DOC 56 **0330/003**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

14 juli 2025

WETSVOORSTEL

tot delen van data uit authentieke bronnen met erkende dienstverleners voor elektronische identificatiemiddelen

Advies van de Gegevensbeschermingsautoriteit

Zie:

Doc 56 **0330/ (B.Z. 2024)**:
001: Wetsvoorstel van de heer Freilich c.s.
002: Amendement.

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

14 juillet 2025

PROPOSITION DE LOI

relative au partage de données provenant de sources authentiques avec les prestataires de services d'identification électronique agréés

Avis de l'Autorité de protection des données

Voir:

Doc 56 **0330/ (S.E. 2024)**:
001: Proposition de loi de M. Freilich et consorts.
002: Amendement.

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

Afkorting bij de nummering van de publicaties:		*Abréviations dans la numérotation des publications:*	
DOC 56 0000/000	*Parlementair document van de 56e zittingsperiode + basisnummer en volgnummer*	*DOC 56 0000/000*	*Document de la 56e législature, suivi du numéro de base et numéro de suivi*
QRVA	*Schriftelijke Vragen en Antwoorden*	*QRVA*	*Questions et Réponses écrites*
CRIV	*Voorlopige versie van het Integraal Verslag*	*CRIV*	*Version provisoire du Compte Rendu Intégral*
CRABV	*Beknopt Verslag*	*CRABV*	*Compte Rendu Analytique*
CRIV	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*	*CRIV*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN	*Plenum*	*PLEN*	*Séance plénière*
COM	*Commissievergadering*	*COM*	*Réunion de commission*
MOT	*Moties tot besluit van interpellaties (beigekleurig papier)*	*MOT*	*Motions déposées en conclusion d'interpellations (papier beige)*

Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 14/2025 van 27 februari 2025

Betreft: adviesaanvraag *betreffende een wetsvoorstel tot delen van data uit authentieke bronnen met erkende dienstverleners voor elektronische identificatiemiddelen (DOC56 0330/001) en een daarmee verband houdend amendement (DOC56 0330/002)* (CO-A-2025-003)

Trefwoorden: elektronische identificatie en authenticatie – Rijksregister – toegang door de private sector – dienstverleners van elektronische identificatiemiddelen – Europese portemonnee voor digitale identiteit – eIDAS-verordening

Vertaling

Inleiding

Het ter advies voorgelegde voorstel wijzigt de wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen* en de wet van 19 juli 1991 *betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten*, teneinde de private sector in het kader van de diensten voor elektronische identificatie een ruimere toegang te geven tot de gegevens uit het Rijksregister, het Register van de Identiteitskaarten en het Register van de Vreemdelingenkaarten. Het beoogt tevens de mogelijkheid te creëren om de "*Belgische digitale portefeuille*"-applicatie te laten gelden als bewijs van inschrijving in de bevolkingsregisters.

Concreet zou het voorstel de invoering mogelijk maken van nieuwe diensten voor de uitwisseling van gegevens uit de bovengenoemde authentieke bronnen, via de dienstverleners van elektronische identificatiemiddelen, op basis van de toestemming van de betrokkene en voor specifieke doeleinden die in het dispositief moeten worden geëxpliciteerd. Het onderhavige advies licht toe onder welke voorwaarden (precisering van het doeleinde, waarborgen met betrekking tot de controle door de betrokkene, enzovoort) dat mogelijk zou zijn, in het bijzonder met betrekking tot de uitvoering van de verplichtingen inzake identificatie van cliënten door de ondernemingen die onderworpen zijn aan de antiwitwaswetgeving.

Voor normatieve teksten die uitgaan van de federale overheid, het Brussels Hoofdstedelijk Gewest en de Gemeenschappelijke Gemeenschapscommissie zijn de adviezen in principe zowel in het Nederlands als in het Frans beschikbaar op de website van de Autoriteit. De 'Originele versie' is de versie die collegiaal gevalideerd werd.

Enerzijds hebben deze entiteiten echter reeds toegang tot het Rijksregister. Anderzijds zouden de Europese portemonnees voor digitale identiteit en de attesteringen van attributen, zoals bedoeld in de recente hervorming van de eIDAS-verordening, het mogelijk moeten maken om de doelstellingen van het voorstel te verwezenlijken. Deze zouden dan ook de voorkeur kunnen krijgen, aangezien zij deel uitmaken van een juridisch, technisch en geharmoniseerd normatief kader op Europees niveau – al is dat weliswaar nog niet volledig geïmplementeerd en van toepassing. Dit kader voorziet bovendien in specifieke waarborgen, waaronder volledige controle door de gebruiker over de Europese portemonnee voor digitale identiteit en meer transparantie.

In het bijzonder, en meer algemeen in het licht van de specifieke doeleinden die zouden worden beoogd, beveelt de Autoriteit in dit verband aan om een effectbeoordeling uit te voeren.

De Autoriteit is overigens van oordeel dat het in dit stadium, aangezien de zojuist genoemde hervorming nog niet volledig van toepassing is, voorbarig is om op dit moment een wettelijk gevolg toe te kennen aan de "*Belgische digitale portefeuille*". De Autoriteit blijft zich echter bewust van het belang en de noodzaak om op Belgisch niveau een Europese portemonnee voor digitale identiteit in te voeren, in overeenstemming met de eIDAS2-verordening, binnen de gestelde termijn.

De Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit"), aanwezig: de dames Cédrine Morlière en Griet Verhenneman, en de heren Yves-Alexandre de Montjoye, Bart Preneel en Gert Vermeulen;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, met name de artikelen 23 en 26 (hierna "WOG");

Gelet op artikel 43 van het Reglement van interne orde volgens hetwelk de beslissingen van de Autorisatie- en Adviesdienst bij meerderheid van stemmen genomen worden;

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");

Gelet op de aanvraag van de heer Peter De Roover, voorzitter van de Kamer van volksvertegenwoordigers (hierna "de aanvrager"), ontvangen op 7 januari 2025;

Gelet op het verzoek om aanvullende informatie dat op 24 januari 2025 aan de aanvrager is toegezonden;

Gelet op het antwoord van de aanvrager van 2 februari 2025;

Brengt op 27 februari 2025 het volgende advies uit:

I. Onderwerp en context van de adviesaanvraag

1. De aanvrager heeft bij de Autoriteit een adviesaanvraag ingediend met betrekking tot een wetsvoorstel *tot delen van data uit authentieke bronnen met erkende dienstverleners voor elektronische identificatiemiddelen (DOC56 0330/001)* (hierna "**het voorstel**"), alsmede een daarmee verband houdend amendement (DOC56 0330/002) (hierna "**het amendement**") (CO-A-2025-003).

2. In wezen beoogt het voorstel, mits de toestemming van de betrokkene, private actoren bijkomende toegang te verlenen tot de gegevens van het Rijksregister (hierna "**RR**"), het Register van de Identiteitskaarten en het Register van de Vreemdelingenkaarten. Dienstverleners van elektronische identificatiemiddelen zouden automatisch updates van persoonsgegevens uit deze gegevensbronnen ontvangen, enerzijds om zelf over up-to-date identificatiegegevens te beschikken met betrekking tot de personen die gebruikmaken van hun diensten, en anderzijds om deze gegevens geheel of gedeeltelijk mee te delen aan de private actoren bij wie deze personen zich via dezelfde diensten identificeren[1].

3. Daartoe voorziet het **voorstel** in de invoeging van een artikel 5*quater* in de wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen* (hierna de "**RR-wet**"), en in de wijziging van artikel 6*bis*, § 3, van de wet van 19 juli 1991 *betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten* (hierna de "**wet van 1991**").

4. Het **amendement** heeft betrekking op een digitale identiteitsportefeuille ("*Digital Identity Wallet*") en wijzigt artikel 6, § 1, van de wet van 1991.

II. Onderzoek

[1] Wat betreft de vraag of het voorstel toegang tot het Register van de Identiteitskaarten en het Register van de Vreemdelingenkaarten beoogt toe te staan aan andere partijen dan dienstverleners van elektronische identificatiemiddelen, zie overweging nr. 11.

Dit advies is als volgt opgebouwd:

II.1. Het amendement – De digitale identiteitsportefeuille

5. Het amendement heeft betrekking op een **digitale identiteitsportefeuille** ("*Digital Identity Wallet*") en wijzigt artikel 6, § 1, van de wet van 1991 door tussen het eerste en het tweede lid een lid in te voegen, luidende: "*De mobiele digitale identiteitsdocumenten in de officiële Belgische digitale portefeuille applicatie, gelden als bewijs van inschrijving in de bevolkingsregisters.*" Op basis van een opzoeking op het internet is deze portefeuille *a priori* **de myGov-applicatie voor mobiele apparaten** (zie https://mygov.be/[2]). De pagina "Gebruiksvoorwaarden" van de website mygov.be vermeldt met name het volgende:

> "*MyGov.be is een toepassing of app die je kan installeren op jouw mobiel toestel. De bedoeling van MyGov.be is het vergemakkelijken van de toegang tot de overheidsdiensten door middel van een eenvoudig en zeker identificatiemiddel. Deze toepassing laat je ook toe om gemakkelijk officiële documenten te vragen en te ontvangen via het* ***Loket****, om deze te bewaren op een veilige plaats en om in alle veiligheid te communiceren met overheidsdiensten via* ***My eBox****, de mobiele versie van My eBox.*

[2] Laatst geraadpleegd op 22/01/2025.

