce qui est des droits des personnes dont les données sont ainsi consultées* » (souligné par l'Autorité)[54].

30. Et **l'Autorité de contrôle** désignée en vertu de l'article 41, 1., de la directive 2016/680 est compétente en la matière[55].

31. De nouveau, s'agissant du rôle que pourraient jouer en la matière les **services de renseignements et de sécurité**[56], comme cela vient d'être évoqué *mutatis mutandis*, ces services devraient, conformément au Règlement ETIAS, être soumis aux règles consacrées dans le titre 2 de la LTD. Il appartiendrait alors au Projet d'identifier comme autorité de contrôle, soit le COC, soit l'Autorité de Protection des Données. **Pour que le Comité R puisse être l'autorité de contrôle compétente en la matière, il faudrait que le législateur belge le désigne comme autorité compétente à l'égard des services de renseignements et de sécurité lorsqu'ils agissent en tant qu'autorité compétente au sens de la Directive 2016/680 et en exécution de l'article 41 de celle-ci[57]**. Le Règlement ETIAS n'apparaît pas laisser de marge de manœuvre pour rendre applicables et compétente des règles et une autorité de contrôle autres que celles découlant de la mise en œuvre de la Directive 2016/680.

II.1.3. Autres finalités

32. ETIAS sera également utilisé par les entreprises de transport[58] et par les autorités compétentes aux frontières[59], ainsi que par les autorités chargées de l'immigration[60], afin de vérifier que les personnes concernées disposent bien de l'autorisation de voyage requise – **finalité de CONTRÔLE DE L'ACCÈS AU TERRITOIRE**.

33. Le traitement de données à caractère personnel réalisé à cette fin par ces autorités publiques est soumis au **RGPD**[61].

---

[53] Article 56, 3., du Règlement ETIAS.
[54] Article 66, 2., du Règlement ETIAS.
[55] Article 66, 3., du Règlement ETIAS.
[56] Voir le considérant n° 96.
[57] Voir également le considérant n° 27.
[58] Voir le Chapitre VII du Règlement ETIAS (articles 45 et s.).
[59] Voir le Chapitre VIII du Règlement ETIAS (articles 47 et s.).
[60] Voir le Chapitre IX du Règlement ETIAS (article 49).
[61] Article 56, 2., al. 1er, du Règlement ETIAS.

34. Enfin, ETIAS contribue aux objectifs de trois autres systèmes d'information européens – **finalité de SOUTIEN**. Premièrement, il soutient les **objectifs du Système d'information Schengen** (ci-après, le « **SIS** »)[62] concernant certains signalements de personnes concernées. Deuxièmement, il soutient les objectifs du système d'entrée/de sortie (soit l' « *Entry/Exit System* », ci-après, l' « **EES** »)[63] (notamment, un processus automatisé d'EES consulte ETIAS pour créer ou mettre à jour la fiche d'entrée/de sortie ou la fiche de refus d'entrée[64]). Il contribue troisièmement, en lien avec d'autres systèmes d'information, à l'identification correcte des personnes, en relation avec le répertoire commun de données d'identité (soit « *Common Identity Repository* », ci-après « **CIR** »)[65].

---

[62] Voir les Règlements européens suivants :

Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 *relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier* ;

Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 *sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) no 1987/2006* ;

Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 *sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) no 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission*.

Selon l'article 5, e), du Règlement ETIAS, les **signalements** suivants sont concernés : « *les objectifs du SIS relatifs aux signalements concernant des ressortissants de pays tiers faisant l'objet d'une non-admission et d'une interdiction de séjour, aux signalements concernant des personnes recherchées en vue d'une arrestation aux fins de remise ou d'extradition, aux signalements concernant des personnes disparues, aux signalements concernant des personnes recherchées pour prêter leur concours dans le cadre d'une procédure judiciaire, aux signalements concernant des personnes aux fins de contrôles discrets ou de contrôles spécifiques et aux signalements concernant des ressortissants de pays tiers faisant l'objet d'une décision de retour* ».

A propos de **SIS**, voir https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/what-sis-and-how-does-it-work_en, dernièrement consulté le 27/06/2023.

Voir **l'avis de l'Autorité n° 121/2022** du 1er juillet 2022 *concernant un avant-projet de loi relatif au fonctionnement et à l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, dans le domaine des vérifications aux frontières et aux fins du retour des ressortissants de pays tiers en séjour irrégulier (CO-A-2022-125)*.

Voir **CEPD, avis 7/2017** *sur la nouvelle base juridique du système d'information Schengen*, 2 mai 2017.

[63] Voir le Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 *portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) no 767/2008 et (UE) no 1077/2011*.

Voir **l'avis de l'Autorité n° 122/2022** du 1er juillet 2022 *concernant un avant-projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, en ce qui concerne le système d'entrée/de sortie (CO-A-2022-138)*.

[64] Article 11*ter* du Règlement ETIAS. Voir également l'article 11*quater* du Règlement ETIAS (révocation d'une autorisation de voyage par le demandeur).

[65] Il s'agit du répertoire établi à l'article 17, 1., du Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 *portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) no 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil* (ci-après, « le **Règlement interopérabilité** »).

Voir **CEPD, avis 4/2018** *sur les propositions de deux règlements portant établissement d'un cadre pour l'interopérabilité des systèmes d'information à grande échelle de l'UE*, 16 avril 2018.

Selon l'article 17, 1., du Règlement interopérabilité :

« *Un répertoire commun de données d'identité (CIR), créant un dossier individuel pour chaque personne enregistrée dans l'EES, le VIS, ETIAS, Eurodac ou l' ECRIS-TCN contenant les données visées à l'article 18, est établi afin de faciliter l'identification correcte des personnes enregistrées dans l'EES, le VIS, ETIAS, Eurodac et l'ECRIS-TCN et d'aider à cette identification conformément à l'article 20, de soutenir le fonctionnement du MID conformément à l'article 21 et de faciliter et de rationaliser l'accès des autorités désignées et d'Europol à l'EES, au VIS, à ETIAS et à Eurodac, lorsque cela est nécessaire à des fins de prévention ou de détection d'infractions terroristes ou d'autres infractions pénales graves ou d'enquêtes en la matière conformément à l'article 22* » (souligné par l'Autorité).

II.2. SCREENING ET AUTORISATIONS DE VOYAGE

35. Le Règlement ETIAS met en place un processus de *screening* automatisé qui a pour but d'aboutir à la délivrance d'une autorisation de voyage ou à son refus.

36. Dans le cadre de son fonctionnement et afin de permettre des vérifications automatisées, le système d'information ETIAS est **interopérable avec cinq autres systèmes d'informations de l'UE**, à savoir : les systèmes **SIS** et **EES** déjà évoqués, le système d'information sur les visas (ci-après, « **VIS** »)[66], **Eurodac**[67] et le et le système européen d'information sur les casiers judiciaires pour les

---

Le **CIR** comporte une infrastructure centrale (développée et gérée par eu-LISA) qui remplace les systèmes centraux de l'EES, du VIS, d'ETIAS, d'Eurodac et de l'ECRIS-TCN, dans la mesure où elle stocke les données visées à l'article 18 du Règlement précité. L'article 18, précité, 1., prévoit ce qui suit :

« *1. Le CIR stocke les données suivantes, séparées logiquement en fonction du système d'information d'où elles proviennent:*

a) les données visées à l'article 16, paragraphe 1, points a) à d), à l'article 17, paragraphe 1, points a), b) et c), et à l'article 18, paragraphes 1 et 2, du règlement (UE) 2017/2226 [(soit le Règlement EES)] ;

b) les données visées à l'article 9, point 4) a) à c), et points 5) et 6), du règlement (CE) no 767/2008 [(soit le Règlement VIS)];

c) les données visées à l'article 17, paragraphe 2, points a) à e), du règlement (UE) 2018/1240 [(soit le Règlement ETIAS)] ».

L'article 6, 2. *bis*, du Règlement ETIAS, concernant l'architecture technique du système d'information ETIAS, dispose que « *Le CIR contient les données d'identité et les données du document de voyage. Les autres données sont stockées dans le système central* ».

Ces données sont les suivantes : le nom (nom de famille), le ou les prénoms (le ou les surnoms), le nom à la naissance; la date de naissance, le lieu de naissance, le sexe, la nationalité actuelle ; le pays de naissance, le ou les prénom(s) des parents du demandeur ; les autres noms (pseudonyme(s), nom(s) d'artiste, nom(s) d'usage), le cas échéant ; les autres nationalités, le cas échéant ; le type de document de voyage, le numéro et le pays de délivrance de ce document ; la date de délivrance du document de voyage et la date d'expiration de sa validité.

Le CIR contient en outre les **données du dossier individuel des ressortissants de pays tiers exemptés de l'obligation de visa** créé par l'autorité frontalière (le garde-frontière chargé, conformément au droit national, d'effectuer des vérifications aux frontières au sens de l'article 2, point 11), du règlement (UE) 2016/399) et visé à l'article 17 du Règlement EES, parmi lesquelles l'image faciale et les données dactyloscopiques de la main droite.

[66] Voir le Règlement (CE) no 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 *concernant le système d'information sur les visas (VIS) et l'échange d'informations entre les États membres sur les visas de court séjour, les visas de long séjour et les titres de séjour (règlement VIS)*.

Entre autres au sujet de **VIS**, « *The Visa Information System (VIS) allows Schengen States to exchange visa data. VIS connects consulates in non-EU countries and all external border crossing points of Schengen States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area.*

The system helps avoid 'visa shopping', supports documenting and prevents irregular migration. It can perform biometric matching, primarily of fingerprints, for identification and verification purposes and assists the authorities protecting the internal security of Member States », voir https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Vis, dernièrement consulté le 27/06/2023.

[67] Voir le Règlement (UE) no 603/2013 du Parlement européen et du Conseil du 26 juin 2013 *relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) no 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) no 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice*.

Notamment, **Eurodac** « *is a large-scale IT system that helps with the management of European asylum applications since 2003, by storing and processing the digitalized fingerprints of asylum seekers and irregular migrants who have entered a European country. In this way, the system helps to identify new asylum applications against those already registered in the database* », https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Eurodac, dernièrement consulté le 27/06/2023.

ressortissants de pays tiers (soit, « *European Criminal Records Information System – Third Country Nationals* », ci-après, « **ECRIS-TCN** »)[68].

37. Le système ETIAS effectue également des vérifications automatisées en interrogeant **les données d'Europol**[69].

38. Le système central ETIAS consultera encore et enfin **deux bases de données d'Interpol**[70] : celle concernant les documents de voyage volés ou perdus (soit « *Stolen and Lost Travel Documents Database* », ci-après « **SLTD** »)[71] et celle portant sur les documents de voyage associés aux notices (soit « *Travel Documents Associated With Notices* », ci-après, « **TDAWN** »).

39. Le processus de *screening* automatisé fonctionne comme suit.

II.2.1. Formulaire complété par la personne concernée

40. Le demandeur, la personne concernée, doit **compléter un formulaire par voie électronique**, à propos d'une série de données à caractère personnel (nom, nom à la naissance, prénoms, nationalités, études, prénoms des parents, profession dans une liste préétablie, réponse à des questions concernant notamment les condamnations pénales à une série d'infractions terroristes ou listée en annexe, etc.[72] ; le système collecte en outre l'adresse IP utilisée par le demandeur).

---

[68] Voir le Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 *portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726*.

En ce qui concerne **ECRIS-TCN**, notamment, « *The European Criminal Records Information System (ECRIS), operational since April 2012, provides an electronic exchange of criminal record information on a decentralised basis between Member States. It allows Member State's criminal records authorities to obtain complete information on previous convictions of EU nationals from the Member State of that person's nationality. ECRIS-TCN, once set up, will be a centralised system that allows Member State's authorities to identify which other Member States hold criminal records on the third country nationals or stateless persons being checked, so that they can then use the existing ECRIS system to address requests for conviction information only to the identified Member States* », voir https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Ecris-Tcn, dernièrement consulté le 27/06/2023.

[69] Définies par l'article 3, 1., 17., du Règlement Etias comme « *les données à caractère personnel traitées par Europol aux fins visées à l'article 18, paragraphe 2, point a), du règlement (UE) 2016/794* » du Parlement européen et du Conseil du 11 mai 2016 *relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI*. Cette disposition vise la finalité de traitement de données poursuivie par Europol consistant à réaliser des :

« *recoupements visant à établir des liens ou d'autres rapports pertinents entre des informations relatives:*

i) aux personnes qui sont soupçonnées d'avoir commis une infraction pénale ou d'avoir participé à une infraction pénale relevant de la compétence d'Europol, ou qui ont été condamnées pour une telle infraction;

ii) aux personnes pour lesquelles il existe des indices concrets ou de bonnes raisons de croire qu'elles commettront des infractions pénales relevant de la compétence d'Europol ».

[70] Voir l'article 12 du Règlement ETIAS.

[71] Voir https://www.interpol.int/How-we-work/Databases/SLTD-database-travel-and-identity-documents,

dernièrement consulté le 27/06/2023.

[72] Voir l'article 17 du Règlement ETIAS.

41. L'Autorité relève au passage dans ce cadre que l'exposé des motifs du Projet confirme **qu'ETIAS collecte des informations au sujet des personnes concernées qui *ne* sont *pas* exigées dans le cadre des demandes de visas**[73]. Ce qui, de manière générale, soulève une interrogation quant au principe d'égalité, découlant toutefois du Règlement ETIAS lui-même[74].

II.2.2. Traitements automatisés

42. Après une analyse de recevabilité[75], les données à caractère personnel communiquées sont ensuite l'objet des **traitements *automatisés* de vérification *par le système central* ETIAS** suivants, à la recherche de « ***réponses positives*** » (c'est-à-dire, des correspondances)[76], conformément aux articles 20 et 23 du Règlement ETIAS.

Traitements automatisés article 20 (général)

43. **Comparaison avec d'autres bases de données** – Le système central ETIAS lance une recherche de correspondances via le portail de recherche européen (soit « *European Search Portal* », ci-après, l'

[73] « *ETIAS collecte des données similaires à ce qui est actuellement d'application pour les visas. Les données suivantes sont cependant collectées uniquement dans le cadre d'une demande d'autorisation de voyage : les autres nationalités du demandeur, le pays de naissance et les prénoms des parents du demandeur, l'adresse électronique, le numéro de téléphone si disponible, les études, l'adresse du premier séjour si disponible, les données personnelles du citoyen de l'Union auxquels s'applique la directive 2004/38/CE ou d'un ressortissant de pays tiers jouissant d'un droit à la libre circulation équivalent à celui des citoyens de l'Union en vertu d'un accord entre l'Union et ses Etats membres, d'une part, et un pays tiers, d'autre part, auquel le demandeur est lié conformément à l'article 2 § 1 c) du règlement ETIAS, les données de l'intermédiaire qui complète la demande au profit du demandeur, les questions complémentaires listées à l'article 17 § 4 du règlement ETIAS ou encore l'adresse IP utilisée par le demandeur lors de sa requête* » (souligné par l'Autorité) (exposé des motifs du Projet, p. 2).

[74] Dans son avis (considérant n° 16), le « *CEDP se demande si la proposition ne crée pas un régime plus intrusif pour les voyageurs exemptés de l'obligation de visa que pour ceux soumis à l'obligation de visas dès lors que davantage de données seront centralisées au niveau de l'Union européenne dans l'ETIAS*[…] *que dans le VIS* ».

[75] Voir l'article 19 du Règlement ETIAS.

Remarque : le screening (traitements automatisés et le cas échéant, traitement manuel dont il sera question dans les développements suivants) est également réalisé si une autorisation de voyage est modifiée en réponse à une demande **d'exercice de ses droits** par le demandeur (personne concernée), conformément à l'article 64, 2., du Règlement ETIAS.

[76] L'article 3, 1., 14., du Règlement ETIAS, définit la réponse positive comme suit :

« *l'existence d'une correspondance établie en comparant les données à caractère personnel enregistrées dans un dossier de demande du système central ETIAS aux indicateurs de risques spécifiques visés à l'article 33 ou aux données à caractère personnel figurant dans un relevé, un dossier ou un signalement enregistré dans le système central ETIAS, dans un autre système d'information ou une autre base de données de l'Union européenne énumérés à l'article 20, paragraphe 2, (ci-après dénommés 'systèmes d'information de l'Union européenne'), dans les données d'Europol ou dans une base de données d'Interpol interrogés par le système central ETIAS* » (souligné par l'Autorité).

« **ESP** »)[77] avec les données des systèmes suivants : ETIAS lui-même, le SIS[78], l'EES, le VIS, Eurodac, l'ECRIS-TCN, les données d'Europol ainsi que les bases de données SLTD et TDAWN[79].

44. **Réponse affirmative à une question et absence d'adresse de domicile** – Le système central vérifie si le demandeur a répondu par l'affirmative à une ou plusieurs des questions posées dans le formulaire et si ce dernier a communiqué une ville et un pays de résidence à la place d'une adresse de domicile[80].

45. **Comparaison avec la liste de surveillance ETIAS** – Des données sont comparées avec la liste de surveillance ETIAS[81].

46. Les articles 21 à 25 du Projet régissent la liste de surveillance ETIAS qui peut être complétée par les **services de police**, la Sûreté de l'Etat (ci-après, « **VSSE** »), le Service Général du Renseignement et de la Sécurité des Forces armées (ci-après, « **SGRS** ») et l'Administration générale des douanes et accises (ci-après, « **AGD&A** »)[82].

47. S'agissant de **l'alimentation de la liste** de surveillance ETIAS, le Projet se limite à se référer aux conditions visées à l'article 34 du Règlement ETIAS et à la **faculté**[83], pour les autorités concernées, d'introduire des données. Dans ce contexte, l'Autorité a interrogé le demandeur quant aux circonstances (et aux règles), notamment compte-tenu du risque de discrimination, dans lesquelles les autorités concernées contribueront à la liste de surveillance ETIAS. Celui-ci a répondu ce qui suit :

> « *L'art 34,§1 stipule que les autorités concernées doivent avoir identifié des personnes soupçonnées d'avoir commis une infraction ou d'y avoir participé et/ou des personnes pour lesquelles il existe des raisons de croire qu'elles pourraient commettre une infraction sur la base de leurs propres informations. L'art 22 du Projet se réfère également à l'art 35,§1 du Règlement qui fixe les conditions à remplir avant d'introduire une donnée.*

---

[77] L'**ESP** est établi part l'article 6 du Règlement interopérabilité. Le 1. de cet article prévoit ce qui suit :

« *Un portail de recherche européen (ESP) est créé afin de faciliter l'accès rapide, continu, efficace, systématique et contrôlé des autorités des États membres et des agences de l'Union aux systèmes d'information de l'UE, aux données d'Europol et aux bases de données d'Interpol pour l'accomplissement de leurs tâches et conformément à leurs droits d'accès ainsi qu'aux objectifs et finalités de l'EES, du VIS, d'ETIAS, d'Eurodac, du SIS et de l'ECRIS-TCN* ». L'ESP comporte notamment une infrastructure centrale, comportant un portail de recherche permettant d'interroger simultanément l'EES, le VIS, ETIAS, Eurodac, le SIS, l'ECRIS-TCN ainsi que les données d'Europol et les bases de données d'Interpol. Il est développé par l'eu-LISA qui en assure également la gestion technique.

[78] Pour certains signalements : non-admission et interdiction de séjour ou arrestation (mandat d'arrêt ou extradition).

[79] Voir l'article 20, 2., du Règlement ETIAS. Voir également l'article 11 du Règlement ETIAS qui prévoit les vérifications automatisées entre systèmes interopérables.

[80] Article 20, 3., du Règlement ETIAS.

[81] Voir l'article 20, 4., du Règlement ETIAS et le considérant n° 19.

[82] Article 21 du Projet.

[83] L'article 21 du Projet précise clairement que les services concernés « *peuvent introduire des données dans la liste de surveillance ETIAS* ».

Un acte d'exécution EU est prévu pour donner un cadre assurant la journalisation et la sécurité des traitements liés à la liste de surveillance.

Le respect du principe de non-discrimination dans l'ensemble des traitements au sein du système d'information ETIAS (y compris la liste de surveillance) est prévu par l'article 14 du Règlement ETIAS.

Le Comité d'examen ETIAS (art 9 du Règlement) et le Comité d'orientation pour les droits fondamentaux (art 10 du Règlement) veillent au respect de ce principe, en particulier en ce qui concerne la mise en œuvre de la liste de surveillance (art 9,§2,b)) ».

48. L'Autorité prend acte de cette explication. Elle relève néanmoins que le Comité d'examen ETIAS est consulté par les Etats membres au sujet de la mise en œuvre de la liste de surveillance et qu'il émet des avis, des lignes directrices, des recommandations et bonnes pratiques en la matière (notamment)[84]. Le Règlement ETIAS fixe un seuil de suspicion à partir duquel une personne peut être signalée dans la liste de surveillance ETIAS mais ne détermine pas **les conditions dans lesquelles les autorités concernées *doivent* signaler une personne dans la liste de surveillance ETIAS**, **ce qui, de l'avis de l'Autorité, est nécessaire** au regard des principes de prévisibilité et de légalité consacré dans l'article 22 de la Constitution et 8 de la CEDH, et afin de diminuer le risque de discrimination des personnes concernées. Le dispositif du Projet doit par conséquent être adapté en conséquence.

49. **Comparaison à des indicateurs de risques spécifiques** – A l'aide d'un algorithme permettant un profilage (les **règles d'examen ETIAS**)[85], une série de données sont comparées à des indicateurs de risques spécifiques[86]. Dans ce contexte, *a priori*, **l'alimentation, par les Etats membres, de la Commission européenne en information afin d'établir des indicateurs de risques spécifiques,** visée à l'article 33, 2., du Règlement ETIAS, nécessitera à la base, du traitement de données à caractère personnel et in fine, aura un impact sur les traitements des données relatives aux personnes concernées par ETIAS.

[84] Article 9, 4., du Règlement ETIAS.

[85] Article 20, 5., du Règlement ETIAS.

[86] À propos de ces risques, voir le considérant n° 12, premier tiret (finalité de prévention des risques d'ETIAS). L'article 33 du Règlement ETIAS détermine ce que constituent les règles d'examen ETIAS et la manière dont elles doivent être établies. La Commission adoptera un acte délégué pour préciser les risques spécifiques concernés, sur la base notamment de statistiques et d'informations, attestées par des éléments factuels et concrets, fournies par les Etats membres. Sur la base des risques spécifiques, l'unité centrale ETIAS établira un ensemble d'indicateurs de risques spécifiques consistant en une combinaison des données visées à l'article 33, 4., du Règlement ETIAS.

50. La manière dont seront établis les indicateurs de risques est d'autant plus importante que comme le CEPD l'a souligné, malgré la disposition générale du Règlement ETIAS visant à lutter contre les discriminations notamment sur la base de certaines catégories particulières de données[87] et l'interdiction de fonder des indicateurs de risques spécifiques sur des catégories particulières de données[88] :

> « *Le CEPD souhaite souligner que, même si les indicateurs de risques ne seront pas directement définis sur la base des premiers critères susmentionnés, le résultat risque d'être très similaire à celui que l'on obtiendrait en utilisant ceux-ci. Sur la base d'informations telles que la nationalité et le lieu de résidence, surtout lorsqu'elles sont combinées à d'autres données, il est possible de se faire une idée relativement précise de la race ou de l'origine ethnique d'un demandeur. De même, les indicateurs de risques ne peuvent pas se fonder sur l'appartenance à un syndicat, mais pourraient être définis en fonction des informations relatives à la profession actuelle. Ces deux types d'informations sont très étroitement liés, raison pour laquelle un profilage sur cette base ne prévient pas réellement le risque de discrimination* »[89].

51. Sur ce point et dans un sens similaire, l'Autorité a déjà souligné que le traitement de la donnée nationale pouvait être considéré comme un traitement portant sur des catégories particulières de données visé à l'article 9 du RGPD[90].

52. L'Autorité a interrogé le demandeur quant aux règles encadrent ces traitements de données à caractère personnel. Celui-ci a répondu ce qui suit :

> « *Nous supposons que la question vise les informations que les Etats membres doivent fournir et qui sont visées à l'article 33,§2, points d), e) et f)*[91]*.*
>
> *Ces informations doivent être fournies par les autorités compétentes pour chaque type de risques soit :*
> *pour le point d) Fedpol, Douanes, Services de renseignements et de sécurité ;*

---

[87] Voir l'article 14 du Règlement ETIAS

[88] L'article 33, 5., du Règlement ETIAS dispose que :

« *Les indicateurs de risques spécifiques sont ciblés et proportionnés. Ils ne sont en aucun cas fondés uniquement sur le sexe ou l'âge d'une personne. Ils ne sont en aucun cas fondés sur des informations révélant la couleur, la race, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, les opinions politiques ou toute autre opinion, la religion ou les convictions philosophiques, l'appartenance à un syndicat, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap ou l'orientation sexuelle d'une personne* ».

[89] Avis CEPD ETIAS, considérant n° 40.

[90] Voir l'avis n° 211/2022 du 9 septembre 2022 *concernant un projet d'arrêté royal portant modification de l'arrêté royal du 22 février 2017 portant création du Service public fédéral Stratégie et Appui (CO-A-2022-187)*.

[91] Ce qui est exact.

pour le point e) Office des étrangers ;
pour le point f) SPF Santé publique.

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 « loi de 2018 ») et éventuellement d'autres règles spécifiques de protection des données qui s'appliquent aux autorités concernées encadrent les traitements de données qui leur permettront de fournir ces informations.

L'article 31 du Projet prévoit l'application de la loi de 2018 dans le cadre de l'évaluation des risques ».

53. L'Autorité attire l'attention du demandeur sur le fait que n'est pas ici visée l'évaluation des risques (dans le cadre des demandes concrètes d'autorisation) mais bien la contribution à l'identification des risques à prévenir via les règles d'examen ETIAS, qui implique d'autres traitements de données qui doivent également être encadrés par le Projet. **Le dispositif de ce dernier doit ainsi déterminer les éléments essentiels de ces traitements de données, en particulier les (catégories de) données traitées ainsi que les autorités publiques responsables de ces traitements de données**.

Traitements automatisés article 23 (SIS particulier)

54. **Comparaison avec SIS pour une partie des signalements**[92] – Le système central ETIAS lance une recherche via l'ESP pour effectuer une comparaison avec certaines données de signalement figurant dans le SIS.

Absence de réponse positive

55. Au terme de ces traitements automatisés, **en l'absence de réponse positive**, l'autorisation de voyage est automatiquement délivrée[93].

II.2.3. <u>Réponse(s) positive(s) et traitement manuel</u>

[92] Personnes disparues, personnes recherchées pour concours à une procédure judiciaire ou signalement aux fins de contrôles discrets (etc.).

[93] Article 21, 1., du Règlement ETIAS.

56. S'il y a **une ou plusieurs réponses positives** aux traitements automatisés article 20 (général)[94, 95], l'unité centrale ETIAS procède à des **vérifications**[96]. En cas de faux positif, l'autorisation de voyage est délivrée automatiquement.

57. Si les vérifications sont positives ou s'il subsiste un doute quant à l'identité du demandeur, **la demande est alors traitée *manuellement* conformément à l'article 26 du Règlement ETIAS, par l'unité *nationale* ETIAS responsable**[97]. Il s'agit par exemple de l'Etat membre qui seul, a introduit ou fourni les données qui ont déclenché une réponse positive. Dans cette hypothèse, les unités nationales ETIAS ont également accès aux données d'autres systèmes d'informations de l'UE visées à l'article 25*bis* du Règlement ETIAS, et dans certaines circonstances, des informations ou documents supplémentaires peuvent être demandés au demandeur et, dans des conditions plus limitées encore, un entretien peut être organisé[98]. Enfin, notamment si plusieurs Etats membres ont communiqué des données ayant déclenché une réponse positive, un processus de consultation entre eux et l'unité nationale ETIAS de l'Etat membre responsable est organisée[99].

Evaluation des risques

58. Le traitement manuel réalisé par l'unité nationale ETIAS responsable[100] mène à une décision de refus ou d'autorisation de voyage prise par celle-ci, dans la plupart des cas[101] au terme d'une **évaluation de risques**[102] qu'elle a réalisé, voire encore, en cas de refus, lorsqu'une unité nationale ETIAS d'un

---

[94] Article 21, 2., et 22 du Règlement ETIAS.

[95] S'il y a une ou plusieurs réponses positives aux traitements automatisés **article 23 (SIS particulier)**, l'unité centrale ETIAS procède également à des vérifications et si la correspondance est confirmée, une notification est envoyée au bureau **SIRENE** (« *Supplementary Information Request at the National Entries* ») de l'Etat membre qui a introduit le signalement. Une telle notification est également envoyée si un traitement manuel a été enclenché à la suite des **traitements automatisés article 20 (général)**.

En ce qui concerne le bureau SIRENE, voir l'article 7 du Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 *sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) no 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission*. En Belgique il s'agit de « Commission SIRENE, Police Fédérale — Direction de la coopération policière internationale (CGI) », voir Document C2023/085/02, Liste des offices N.SIS et des bureaux SIRENE nationaux, *J.O.*, C, 85 du 7.3.2023, pp. 299-308, accessible à partir de https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/sirene-cooperation_fr,

dernièrement consulté le 28/06/2023, et l'article 5 de la loi du 2 mars 2023 *relative au fonctionnement et à l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, dans le domaine des vérifications aux frontières et aux fins du retour des ressortissants de pays tiers en séjour irrégulier*.

[96] Prévues à l'article 22 du Règlement ETIAS.

[97] L'article 25 du Règlement ETIAS identifie l'Etat membre responsable, selon les hypothèses.

Le commentaire des articles du Projet (p. 11), indique que « *toute donnée introduite dans une base de données européenne trouve son origine dans une base de données 'source', qui est en réalité une base de données nationale* ».

[98] Voir l'article 27 du Règlement ETIAS.

[99] Voir l'article 28 du Règlement ETIAS. Un processus similaire existe lorsque les données concernées proviennent d'Europol, voir l'article 29 du Règlement ETIAS.

[100] Article 26 du Règlement ETIAS.

[101] Pour les hypothèses où un refus doit être délivré sans évaluation de risque, voir l'article 26, 3., a), 3*bis*, a),

[102] Voir l'article 26, 3., b), 3*bis*, b), 4., 5. et 6., du Règlement ETIAS.

Etat membre consulté a rendu un avis négatif motivé (c'est alors cet autre Etat Membre qui a évalué les risques)[103]. La **décision** sur la demande doit être rendue dans un délai de principe particulièrement réduit : **96 heures** à compter de la recevabilité de la demande[104].

59. Selon le Projet, au sein de l'U.N.E. belge, un avis motivé sur l'évaluation des risques en matière de **SÉCURITÉ** et de **RISQUE ÉPIDÉMIQUE ÉLEVÉ** est réalisé par les « ***membres détachés*** »[105] des services concernés (services de police, le SPF Santé Publique, la VSSE, le SGRS et l'AGD&A)[106] relevant de la **Section du CCN**[107], qui a cette fin, ont « *accès aux bases de données nécessaires gérés par leurs services d'origine respectifs* » (souligné par l'Autorité)[108], et relèvent dans ce contexte, de l'autorité du fonctionnaire dirigeant[109]. Ce qui soulève les deux commentaires suivants.

60. Premièrement, l'Autorité a interrogé le demandeur afin que celui-ci confirme que les **évaluations des risques** réalisées par les membres détachés de la Section CCN sont bien réalisées par ceux-ci **sous l'autorité du fonctionnaire dirigeant** (s'agissant de l'exécution des missions de l'U.N.E.). Le demandeur l'a confirmé.

61. Deuxièmement, l'Autorité est d'avis qu'en se limitant à viser « *les bases de données nécessaires* », le Projet **ne répond pas aux principes de prévisibilité et de légalité** consacrés dans les articles 8 CEDH et 22 de la Constitution : il ne permet pas d'identifier les (catégories de) données qui originellement traitées par ces services, seront ultérieurement traitées aux finalités poursuivies par le Règlement ETIAS. Le dispositif du Projet **doit identifier les bases de données qui *doivent* être consultées en se référant à leur fondement légal et en précisant quelles (catégories de) données à caractère personnel issues de ces banques de données peuvent être réutilisées aux fins du Règlement ETIAS**. Cette adaptation permettra également **d'identifier dans le cadre de quelles missions de ces autres autorités, les données collectées (et quelles données) peuvent être réutilisées aux fins d'ETIAS**. A défaut de précision en la matière, il est également impossible pour l'Autorité de contrôler l'application de l'article 6, 4., du RGPD et de l'article 4, 1. et 2., de la Directive 2016/680.

---

[103] Voir l'article 28 du Règlement ETIAS.

[104] Voir l'article 32 du Règlement ETIAS.

[105] Définis à l'article 6, 2°, du Projet.

[106] De ces autorités, le SPF Santé Publique (soumis au RGPD) et l'AGD&A (bien que soumise au titre 2 de la LTD dans certaines conditions – voir notamment, le *Protocole de coopération entre les autorités de contrôle fédérales belges en matière de protection des données, Convention entre l'Autorité de Protection des données, l'Organe de Contrôle de l'Information Policière, le Comité Permanent de contrôle des services de renseignement et le Comité Permanent de contrôle des services de police*, 24 novembre 2020, p. 10, disponible sur https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-les-autorites-de-controle-federales-belges-en-matiere-de-protection-des-donnees.pdf, dernièrement consulté le 05/07/2023) **relèvent de la compétence de contrôle de l'Autorité de Protection des Données**.

[107] Article 11, § 1er, du Projet.

[108] Article 12, § 1er, du Projet. Le paragraphe 2 de cette disposition prévoit également un accès au casier judiciaire central en cas de réponse positive en lien avec ECRIS-TCN.

[109] Article 8, § 2, du Projet.

62. Il se dégage de la logique du Projet que la **Section OE** est compétente pour évaluer et se prononcer en cas de risque **d'IMMIGRATION ILLÉGALE**[110]. L'article 27 du Projet ne l'exprime toutefois pas directement et devrait être formulé plus clairement, à la manière des dispositions applicables à la Section du CCN.

63. Dans ce contexte en outre, le Projet n'identifie pas **sur la base de quelles informations ((catégories de) données) et systèmes d'information belges** la Section OE va réaliser son analyse. L'Autorité a interrogé le demandeur à ce sujet et celui-ci a répondu ce qui suit :

> « *L'OE n'a pas jugé utile de prévoir cela pour leur section. Nous savons qu'ils utiliseront au moins leur base de données Evibel* »[111].

64. La position développée au considérant n° 61 vaut en l'occurrence également : le dispositif du Projet doit identifier les **banques de données (et leur fondement légal) et (catégories de) données qui *doivent* être réutilisées aux fins du Règlement** ETIAS par l'O.E. A défaut de précision en la matière, il est également de nouveau impossible pour l'Autorité de contrôler l'application de l'article 6, 4., du RGPD[112].