*MyGov.be is ook een **digitale sleutel** waarmee je jezelf online kan authentificeren. Je kan op een betrouwbaar hoog vertrouwensniveau aantonen dat jij het bent. Meer informatie over digitale sleutels vindt u hier: https://csam.be/nl/egov-profiel.html.*
*In de toekomst zal de app de mogelijkheid bieden om een gekwalificeerde **elektronische handtekening** te plaatsen.*"

6. In **Europees recht** vallen Europese portemonnees voor digitale identiteit onder de artikelen 3, 42. (definitie[3]), en 5*bis* tot en met 5*septies* van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 *betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG* (hierna "**eIDAS-verordening**"), zoals ingevoegd door Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 *tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit* (hierna "**eIDAS2-verordening**").

7. In **Belgisch recht** bepaalt de wet van 15 augustus 2012 *houdende oprichting en organisatie van een federale dienstenintegrator* (hierna "**de wet dienstenintegrator**") dat de federale dienstenintegrator (dat wil zeggen de Federale Overheidsdienst bevoegd voor Digitalisering[4]) een Europese portemonnee voor digitale identiteit uitbouwt en ter beschikking stelt[5].

8. Artikel 5*quinquies* van de eIDAS-verordening voorziet met name in een verplichting voor de lidstaten om de Commissie te informeren in geval van verstrekking en certificering van een Europese portemonnee voor digitale identiteit, alsmede in een verplichting voor de Commissie om een lijst van deze portemonnees te publiceren. De Autoriteit heeft de aanvrager bevraagd over de volgende punten, aangezien het normatief kader ter zake nog niet volledig gedefinieerd en van toepassing lijkt te zijn: Werd de Commissie geïnformeerd over de hierboven genoemde "*Belgische digitale portefeuille*" en zo niet, waarom niet?; Waar is de lijst van gecertificeerde Europese portemonnees voor digitale identiteit raadpleegbaar?; Wordt, naast de wet dienstenintegrator, de "Belgische digitale portefeuille" ook geregeld door andere Belgische rechtsregels ter uitvoering van de eIDAS-verordening, en zo ja, welke?

---

[3] Namelijk: "*een elektronisch identificatiemiddel dat de gebruiker in staat stelt gegevens voor persoonsidentificatie en elektronische attesteringen van attributen veilig op te slaan, te beheren en te valideren met het oog op de verstrekking ervan aan vertrouwende partijen en andere gebruikers van Europese portemonnees voor digitale identiteit, en te ondertekenen middels gekwalificeerde elektronische handtekeningen of te verzegelen middels gekwalificeerde elektronische zegels*".

[4] Artikel 3 van de wet dienstenintegrator.

[5] Volgens artikel 4, 3., van de wet dienstenintegrator staat hij in voor "*het uitwerken van de technische modaliteiten en de voorwaarden om de toegangskanalen tot gegevensbanken, waaronder webdiensten, mobiele applicaties, de Europese portemonnee voor digitale identiteit en online portalen, zo efficiënt en veilig mogelijk uit te bouwen, met elkaar te verbinden en ter beschikking te stellen*".

Volgens artikel 4, 14., van dezelfde wet staat hij in voor "*het ontwerpen en het ter beschikking stellen van een Europese portemonnee voor digitale identiteit bedoeld in artikel 3, punt 42, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, zoals gewijzigd door Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit, en via de Europese portemonnee voor digitale identiteit het ontsluiten van gegevens opgenomen in gegevensbanken en het attesteren van gegevens*".

Wordt daarin de naam vermeld van de portefeuille, evenals de rollen en verantwoordelijkheden van de partij(en) die deze aanbieden, enzovoort? De aanvrager antwoordde het volgende: "*Wij hebben geen contact gehad met de Europese Commissie*", en verwees naar een webpagina die de gezochte lijst niet lijkt te bevatten[6]. Zoals de aanvrager overigens in een ander antwoord aan de Autoriteit aangeeft, is het normatief kader van de hervormde eIDAS-verordening nog niet van toepassing[7].

9. Onder deze omstandigheden **lijkt het**, hoewel de bedoeling van het amendement lovenswaardig is aangezien deze zou kunnen passen binnen het streven om de eIDAS2-verordening in Belgisch recht om te zetten, **niettemin voorbarig om op dit moment een bijzonder wettelijk gevolg toe te kennen aan de "officiële 'Belgische digitale portefeuille' applicatie"**. **Enerzijds wordt deze applicatie niet gedefinieerd in het dispositief van het amendement** (zelfs niet via een specifieke verwijzing naar de relevante bepalingen van de eIDAS-verordening of naar de regels van Belgisch recht ter uitvoering daarvan), **anderzijds kan zij wettelijk nog niet bestaan als portemonnee voor digitale identiteit in de zin van de eIDAS-verordening**. Dit neemt niet weg dat de Autoriteit zich ten volle bewust is van de noodzaak om de uitvoering van de eIDAS-verordening in Belgisch recht voor te bereiden.

II.2. Het voorstel – Wijziging van de RR-wet en van de wet van 1991

II.2.1. Dispositief en motivering van het voorstel

10. Het voorgestelde artikel 5*quater* van de RR-wet luidt als volgt:

> "*Art. 5quater. § 1. Onverminderd artikel 5 kan een meerderjarige eveneens de* ***toelating geven*** *dat de diensten van het Rijksregister zijn/haar informatiegegevens bedoeld in artikel 3, eerste lid en de wijzigingen aangebracht aan deze informatiegegevens meedelen* ***aan aanbieders van een dienst voor elektronische identificatie van het niveau hoog of substantieel*** *zoals bedoeld in de Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/ EG, die zijn erkend bij koninklijk besluit of door een overheidsdienst die door of krachtens een wet, een decreet of een ordonnantie de opdracht heeft om een dienst voor gebruikers- en toegangsbeheer aan te bieden,* ***uitsluitend voor de identificatie en authenticatie van een natuurlijke persoon die diensten op het gebied van identificatie, authenticatie***

[6] Zie https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_nl, laatst geraadpleegd op 06/02/2025.

[7] Zie overweging nr. 38.

***of elektronische handtekeningen wil afnemen van deze aanbieders, en met het oog op de uitvoering van deze diensten**.*

*§ 2. De voorwaarden bedoeld in artikel **5ter, § 2, 1° en 3° tot 6°** zijn van toepassing op de mededeling van de wijzigingen bedoeld in paragraaf 1.*

*§ 3. De **stopzetting van de contractuele relatie tussen de natuurlijke persoon en de aanbieders van een dienst voor elektronische identificatie** brengt de stopzetting van elke mededeling van gegevens uit het Rijksregister met zich mee. De dienst voor elektronische identificatie is verplicht om de stopzetting van deze contractuele relatie mee te delen aan de diensten van het Rijksregister.*

*Aanbieders van een dienst voor elektronische identificatie **mogen gegevens die overeenkomstig paragraaf 1 zijn verkregen alleen met toestemming** van de natuurlijke persoon **aan derden doorgeven**.*" (in vet aangeduid door de Autoriteit)

11. In de toelichting van het voorstel wordt gepreciseerd dat het de bedoeling is "*welbepaalde dienstverleners **automatische** updates en aanvullingen te laten ontvangen van authentieke bronnen, zoals bijvoorbeeld het Rijksregister, **die zij** onder welbepaalde voorwaarden en op een door de burger gecontroleerde manier **kunnen delen met ondernemingen die bijvoorbeeld aan een identificatieverplichting zijn onderworpen***" (in vet aangeduid door de Autoriteit). Op dit punt wordt in de toelichting met name nog het volgende vermeld: "*Het hergebruik van gegevens uit authentieke bronnen biedt **ondernemingen** de mogelijkheid om te **voldoen aan hun verplichtingen om gegevens regelmatig aan te vullen en bij te werken**. Het faciliteert **ook** hun **identificatieverplichtingen** wanneer zij een tool hebben om op de hoogte te blijven van wijzigingen en aanvullingen van de identificatiegegevens. Het brengt **ook** **administratieve vereenvoudiging** met zich mee. Zo vermijden ondernemingen dat ze ontelbare keren **gegevens** opnieuw moeten opvragen, wat zorgt voor **administratieve lasten**. Het **helpt** tevens **in de strijd tegen (identiteits)fraude** en is zelf fraudebestendig en veilig.*" (in vet aangeduid en onderstreept door de Autoriteit)

12. De toelichting preciseert nog het volgende: "*Een dergelijke gegevensdeling vanuit het Rijksregister is vandaag niet mogelijk. Hoewel de artikelen 5, 5ter en 8 van de Rijksregisterwet reeds **mogelijkheden** bevatten om gegevens of updates ervan met private partijen te delen, **volstaan** deze **niet**. **De minister van Binnenlandse Zaken of de FOD Binnenlandse Zaken geeft bijvoorbeeld geen machtiging voor gegevensdeling (art. 5) of de gegevensdeling is slechts mogelijk onder een hele reeks beperkende voorwaarden en strikte interpretaties (art. 5ter en art. 8, § 3***

en § 5). *Daarom willen de indieners een nieuw artikel 5quater invoegen in de Rijksregisterwet.*" (in vet aangeduid door de Autoriteit)

13. Bovendien vermeldt de aanvrager het volgende in het adviesaanvraagformulier:

"*Het blijft voor de burger altijd mogelijk om handmatig gegevens bij te werken bij de verschillende entiteiten of bedrijven die persoonsgegevens actueel willen en moeten houden, met name voor identificatiedoeleinden en naleving van wettelijke verplichtingen.*
Dit houdt echter in dat de burger actie moet ondernemen bij elke entiteit of elk bedrijf waar zijn/haar identificatiegegevens moeten worden bijgewerkt, wat lastig kan zijn en het risico op fouten of het niet tijdig handelen vergroot.
Deze actie kan eruit bestaan:

- ***Zich fysiek te begeven naar kantorennetwerk van (elke) derde partij, zoals banken****, die hierbij een correcte uitlezing en validatie van de gegevens van een (e)ID document dienen te verrichten;*
  o Naast de inspanning die hierbij wordt gevraagd van de betrokkenen, vergt dit ook een aanzienlijke werklast van de derde partijen in kwestie;
- ***Een foto of scan van het eID document maken en doorsturen****, hetgeen:*
  o enerzijds leidt tot complexiteit in de handelingen zoals die worden vereist van de betrokkene;
  o anderzijds onvermijdelijk leidt tot een verminderde betrouwbaarheid van de dusdanig bekomen gegevens: fouten in de overname van identiteitsgegevens via optische tekstherkenning zijn onvermijdelijk, en sterk afhankelijk van de kwaliteit van de scan en/of foto van het document;
- ***Het opsturen van een papieren document welke de identiteit van de gebruiker kan staven op basis van kopie van een ID document, een factuur van een nutsbedrijf of officiële instanties of andere****. Naast de hoge werklast zowel aan de kant van de betrokkene als van derde partijen, leidt dit ook overmijdelijk tot een verminderde betrouwbaarheid van deze identiteitsgegevens.*
- ***Online uitlezen van het eID document op websites van derden****. Dit vereist het gebruik van een kaartlezer en kennis van de persoonlijke pincode, hetgeen voor een groter deel van betrokkenen een complexiteit meebrengt die onoverkomelijk is gebleken sinds de initiële uitgifte van de eID kaarten in 2004.*

Samenvattend kan men stellen dat voor elk van deze alternatieve manieren deze:

- *ineffectief en onnauwkeurig zijn: identificatieprocessen worden hier vaak uitgevoerd met onnauwkeurige gegevens. Zo bieden scans van bijvoorbeeld papieren documenten zoals een identiteitskaart of factuur geen garantie voor de juistheid van*

de gegevens. Hierdoor is het voor betrokken entiteiten moeilijk om aan hun verplichtingen te voldoen, wat onder andere een groter risico op witwassen met zich meebrengt;

• duur, tijdrovend en onhandig zijn voor de burgers: het stelt digitale dienstverleners niet in staat om het bijwerken van verwerkte gegevens gebruiksvriendelijk en snel te maken voor burgers, wat leidt tot een slechte ervaring. Burgers moeten verschillende identificatieprocessen doorlopen met verschillende entiteiten, op verschillende tijdstippen, terwijl hun gegevens centraal beschikbaar en geverifieerd zijn vanuit authentieke bronnen. Verlopen gegevens kunnen uiteindelijk leiden tot het blokkeren van essentiële diensten (zoals het verlies van toegang tot bankrekeningen);

• niet aangepast zijn aan de digitaliseringstrend in een post-COVID-19 tijdperk: zowel burgers als entiteiten moeten vaak hun identiteit verifiëren aan de hand van papieren documenten (bijv. via scans) en persoonlijke identificatie;

• kostbaar en tijdrovend zijn voor entiteiten en bedrijven die gegevens die al beschikbaar zijn uit authentieke bronnen opnieuw moeten verzamelen."

14. Gewijzigd door het voorstel, zou **artikel 6*bis*, § 3, van de wet van 1991** bovendien het volgende bepalen:

"*Onder de voorwaarden bedoeld in artikel 5 quater, § 2, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen* ***zijn de aanbieders*** *bedoeld in artikel 5quater, § 1, van dezelfde wet* ***gemachtigd om de informatiegegevens bedoeld in paragraaf 1[8] te kennen*** *met inachtneming van de in het eerste lid bedoelde machtiging.*" (in vet aangeduid door de Autoriteit)

15. In de toelichting bij de artikelen van het voorstel wordt deze bepaling als volgt gerechtvaardigd:

"*Wegens de mogelijkheid tot verificatie van de geldigheid van de identiteitskaart waarmee de betrokkenen kunnen worden geïdentificeerd, acht de indiener het raadzaam om artikel 6bis van de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten aan te passen zodat* ***erkende dienstverleners van identificatiemiddelen toegang krijgen tot de relevante informatie betreffende de identiteitskaart****, op basis van voorafgaande autorisatie. Dit zal de erkende dienstverleners in staat stellen om* ***de validiteit te controleren conform eIDAS van het identiteitsdocument****, op basis waarvan zij de betrokken persoon identificeren en de gegevens van de identiteitskaart conform AVG bijwerken. Deze*

[8] Zie voetnoot nr. 13.

aanpassing past bovendien volledig in de recente aanbevelingen door de Europese bevoegde instanties rond ***betrouwbare online identificatie*** *(ENISA, maart 2024).*" (in vet aangeduid en onderstreept door de Autoriteit)

II.2.2. Twee categorieën van gegevensstromen en betrokken actoren

16. Het voorstel voorziet bijgevolg in twee categorieën van gegevensstromen. De **eerste categorie van gegevensstromen** houdt in dat **erkende dienstverleners van elektronische identificatiemiddelen** gegevens en updates van gegevens uit het RR, het Register van de Identiteitskaarten en het Register van de Vreemdelingenkaarten kunnen ontvangen. "*Op die manier kunnen die actoren er onder welbepaalde voorwaarden en op een door de burger gecontroleerde manier voor zorgen dat de gegevens waarover zij beschikken altijd volledig en up-to-date zijn.*" Het gaat hierbij om aanbieders van een **dienst voor elektronische identificatie van het niveau hoog of substantieel** zoals bedoeld in de eIDAS-verordening, die erkend zijn.

17. Wat de erkenning betreft, bestaat er in het Belgisch positief recht een koninklijk besluit van 22 oktober 2017 *tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van diensten voor elektronische identificatie voor overheidstoepassingen* (hierna "**het KB van 2017**"). Dit besluit geeft uitvoering aan de wet van 18 juli 2017 *inzake elektronische identificatie* (hierna "**de wet van 2017**").

18. Op het moment van het opstellen van het onderhavige advies heeft België twee **stelsels voor identificatie** met een **hoog** betrouwbaarheidsniveau aangemeld, namelijk de **eID** (de elektronische identiteitskaart)[9] en **Itsme** (een mobiele applicatie)[10].
De Autoriteit heeft de aanvrager gevraagd welke dienstverleners momenteel erkend zijn en waar de lijst daarvan kan worden geraadpleegd. Daarnaast werd gevraagd naar de dienstverleners die eveneens erkend zouden zijn "*door een overheidsdienst die door of krachtens een wet, een decreet of een ordonnantie de opdracht heeft om een dienst voor gebruikers- en toegangsbeheer aan te bieden*". Hij antwoordde met name het volgende (vrije vertaling): "*Wegens de strenge vereisten van het koninklijk besluit eIDAS is tot op heden slechts één entiteit geaccrediteerd. De dienstverlener van elektronische identificatiemiddelen die tot op heden geaccrediteerd is onder het koninklijk besluit eIDAS, is Belgian Mobile ID (voor het aanbieden van de elektronische identificatiemiddelen itsme®).*"

[9] Zie https://ec.europa.eu/digital-building-blocks/sites/display/EIDCOMMUNITY/Belgium+-+eID, laatst geraadpleegd op 13/01/2025.
[10] Zie https://ec.europa.eu/digital-building-blocks/sites/display/EIDCOMMUNITY/Belgium+-+Itsme, laatst geraadpleegd op 13/01/2025.

19. De Autoriteit is van oordeel dat **het voorstel moet verduidelijken welke dienstverleners erkend zijn** "*door een overheidsdienst die door of krachtens een wet, een decreet of een ordonnantie de opdracht heeft om een dienst voor gebruikers- en toegangsbeheer aan te bieden*", alsook welke overheidsdiensten daarbij eventueel betrokken zijn en welk normatief kader van toepassing is. Zo niet, dient de verwijzing ernaar te worden weggelaten. De Autoriteit spreekt zich hierover niet uit, aangezien zij geen zicht heeft op de entiteiten of de overheidsdienst waarop de bepaling in ontwerp betrekking heeft.