Décision de l'U.N.E.

65. S'il n'existe aucun indice concret ni aucun motif raisonnable fondé sur des indices concrets permettant de conclure que la présence de la personne sur le territoire des Etats membres présente un risque en matière de sécurité ou d'immigration illégale ou un risque épidémique élevé, **une autorisation de voyage (valable 3 ans) est délivrée**[113].

66. En **cas de doute**, l'unité nationale ETIAS a la possibilité de délivrer l'autorisation moyennant la mise en œuvre d'une **vérification de deuxième ligne**[114]. L'Autorité a interrogé le demandeur quant aux circonstances (les règles) dans lesquelles cette vérification de deuxième ligne peut être exigée. Celui-

---

[110] Voir l'article 27 du Projet.

[111] « Evibel » apparaît être la base de données de l'OE dans laquelle se trouve les données relatives à l'asile, la migration et aux procédures de retour, voir European Migration Network Belgium, « *Accurate, timely, interoperable : data management in the asylum procedure* », disponible sur https://emnbelgium.be/sites/default/files/publications/Standalone%20FINAL_1.pdf, dernièrement consulté le 06/07/2023, p. 15.

[112] Ou de l'article 4, 1. et 2., de la Directive 2016/680, voir le considérant n° 87.

[113] Article 36, 1., du Règlement ETIAS.

[114] Article 36, 2., du Règlement ETIAS. Cette vérification est définie comme (article 3, 1., 3., du Règlement ETIAS) « *une vérification de deuxième ligne au sens de l'article 2, point 13), du règlement (UE) 2016/399* », soit « *une vérification supplémentaire pouvant être effectuée en un lieu spécial à l'écart de celui où toutes les personnes sont soumises à des vérifications (première ligne)* », s'agissant de vérifications aux frontières. Une telle mention peut aussi être demandée par un Etat membre consulté. Conformément à l'article 36, 3., du Règlement ETIAS, une mention peut aussi être insérée dans le système selon laquelle une réponse positive spécifique a été déclenchée pendant le traitement de la demande.

ci a notamment rappelé que cette possibilité était encadrée par un acte délégué de la Commission européenne (non encore publié toutefois mais accessible en ligne[115]).

67. C'est « ***la section*** » compétente de l'U.N.E., qui « *prend ses décisions* »[116], étant entendu que le « *fonctionnaire dirigeant* » de la Section est responsable « *de la bonne exécution des missions de l'U.N.E. qui incombent à sa section* »[117]. Si des réponses positives pour une même demande, doivent être évaluées par les deux Sections, la Section du CCN prend la décision et doit suivre l'avis négatif de la Section OE[118]. L'Autorité a interrogé le demandeur afin que celui-ci confirme cette analyse (décision prise par le fonctionnaire dirigeant) et le demandeur a répondu ce qui suit :

> « *Oui. Un arrêté royal d'exécution est prévu qui précise que le fonctionnaire dirigeant désigne les membres de sa section habilités à prendre les décisions. Ce ne seront pas les détachés des services compétents qui eux évaluent les risques mais des collaborateurs opérationnels (attachés NCCN)* » (souligné par l'Autorité)[119].

68. L'Autorité prend acte de cette explication mais **est d'avis que le dispositif du Projet lui-même doit spécifier que le fonctionnaire dirigeant prend les décisions, dès lors que cela a un impact direct** (notamment) **sur la détermination des rôles et responsabilités au regard du traitement de données à caractère personnel** et des éventuelles incompatibilités dans l'exercice des fonctions concernées[120].

69. L'article 37 du Règlement ETIAS liste les hypothèses où sont **refusées** les autorisations de voyage. Les décisions prises par les Section de l'U.N.E. doivent être **motivées**[121].

70. **Exceptionnellement**, lorsque le traitement manuel n'est pas encore achevé ou lorsqu'une autorisation de voyage a été refusée, annulée ou révoquée, l'Etat membre de destination du

---

[115] Voir la note de bas de page n° 15, huitième référence.

[116] Articles 11, § 3, et 29 du Projet.

[117] Article 7, 1°, du Projet, et article 26, § 2, du Projet.

[118] Article 29 du Projet.

[119] En outre, le commentaire des articles du Projet (p. 11), précise, au sujet du processus d'évaluation de risque que ce « *processus implique que ce ne sont pas les membres détachés qui prennent la décision finale mais les collaborateurs opérationnels habilités par le fonctionnaire dirigeant* ».

[120] Voir les considérants nos 102.

[121] Voir les articles 28, 3., et 39, 4., du Règlement ETIAS. De manière générale, les motifs de la décision sont en principe toujours renseignés dans le dossier de demande. En vertu de l'article 26, 7., du Règlement ETIAS : « *Les résultats de l'évaluation du risque en matière de sécurité ou d'immigration illégale ou du risque épidémique élevé et les motifs sous-tendant la décision de délivrer ou de refuser une autorisation de voyage sont enregistrés dans le dossier de demande par l'agent ayant réalisé l'évaluation des risques* ». Voir également l'article 39, 3., d), et les articles 40, 4. (annulation), 41, 6. (révocation) et 43 (décision d'annuler ou révoquer), 2., du Règlement ETIAS.

Voir également les annexes de la Décision d'exécution (UE) 2022/102 de la Commission du 25 janvier 2022 *établissant des formulaires de refus, d'annulation ou de révocation d'une autorisation de voyage*, prévoyant des formulaires de notification de décisions reprenant, outre l'identification du motif de la décision (disposition concernée du Règlement ETIAS), un cadre intitulé « *Exposé des faits pertinents et motivation supplémentaire sous-jacente à la décision* ».

demandeur peut délivrer une autorisation de voyage à **validité territoriale limitée** pour des motifs humanitaires, pour des raisons d'intérêt national ou en vertu d'obligations internationales, conformément à l'article 44 du Règlement ETIAS.

Procédure de recours

71. Un **recours** est ouvert au demandeur contre un refus d'autorisation de voyage, processus organisé en droit belge dans le cadre du **Projet modificatif**[122]. Ce dernier précise que les décisions prises par l'U.N.E. sont susceptibles de **recours *en annulation* devant le Conseil du contentieux des étrangers, visé à l'article 39/1 de la loi du 15 décembre 1980**[123]. Le recours en annulation est consacré aux articles 39/78 et s., de la loi du 15 décembre 1980 *sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers* (ci-après, « **la loi de 1980** »). L'article 39/2 de la loi de 1980 établit une distinction entre le recours de pleine juridiction introduit contre les décisions du Commissaire général aux réfugiés et aux apatrides et le recours en annulation, pour violation des formes soit substantielles, soit prescrites à peine de nullité, excès ou détournement de pouvoir[124]. **L'exposé des motifs n'explique pas ce choix d'un recours en annulation plutôt qu'un recours en pleine juridiction**.

72. **Or l'Autorité est d'avis qu'*a priori*, un recours en pleine juridiction est de nature à mieux garantir les droits et libertés des personnes concernées**. Par conséquent, l'exposé des motifs doit motiver la raison pour laquelle il est recouru à un recours en annulation plutôt qu'un recours en pleine juridiction.

---

[122] Article 37, 3., du Règlement ETIAS.

[123] Voir également le considérant n° 78, concernant le recours à l'égard d'une décision prise par l'U.N.E. sur une demande de rectification ou de suppression des données.

[124] Selon cette disposition :

« *§ 1er. Le Conseil statue, par voie d'arrêts, sur les recours introduits à l'encontre des décisions du Commissaire général aux réfugiés et aux apatrides.*

Le Conseil peut :

1° confirmer ou réformer la décision attaquée du Commissaire général aux réfugiés et aux apatrides;

2° annuler la décision attaquée du Commissaire général aux réfugiés et aux apatrides soit pour la raison que la décision attaquée est entachée d'une irrégularité substantielle qui ne saurait être réparée par le Conseil, soit parce qu'il manque des éléments essentiels qui impliquent que le Conseil ne peut conclure à la confirmation ou à la réformation visée au 1° sans qu'il soit procédé à des mesures d'instruction complémentaires;

3° sans préjudice du 1° ou du 2°, annuler la décision attaquée du Commissaire général aux réfugiés et aux apatrides d'irrecevabilité de la demande de protection internationale visée à l'article 57/6 § 3, pour le motif qu'il existe des indications sérieuses que le requérant peut prétendre à la reconnaissance de la qualité de réfugié au sens de l'article 48/3 ou à l'octroi de la protection subsidiaire au sens de l'article 48/4.

§ 2. Le Conseil statue en annulation, par voie d'arrêts, sur les autres recours pour violation des formes soit substantielles, soit prescrites à peine de nullité, excès ou détournement de pouvoir ».

Pour ce qui concerne les dispositions spécifiques applicables aux recours de pleine juridiction contre les décisions du Commissaire précité, voir les articles 39/69 et s. de la loi de 1980. Les articles 39/78 et s. concernent le recours en annulation.

73. En outre, il découle du dispositif ETIAS[125] que lorsque l'U.N.E. d'un Etat membre refuse une autorisation de voyage en raison d'un **avis négatif émis par l'autorité d'un autre Etat membre** émis à l'occasion d'une consultation par la première U.N.E.[126], la personne concernée dispose d'un recours contre l'avis négatif rendu par l'U.N.E. de cet autre Etat Membre, conformément au droit de cet autre Etat Membre. Or le Projet modificatif se réfère de manière générale aux « *décisions* » de l'U.N.E., tandis que le Règlement ETIAS se réfère à refuser/délivrer (*décision* sur la demande) et rendre un avis dans le cadre des consultations entre Etats Membres. **L'Autorité est d'avis que le Projet modificatif doit clarifier que *l'avis* négatif émis par une Section de l'U.N.E. dans le cadre des consultations visées à l'article 28 du Règlement ETIAS constitue une décision susceptible de recours**.

74. Pendant la procédure de recours, « *le requérant a **accès aux informations** figurant dans le dossier de demande **conformément aux règles en matière de protection des données** visées à l'article 56 du présent règlement* » (gras ajouté par l'Autorité)[127]. Dans ce contexte, l'Autorité a invité le demandeur à confirmer que les **évaluations des risques** réalisées par les membres détachés de la Section CCN seront bien communiquées à la Section CCN (au fonctionnaire dirigeant) afin que celle-ci prenne sa décision (plus que le simple *résultat* de l'évaluation), de telle sorte que la personne concernée disposera d'un droit d'accès à l'égard de cette évaluation (ce document), en vertu des règles de protection des données. Le demandeur a répondu dans un deuxième temps[128] ce qui suit :

> « *Je vous confirme que la personne concernée pourra bien avoir accès au raisonnement justifiant le résultat de l'évaluation, lequel servira également à motiver la décision qui sera prise par l'UNE et qui lui sera notifiée. Cela ressort, selon nous, de l'article 26, §7, al 2 du Règlement (qui vise le résultat de l'évaluation et les motifs sous-tendant la décision) ainsi que de l'article 11,§1 du Projet (qui mentionne un 'avis motivé').*

[125] Voir le formulaire repris à l'annexe I de la **décision d'exécution 2022/102**.

Dans cette logique, ne sont pas accessibles à la personne concernée, dans le dossier de demande, l'avis émis par un Etat membre consulté (voir l'article 28, 3., al. 3, du Règlement ETIAS) ainsi que le motif y lié de la décision (article 39, 4., du Règlement ETIAS), ou notamment la mention relative à un contrôle de deuxième ligne (lorsqu'elle est demandée par un Etat membre consulté ; voir l'article 36, 2., al. 2, du Règlement ETIAS ; à noter que cette mention est effacée automatiquement une fois que les autorités frontalières ont procédé à la vérification) (article 36, 2., al. 3, du Règlement ETIAS).

[126] Voir l'article 28 du Règlement ETIAS qui régit les hypothèses de consultations d'autres Etats Membres.

[127] Article 37, 3., du Règlement ETIAS.

[128] Pour être complet, avant d'être réinterrogé sur le sujet, le demandeur avait répondu ce qui suit à l'Autorité :

« *Nous confirmons que les résultats de l'évaluation du risque seront enregistrés dans le dossier du demandeur mais pas sous la forme d'un « document », en vertu de l'art 26, §7, al 2, du Règlement. Pour y accéder, il faudra consulter le software ETIAS. Cet avis motivé servira de base à la décision. En cas de recours, il devrait être disponible dans le dossier administratif (nous ne pouvons le garantir à ce stade car nous ne sommes pas responsables du software ETIAS mais nous avons fait cette demande en vue d'assurer le contrôle de légalité des décisions ETIAS). La personne concernée pourra également y avoir accès, comme prévu par l'article 64 du Règlement* ».

Pour être exhaustive, je vous signale qu'il se peut que cet accès soit limité si l'évaluation du risque en cause relève de la Directive 2016/680, soit des titres 2 ou 3 de la loi de 2018[129] *- nouveau sous-titre 5bis inséré par l'article 41 du Projet* ».

75. L'Autorité prend acte de cette explication. **Elle est toutefois d'avis qu'en tout état de cause, la personne concernée doit pouvoir disposer de l'évaluation de risques produite et communiquée au fonctionnaire dirigeant (ou à ses collaborateurs opérationnels[130]) en vue de prendre sa décision**. Ce qui n'exclut pas que les traitements de données (et les données traitées dans ce contexte) réalisés afin de rédiger l'évaluation par les autorités compétentes soumises à la Directive 2016/680 puissent eux-mêmes être soumis à des règles limitatives des droits de la personne concernée en exécution de la Directive 2016/680. La Section (le fonctionnaire dirigeant) qui prend une décision dans le cadre d'ETIAS est soumise au RGPD et **l'évaluation de risques** au-delà de son simple résultat (à savoir, présente ou pas un risque spécifique) **constitue l'élément déterminant qui motive sa prise de décision et est nécessaire à la personne concernée tant pour vérifier que les données à caractère personnel traitées à son sujet le sont licitement**, **qu'en vue de l'éventuel exercice de son droit de recours** contre la décision de l'U.N.E. En l'état du Projet, l'Autorité est d'avis que c'est aux membres détachés qu'incombe la responsabilité d'être attentifs dans la production de leur analyse de risques : l'interaction directe de leur activité d'analyse avec les droits et libertés des personnes concernées nécessite que la personne concernée puisse accéder à cette analyse[131]. Cela étant précisé, corrélativement, dans le cadre d'un **contrôle interne**, lorsque cela est nécessaire pour **vérifier l'exactitude d'une donnée à caractère personnel de l'analyse** qui lui est communiquée (par exemple, une imputation à l'égard de la personne concernée), le Projet devrait également permettre au fonctionnaire dirigeant (responsable de la décision à prendre et autorité hiérarchique des membres détachés) de consulter la donnée à caractère personnel de base, dans la base de donnée concernée, *conformément aux règles (y compris de protection des données) régissant cette base de données*. Remarque : cette possibilité ne peut être détournée en vue de vider les analyses de risques de leur substance, en particulier au motif qu'elles seraient accessibles aux personnes concernées.

76. Toujours à propos de l'évaluation des risques dont il vient d'être question, l'Autorité relève que le Projet doit également établir clairement que celle-ci, émanant des membres détachés mais réalisée sous l'autorité du fonctionnaire dirigeant de la Section, **n'est pas soumise aux exceptions générales aux droits des personnes concernées consacrées dans les articles 11 et 14 de la LTD**

[129] Sur l'accès indirect via les autorités de contrôles, voir les conclusions de l'Avocate générale L. Medina présentées le 15 juin 2023 dans l'Aff. C-333/22, *Ligue des droits humains ASBL, BA c/ L'organe de contrôle de l'information policière*.

[130] Voir la note de bas de page n° 119.

[131] Et ce d'autant plus que le Règlement ETIAS lie le droit d'accès au dossier dans le cadre d'un recours à l'accès aux données sous l'angle de la protection des données. En tout état de cause, l'Autorité ne percevrait pas pour quelle raison l'analyse pourrait être consultée dans le cadre d'un recours mais pas dans le cadre d'un accès sur le plan de la protection des données.

(inapplicabilité de droits à l'égard de données reçues notamment des services de police et des services de renseignements et de sécurité).

77. Enfin, dans le contexte de **l'exercice de ses droits par le demandeur**, le Règlement ETIAS prévoit que l'unité nationale ETIAS (ou l'unité centrale ETIAS) qui ne partage pas la position du demandeur quant à la rectification ou suppression de ses données « *adopte sans retard une décision administrative expliquant par écrit à la personne concernée pourquoi elle n'est pas disposée à rectifier ou à effacer les données la concernant* », décision devant indiquer la voie de recours disponible[132].

78. Il est par conséquent question d'une **hypothèse additionnelle de « *décision* » de l'U.N.E.** qui, en l'état du Projet modificatif, pourra faire l'objet d'un recours devant le Conseil du contentieux des étrangers. L'article 55, 8., du Règlement ETIAS prévoit d'ailleurs que sans « *préjudice de tout recours administratif ou extrajudiciaire à leur disposition, les personnes concernées* ***disposent d'un droit de recours juridictionnel effectif pour garantir que les données conservées dans ETIAS sont modifiées ou effacées*** » (gras ajouté par l'Autorité). Ceci est sans préjudice de la possibilité qui est offerte à la personne concernée, conformément aux règles de protection des données, d'introduire une plainte auprès de l'autorité de contrôle compétente. **L'Autorité est d'avis dans ce contexte, qu'afin de garantir au mieux l'effectivité des règles de protection des données, c'est un recours *de pleine juridiction* qui doit être mis en place,** de manière telle que le Conseil du contentieux des étrangers (une juridiction administrative) puisse substituer son analyse à celle de l'U.N.E.

Possibilités d'annulation ou de révocation

79. Lorsqu'un Etat membre est en mesure de prouver que les conditions de délivrance d'une autorisation de voyage n'étaient pas remplies au moment de la délivrance ou ne le sont plus, l'unité nationale concernée *doit* respectivement annuler (annulation) ou révoquer (révocation) l'autorisation de voyage[133].

80. Outre **l'interaction automatique avec le SIS ainsi que l'interaction avec la liste de surveillance ETIAS** (traitements automatisés additionnels) qui sont directement encadrées par le Règlement ETIAS[134], l'Autorité a interrogé le demandeur quant aux **circonstances** dans lesquelles (et aux règles selon lesquelles) l'U.N.E. serait susceptible de devoir se prononcer au sujet d'une annulation ou d'une révocation. Le demandeur a répondu ce qui suit :

[132] Article 64, 3. et 4., du Règlement ETIAS.

[133] Voir les articles 40 et 41 du Règlement ETIAS.

[134] Visées à l'article visée l'article 41, 3. et 4. du Règlement ETIAS.

> « *Nous considérons que toute autorité belge impliquée directement ou indirectement dans le processus d'examen des demandes pourrait avoir connaissance d'une nouvelle information ou d'une information qui n'aurait pas été prise en compte au moment de la prise de décision, qui serait de nature à entraîner une annulation ou une révocation de l'autorisation de voyage. Il semble aller de soi que cette information doit être communiquée à l'UNE. Les dispositions exigent des preuves, ce qui suppose des éléments tangibles et vérifiables. Ceux-ci doivent être mis en parallèle avec les motifs pouvant être utilisés pour annuler ou révoquer l'autorisation de voyage (art 37, §1 et 2 du Règlement).*
>
> *Nous avons renoncé à introduire une disposition à ce sujet dans le Projet car nous ne sommes pas parvenus à la formuler de manière à lui donner une valeur ajoutée par rapport aux dispositions du Règlement* » (souligner par l'Autorité).

81. D'une manière ou d'une autre, cette approche implique par conséquent un suivi (avec quelle périodicité ?)[135] des personnes concernées auxquelles une autorisation de voyage a été délivrée, et **une responsabilité/une obligation** (également au regard du traitement de données[136]) des autorités qui sont impliquées dans le processus d'examen des demandes. Celles-ci ont l'obligation de communiquer à l'U.N.E., potentiellement *même en dehors d'un processus d'évaluation d'une demande d'autorisation*[137] (si telle est bien l'intention du demandeur), les informations pertinentes dont elles prendraient connaissance à l'occasion de l'exercice de leurs missions (à identifier). **L'Autorité est d'avis qu'une telle obligation, mettant en place un traitement de données à caractère personnel, doit être organisée par le dispositif du Projet** devant fixer les éléments essentiels des traitements de données envisagés.

II.2.4. Mise à jour et exactitude des données

82. **Obligation de mise à jour et de veiller à l'exactitude des données**. L'unité centrale ETIAS et les unités nationales ont l'obligation de mettre à jour les données et de veiller à leur exactitude[138]. Dans ce contexte, l'Autorité a interrogé le demandeur quant aux mesures d'exécution prises en exécution de l'article 55, 1., du Règlement ETIAS afin d'assurer que les données sont mises à jour.

---

[135] L'autorité concernée doit pouvoir lier, dans l'exercice de ses missions et selon le suivi escompté, les données dont elle dispose au sujet du personne concernée au fait que celle-ci est ou pas titulaire d'une autorisation de voyage couverte par le Règlement ETIAS.

[136] Voir les considérants nos 102 et s.

[137] Ainsi, la mise à jour pourrait n'être effectuée que lorsqu'à l'occasion d'une demande d'autorisation, sont identifiées des données également pertinentes pour une autre demande d'autorisation. Pour une hypothèse de ce type, dans un autre contexte de *screening*, voir l'Avis de l'Autorité n° 245/2022 du 21 octobre 2022 *concernant un avant-projet de loi relative à l'approche administrative communale, à la mise en place d'une enquête d'intégrité communale et portant création d'une Direction chargée de l'Evaluation de l'Intégrité pour les Pouvoirs publics (CO-A-2022-248)*, considérants nos 51 et s. et considérant n° 56 en particulier.

[138] Voir l'article 55, 1. à 4., du Règlement ETIAS.

Etant entendu que pour ce qui concerne la liste de surveillance ETIAS, l'article 35 du Règlement ETIAS consacre lui-même une obligation périodique. Le demandeur a répondu ce qui suit :

> « *L'art 55,§1 vise uniquement les données que l'UCE ou l'UNE ont elles-mêmes enregistrées sur la base des dispositions du Règlement (ex : art 39 qui prévoit les données à ajouter après la prise de décision – ces données devront être modifiées en cas d'annulation ou de révocation subséquente en vertu des art 40 et 41). Nous considérons que l'obligation de mise à jour est explicitée dans les autres § de l'article 55. Il faut en effet un déclencheur qui peut provenir d'une demande d'accès aux données personnelles, de la communication d'une nouvelle information par une autorité impliquée,..* ».

83. L'Autorité prend acte de cette explication qui est à lier aux développements concernant l'annulation et la révocation des autorisations[139].

II.3. UTILISATION D'ETIAS À DES FINS RÉPRESSIVES

84. Comme évoqué précédemment, ETIAS peut être consulté par les autorités désignées par les Etats membres à des fins répressives.

II.3.1. Autorités concernées

85. Dans ce cadre, les Etats membres doivent désigner les **autorités habilitées (les autorités désignées)** à demander la consultation des données d'ETIAS[140], et lister les **unités opérationnelles** qui seules[141], au sein de ces autorités[142], sont autorisées à demander la consultation d'ETIAS. Ils doivent encore désigner un **point d'accès central** qui a accès au système ETIAS et qui vérifie que les conditions d'accès à ETIAS établies à l'article 52 sont remplies[143]. Le Règlement ETIAS prévoit en outre l'indépendance du point d'accès central par rapport aux autorités désignées[144]. L'article 52 du Règlement ETIAS détermine les conditions cumulatives dans lesquelles les données peuvent être consultées[145].

---

[139] Voir les considérants nos 79-81.

[140] Article 50, 1., du Règlement ETIAS

[141] C'est en effet l'unité opérationnelle qui doit présenter la demande motivée de consultation d'ETIAS, voir l'article 51 du Règlement ETIAS.

[142] Article 50, 3., du Règlement ETIAS.

[143] Article 50, 2., du Règlement ETIAS.

[144] Voir l'article 50, 2., als 2 et 3, du Règlement ETIAS.

[145] L'article 52, 1*bis*, vise également l'hypothèse où l'autorité désignée est informée de l'existence de données dans ETIAS via une consultation du **CIR** visée à l'article 22 du Règlement **interopérabilité**. Voir la note de bas de page n° 65.

86. Les articles 14 à 20 du Projet exécutent le Règlement ETIAS en la matière. Ils identifient *a priori* comme **autorités habilités (désignées)** : les services de police, la VSSE, le SGRS, l'AGD&A et l'Office des Etrangers (ci-après, « **OE** »).

87. L'Autorité relève au passage que l'article 41 du Projet fait désormais de **l'OE une autorité compétente** au sens du titre 2 de la LTD, en modifiant l'article 26, 7°, de la LTD, lorsque celui-ci exerce ses compétences répressives en vertu de l'article 81 de la loi du 15 décembre 1980[146]. Cette modification a une **portée qui dépasse les objectifs du Projet**. L'exposé des motifs du Projet se borne à préciser que cette intégration a lieu « *compte tenu des compétences répressives* » de l'OE[147].

88. L'Autorité **prend acte de cette modification** et du fait que l'Autorité de Protection des Données reste l'autorité de contrôle de l'OE.

89. L'Autorité a interrogé le demandeur quant aux **unités opérationnelles** au sens du Règlement ETIAS, qui seront désignées (le seront-elles ultérieurement et par qui ?). Le demandeur a répondu ce qui suit :

> « *Chaque service devra en effet désigner les unités opérationnelles autorisées à faire une demande de consultation et en communiquer la liste à l'UNE. Les services de renseignements et de sécurité ainsi que l'Administration des douanes et accises ont souhaité ajouter un processus de validation interne de ces demandes par un responsable hiérarchique (art 15, al 1, du Projet)* » (souligné par l'Autorité).

90. L'Autorité ne retrouve cependant *a priori* pas dans le dispositif du Projet le principe selon lequel les autorités désignées doivent identifier les unités opérationnelles au sens du Règlement ETIAS. En tout état de cause, dès lors que la désignation de ces unités a un impact direct sur les rôles et responsabilités en matière de traitement de données à caractère personnel, l'Autorité est d'avis que c'est **une norme qui doit les identifier,** et que ce pouvoir (de désignation) ne peut être laissé à l'appréciation des services concernés. En l'occurrence, **le dispositif du Projet peut prévoir que le**

---

[146] Selon cette disposition :

« *Les infractions à la présente loi (et aux articles 433quinquies à 433octies et 433decies à 433duodecies du Code pénal) sont recherchées et constatées par tous les officiers de police judiciaire, en ce compris ceux dont la compétence est limitée, (par les fonctionnaires de la police fédérale et de la police locale), par les (agents de l'Office des étrangers) et de l'Administration des douanes et accises, par les inspecteurs du Ministère de l'Emploi et du Travail et du Ministère des Classes moyennes ainsi que par ceux de l'Office national de la sécurité sociale.*

Ils rassemblent les preuves des infractions et en livrent les auteurs aux autorités judiciaires, conformément aux dispositions du Code d'instruction criminelle.

Ils communiquent au ministre ou à son délégué tous documents et informations utiles à l'exercice de ses missions.

Les documents ou informations visés à l'alinéa précédent peuvent également être communiqués par les inspecteurs du Ministère flamand du Travail et de l'Economie sociale, par les inspecteurs de la Direction générale opérationnelle Economie, Emploi et Recherche du Service public de Wallonie, par les inspecteurs de la Direction de l'Inspection régionale de l'emploi de la Région Bruxelles-Capitale, par les inspecteurs du Ministère de la Communauté germanophone, département emploi ».

[147] P. 20.

Roi détermine au sein des services précités, quelles sont les unités opérationnelles au sens du Règlement ETIAS.

II.3.2. Finalité et extension aux services de renseignements et de sécurité

91. Avant tout, l'Autorité est d'avis que l'article 31, §§ 2 et 3, du Projet (déterminant les règles de protection des données applicables), doit être précisé afin de bien confirmer que « *la consultation du système d'information ETIAS* » dont il est question est la **consultation du système d'information ETIAS aux fins répressives** au sens du Règlement ETIAS, à savoir les consultations visées à la section 4, du Chapitre 3, du Projet, sans préjudice du commentaire émis ci-après.

92. Ensuite concernant les fins répressives, le commentaire des articles[148] explique que les infractions concernées en droit belge ne sont pas directement listées (il est simplement renvoyé aux textes européens, comme y procède ETIAS) pour les raisons suivantes :

> « […] *il est renvoyé à leur traduction en droit national pour justifier la consultation des données. Il n'est en effet pas souhaitable de dresser une liste exhaustive de ces infractions dans la loi même d'une part en raison de l'évolution constante du Code pénal et des autres réglementations pertinentes et, d'autre part, en raison du fait que le seuil de gravité des infractions pénales établi par le règlement ne suffit pas à lui seul pour écarter les infractions de criminalité 'ordinaire' (voir à cet égard le point 151*[149] *de l'arrêt de la CJUE du 21 juin 2022 relatif à l'affaire 'Ligue des droits humains' C-817/19* » (souligné par l'Autorité).

93. **L'Autorité est d'avis que cette motivation n'est pas complètement convaincante** et ce, pour les deux raisons suivantes. Premièrement, l'évolution du droit pénal n'empêche pas le législateur dans d'autres domaines, de légiférer sur la base de listes d'infractions de droit pénal belge concernées, afin de définir la criminalité grave, et ce, en se référant aux fondements légaux de ces infractions[150]. Les incriminations visées par le Règlement ETIAS sont pour le reste déjà très variées (infractions terroristes, participation à une organisation criminelle, traite des êtres humains, trafic illicite de stupéfiants et de substances psychotropes, corruption, cybercriminalité, faux monnayage, escroquerie,

---

[148] P. 12.

[149] Les considérants nos 151 et 152 sont rédigés comme suit :

« *151. Toutefois, dans la mesure où l'article 3, point 9, de la directive PNR se réfère non pas à la peine minimale applicable, mais à la peine maximale applicable, il n'est pas exclu que des données PNR puissent faire l'objet d'un traitement à des fins de lutte contre des infractions qui, bien qu'elles remplissent le critère prévu par cette disposition relatif au seuil de gravité, relèvent, compte tenu des spécificités du système pénal national, non pas des formes graves de criminalité, mais de la criminalité ordinaire.*

152. Il incombe donc aux États membres d'assurer que l'application du système établi par la directive PNR est effectivement limitée à la lutte contre des formes graves de criminalité et que ce système n'est pas étendu à des infractions qui relèvent de la criminalité ordinaire » (souligné par l'Autorité).

[150] Voir à ce sujet, notamment, l'Avis de l'Autorité n° 245/2022 du 21 octobre 2022 *concernant un avant-projet de loi relative à l'approche administrative communale, à la mise en place d'une enquête d'intégrité communale et portant création d'une Direction chargée de l'Evaluation de l'Intégrité pour les Pouvoirs publics (CO-A-2022-248)*, considérants nos 18 et s.

contrefaçon et piratage de produits, racisme et xénophobie, racket, falsifications de documents administratifs et trafic de faux, viol, incendie volontaire, détournement d'avion, ***etc.***) de telle sorte qu'il puisse être douté du fait que des mises à jour fréquentes seront nécessaires. En outre, un renvoi vers l'incrimination de droit belge n'empêche pas celle-ci d'évoluer dans le Code pénal, sans qu'une modification du Projet ne soit nécessaire (sauf évidemment si la modification a un impact sous l'angle de la gravité de l'incrimination concernée).

94. Deuxièmement plus fondamentalement, l'approche proposée dans le dispositif du Projet **ne répond pas à la préoccupation exprimée par la Cour de justice** dès lors qu'elle ne comporte aucune règle – aucune condition – permettant la prise en compte de la position de la Cour – elle se borne à renvoyer à la liste des infractions visées par ETIAS et à la peine maximale minimum considérée. En conclusion sur ce point, **l'Autorité est d'avis que le Projet doit identifier les infractions de droit belge de criminalité grave concernées**.

95. Dans un tout autre registre, le Projet[151] **étend les possibilités de consultation ETIAS à des finalités poursuivies par les services de renseignements et de sécurité**, en prévoyant qu'un accès au système central peut être demandé en matière « *de suivi des activités visées aux articles 7, 1°*[152], *et 3°/1*[153], *et 11, § 1er, 1°, 2°, 3°, et 5°*[154] *de la loi du 30 novembre 1998 organique des*

---

[151] Article 14, § 1er, 3°, du Projet.

[152] « *1° de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'Etat et les relations internationales, le potentiel scientifique ou économique défini par le Conseil national de sécurité, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité* » (souligné par l'Autorité).

[153] Il s'agit « *de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge* » (souligné par l'Autorité).

[154] Il s'agit de « *1° de rechercher, d'analyser et de traiter le renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir, ainsi que le renseignement relatif à toute activité qui menace ou pourrait menacer:*

a) l'intégrité du territoire national ou la population,

b) les plans de défense militaires,

c) le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du ministre de la Justice et du ministre de la Défense,

d) l'accomplissement des missions des Forces armées,

e) la sécurité des ressortissants belges à l'étranger,

f) tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité;

et d'en informer sans délai les ministres compétents ainsi que de donner des avis au gouvernement, à la demande de celui-ci, concernant la définition de sa politique intérieure et étrangère de sécurité et de défense;

2° de veiller au maintien de la sécurité militaire du personnel relevant du Ministre de la Défense nationale, et des installations militaires, armes et systèmes d'armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires et, dans le cadre des cyberattaques de systèmes d'armes, de systèmes informatiques et de communications militaires ou de ceux que le Ministre de la Défense nationale gère, de neutraliser l'attaque et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit des conflits armés;

[…]

5° de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge » (souligné par l'Autorité).

services de renseignement et de sécurité ». **Or** comme cela a été précédemment mis en évidence, ETIAS peut être consulté par les autorités désignées par les Etats membres dans le domaine de la **prévention, de la détection et des enquêtes concernant des infractions terroristes ou d'autres infractions pénales graves**, ces deux derniers concepts étant en outre définis (limitativement) par le Règlement ETIAS[155]. Force est de constater que les finalités poursuivies par la VSSE et le SGRS visées par le Projet **excèdent ce qui est permis par le Règlement ETIAS**. L'Autorité a interrogé le demandeur à propos de la justification de l'extension des finalités de la consultation d'ETIAS réalisée via le Projet et celui-ci a répondu ce qui suit :

> « *Voyez l'exposé des motifs, page 5.*
>
> *Il a été décidé d'inclure les services de renseignements et de sécurité dans les traitements liés aux finalités répressives à l'instar de ce qui a été mis en place pour l'Unité d'information des passagers (système PNR), dans la mesure où ils jouent un rôle important en matière de détection et de prévention des infractions terroristes et d'autres phénomènes de criminalité grave visés dans le Règlement. Il faut également prendre en considération ces deux éléments*
> *-la Belgique est un pays particulièrement 'à risque' du point de vue sécuritaire à la fois comme pays hôte de l'UE et de l'OTAN, notamment, et comme nœud de transports internationaux pouvant être utilisé comme 'plaque tournante' par les organisations criminelles ;*
> *-les phénomènes criminels sont de plus en plus hybrides et la détection des menaces requière une approche intégrée et complémentaire des différents services impliqués.*
>
> *Nous considérions qu'il n'était pas nécessaire pour autant d'ajouter ce point 3° à l'article 14, §1 du Projet dans la mesure où la demande de consultation devra mentionner l'infraction précise en cause (article 14,§2 du Projet), étant entendu que cette infraction fait partie de celles visées aux points 1° et 2°. Les services de renseignements et de sécurité ont cependant insisté pour ajouter ce point 3°, du moins tant que la Cour constitutionnelle ne l'aura pas formellement invalidé (voir l'Affaire Ligue des droits humains, CJUE C-817/19, cinquième question préjudicielle, arrêt de la Cour constitutionnelle attendu -n° de rôle 6713)* » (souligné par l'Autorité).

96. L'Autorité est d'avis que **le dispositif du Projet doit être adapté de manière telle que la VSSE et le SGRS ne puissent, en exécution du Projet, consulter ETIAS** (et plus largement, interagir

[155] Voir l'article 3, 1., 2., du Règlement ETIAS. L'article 3, 1., 15., du Règlement ETIAS définit **l'infraction terroriste** comme « *une infraction qui correspond ou est équivalente à l'une des infractions visées dans la directive (UE) 2017/541* » du Parlement européen et du Conseil du 15 mars 2017 *relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil*.

L'article 3, 1., 16., du Règlement ETIAS définit **l'infraction pénale grave** comme « *une infraction qui correspond ou est équivalente à l'une des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI, si elle est passible, en droit national, d'une peine ou d'une mesure de sûreté privative de liberté d'une durée maximale d'au moins trois ans* ».

avec l'écosystème ETIAS) **<u>que</u> lorsqu'ils exercent leurs compétences *dans la finalité poursuivie par ETIAS***, à savoir dans le cadre des fins répressives telles que définies exhaustivement par le Règlement ETIAS[156] (et ce, **sans préjudice des développements précédents concernant le droit de la protection des données applicables à ces services et l'autorité de contrôle compétente en la matière**)[157]. Si l'Etat belge entend joindre les services de renseignement et de sécurité aux unités opérationnelles qui peuvent accéder au système central ETIAS, cela ne peut se faire que dans les limites permises par le Règlement ETIAS lui-même et autrement dit, dans le cadre de la prévention, de la détection et des enquêtes relatives aux infractions pénales visées par le Règlement ETIAS et aux conditions fixées par ce Règlement. Dans le cas contraire, le Projet méconnaîtrait la délimitation des finalités du système ETIAS et violerait les principes de licéité des traitements et de finalité. **En d'autres termes, l'Autorité est d'avis que l'article 14, § 1er, 3°, du Projet doit être omis**.

97. **Cette constatation a également un impact direct sur l'article 21 du Projet** qui permet à la VSSE et au SGRS d'introduire des données dans la liste de surveillance ETIAS pour les finalités visées à l'article 14, § 1er, du Projet. De nouveau, la finalité poursuivie par le Règlement ETIAS ne peut pas être détournée par une norme de droit belge.

II.3.3. <u>Point d'accès central</u>

98. C'est la **Section du CCN** qui est désignée comme point d'accès central, et « *vérifie en toute indépendance* » la satisfaction des conditions d'accès prévues à l'article 52 du Règlement ETIAS[158].

99. Comme l'Autorité l'a déjà mis en évidence, il doit tout d'abord se dégager clairement du Projet que c'est le **fonctionnaire dirigeant** qui prend les décisions en la matière. Ceci est d'autant plus important que les membres détachés sont issus des services qui sont demandeurs des consultations des données. Autrement dit, leur implication directe dans le processus de vérification indépendante exigé par le Règlement ETIAS est susceptible de causer problème à cet égard, et ce d'autant plus pour les trois raisons suivantes additionnelles.

---

[156] Dans un sens similaire, voir C.J.U.E. (Gr. Ch.), 21 juin 2022 (LIGUE DES DROITS HUMAINS C/ CONSEIL DES MINISTRES), aff. C-817/19, considérants nos 230-237.

[157] Voir les considérants nos 22-26 et 31.

[158] Article 16 du Projet. Plus en détails, l'article 50, 2., als 2 et 3, du Règlement ETIAS prévoit ce qui suit :

« *L'autorité désignée et le point d'accès central <u>peuvent faire partie de la même organisation</u> si le droit national le permet, mais <u>le point d'accès central agit en toute indépendance à l'égard des autorités désignées</u> quand il accomplit ses missions au titre du présent règlement. Le point d'accès central <u>est distinct des autorités désignées</u> et <u>ne reçoit d'elles aucune instruction</u> concernant le résultat de ses vérifications, qu'il effectue de manière indépendante.*

Les États membres peuvent désigner plusieurs points d'accès centraux afin de tenir compte de leurs structures organisationnelles et administratives dans l'accomplissement de leurs obligations constitutionnelles ou autres obligations légales » (souligné par l'Autorité).

100. Premièrement, l'exposé des motifs prévoit que « *L'autorité hiérarchique est également conservée par les services d'origine en ce qui concerne l'évaluation des détachés et les aspects disciplinaires* »[159]. Deuxièmement, il prévoit également que les membres détachés continueront d'assumer des fonctions pour leurs services d'origine dans le cadre d'ETIAS, dans la mise à jour de la liste de surveillance ETIAS[160]. Et troisièmement, le Projet n'encadre pas le détachement de conditions particulières (durée, possibilité d'y mettre un terme, par qui et dans quelles conditions, etc.).

101. **Dans ce contexte, l'Autorité est d'avis que les membres détachés ne peuvent pas être impliqués dans le processus de vérification incombant au point d'accès central, processus qui doit relever de la compétence d'autres agents de la Section CCN**. Ce que le dispositif du Projet doit prévoir, étant entendu qu'en l'état, il est silencieux sur ce point.

II.4. RESPONSABLES DU TRAITEMENT

102. Au-delà de la fixation de la responsabilité des institutions européennes concernées (dont eu-LISA), le Règlement ETIAS prévoit directement qu'en « *ce qui concerne les traitement de données à caractère personnel dans le système central ETIAS par un Etat membre, **l'unité nationale ETIAS** est considérée comme le **responsable du traitement*** » au sens du RGPD ; elle « *assume la **responsabilité centrale** du traitement de données à caractère personnel dans le système central ETIAS par le dit Etat membre* »[161] (gras ajouté et souligné par l'Autorité).

103. L'article 32, al. 1er, du Projet prévoit quant à lui en outre que « *le président du SPF Intérieur est en charge de la responsabilité opérationnelle du traitement des données à caractère personnel dans le système central ETIAS. A ce titre, il veille à ce que les accès prévus pour les autorités visées à l'article 13, § 2, 4, 4bis et 4ter du Règlement ETIAS seront limités à des personnes dûment autorisées et respectent les finalités de traitement définies dans le règlement* » (souligné par l'Autorité).

104. S'agissant de l'identification du responsable du traitement, l'Autorité rappelle sa pratique d'avis selon laquelle une autorité publique est en principe **responsable du traitement de données nécessaire à la mise en œuvre de la mission d'intérêt public ou de l'obligation légale[162] qui lui incombent, ou encore, qui relève de l'autorité publique dont elle est investie, en vertu de**

---

[159] P. 10.

[160] « *Quand ils assurent une mission de leurs services, ils en répondent à leur hiérarchie. La mise à jour des données de la liste de surveillance doit être contrôlée par la hiérarchie des services d'origine et non par le fonctionnaire dirigeant de la section* », p. 10.

[161] Article 57, 2., du Règlement ETIAS.

[162] Pour une application dans le domaine de l'analyse de la menace, voir l'avis de l'Autorité n° 184/2021 du 4 octobre 2021 *concernant un avant-projet de loi modifiant la loi du 10 juillet 2006 relative à l'analyse de la menace (CO-A-2021-174)*, considérants nos 36-38.

la norme concernée[163, 164]. Les responsables du traitement peuvent en outre être **conjoints**[165]. L'objectif de la définition large du concept de responsable du traitement[166] est d'assurer une protection efficace et complète des personnes concernées[167]. Selon les faits, une responsabilité conjointe de traitement peut lier plusieurs acteurs, la personne concernée pouvant alors exercer ses droits à l'égard de et contre chacun d'entre eux[168]. Toutefois, « *l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente* […et a]*u contraire*, [l]*es opérateurs peuvent être impliqués à différents stades du traitement de données et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce* »[169]. C'est dans « *le cadre de ses responsabilités, de ses compétences et de ses possibilités* » que le responsable conjoint veillera à la conformité de son activité aux règles de protection des données[170]. Les responsables conjoints du traitement **devront conclure un accord entre eux déterminant leurs obligations respectives**, « *sauf si, et dans la mesure où leurs obligations respectives sont définies* » dans le contexte normatif national pertinent[171].

---

[163] Et la responsabilité au regard du traitement peut porter sur des obligations/missions de nature technique au regard de ce traitement, voir par exemple l'article 57, 1., du Règlement ETIAS (responsabilité d'eu-LISA au regard de la sécurité de l'information dans le système central ETIAS, et

Sur la pratique de l'Autorité en matière de désignation du responsable du traitement, voir : avis n° 129/2022 du 1er juillet 2022 *concernant les articles 2 et 7 à 47 d'un projet de loi portant des dispositions diverses en matière d'Economie*, considérants nos 42 et s. ; avis n° 131/2022 du 1er juillet 2022 *concernant un projet de loi portant création de la Commission du travail des arts et améliorant la protection sociale des travailleurs des arts*, considérants nos 55 et s. ; l'avis n° 112/2022 du 3 juin 2022 *concernant un projet de loi modifiant le Code pénal social en vue de la mise en place de la plateforme eDossier*, considérants nos 3-41 et 87-88 ; avis n° 231/2021 du 3 décembre 2021 *concernant un avant-projet d'ordonnance concernant l'interopérabilité des systèmes de télépéage routier*, considérants nos 35-37 ; l'avis n° 37/2022 du 16 février 2022 *concernant un avant-projet de décret instituant la plateforme informatisée centralisée d'échange de données 'E-Paysage'*, considérant n° 22 ; l'avis n° 13/2022 du 21 janvier 2022 *concernant un projet d'arrêté du Gouvernement de la Région de Bruxelles-Capitale relatif à l'octroi de primes à l'amélioration de l'habitat et un projet d'arrêté du Gouvernement de la Région de Bruxelles-Capitale modifiant l'arrêté du Gouvernement de la Région de Bruxelles-Capitale du 9 février 2012 relatif à l'octroi d'aides financières en matière d'énergie*, considérants nos 9-17 ; l'avis n° 65/2019 du 27 février 2019 *concernant un projet d'accord de coopération modifiant l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative*, considérants nos 90-113.

[164] Voir également sur le sujet les conclusions de l'Avocate générale L. Medina présentées le 8 juin 2023 dans l'Aff. C-231/22, *Etat belge c/ Autorité de protection des données*.

[165] Pour une application dans le domaine de **l'analyse de la menace**, voir l'avis de l'Autorité n° 184/2021 du 4 octobre 2021 *concernant un avant-projet de loi modifiant la loi du 10 juillet 2006 relative à l'analyse de la menace (CO-A-2021-174)*, considérants nos 59-62.

Pour une application dans le cadre de l'**EES**, voir l'avis de l'Autorité n° 122/2022 du 1er juillet 2022 précité, note de bas de page n° 9.

Pour une application dans le cadre du **SIS**, voir l'avis de l'Autorité n° 121/2022 du 1er juillet 2022 précité, considérants n° 17 et 25 et s.

[166] Les notions de responsable du traitement et de sous-traitant sont définies à l'article 4, 7) et 8) du RGPD. Lire également l'avis G29 n° 1/2010 « sur les notions de "responsable du traitement" et de "sous-traitant" (WP169) », 16 février 2010.

[167] CJUE (Gr. Ch.), 13 mai 2014 (GOOGLE SPAIN SL, GOOGLE INC. c/ AEPD), aff. C-132/12, considérant n° 34 ; CJUE (Gr. Ch.), 5 juin 2018 (UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIM c/ WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN GMBH), aff. C-210/16, considérant n° 28.

[168] Article 26, 3., du RGPD.

[169] CJUE (Gr. Ch.), 5 juin 2018 (UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIM c/ WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN GMBH), aff. C-210/16, considérant n° 43. Lire également, notamment, G29, Avis n° 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », 16 février 2010, p. 20.

[170] CJUE (Gr. Ch.), 13 mai 2014 (GOOGLE SPAIN SL, GOOGLE INC. c/ AEPD), aff. C-132/12, considérant n° 38.

[171] Article 26, 1., *in fine* du RGPD.

105. L'Autorité souligne que les concepts de responsabilités « *centrale* » (Règlement ETIAS) et « *opérationnelle* » (Projet), n'existent pas dans le RGPD. Elle est par conséquent d'avis **qu'il convient d'omettre du Projet le concept de « *responsabilité opérationnelle du traitement* »**.

106. Le **Règlement ETIAS prévoit explicitement que la personne concernée peut exercer ses droits auprès de l'unité centrale ETIAS ou de l'U.N.E.**[172]. Pour le reste, le Règlement ETIAS et le Projet assurent une répartition des rôles et responsabilités entre les autorités publiques nationales et européennes concernées, qui de concert et indissociablement, participent à la réalisation des finalités poursuivies par le Règlement ETIAS. L'Autorité est d'avis que ces autorités se trouvent dans une situation de **responsabilité conjointe au regard des traitements de données à caractère personnel** mis en œuvre en exécution du Projet et du Règlement ETIAS, **chacune étant responsable du traitement à la mesure des obligations et missions qui lui incombent en vertu du Projet et du Règlement ETIAS**, **et conformément aux règles de protection des données qui s'appliquent à elles[173]**.

107. Cela n'empêche pas que le Projet puisse imputer au président du SPF Intérieur une responsabilité spécifique au regard du traitement, découlant d'obligations qui seraient mises à sa charge par le Projet. En l'état, l'article 32 du Projet lui impute une responsabilité particulière au titre des mesures techniques et organisationnelles à mettre en œuvre ainsi qu'en matière d'*accountability*.

108. Par ailleurs, ces responsabilités seront organisées selon les finalités d'ETIAS, dont la finalité de prévention de risques d'ETIAS[174] et la consultation à des fins répressives de ce dernier[175]. Les rôles des différentes autorités concernées varient en effet selon les finalités et missions poursuivies, tout comme les règles de protection des données matériellement applicables.

II.5. <u>SANCTIONS SPÉCIFIQUES AU RÈGLEMENT ETIAS</u>

109. L'article 62 du Règlement ETIAS, consacré dans un titre relatif à la protection des données, prévoit que les Etats membres doivent déterminer un régime de sanctions (effectives, proportionnées et dissuasives) applicables en cas de violation du Règlement. Le Projet ne prévoit rien en la matière de telle sorte que l'Autorité a interrogé le demandeur à ce sujet. Celui-ci a répondu ce qui suit :

---

[172] Voir l'article 64, 2., du Règlement ETIAS.

[173] Par exemple, si une autorité publique évalue un risque selon les règles du titre 2 ou du titre 3 de la LTD, cela n'empêche pas que les données à caractère personnel qu'elle communique à une autre autorité pour l'exercice de ses propres missions, devront être traitées par cette autorité, conformément au RGPD si celle-ci relève du champ d'application du RGPD. Voir notamment l'avis de l'Autorité n° 184/2021 du 4 octobre 2021 *concernant un avant-projet de loi modifiant la loi du 10 juillet 2006 relative à l'analyse de la menace (CO-A-2021-174)*, considérant n° 12.

[174] Voir les considérants nos 13-27.

[175] Voir les considérants nos 28-30.

> « *Nous avons considéré que cette disposition qui est incluse dans le chapitre Protection des données du Règlement, visait en particulier la violation du droit applicable en matière de protection des données. Nous avons donc considéré que les sanctions prévues par la loi de 2018 étaient d'application et qu'il n'était pas nécessaire de prévoir une disposition à ce sujet dans le Projet* » (souligné par l'Autorité).

110. L'Autorité prend acte de cette motivation. Cela étant précisé, force est de constater que les auteurs du Règlement ETIAS ont estimé utile d'insérer une telle disposition en étant à la fois tout à fait conscient de l'existence du RGPD et de la Directive 2016/680 ainsi que des règles les exécutant/transposant en droit national.

111. Dans ces conditions, **l'Autorité invite le demandeur à réfléchir à des possibilités de sanctions spécifiques qui pourraient s'appliquer dans le contexte du Règlement ETIAS**. Par exemple, le sujet de la recevabilité des preuves et des poursuites pourrait être exploré, dans la mesure pertinente, etc.

112. De manière générale, l'Autorité est d'avis que le Projet devrait prévoir une obligation spécifique à charge de l'U.N.E. de publier un rapport synthétique et anonymisé sur les manquements en matière de protection des données constatés par les autorités de contrôle, notamment au terme des audits que celles-ci doivent mener. Une telle mesure de transparence est de nature à garantir un meilleur contrôle par la société, des activités de l'U.N.E., et de la sorte, une meilleure effectivité des règles de protection des données. Au passage, l'Autorité rappelle qu'il « *convient que chaque autorité de contrôle soit dotée des moyens financiers et humains,* […] *nécessaires à la bonne exécution de ses missions, y compris celles qui sont liées à l'assistance mutuelle et à la coopération avec d'autres autorités de contrôle dans l'ensemble de l'Union* »[176]. La publication juste évoquée devrait également être assortie de cette mise en contexte, compte-tenu du fait que le Règlement ETIAS aura un impact sur la charge de travail de ces autorités.

II.6. DIVERS

II.6.1. Autorité de contrôle de l'AGD&A

113. L'Autorité attire l'attention du demandeur sur le fait que même lorsqu'elle agit dans le cadre du titre 2 de la LTD, **l'AGD&A demeure soumise au contrôle de l'Autorité de Protection des**

[176] Considérant n° 120 du RGPD.

Données[177]. Or l'article 34 du Projet, concernant l'accès à ETIAS à des fins répressives[178], ne modifie que l'article 281 de la loi du 18 juillet 1977 *générale sur les douanes et accises*[179]. La compétence octroyée au COC à l'égard de l'AGD&A dans le cadre du fonctionnement de l'UIP a nécessité une **modification de l'article 71 de la LTD**[180]. Dans la logique du Projet, le COC devrait également être désigné, pour l'accès à ETIAS aux fins répressives, par l'AGD&A, via une modification de l'article 71 de la LTD.

II.6.2. Outils techniques

114. Outils techniques. L'article 25, § 1er, du Projet se réfère aux « *outils techniques nationaux nécessaires afin d'accomplir les missions* » incombant au fonctionnaire dirigeant et aux personnes de sa section. L'Autorité a interrogé le demandeur quant à la question de savoir ce qu'il était entendu par « *outils techniques* » et celui-ci a répondu ce qui suit :

> « *Les outils propres à l'UNE : Application nationale Beltias nécessaire pour gérer la liste de surveillance et les demandes de consultation (mentionnée dans l'exposé des motifs, p 14), les accès prévus dans le Projet au RNN et au Casier judiciaire.*

---

[177] Voir la note de bas de page n° 106.

[178] Pour l'évaluation des risques en matière de sécurité, l'AGD&A doit continuer de relever de la compétence de l'Autorité de Protection des Données, voir le considérant n° 17.

[179] Celui-ci est rédigé comme suit :

« *Art. 281.§ 1er. Toutes actions du chef de contraventions, fraudes ou délits, contre lesquels les lois en matière de douanes et accises prononcent des peines seront portées en première instance devant les tribunaux correctionnels, et, en cas d'appel, devant la cour d'appel du ressort, pour y être instruites et jugées conformément au Code d'instruction criminelle.*

§ 2. Toutes celles des actions susmentionnées qui tendent à l'application d'amendes, de confiscations, ou à la fermeture de fabriques ou usines, seront intentées et poursuivies par l'administration ou en son nom devant lesdits tribunaux, lesquels, en tout cas, ne prononceront sur ces affaires qu'après avoir entendu les conclusions du ministère public. Toutefois, sur la demande écrite qui lui en est faite par un fonctionnaire de l'Administration générale des douanes et accises ayant au moins le grade de conseiller général désigné pour l'administration en charge des contentieux, le ministère public peut requérir le juge d'instruction d'informer, l'exercice de l'action publique restant pour le surplus réservé à l'administration.

§ 3. Dans les cas qu'un même fait de transgression aux lois précitées donne lieu à deux actions différentes, dont l'une doit être intentée par le ministère public et l'autre par l'administration ou en son nom, ces actions seront instruites simultanément, et il y sera statué par un seul et même jugement; mais, dans ces cas, le ministère public n'agira pas avant que l'administration ait, de son côté, porté plainte ou intenté l'action.

§ 4. En recherchant les crimes et délits visés à l'article 8, § 1er, 5°, de la loi du 25 décembre 2016 relative au traitement des données des passagers, le conseiller-général désigné pour l'administration en charge des contentieux peut, par une décision écrite et motivée, charger un agent des douanes et accises, de requérir l'UIP afin de communiquer les données des passagers conformément à l'article 27 de la loi du 25 décembre 2016 relative au traitement des données des passagers.

La motivation de la décision reflète le caractère proportionnel eu égard à la protection des données à caractère personnel et subsidiaire à tout autre devoir d'enquête.

La décision et sa motivation sont notifiées à l'Organe de contrôle de l'information policière visé à l'article 71 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

L'Organe de contrôle de l'information policière interdit au conseiller-général désigné pour l'administration en charge des contentieux d'exploiter les données recueillies dans des conditions qui ne respectent pas les conditions légales ».

[180] Voir l'article 13 de la loi du 2 mai 2019 modifiant diverses dispositions relatives au traitement des données des passagers, selon lequel :

« *L'article 71, § 1er, de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, est complété par un alinéa rédigé comme suit:*

"Elle est également, vis-à-vis de l'autorité compétente visée à l'article 26, § 1er, 7°, e), chargée de surveiller l'application de l'article 281, § 4, de la loi générale sur les douanes et accises du 18 juillet 1977" » (souligné par l'Autorité).

Divers outils IT nécessaires pour faciliter les missions de l'UNE : JBOX ou autre système permettant un échange électronique des pièces de procédure pour les recours, application Teams pour les interviews[181]*,…*

Nous avons utilisé ce terme générique car ces outils peuvent évoluer » (souligné par l'Autorité).

115. L'Autorité prend acte de cette explication et du fait que cette disposition **n'ait pas pour objectif d'encadrer le traitement de données à caractère personnel**.

II.6.3. Communication de données à des pays non-Membres de l'Union

116. **Sans préjudice des divers commentaires qui ont déjà été émis au sujet du rôle des services de renseignements et de sécurité dans le cadre du Règlement ETIAS**, l'article 20 du Projet prévoit une possibilité, en vertu des articles 93 et 94 de la LTD, ainsi que dans les conditions fixées par cette disposition elle-même, pour ces services, de communiquer des données à des pays non-membres de l'Union européenne. C'est l'article 65 du Règlement ETIAS qui encadre ces possibilités de flux transfrontières. L'article 65, 2., du Règlement ETIAS consacre une interdiction très générale s'appliquant « *également si ces données font l'objet d'un traitement ultérieur au niveau national ou entre Etats membres* ».

117. Parmi les exceptions pertinentes, **c'est l'article 65, 5.**, du Règlement ETIAS qui vise l'hypothèse de la communication de données visées à l'article 52, 4., du Règlement ETIAS, après une consultation aux fins répressives et dans les limites fixées par cette disposition[182]. Notamment, un tel transfert ne peut être réalisé que conformément aux dispositions pertinentes de la Directive 2016/680, et il se dégage du Règlement ETIAS qu'il est alors soumis à l'autorité de contrôle désignée conformément à l'article 41, 1., de la Directive 2016/680. **Le législateur belge ne dispose pas de marge de manœuvre en la matière et l'article 20 du Projet doit par conséquent doit être omis ou adapté de manière telle que les services de renseignements et de sécurité soient à cette fin, considérés comme des autorités compétentes visées par le titre 2 de la LTD** (avec désignation de l'autorité de contrôle compétente).

---

[181] Voir quant au moyen audiovisuel utilisé pour les entretiens, la **Décision d'exécution (UE) 2022/1462 de la Commission du 2 septembre 2022** *relative aux exigences applicables aux moyens de communication audiovisuels utilisés pour l'entretien conformément à l'article 27, paragraphe 5, du règlement (UE) 2018/1240 du Parlement européen et du Conseil*.

[182] L'article 65, 3., vise l'hypothèse particulière d'un retour qui n'est pas pertinente au regard de l'article 20 du Projet.

Par ces motifs,
L'Autorité est d'avis que

1. Le Règlement ETIAS et le Projet entraînent une ingérence importante dans les droits et libertés des personnes concernées (**considérant n° 8**) ;

2. l'article 31, § 2, du Projet peut prévoir l'application du titre 2 de la LTD à « *l'évaluation des risques sécuritaires* », pour autant que l'Autorité de Protection des Données soit l'autorité de contrôle compétente dans ce contexte, sauf pour ce qui concerne la compétence du COC à l'égard des services de police, dès lors que celui-ci a aussi été désigné comme autorité de contrôle en vertu du RGPD (**considérants nos 14 et 17-19**) ;

3. Le Projet doit être revu en ce qui concerne les règles régissant le droit de la protection des données applicable aux services de renseignements et de sécurité ainsi que l'autorité compétente à leur égard en ce qui concerne d'une part, les membres détachés dans le cadre de l'évaluation des risques liés à la sécurité, et d'autre part, l'accès à ETIAS à des fins répressives (**considérant nos 22-26 et 31**) ;

4. L'article 21 du Projet doit être adapté en ce qu'il se réfère aux finalités répressives d'ETIAS plutôt qu'à la finalité de prévention du risque de sécurité. Et il peut prévoir l'application du titre 2 de la LTD en vue de l'alimentation de la liste de surveillance ETIAS, pour autant que l'Autorité de Protection des Données soit l'autorité de contrôle compétente, sauf pour les services de police (**considérant nos 17 et 21**) ;

5. ETIAS soulève une interrogation quant au respect du principe d'égalité entre personnes devant être titulaires d'un visa et personnes devant disposer d'une autorisation de voyage selon ETIAS (**considérants nos 40-41**) ;

6. Le dispositif du Projet ne peut se limiter à prévoir une faculté d'alimenter la liste de surveillance ETIAS mais doit fixer les conditions dans lesquelles les autorités concernées doivent signaler une personne dans la liste de surveillance ETIAS (**considérants nos 45-48**);

7. Le dispositif du Projet doit déterminer les éléments essentiels des traitements de données nécessaires à la contribution de l'Etat belge à l'établissement des indicateurs de risques spécifiques (**considérants nos 49-53**) ;

8. Le dispositif du Projet doit identifier les « *bases de données nécessaires* » qui doivent être consultées par les membres détachés aux fins de la réalisation de l'évaluation des risques de sécurité, sous l'autorité du fonctionnaire dirigeant de la Section CCN de l'U.N.E. (**considérants nos 58-61**) ;

9. L'article 27 du Projet doit clairement préciser que la Section OE de l'U.N.E. est chargée de se prononcer sur le risque d'immigration illégale et d'évaluer ce dernier. Et le Projet doit encore identifier les (catégories de) données à caractère personnel et systèmes d'information qui doivent être réutilisés à cette fin (**considérants nos 62-64**) ;

10. Le dispositif du Projet lui-même doit spécifier que le fonctionnaire dirigeant prend les décisions pour la Section qu'il dirige (**considérants nos 67-68**) ;

11. Un recours en pleine juridiction contre les décisions de l'U.N.E. constitue *a priori* une meilleure garantie pour les droits et libertés des personnes concernées et l'exposé des motifs du Projet modificatif doit en tout état de cause justifier la raison pour laquelle un recours en annulation serait plutôt nécessaire (**considérants nos 71-72**) ;

Le mise en œuvre d'un recours en pleine juridiction se justifie d'autant plus à l'égard des décisions de l'U.N.E. concernant la rectification ou la suppression des données à caractère personnel, de telle sorte qu'un tel recours devrait être prévu dans cette hypothèse par le Projet modificatif (**considérants nos 77-78**) ;

12. Le dispositif du Projet modificatif doit clarifier que l'avis négatif émis par une Section de l'U.N.E. dans le cadre des consultations visées à l'article 28 du Règlement ETIAS constitue une décision susceptible de recours (**considérants n° 73**) ;

13. Le dispositif du Projet doit être adapté et garantir clairement que la personne concernée disposera du droit d'accès à l'évaluation des risques qui a été réalisée à son sujet et sur la base de laquelle une décision administrative est prise à son sujet par l'U.N.E. (**considérants nos 74-76**) ;

14. Le dispositif du Projet doit déterminer dans quelles conditions les autorités concernées doivent communiquer à l'U.N.E. les données à caractère personnel de nature à entraîner l'annulation ou la révocation d'une autorisation de voyage (**considérants nos 79-81**) ;

15. Une norme (et non une décision des services concernés) doit identifier quelles sont les unités opérationnelles au sens du Règlement ETIAS qui peuvent introduire des demandes de consultation d'ETIAS aux fins répressives (**considérants nos 89-90**) ;

16. L'article 31, §§ 2 et 3, du Projet, doit être adapté afin de clarifier qu'il vise la consultation d'ETIAS aux fins répressives (**considérants n° 91**) ;

17. Le Projet doit identifier les infractions de droit belge pertinentes relevant de la criminalité grave visée par le Règlement ETIAS (**considérants nos 92-94**) ;

18. Le Projet doit être modifié (notamment, l'article 14, § 1er, 3°, doit être omis) en ce qu'il entend étendre les finalités d'ETIAS à d'autres finalités poursuivies par les services de renseignement et de sécurité, contrairement à ce que permet le Règlement ETIAS (**considérants nos 95-97**) ;

19. Les membres détachés ne peuvent pas être impliqués dans le processus de vérification incombant au point d'accès central, processus qui doit relever de la compétence d'autres agents de la Section CCN. Ce que le dispositif du Projet doit prévoir, étant entendu qu'en l'état, il est silencieux sur ce point (**considérants nos 98-101**) ;

20. Le Règlement ETIAS et le Projet organisent des responsabilités conjointes au regard du traitement de données et le Projet doit être adapté en conséquence (**considérants nos 102-108**) ;

21. Le demandeur doit explorer la possibilité de consacrer des sanctions particulières en cas de violation des règles de protection des données en exécution du Règlement ETIAS (**considérants nos 109-111**) ;

22. Le Projet doit modifier l'article 71 de la LTD afin que le COC soit également l'Autorité de contrôle de l'AGD&A lorsque celle-ci consulte ETIAS aux fins répressives (**considérant n° 113**) ;

23. L'article 25, § 1er, du Projet (visant les « *outils techniques nationaux nécessaires* ») ne peut pas avoir pour objectif d'encadrer le traitement de données à caractère personnel (**considérants nos 114-115**) ;

24. L'article 20 du Projet doit être omis ou adapté à l'aune de l'article 65, 5., du Règlement ETIAS (**considérants nos 116-117**).

Pour le Centre de Connaissances,
Cédrine Morlière , Directrice

Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 121/2023 van 18 juli 2023

Betreft:
Adviesaanvraag over een voorontwerp van wet betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E), (CO-A-2023-236)
Adviesaanvraag over een voorontwerp van wet tot wijziging van de wet betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E) (CO-A-2023-237)

Vertaling[1]

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit"),
aanwezig: de dames Cédrine Morlière, Nathalie Ragheno en Griet Verhenneman, en de heren Yves-Alexandre de Montjoye en Bart Preneel;

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");

[1] Voor de oorspronkelijke versie van de tekst, die collegiaal werd gevalideerd, cf. de Franse versie van de tekst, die beschikbaar is in de FR-versie van de rubriek "adviezen" van de website van de Autoriteit.

Gelet op het verzoek om advies van mevrouw Annelies Verlinden, Minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische Vernieuwing, (hiernae de aanvrager) ontvangen op 8 juni 2023;

Brengt op 18 juli 2023, het volgend advies uit:

I. Onderwerp en context van de adviesaanvraag

1. De minister vroeg de Autoriteit om advies betreffende een voorontwerp van wet betreffende de *oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E)* (CO-A-2023-**236**) (hierna «het ontwerp»), en een adviesaanvraag betreffende een voorontwerp *van wet tot wijziging van de wet betreffende de wet betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E)* (CO-A-2023-237) (hierna «**het wijzigingsontwerp** »).

2. Deze ontwerpen geven uitvoering aan sommige bepalingen van de Verordening (EU) 2018/1240 van het Europees Parlement en de Raad van 12 september 2018 *tot oprichting van een Europees reisinformatie- en -autorisatiesysteem (Etias) en tot wijziging van de Verordeningen (EU) nr. 1077/2011, (EU) nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 en (EU) 2017/2226* (hierna "**de ETIAS-verordening" genoemd**). Deze regeling, die deel uitmaakt van een complexe wetgevingscontext, heeft betrekking op onderdanen van derde landen die, vrijgesteld van de visumplicht, binnen de EU willen reizen. Bij de oprichting werd ETIAS geïnspireerd door het Amerikaanse ESTA, het Canadese AVE en het Australische eVisitor.

3. De Europese Toezichthouder voor gegevensbescherming (hierna "**EDPS**" genoemd) heeft een advies uitgebracht over de voorgestelde ETIAS-verordening waarnaar de Autoriteit ter informatie verwijst.[2].

[2] De EDPS heeft er echter op gewezen dat (de Autoriteit vertaalt): «*zonder een gegevenseffectbeoordeling, die een essentiële voorwaarde is, het onmogelijk is een alomvattende beoordeling te maken van de noodzaak en evenredigheid van ETIAS zoals dat thans wordt voorgesteld* » **EDPS, Advies 3/2017** *over het voorstel voor een verordening tot invoering van een Europees reisinformatie- en autorisatiesysteem (ETIAS)*, 6 maart 2017 (hierna **het ETIAS-advies van de EDPS**). Zie daarna EDPS, advies over de ETIAS AIPD, dossier 2021-0640, beschikbaar op
https://edps.europa.eu/system/files/2022-03/22_03_27_formal_consultation_etias_dpia_fr.pdf,
laatst geraadpleegd op 05/07/2023.