20. De **tweede categorie van gegevensstromen** betreft **het mogelijk maken van de mededeling van gegevens uit het RR, of zelfs uit het Register van de Identiteitskaarten en het Register van de Vreemdelingenkaarten**, **aan ondernemingen** waarbij de betrokkene zich identificeert met behulp van de betrokken dienst voor elektronische identificatie. Hoewel artikel 3 van het ontwerp de toegang tot gegevens uit het Register van de Identiteitskaarten en het Register van de Vreemdelingenkaarten lijkt te beperken tot dienstverleners van elektronische identificatiemiddelen, suggereren de antwoorden van de aanvrager dat ook deze gegevens zouden kunnen worden meegedeeld aan andere private actoren (namelijk de entiteiten waarbij de betrokkene zich identificeert met het oog op de uitvoering van de betrokken contracten)[11].

II.2.3. Verband tussen het voorstel en artikel 5ter van de RR-wet

21. Wat betreft de voorwaarden waaronder toegang tot het RR kan worden verleend, rechtvaardigt het voorstel dat het in overeenstemming is met de AVG door met name te preciseren dat het voorziet in het gebruik van *opt-in* en toestemming van de burger, dat het geen afbreuk doet aan artikel 5 van de RR-wet (dat de machtiging van de minister van Binnenlandse Zaken vereist), en dat het voorziet in de toepassing van de voorwaarden bedoeld in artikel **5*ter*,** § 2, 1° en 3° tot 6°, van de **RR-wet**, **in lijn waarvan het is opgesteld**. Wat dit laatste punt betreft, wordt in de toelichting bij artikel 2 van het voorstel immers gepreciseerd dat het nieuwe artikel 5*quater* van de RR-wet "*volgt op artikel 5ter van de Rijksregisterwet dat eenzelfde uitkomst beoogt, namelijk het verkrijgen van automatische updates van het Rijksregister*".

22. Die laatste bepaling werd ingevoegd in de RR-wet door de **wet van 25 november 2018** *houdende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters*. Zij breidt op ongekende wijze, voor doeleinden die **geen verband houden met het algemeen belang**, de mogelijkheden van toegang tot het RR **door de private sector** uit. Het voorontwerp van deze wet was het voorwerp van een advies van de Commissie voor de bescherming van de persoonlijke

[11] De foto staat niet in het RR, maar wel in het Register van de Identiteitskaarten. Zie overwegingen nrs. 14 en 37.

levenssfeer nr. 19/2018 van 28 februari 2018 *betreffende een voorontwerp van wet houdende diverse bepalingen "Binnenlandse Zaken" (CO-A-2018-002)* (hierna "**het advies van de CBPL**").

23. De Autoriteit merkt echter in de eerste plaats op dat artikel **5*quater*** in ontwerp van de RR-wet een **ruimere draagwijdte** heeft dan artikel 5*ter* van de RR-wet, waarnaar in de toelichting van het ontwerp wordt verwezen, en **verder gaat** wat betreft de toegankelijkheid van gegevens uit het RR, het Register van de Identiteitskaarten en het Register van de Vreemdelingenkaarten. Artikel **5*ter*** heeft alleen betrekking op de gegevens bedoeld in **artikel 3, eerste lid, 1°, 5° en 6°**, van de RR-wet (namelijk de naam en voornamen, de hoofdverblijfplaats en de plaats en datum van het overlijden, of, in het geval van een verklaring van afwezigheid, de datum van de overschrijving van de beslissing houdende verklaring van afwezigheid).

24. Wat **de toegang tot het RR** betreft, heeft het voorstel echter betrekking op ***alle* gegevens bedoeld in artikel 3, eerste lid, van de RR-wet**[12]. Artikel 3 van het voorstel, dat artikel 6*bis* van de wet van 1991 wijzigt, "*machtigt*" **ook** de aanbieders van een dienst voor elektronische identificatie om informatiegegevens "te kennen" die zijn opgenomen in het centraal bestand van de identiteitskaarten

[12] Het gaat om de volgende gegevens:

"*1° de naam en voornamen;*

2° de geboorteplaats en -datum;

3° het geslacht;

4° de nationaliteit;

5° de hoofdverblijfplaats;

6° (de plaats en datum van het overlijden, of, in het geval van een verklaring van afwezigheid, de datum van de overschrijving van de beslissing houdende verklaring van afwezigheid); <W 2007-05-09/44, art. 52, 021; Inwerkingtreding : 01-07/2007>

7° [4 ...]4

8° de burgerlijke staat;

9° de samenstelling van het gezin.

[1 9° /1 [4 de akten en beslissingen betreffende de rechtsbekwaamheid en de beslissingen tot bewind over de goederen of over de persoon bedoeld in [6 artikel 1250]6, eerste lid, van het Gerechtelijk Wetboek; de naam, de voornaam en het adres van de persoon die een minderjarige, een onbekwaam verklaarde, een geïnterneerde of een persoon die onder het statuut van verlengde minderjarigheid geplaatst is, vertegenwoordigt of bijstaat of van de bewindvoerder over de goederen of de persoon van wie melding wordt gemaakt in de in [6 artikel 1250]6, eerste lid, van het Gerechtelijk Wetboek bedoelde beslissing.]4]1

(10° de vermelding van het register waarin de in artikel 2 bedoelde personen zijn ingeschreven [5 of vermeld] 5;
11° de administratieve toestand van de in artikel 2, eerste lid, 3°, bedoelde personen;) <W 1994-05-24/39, art. 9, 005; Inwerkingtreding : 01-02-1995>

(12° in voorkomend geval, het bestaan van het identiteits- en handtekeningscertificaat, zoals bepaald in de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten;

13° de wettelijke samenwoning.) <W 2003-03-25/30, art. 3, 013; Inwerkingtreding : 07-04-2003>

(14° de verblijfstoestand voor de vreemdelingen bedoeld in artikel 2.) <W 2006-12-27/30, art. 166, 018; Inwerkingtreding : 01-04-2007>

[3 15° de vermelding van de ascendenten in de eerste graad, ongeacht of de afstamming tot stand komt door de geboorteakte, een gerechtelijke beslissing, een erkenning of een adoptie;

16° de vermelding van de afstammelingen in rechtstreekse, dalende lijn in de eerste graad, ongeacht of de afstamming tot stand komt door de geboorteakte, een gerechtelijke beslissing, een erkenning of een adoptie;

17° [4 in voorkomend geval de contactgegevens van de burgers, die enkel op vrijwillige basis worden meegedeeld, zoals bepaald door de Koning, bij een besluit vastgesteld na overleg in de Ministerraad; de Koning bepaalt eveneens de nadere regels van de mededeling van deze gegevens aan de diensten van het Rijksregister van de natuurlijke personen en de nadere regels van de wijziging van deze gegevens door de burger;]4]3".

en het centraal bestand van de vreemdelingenkaarten, dat wil zeggen **het Register van de Identiteitskaarten en het Register van de Vreemdelingenkaarten**[13]. Een dergelijke mogelijkheid wordt niet voorzien in de context van artikel 5*ter* van de RR-wet.

25. Bovendien, **in tegenstelling tot artikel 5*ter* van de RR-wet**, gelezen in samenhang met artikel 5 van diezelfde wet, waarin wordt bepaald dat elke instelling door de minister van Binnenlandse Zaken moet worden gemachtigd om toegang te krijgen tot de gegevens van het RR, voorziet het voorstel in een **beperktere machtigingsrol voor de minister van Binnenlandse Zaken**, die alleen de toegang door de dienstverleners van elektronische identificatiemiddelen moet machtigen (en niet de ondernemingen die via deze dienstverleners toegang krijgen tot de gegevens uit het RR en de bovengenoemde registers).