II. Onderzoek

4. De bespreking van de ontwerpen is als volgt gestructureerd :

5. **Wat de gegevensbescherming** betreft, valt ETIAS binnen het toepassingsgebied van de **AVG**, Richtlijn **2016/680**[3] en **Verordening 2018/1725**[4]. Ontwerpartikel 31 regelt het ontwerp in overeenstemming met de toepasselijke Belgische regels inzake gegevensbescherming. In overeenstemming met de WVG wijst de Autoriteit erop dat zij geen advies uitbrengt over de verwerking van persoonsgegevens door de bevoegde autoriteiten (met inbegrip van politiediensten) als bedoeld in titel 2 van de WVG, waarvoor het Controleorgaan op de politionele gegevens (hierna "**COC**" genoemd) verantwoordelijk is, of door de inlichtingen- en veiligheidsdiensten als bedoeld in titel 3 van de WVG, waarvoor het Vast Comité voor de inlichtingen- en veiligheidsdiensten verantwoordelijk is. Deze autoriteiten zijn door de aanvrager binnen hun respectieve bevoegdheidsgebieden aangezocht.

6. De **ETIAS-verordening** zelf bevat **een reeks bepalingen die specifiek betrekking hebben op de verwerking van persoonsgegevens**: artikel 13 (toegang tot gegevens in ETIAS) ; hoofdstuk XI (artikelen 54 en 55) (bewaren[5] en wijzigen van gegevens) ; hoofdstuk XII (gegevensbescherming), waarvan artikel 56 de toepassing van de AVG en Richtlijn 2016/680 uitsplitst, artikel 57 die een verwerkingsverantwoordelijke aanwijst en artikel 58 een verwerker, artikel 59 heeft betrekking op de veiligheid van de verwerking, artikel 60 op veiligheidsincidenten, artikel 61 op zelfcontrole, artikel 62 op sancties, Artikel 63 betreft aansprakelijkheid (civielrechtelijk - recht op schadevergoeding), artikel 64 betreft het recht van toegang, artikel 65 beperkt de mededeling van persoonsgegevens aan derde landen of particuliere entiteiten, de artikelen 66 tot en met 68 betreffen het toezicht door de toezichthoudende autoriteiten en hun samenwerking, en de artikelen 69 en 70 voorzien in het bijhouden van registers.

7. Samengevat zijn de voor advies voorgelegde ontwerpen onder meer gebaseerd op een institutionele logica (oprichting van de Belgische nationale ETIAS-eenheid, taakverdeling, enz.) en procedurele logica (organisatie van de toegang, organisatie van een beroepsprocedure in de ontwerpwijziging, enz.)

---

[3] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van *27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.*

[4] Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG*.

Aangezien Europol hierbij betrokken is, moet volledigheidshalve ook Verordening (EU) 2016/794 van het Europees Parlement en de Raad van 11 mei 2016 *inzake het agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol), ter vervanging en intrekking van Besluiten 2009/371/JBZ, 2009/934/JBZ, 2009/935/JBZ, 2009/936/JBZ en 2009/968/JBZ* van de Raad, worden vermeld.

[5] Het aanvraagdossier wordt bewaard gedurende de geldigheidsduur van de reisautorisatie of tot vijf jaar na de laatste weigering, annulatie of herroeping (behoudens vervroegde annulering, zie artikel 54.1.b) van de ETIAS-verordening). Aanvragers kunnen er ook mee instemmen dat hun dossier wordt bewaard om een nieuwe aanvraag te vergemakkelijken (artikel 54.2, van de ETIAS-verordening). Het aanvraagdossier wordt automatisch verwijderd uit het centrale systeem van ETIAS wanneer de bewaartermijn is verstreken.

8. De ETIAS-verordening en het ontwerp houden duidelijk **een bijzonder** aanzienlijke inmenging in de rechten en vrijheden van de betrokkenen in. Meer bepaald in die zin dat: de geplande verwerkingen zijn grootschalig zijn[6], ze een directe impact hebben op de vrijheid van de betrokkenen om binnen de Unie te reizen[7], ze betrekking hebben op gegevens die gevoelig kunnen zijn en een discriminatierisico[8] inhouden, ze op de een of andere manier een zekere mate van permanent toezicht op de betrokkenen impliceren [9], ze tot onderlinge koppeling leiden van verschillende informatiesystemen met verschillende doeleinden[10], en ze gebaseerd zijn op geautomatiseerde verwerking van gegevens (*screening*) die op hun beurt gebaseerd zijn op profilering[11].

II.1. ETIAS, DOELEINDEN EN TOEPASSELIJKE GEGEVENSBESCHERMINGSREGELS

9. De ETIAS-verordening richt een Europees reisinformatie- en autorisatiesysteem op (hierna « **ETIAS** », voor « *European Travel Information and Authorisation System* »[12]). Wanneer de verordening van kracht wordt, zullen onderdanen van ongeveer zestig derde landen[13] die geen visum nodig hebben om dertig Europese landen binnen te komen[14], een reisautorisatie moeten aanvragen via ETIAS, die toegankelijk is via een website en een mobiele applicatie en wordt afgegeven na een geautomatiseerde *screening die* wordt georganiseerd door de verordening en deels berust bij de lidstaten.

[6] Zie de overwegingen 9-10.

[7] Zie de overwegingen 9-13.

[8] Zie overweging 50.

[9] Zie de overwegingen 79-81.

[10] Met name in overweging 15 van zijn advies, wenst de EGPD het volgende « *insister sur le fait que, bien qu'il existe des interactions entre la migration et la sécurité intérieure, il s'agit de deux domaines de l'ordre public différents dont les objectifs et les acteurs principaux sont distincts* ». Zie in dit verband ook de overwegingen 35 en volgende.

[11] Zie de overwegingen35 e.v.

[12] Zie https://travel-europe.europa.eu/etias/what-etias_en, laatst geraadpleegd op 27/06/2023.

[13] Zier https://travel-europe.europa.eu/etias/who-should-apply_en#who-needs-an-etias-travel-authorisation,

laatst geraadpleegd op 27/06/2023. Artikel 2 van de ETIAS-verordening bepaalt op welke categorieën onderdanen van derde landen zij wel en niet van toepassing is.

[14] d.w.z. de 27 lidstaten, Zwitserland, Liechtenstein en Noorwegen,

zie https://travel-europe.europa.eu/etias/who-should-apply_en#ETIAS-countries, laatst geraadpleegd op 27/06/2023.

10. De ETIAS-verordening[15] beschrijft in detail het normatieve kader voor de werking van ETIAS (en het ETIAS-informatiesysteem[16]) op zodanige wijze dat de **Belgische staat weinig speelruimte heeft**. Op Europees niveau wordt ETIAS ontwikkeld en technisch beheerd door het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (hierna genoemd «**u-LISA** »)[17]. **De centrale ETIAS-eenheid** (d.w.z. een administratieve eenheid) wordt opgericht binnen het **Europees Grens- en kustwachtagentschap**[18]. Krachtens de ETIAS-verordening zijn dit Agentschap en eu-LISA ook verantwoordelijk voor de verwerking van gegevens[19].

11. In het kader van *screening* en reisautorisaties wordt beroep gedaan op **de nationale ETIAS-eenheden** (hierna de "E.N.E." en dit »)[20]in bepaalde gevallen wanneer *de* geautomatiseerde screening

---

[15] Het verleent de Commissie ook de bevoegdheid om gedelegeerde en uitvoeringshandelingen vast te stellen. De volgende teksten kunnen worden aangehaald. Zie met name: :

Gedelegeerd besluit (EU) 2019/969 van de Commissie van 22 februari 2019 *betreffende een instrument waarmee aanvragers hun toestemming voor het gedurende een extra bewaringstermijn opslaan van hun aanvraagdossier kunnen geven of intrekken, overeenkomstig artikel 54, lid 2, van Verordening (EU) 2018/1240 van het Europees Parlement en de Raad* ;

Uitvoeringsbesluit (EU) 2021/627 van de Commissie van 15 april 2021 *tot vaststelling van regels betreffende het bijhouden van en de toegang tot de logbestanden in het Europees reisinformatie- en -autorisatiesysteem (Etias) uit hoofde van Verordening (EU) 2018/1240 van het Europees Parlement en de Raad* ;

Gedelegeerde Verordening (EU) 2021/916 van de Commissie van 12 maart 2021 *tot aanvulling van Verordening (EU) 2018/1240 van het Europees Parlement en de Raad tot oprichting van een Europees reisinformatie- en -autorisatiesysteem (Etias) wat betreft de vooraf vastgestelde lijst van beroepsgroepen die in het aanvraagformulier wordt gebruikt* ;

Uitvoeringsbesluit (EU) 2021/1028 van de Commissie van 21 juni 2021 *tot vaststelling van maatregelen voor de toepassing van Verordening (EU) 2018/1240 van het Europees Parlement en de Raad wat betreft de toegang tot en de wijziging, het wissen en vervroegd wissen van gegevens in het centrale Etias-systeem* ;

Uitvoeringsverordening (EU) 2022/1380 van de Commissie van 8 augustus 2022 *tot vaststelling van de regels en voorwaarden inzake verificatiezoekopdrachten van vervoerders, bepalingen inzake gegevensbescherming en — beveiliging voor het authenticatiesysteem voor vervoerders alsook vangnetprocedures in geval van technische onmogelijkheid, en tot intrekking van Uitvoeringsverordening (EU) 2021/1217* ;

Uitvoeringsbesluit (EU) 2022/102 van de Commissie van 25 januari 2022 *tot vaststelling van formulieren voor weigering, nietigverklaring of intrekking van een reisautorisatie*, hierna « **het utvoeringsbesluit 2022/102** » ;

Gedelegeerd besluit (EU) 2022/1612 van de Commissie van 16 februari 2022 van 16 februari 2022 *tot vaststelling van de inhoud en de vorm van de vooraf vastgestelde lijst van opties die moet worden gebruikt om om aanvullende informatie of documentatie te verzoeken overeenkomstig artikel 27, lid 3, van Verordening (EU) 2018/1240 van het Europees Parlement en de Raad*;

Commission Delegated Decision of 10.12.2020 *supplementing Regulation (EU) 2018/1240 of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) as regards flagging* ;

Commission Delegated Decision of 23.11.2021 *on further defining security, illegal immigration or high epidemic risk*, C(2021) 4981 final ;

Commission Delegated Decision of 27.3.2023 *supplementing Regulation (EU) 2018/1240 of the European Parliament and of the Council, as regards specifying the conditions for the correspondence between the data present in a record, alert or file of the other EU information systems consulted and an ETIAS application file,* C(2023) 950 final ;

[16] Zie de artikelen 5 en 6 van de ETIAS-verordening, waarin wordt omschreven wat ETIAS is en wat de technische architectuur van het ETIAS-informatiesysteem is. ETIAS bevat met name « *een op gemeenschappelijke technische specificaties gebaseerde en voor alle lidstaten identieke nationale uniforme interface (**NUI**) in elke lidstaat, waarmee een beveiligde aansluiting tussen het centrale Etias-systeem en de nationale grensinfrastructuur en de in artikel 50, lid 2, bedoelde centrale toegangspunten in de lidstaten tot stand kan worden gebracht*» (vet toegevoegd door de Autoriteit) (artikel 6.2.b) van de ETIAS-verordening).

[17] Zie artikel 6 van de ETIAS-verordening. Zie ook de verantwoordelijkheden als vastgesteld in de artikelen 73 en 74 van de ETIAS-verordening.

[18] Zie artikel 7 van de ETIAS-verordening. Zie ook de verantwoordelijkheden als vastgesteld in artikel 75 van de ETIAS-verordening.

[19] Zie artikel 57 van de ETIAS-verordening. Zie de overwegingen 102 en volgende.

[20] Artikel 8 van de ETIAS-verordening.

een "manuele" verwerking vereist[21]. Het ontwerp creëert de Belgische E.N.E. **binnen het Nationaal Crisiscentrum**, « **hierna NCC** »)[22].

12. ETIAS streeft een aantal doelen[23] na die kunnen worden samengevat in drie grote doelstellingsgroepen, waarvan de eerste twee de het zwaartepunt vormen van de opmerkingen in dit advies.

II.1.1. <u>Doeleinde van risicopreventie</u>

13. In de eerste plaats heeft ETIAS tot doel bepaalde risico's in verband met de binnenkomst van de betrokken personen op Europees grondgebied te voorkomen : een **VEILIGHEIDSRISICO**[24], een risico op **ILLEGALE IMMIGRATIE**[25] en een **HOOG EPIDEMIOLOGISCH RISICO**[26]. Het doel is om risico's te voorkomen.

14. De **AVG** is van toepassing op de verwerking door de **nationale eenheden van ETIAS** « *die de* ***<u>aanvragen voor een reisautorisatie van de betrokkenen</u>*** *beoordelen* »[27] (vet toegevoegd en onderstreept door de Autoriteit).

15. Maar «*wanneer de verwerking van persoonsgegevens door de nationale Etias-eenheden, wordt uitgevoerd door de* ***bevoegde autoriteiten*** *die* ***<u>de aanvragen beoordelen</u>*** *met het oog op het* ***voorkomen****, of* ***opsporen*** *van* ***terroristische misdrijven of van andere ernstige strafbare feiten****, of onderzoeken ter zake, is* ***Richtlijn (EU) 2016/680*** *van toepassing* »[28] (vet toegevoegd en onderstreept door de Autoriteit).

16. « *Wanneer de nationale Etias-eenheid* ***<u>beslist</u>*** *over de afgifte, weigering, intrekking of nietigverklaring van een reisautorisatie*», (vet toegevoegd en onderstreept door de Autoriteit), is de **AVG** *van* toepassing[29].

---

[21] Artikel 76 van de ETIAS-verordening bepaalt de verantwoordelijkheden die op de Lidstaten rusten.

[22] Artikel 4 van het ontwerp.

[23] Artikel 4 van de ETIAS-verordening bepaalt in het bijzonder het doel van de Verordening.

[24] Artikel 3.1.6 van de ETIAS-verordening definieert dit als «*het risico van een dreiging voor de openbare orde, de interne veiligheid of de internationale betrekkingen van een van de lidstaten* ».

[25] Artikel 3.1.7 van de ETIAS-verordening definieert dit als « *het risico dat een onderdaan van een derde land niet voldoet aan de voorwaarden voor toegang en verblijf als bepaald in artikel 6 van Verordening (EU) 2016/399* ».

[26] Artikel 3.1.8. van de ETIAS-verordening definieert dit als « *elke potentieel epidemische ziekte als omschreven in de internationale gezondheids regelingen van de Wereldgezondheidsorganisatie of het Europees Centrum voor ziektepreventie en -bestrijding (ECDC) en andere infectieziekten of besmettelijke parasitaire ziekten indien voor die ziekten voorzien is in bescher mende regelingen die van toepassing zijn op de onderdanen van de lidstaten* ».

[27] Artikel 56, 2, 1ste lid van de ETIAS-verordening.

[28] Artikel 56, 2, 2de lid van de ETIAS-verordening.

[29] Artikel 56, 2, 3de lid van de ETIAS-verordening.

17. En met betrekking tot de **toezichthoudende autoriteit**, bepaalt de verordening in het algemeen het volgende «*elke lidstaat zorgt ervoor dat de overeenkomstig artikel 51, lid 1, van Verordening (EU) 2016/679 ingestelde toezichthoudende autoriteit onafhankelijk toezicht houdt op de rechtmatigheid van de verwerking van persoonsgegevens uit hoofde van deze verordening door de betrokken lidstaat, met inbegrip van de doorgifte van die gegevens naar en vanuit Etias*» (onderstreept door de Autoriteit)[30]. De ETIAS-verordening verwijst alleen naar de in artikel 41 van Richtlijn 2016/680 bedoelde toezichthoudende autoriteit in artikel 65 (betreffende de mededeling aan derde landen van gegevens[31]) en betreffende het gebruik van ETIAS voor repressieve doeleinden[32]. Met andere woorden, **de Autoriteit concludeert dat de krachtens de AVG aangewezen toezichthoudende autoriteit ook bevoegd moet zijn voor de risicobeoordeling, hoewel die beoordeling onderworpen is aan Richtlijn 2016/680[33]**.

18. Het ontwerp verdeelt de bevoegdheden,inzake risicopreventie door ETIAS, tussen twee verschillende afdelingen van de Belgische E.N.E.[34] :

- De **sectie van de Dienst Vreemdelingenzaken** (hierna «**sectie DVZ**»)[35] die bevoegd is voor de risico's van illegale immigratie ;

- En de **sectie van het Nationaal Crisiscentrum** (hierna «**sectie NCC**»)[36], dat bevoegd is voor de andere risico's (meer bepaald, het veiligheidsrisico en het hoge epidemiologisch risico)[37].

19. Gelet op wat zojuist is gezegd, kan artikel 31, §2, van het ontwerp voorzien in de toepassing van titel 2 van de WVG op «*de beoordeling van veiligheidsrisico's* », **mits de Gegevensbeschermingsautoriteit in dit verband de bevoegde toezichthoudende autoriteit is**, **, behalve wat betreft de bevoegdheid van het COC met betrekking tot politiediensten**, aangezien het COC ook is aangewezen als toezichthoudende autoriteit krachtens de AVG[38].

---

[30] Artikel 66.1, van de ETIAS-verordening .

[31] Zie in dit verband de overwegingen 115-116.

[32] Overwegingen 28 en volgende.

[33] Dit kan worden gerelativeerd aan de hand van de mogelijkheid die artikel 41.3 van Richtlijn 2016/680 de lidstaten biedt om een krachtens de AVG opgerichte toezichthoudende autoriteit aan te wijzen als toezichthoudende autoriteit voor de toepassing van deze richtlijn.

[34] Het gaat meer bepaald over de verwerking *van de* hits, zie hierover de overwegingen 42-58. Artikel 5, §1 van het ontwerp.

[35] Artikel 26 van het ontwerp bepaalt de samenstelling ervan.

[36] De artikelen 6 tot 10 van het ontwerp bepaalt de samenstelling ervan.

[37] Deze bevat een verbindingsofficier van de Dienst Vreemdelingenzaken, artikel 6, 3°, van het ontwerp, die onder het gezag staat van het hoofd van de sectie DVZ van de E.N.E. Deze opdracht wordt omschreven in artikel 30 van het ontwerp.

[38] Artikel 4 § 2, 4de lid van de WOG stelt :

« *De competenties, taken en bevoegdheden als toezichthoudende autoriteit voorzien door de Verordening 2016/79 worden, ten aanzien van de politiediensten in de zin van artikel 2,2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde*

20. Ook moet worden benadrukt dat het opstellen van de **ETIAS-observatielijst deel uitmaakt van de risicopreventiedoelstelling**[39]. Dit is een lijst met informatie die door Europol of de lidstaten is ingevoerd op basis van informatie over **terroristische misdrijven of andere ernstige strafbare feiten** - dit omvat ook verdachte personen[40, 41]. Deze lijst wordt automatisch verwerkt in het kader van de *screening* die is opgezet krachtens de ETIAS-verordening[42].

21. **In dit verband,. moet artikel 21 van het ontwerp worden aangepast in die zin dat het verwijst naar de repressieve doeleinden van ETIAS in plaats van het doel om veiligheidsrisico's te voorkomen. Hoewel de ETIAS-verordening op dit punt**[43] niet kristalhelder is, is de Autoriteit van mening dat de aanvrager er in het algemeen van uit kan gaan dat de bijdrage aan de ETIAS-observatielijst bijdraagt aan de beoordeling van aanvragen met betrekking tot veiligheidsrisico's en derhalve, onderworpen kan zijn aan de regels tot omzetting van Richtlijn 2016/680[44], met dien verstande dat, zoals zojuist is opgemerkt, de Gegevensbeschermingsautoriteit de toezichthoudende autoriteit is als bedoeld in de ETIAS-verordening, uitgezonderd voor de politiediensten. Met andere woorden, **artikel 21 van het ontwerp kan voorzien in de toepassing van titel 2 van de WVG «*met het oog op het beheer van de ETIAS-observatielijst*», op voorwaarde dat de Gegevensbeschermingsautoriteit de bevoegde toezichthoudende autoriteit is, behalve voor politiediensten**.

22. Ten slotte moet worden gezegd dat, hoewel de Autoriteit op grond van het Belgische positieve recht in beginsel niet bevoegd is om zich uit te spreken over de regels voor de verwerking van gegevens waarvoor **de inlichtingen- en veiligheidsdiensten** verantwoordelijk zijn, het ontwerp deze diensten in de ETIAS-verordening wil opnemen door hen de bevoegdheid te geven aanvragen op veiligheidsrisico's te beoordelen. **Zonder aanpassing van de Belgische wet zou de Gegevensbeschermingsautoriteit op basis van haar residuele bevoegdheid[45] , bevoegd zijn ten aanzien van gedetacheerde leden van de inlichtingen- en veiligheidsdiensten in het kader van de uit te voeren risicoanalyse** (in uitvoering van de gegevensbeschermingsregels van titel 2 van de WVG).

---

politie gestructureerd op twee niveaus, uitgeoefend door het Controleorgaan op de politionele informatie bedoeld in artikel 44/6, § 1, van de wet van 5 augustus 1992 op het politieambt ».

[39] Zie artikel 20, 4 van de ETIAS-verordening.

[40] Artikel 34, 3 van de ETIAS-verordening. De artikelen 34,3 en 35 van de ETIAS-verordening bepalen de **verantwoordelijkheden van de Lidstaten** (en Europol) ter zake.

[41] Zie artikel 34,2 van de ETIAS-verordening en voetnoot 52. Artikel 34, 2 van de ETIAS-verordening omschrijft de gegevens die in de lijst worden opgenomen (de naam, andere namen zoals eventuele pseudoniemen, e-mailadres, IP-adres, voornamen, nationaliteit, enz.).

[42] Zie overweging 45 en volgende.

[43] Artikel 56, 2 is niet rechtstreeks gericht op het bijdragen aan de observatieliljst.

[44] Zie artikel 31, § 2 van het ontwerp, dat titel 2 van de WVG toepasbaar maakt.

[45] Zie artikel 4, § 2, 2de lid van de WOG.

23. **In dit verband betwijfelt de Autoriteit of de ETIAS-verordening zou toestaan dat een deel van de gegevensverwerking waarop zij van toepassing is, wordt voorgelegd aan een toezichthoudende autoriteit die niet zou worden aangewezen bij de tenuitvoerlegging van de AVG of bij de omzetting van Richtlijn 2016/680, d.w.z. een autoriteit buiten de werkingssfeer van de Europese wetgeving.** Het doel van het ontwerp is om inlichtingen- en veiligheidsdiensten in staat te stellen in te grijpen in zaken die onder de bevoegdheid van de bevoegde autoriteiten vallen in de zin van Titel 2 van de WVG en Richtlijn 2016/680 - d.w.z. een **ander** *doel* dan het doel dat hun uitsluiting van de Europese wetgeving in het algemeen rechtvaardigt[46]. Welnu, artikel 42 van het ontwerp, dat in titel 3 van de WVG een nieuwe ondertitel 5 *bis* invoegt met als titel «*Bescherming van natuurlijke personen in verband met bepaalde verwerkingen van persoonsgegevens door de sectie van het Nationaal Crisiscentrum van de ETIAS Nationale Eenheid*», kent echter een bevoegdheid toe aan het Vast Comité I bedoeld in artikel 95 van de WVG, een autoriteit die naar Belgisch recht niet is aangewezen op grond van de voornoemde Europese regels inzake gegevensbescherming.

24. In deze omstandigheden lijkt **de Autoriteit te kunnen concluderen dat uit het bovenstaande** (in het bijzonder met betrekking tot de door de ETIAS-verordening[47]) **aangewezen toezichthoudende autoriteit) juridisch volgt dat de Gegevensbeschermingsautoriteit moet worden aangewezen als toezichthoudende autoriteit** op dit gebied (risicobeoordeling, met inbegrip van de ETIAS-observatielijst) - onverminderd de latere opmerkingen met betrekking tot de door inlichtingen- en veiligheidsdiensten nagestreefde doeleinden[48]. En dit, **tenzij de Belgische wetgever**, op dezelfde manier als hij heeft gedaan voor de politiediensten**, het Comité I aanwijst als de bevoegde Belgische autoriteit in toepassing van de AVG, voor de inlichtingen- en veiligheidsdiensten** (momenteel de verantwoordelijkheid van de Gegevensbeschermingsautoriteit)**, wanneer hun gegevensverwerking binnen de werkingssfeer van de AVG valt[49]**.

25. **De regels waaraan de inlichtingen- en veiligheidsdiensten volgens het ontwerp op dit gebied onderworpen zouden zijn, roepen ook vragen op**. Krachtens artikel 184/2 in ontwerp van de WVG (dat wordt ingevoegd door artikel 42 van het ontwerp), is deze van toepassing «*op de verwerkinng van persoonsgegevens van de gedetacheerden van de [VSSE] en de [ADIV] binnen de*

[46] Het ontwerp wil zelfs verder gaan, op een twijfelachtige manier, zie de overwegingen 95 e.v.

[47] Zie overweging 17.

[48] Zie de overwegingen 95-97.

[49] Ter herinnering: artikel 73 van de WVG bepaalt dat : «*Deze ondertitel is van toepassing op elke verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten en hun verwerkers, uitgevoerd in het kader van de opdrachten van deze diensten als bedoeld in artikelen 7 en 11 van de wet van 30 november 1998 alsook door of krachtens bijzondere wetten*». In wezen zijn de inlichtingen- en veiligheidsdiensten bij het uitvoeren van hun nationale veiligheidstaken onderworpen aan de Belgische regels inzake gegevensbescherming die niet voortvloeien uit de wetgeving van de Europese Unie. In dit kader is het Comité I de bevoegde toezichthoudende autoriteit, in overeenstemming met artikel 95 van de WVG.

sectie van het Nationaal Crisiscentrum van de E.N.E.», in het kader van de doeleinden bedoeld in artikel 14, § 1, 3° van het ontwerp, namelijk de raadpleging van ETIAS *voor repressieve doeleinden*. Om te beginnen merkt de Autoriteit op dat artikel 31, § 3, van het ontwerp en artikel 184/2, van de WVG zodanig moeten worden geherformuleerd dat de verwerkingsactiviteiten van gedetacheerde leden van de inlichtingen- en veiligheidsdiensten *wanneer zij risicobeoordelingen voor de NCC-sectie uitvoeren*, ook duidelijk worden geregeld.

26. Meer fundamenteel is de Autoriteit echter, gelet op wat zojuist is gezegd[50] en op artikel 66, 2, van de ETIAS-verordening[51], van mening dat **titel 2 van de WVG in beginsel mutatis mutandis van toepassing moet zijn, en niet een andere titel die voorziet in beperkte voorschriften *sui generis* voor de verwerking van persoonsgegevens**. Uit de ETIAS-verordening blijkt duidelijk dat de gegevensverwerking die op grond daarvan wordt verricht, moet voldoen aan de AVG of aan Richtlijn 2016/680. Overeenkomstig artikel 56, 2, tweede lid, van de ETIAS-verordening is dit laatste van toepassing op de veiligheidsrisicobeoordeling.

27. **Concluderend kunnen bovenstaande redeneringen als volgt worden samengevat met betrekking tot inlichtingen- en veiligheidsdiensten. Als de Belgische staat het Europese ETIAS-systeem wil uitbreiden tot zijn inlichtingen- en veiligheidsdiensten wanneer zij optreden voor de doeleinden van ETIAS, moet hij hen onderwerpen aan de toepasselijke Europese gegevensbeschermingsregels voor deze doeleinden, aangezien zij in dat geval optreden als bevoegde autoriteiten in de zin van Richtlijn 2016/680.** Enerzijds moet de activiteit van inlichtingendiensten op dit gebied *mutatis mutandis* worden onderworpen aan de regels van het Belgische recht tot omzetting van deze richtlijn (titel 2 van het WVG), aangezien risicobeoordeling (met inbegrip van de bijdrage aan de observatielijst) onderworpen is aan Richtlijn 2016/680 wanneer zij wordt uitgevoerd door de bevoegde autoriteiten. Met betrekking tot de bevoegde toezichthoudende autoriteit vereist de ETIAS-verordening dat dit de autoriteit is die is aangewezen in uitvoering van de AVG, wat voor deze diensten alleen de Gegevensbeschermingsautoriteit kan zijn. Tenzij de Belgische wetgever, op dezelfde manier als hij heeft gedaan voor de politiediensten, Comité I aanwijst als de Belgische bevoegde autoriteit zoals bedoeld in de AVG voor de inlichtingen- en veiligheidsdiensten, wanneer hun gegevensverwerking binnen het toepassingsgebied van de AVG valt[52].

II.1.2. <u>Repressieve doeleinden</u>

[50] Overwegingen 22-23.

[51] Zie overweging 29.

[52] Zie voetnoot 48.

28. Zoals aangekondigd, draagt ETIAS bij aan het voorkomen, opsporen en onderzoeken van terroristische misdrijven en andere ernstige strafbare feiten - hetzij de "**repressieve doeleinden**" van ETIAS[53].

29. De gegevensverwerking die in deze context wordt uitgevoerd, is onderworpen aan **Richtlijn 2016/680**[54]. Elke Lidstaat zorgt ervoor dat «*de wettelijke en bestuursrechtelijke bepalingen die overeenkomstig Richtlijn (EU) 2016/680 in het nationale recht zijn vastgesteld, ook gelden voor de toegang tot Etias door zijn nationale autoriteiten in overeenstemming met hoofdstuk X van deze verordening, mede met betrekking tot de rechten van de personen tot wier gegevens aldus toegang wordt verkregen*»[55].

30. En de krachtens artikel 41, 1, van Richtlijn 2016/680 aangewezen **toezichthoudende autoriteit** is bevoegd ter zake[56].

31. Nogmaals, wat betreft de rol die **inlichtingen- en veiligheidsdiensten**[57] op dit gebied zouden kunnen spelen, moeten deze diensten, zoals zojuist *mutatis mutandis* is opgemerkt, overeenkomstig de ETIAS-verordening worden onderworpen aan de regels van titel 2 van de WVG. Het is dan aan het ontwerp om ofwel het COC ofwel de Gegevensbeschermingsautoriteit als toezichthoudende autoriteit aan te wijzen. **Opdat Comité I de bevoegde toezichthoudende autoriteit op dit gebied zou zijn, zou de Belgische wetgever het moeten aanwijzen als de bevoegde autoriteit ten aanzien van inlichtingen- en veiligheidsdiensten wanneer zij optreden als bevoegde autoriteit in de zin van Richtlijn 2016/680 en ter uitvoering van artikel 41 daarvan[58]**. De ETIAS-verordening lijkt geen speelruimte te laten om andere toepasselijke regels en bevoegde toezichthoudende autoriteit toepasselijk te maken dan die welke voortvloeien uit de tenuitvoerlegging van Richtlijn 2016/680.

II.1.3. Andere doeleinden

32. ETIAS zal ook worden gebruikt door vervoersbedrijven[59], bevoegde grensautoriteiten[60] en immigratiediensten[61] om te controleren of de betrokken personen over de vereiste reisautorisatie beschikken - **met als doel DE TOEGANG TOT HET GRONDGEBIED TE CONTROLEREN**.

---

[53] Zie Hoofdstuk X van de ETIAS-verordening (artikels 50 e.v.). Zie de overwegingen 84 e.v.

[54] Artikel 56, 3 van de ETIAS-verordening.

[55] Artikel 66, 2 van de ETIAS-verordening (EG) .

[56] Artikel 66, 3 van de ETIAS-verordening.

[57] Zie overweging 96..

[58] Zie ook overweging 27..

[59] Zie Hoofdstuk VII van de ETIAS-verordening (artikelen 45 e.v.).

[60] Zie Hoofdstuk VIII van de ETIAS-verordening (artikelen 47 e.v.).

[61] Zie Hoofdstuk X van de ETIAS-verordening (artikels 49).

33. De verwerking van persoonsgegevens voor dit doel door deze overheidsinstanties is onderworpen aan de **AVG**[62].

34. Tot slot draagt ETIAS bij aan de doelstellingen van drie andere Europese informatiesystemen - **ONDERSTEUNINGSDOELEINDE**. Ten eerste ondersteunt het de **doelstellingen van het Schengeninformatiesysteem** (hierna «**het SIS**»)[63] genoemd) met betrekking tot bepaalde signaleringen van betrokkenen. Ten tweede ondersteunt het de doelstellingen van het «*Entry/Exit System*» hierna **EES** »)[64] (een geautomatiseerd EES-proces raadpleegt ETIAS om het inreis-/uitreisformulier of het weigeringsformulier aan te maken of bij te werken[65]). Ten derde draagt het, in combinatie met andere informatiesystemen, bij aan de correcte identificatie van individuen, in relatie tot « *Common Identity Repository* », hierna « **CIR** »)[66].

---

[62] Artikel 56, 2, 1ste lid van de ETIAS-verordening.

[63] Zie de volgende Europese verordeningen:

Verordening (EU) 2018/2018 van het Europees Parlement en de Raad van 28 november 2018 *betreffende het gebruik van het Schengeninformatiesysteem voor de terugkeer van illegaal verblijvende onderdanen van derde landen* ;

Verordening (EU) 2018/1861 van het Europees Parlement en de Raad van 28 november 2018 *betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van grenscontroles, tot wijziging van de Overeenkomst ter uitvoering van het Akkoord van Schengen en tot wijziging en intrekking van Verordening (EG) nr. 1987/2006* ;

Verordening (EU) 2018/1862 van het Europees Parlement en de Raad van 28 november *2018 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van politiële en justitiële samenwerking in strafzaken, tot wijziging en intrekking van Besluit 2007/533/JBZ van de Raad en tot intrekking van Verordening (EG) nr. 1986/2006 van het Europees Parlement en de Raad en Besluit 2010/261/EU van de Commissie*.

Volgens artikel 4, e) van de ETIAS-**verordening**, het betreft deze **signaleringen**: «*de SIS-doelstellingen ondersteunen die betrekking hebben op signaleringen van onderdanen van derde landen aan wie de inreis en het verblijf is geweigerd, signaleringen van personen die met het oog op aanhouding ten behoeve van overlevering of uitlevering worden gezocht, signaleringen van vermiste personen, signaleringen van personen die worden gezocht met het oog op hun medewerking in het kader van een gerechtelijke procedure, signaleringen van personen die discreet of gericht moeten worden gecontroleerd en signaleringen van onderdanen van derde landen jegens wie een terugkeerbesluit is uitgevaardigd* ».

Over **SIS**, zie : https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/what-sis-and-how-does-it-work_en, laatst bekeken op 27/06/2023.

Zie het **advies van de Autoriteit** van 1 juli 2022 *over een voorontwerp van wet betreffende de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van politiële en justitiële samenwerking in strafzaken, op het gebied van grenscontroles en voor de terugkeer van illegaal verblijvende onderdanen van derde landen* [SIS-wet] (CO-A-2022-125).

Advies **nr. 7/2017 van het EDPB** *over het nieuwe rechtskader van het Schengeninformatiesysteem, 2 mei* 2017.