26. De Autoriteit heeft de aanvrager gevraagd of er vooraf een **effectbeoordeling** is uitgevoerd. Zij heeft hem ook gevraagd of hij over gegevens beschikt met betrekking tot de tenuitvoerlegging van artikel 5*ter* van de RR-wet (aantal betrokken ondernemingen, aantal betrokkenen, enz.), aangezien dit een belangrijk punt van discussie was bij de bespreking van het ontwerp. De aanvrager gaf met name aan niet over cijfers ter zake te beschikken en verwees naar het RR. Uit het antwoord leidt de Autoriteit af dat er geen effectbeoordeling als zodanig is uitgevoerd[14]. De Autoriteit heeft het RR bevraagd over de

---

[13] Namelijk de gegevens bedoeld in artikel 6*bis*, § 1, van de wet van 1991:

" *1° [4 voor iedere houder: het identificatienummer van het Rijksregister van de natuurlijke personen, de foto van de houder die overeenstemt met de foto van de laatste kaart, alsook de foto's van de houder die voorkomen op de identiteitskaarten die hem gedurende de laatste vijftien jaar werden afgeleverd, het elektronische beeld van de handtekening van de houder, alsook de historiek van de elektronische beelden van de handtekeningen, de gevraagde taal voor de uitgifte van de kaart en het volgnummer van de kaart. De Koning bepaalt de datum vanaf wanneer de historiek van de foto's en de historiek van de elektronische beelden van de handtekeningen opgeslagen en bewaard worden in het centrale bestand van de identiteitskaarten en in het centrale bestand van de vreemdelingenkaarten;]4*

2° voor elke uitgegeven (kaart) : <W 2007-05-15/42, art. 12, 013; Inwerkingtreding : 18-06-2007>
a) de datum van aanvraag met aansluitend de datum van uitgifte van het basisdocument, de datum van uitgifte, de vervaldatum en in voorkomend geval de datum van vernietiging;

b) de datum van uitreiking en de gemeente die ze uitgereikt heeft;

c) het volgnummer van de kaart;

d) het sequentienummer (eerste, tweede, derde kaart, enz.);

e) de informatie waaruit blijkt dat de kaart geldig, vervallen of vernietigd is en, in dat geval, de reden;

f) het type van (kaart); <W 2007-05-15/42, art. 12, 013; Inwerkingtreding : 18-06-2007>

g) de aanwijzing van het bestaan of de afwezigheid van de functie " elektronische handtekening ";

h) de datum van de laatste bijwerking;

i) de datum van de laatste bijwerking betreffende de hoofdverblijfplaats.

(j) de andere vermeldingen, opgelegd door de wetten;) <W 2007-05-15/42, art. 12, 013; Inwerkingtreding : 18-06-2007> [3 k) de in artikel 374/1 van het Burgerlijk Wetboek bedoelde vermelding]3".

[14] De aanvrager antwoordde het volgende:

"*Wat het toepassingsgebied van het wetsvoorstel betreft, breidt artikel 5quater het toepassingsgebied van artikel 5ter uit om tegemoet te komen aan de bredere behoefte van de private sector om toegang te krijgen tot kwalitatief betere gegevens via een praktisch en veilig proces. Dit verruimde toepassingsgebied is nodig om te voorkomen dat burgers minder nauwkeurige en minder veilige methoden gebruiken om hun gegevens aan private entiteiten te verstrekken, zoals processen op papier of het gebruik van een kopie van identiteitsdocumenten/paspoorten in combinatie met manuele processen voor het bijwerken van gegevens op initiatief van de burger.*"

tenuitvoerlegging van artikel 5*ter* van de RR-wet, en het RR antwoordde **dat tot op heden geen enkele machtigingsaanvraag is ingediend op basis van artikel 5*ter* van de RR-wet**.

27. Met het oog op een doeltreffend parlementair debat over het ontwerp, rekening houdend met de beoogde uitbreiding van de toegang van de private sector tot de gegevens uit het RR, het Register van de Identiteitskaarten en het Register van de Vreemdelingenkaarten, **beveelt de Autoriteit de aanvrager aan om een effectbeoordeling uit te voeren, mede in het licht van de in dit advies opgeworpen vragen**.

II.2.4. Elektronische identificatie in de eIDAS-verordening ten aanzien van de doelstellingen van het voorstel

28. De **doelstellingen van het voorstel zijn onduidelijk**. De Autoriteit benadrukt dat **elektronische identificatie** in het kader van de eIDAS-verordening in wezen tot doel heeft de identiteit van een persoon met een bepaalde mate van betrouwbaarheid (laag, substantieel of hoog) vast te stellen en te bevestigen (authenticatie) op basis van gegevens die deze persoon op unieke wijze vertegenwoordigen overeenkomstig het toepasselijk recht. De eIDAS-verordening heeft **het minimale pakket persoonsidentificatiegegevens vastgesteld dat nodig is om een persoon** (natuurlijke persoon of rechtspersoon) **op unieke wijze te vertegenwoordigen**, en voor natuurlijke personen gaat het om de volgende **verplichte** gegevens: huidige familienaam of familienamen; huidige voornaam of voornamen; geboortedatum; unieke identificatiecode, door de lidstaat van verzending vastgesteld volgens de technische specificatie voor grensoverschrijdende identificatie, zodanig dat deze zo lang mogelijk stabiel blijft[15]. Het minimale pakket gegevens ***kan*** ook een of meer van de volgende aanvullende attributen bevatten: voornaam of voornamen en familienaam of familienamen bij geboorte; geboorteplaats; huidig adres; geslacht[16]. In dit verband wijst de Autoriteit erop dat het toevoegen van facultatieve gegevens moet worden **gerechtvaardigd overeenkomstig het beginsel van minimale gegevensverwerking zoals neergelegd in artikel 5, 1., c), van de AVG[17]**. Terloops, en zonder dit onderwerp te analyseren, merkt de Autoriteit op dat volgens de online beschikbare technische documentatie over **Itsme de "*attributen*" (of "*claims*")** die over de gebruiker kunnen worden meegedeeld, talrijker zijn en dus verder lijken te gaan dan loutere identificatie in de zin van de eIDAS-verordening[18].

---

[15] Zie artikel 12, 3., d), van de eIDAS-verordening en de bijlage van Uitvoeringsverordening (EU) 2015/1501 van de Commissie van 8 september 2015 *betreffende het interoperabiliteitskader bedoeld in artikel 12, lid 8, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt*.

[16] *Ibidem*.

[17] In België **volstaan de namen, de voornamen, de geboortedatum en het RR-nummer per definitie om een betrokkene op unieke wijze te vertegenwoordigen**. De voornaam of voornamen en familienaam of familienamen bij geboorte, de geboorteplaats, het huidige adres en het geslacht zijn niet noodzakelijk. Logischerwijs benadrukt de Autoriteit dat de eIDAS-verordening geen afbreuk doet aan de AVG (zie artikel 2, 4., van de eIDAS-verordening.

[18] Zonder in detail te treden, behoren **in het kader van eIDAS** voor België de volgende gegevens tot de **facultatieve** gegevens: het geslacht ("*User's gender. Possible values are: female male unknown n/a. If the value mentioned on the user's*

29. Elektronische identificatie in de zin van de eIDAS-verordening **is niet bedoeld om persoonsgegevens uit een authentieke bron rechtstreeks** door een "*aanbieder van een dienst voor elektronische identificatie*"[19] **te laten meedelen** aan ondernemingen waarbij de betrokkene gebruikmaakt van die aanbieder (in feite een bepaald stelsel voor identificatie). **Het is niet de bedoeling dat die ondernemingen die gegevens gebruiken voor het nakomen van wettelijke verplichtingen of het verwezenlijken van andere doeleinden die hun eigen zijn, maar enkel om de door de betrokkene opgegeven identiteit te bevestigen aan de hand van vooraf vastgelegde identificatiegegevens[20, 21]**.

30. In dit verband **is hier geen sprake van Europese portemonnees voor digitale identiteit** of **elektronische attesteringen van attributen[22]**. Daarbij moet worden opgemerkt dat de doeleinden van de Europese portemonnee voor identiteit verder gaan dan loutere identificatie zoals bedoeld in de eIDAS-verordening[23], en dat deze portemonnee gepaard gaat met een reeks aanvullende waarborgen op het gebied van transparantie en controle door de betrokkene[24].

31. Bovendien definieert artikel 1, 1°, van **het KB van 2017** in Belgisch recht de "*dienst voor elektronische identificatie*" als "*de dienst die de identiteit garandeert van de gebruiker die toegang zoekt **tot overheidstoepassingen** op basis van een aanmeldoptie*" (in vet aangeduid door de Autoriteit)[25]. In

---

ID document is different from those (local language, letter code...), then we apply a best-effort mapping to one of those values."), evenals de "*official_gender*" ("*User's gender unaltered, exactly as mentioned on their ID document.*"); de geboorteplaats (stad en land); het adres. **Naast** de gegevens bedoeld in de eIDAS-verordening zijn met name ook de volgende gegevens beschikbaar: de nationaliteit (in twee formaten: zoals vermeld op het identiteitsdocument en volgens de ISO 3166-1 alpha-3-code); het identificatienummer van het identiteitsdocument; informatie over het apparaat van de gebruiker (OS, model, enz.); de datum van afgifte van het identiteitsdocument en de vervaldatum ervan; het type identiteitsdocument en het land dat het heeft afgegeven; en de **foto** (namelijk "*User's ID picture, represented as a URL string. This URL points to an image file (for example, a JPEG, JPEG2000, or PNG image file). This image is the raw (unprocessed) image contained on the ID document. Accessing this URL has to be done with your bearer token. Example:* […]"). Zie

https://belgianmobileid.github.io/doc/authentication/#user-data, https://belgianmobileid.github.io/doc/identification/#user-data, https://belgianmobileid.github.io/doc/confirmation/#user-data en https://belgianmobileid.github.io/doc/claims/, laatst geraadpleegd op 23/01/2025. De beschikbare attributen variëren naargelang het officiële document op basis waarvan het Itsme-account is aangemaakt.

[19] In de eIDAS-verordening moet een onderscheid worden gemaakt tussen de elementen die worden gevraagd in het stelsel voor identificatie, namelijk een identificatiemiddel – een materiële en/of immateriële eenheid; en een authenticatie – een proces.

Artikel 1, 1°, van het KB van 2017 definieert de "*dienst voor elektronische identificatie*" als "*de dienst die de identiteit garandeert van de gebruiker die toegang zoekt **tot overheidstoepassingen** op basis van een aanmeldoptie*" (in vet aangeduid door de Autoriteit).

[20] Zie overweging nr. 28 met betrekking tot **het minimale pakket gegevens**.

[21] Opmerking: zonder deze hypothese te analyseren, merkt de Autoriteit op dat de FAS ("*Federal Authentication Service*") wel degelijk "*attributen van een eindgebruiker bij één of meer betrouwbare bronnen die zich bevinden bij andere overheidsinstellingen (i.e., Rijksregister, KSZ en KBO)*" lijkt "*op te halen*". Zie https://bosa.belgium.be/nl/services/federal-authentication-service-fas#anchor-3, laatst geraadpleegd op 23/01/2025. Deze dienst wordt echter geleverd door een overheidsinstantie en met het oog op toegang tot overheidstoepassingen. Het gaat dus om een andere context.

[22] Zie de artikelen 3, 43) – 46), en 45*ter* tot en met 45*nonies* van de eIDAS-verordening, en bijlage VI van diezelfde verordening, waarin een **minimale lijst van attributen** is vastgesteld (waaronder adres, leeftijd, geslacht, burgerlijke staat, gezinssamenstelling, diploma's, enz.).

[23] Zie overweging nr. 6.

[24] Zie met name in dit verband overweging nr. 51.

[25] Het begrip "*dienstverlener*" verwijst naar "*de aanbieder van een erkende dienst voor elektronische identificatie*".

tegenstelling tot de Europese portemonnee voor digitale identiteit, die bedoeld lijkt om **elektronische identificatie** mogelijk te maken **ten aanzien van de <u>private sector</u> in het algemeen**, **in lijn met de logica van de hervorming van de eIDAS-verordening**, lijkt dat niet het geval te zijn voor de wet van 2017 en het KB van 2017.

32. In dit verband **heeft de Autoriteit de aanvrager meerdere vragen gesteld**[26], waarvan de antwoorden in de volgende uiteenzettingen in overweging worden genomen.

<u>II.2.5. De waarborg die de erkenning krachtens het KB van 2017 vormt</u>

33. Aangezien het voorstel de erkenning krachtens het KB van 2017 als een belangrijke waarborg in zijn context voorstelt, heeft de Autoriteit de aanvrager vragen gesteld over de toepasbaarheid van dit koninklijk besluit in het kader van identificatie in de private sector. Hij antwoordde het volgende (vrije vertaling):

> "*De accreditatie van aanbieders van een dienst voor elektronische identificatie in het kader van het koninklijk besluit eIDAS betreft de machtiging om diensten aan te bieden **in het kader van overheidstoepassingen**. Het is **echter** essentieel om op te merken dat de elektronische identificatiemiddelen die onder de accreditatie vallen, **zowel in het kader van diensten aan de publieke sector als aan de private sector worden aangeboden**. Dit punt wordt overigens onderstreept door het koninklijk besluit eIDAS zelf, dat vereist dat deze dienstverleners deze diensten al aanbieden overeenkomstig de vereisten van de eIDAS-verordening vóór de accreditatie (zie artikel 28 van het koninklijk besluit eIDAS). In het bijzonder zijn de elektronische identificatiemiddelen zelf onderworpen aan strikte vereisten krachtens de eIDAS-verordening.*
>
> ***In zekere zin fungeert de accreditatie zoals bedoeld in het koninklijk besluit eIDAS als een extra laag** voor aanbieders van een dienst voor elektronische identificatie. Deze extra laag **blijft** niettemin **relevant** (naast de bestaande vereisten krachtens de eIDAS-verordening zelf) **voor het aanbieden** van elektronische identificatiemiddelen door geaccrediteerde aanbieders van een dienst voor elektronische identificatie **in de private***

[26] Zou het doeleinde van het voorstel in feite niet kunnen worden bereikt via de Belgische (Europese) portemonnee voor digitale identiteit en de elektronische attesteringen van attributen? Wat is de meerwaarde ervan in dit opzicht? Is het doel werkelijk om, via de door de betrokkene gebruikte dienstverlener van elektronische identificatiemiddelen, gegevens uit het RR mee te delen aan de ondernemingen waarbij deze persoon zich identificeert, zodat deze ondernemingen hun wettelijke verplichtingen kunnen nakomen, en om welke verplichtingen gaat het dan? Kan een concreet voorbeeld worden gegeven van de beoogde scenario's? Kan worden bevestigd of ontkend dat de in het KB van 2017 bedoelde erkenning betrekking heeft op diensten voor identificatie die worden gebruikt voor toegang tot overheidstoepassingen (en niet tot diensten die worden verleend door private entiteiten)? In geval van bevestiging: op basis van welke regels zouden dienstverleners dan worden erkend met betrekking tot toegang tot diensten die worden aangeboden door de private sector? De Autoriteit heeft de aanvrager ook verzocht te rechtvaardigen waarom werd overwogen toegang te verlenen tot gegevens die verder gaan dan het minimale pakket verplichte persoonsidentificatiegegevens dat nodig is om een persoon op unieke wijze te vertegenwoordigen, zoals bedoeld in de eIDAS-verordening (zie overweging nr. 28), terwijl het enkel om identificatie gaat?

> ***sector**. Het koninklijk besluit eIDAS legt **bijkomende vereisten** op **die gelden voor de volledige organisatie van dienstverleners**. Die laatste zijn in het bijzonder onderworpen aan auditverplichtingen die gelden voor hun volledige organisatie, en moeten strikte waarborgen bieden **die van toepassing zijn op al hun processen en diensten, ongeacht of deze aan overheidsinstanties of aan private entiteiten worden aangeboden**. Een voorbeeld hiervan is de verplichting om strikt te voldoen aan – en te worden gecontroleerd op – de AVG, de veiligheidsvereisten, enzovoort. Het toezicht van de Belgische autoriteiten op geaccrediteerde aanbieders van een dienst voor elektronische identificatie in het kader van het koninklijk besluit eIDAS r**eikt dus verder dan alleen hun diensten in het kader van overheidstoepassingen**."* (in vet aangeduid door de Autoriteit)[27]

34. De Autoriteit neemt akte van dit antwoord. **Opdat de in het voorstel bedoelde erkenning daadwerkelijk de waarborg kan bieden die zij krachtens het voorstel en de motivering ervan geacht wordt te bieden, is de Autoriteit van oordeel dat het volgende vereist is**:

- de aanvrager moet **nagaan** of een erkenning zoals bedoeld in het KB van 2017 wel kan worden opgelegd bij het aanbieden van diensten voor identificatie in de private sector op grond van het feit dat de betrokken dienstverlener toegang krijgt tot authentieke gegevensbronnen;

---

[27] De aanvrager antwoordde ook het volgende (vrije vertaling):

"*De specifieke status en rol van erkende dienstverleners van elektronische identificatiemiddelen in de private sector en het feit dat zij bijkomende waarborgen bieden, waardoor zij met name specifieke gegevens kunnen verwerken in het kader van de wet op de rijksregisters, zijn reeds herhaaldelijk erkend door de Belgische wetgever.*

In 2018, onmiddellijk na de invoering van de status van aanbieders van een dienst voor elektronische identificatie, werd de wet op het Rijksregister gewijzigd om deze dienstverleners specifiek te machtigen het Rijksregisternummer te verwerken voor identificatie- en authenticatiedoeleinden in het kader van de diensten die zij aan private entiteiten aanbieden (zie artikel 8, § 5, van de wet op het Rijksregister). Aanbieders van een dienst voor elektronische identificatie zijn in dit verband ook gemachtigd om het Rijksregisternummer door te geven aan private entiteiten die gebruikmaken van hun identificatie- en authenticatiediensten, voor dezelfde identificatie- en authenticatiedoeleinden (zie de toelichting bij artikel 8, § 5, in het wetsvoorstel houdende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters, Artikelsgewijze toelichting, St., K., 2017-2018, nr. 3256/001, pp. 26-27).

In 2020 heeft de Belgische wetgever de vijfde antiwitwasrichtlijn (EU-richtlijn 2018/843 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering) omgezet door de wet van 20 juli 2020 aan te nemen. In het kader van deze omzetting heeft de Belgische wetgever erkend dat met name de lidstaten de private sector moeten aanmoedigen om vrijwillig gebruik te maken van de elektronische identificatiemiddelen die zijn erkend in het kader van een aangemeld stelsel, dat wil zeggen met name de elektronische identificatiemiddelen die zijn geaccrediteerd in het kader van het koninklijk besluit eIDAS (zie met name de toelichting in het wetsvoorstel houdende diverse bepalingen tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten, Memorie van toelichting, St., K., 2019-2020, nr. 1324/001, pp. 10-11). De wetgever heeft dus uitdrukkelijk erkend dat het gebruik van de elektronische identificatiemiddelen die worden aangeboden door erkende dienstverleners van elektronische identificatiemiddelen, voldoende wordt geacht om te voldoen aan de KYC-verplichtingen in verband met de verificatie van te identificeren personen in het kader van de verplichtingen ter bestrijding van het witwassen van geld en de financiering van terrorisme (zie artikel 27, § 1, 2°, van de Belgische wet ter bestrijding van het witwassen van geld)."