[64] Zie de verordening (EU) 2017/2226 van het Europees Parlement en de Raad van 30 *november 2017 tot instelling van een inreis-uitreissysteem (EES) voor de registratie van inreis- en uitreisgegevens en van gegevens over weigering van toegang ten aanzien van onderdanen van derde landen die de buitengrenzen overschrijden en tot vaststelling van de voorwaarden voor toegang tot het EES voor rechtshandhavingsdoeleinden en tot wijziging van de overeenkomst ter uitvoering van het te Schengen gesloten akkoord en Verordeningen (EG) nr. 767/2008 en (EU) nr. 1077/2011*.

Zie **het advies van de Autorieit 122/2022** van 1 *juli 2022 met betrekking tot een voorontwerp van wet tot wijziging van de wet van verblijf, de vestiging en de verwijdering van vreemdelingen, wat betreft het inreis-uitreissysteem (CO-A-2022-138)*.

[65] Artikel *11* van de ETIAS-verordening. Zie ook artikel 11*quater* van de ETIAS-verordening (intrekking van een reisautorisatie door de aanvrager).

[66] Het betreft het register als vastgesteld in artikel 17.1 van de verordening (EU) 2019/817 van het Europees Parlement en de Raad van 20 mei 2019 *tot vaststelling van een kader voor interoperabiliteit tussen de Unie-informatiesystemen op het gebied van grenzen en visa en tot wijziging van Verordeningen (EG) nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 en (EU) 2018/1861 van het Europees Parlement en de Raad, Beschikking 2004/512/EG van de Raad en Besluit 2008/633/JBZ van de Raad* (hierna de **interoperabiliteit-verordening** »).

Zie **EPDS, advies 4/2018** *sur les propositions de deux règlements portant établissement d'un cadre pour l'interopérabilité des systèmes d'information à grande échelle de l'UE*, 16 april 2018.

Volgens artikel 17, 1 van de interoperabiliteit-verordening:

« *Er wordt een gemeenschappelijk identiteitsregister (common identity repository - CIR) ingesteld, waarin voor elke in het EES, VIS, Etias, Eurodac of ECRIS-TCN geregistreerde persoon een afzonderlijk bestand met de in artikel 18 bedoelde gegevens wordt aangelegd, met als doel de correcte identificatie van in het EES, VIS, Etias, Eurodac of ECRIS- TCN geregistreerde*

II.2. <u>SCREENING EN REISAUTORISATIE</u>

35. De ETIAS-verordening stelt een geautomatiseerd screeningproces in dat tot doel heeft een reisautorisatie af te geven of te weigeren.

36. Als onderdeel van zijn werking en om geautomatiseerde controles mogelijk te maken, is het ETIAS-**informatiesysteem interoperabel met vijf andere EU-informatiesystemen,** namelijk : de reeds genoemde systemen **SIS** en **EES**, het visuminformatiesysteem (hierna «**VIS** »)[67], **Eurodac**[68]»

<u>personen te vergemakkelijken</u> en te bevorderen overeenkomstig artikel 20, de werking van de MID te ondersteunen overeenkomstig artikel 21 en de toegang van aangewezen autoriteiten en Europol tot het EES, VIS, ETIAS en Eurodac te vergemakkelijken en te stroomlijnen wanneer dat nodig is voor de preventie, de opsporing of het onderzoek van terroristische misdrijven of andere ernstige strafbare feiten overeenkomstig artikel 22» (onderstreept door de Autoriteit).

De **CIR** bestaat uit een centrale infrastructuur die in de plaats komt van de centrale systemen van respectievelijk het EES, VIS, Etias, Eurodac en ECRIS-TCN, voor zover de in artikel 18 bedoelde gegevens in deze centrale infrastructuur worden opgeslagen. Het voornoemd artikel 18, 1 bepaalt het volgende:

« *1. In het CIR worden de volgende gegevens – logisch gescheiden – opgeslagen per informatiesysteem waaruit de gegevens afkomstig zijn:*

a) de gegevens bedoeld in artikel 16, lid 1, onder a) tot en met d), artikel 17, lid 1, onder a), b) en c) en artikel 18, leden 1 en 2, van Verordening (EU) 2017/2226 [(de EES-verordening)];

b) de gegevens bedoeld in artikel 9, punt 4, onder a) tot en met c), en de punten 5 en 6 van Verordening (EG) nr. 767/2008 [(de VIS-verordening)];

c) de gegevens bedoeld in artikel 17, lid 2, onder a) tot en met e), van Verordening (EU) 2018/1240 [(de ETIAS-verordening)]

Aritkel 6, 2 *bis* van de ETIAS-verordening betreft de technische infrastructuur van het ETIAS-informatiesysteem *en bepaalt «Het CIR bevat de identiteitsgegevens en reisdocumentgegevens. De overige gegevens worden opgeslagen in het centrale systeem* ».

Deze persoonsgegevens zijn de volgende: achternaam (familienaam), voorna(a)m(en) (bijnamen), naam bij geboorte; geboortedatum, geboorteplaats, geslacht, huidige nationaliteit; geboorteland, voorna(a)m(en) van de ouders van de aanvrager ; andere namen (pseudoniem(en), artiestennaam/-namen, gebruikelijke naam/namen), indien van toepassing ; andere nationaliteiten, indien van toepassing; type reisdocument, nummer en land van uitgifte van dit document ; datum van uitgifte van het reisdocument en vervaldatum van de geldigheid ervan.

Het CIR bevat ook **gegevens uit het persoonsdossier van onderdanen van derde landen die zijn vrijgesteld van de visumplicht** en die zijn aangemaakt door de grensautoriteit (de grenswacht die naar nationaal recht verantwoordelijk is voor het uitvoeren van grenscontroles in de zin van artikel 2, punt 11, van Verordening (EU) 2016/399) en waarnaar wordt verwezen in artikel 17 van de EES-verordening, waaronder de gezichtsopname en vingerafdrukgegevens van de rechterhand.

[67] Zie Verordening (EG) nr. 767/2008 van 9 juli 2008 *betreffende het Visuminformatiesysteem (VIS) en de uitwisseling tussen de lidstaten van gegevens op het gebied van visa voor kort verblijf (VIS-verordening)*.

Onder andere met betrekking tot **VIS**, « *The Visa Information System (VIS) allows Schengen States to exchange visa data. VIS connects consulates in non-EU countries and all external border crossing points of Schengen States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area.*

The system helps avoid 'visa shopping', supports documenting and prevents irregular migration. It can perform biometric matching, primarily of fingerprints, for identification and verification purposes and assists the authorities protecting the internal security of Member States », zie https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Vis, laatst geraadpleegd op 27/06/2023.

[68] Zie Verordening (EU) nr. 603/2013 van het Europees Parlement en van de Raad van 26 juni 2013 *betreffende de instelling van „Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van Verordening (EU) nr. 604/2013 tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend en betreffende verzoeken van rechtshandhavingsinstanties van de lidstaten en Europol om vergelijkingen van Eurodac-gegevens ten behoeve van rechtshandhaving, en tot wijziging van Verordening (EU) nr. 1077/2011 tot oprichting van een Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht*.

Met name, **Eurodac** « *is a large-scale IT system that helps with the management of European asylum applications since 2003, by storing and processing the digitalized fingerprints of asylum seekers and irregular migrants who have entered a European*

genoemd) en het Europees Strafregister Informatiesysteem voor onderdanen van derde landen (hetzij « *European Criminal Records Information System - Third Country Nationals»* , hierna genoemd «**ECRIS-TCN** »)[69].

37. Het ETIAS-systeem voert ook geautomatiseerde controles uit door **Europol-gegevens op te vragen**[70].

38. Het centrale ETIAS-systeem raadpleegt ook **twee databanken van Interpol**[71]: namelijk, de Gegevensbank gestolen en verloren reisdocumenten (hetzij « *Stolen and Lost Travel Documents Database* », hierna « **SLTD** »)[72] en de Gegevensbank reisdocumenten vergezeld van berichten (hetzij « *Travel Documents Associated With Notices* », hierna « **TDAWN** »).

39. Het geautomatiseerde screeningsproces werkt als volgt.

II.2.1. Formulier ingevuld door de betrokken persoon

40. De aanvrager, de betrokkene, moet **elektronisch een formulier invullen** met een reeks persoonsgegevens (naam, geboortenaam, voornamen, nationaliteit, opleiding, voornamen van de ouders, beroep uit een vooraf opgestelde lijst, antwoorden op vragen over met name strafrechtelijke

country. In this way, the system helps to identify new asylum applications against those already registered in the database », https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Eurodac, dernièrement consulté le 27/06/2023.

[69] Verordening (EU) 2019/816 van het Europees Parlement en de Raad van 17 april 2019 *tot invoering van een gecentraliseerd systeem voor de vaststelling welke lidstaten over informatie beschikken inzake veroordelingen van onderdanen van derde landen en staatlozen (Ecris-TCN) ter aanvulling van het Europees Strafregisterinformatiesysteem en tot wijziging van Verordening (EU) 2018/1726*.

Aangaande **ECRIS-TCN**, met name, « *The European Criminal Records Information System (ECRIS), operational since April 2012, provides an electronic exchange of criminal record information on a decentralised basis between Member States. It allows Member State's criminal records authorities to obtain complete information on previous convictions of EU nationals from the Member State of that person's nationality. ECRIS-TCN, once set up, will be a centralised system that allows Member State's authorities to identify which other Member States hold criminal records on the third country nationals or stateless persons being checked, so that they can then use the existing ECRIS system to address requests for conviction information only to the identified Member States* », zie https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Ecris-Tcn, laatst geraadpleegd op 27/06/2023.

[70] Als volgt gedefinieerd in artikel 3, 1, 17 van de ETIAS-verordening « *persoonsgegevens die door Europol worden verwerkt voor het in artikel 18, lid 2, onder a), van Verordening (EU) 2016/794 vermelde doel*» van het Europees Parlement en de Raad van 11 mei 2016 *betreffende het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol) en tot vervanging en intrekking van de Besluiten 2009/371/JBZ, 2009/934/JBZ, 2009/935/JBZ, 2009/936/JBZ en 2009/968/JBZ van de Raad*. Deze bepaling verwijst naar het doel van de gegevensverwerking door Europol, namelijk het uitvoeren van :

« *het uitvoeren van kruiscontroles om connecties op te sporen of andere relevante verbanden met betrekking tot:*

i) personen die worden verdacht van het plegen van of deelnemen aan een strafbaar feit dat onder de bevoegdheid van Europol valt, of die voor een dergelijk strafbaar feit veroordeeld zijn;

personen ten aanzien van wie er feitelijke aanwijzingen zijn of een redelijk vermoeden bestaat dat zij strafbare feiten zullen plegen die onder de bevoegdheid van Europol vallen ».

[71] Zie artikel 12 van de ETIAS-verordening.

[72] Zie https://www.interpol.int/How-we-work/Databases/SLTD-database-travel-and-identity-documents,

laatst geraadpleegd op 27/06/2023.

veroordelingen voor een reeks terroristische misdrijven of misdrijven die in de bijlage zijn opgenomen, enz.[73]; het systeem verzamelt ook het IP-adres dat de aanvrager gebruikt).

41. In dit verband merkt de Autoriteit terloops op dat in de memorie van toelichting bij het ontwerp wordt bevestigd da**t ETIAS informatie over betrokkenen verzamelt die niet vereist is voor visumaanvragen**[74]. In het algemeen roept dit vragen op over het gelijkheidsbeginsel, dat echter voortvloeit uit de ETIAS-verordening zelf[75].

II.2.2. Geautomatiseerde verwerkingen

42. Na een ontvankelijkheidsanalyse[76] worden de verstrekte persoonsgegevens vervolgens **geautomatiseerd verwerkt voor verificatie door het centrale ETIAS-systeem**, op zoek naar "**hits**" (d.w.z. overeenkomsten)[77], overeenkomstig de artikelen 20 en 23 van de ETIAS-verordening.

Geautomatiseerde verwerkingen artikel 20 (algemeen)

43. **Vergelijking met andere databanken** - Het centrale systeem van ETIAS zoekt naar overeenkomsten via het Europese zoekportaal (hetzij *"European Search Portal"*, hierna« **"ESP"** »)[78]

---

[73] Zie artikel 17 van de ETIAS-verordening.

[74] « *ETIAS verzamelt gegevens die vergelijkbaar zijn met wat momenteel voor visa geldt. De volgende gegevens worden echter alleen verzameld in het kader van een aanvraag voor reisautorisatie: de andere nationaliteiten van de aanvrager, geboorteland en voornamen van de ouders van de aanvrager, e-mailadres, telefoonnummer indien beschikbaar, opleiding, adres van het eerste verblijf indien beschikbaar, de persoonsgegevens van een burger van de Unie op wie Richtlijn 2004/38/EG van toepassing is of van een onderdaan van een derde land die een recht van vrij verkeer geniet dat gelijkwaardig is aan het recht van vrij verkeer voor burgers van de Unie op grond van een overeenkomst tussen de Unie en haar lidstaten, enerzijds, en een derde land, anderzijds, waarmee de aanvrager verbonden is overeenkomstig artikel 2, lid 1, c), van de ET/AS-verordening; de gegevens van de tussenpersoon die de aanvraag voor de aanvrager invult, de in artikel 17, lid 4, van de ETIASverordening genoemde aanvullende vragen of het door de aanvrager bij de aanvraag gebruikte IPadres »* (onderstreept door de Autoriteit) (Memorie van Toelichting van het ontwerp, blz. 2).

[75] In zijn advies (overweging 16)« *CEDP se demande si la proposition ne crée pas un régime plus intrusif pour les voyageurs exemptés de l'obligation de visa que pour ceux soumis à l'obligation de visas dès lors que davantage de données seront centralisées au niveau de l'Union européenne dans l'ETIAS*[…] *que dans le VIS* ».

[76] Zie artikel 19 van de ETIAS-verordening.

Opmerking: Screening (geautomatiseerde verwerking en, indien van toepassing, handmatige verwerking zoals hieronder beschreven) wordt ook uitgevoerd als een reisautorisatie wordt gewijzigd naar aanleiding van een verzoek van de aanvrager (betrokkene) om zijn **rechten uit te oefenen**, overeenkomstig artikel 64.2 van de ETIAS-verordening.

[77] Artikel 3, 1, 14 van de ETIAS-verordening definieert een hit als volgt:

« *het bestaan van een overeenstemming die wordt geconstateerd door vergelijking van de in een aanvraagdossier van het centrale Etias-systeem opgenomen persoonsgegevens met de in artikel 33 vermelde specifieke risico-indicatoren of met de persoonsgegevens in een notitie, dossier of signalering in het centrale Etias-systeem, in een ander informatiesysteem van de Unie of in een in artikel 20, lid 2, vermelde databank („EU-informatiesystemen"), inEuropol-gegevens of in een Interpol-databank die worden doorzocht door het centrale Etias-systeem*» (onderstreept door de Autoriteit).

[78] **ESP is opgericht met artikel 6 van de interoperabiiteitverordening. Punt 1. lid van dit artikel bepaalt:**

« *Er wordt een Europees zoekportaal (European search portal - ESP) ingesteld om ervoor te zorgen dat de lidstatelijke autoriteiten en de -Unie-agentschappensnel, ononderbroken, efficiënt, systematisch en gecontroleerd toegang hebben tot de Unie-informatiesystemen, de Europol-gegevens en de Interpol-databanken die zij nodig hebben om hun taken te verrichten overeenkomstig hun toegangsrechten en de doelstellingen van het EES, VIS, Etias, Eurodac, SIS en ECRIS-TCN*». Het ESP omvat een centrale infrastructuur met een zoekportaal waarmee gelijktijdig EES-, VIS-, ETIAS-, Eurodac-, SIS-, ECRIS-TCN-, Europol- en Interpolgegevensbanken kunnen worden geraadpleegd. Het is ontwikkeld door eu-LISA, dat ook verantwoordelijk is voor het technisch beheer.

met gegevens uit de volgende systemen : ETIAS zelf, SIS[79], EES, VIS, Eurodac, ECRIS-TCN, Europol-gegevens en de SLTD- en TDAWN-databanken[80].

44. **Een vraag bevestigend beantwoorden en geen huisadres opgeven - Het centrale systeem controleert of de aanvrager een of meer vragen op het formulier bevestigend heeft beantwoord en of de aanvrager een stad en land van verblijf heeft opgegeven in plaats van een huisadres**[81].

45. **Vergelijking met de ETIAS observatielijst - Gegevens worden vergeleken met de ETIAS observatielijst**[82].

46. De artikelen 21 tot en met 25 van het ontwerp regelen de ETIAS-observatielijst, die kan worden aangevuld door de **politiediensten**, de Veiligheid van de Staat (hierna "**VSSE**" genoemd), de Algemene Dienst Inlichting en Veiligheid van de Strijdkrachten (hierna "**ADIV**" genoemd) en de Algemene Administratie der Douane en Accijnzen (hierna "**AGD&A**" genoemd) »)[83].

47. Met betrekking tot de **voeding van de ETIAS-observatielijst** beperkt het ontwerp zich tot een verwijzing naar de voorwaarden in artikel 34 van de ETIAS-verordening en naar de mogelijkheid[84] voor de betrokken autoriteiten om gegevens in te voeren. In deze context heeft de Autoriteit de aanvrager bevraagd over de omstandigheden (en regels), in het bijzonder met het oog op het risico van discriminatie, waarin de betrokken autoriteiten zullen bijdragen aan de ETIAS-observatielijst. Hij antwoordde het volgende (de Autoriteit vertaalt:

> « *Artikel 34, §1, bepaalt dat de betrokken autoriteiten, de personen die ervan worden verdacht een strafbaar feit te hebben gepleegd of aan een strafbaar feit te hebben deelgenomen en/of personen ten aanzien van wie er reden is om aan te nemen dat zij een strafbaar feit zouden kunnen plegen, moeten hebben geïdentificeerd op basis van hun eigen informatie. Artikel 22 van het ontwerp verwijst ook naar artikel 35, §1, van de verordening, waarin de voorwaarden worden genoemd waaraan moet worden voldaan voordat gegevens kunnen worden ingevoerd.*

[79] Voor bepaalde signaleringen: niet-toelating en verblijfsverbod of arrestatie (aanhoudingsbevel of uitlevering).

[80] Artikelen 20, 2, van de ETIAS-verordening. Zie ook artikel 11 van de ETIAS-verordening, dat voorziet in geautomatiseerde controles tussen interoperabele systemen.

[81] Artikel 20, 3 van de ETIAS-verordening.

[82] Zie artikel 20,4 van de ETIAS-verordening en overweging 19..

[83] Artikel 21 van het ontwerp.

[84] Artikel 21 van het ontwerp stelt duidleijk dat de *betrokken diensten* «kunnen gegevens invoeren in de ETIAS-observatielijst».

Er is een EU-uitvoeringshandeling gepland dat een kader zal bieden waarmee de logging en de veiligheid van de verwerkingen in verband met de observatielijst worden gewaarborgd.

Artikel 14 van de ETIAS-verordening voorziet in de naleving van het non-discriminatiebeginsel bij alle verwerkingen in het ETIAS-informatiesysteem (met inbegrip van de observatielijst).

De ETIAS-screeningsraad (art. 9 van de Verordening) en de Sturingsraad voor de Grondrechten (art. 10 van de Verordening) zien toe op de naleving van dit beginsel, in het bijzonder met betrekking tot de tenuitvoerlegging van de observatielijst (art. 9, §2, b)). ».

48. De Autoriteit neemt akte van deze uitleg. Zij merkt echter op dat de ETIAS-screeningsraad door de lidstaten wordt geraadpleegd over de tenuitvoerlegging van de observatielijst en dat zij (met name) adviezen, richtsnoeren, aanbevelingen en beste praktijken op dit gebied uitbrengt[85]. De ETIAS-verordening stelt een verdenkingsdrempel vast waarboven een persoon aan de ETIAS-observatielijst kan worden gemeld, maar **bepaalt niet onder welke voorwaarden de betrokken autoriteiten een persoon aan de ETIAS-observatielijst moeten melden. Volgens de Autoriteit is dit noodzakelijk** in het licht van het voorspelbaarheids- en rechtmatigheidsbeginsel van artikel 22 van de Grondwet en artikel 8 van het EVRM, en om het risico van discriminatie van de betrokken personen te beperken. Het ontwerp moet dienovereenkomstig worden aangepast.

49. **Vergelijking met specifieke risico-indicatoren - Met behulp van een profileringsalgoritme (ETIAS-screeningsregels**)[86] wordt een reeks gegevens vergeleken met specifieke risico-indicatoren[87]. In dit verband vereist de informatie-input, **door de lidstaten van de Europese Commissie met het oog op de vaststelling van specifieke risico-indicatoren,** als bedoeld in artikel 33, lid 2, van de ETIAS-verordening, de verwerking van persoonsgegevens en zal dit uiteindelijk gevolgen hebben voor de verwerking van gegevens over de bij ETIAS betrokken personen.

50. De manier waarop risico-indicatoren zullen worden vastgesteld is des te belangrijker en dat, zoals de EDPS heeft opgemerkt, ondanks de algemene bepaling van de ETIAS-verordening die gericht is op het bestrijden van discriminatie op basis van bepaalde categorieën gegevens[88] en het verbod om specifieke risico-indicatoren te baseren op bepaalde categorieën gegevens (de Autoriteit vertaalt)[89] :

---

[85] Artikel 9, 4 van de ETIAS-verordening.

[86] ARtikel 20, 5 van de ETIAS-verordening.

[87] Zie voor deze risico's overweging 12, eerste streepje (risicopreventiedoel van ETIAS). Artikel 33 van de ETIAS-verordening bepaalt wat de ETIAS-screeningsregels zijn en hoe ze moeten worden opgesteld. De Commissie zal een gedelegeerde handeling vaststellen om de specifieke risico's in kwestie te specificeren, met name op basis van statistieken en informatie, gestaafd door feitelijke en concrete elementen, die door de lidstaten worden verstrekt. Op basis van de specifieke risico's stelt de centrale eenheid van ETIAS een reeks specifieke risico-indicatoren vast die bestaan uit een combinatie van de gegevens als bedoeld in artikel 33, lid 4, van de ETIAS-verordening.

[88] Zie artikel 14 van de ETIAS-verordening.

[89] Artikel 33, 5 van de ETIAS-verordening bepaalt:

> « *De EDPS wenst te benadrukken dat, hoewel de risico-indicatoren niet rechtstreeks zullen worden gedefinieerd op basis van de eerste bovengenoemde criteria, het resultaat waarschijnlijk zeer vergelijkbaar zal zijn met het resultaat dat zou worden verkregen door deze te gebruiken. Op basis van informatie zoals nationaliteit en woonplaats, vooral in combinatie met andere gegevens, is het mogelijk om een vrij nauwkeurig beeld te vormen van het ras of de etnische afkomst van een aanvrager. Evenzo kunnen risico-indicatoren niet worden gebaseerd op vakbondslidmaatschap, maar kunnen ze worden gedefinieerd op basis van informatie over het huidige beroep. Deze twee soorten informatie zijn zeer nauw met elkaar verbonden en daarom kan profilering op deze basis het risico op discriminatie niet echt voorkomen* »[90].

51. Op dit punt en in vergelijkbare zin heeft de Autoriteit er al op gewezen dat de verwerking van het nationale gegeven kan worden beschouwd als een verwerking van bijzondere categorieën gegevens als bedoeld in artikel 9 van de AVG[91].

52. De Autoriteit vroeg de aanvrager naar de regels voor de verwerking van persoonsgegevens. Hij antwoordde het volgende (de Autoriteit vertaalt):

> « *Wij gaan ervan uit dat de vraag betrekking heeft op de informatie die de lidstaten moeten verstrekken en waarnaar wordt verwezen in artikel 33, §2, punten d), e) en f).*[92]*.*
>
> *Deze informatie moet worden verstrekt door de bevoegde autoriteiten voor elk type risico :*
> *voor punt d) Fedpol, douane, inlichtingen- en veiligheidsdiensten ;*
> *voor punt e) Dienst Vreemdelingenzaken ;*
> *voor punt f) FOD Volksgezondheid.*
>
> *De wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens (hierna " wet van 2018 ") en mogelijk andere specifieke regels inzake gegevensbescherming die van toepassing zijn op de betrokken autoriteiten*

« *De specifieke risico-indicatoren zijn gericht en evenredig. Zij mogen in geen geval uitsluitend gebaseerd zijn op geslacht of leeftijd. Zij mogen in geen geval gebaseerd zijn op informatie waaruit huidskleur, ras, etnische of sociale afkomst, genetische kenmerken, taal, politieke of andere denkbeelden, godsdienst of levensbeschouwelijke overtuiging, lidmaatschap van een vakvereniging, het behoren tot een nationale minderheid, vermogen, geboorte, handicap, of seksuele geaardheid af teleiden zijn* ».

[90] Advies EPDS, overweging 40.

[91] Zie het advies 211/2022 van 9 september 2022 *over een ontwerp van Koninklijk besluit houdende de wijziging van het koninklijk besluit van 22 februari 2017 houdende oprichting van de Federale Overheidsdienst Beleid en Ondersteuning (CO-A-2022-187)*.

[92] Wat correct is.

bieden een kader voor de gegevensverwerking dat hen in staat stelt deze informatie te verstrekken.

Artikel 31 van het ontwerp voorziet in de toepassing van de wet van 2018 in verband met risicobeoordeling ».

53. De Autoriteit vestigt de aandacht van de aanvrager op het feit dat het hier niet gaat om een risicobeoordeling (in de context van specifieke autorisaties), maar om een bijdrage aan de identificatie van risico's die moeten worden voorkomen via de ETIAS-screeningssregels, waarbij andere gegevensverwerkingsactiviteiten betrokken zijn die ook onder het ontwerp moeten vallen. **In het dispositief moeten daarom de essentiële elementen van deze gegevensverwerking worden vastgelegd, in het bijzonder de (categorieën van) gegevens die worden verwerkt en de overheidsinstanties die verantwoordelijk zijn voor deze gegevensverwerking**.

Geautomatiseerde verwerkingen artikel 23 (SIS bijzonder)

54. **Vergelijking met SIS voor een deel van de signaleringen** [93]- Het centrale systeem van ETIAS voert een zoekopdracht uit via ESP om een vergelijking te maken met bepaalde signaleringsgegevens in het SIS.

Geen hit

55. Aan het einde van deze geautomatiseerde verwerking **wordt de reisautorisatie automatisch afgegeven als er geen hit** is[94].

II.2.3. <u>Hits en manuele verwerking</u>

[93] Vermiste personen, personen die gezocht worden in verband met gerechtelijke procedures of voor discrete controles (enz.).
[94] Artikel 21, 1 van de ETIAS-verordening.

56. Als er **een of meer hits** zijn bij de geautomatiseerde verwerkingen op grond van artikel 20 (algemeen)[95, 96], voert de centrale eenheid van ETIAS **controles uit**[97]. Bij een valse hit uitslag wordt automatisch een reisautorisatie afgegeven.

57. Als de controles positief zijn of als er twijfel bestaat over de identiteit van de aanvrager, **wordt de aanvraag handmatig verwerkt overeenkomstig artikel 26 van de ETIAS-verordening door de verantwoordelijke nationale ETIAS-eenheid**[98]. Het gaat hier bijvoorbeeld over de lidstaat die als enige de gegevens heeft ingevoerd of verstrekt die tot een hit hebben geleid. In dit geval hebben de nationale ETIAS-eenheden ook toegang tot gegevens van andere EU-informatiesystemen als bedoeld in artikel 25 bis van de ETIAS-verordening, en in bepaalde omstandigheden kan de aanvrager om aanvullende informatie of documenten worden gevraagd en in nog beperktere omstandigheden kan een onderhoud worden geregeld[99]. Tot slot wordt, als meerdere lidstaten gegevens hebben doorgegeven die een hit hebben uitgelokt, een overlegprocedure georganiseerd tussen deze lidstaten en de nationale ETIAS-eenheid van de verantwoordelijke lidstaat[100].

Beoordeling van de risico's

58. De handmatige verwerking door de verantwoordelijke nationale ETIAS-eenheid[101] leidt in de meeste gevallen tot een beslissing tot weigering of reisautorisatie [102] na **een door haar uitgevoerde risicobeoordeling**[103] , of zelfs, in geval van weigering, wanneer een geraadpleegde nationale ETIAS-eenheid van een lidstaat een met redenen omkleed negatief advies heeft uitgebracht (in dat geval is

---

[95] Artikel 21, 2 van de ETIAS-verordening.

[96] Indien er een of meer hits zijn voor de geautomatiseerde verwerkingen **van artikel 23 (met name het SIS)**, voert de centrale ETIAS-eenheid ook controles uit en indien de hit wordt bevestigd, wordt een **kennisgeving gestuurd naar** (« het **SIRENE**-bure*au (Supplementary Information Request at the National Entries*) van de signalerende lidstaat. Een dergelijke kennisgeving wordt ook verstuurd als een handmatige verwerking is **gestart na geautomatiseerde verwerkingen op grond van artikel 20 (algemeen)**.

Aangaande het SIRENE-bureau, zie artikel 7 van de Verordening (EU) 1986/2006 van het Europees Parlement en de Raad van 28 november 2018 betreffende de instelling, de werking en het gebruik *van het Schengeninformatiesysteem (SIS) op het gebied van politiële en justitiële samenwerking in strafzaken, tot wijziging en intrekking van Besluit 2007/533/JBZ van de Raad en tot intrekking van Verordening (EG) nr. 1986/2006 van het Europees Parlement en de Raad en Besluit 2010/261/EU van de Commissie.* In België betreft dit de "Sirene Commissie Federale Politie — Directie van de internationale politiesamenwerking (GGI)", zie document C2023/085/02, Lijst van N.SIS-instanties en nationale Sirene-bureaus, PB, *C*, , 85 van 7.3.2023, blz. 299-308, raadpleegbaar op https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:C:2023:085:FULL,

laatst geraadpleegd op 28/06/2023, en artikel 5 van de wet van 2 maart *2023 betreffende de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van politiële en justitiële samenwerking in strafzaken, grenscontroles en de terugkeer van onderdanen van derde landen die illegaal op het grondgebied van de lidstaten verblijven*.

[97] Voorzien in artikel 22 van de ETIAS-verordening.

[98] Artikel 25 van de ETIAS-verordening identificeert de verantwoordelijke Lidstaat, al naargelang het geval.

Het commentaar bij de artikelen van het ontwerp (blz. 11) stelt het volgende «*alle gegevens die in een Europese databank worden ingevoerd komen echter uit een "bron"-databank, die in feite een nationale databank is* ».

[99] Zie artikel 27 van de ETIAS-verordening.

[100] Zie artikel 28 van de ETIAS-verordening. Er bestaat een soortgelijke procedure wanneer de betrokken gegevens afkomstig zijn van Europol, zie artikel 29 van de ETIAS-verordening.

[101] Artikel 26 van de ETIAS-verordening.

[102] Voor gevallen waarin een weigering moet worden afgegeven zonder risicobeoordeling, zie artikel 26, 3. a), 3,*bis*, a),

[103] Zie artikel 26,3, b), 3bis, *b*), 4, 5 en 6 van de ETIAS-verordening.

het die andere lidstaat[104] die de risico's heeft beoordeeld). De **beslissing** over de aanvraag moet worden genomen binnen een bijzonder korte termijn, in principe: **96 uur** vanaf de datum van ontvankelijkheid van de aanvraag[105].

59. Volgens het ontwerp wordt binnen de Belgische E.N.E. een met redenen omkleed advies over de beoordeling van **VEILIGHEIDSRISICO'S** en **hoge epidemiologische RISICO's** opgesteld door «***gedetacheerde leden*** »[106] van de betrokken diensten (politiediensten, de FOD Volksgezondheid, de VSSE, de ADIV en de AGD&A)[107] die verslag uitbrengen aan de **Sectie NCC**[108], en die daartoe «*toegang hebben tot de nodige databanken tot de door zijn eigen dienst beheerde databanken*» (onderstreept door de Autoriteit)[109], en in deze context onder het gezag staan van de leidende ambtenaar[110]. Dit roept de volgende twee opmerkingen op.

60. Ten eerste vroegde Autoriteit de aanvrager te bevestigen dat de **risicobeoordelingen** die door de gedetacheerde leden van de NCC-sectie zijn uitgevoerd, inderdaad door hen zijn uitgevoerd **onder het gezag van de leidende ambtenaar (**voor wat betreft de uitvoering van de taken van de E.N.E.). De aanvrager heeft dat bevestigd.

61. Ten tweede is de Autoriteit van mening dat het ontwerp, door te verwijzen naar de *«nodige databanken»*, **niet voldoet aan het voorspelbaarheids - en rechtmatigheidsbeginsel** die zijn vastgelegd in artikel 8 EVRM en artikel 22 van de Grondwet: de oorspronkelijk door deze diensten verwerkte (categorieën) gegevens die vervolgens worden verwerkt voor de doeleinden van de ETIAS-verordening, kunnen niet worden geïdentificeerd. In het ontwerp moet worden **aangegeven welke gegevensbanken moeten worden geraadpleegd door te verwijzen naar hun rechtsgrondslag en welke (categorieën) persoonsgegevens uit deze gegevensbanken mogen worden hergebruikt voor de doeleinden van de ETIAS-verordening** . Deze aanpassing maakt het ook mogelijk de taken van deze andere overheidsinstanties **vast te stellen in verband waarmee de verzamelde gegevens (en welke gegevens) kunnen worden hergebruikt voor ETIAS-doeleinden**. Bij gebrek aan verduidelijking op dit gebied is het voor de Autoriteit ook

---

[104] Zie artikel 28 van de ETIAS-verordening.

[105] Zie artikel 32 van de ETIAS-verordening.

[106] Gedefinieerd in artikel 6, 2° van het ontwerp.

[107] Van deze overheidsinstanties vallen de FOD Volksgezondheid (onderworpen aan de AVG) en de AGD&A - (hoewel onderworpen aan titel 2 van de WVG onder bepaalde voorwaarden - zie in het bijzonder het *Samenwerkingsprotocol tussen de Belgische Federale Toezichthoudende Autorieiten op het vlak van dataprotectie, Overeenkomst tussen de Gegevensbeschermingsautoriteit, het Controleorgaan op de Politionele Informatie, het Vast Comité van Toezicht op de Inlichtingendiensten en het Vast Comité van Toezicht op de Politiediensten*, 24 november 2020, blz. 10, te raadplegen op https://www.gegevensbeschermingsautoriteit.be/publications/samenwerkingsprotocol-tussen-de-belgische-federale-toezichthoudende-autoriteiten-op-het-vlak-van-dataprotectie.pdf, , laatst geraadpleegd op 05/07/2023) **- onder bevoegdheid van de Gegevensbeschermingsautoriteit**.

[108] Artikel 11, §1 van het ontwerp.

[109] Artikel 12, §1 van het ontwerp. Paragraaf 2 van deze bepaling voorziet ook in toegang tot het centraal strafregister in het geval van een hit in verband met ECRIS-TCN.

[110] Artikel 8, §2, van het ontwerp.

onmogelijk om toezicht te houden op de toepassing van artikel 6, 4, van de AVG en artikel 4, 1 en 2, van Richtlijn 2016/680.

62. Uit de logica van het ontwerp blijkt duidelijk dat de **Sectie VZ** bevoegd is voor het beoordelen van en beslissen over gevallen waarin het risico op **ILLEGALE IMMIGRATIE**[111] bestaat. Artikel 27 van het ontwerp verwoordt dit echter niet rechtstreeks en zou duidelijker moeten worden geformuleerd, naar het voorbeeld van de bepalingen die van toepassing zijn op de NCC-sectie.

63. In deze context specificeert het ontwerp bovendien niet **op basis van welke Belgische informatie ((categorieën van) gegevens) en informatiesystemen** de VZ-sectie haar analyse zal uitvoeren. Daarom bevroeg de Autoriteit de aanvrager hierover, die als volgt antwoordde (de Autoriteit vertaalt):

> « *VZ vond het niet nuttig om dit voor hun sectie te voorzien. We weten dat ze in ieder geval hun Evibel database zullen gebruiken* »[112].

64. Het standpunt in overweging 61 is ook in dit geval van toepassing: het ontwerp moet de **databanken (en hun rechtsgrondslag) en (categorieën van) gegevens aanduiden die door VZ *moeten*** worden **hergebruikt voor de doeleinden van** de ETIAS-verordening. Bij gebrek aan verduidelijking op dit gebied is het voor de Autoriteit ook onmogelijk om toezicht te houden op de toepassing van artikel 6, 4 van de AVG[113].

Beslissing van de E.N.E.

65. Indien er geen concrete aanwijzingen of redelijke gronden zijn op basis van concrete aanwijzingen om te concluderen dat de aanwezigheid van de persoon op het grondgebied van de lidstaten een risico voor de veiligheid of illegale immigratie of een hoog epidemiologisch risico met zich meebrengt, **wordt een reisautorisatie (met een geldigheidsduur van 3 jaar) afgegeven**[114].

66. **In geval van twijfel** kan de nationale ETIAS-eenheid de autorisatie afgeven **na een tweedelijnscontrole**[115]. De Autoriteit vroeg de aanvrager onder welke omstandigheden (regels) deze

---

[111] Zie artikel 27 van het ontwerp.

[112] " Evibel " blijkt de VZ-gegevensbank te zijn waarin gegevens met betrekking tot asiel-, migratie- en terugkeerprocedures te vinden zijn, zie European Migration Network Belgium, « *Accurate, timely, interoperable : data management in the asylum procedure* », disponible sur https://emnbelgium.be/sites/default/files/publications/Standalone%20FINAL_1.pdf,

laatst geraadpleegd op 06/07/2023, blz. 15.

[113] Of artikel 4, 1 en 2 van de Richtlijn 2016/680, zie overweging 87.

[114] Artikel 36, 1 van de ETIAS-verordening.

[115] Artikel 36, 2 van de ETIAS-verordening. Deze controle wordt als volgt omschreven (artikel 3, 1, *3 van de ETIAS-verordening) «tweedelijnscontrole zoals gedefinieerd in artikel 2, punt 13, van Verordening (*EU) 2016/399», *hetzij «een verdere controle die op een speciale locatie kan worden verricht, apart van de locatie waar iedereen wordt gecontroleerd (eerste lijn)*», voor grenscontroles. Een geraadpleegde lidstaat kan ook om een dergelijke vermelding verzoeken. Overeenkomstig artikel 36, 3, van

tweedelijnscontrole vereist kan zijn. Hij wees er met name op dat deze mogelijkheid wordt geregeld door een gedelegeerde handeling van de Europese Commissie (nog niet gepubliceerd, maar wel online beschikbaar[116]).

67. Het is de bevoegde « ***sectie*** » van de E.N.E. die «*haar beslissingen* »[117] neemt, met dien verstande dat de « *leidende ambtenaar*» van de sectie verantwoordelijk is «*voor de goede uitvoering van de opdrachten van de E.N.E. waar diens sectie vrantwoordelijke voor is* »[118]. Als de hits voor dezelfde aanvraag door beide secties moeten worden beoordeeld, neemt de sectie NCC de beslissing en moet zij het negatieve advies van de sectie VZ opvolgen[119]. De Autoriteit vroeg de aanvrager om deze analyse te bevestigen ("beslissing van de leidende ambtenaar") en de aanvrager antwoordde als volgt :

> « *Ja, een koninklijk uitvoeringsbesluit bepaalt dat de leidende ambtenaar de leden van zijn sectie aanwijst die gemachtigd zijn om beslissingen te nemen. Het zal niet het gedetacheerde personeel van de relevante diensten zijn die de risico's beoordeelt, maar het operationele personeel (NCC-attachés)*» (onderlijnd door de Autoriteit)[120].

68. De Autoriteit neemt nota van deze uitleg, maar **is van mening dat in het dispositief van het ontwerp zelf moet worden gespecificeerd dat de leidende ambtenaar de beslissingen neemt, aangezien dit** (met name**) rechtstreeks van invloed is op de vaststelling van taken en verantwoordelijkheden met betrekking tot de verwerking van persoonsgegevens** en eventuele onverenigbaarheden bij de uitvoering van de betrokken functies[121].

69. Artikel 37 van de ETIAS-verordening vermeldt de omstandigheden waarin reisautorisaties kunnen worden **geweigerd**. De beslissingen va de sectie E.N.E. moeten met redenen omkleed **zijn**[122].

---

de ETIAS-verordening kan in het systeem ook een vermelding worden opgenomen dat tijdens de behandeling van de aanvraag een specifieke hit is opgetreden.

[116] Zie voetnoot 15, achtste verwijzing.

[117] Artikelen 11, § 3 en 29 van het ontwerp.

[118] Artikel 7, 1° van het ontwerp en artikel 26, §2 van het ontwerp.

[119] Artikel 29 van het ontwerp.

[120] Bovendien, stelt het commentaar bij de artikelen van het ontwerp (blz. 11) over het risicobeoordelingsproces het volgende «*dit proces houdt in dat het niet de gedetacheerde leden zijn die de uiteindelijke beslissing nemen, maar de operationele medewerkers die door de leidend ambtenaar gemachtigd worden* ».

[121] Zie de overweging 102.

[122] Zie de artikelen 28, 3, en 39, 4 van de ETIAS-verordening. Als algemene regel geldt dat de redenen voor de beslissing altijd worden vermeld in het aanvraagdossier. Krachtens artikel 26, 7 van de ETIAS-verordening: *De resultaten van de beoordeling van het veiligheidsrisico, het risico op het gebied van illegale immigratie of het hoge epidemiologische risico en de verantwoording van de beslissing tot afgifte dan wel weigering van een reisautorisatie, wordt in het aanvraagdossier opgenomen door het personeelslid dat de risicobeoordeling* heeft uitgevoerd. Zie ook artikel 39, 3, d) en de artikelen 40, 4. (nietigverklaring), 41,6. (intrekking) en 43 (beslissing tot nietigverklaring of intrekking, 2 van de ETIAS-verordening.

Zie ook de bijlagen van het Uitvoeringsbesluit (EU) 2022/102 van de Commissie van 25 januari 2022 *tot vaststelling van formulieren voor weigering, nietigverklaring of intrekking van een reisautorisatie*,voorzien in formulieren voor de kennisgeving van beslissingen die, naast de vermelding van de reden voor de beslissing ("desbetreffende bepaling van de ETIAS-verordening"), een vak «*Relevante feiten en nadere motivering van de beslissing" bevatten* ».

70. **Wanneer de handmatige verwerking nog niet is voltooid of wanneer een reisautorisatie is geweigerd, geannuleerd of ingetrokken, kan de lidstaat van bestemming van de aanvrager bij wijze van uitzondering een reisautorisatie met territoriaal beperkte geldigheid afgeven op humanitaire gronden, om redenen van nationaal belang of op grond van internationale verplichtingen, overeenkomstig artikel 44 van de ETIAS-verordening.**

Beroepsprocedures

71. Aanvragers kunnen in **beroep** gaan tegen een geweigerde reisautorisatie, een proces dat onder Belgisch recht wordt **georganiseerd als onderdeel van het Wijzigingsontwerp**[123]**. Deze laatste bepaalt dat tegen de beslissingen van de E.N.E. *annulatieberoep* kan worden aangetekend bij de Raad voor vreemdelingenbetwistingen, als bedoeld in artikel 39/1 van de wet van 15 december 1980**[124]**. Het annulatieberoep valt onder de artikelen 39/78 en volgende van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen (hierna "de wet van 1980").** Artikel 39/2 van de wet van 1980 maakt onderscheid tussen een beroep met volle rechtsmacht tegen beslissingen van de Commissaris-generaal voor de Vluchtelingen en de Staatlozen en een annulatieberoep, wegens overtreding van hetzij substantiële, hetzij op straffe van nietigheid voorgeschreven vormen, overschrijding of afwending van macht[125]. **In de toelichting wordt de keuze voor een annulatieberoep in plaats van een beroep met volle rechtsmacht niet toegelicht**.

72. **De Autoriteit is van mening dat,een beroep met volle rechtsmacht de rechten en vrijheden van de betrokken personen *a priori* waarschijnlijk beter zal waarborgen**. Bijgevolg moet in

---

[123] Artikel 37, 3 van de ETIAS-verordening.

[124] Zie ook overweging 78 betreffende beroepen tegen een beslissing van de E.N.E. over een verzoek om rectificatie of verwijdering van gegevens.

[125] Deze bepaling luidt als volgt:

« *§ 1. De Raad doet uitspraak, bij wijze van arresten, op de beroepen die zijn ingesteld tegen de beslissingen van de Commissaris-generaal voor de vluchtelingen en de staatlozen.*

De Raad kan:

1° de bestreden beslissing van de Commissaris-generaal voor de vluchtelingen en de staatlozen bevestigen of hervormen;

2° de bestreden beslissing van de Commissaris-generaal voor de vluchtelingen en de staatlozen vernietigen hetzij omdat aan de bestreden beslissing een substantiële onregelmatigheid kleeft die door de Raad niet kan worden hersteld, hetzij omdat essentiële elementen ontbreken die inhouden dat de Raad niet kan komen tot de in 1° bedoelde bevestiging of hervorming zonder aanvullende onderzoeksmaatregelen hiertoe te moetenbevelen;

3° onverminderd het bepaalde in 1° en 2°, de bestreden beslissing [3 van de Commissaris-generaal voor de vluchtelingen en de staatlozen tot niet-ontvankelijkheid van het verzoek om internationale bescherming, bedoeld in artikel 57/6, § 3,]3 vernietigen omdat er ernstige aanwijzingen bestaan dat de verzoeker in aanmerking zou komen voor de erkenning van de hoedanigheid van vluchteling, zoals bepaald in artikel 48/3, of voor de toekenning van de subsidiaire bescherming, zoals bepaald in artikel 48/4.

§ 2. De Raad doet uitspraak, bij wijze van arresten als annulatierechter over de overige beroepen wegens overtreding van hetzij substantiële, hetzij op straffe van nietigheid voorgeschreven vormen, overschrijding of afwending van macht. ».

Wat betreft de specifieke bepalingen die van toepassing zijn op beroepen met volle rechtsmacht tegen beslissingen van de voornoemde Commissaris, zie artikel 39/69 e.v. van de wet van 1980. Artikelen 39/78 en volgende betreffende het annulatieberoep.

de memorie van toelichting worden vermeld waarom een annulatieberoep wordt ingesteld in plaats van een beroep met volle rechtsmacht.

73. Bovendien volgt uit het ETIAS-dispositief[126] dat, wanneer de E.N.E. van een lidstaat een reisautorisatie weigert op grond van een **negatief advies dat door de autoriteit van een andere lidstaat is uitgebracht** tijdens een raadpleging door de eerste E.N.E.[127], de betrokkene het recht heeft om in beroep te gaan tegen het negatieve advies dat door de E.N.E. van die andere lidstaat is uitgebracht, en dit overeenkomstig de wetgeving van die andere lidstaat. Het wijzigingsontwerp verwijst echter in het algemeen naar " *beslissingen* " van de E.N.E., terwijl de ETIAS-verordening verwijst naar weigering/uitgifte (beslissing over de aanvraag) en het uitbrengen van een advies in het kader van overleg tussen de lidstaten. **De Autoriteit is van mening dat de wijzigingsontwerp moet verduidelijken dat een negatief *advies* van een afdeling van de E.N.E. in het kader van de in artikel 28 van de ETIAS-verordening bedoelde raadplegingen een beslissing vormt waartegen beroep kan worden ingesteld**.

74. Tijdens de beroepsprocedure heeft «*degene die beroep instelt **toegang tot de informatie** in het aanvraagdossier **overeenkomstig de gegevensbeschermingsregels** vermeld in artikel 56 van deze verordening*» (vet toegevoegd door de Autoriteit)[128]. In dit verband heeft de Autoriteit de aanvrager verzocht te bevestigen dat de **risicobeoordelingen** die door de gedetacheerde leden van de sectie NCC worden uitgevoerd, inderdaad zullen worden meegedeeld aan de sectie NCC (aan de leidende ambtenaar) zodat deze laatste zijn beslissing kan nemen (meer dan alleen het resultaat van de beoordeling), zodat de betrokkene recht heeft op toegang tot deze beoordeling (dit document) op grond van de gegevensbeschermingsregels. De aanvrager antwoordde later[129] als volgt (de Autoriteit vertaalt):

> « *Ik kan bevestigen dat de betrokkene toegang zal hebben tot de redenering achter het resultaat van de beoordeling, die ook zal worden gebruikt om de beslissing te rechtvaardigen*

---

[126] Zie het formulier in bijlage I **bij Uitvoeringsbesluit 2022/102**.

Bijgevolg zijn het door een geraadpleegde lidstaat uitgebrachte advies (zie artikel 28, 3, lid 3, van de ETIAS-verordening) en de daarmee verband houdende motivering van de beslissing (artikel 39, 4, van de ETIAS-verordening) niet toegankelijk voor de betrokkene in het aanvraagdossier, en met name de vermelding van een tweedelijnscontrole (wanneer een geraadpleegde lidstaat daarom verzoekt ; zie artikel 36, 2, tweede alinea, van de ETIAS-verordening; er wordt opgemerkt dat deze informatie automatisch wordt gewist zodra de grensautoriteiten de controle hebben uitgevoerd) (artikel 36, 2, derde alinea, van de ETIAS-verordening).

[127] Zie artikel 28 van de ETIAS-verordening, dat de mogelijkheid van overleg met andere lidstaten regelt.

[128] Artikel 37, 3 van de ETIAS-verordening.

[129] Volledigheidshalve had de aanvrager, voordat hij hierover opnieuw werd ondervraagd, de Autoriteit als volgt geantwoord (de Autoriteit vertaalt):

« *We bevestigen dat de resultaten van de risicobeoordeling zullen worden opgenomen in het dossier van de aanvrager, maar niet in de vorm van een "document", overeenkomstig artikel 26, §7, lid 2, van de Verordening. Om toegang te krijgen, moet je de ETIAS-software raadplegen. Dit met redenen omklede advies dient als basis voor de beslissing. In het geval van een beroep moet het beschikbaar zijn in het administratieve dossier (we kunnen dit in dit stadium niet garanderen omdat we niet verantwoordelijk zijn voor de ETIAS-software, maar we hebben dit verzoek gedaan om de rechtmatigheid van ETIAS-beslissingen te waarborgen). De betrokkene kan er ook toegang toe krijgen, zoals bepaald in artikel 64 van de verordening* ».

die door de E.N.E. is genomen en aan de betrokkene is meegedeeld. Volgens ons blijkt dit duidelijk uit artikel 26, §7, lid 2, van de Verordening (dat verwijst naar het resultaat van de beoordeling en de redenen die aan de beslissing ten grondslag liggen) en artikel 11, §1, van het ontwerp (dat verwijst naar een "met redenen omkleed advies").

Volledigheidshalve wijs ik erop dat deze toegang beperkt kan zijn als de risicobeoordeling in kwestie valt onder het toepassingsgebied van Richtlijn 2016/680, of van titel 2 of 3 van de wet van 2018[130] *- nieuwe subtitel 5a ingevoegd door artikel 41 van het ontwerp* ».

75. De Autoriteit neemt akte van deze uitleg. **Zij is echter van mening dat de betrokkene in ieder geval toegang moet hebben tot de risicobeoordeling die is opgesteld en aan de leidende ambtenaar (of zijn operationeel personeel[131]) is meegedeeld om zijn beslissing te kunnen nemen**. Dit sluit niet uit dat de gegevensverwerking (en de in deze context verwerkte gegevens) die wordt uitgevoerd om de beoordeling door de bevoegde autoriteiten op te stellen die onder Richtlijn 2016/680 vallen, zelf onderworpen kan zijn aan regels die de rechten van de betrokkene beperken op grond van Richtlijn 2016/680. De sectie (de leidend ambtenaar) die een beslissing neemt in het kader van ETIAS is onderworpen aan de AVG en de **risicobeoordeling** die verder gaat dan het eenvoudige resultaat ervan (d.w.z. of er al dan niet een specifiek risico is) **vormt het beslissende element dat zijn besluitvorming motiveert en is noodzakelijk voor de betrokkene, zowel om te controleren of de persoonsgegevens die over hem worden verwerkt rechtmatig zijn als met het oog op de mogelijke uitoefening van zijn recht om beroep aan te tekenen** tegen de beslissing van de E.N.E. Zoals het ontwerp er nu uitziet, is de Autoriteit van mening dat het de verantwoordelijkheid van de gedetacheerde leden is om zorgvuldig te zijn bij het opstellen van hun risicoanalyse : de rechtstreekse interactie van hun analyseactiviteit met de rechten en vrijheden van de betrokkenen betekent dat de betrokkene toegang moet kunnen krijgen tot deze analyse[132]. Dienovereenkomstig moet het ontwerp in het kader van de **interne controle**, wanneer dit nodig is om de juistheid van de persoonsgegevens **te verifiëren in de analyse** die aan hem is meegedeeld (bijvoorbeeld een verdenking met betrekking tot de betrokkene), ook de leidende ambtenaar (die verantwoordelijk is voor het te nemen besluit en de hiërarchische autoriteit van de gedetacheerde leden) in staat stellen om de fundamentele persoonsgegevens in de betreffende database te raadplegen, *in overeenstemming met de regels (inclusief gegevensbescherming) die voor die databank*

[130] Over onrechtstreekse toegang via de toezichthoudende autoriteiten, zie de conclusies van advocaat-generaal L. Medina uiteengezet op 15 juni 2023 in de zaak C-333/22, *Ligue des droits humains ASBL, BA c/ L'organe de contrôle de l'information policière*.

[131] Zie voetnoot 119.

[132] Temeer daar de ETIAS-verordening het recht op toegang tot het dossier in het kader van een beroep koppelt aan toegang tot gegevens vanuit het oogpunt van gegevensbescherming. In ieder geval ziet de Autoriteit geen reden waarom de analyse wel zou kunnen worden geraadpleegd in het kader van een beroepsprocedure, maar niet in het kader van een toegang op vlak van gegevensbescherming.

gelden. Opmerking: deze mogelijkheid mag niet worden misbruikt om risicoanalyses zinloos te maken, met name omdat ze toegankelijk zouden zijn voor de betrokken personen.

76. Nog steeds met betrekking tot de hierboven genoemde risicobeoordeling merkt de Autoriteit op dat het ontwerp ook duidelijk moet maken dat deze beoordeling, die wordt uitgevoerd door gedetacheerde leden onder het gezag van de leidende ambtenaar van de sectie, **niet onderworpen is aan de algemene uitzonderingen op de rechten van betrokkenen die zijn vastgelegd in de artikelen 11 en 14 van de WVG** (niet-toepasselijkheid van rechten op gegevens die met name worden ontvangen van de politie en inlichtingen- en veiligheidsdiensten).

77. Wat ten slotte de **uitoefening van de rechten door de aanvrager** betreft, bepaalt de ETIAS-verordening dat de nationale eenheid van ETIAS (of de centrale eenheid van ETIAS) die het niet eens is met het standpunt van de aanvrager over het corrigeren of wissen van zijn gegevens «*[...] onverwijld een administratieve beslissing (neemt) waarbij de betrokkene schriftelijk wordt uitgelegd waarom de eenheid niet bereid is de gegevens die op de betrokkene betrekking hebben, te corrigeren of te wissen*», en in deze beslissing moeten de beschikbare beroepsmogelijkheden worden vermeld[133].

78. Er is dus sprake van **een bijkomende mogelijkheid van "*beslissing*" *van* de E.N.E.,** waartegen volgens het wijzigingsontwerp beroep kan worden ingesteld bij de Raad voor Vreemdelingenbetwistingen. Artikel 55, 8 van de ETIAS-verordening bepaalt overigens dat «*onverminderd beschikbare mogelijkheden van administratief of buitengerechtelijk beroep (...) betrokkenen* ***toegang (hebben) tot een doeltreffend beroep voor de rechter om de in Etias opgeslagen gegevens te laten wijzigen of wissen***» (vet toegevoegd door de Autoriteit). Dit doet geen afbreuk aan de mogelijkheid die de betrokkene wordt geboden om, in overeenstemming met de gegevensbeschermingsregels, een klacht in te dienen bij de bevoegde toezichthoudende autoriteit. I**n dit verband is de Autoriteit van mening dat, om de doeltreffendheid van de gegevensbeschermingsregels zo goed mogelijk te waarborgen, een beroep met volle rechtsmacht moet worden ingevoerd**, zodat de Raad voor Vreemdelingenbetwistingen (een administratieve rechtbank) zijn analyse in de plaats kan stellen van die van de E.N.E.

Annulerings- en intrekkingsopties

79. Wanneer een lidstaat kan aantonen dat op het moment van afgifte niet aan de voorwaarden voor de afgifte van een reisautorisatie werd voldaan of niet langer wordt voldaan, *moet* de betrokken nationale eenheid de reisautorisatie annuleren (annulatie) of intrekken (intrekking)[134].

[133] Artikel 64, 3 en 4 van de ETIAS-verordening.

[134] Zie de artikelen 40 en 41 van de ETIAS-verordening.

80. Naast **de automatische interactie met het SIS en de interactie met de observatielijst van ETIAS** (aanvullende geautomatiseerde verwerking), die rechtstreeks worden geregeld door de ETIAS-verordening[135], heeft de Autoriteit de aanvrager gevraagd naar de **omstandigheden** waarin (en de regels volgens welke) de E.N.E. zich mogelijk moet uitspreken over een annulering of intrekking. De aanvrager antwoordde het volgende (de Autoriteit vertaalt):

> « *Wij zijn van mening dat elke Belgische autoriteit die rechtstreeks of onrechtstreeks betrokken is bij de beoordeling van de aanvraag kennis kan nemen van nieuwe informatie of informatie waarmee geen rekening werd gehouden toen de beslissing werd genomen, wat kan leiden tot de annulering of intrekking van de reisautorisatie. Het lijkt vanzelfsprekend dat deze informatie wordt doorgegeven aan E.N.E. De bepalingen vereisen bewijs, wat tastbare en controleerbare elementen veronderstelt. Deze moeten worden vergeleken met de gronden die kunnen worden gebruikt om de reisautorisatie te annuleren of in te trekken (art. 37, lid 1 en 2 van de verordening).*
>
> *We hebben besloten geen bepaling over dit onderwerp in het ontwerp op te nemen omdat we er niet in zijn geslaagd deze zodanig te formuleren dat ze een toegevoegde waarde heeft ten opzichte van de bepalingen van de verordening*» (onderstreping toegevoegd door de Autoriteit).

81. Op de een of andere manier impliceert deze aanpak dus monitoring (met welke frequentie ?)[136] van de betrokkenen aan wie een reisautorisatie is afgegeven, en **een verantwoordelijkheid/verplichting** (ook met betrekking tot gegevensverwerking[137]) van de autoriteiten die betrokken zijn bij de behandeling van de aanvraag. Deze zijn verplicht om de E.N.E. alle relevante informatie mee te delen (identificeren) waarvan zij bij de uitvoering van hun taken kennis nemen, *mogelijk zelfs buiten het proces van beoordeling van een autorisatie-aanvraag om*[138] (indien de aanvrager dit van plan is). **De Autoriteit is van mening dat een dergelijke verplichting, die een verwerking van persoonsgegevens met zich meebrengt, moet worden georganiseerd door de bepalingen van het ontwerp,** waarin de essentiële elementen van de beoogde gegevensverwerking moeten worden vastgelegd.

---

[135] Bedoeld in artikel 41, 3 en 4, van de ETIAS-verordening.

[136] De betrokken autoriteit moet bij de uitoefening van haar taken en overeenkomstig de verwachte follow-up de gegevens die zij over de betrokkene in haar bezit heeft, kunnen koppelen aan het feit dat de betrokkene al dan niet houder is van een onder de ETIAS-verordening vallende reisautorisatie.

[137] Zie de overwegingen 102 en volgende.

[138] Dit betekent dat updates alleen zouden kunnen worden uitgevoerd wanneer in de loop van een autorisatieaanvraag gegevens worden aangetroffen die ook relevant zijn voor een andere autorisatieaanvraag. Zie voor een geval van dit type, in een andere context, het *advies 245*/2022 van 21 oktober 2022 van de Autoriteit *met betrekking tot een voorontwerp van wet betreffende de gemeentelijke bestuurlijke handhaving, de instelling van een gemeentelijk integriteitsonderzoek en houdende oprichting van een Directie Integriteitsbeoordeling voor Openbare Besturen (CO-A-2022-248*), overwegingen 51 ev. en overweging 56 in het bijzonder.

II.2.4. Juistheid en bijwerken van de gegevens

82. **De verplichting om de gegevens bij te werken en toezien op de juistheid van de gegevens**. De centrale eenheid van ETIAS en de nationale eenheden zijn verplicht om de gegevens bij te werken en ervoor te zorgen dat ze juist zijn[139]. In dit verband vroeg de Autoriteit aan de aanvrager welke uitvoeringsmaatregelen overeenkomstig artikel 55, 1, van de ETIAS-verordening zijn genomen om ervoor te zorgen dat de gegevens actueel blijven. Er moet worden opgemerkt dat, wat de ETIAS observatielijst betreft, artikel 35 van de ETIAS-verordening zelf een periodieke verplichting bevat. De aanvrager antwoordde het volgende (de Autoriteit vertaalt):

> « *Artikel 55, § 1, verwijst alleen naar gegevens die CEE of ENE zelf heeft vastgelegd op basis van de bepalingen van de verordening (bijv: art 39, dat bepaalt welke gegevens moeten worden toegevoegd nadat de beslissing is genomen - deze gegevens moeten worden gewijzigd in geval van annulering of intrekking volgens art 40 en 41). Wij zijn van mening dat de verplichting om bij te werken uitdrukkelijk is omschreven in de andere §en van artikel 5. Er moet een trigger zijn, bijvoorbeeld een verzoek om toegang tot persoonsgegevens, of de mededeling van nieuwe informatie door een betrokken autoriteit, enz.* ».

83. De Autoriteit neemt nota van deze uitleg, die samenhangt met de ontwikkelingen inzake het annuleren en intrekken van autorisaties[140].

II.3. GEBRUIK VAN ETIAS VOOR REPRESSIEVE DOELEINDEN

84. Zoals hierboven vermeld, kan ETIAS voor repressieve doeleinden worden geraadpleegd door de autoriteiten die door de lidstaten zijn aangewezen.

II.3.1. Betrokken autoriteiten

85. In dit verband moeten de lidstaten de **autoriteiten aanwijzen die gemachtigd zijn** om ETIAS-gegevens te raadplegen[141] (aangewezen autoriteiten) en de **operationele eenheden**[142] binnen deze autoriteiten opsommen die als enige bevoegd[143] zijn om ETIAS-gegevens te raadplegen. Zij moeten ook een **centraal toegangspunt** aanwijzen dat toegang heeft tot het ETIAS-systeem en dat

[139] Zie artikel 55, 1 tot 4, van de ETIAS-verordening.

[140] Zie de overwegingen 79-81.

[141] Artikel 50, 1 van de ETIAS-verordening.

[142] Het is de operationele eenheid die het met redenen omklede verzoek tot raadpleging van ETIAS moet indienen, zie artikel 51 van de ETIAS-verordening.

[143] Artikel 50, 3 van de ETIAS-verordening.

controleert of aan de in artikel 52 vastgestelde voorwaarden voor toegang tot ETIAS is voldaan[144]. De ETIAS-verordening voorziet ook in de onafhankelijkheid van het centraal toegangspunt van de aangewezen autoriteiten[145]. Artikel 52 van de ETIAS-verordening bevat de cumulatieve voorwaarden waaronder gegevens mogen worden geraadpleegd[146].

86. De artikelen 14 tot en met 20 van het ontwerp implementeren in dit opzicht de ETIAS-verordening. Identificeren zich a priori als **gemachtigde (aangewezen) autoriteiten**: de politiediensten, de VSSE, de ADIV, de AGD&A en de Dienst Vreemdenlingenzaken (hierna **«DVZ** »).

87. De Autoriteit merkt terloops op dat artikel 41 van het ontwerp de **DVZ nu tot een bevoegde autoriteit** maakt als bedoeld in titel 2 van de WVG, door artikel 26, 7°, van het WVG te wijzigen, wanneer het zijn repressieve bevoegdheden krachtens artikel 81 van de wet van 15 december 1980 uitoefent[147]. De **reikwijdte van deze wijziging gaat verder dan de doelstellingen van het ontwerp**. In de toelichting bij het ontwerp staat alleen dat deze integratie plaatsvindt « *gelet op de repressieve bevoegdheden* » van de DVZ[148].

88. De Autoriteit **neemt nota van deze wijziging** en van het feit dat de Gegevensbeschermingsautoriteit de toezichthoudende autoriteit van de DVZ blijft.

89. De Autoriteit vroeg de aanvrager welke **operationele eenheden** als bedoeld in de ETIAS-verordening zullen worden aangewezen (zullen ze op een later tijdstip worden aangewezen en door wie ?). De aanvrager antwoordde het volgende (de Autoriteit vertaalt):

> « *Elk dienst moet de operationele eenheden aanwijzen die gemachtigd zijn om een raadplegingsverzoek in te dienen en de lijst naar ENE sturen. De inlichtingen- en*

---

[144] Artikel 50, 2 van de ETIAS-verordening.

[145] Zie artikel 50, 2 van de ETIAS-verordening.

[146] Artikel 52, 1*bis*, heeft ook betrekking op het geval waarin de aangewezen autoriteit in kennis wordt gesteld van het bestaan van gegevens in ETIAS door middel van een **CIR**-raadpleging als bedoeld in artikel 22 van de **interoperabiliteitsverordening**. Zie voetnoot 65..

[147] Deze bepaling luidt als volgt:

« *De misdrijven tegen deze wet (en tegen de artikelen 433quinquies tot 433octies en 433decies tot 433duodecies van het Strafwetboek) worden opgespoord en vastgesteld door alle officieren van gerechtelijke politie, met inbegrip van diegenen wier bevoegdheid beperkt is, (door de ambtenaren van de federale en van de lokale politie), door de (ambtenaren van de Dienst Vreemdelingenzaken) en van het Bestuur der Douanen en Accijnzen, door de inspecteurs van het Ministerie van Tewerkstelling en Arbeid en van het Ministerie van Middenstand, alsmede door de inspecteurs van de Rijksdienst voor Sociale Zekerheid.*

Zij verzamelen de bewijzen van de misdrijven en leveren de daders ervan over aan de rechterlijke overheden overeenkomstig de bepalingen van het Wetboek van Strafvordering.

Zij bezorgen de minister of zijn gemachtigde alle documenten en inlichtingen die nuttig zijn voor het uitoefenen van zijn taken.

De in het vorig lid bedoelde documenten of inlichtingen kunnen eveneens worden bezorgd door de inspecteurs van het Vlaamse Ministerie voor Werk en Sociale Economie, de inspecteurs van de "Direction générale opérationnelle Economie, Emploi et Recherche" van de Waalse overheid, de inspecteurs van de Directie van de Gewestelijke Arbeidsinspectie van het Brussels Hoofdstedelijk Gewest, en de inspecteurs van het Ministerie van de Duitstalige Gemeenschap, afdeling werk ».

[148] Blz. 20.

veiligheidsdiensten en de Administratie der Douane en Accijnzen wensten een interne valideringsprocedure voor deze verzoeken door een hiërarchische meerdere toe te voegen (artikel 15, lid 1, van het ontwerp)» (onderstreping toegevoegd door de Autoriteit).

90. De Autoriteit vindt in de bepalingen van het ontwerp echter niet a priori het beginsel terug dat aangewezen autoriteiten operationele eenheden in de zin van de ETIAS-verordening moeten aanwijzen. Hoe dan ook**, aangezien de aanwijzing van deze eenheden** een directe impact heeft op de rol en verantwoordelijkheid op het gebied van de verwerking van persoonsgegevens, is de Autoriteit van mening dat **het een norm is die hen moet aanwijzen,** en dat deze bevoegdheid (van aanwijzing) niet kan worden overgelaten aan de beoordeling van de betrokken diensten. In dat geval **kunnen de bepalingen van het ontwerp bepalen dat de Koning binnen de voornoemde diensten bepaalt welke de operationele eenheden zijn als bedoeld in de ETIAS-verordening**.

II.3.2. <u>Doeleinde en uitbreiding tot inlichtingen- en veiligheidsdiensten</u>

91. Eerst en vooral is de Autoriteit van mening dat artikel 31, §§ 2 en 3, van het ontwerp (tot vaststelling van de toepasselijke gegevensbeschermingsregels) nauwkeuriger moeten worden omschreven om duidelijk te bevestigen dat "de raadpleging van het ETIAS-informatiesysteem" waarnaar wordt verwezen, **de raadpleging van het ETIAS-informatiesysteem voor repressieve doeleinden is** als bedoeld in de ETIAS-verordening, d.w.z. de raadplegingen waarnaar wordt verwezen in afdeling 4, hoofdstuk 3, van het ontwerp, onverminderd de onderstaande opmerking.

92. Ten tweede, wat de repressieve doeleinden betreft[149], legt het commentaar bij de artikelen uit dat de betrokken misdrijven naar Belgisch recht niet rechtstreeks worden opgesomd (er wordt gewoon verwezen naar de Europese teksten, zoals bij ETIAS) om de volgende redenen :

« […] *er wordt verwezen naar de vertaling ervan in het nationale recht om de raadpleging van de gegevens te rechtvaardigen. Het is inderdaad niet wenselijk een exhaustieve lijst van deze strafbare feiten in de wet zelf vast te leggen, enerzijds omdat <u>het Strafwetboek en andere relevante regelingen voortdurend evolueren</u>, en anderzijds omdat <u>de in de verordening vastgestelde drempelwaarde voor de ernst van de strafbare feiten op zich niet volstaat om strafbare feiten van "gewone" aard uit te sluiten</u> (zie in dit verband punt 151*[150] *van het arrest van het HvJ-EU van 21 juni 2022 in de zaak "Ligue des droits humains" C-817/19).*

[149] Blz. 12.