Deze overwegingen zijn in het onderhavige geval echter niet doorslaggevend. Enerzijds zijn de certificaten (authenticatie- en handtekeningcertificaten) opgenomen op de Belgische identiteitskaart waarop het RR-nummer staat vermeld, waardoor de verwerking van dat nummer noodzakelijk is voor elke oplossing die op deze certificaten is gebaseerd. Een aanpassing van de RR-wet was bijgevolg noodzakelijk om elektronische identificatie en ondertekening op basis van de betrokken certificaten mogelijk te maken (de verwerking van het RR-nummer is noodzakelijk voor de verificatie van de certificaten). In dit verband wordt aangenomen dat het gebruiksdoel van het RR-nummer uitsluitend beperkt is tot hetgeen in artikel 8, §§ 5 en 3, van de RR-wet is vastgelegd. Anderzijds is het feit dat de wetgever het gebruik van de betrokken erkende diensten aanmoedigt, niet doorslaggevend voor de vaststelling van het toepassingsgebied van de regels van het KB van 2017.

- de aanvrager moet met zekerheid vaststellen dat het KB van 2017 juridisch ook van toepassing is op het verlenen van diensten voor elektronische identificatie in de private sector door erkende dienstverleners, en in welke mate dat het geval is. De Autoriteit kan dit niet bevestigen en heeft daar twijfels over[28], hoewel bepaalde voorwaarden van de erkenning betrekking hebben op de activiteit van de dienstverlener in het algemeen. Bovendien beoogt het voorstel verder te gaan dan loutere identificatie in de zin van de eIDAS-verordening[29]. **Aangezien het KB van 2017 oorspronkelijk niet is opgesteld met het voorstel in gedachten** (voor toepassingen in de private sector met het oog op de identificatie en uitwisseling van aanvullende gegevens), **moet het worden aangepast** om ook en met de nodige zekerheid, voor zover relevant[30], van toepassing te zijn op het verlenen van diensten zoals bedoeld in het voorstel in de private sector;

- de regels en het proces inzake erkenning moeten voorzien in de inachtneming en de beoordeling van de toepassing van de beginselen en waarborgen inzake gegevensbescherming, met name in het licht van latere ontwikkelingen[31].

II.2.6. Doelstellingen van het voorstel en verwerkte gegevens

A) Aanvullende informatie verstrekt door de aanvrager

35. Wat **het doeleinde** van het voorstel betreft, heeft de aanvrager het volgende gepreciseerd (vrije vertaling):

> "*Het voorstel heeft een tweeledig doel:* ***(i) de beveiliging van gegevensuitwisselingen verbeteren en tegemoetkomen aan de behoefte aan een betere gegevenskwaliteit in de private sector, met name om redenen van naleving, en (ii) de administratieve lasten voor burgers en private entiteiten verminderen****.*

[28] Zie met name de artikelen 1, 1° (definitie van de dienst voor elektronische identificatie); 2, § 1 (het gevolg van de erkenning is de machtiging om de dienst ter beschikking te stellen voor het gebruik voor overheidstoepassingen); 4 (verband met de aanmeldoptie waarmee toegang wordt verzocht tot de overheidstoepassing); 16, § 1 (beoogt alleen de geraadpleegde overheidstoepassingen); 20 (betreffende de te verstrekken ondersteuning); 33 en 34 (operationele gevolgen van de erkenning in verband met overheidstoepassingen); 41 (vergoeding van dienstverleners), enzovoort. Het KB van 2017 **bepaalt overigens niet uitdrukkelijk dat de daarin opgenomen voorwaarden ook van toepassing zijn op het aanbieden van diensten in het kader van de toepassingen in de private sector, noch sluit het uit dat de erkende dienstverlener** in datzelfde kader **diensten voor elektronische identificatie aanbiedt onder andere voorwaarden, die niet zouden voldoen aan de voorwaarden van de erkenning**. Hoe zit het bijvoorbeeld met de toepasbaarheid van de vereisten inzake de beschikbaarheid van de dienstverlening, de reactietijd, het uitrolbeheer, enzovoort?

[29] Zie overwegingen nrs. 35 en 41-42.

[30] Daarbij moet ook rekening worden gehouden met de mogelijkheid dat bepaalde dienstverleners hun diensten niet wensen aan te bieden voor identificatie binnen overheidstoepassingen – welke regels inzake erkenning moeten in dat geval van toepassing blijven?

[31] Zie overweging nr. 51.

Het voorstel biedt aanbieders van een dienst voor elektronische identificatie de mogelijkheid om de gegevens die bij de identificatie van burgers zijn verzameld (met inbegrip van de gegevens die zijn verkregen uit de identiteitskaart van burgers), indien nodig, bij te werken, op voorwaarde dat zij van de betrokken burgers een geldige toestemming in de zin van de AVG hebben ontvangen en dat deze toestemming op het moment van de bijwerking nog steeds geldig is. Dit betreft de gegevens waarvan de authentieke bron het Rijksregister is (cf. het voorstel voor een nieuw artikel 5quater in het kader van de wet op het Rijksregister van 8 augustus 1983) en het Register van de Identiteitskaarten (cf. het voorstel tot wijziging van artikel 6bis, derde lid, van de wet betreffende de bevolkingsregisters en de identiteitskaarten van 19 juli 1991). Dit garandeert dat burgers geen verouderde gegevens delen wanneer zij zich bij private entiteiten moeten identificeren en beslissen om daarvoor hun elektronisch identificatiemiddel te gebruiken. Elk ***verder*** *gebruik van de elektronische identificatiemiddelen om burgers te identificeren en elke doorgifte van persoonsgegevens in verband met deze elektronische identificatiemiddelen zal altijd met de toestemming van de betrokken burger gebeuren en* ***kan om verschillende redenen vereist zijn, met name de noodzaak om met voldoende zekerheid de persoon te identificeren en te authenticeren met wie een private entiteit in contact staat en met wie zij mogelijk een contract afsluit, of de wettelijke verplichting om bepaalde gegevens over de burger te verzamelen in het geval van een entiteit die onderworpen is aan het juridisch kader inzake de bestrijding van het witwassen van geld, bijvoorbeeld****.*

Het voorstel beoogt ***de lasten voor burgers bij het bijwerken van hun gegevens te verminderen en ervoor te zorgen dat zij zo min mogelijk proactief moeten optreden om hun gegevens handmatig bij te werken.*** *In de praktijk moeten burgers hun gegevens voortdurend bijwerken en opnieuw aan ondernemingen verstrekken, omdat wijzigingen in persoonsgegevens (bijvoorbeeld een adreswijziging) niet automatisch worden doorgegeven aan en niet gemakkelijk toegankelijk zijn voor de private sector (zoals hieronder wordt uiteengezet).*

Dit leidt tot verschillende inefficiënties en risico's, waaronder:

1. Ten eerste houdt elke gegevensdeling beveiligings- en vertrouwelijkheidsrisico's in wanneer deze niet via beveiligde kanalen verloopt.
2. Bovendien vereist deze manier van werken iedere keer een initiatief van een actor die vaak de burger zelf is.
3. Bij gebrek aan initiatief wordt informatie niet geüpdatet en dreigt foutieve (onvolledige of niet up-to-date) informatie te circuleren doordat updates of wijzigingen niet tijdig worden meegedeeld. Daardoor ontstaat rechtsonzekerheid. Ondernemingen kunnen niet aan hun

identificatieverplichtingen voldoen, noch aan de algemene verplichting onder de AVG om alleen met juiste gegevens te werken, met alle risico's van dien (identiteitsfraude, digitale uitsluiting, enz.). Denk bijvoorbeeld aan een onderneming die niet tijdig op de hoogte wordt gebracht van een adreswijziging van zijn klant.

*Bovendien **zijn de processen voor het bijwerken van gegevens ondoeltreffend, duur en tijdrovend, zowel voor burgers als voor private entiteiten**. Wanneer hun gegevens wijzigen, moeten burgers ook verschillende procedures volgen bij verschillende entiteiten (wanneer zij bijvoorbeeld van adres veranderen, moeten zij alle ondernemingen waarmee zij een duurzame relatie hebben op de hoogte brengen van deze wijziging), en dat op verschillende tijdstippen. Als gegevens niet tijdig worden bijgewerkt, kan dat uiteindelijk leiden tot het verlies van toegang tot essentiële diensten, zoals een geblokkeerde bankrekening. In het bijzonder kan dit ook tot gevolg hebben dat een geldig elektronisch identificatiemiddel niet meer kan worden gebruikt. Dit is des te problematischer omdat burgers soms denken dat hun elektronisch identificatiemiddel al gekoppeld is aan de authentieke bron, en daardoor niet de reflex hebben om hun elektronisch identificatiemiddel proactief bij te werken.*

Voor burgers die geen toestemming geven om hun gegevens te laten bijwerken, blijven die aanvullende maatregelen bestaan – al zijn die omslachtiger en minder doeltreffend – om hun gegevens alsnog bij te werken.