[150] De overwegingen 151 en 152 zijn als volgt geformuleerd:

« *151. Aangezien artikel 3, punt 9, van de PNR-richtlijn het <u>niet over de toepasselijke minimumstraf maar over de toepasselijke maximumstraf</u> heeft, valt evenwel niet uit te sluiten dat er PNR-gegevens worden verwerkt om strafbare feiten te bestrijden die*

93. **Volgens de Autoriteit is deze redenering niet helemaal overtuigend, en wel om de volgende twee redenen.** Ten eerste verhinderen de evoluties in het strafrecht niet dat de wetgever op andere gebieden wetgeving opstelt op basis van lijsten van relevante Belgische strafrechtelijke inbreuken om zware criminaliteit te definiëren, met verwijzing naar de rechtsgrondslag van deze inbreuken[151]. De strafbare feiten die onder de ETIAS-verordening vallen, zijn al zeer gevarieerd (terroristische misdrijven, deelname aan een criminele organisatie, mensenhandel, illegale handel in verdovende middelen en psychotrope stoffen, corruptie, cybercriminaliteit, namaak en productpiraterij, racisme en vreemdelingenhaat, racketeering, vervalsing van administratieve documenten en handel in vervalsingen, verkrachting, brandstichting, vliegtuigkaping, **enz.**) op zodanig wijze dat het twijfelachtig is of frequente updates nodig zullen zijn. Bovendien verhindert een verwijzing naar het strafbare feit naar Belgisch recht niet dat het evolueert in het Strafwetboek, zonder dat een wijziging van het ontwerp nodig is (tenzij de wijziging uiteraard gevolgen heeft voor de ernst van het betrokken strafbare feit).

94. Ten tweede, en meer fundamenteel, komt de in het dispositief van het ontwerp voorgestelde aanpak **niet tegemoet aan de door het Hof van Justitie geuite bezorgdheid**, aangezien het geen enkele regel - geen enkele voorwaarde - bevat die het mogelijk maakt rekening te houden met het standpunt van het Hof - het verwijst alleen naar de lijst van strafbare feiten die onder ETIAS vallen en naar de desbetreffende minimale maximumstraf. Concluderend **is de Autoriteit op dit punt van mening dat in het ontwerp moet worden aangegeven om welke ernstige strafbare feiten naar Belgisch recht het gaat** .

95. In een heel andere geest[152] **breidt het ontwerp de mogelijkheden om ETIAS te raadplegen uit tot doeleinden die worden nagestreefd door inlichtingen- en veiligheidsdiensten**, door te bepalen dat toegang tot het centrale systeem kan worden gevraagd voor «het toezien *op activiteiten*

weliswaar aan het ernstcriterium in deze bepaling voldoen maar die, gelet op de bijzonderheden van het nationale strafrechtsysteem, geen ernstige criminaliteit maar gewone criminaliteit uitmaken.,

152. Het staat dus aan de lidstaten om ervoor te zorgen dat het bij de PNR-richtlijn ingevoerde systeem daadwerkelijk enkel wordt toegepast in de strijd tegen ernstige criminaliteit en niet wordt uitgebreid naar strafbare feiten die gewone criminaliteit vormen» (onderstreept door de Autoriteit).

[151] Zie bijvoorbeeld het advies 245/2022 van 21 oktober *2022 van de Autoriteit met betrekking tot een voorontwerp van wet betreffende de gemeentelijke bestuurlijke handhaving, de instelling van een gemeentelijk integriteitsonderzoek en houdende oprichting van een Directie Integriteitsbeoordeling voor Openbare Besturen (CO-A-2022-248),* overwegingen 18 en volgende.

[152] Artikel 14, § 1,3° van het ontwerp.

bedoeld in de artikelen 7, 1°[153], *en 3°/1*[154], *en 11, § 1,*[155] 1°, 2°, 3°, en 5° *van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten*». **Maar** zoals eerder benadrukt, kan ETIAS worden geraadpleegd door de autoriteiten die door de lidstaten zijn aangewezen op het gebied van het **voorkomen, opsporen en onderzoeken van terroristische misdrijven of andere ernstige strafbare feiten**, welke laatste twee begrippen overigens (restrictief) zijn gedefinieerd in de ETIAS-verordening[156]. Het moet gezegd dat de doelen die worden nagestreefd door de VSSE en de ADIV die met het ontwerp worden beoogd, **verder gaan dan wat is toegestaan volgens de ETIAS-verordening**. De Autoriteit vroeg de aanvrager naar een rechtvaardiging voor de uitbreiding van de doeleinden van de ETIAS-raadpleging die via het ontwerp wordt uitgevoerd en de aanvrager antwoordde als volgt (de Autoriteit vertaalt) :

« *Zie de Memorie van Toelichting, bladzijde 5.*

---

[153] « *1° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel, zoals gedefinieerd door de Nationale Veiligheidsraad, of elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad, bedreigt of zou kunnen bedreigen» (onderstreept door de Autoriteit).*

[154] Het betreft «*het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied*» (onderstreept door de Autoriteit).

[155] *Het betreft « 1° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties, alsook de inlichtingen die betrekking hebben op elke activiteit die:*

a) de onschendbaarheid van het nationaal grondgebied of de bevolking,,

b) de militaire defensieplannen,,

c) het wetenschappelijk en economisch potentieel met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren die verbonden zijn met defensie en die opgenomen zijn in een op voorstel van de minister van Justitie en de minister van Landsverdediging door de Nationale Veiligheidsraad goedgekeurde lijst,

d) de vervulling van de opdrachten van de strijdkrachten,,

e) de veiligheid van de Belgische onderdanen in het buitenland, ,

f) elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad,

bedreigt of zou kunnen bedreigen en er de bevoegde ministers onverwijld over inlichten alsook de regering, op haar verzoek, advies te verlenen bij de omschrijving van haar binnen- en buitenlands beleid inzake veiligheid en defensie

2° het zorgen voor het behoud van de militaire veiligheid van het personeel dat onder de Minister van Landsverdediging ressorteert, dew militaire installaties, wapens en wapensystemen, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen en, in het kader van de cyberaanvallen op wapensystemen, militaire informatica- en verbindingssystemen of systemen die de Minister van Landsverdediging beheert, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het internationaal recht ;,

[…]

5° Het betreft «het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied » (onderstreept door de Autoriteit).

[156] Zie artikel 3,1, 2 van de ETIAS-verordening. Artikel 3, 1, 15 van de ETIAS-verordening definieert **terroristische misdrijf** als: «*strafbaar feit dat overeenkomt met of gelijkwaardig is aan een van de in Richtlijn (EU) 2017/541 bedoelde misdrijven*» van het Europees Parlement en de Raad van 15 maart 2017 *inzake terrorismebestrijding en ter vervanging van Kaderbesluit 2002/475/JBZ van de Raad en tot wijziging van Besluit 2005/671/JBZ van de Raad.*

Artikel 3, 1, 16 van de ETIAS-verordening definieert **ernstige strafbaar feit** als: «*strafbaar feit dat overeenkomt met of gelijkwaardig zijn aan een van de in artikel 2, lid 2, van Kaderbesluit 2002/584/JBZ bedoelde strafbare feiten, indien het naar nationaal recht strafbaar is gesteld met een vrijheidsstraf of een tot vrijheids beneming strekkende maatregel met een maximumduur van ten minste drie jaar* ».

Er is besloten om, naar het voorbeeld van de passagiersinformatie-eenheid (PNR-systeem), ook inlichtingen- en veiligheidsdiensten te betrekken bij de verwerking voor repressieve doeleinden, omdat zij een belangrijke rol spelen bij het opsporen en voorkomen van terroristische misdrijven en andere vormen van zware criminaliteit die onder de verordening vallen. Ook moet met deze twee elementen rekening worden gehouden
- België is een bijzonder "risicoland" vanuit veiligheidsoogpunt, zowel als gastland voor de EU en de NAVO in het bijzonder, als een internationaal transportknooppunt dat door criminele organisaties als "draaischijf" kan worden gebruikt;
- criminele verschijnselen zijn in toenemende mate hybride en de opsporing van bedreigingen vereist een geïntegreerde en complementaire aanpak van de verschillende betrokken diensten.

Wij waren van mening dat het niet nodig was om een punt 3° toe te voegen aan artikel 14, §1 van het ontwer omdat het verzoek om raadpleging de precieze inbreuk in kwestie zal moeten vermelden (artikel 14, §2 van het ontwerp), met dien verstande dat deze inbreuk een van de in de punten 1° en 2° bedoelde is. De inlichtingen- en veiligheidsdiensten hebben er echter op aangedrongen een punt 3° toe te voegen, ten minste totdat het Grondwettelijk Hof het formeel ongeldig heeft verklaard (zie zaak Liga voor de rechten van de mens, HvJEU C-817/19, vijfde prejudiciële vraag, uitspraak Grondwettelijk Hof afgewacht - rolnummer 6713)»
(onderstreping toegevoegd door de Autoriteit).

96. De Autoriteit is van mening dat **het dispositief van het ontwerp zodanig moeten worden aangepast dat de VSSE en de ADIV bij de uitvoering van het ontwerp, ETIAS alleen mogen raadplegen** (en meer in het algemeen, alleen met het ETIAS-ecosysteem mogen interageren) **wanneer zij hun bevoegdheden uitoefenen *voor het doel dat ETIAS nastreeft***, d.w.z. voor repressieve doeleindenzoals exhaustief gedefinieerd in de ETIAS-verordening[157] (en **dit onverminderd de voorgaande redenering met betrekking tot het gegevensbeschermingsrecht dat van toepassing is op deze diensten en de ter zake bevoegde toezichthoudende autoriteit)**)[158]. Als de Belgische staat de inlichtingen- en veiligheidsdiensten wil aansluiten bij de operationele eenheden die toegang hebben tot het centrale ETIAS-systeem, kan dat alleen binnen de grenzen die de ETIAS-verordening zelf stelt en met andere woorden in het kader van het voorkomen, opsporen en onderzoeken van strafbare feiten die onder de ETIAS-verordening vallen en onder de voorwaarden die deze verordening stelt. Als dit niet het geval zou zijn, zou het ontwerp geen rekening houden met de afbakening van de doeleinden van het ETIAS-systeem en zou het in strijd zijn met de beginselen van rechtmatigheid van de verwerking en het doel.

[157] In gelijkaardige zin, zie het HvJEU (Gr. Ch.), 21 juni 2022 (LIGA VAN DE MENSENRECHTEN VS/MINISTERRAAD), zaak C-817/19, overwegingen 230-237.

[158] Zie de overwegingen 22-26 en 31.

Met andere woorden, de Autoriteit is van mening dat artikel 14, §1, 3°, van het ontwerp moet worden weggelaten.

97. **Deze bevinding heeft ook directe gevolgen voor artikel 21 van het ontwerp, dat de VSSE en de ADIV toestaat gegevens in de ETIAS observatielijst op te nemen voor de in artikel 14, § 1 van het ontwerp genoemde doeleinden.** Nogmaals, het doel van de ETIAS-verordening kan niet worden omzeild door een regel van Belgisch recht.

II.3.3. <u>Centraal toegangspunt</u>

98. De **NCC-sectie** wordt aangewezen als centraal toegangspunt en "*verifieert op onafhankelijke wijze*" of aan de toegangsvoorwaarden van artikel 52 van de ETIAS-verordening is voldaan[159].

99. Zoals de Autoriteit al heeft opgemerkt, moet uit het ontwerp duidelijk blijken dat het de **leidende ambtenaar** is die de beslissingen op dit gebied neemt. Dit is des te belangrijker omdat de gedetacheerde leden afkomstig zijn van de diensten die de gegevens raadplegen. Met andere woorden, hun directe betrokkenheid bij het onafhankelijke verificatieproces dat door de ETIAS-verordening wordt vereist, zal in dit opzicht waarschijnlijk problemen veroorzaken, des te meer om de volgende drie extra redenen.

100. Vooreerst bepaalt de memorie van toelichting het volgende «*de hiërarchische autoriteit blijft ook bij de oorspronkelijke diensten berusten voor wat betreft de beoordeling van de gedetacheerden en disciplinaire zaken* »[160]. Ten tweede wordt ook bepaald dat gedetacheerde leden hun functies voor hun oorspronkelijke diensten in het kader van ETIAS blijven vervullen, bij de actualisering van de ETIAS-observatielijst[161]. En ten derde bevat het ontwerp geen specifieke voorwaarden voor detachering (duur, mogelijkheid van beëindiging, door wie en onder welke voorwaarden, enz.).

101. **In dit verband is de Autoriteit van mening dat gedetacheerde leden niet betrokken kunnen worden bij het verificatieproces dat onder de verantwoordelijkheid van het centraal toegangspunt valt, een proces dat onder de bevoegdheid van ander personeel van de NCC-**

---

[159] Artikel 16 van het ontwerp. Meer in detail wordt in artikel 50, 2, leden 2 en 3, van de ETIAS-verordening het volgende bepaald :

« *Indien het nationale recht dit toestaat, <u>kunnen</u> de aangewezen autoriteiten het centrale toegangspunt <u>deel uitmaken van dezelfde organisatie</u>, maar het centrale toegangspunt <u>treedt</u> bij de uitvoering van zijn taken op grond van deze verordening <u>volledig onafhankelijk van de aangewezen autoriteiten op</u>. Het centrale toegangspunt <u>staat los van de aangewezen autoriteiten en ontvangt van dezen geen instructies</u> met betrekking tot de resultaten van de verificatie, die het onafhankelijk verricht.*

De lidstaten kunnen, afhankelijk van hun organisatorische en bestuurlijke structuur, meer dan één centraal toegangspunt aanwijzen om hun grondwettelijke of andere wettelijke vereisten na te komen» (onderstreept door de Autoriteit).

[160] Blz. 10.

[161] « *Wanneer zij een opdracht van hun diensten uitvoeren, zijn zij verantwoording verschuldigd aan hun hiërarchie. Het bijwerken van de gegevens van de observatielijst moet worden gecontroleerd door de hiërarchie van de oorspronkelijke diensten, en niet door de leidend ambtenaar van de sectie*», blz. 10.

sectie moet vallen. De bepalingen van het ontwerp moeten hierin voorzien, aangezien het ontwerp in zijn huidige vorm hierover zwijgt.

II.4. VERWERKINGSVERANTWOORDELIJKEN

102. Naast het vaststellen van de verantwoordelijkheid van de betrokken Europese instellingen (met inbegrip van eu-LISA), bepaalt de ETIAS-verordening rechtstreeks « *dat in het centrale Etias-systeem door een lidstaat* ***wordt de nationale Etias-eenheid*** *beschouwd als* ***verwerkingsverantwoordelijke***» als bedoeld in de AVG; zij «Zij draagt ***de centrale verantwoordelijkheid*** voor de verwerking van persoonsgegevens in het centrale Etias-systeem door die lidstaat» *voor de verwerking* »[162]van persoonsgegevens in het centrale systeem van ETIAS door de betrokken lidstaat (vet toegevoegd en onderstreept door de Autoriteit).

103. Artikel 32, 1ste lid van het ontwerp bepaalt daarentegen ook «*de voorzitter van de FOD Binnelandse Zaken (is) operationeel verantwoordelijk voor de verwerking van persoonsgegevens in het centrale ETIAS-systeem. In die hoedanigheid ziet hij erop toe dat de toegang voor de in artikel 13, leden 2, 4, 4bis en 4ter van de ETIAS-verordening bedoelde autoriteiten beperkt blijft tot naar behoren gemachtigde personen en de in de verordening omschreven verwerkingsdoeleinden respecteert» (onderstreept door de Autoriteit).*

104. Betreffende de aanwijzing van de verwerkingsverantwoordelijken herinnert de Autoriteit aan haar vaste adviespraktijk **dat een overheidsinstantie in beginsel verantwoordelijk is voor de verwerking van gegevens die noodzakelijk is voor de vervulling van de haar toevertrouwde openbare opdracht of wettelijke verplichting[163] die, krachtens de**

[162] Artikel 57, 2 van de ETIAS-verordening.

[163] Voor een toepassing in het domein van de dreigingsanalyse, zie het advies van de Autoriteit 184/2021 van 4 oktober 2021 *met betrekking tot een voorontwerp van wet tot wijziging van de wet van 10 juli 2006 betreffende de analyse van de dreiging (CO-A-2021-174)*, overwegingen 36-38.

betrokken norm[164, 165] **binnen de werkingssfeer van het aan haar toevertrouwde openbaar gezag valt.** De verwerkingsverantwoordelijken kunnen bovendien **gezamenlijke**[166]. verantwoordelijken zijn. De bedoeling van een ruime definitie van het concept verwerkingsverantwoordelijke[167] is het verzekeren van een efficiënte en volledige bescherming van de betrokkenen[168]. In feite kan een gezamenlijke verwerkingsverantwoordelijkheid meerdere actoren binden, waarbij de betrokkene zijn rechten met betrekking tot en jegens ieder van hen kan uitoefenen[169]. Echter, « *het bestaan van een gezamenlijke verantwoordelijkheid uit zich niet noodzakelijkerwijs in een gelijkwaardige* verantwoordelijkheid [… en] *deze* actoren *kunnen juist in verschillende stadia en in verschillende mate bij de verwerking betrokken zijn, zodat het niveau van verantwoordelijkheid van elk van hen moet worden beoordeeld in het licht van alle relevante omstandigheden van het geval»* »[170]. Het is in «*het kader van zijn verantwoordelijkheden, zijn bevoegdheden en zijn mogelijkheden*" dat de gezamenlijke verwerkingsverantwoordelijke ervoor zal zorgen dat zijn activiteit in overeenstemming is met de regels inzake gegevensbescherming[171]. De gezamenlijke verwerkingsverantwoordelijken zullen een **overeenkomst moeten sluiten waarin**

---

[164] En de verantwoordelijkheid voor de verwerking kan betrekking hebben op verplichtingen/taken van technische aard met betrekking tot deze verwerking, zie bijvoorbeeld artikel 57, lid 1, van de ETIAS-verordening (verantwoordelijkheid van eu-LISA met betrekking tot de beveiliging van informatie in het centrale systeem van ETIAS, en

Over de praktijk van de Autoriteit met betrekking tot het aanwijzen van de verwerkingsverantwoordelijke, zie : advies nr. 129/2022 van 1 juli 2022 *betreffende de artikelen 2 en 7 tot en met 47 van een ontwerp van wet houdende diverse bepalingen inzake Economie,* overweging 42 en volgende; *advies 131/2022 van 1 juli 2022 met betrekking tot een wetsontwerp tot oprichting van de Kunstwerkcommissie en ter verbetering van de sociale bescherming van de kunstwerkers, overwegingen 55 en volgende;* advies nr. 112/2022 van 3 juni 2022 *met betrekking tot een ontwerp van wet tot wijziging van het Sociaal Strafwetboek met het oog op de invoering van het eDossier-platform* , overwegingen nrs. 3-41 en 87-88; advies nr. 231/2021 van *3 december 2021 met betrekking tot een voorontwerp van ordonnantie betreffende de interoperabiliteit van elektronische tolheffingssystemen voor het wegverkeer*, overwegingen nrs. 35-37; advies nr. 37/2022 van 16 *februari 2022 "concernant un avant-projet de décret instituant la plateforme informatisée centralisée d'échange de données 'E-Paysage'"* (nog niet beschikbaar in het Nederlands*), overweging nr. 22; advies nr. 13/2022 van 21 januari 2022 met betrekking tot een ontwerp van besluit van de Brusselse Hoofdstedelijke Regering betreffende de toekenning van premies voor de verbetering van het woonmilieu en een ontwerp van besluit van de Brusselse Hoofdstedelijke Regering tot wijziging van het besluit van de Brusselse Hoofdstedelijke Regering van 9 februari 2012 betreffende de toekenning van* financiële steun voor energie; overwegingen nrs. 9-17; advies nr. 65/2019 van 27 *februari 2019 betreffende een ontwerp van samenwerkingsakkoord tot wijziging van het samenwerkingsakkoord van 23 mei 2013 tussen het Waalse Gewest en de Franse Gemeenschap over het opstarten van een gemeenschappelijk initiatief om gegevens te delen en over het gemeenschappelijk beheer van dit initiatief,* overwegingen nrs. 90-113.

[165] Zie in dezelfde zin eveneens de conclusie van advocaat-generaal L. Medina uiteengezet op 8 juni 2023 in de zaak C-231/22, *Belgische staat vs/Gegevensbeschermingsautoriteit*.

[166] Voor een toepassing in het domein van de **dreigingsanalys**e, zie het advies van de Autoriteit 184/2021 van 4 oktober 2021 *met betrekking tot een voorontwerp van wet tot wijziging van de wet van 10 juli 2006 betreffende de analyse van de dreiging (CO-A-2021-174)*, overwegingen 59-62.

Voor een toepassing in het kader van **EES**,.zie het voornoemd advies 122/2022 van de Autoriteit d.d. 1 juli 2022, voetnoot 9.

Voor een toepassing in het kader van **SIS,** zie het voornoemd advies van de Autoriteit 121/2022 van 1 juli 2022, overwegingen 17 en 25 ev.

[167] De begrippen verwerkingsverantwoordelijke en verwerker zijn gedefinieerd in artikel 4, punten 7) en 8) van de AVG. Lees eveneens het Advies G29, nr. 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", (WP169), 16 februari 2010.

[168] HvJ-EU, (Gr. Kam.), 13 mei 2014 (GOOGLE SPAIN SL, GOOGLE INC. tegen AEPD), zaak C-132/12, punt 34. HvJ-EU, (Gr. Kam. , 5 juni 2018 (UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIM tegen Wirtschaftsakademie SCHLESWIG-HOLSTEIN GMBH), zaak C-210/16, punt 28.

[169] Artikel 26, lid 3, van de AVG.

[170] HvJ-EU, (Gr. Ka. , 5 juni 2018 (UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIM TEGEN WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN GMBH), zaak C-210/16, punt 43. Lees ook het Advies G29, 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", 16 februari 2010, blz. 20.

[171] EHvJ, (Gr. Ka.), 13 mei 2014 (GOOGLE SPAIN SL, GOOGLE INC. tegen AEPD), zaak C-132/12, punt 38.

hun respectieve verantwoordelijkheden worden bepaald, « *behalve indien en voor zover hun respectieve verplichtingen zijn vastgelegd* in de relevante nationale normatieve context[172].

105. De Autoriteit wijst erop dat de begrippen «*centrale*» (ETIAS-verordening) en «*operationele*» (ontwerp) verantwoordelijkheden niet bestaan in de AVG. Daarom is zij van **mening dat het begrip «*operationele verantwoordelijkheid voor de verwerking* uit het ontwerp moet worden weggelaten »**.

106. De **ETIAS-verordening bepaalt uitdrukkelijk dat de betrokkene zijn rechten kan uitoefenen bij de centrale eenheid van ETIAS of bij E.N.E**[173]. Voor het overige zorgen de ETIAS-verordening en het ontwerp voor een verdeling van taken en verantwoordelijkheden tussen de betrokken nationale en Europese overheidsinstanties, die samen en onlosmakelijk deelnemen aan de verwezenlijking van de doeleinden van de ETIAS-verordening. De Autoriteit is van mening dat deze autoriteiten in een situatie van **gezamenlijke verantwoordelijkheid verkeren met betrekking tot de verwerking van persoonsgegevens** in het kader van het ontwerp en de ETIAS-verordening**, waarbij elke autoriteit verantwoordelijk is voor de verwerking voor zover het haar verplichtingen en taken in het kader van het ontwerp en de ETIAS-verordening betreft**, **en in overeenstemming met de regels inzake gegevensbescherming die op haar van toepassing zijn[174]**.

107. Dit belet niet dat het ontwerp een specifieke verantwoordelijkheid inzake verwerking toekent aan de voorzitter van de FOD Binnenlandse Zaken, die voortvloeit uit verplichtingen die het ontwerp hem oplegt. In zijn huidige vorm legt artikel 32 van het ontwerp een bijzondere verantwoordelijkheid op wat betreft de technische en organisatorische maatregelen die moeten worden uitgevoerd, en wat betreft *accountability*.

108. Bovendien zullen deze verantwoordelijkheden worden georganiseerd volgens de doeleinden van ETIAS[175], met inbegrip van risicopreventie en raadpleging voor repressieve doeleinden[176]. De rol van de verschillende betrokken autoriteiten variëren afhankelijk van de doelen en opdrachten die worden nagestreefd, net als de materiële toepasselijke regels voor gegevensbescherming.

---

[172] Artikel 26, 1, *in fine*, van de AVG.

[173] Zie artikel 64, 2,van de ETIAS-verordening.

[174] Als een overheidsinstantie bijvoorbeeld een risico beoordeelt in overeenstemming met de regels van titel 2 of titel 3 van de WVG, voorkomt dit niet dat de persoonsgegevens die zij voor de uitvoering van haar eigen taken aan een andere instantie verstrekt, door die instantie moeten worden verwerkt in overeenstemming met de AVG als ze binnen het toepassingsgebied van de AVG vallen. Zie met name het advies van de Autoriteit 184/2021 van 4 oktober 2021 *met betrekking tot een voorontwerp van wet tot wijziging van de wet van 10 juli 2006 betreffende de analyse van de dreiging (CO-A-2021-174)*, overweging 12.

[175] Zie de overwegingen 13-27.

[176] Zie de overwegingen 28-30.

II.5. <u>SANCTIES SPECIFIEK VOOR DE ETIAS-VERORDENING</u>

109. Artikel 62 van de ETIAS-verordening, dat is opgenomen in een titel over gegevensbescherming, bepaalt dat de lidstaten een sanctieregeling moeten vaststellen (doeltreffend, evenredig en afschrikkend) die van toepassing is in geval van schending van de verordening. Le Projet ne prévoit rien en la matière de telle sorte que l'Autorité a interrogé le demandeur à ce sujet. Hij antwoordde het volgende (de Autoriteit vertaalt):

> « *Wij waren van mening dat deze bepaling, die is opgenomen in het hoofdstuk Gegevensbescherming van de verordening, met name gericht was op inbreuken op de toepasselijke wetgeving inzake gegevensbescherming. Wij <u>waren daarom van mening dat de sancties van de wet van 2018 van toepassing waren en dat het niet nodig was om een bepaling over dit onderwerp in het ontwerp op te nemen</u>* » (onderstreping toegevoegd door de Autoriteit).

110. De Autoriteit neemt akte van deze motivering. Dit gezegd zijnde, is het duidelijk dat de auteurs van de ETIAS-verordening het nuttig achtten om een dergelijke bepaling op te nemen, aangezien zij zich volledig bewust waren van het bestaan van de AVG en Richtlijn 2016/680 en de regels voor de uitvoering/omzetting daarvan in nationaal recht.

111. In deze omstandigheden **verzoekt de Autoriteit de aanvrager de mogelijkheid van specifieke sancties te overwegen die van toepassing zouden kunnen zijn in het kader van de ETIAS-verordening**. Het onderwerp van de ontvankelijkheid van bewijs en vervolging kan bijvoorbeeld worden verkend, voor zover dit relevant is, enz.

112. In het algemeen is de Autoriteit van mening dat het ontwerp een specifieke verplichting voor E.N.E. moet bevatten om een samenvattend en geanonimiseerd verslag te publiceren over inbreuken op de gegevensbescherming die door de toezichthoudende autoriteiten zijn vastgesteld, met name na de audits die zij moeten uitvoeren. Een dergelijke transparantie zal waarschijnlijk zorgen voor een betere controle door de samenleving van de activiteiten van de E.N.E., en daarmee voor een grotere doeltreffendheid van de regels inzake gegevensbescherming. Terloops herinnert de Autoriteit eraan dat «*Iedere toezichthoudende autoriteit dient te beschikken over de financiële en personele middelen, dienstruimten en infrastructuur die* […] *noodzakelijk zijn om haar taken, waaronder die in het kader van wederzijdse bijstand en samenwerking met andere toezichthoudende autoriteiten in de Unie, effectief uit te voeren* »[177]. De bovengenoemde publicatie moet ook in deze context worden geplaatst, aangezien de ETIAS-verordening gevolgen zal hebben voor de werklast van deze autoriteiten.

[177] Overweging 120 AVG.

II.6. VARIA

II.6.1. Toezichthoudende autoriteit AGD&A

113. De Autoriteit vestigt de aandacht van de aanvrager op het feit dat de AGD&A, zelfs wanneer zij handelt in het kader van titel 2 van de WVG, **onderworpen blijft aan de controle van de Gegevensbeschermingsautoriteit**[178]. Artikel 34 van het ontwerp, betreffende de toegang tot ETIAS voor repressieve doeleinden[179], wijzigt echter alleen artikel 281 van de Algemene Douane- en Accijnswet van 18 juli 1977[180]. De aan het COC verleende bevoegdheid met betrekking tot de AGD&A in het kader van de werking van de UIP, vereiste een **wijziging van artikel 71 van de WVG**[181]. In overeenstemming met het ontwerp moet het COC ook door AGD&A worden aangewezen voor toegang tot ETIAS voor repressieve doeleinden, via een wijziging van artikel 71 van de WVG.

II.6.2. Technische Instrumenten

---

[178] Zie voetnoot nr. 107.

[179] Voor de beoordeling van veiligheidsrisico's moeten de AGD&A onder de bevoegdheid van de gGgevensbeschermingsautoriteit blijven vallen, zie overweging 17.

[180] Deze luidt als volgt:

« *"Art. 281. § 1. Alle vorderingen wegens overtredingen, fraudes en misdrijven, waartegen bij de wetten inzake douane en accijnzen, straffen zijn bepaald, zullen in eerste aanleg worden gebracht voor de correctionele rechtbanken, en, in geval van hoger beroep, voor het hof van beroep van het rechtsgebied, ten einde te worden geïnstrueerd en berecht overeenkomstig het wetboek van Strafvordering.*

§ 2. Alle bovengemelde vorderingen, welke strekken tot toepassing van boeten, verbeurdverklaringen of het sluiten van fabrieken of werkplaatsen, zullen voor dezelfde rechtbanken worden aangelegd en vervolgd, door of in naam van de administratie; echter zullen deze daarin geen recht spreken, dan na de conclusies van het openbaar ministerie te hebben gehoord. Evenwel mag, op schriftelijk verzoek hem daartoe gedaan door een ambtenaar van de Algemene Administratie van de Douane en Accijnzen met minstens de graad van adviseur-generaal die aangewezen is voor de administratie bevoegd voor de geschillen[3], het openbaar ministerie de onderzoeksrechter vorderen te informeren, alhoewel de uitoefening van de publieke vordering voor het overige aan de administratie voorbehouden blijft.

§ 3. In die gevallen, dat uit dezelfde daad van overtreding van de voormelde wetten twee verschillende vorderingen voortspruiten, waarvan de ene door het openbaar ministerie en de andere door of namens de administratie moet worden ingesteld, zullen beide vorderingen gelijktijdig worden geïnstrueerd en bij één en hetzelfde vonnis worden rechtgesproken; in dat geval zal door het openbaar ministerie niet worden geageerd, alvorens de administratie van hare zijde aanklacht heeft gedaan of de vordering ingesteld.

§ 4. Bij het opsporen van de misdaden en wanbedrijven bedoeld in artikel 8, § 1, 5°, van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, kan de adviseur-generaal die aangewezen is voor het departement geschillen, bij een schriftelijke en met redenen omklede beslissing, de ambtenaar van de douane en accijnzen opdragen de PIE te vorderen tot het meedelen van de passagiersgegevens overeenkomstig artikel 27 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens.

De motivering weerspiegelt de proportionaliteit met inachtneming van de bescherming van persoonsgegevens en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.

De motivering van de beslissing weerspiegelt de proportionaliteit met inachtneming van de bescherming van persoonsgegevens en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.

Het Controleorgaan op de politionele informatie verbiedt de adviseur-generaal die aangewezen is voor het departement geschillen om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen ».

[181] Zie artikel 13 van de wet van 2 mei 2019 **tot wijziging van diverse bepalingen betreffende de verwerking van passagiersgegevens**, dat het volgende bepaalt:

« *Artikel 71, § 1, van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, wordt aangevuld met een lid luidende:*

Zij is eveneens ten aanzien van de bevoegde overheid bedoeld in artikel 26, § 1, 7°, e), belast met het toezicht op de toepassing van artikel 281, § 4, van de algemene wet inzake douane en accijnzen van 18 juli 1977» (onderstreept door de Autoriteit).

114. Artikel 25, § 1, van het Ontwerp verwijst naar de «*nationale technische instrumenten die nodig zijn voor de uitvoering van de opdrachten*» waarmee de leidende ambtenaar en de personen in zijn sectie belast zijn. De Autoriteit vroeg de aanvrager wat werd bedoeld met «*technische instrumenten*» en de aanvrager antwoordde als volgt (de Autoriteit vertaalt) :

> « *De instrumenten eigen aan ENE: De Beltias nationale applicatie die nodig is voor het beheer van de observatielijst en raadplegingsverzoeken (vermeld in de toelichting, p. 14), en de in het ontwerp voorziene toegang tot het RR en het strafregister.*
>
> *Er zijn verschillende IT-tools nodig om de opdrachten van de ENE te vergemakkelijken: JBOX of ander systeem voor elektronische uitwisseling van processtukken voor beroepsprocedures, Teams aanvraag voor gesprekken*[182]*,…*
>
> *We hebben deze algemene term gebruikt omdat deze instrumenten kunnen evolueren*" (onderstreping toegevoegd door de Autoriteit).

115. De Autoriteit neemt nota van deze uitleg en van het feit **dat het doel van deze bepaling niet is om de verwerking van persoonsgegevens te reguleren**.

II.6.3. Mededeling van gegevens aan landen die geen lid zijn van de Unie

116. **Onverminderd de verschillende opmerkingen die reeds zijn gemaakt over de rol van inlichtingen- en veiligheidsdiensten in het kader van de ETIAS-verordening**, voorziet artikel 20 van het ontwerp in de mogelijkheid dat deze diensten op grond van de artikelen 93 en 94 van de WVG en onder de in deze bepaling zelf vastgestelde voorwaarden gegevens meedelen aan landen die geen lid zijn van de Europese Unie. Artikel 65 van de ETIAS-verordening biedt een kader voor deze grensoverschrijdende stromen. Artikel 65, 2 van de ETIAS-verordening verankert een zeer algemeen verbod dat ook geldt «*indien deze gegevens op nationaal niveau of tussen de lidstaten verder worden verwerkt* ».

117. Een van de relevante uitzonderingen **is artikel 65, 5,** van de ETIAS-verordening, dat betrekking heeft op de mededeling van gegevens als bedoeld in artikel 52, 4, van de ETIAS-verordening, na raadpleging voor repressieve doeleindenen binnen de in die bepaling vastgestelde grenzen[183]. In het bijzonder kan een dergelijke doorgifte alleen worden uitgevoerd in overeenstemming met de relevante bepalingen

[182] Wat betreft de audiovisuele middelen die voor het ondervraging worden gebruikt, zie **Uitvoeringsbesluit (EU) 2022/1462 van de Commissie van 2 september 2022** *betreffende de vereisten die van toepassing zijn op audiovisuele communicatiemiddelen die worden gebruikt voor het ondervraging overeenkomstig artikel 27, §5, van Verordening (EU) 2018/1240 van het Europees Parlement en de Raad*.

[183] Artikel 65, 3, verwijst naar het specifieke geval van terugkeer, dat niet relevant is voor artikel 20 van het ontwerp.

van Richtlijn 2016/680, en uit de ETIAS-verordening volgt dat deze dan onderworpen is aan de toezichthoudende autoriteit die is aangewezen overeenkomstig artikel 41, 1, van Richtlijn 2016/680. **De Belgische wetgever heeft terzake geen speelruimte en artikel 20 van het ontwerp moet dan ook worden weggelaten of zodanig worden aangepast dat de inlichtingen- en veiligheidsdiensten hiertoe worden beschouwd als bevoegde autoriteiten die onder titel 2 van de WVG vallen** (met aanwijzing van de bevoegde toezichthoudende autoriteit).

Om deze redenen,
oordeelt de Autoriteit als volgt :

1. de ETIAS-verordening en het ontwerp betekenen een aanzienlijke inbreuk op de rechten en vrijheden van de betrokkenen **(overweging nr. 8**) ;

2. artikel 31§ 2 van het ontwerp kan voorzien in de toepassing van titel 2 van de WVG op de "beoordeling van veiligheidsrisico's", op voorwaarde dat de Gegevensbeschermingsautoriteit in dit verband de bevoegde toezichthoudende autoriteit is, behalve wat betreft de bevoegdheid van het COC met betrekking tot politiediensten, aangezien het COC ook is aangewezen als toezichthoudende autoriteit in het kader van de AVG **(overwegingen 14 en 17-19**) ;

3. het ontwerp moet worden herzien met betrekking tot de regels inzake gegevensbeschermingsrecht die van toepassing zijn op inlichtingen- en veiligheidsdiensten en de voor hen bevoegde autoriteit, enerzijds, de leden die zijn gedetacheerd voor de beoordeling van veiligheidsrisico's en, anderzijds, de toegang tot ETIAS voor repressieve doeleinden**(overwegingen 22-26 en 31**) ;

4. artikel 21 van het ontwerp moet worden aangepast omdat het verwijst naar de repressieve doeleinden van ETIAS in plaats van het doeleinde dat erin bestaat veiligheidsrisico's te voorkomen. Het kan ook voorzien in de toepassing van titel 2 van de WVG met het oog op het voeden van de ETIAS observatielijst, op voorwaarde dat de Gegevensbeschermingsautoriteit de bevoegde toezichthoudende autoriteit is, behalve in het geval van de politiediensten **(overwegingen 17 en 21**) ;

5. ETIAS doet vragen rijzen over de naleving van het gelijkheidsbeginsel tussen mensen die een visum nodig hebben en mensen die een reisautorisatie nodig hebben krachtrens ETIAS **(overwegingen 40-41**) ;

6. het dispositief van het ontwerp mag niet beperkt blijven tot het bieden van een mogelijkheid om een persoon toe te voegen aan de ETIAS-observatielijst, maar moeten de voorwaarden bevatten waaronder de betrokken autoriteiten een persoon moeten melden op de ETIAS-observatielijst**48**) ;

7. het ontwerp moet de essentiële elementen van de gegevensverwerking bepalen die nodig zijn voor de bijdrage van de Belgische Staat tot de vaststelling van specifieke risico-indicatoren **(overwegingen 49-53**) ;

8. in het dispositief van het ontwerp moeten de *"nodige gegevensbanken*" worden vermeld die door de gedetacheerde leden moeten worden geraadpleegd voor het uitvoeren van de veiligheidsrisicobeoordeling, onder het gezag van het hoofd van de sectie NCC van de E.N.E. **(Overwegingen 58-61**) ;

9. in artikel 27 van het ontwerp moet duidelijk worden vermeld dat de sectie VZ van de E.N.E. verantwoordelijk is voor de beoordeling van het risico van illegale immigratie. En het ontwerp moet nog bepalen welke (categorieën) persoonsgegevens en informatiesystemen voor dit doel zullen worden hergebruikt **(overwegingen 62-64**) ;

10. in het dispositief van het ontwerp zelf moet worden vermeld dat de leidende ambtenaar beslissingen neemt namens de sectie waaraan hij of zij leiding geeft **(overwegingen 67-68**);

11. een beroep met volle rechtsmacht tegen de beslissingen van de E.N.E. vormt a priori een betere garantie voor de rechten en vrijheden van de betrokken personen en in de memorie van toelichting bij het wijzigingsontwerp moet in elk geval worden gemotiveerd waarom een beroep tot annulatie eerder noodzakelijk zou zijn **(overwegingen 71-72**) ;

de invoering van een beroep in volle rechtsmacht is des te meer gerechtvaardigd met betrekking tot beslissingen van de E.N.E. inzake de rectificatie of verwijdering van persoonsgegevens, zodat in dit geval in een dergelijk beroep moet worden voorzien door het wijzigingsontwerp (**overwegingen 77-78**) ;

12. het wijzigingsontwerp moet verduidelijken dat een negatief advies van een afdeling van de E.N.E. in het kader van de in artikel 28 van de ETIAS-verordening bedoelde raadplegingen een beslissing vormt waartegen beroep kan wordeningesteld **(overweging 73**) ;

13. het dispositief van het ontwerp moet worden aangepast en duidelijk garanderen dat de betrokkene recht heeft op toegang tot de risicobeoordeling die op hem of haar is uitgevoerd en op basis waarvan E.N.E. een administratieve beslissing over hem of haar neemt **(overwegingen 74-76.**) ;

14. het dispositief van het ontwerp moet de voorwaarden bepalen waaronder de betrokken autoriteiten aan E.N.E. persoonsgegevens moeten meedelen die kunnen leiden tot de annulatie of intrekking van een reisautorisatie **(overwegingen 79-81**) ;

15. in een norm (en niet in een beslissing van de betrokken diensten) moet worden vastgesteld welke operationele eenheden, als bedoeld in de ETIAS-verordening, verzoeken om raadpleging van ETIAS voor repressieve doeleinden mogen indienen **(overwegingen 89-90**) ;

16. artikel 31, §§ 2 en 3, van het ontwerp moet worden aangepast om te verduidelijken dat het verwijst naar raadpleging van ETIAS voor repressieve doeleinden **(overweging 91**) ;

17. het ontwerp moet de relevante strafbare feiten naar Belgisch recht vaststellen die vallen onder de zware criminaliteit waarop de ETIAS-verordening van toepassing is**94**) ;

18. het ontwerp moet worden gewijzigd (met name artikel 14, § 1, 3°, moet worden weggelaten) omdat het de doelstellingen van ETIAS wil uitbreiden tot andere doeleinden van inlichtingen- en veiligheidsdiensten, in tegenstelling tot wat de ETIAS-verordening toestaat **(overwegingen 95-97**) ;

19. gedetacheerde leden mogen niet betrokken zijn bij het verificatieproces dat wordt uitgevoerd door het centrale toegangspunt; dit moet de verantwoordelijkheid zijn van ander personeel van de NCC-sectie. Het dispositief zou daarin moeten voorzien, aangezien het in zijn huidige vorm op dit punt zwijgt **(overwegingen 98-101**) ;

20. de ETIAS-verordening en het ontwerp organiseren gezamenlijke verantwoordelijkheden met betrekking tot gegevensverwerking en het ontwerp moet dienovereenkomstig worden aangepast **(overwegingen 102-108**) ;

21. de aanvrager moet de mogelijkheid onderzoeken om specifieke sancties op te leggen voor inbreuken op de gegevensbeschermingsregels bij de uitvoering van de ETIAS-verordening **(overwegingen 109-111**) ;

22. het ontwerp moet artikel 71 van de WVG wijzigen zodat het COC ook de controleautoriteit van de AGD&A is wanneer de AGD&A ETIAS raadpleegt voor repressieve doeleinden **(overweging 113**) ;

23. artikel 25, § 1, van het ontwerp (waarin wordt verwezen naar de **"***noodzakelijke nationale technische instrumenten") kan niet bedoeld zijn om de verwerking van persoonsgegevens te regelen (**overwegingen 114-115***) ;

24. artikel 20 van het ontwerp moet worden weggelaten of aangepast overeenkomstig artikel 65, 5, van de ETIAS-verordening **(overwegingen 116-117**).

Voor het Kenniscentrum,
(get.) Cédrine Morlière, Directeur

Comité Permanent de Contrôle
des services de renseignements et de sécurité
Vast Comité van Toezicht
op de inlichtingen- en veiligheidsdiensten

ADVIES 006/VCI /2023 VAN 25 AUGUSTUS 2023

VOORONTWERPEN VAN WET BETREFFENDE DE ETIAS NATIONALE EENHEID

Bij brief 15 mei 2023, ontvangen op 30 mei 2023 en bij mail van 13 juni 2023, vroeg de minister van Binnenlandse Zaken in toepassing van artikel 36.4 van de Algemene Verordening Gegevensbescherming (AVG) en artikel 33, achtste lid, van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse (W.Toezicht) om advies over:

- het Voorontwerp van wet betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E); en
- het Voorontwerp van wet tot wijziging van de wet betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E).

Bevoegdheid Vast Comité I en limieten van het advies

1. Voorliggend advies werd aan het Vast Comité I gevraagd op basis van de AVG en de W.Toezicht. Wat betreft de dataprotectie blijkt de adviesbevoegdheid van het Comité meer specifiek uit diverse bepalingen opgenomen in Titel 3. van de gegevensbeschermingswet van 30 juli 2018.

Het Comité zal de adviesaanvraag dan ook zowel behandelen vanuit zijn reguliere controleopdracht als vanuit zijn taak als Bevoegde Toezichthoudende Autoriteit in de zin van de gegevensbeschermingswet.

AVIS 006/CPR /2023 DU 25 AOUT 2023

AVANT-PROJETS DE LOI RELATIFS À L'UNITÉ NATIONALE ETIAS

Par lettre du 15 mai 2023, reçue le 30 mai 2023, et par e-mail du 13 juin 2023, en application de l'article 36.4 du Règlement général sur la protection des données (RGPD) et de l'article 33, alinéa 8, de la Loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (L.Contrôle), la ministre de l'Intérieur a demandé un avis sur :

- L'Avant-projet de loi relatif à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E) ; et
- L'Avant-projet de loi modifiant la loi relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E).

Compétence du Comité permanent R et limites de l'avis

1. Il a été demandé au Comité permanent R de rendre le présent avis sur la base du RGPD et de la L.Contrôle. En ce qui concerne la protection des données, la compétence d'avis du Comité ressort plus particulièrement des diverses dispositions reprises au Titre 3. de la Loi du 30 juillet 2018 relative à la protection des données.

Par conséquent, le Comité examinera la demande d'avis à la fois sous l'angle de sa mission de contrôle ordinaire et de son rôle d'Autorité de contrôle compétente au sens de la loi relative à la protection des données.

2. Gelet op de bevoegdheden van het Comité is het advies beperkt tot het eerste voorontwerp.

Advies van het Vast Comité I

3. Ingevolge artikel 6, 2° c) en d) van het eerste voorontwerp zullen vanuit de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichting en Veiligheid (ADIV) gedetacheerde personeelsleden deel uitmaken van de sectie die ondergebracht is bij het Nationaal Crisiscentrum, dat bevoegd is *'om hits met betrekking tot veiligheidsrisico's en hoge epidemiologische risico's te verwerken.'* (art. 5 § 1 en 11 van het ontwerp).

Deze gedetacheerden kunnen ook personen op de zogenaamde observatielijst plaatsen (art. 21 van het ontwerp) en raadplegingen verrichten in het Centrale ETIAS-systeem (art. 14 § 1, 3° van het ontwerp).

Finaliteit van het optreden van de Belgische veiligheids- en inlichtingendiensten binnen een Europese context

4. In de Memorie van Toelichting wordt terecht gesteld dat *'de nationale veiligheid niet binnen het toepassingsgebied van het recht van de Europese Unie valt'* maar dat *'de Belgische wetgever, uit hoofde van zijn nationale soevereiniteit inzake nationale veiligheid, de inlichting- en veiligheidsdiensten integreert.'* Zij doet dit omdat het opsporen en voorkomen van terroristische misdrijven en ernstige strafbare feiten een nationale bevoegdheid is die niet is uitgesloten van de toepassing van het EU recht.

In dit opzicht stelt de voorgestelde betrokkenheid van de VSSE en de ADIV uiteraard geen probleem en is zij volkomen gewettigd.

5. Echter, het voorontwerp breidt het toepassingsgebied van de Verordening uit

2. Vu les compétences du Comité, l'avis se limitera au premier avant-projet.

Avis du Comité permanent R

3. Conformément à l'article 6, 2° c) et d) du premier avant-projet, des membres détachés de la Sûreté de l'État (VSSE) et du Service Général du Renseignement et de la Sécurité (SGRS) feront partie de la section hébergée au Centre de crise National, qui est compétente pour *« traiter les réponses positives relatives aux risques en matière de sécurité et aux risques épidémiques élevés. »* (art. 5 § 1er et 11 du projet).

Ces membres détachés peuvent également placer des personnes sur la liste de surveillance (art. 21 du projet) et effectuer des consultations dans le système central ETIAS (art. 14 § 1er, 3° du projet).

Finalité de l'action des services de renseignement et de sécurité dans un contexte européen

4. Dans l'exposé des motifs, il est indiqué, à juste titre, que *« la sécurité nationale ne ressort pas du champ d'application du droit de l'Union européenne »* mais que *« le législateur belge, exerçant sa souveraineté en matière de sécurité nationale, intègre les services de renseignement et de sécurité (...). »* Il le fait parce que la détection et la prévention des infractions terroristes et des infractions pénales graves est une compétence nationale qui n'est pas exclue de l'application du droit de l'UE.

À cet égard, l'implication proposée de la VSSE et du SGRS ne pose naturellement aucun problème et est parfaitement légitime.

5. L'avant-projet élargit toutefois le champ d'application du Règlement en permettant aux

door de twee Belgische inlichtingendiensten de mogelijkheid te geven om het ETIAS-informatiesysteem aan te wenden voor *alle* dreigingen die ze ingevolge de Inlichtingenwet van 30 november 1998 moeten opvolgen, zoals bijvoorbeeld ook spionage, extremisme of schadelijke sektarische organisaties. Zo verwijst art. 14 § 1, 3° van het ontwerp naar *alle* dreigingen en te verdedigen belangen waarvoor de inlichtingendiensten bevoegd zijn en verwijst art. 21 van het ontwerp naar dit artikel 14 § 1.

Dit is in tegenspraak met de ETIAS Verordening die zowel de consultaties als de plaatsing op een observatielijst beperkt tot personen die gelinkt kunnen worden aan '*terroristische misdrijven of andere ernstige strafbare feiten*' (zie bijvoorbeeld art. 1.2., 4 f) en 34 van de ETIAS-Verordening). Hetzelfde blijkt uit diverse passages uit de preambule van de verordening. Zo stelt overweging nr. 41 uitdrukkelijk dat de verwerking van Etias-gegevens beperkt is tot hetgeen strikt noodzakelijk is voor het voorkomen, opsporen, en onderzoeken van terroristische misdrijven en andere ernstige feiten, zulks overeenkomstig de jurisprudentie van het Hof. In overweging 43 staat dat dient te worden bepaald welke autoriteiten van de lidstaten om deze toegang mogen verzoeken met als specifiek doel terroristische misdrijven of andere ernstige misdrijven te voorkomen, op te sporen of te onderzoeken.

Hierbij aansluitend moet ook opgemerkt worden dat de inlichtingendiensten slechts een onbetwistbare rol hebben bij de bestrijding van terrorisme. Wat betreft de '*andere zware misdrijven*' is de rol van de VSSE beperkt tot '*vormen en structuren van de criminele organisaties die wezenlijk betrekking hebben op de activiteiten bedoeld in artikel 8, 1°, a) tot e) en g), of die destabiliserende gevolgen kunnen hebben op het politieke of sociaal-economische vlak*'. Voor de ADIV is de rol inzake de strijd tegen '*andere zware misdrijven*' nog minder evident.

deux services de renseignement belges d'utiliser le système d'information ETIAS pour *toutes* les menaces qu'ils ont l'obligation de suivre en vertu de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité, comme par exemple l'espionnage, l'extrémisme ou les organisations sectaires nuisibles. Ainsi, l'art. 14 § 1er, 3° du projet se réfère à *toutes* les menaces et *tous* les intérêts à défendre pour lesquels les services de renseignement sont compétents, et l'art. 21 du projet fait référence à cet article 14 § 1er.

Ceci est en contradiction avec le Règlement ETIAS qui limite les consultations et l'inscription sur une liste de surveillance aux personnes susceptibles d'être liées à des « *infractions terroristes ou à d'autres infractions pénales graves* » (voir par exemple les articles 1.2, 4(f) et 34 du Règlement ETIAS). C'est ce qui ressort également de plusieurs passages du préambule du Règlement. Par exemple, le considérant 41 mentionne explicitement que le traitement des données Etias se limite à ce qui est strictement nécessaire à la prévention et à la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux enquêtes en la matière, conformément à la jurisprudence de la Cour. Le considérant 43 prévoit la nécessité de déterminer quelles sont les autorités des États membres qui peuvent demander un tel accès spécifiquement en vue de prévenir et détecter les infractions terroristes et autres infractions pénales graves ou d'enquêter sur ces infractions.

Dans le même ordre d'idées, il convient également de noter que les services de renseignement ne jouent un rôle incontestable que dans la lutte contre le terrorisme. En ce qui concerne les « *autres infractions graves* », le rôle de la VSSE se limite aux « *formes et structures des organisations criminelles qui se rapportent intrinsèquement aux activités visées à l'article 8, 1°, a) à e) et g), ou qui peuvent avoir des conséquences déstabilisantes sur le plan politique ou socio-économique* ». En ce qui concerne le SGRS, le rôle en matière de lutte contre les « *autres formes de criminalité grave* » est encore moins évident.

6. Door de inlichtingendiensten dus een algemene consultatiemogelijkheid te geven en door hen toe te laten personen op de observatielijst te plaatsen die buiten de finaliteit van het ETIAS-systeem vallen, wordt de verordening niet juist toegepast.

In de Memorie van Toelichting wordt gesteld dat *'de Belgische wetgever in het ETIAS-ontwerp rekening heeft gehouden met de bepalingen van de verordening wat betreft de inlichtingendiensten en hun wettelijke bevoegdheden.'* Het Comité vindt in de verordening echter geen bepaling(en) terug die hierop betrekking hebben en die zouden toelaten het Centrale ETIAS-systeem te gebruiken voor puur nationale veiligheidsdoelen indien die buiten de in de Verordening geëxpliciteerde doelstellingen vervat liggen.

De enige bepaling die – vreemd genoeg aangezien de Europese Unie ter zake geen bevoegdheid heeft – verwijst naar aspecten van de 'nationale veiligheid' is de onder art. 3.6. van de ETIAS-Verordening opgenomen definitie van de term 'veiligheidsrisico' (zie verder onder randnummer 8.).

Handmatige controles na een hit

7. Blijkens artikel 11 § 1 van het ontwerp zullen de gedetacheerden van de twee inlichtingendiensten het veiligheidsrisico bij de dossiers die hen vanuit de centrale ETIAS-eenheid worden voorgelegd, moeten beoordelen *'in het kader van hun [...] bevoegdheden'*. Zo gesteld, zou een negatief advies voor een reisautorisatie bijvoorbeeld kunnen gegeven worden omdat een persoon volgens de Belgische inlichtingendienst een gevaar vormt voor 'inmenging', terwijl dit risico potentieel niet wordt beoogd door het Europese autorisatiesysteem, dat, wat het aspect veiligheid betref, in essentie gericht is op de strijd tegen terrorisme en andere vormen van zware criminaliteit.

8. Het 'veiligheidsrisico' wordt in de Verordening zeer ruim gedefinieerd als *'een*

6. Dès lors, en donnant aux services de renseignement une possibilité de consultation générale et en leur permettant d'inscrire sur la liste de surveillance des personnes qui ne relèvent pas dela finalité du système ETIAS, le Règlement n'est pas appliqué correctement.

Dans l'exposé des motifs, il est relevé que *« le législateur belge a pris en compte les dispositions du règlement pour ce qui concerne les services de renseignements et leurs compétences légales (...). »* Cependant, le Comité ne trouve dans le Règlement aucune disposition qui permettrait d'utiliser le système central ETIAS à des fins strictes de sécurité nationale si elles ne correspondent pas aux objectifs explicités dans le Règlement.

La seule disposition qui – curieusement vu que l'Union européenne n'est pas compétente en la matière – fait référence à des aspects de 'sécurité nationale' est la définition de la notion de 'risque en matière de sécurité' à l'article 3.6 du Règlement ETIAS (*cf.* point 8 *infra*).

Contrôles manuels après un hit

7. En vertu de l'article 11 § 1er du projet, les détachés des deux services de renseignement devront évaluer le risque en matière de sécurité dans les dossiers qui leur seront soumis via l'unité centrale ETIAS *« en fonction de leurs compétences [...] »*. En d'autres termes, un avis négatif pour une autorisation de voyage pourrait, par exemple, être rendu parce que, selon le service de renseignement belge, une personne présente un risque d''ingérence', alors que ce risque n'est potentiellement pas envisagé par le système d'autorisation européen qui, en matière de sécurité, vise essentiellement à lutter contre le terrorisme et d'autres formes de criminalité grave.

8. Le 'risque en matière de sécurité' est défini de manière très large dans le Règlement comme *« un*

dreiging voor de openbare orde, de interne veiligheid of de internationale betrekkingen van een van de lidstaten' (art. 3.6. van de ETIAS-Verordening). Elders wordt melding gemaakt van *'door de lidstaat geconstateerde veiligheidsdreigingen'* (art. 33.2. d) van de Verordening. Zoals gesteld in de overwegingen 61 en 63 van de preambule van de Verordening behoort het tot de bevoegdheid van de Commissie om de veiligheidsrisico's, de risico's op het gebied van illegale immigratie, of hoge epidemiologische risico's nader te omschrijven waarop de specifieke risico-indicatoren zullen worden vastgesteld.
In overweging 27 van de preambule wordt eveneens uitgelegd dat de specifieke risico-indicatoren moeten worden gedefinieerd door de centrale Etias-eenheid. Er zal worden toegekeken op de naleving van de grondrechten door een Etias-sturingsraad.
Pas dan zal duidelijk zijn wat met deze ruime definitie wordt bedoeld en dus welke invulling de diensten eraan mogen geven. [1]

risque de menace pour l'ordre public, la sécurité intérieure ou les relations internationales de l'un des États membres » (art. 3.6 du Règlement ETIAS). Il est fait référence ailleurs aux *« menaces détectées par l'État membre concerné »* (article 33.2 d) du Règlement). Comme l'indiquent les considérants 61 et 63 du préambule du Règlement, il appartient à la Commission de définir plus précisément les risques en matière de sécurité, les risques liés à l'immigration clandestine ou les risques épidémiques élevés sur la base desquels les indicateurs de risque spécifiques seront établis.

Le considérant 27 explique également que les indicateurs de risque spécifiques doivent être définis par l'unité centrale Etias. Le respect des droits fondamentaux sera contrôlé par un comité d'examen Etias.

C'est seulement à ce moment-là que pourra être déterminé ce que cette définition large recouvre, et donc quelle interprétation les services peuvent en faire.[3]

9. Alleszins moet de ontworpen tekst in die zin worden aangepast dat de beoordeling van de inlichtingendiensten moet plaatsvinden *'in het kader van hun [...] bevoegdheden en moet aansluiten bij de wijze waarop het in de Verordening bedoeld veiligheidsrisico werd geoperationaliseerd.'* Zoniet wordt afbreuk gedaan aan de finaliteit van het Centraal ETIAS-systeem en wordt het toepassingsgebied van de Verordening onwettige wijze uitgebreid.

9. Le projet de texte doit en tout cas être amendé de manière à ce que l'évaluation des services de renseignement soit effectuée *« en fonction de leurs compétences [...] et en cohérence avec la manière dont le risque en matière de sécurité visé dans le Règlement a été opérationnalisé. »* Dans le cas contraire, il serait porté préjudice à la finalité du système central ETIAS et le champ d'application du Règlement serait élargi de manière illégale.

Het Comité wijst in dit verband tevens op het arrest van 21 juni 2022 van het Hof van Justitie van de Europese Unie in de zaak C-

Dans ce contexte, le Comité attire par ailleurs l'attention sur l'arrêt du 21 juin 2022 de la Cour de justice de l'Union européenne dans l'affaire

---

[1] De *Commission Delegated Decision C(2021) 4981 final - Further defining security, illegal immigration or high epidemic risks* () biedt op dit vlak geen duidelijkheid. De *Implementing Decision (Commission Delegated Decision C(2021) 4980 final - Specifying risks related to security, illegal immigration or high epidemic risk as defined in Regulation (EU) 2018/1240 of the European Parliament and of the Council)*, waarin mogelijk meer invulling werd gegeven aan het begrip veiligheidsrisico, werd nog niet gepubliceerd.

[3] La *Commission Delegated Decision C(2021) 4981 final - Further defining security, illegal immigration or high epidemic risks* () n'apporte aucune clarification en la matière. La *Implementing Decision (Commission Delegated Decision C(2021) 4980 final - Specifying risks related to security, illegal immigration or high epidemic risk as defined in Regulation (EU) 2018/1240 of the European Parliament and of the Council)*, qui aurait pu donner davantage de substance à la notion de risque en matière de sécurité, n'a pas encore été publiée.

817/19[2] waar het oordeelt dat de PNR-richtlijn, gelezen in het licht van het Handvest, zich verzet tegen nationale wetgeving volgens welke PNR-gegevens die overeenkomstig deze richtlijn zijn verzameld, mogen worden verwerkt voor andere doeleinden dan die welke uitdrukkelijk in artikel 1, lid 2, ervan worden genoemd.

C-817/19[4], dans lequel la Cour a estimé que la directive PNR, lue au regard de la Charte, s'oppose à une législation nationale en vertu de laquelle les données PNR collectées conformément à cette directive peuvent être traitées à des fins autres que celles expressément mentionnées à l'article 1er, alinéa 2.

Toewijzing van hits aan een van de twee secties

10. Artikel 5 § 1 van het voorontwerp bepaalt duidelijk welke *hits* onder welke sectie vallen. Het Comité begrijpt dan ook niet waarom § 2 van diezelfde bepaling de Koning opdraagt nader te bepalen welke *hit* onder welke sectie valt.

Attribution des hits à l'une des deux sections

10. L'article 5, § 1er de l'avant-projet définit clairement quels *hits* relèvent de quelle section. Le Comité ne comprend donc pas pourquoi le § 2 de cette même disposition charge le Roi de préciser quel *hit* relève de quelle section.

Controle door het Vast Comité I op raadplegingen

11. Onder voorbehoud van bovenstaande opmerkingen, is het Comité het eens met de onder artikel 40 van het ontwerp voorgestelde regeling waarbij de modaliteiten van en de controle op de raadplegingen worden ondergebracht in artikel 16/3 van de Inlichtingenwet en worden gelijkgeschakeld met de raadplegingen in BelPiu.

Het Comité vindt het evenwel onaanvaardbaar dat de lijst van de raadplegingen slechts *'een keer per maand aan het Vast Comité I [worden] doorgegeven'* indien de beslissing kadert in een geheel van gegevens die betrekking hebben op een specifiek inlichtingenonderzoek. Op die wijze is het niet mogelijk tijdig in te grijpen en wordt de controle de facto uitgehold.

Contrôle des consultations par le Comité permanent R

11. Sous réserve des commentaires formulés ci-dessus, le Comité approuve la réglementation proposée à l'article 40 du projet, selon laquelle les modalités et le contrôle des consultations seraient intégrés à l'article 16/3 de la Loi organique des services de renseignement et de sécurité et alignées sur les consultations de BelPiu.

Le Comité trouve cependant inacceptable que la liste des consultations soit seulement *« communiquée une fois par mois au Comité permanent R »* si la décision fait partie d'un ensemble de données relatives à une enquête de renseignement spécifique. Cela ne permet pas au Comité d'intervenir en temps utile et érode *de facto* le contrôle.

[2] Dit arrest werd gewezen na een prejudiciële vraag van het Grondwettelijk Hof dat zich moet buigen over de Belgische PNR-regeling. Bij het afsluiten van dit advies heeft het Hof nog geen arrest geveld.
[4] Cet arrêt a été rendu à la suite d'une question préjudicielle posée par la Cour constitutionnelle aux fins d'examen du système PNR belge. À l'heure de finaliser le présent avis, la Cour n'a pas encore rendu son arrêt.

Personele middelen

12. Ingevolge artikel 8 van het ontwerp moet elke betrokken dienst *'een voldoende aantal personeelsleden'* naar de sectie detacheren *'om de opdrachten te kunnen uitvoeren waarmee zij krachtens deze wet zijn belast.'* Deze passage heeft geen normatieve waarde en hoort thuis in de Memorie van Toelichting. Het is aan de uitvoerende macht om er op toe te zien dat de middelen aanwezig zijn om uitvoering te geven aan een wet.

Moyens humains

12. L'article 8 du projet prévoit que chaque service concerné détache *« un nombre suffisant de membres de son personnel »* auprès de la section *« pour pouvoir exécuter les missions qui leur incombent en vertu de la présente loi »*. Ce passage ne revêt pas de valeur normative et a sa place dans l'exposé des motifs. Il appartient au pouvoir exécutif de s'assurer de l'existence des moyens nécessaires à l'exécution d'une loi.

De bewaartermijn van persoonsgegevens

13. Artikel 70 van de verordening stelt dat *'de persoonsgegevens na 1 maand dienen te worden gewist uit alle nationale en Europol bestanden, indien deze gegevens niet vereist zijn voor het specifieke lopende strafrechtelijk onderzoek* [wij onderlijnen] *in het kader waarvan die lidstaat of Europol om de gegevens heeft verzocht.'*

Artikel 18 van het voorontwerp breidt die bepaling echter uit naar alle onderzoeken. In de Memorie van Toelichting wordt dit verantwoord door te stellen dat op die manier deze bewaartermijn ook van toepassing is op de door de inlichtingendiensten gevoerde onderzoeken. Aldus wordt opnieuw het toepassingsgebied van de verordening uitgebreid.

La durée de conservation des données à caractère personnel

13. L'article 70 du Règlement prévoit que *« les données à caractère personnel sont effacées de tous les dossiers nationaux et de ceux d'Europol à l'issue d'un délai d'un mois, à moins que ces données ne soient nécessaires aux fins de l'enquête pénale spécifique en cours* [nous soulignons] *pour laquelle elles avaient été demandées par un État membre ou par Europol. »*

Toutefois, l'article 18 de l'avant-projet étend cette disposition à toutes les enquêtes. L'exposé des motifs le justifie en indiquant que de la sorte, cette durée de conservation s'applique également aux enquêtes menées par les services de renseignement. Le champ d'application du Règlement s'en trouve donc à nouveau élargi.

Gebruik van geclassificeerde info

14. Het ontwerp houdt geen rekening met het feit dat de adviezen van de VSSE en de ADIV mogelijks kunnen gebaseerd zijn op geclassificeerde informatie, die bijvoorbeeld moet besproken worden met de andere leden van de eenheid in geval van een gemeenschappelijk advies of die opgenomen worden in de motieven van een beslissing. In dit geval dienen alle leden van de eenheid/sectie

Utilisation d'informations classifiées

14. Le projet ne tient pas compte du fait que les avis de la VSSE et du SGRS peuvent éventuellement se fonder sur des informations classifiées, qui doivent par exemple être discutées avec les autres membres de l'unité dans le cas d'un avis conjoint ou être reprises dans les motifs d'une décision. Dans ce cas de figure, tous les membres de l'unité/de la section doivent disposer de l'habilitation de sécurité requise. De plus, il y a lieu de prévoir une réglementation permettant

over de vereiste veiligheidsmachtiging te beschikken en dient in een regeling te worden voorzien waarbij geclassificeerde gegevens kunnen geweerd worden uit de aan de betrokkene ter kennis gebrachte beslissing.

d'exclure les informations classifiées de la décision notifiée à la personne concernée.

Aanduiding verwerkingsverantwoordelijke

15. Om alle discussies te vermijden, moet de wetgever de verwerkingsverantwoordelijke voor de verwerkingen van persoonsgegevens door de gedetacheerden van de VSSE en de ADIV expliciet aanduiden. Naar oordeel van het Comité zijn dit respectievelijk de administrateur-generaal van de VSSE en de chef van de ADIV.

Désignation du responsable du traitement

15. Afin d'éviter toute discussion, il convient que le législateur désigne explicitement le responsable du traitement des données à caractère personnel par les membres détachés de la VSSE et du SGRS. Le Comité estime qu'il s'agit respectivement de l'Administrateur général de la VSSE et du Chef du SGRS.

Technische opmerking

16. Art. 12 § 2 van het ontwerp verwijst naar een controle uitgevoerd op grond van '*artikel 20, lid 2, punt n), van de ETIAS-Verordening*,' Het Comité gaat er van uit dat het een foutieve verwijzing betreft.

Commentaire technique

16. L'article 12, § 2 du projet fait référence à un contrôle effectué en vertu de *« l'article 20, alinéa 2, point n), du Règlement ETIAS »*. Selon le Comité, cette référence est erronée.

Algemeen besluit

17. Gelet op bovenstaande opmerkingen dient de rol van de VSSE en de ADIV binnen de door de steller van het ontwerp voorgestelde ETIAS-regeling fundamenteel te worden herbekeken opdat de verordening correct zou worden toegepast.

Conclusion générale

17. Compte tenu des commentaires émis dans le présent avis, le rôle de la VSSE et du SGRS dans la réglementation ETIAS proposée par l'auteur du projet doit être fondamentalement réévalué pour permettre une application correcte du Règlement.

Brussel, 25 augustus 2023

Bruxelles, le 25 août 2023

VOOR HET VAST COMITÉ I

POUR LE COMITÉ PERMANENT R

Serge LIPSZYC

Voorzitter

Président

Bjorn VERSCHAEVE

Griffier d.d.

Greffier ff.

Imprimerie centrale – Centrale drukkerij