*Tot slot merken wij op dat het voorstel, voor het merendeel van de betrokken persoonsgegevens, betrekking heeft op **persoonsgegevens die reeds door aanbieders van een dienst voor elektronische identificatie worden verwerkt voor hetzelfde identificatiedoeleinde**. **Bijgevolg zou de impact op de hoeveelheid verwerkte persoonsgegevens van burgers beperkt moeten blijven.***" (in vet aangeduid door de Autoriteit)

36. De aanvrager heeft bovendien een **concreet voorbeeld** gegeven van de implementatie van het voorstel op basis van de Itsme-applicatie.

37. Wat betreft de rechtvaardiging voor de toegang tot gegevens **die verder gaan dan het minimale pakket verplichte persoonsidentificatiegegevens** dat nodig is om een persoon op unieke wijze te vertegenwoordigen zoals voorzien in de eIDAS-verordening[32], verklaarde de aanvrager het volgende (vrije vertaling):

[32] Zie overwegingen nrs. 23 en 28.

"*Toegang tot een breder pakket identificatiegegevens is* ***essentieel om het aanbieden van veilige en betrouwbare identificatiediensten die beantwoorden aan de verschillende behoeften in alle sectoren, te ondersteunen****. Het faciliteren van de toegang tot deze gegevens is tevens in overeenstemming met de algemene tendens in wetgeving op EU-niveau (zoals Verordening (EU) 2022/668, dat wil zeggen de verordening betreffende datagovernance, en Verordening (EU) 2023/2854, dat wil zeggen de dataverordening) en met de EU-strategie 2030 voor een data-economie. Deze initiatieven zijn erop gericht EU-burgers een betrouwbaarder en veiliger juridisch kader en infrastructuur te bieden om hun gegevens te controleren en deze in alle sectoren (zowel met publieke als private entiteiten) te kunnen delen.*

In het bijzonder kan de toegang tot de volgende gegevens in het Rijksregister als volgt worden gerechtvaardigd*:*

- *de naam en voornamen, de geboorteplaats en -datum, de hoofdverblijfplaats en de nationaliteit (artikel 3, 1°, 2°, 4°, 5°):*

Deze informatie is vereist voor de identificatie (met inbegrip van de verificatie van de identiteit) door de ***AML-richtlijn EU 2015/849*** *(zoals gewijzigd door de AML-richtlijn 2018/843), die werd omgezet in de* ***Belgische wet van 17 september 2017*** *(zoals gewijzigd door de wet van 20 juli 2020), waarbij de geboorteplaats als bijkomend element werd toegevoegd. Deze wettelijke verplichting geldt voor zeer uiteenlopende sectoren, met name voor financiële instellingen en de verzekeringssector, maar ook voor de boekhoudsector, de kansspelsector, de postdiensten, de diamantsector, enzovoort (cf. artikel 5 van de Belgische wet tot bestrijding van het witwassen van geld). In het bijzonder vereisen de richtsnoeren van de NBB inzake de bestrijding van het witwassen van geld in de financiële sector dat deze gegevens worden bijgehouden, wat in overeenstemming is met de algemene verplichtingen van de AVG.*
Bovendien moet bij ***het aanmaken van een*** *gekwalificeerd* ***certificaat*** *voor natuurlijke personen de namen en voornamen, de geboortedatum en, in bepaalde gevallen, de nationaliteit worden vermeld, overeenkomstig de eIDAS- en ETSI-normen.*

- ***de plaats en datum van het overlijden, of, in het geval van een verklaring van afwezigheid, de datum van de overschrijving van de beslissing houdende verklaring van afwezigheid (artikel 3, 6°)****:*

Overeenkomstig de ***eIDAS-verordening*** *zijn aanbieders van elektronische identificatiemiddelen verplicht om de uiterst betrouwbare identificatie van natuurlijke personen te baseren op procedures die de voortdurende geldigheid van deze identificatie*

aantonen. Het gebruik van deze informatie is dan ook van cruciaal belang om te waarborgen dat de elektronische identificatiemiddelen niet meer worden gebruikt na het overlijden van de betrokken burger;

- ***het geslacht, de burgerlijke staat, de samenstelling van het gezin, de wettelijke samenwoning, de verblijfstoestand voor de vreemdelingen, de vermelding van het register waarin de personen zijn ingeschreven: het bevolkingsregister, het vreemdelingenregister, het "wachtregister" of het consulaire register; de administratieve toestand van de personen die zijn ingeschreven in het consulaire register (artikel 3, 3°, 8°, 9°, 10°, 11°, 13°, 14°)****;*

Overeenkomstig de wetgeving tot bestrijding van het witwassen van geld en de richtsnoeren van de financiële regelgevende instanties, betreft het hier ***aanvullende informatie die de betrokken entiteiten moeten opvragen in het kader van hun KYC-proces****, hetzij in het kader van "bijkomende informatie die moet worden gevraagd in geval van maatregelen van verhoogde waakzaamheid", hetzij om een nauwkeurige beoordeling te maken van de risico's in verband met de bestrijding van het witwassen van geld in het kader van de relatie met de te identificeren persoon. Het gaat om gegevens die onder meer informatie kunnen verschaffen over de herkomst van de middelen en de eigendom van de goederen.*

- *de akten en beslissingen betreffende de* ***rechtsbekwaamheid en de beslissingen tot bewind over de goederen of over de persoon bedoeld in artikel 1250, eerste lid, van het Gerechtelijk Wetboek (artikel 3, 9°/1); en, in voorkomend geval, het bestaan van het identiteits- en handtekeningscertificaat, zoals bepaald in de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten*** *(artikel 3, 12°):*

Deze informatie is nodig om te bepalen of de burger daadwerkelijk de rechtsbekwaamheid heeft om als volwassene een contract af te sluiten en digitaal te communiceren met andere private entiteiten.

In het bijzonder kan de toegang tot de volgende gegevens ***in het Register van de Identiteitskaarten*** *als volgt worden gerechtvaardigd:*

- *Voor* ***de eIDAS-regelgeving*** *en* ***de identificatie van de persoon voor wie de elektronische identificatiemiddelen worden afgegeven, alsmede voor het***

aanmaken van een gekwalificeerd certificaat *voor natuurlijke personen, moet er een middel zijn om de persoon op unieke wijze te identificeren en te koppelen aan het erkende en geldige identiteitsdocument dat oorspronkelijk voor de identificatie is gebruikt. Daartoe moeten deze entiteiten ten minste de volgende gegevens verzamelen:*

- *de datum van aanvraag met aansluitend de datum van uitgifte van het basisdocument, de datum van uitgifte, de vervaldatum en in voorkomend geval de datum van vernietiging;*
- *het sequentienummer van de kaart;*
- *de informatie waaruit blijkt dat de kaart geldig, vervallen of vernietigd is en, in dat geval, de reden;*
- *het identificatienummer in het Rijksregister van de natuurlijke personen;*

- *De volgende bijkomende informatie is ook vereist voor de identificatie (met inbegrip van de verificatie van de identiteit) door de* ***AML-richtlijn EU 2015/849*** *(zoals gewijzigd door de AML-richtlijn 2018/843), die werd omgezet in de* ***Belgische wet van 17 september 2017*** *(zoals gewijzigd door de wet van 20 juli 2020),* ***met inbegrip van de foto van de betrokkene als bijkomend element, maar ook de rechtsbekwaamheid en de verblijfplaats****. Deze wettelijke verplichting geldt voor zeer uiteenlopende sectoren, met name voor financiële instellingen en de verzekeringssector, maar ook voor de boekhoudsector, de kansspelsector, de postdiensten, de diamantsector, enzovoort (cf. artikel 5 van de Belgische wet tot bestrijding van het witwassen van geld). Deze gegevens omvatten:*
  - *de foto van de houder die overeenkomt met de foto op de laatste kaart;*
  - *het type van kaart;*
  - *de aanwijzing van het bestaan of de afwezigheid van de functie "elektronische handtekening";*
  - *de datum van de laatste bijwerking;*
  - *de datum van de laatste bijwerking betreffende de hoofdverblijfplaats;*
  - *de eventuele vermelding betreffende de uitoefening van het ouderlijk gezag zoals bedoeld in artikel 374/1 van het Burgerlijk Wetboek.*" (in vet aangeduid door de Autoriteit)

38. Wat betreft de **mogelijkheid om de doelstellingen van het voorstel te verwezenlijken in het kader van de recent hervormde eIDAS-verordening**, antwoordde de aanvrager het volgende (vrije vertaling):

"*Attesteringen van attributen zijn* ***nieuwe diensten*** *die in de komende wijzigingen van de eIDAS-verordening worden voorzien. Deze herziene versie van de eIDAS-verordening is echter*

> ***nog niet volledig geïmplementeerd en van toepassing***. *De volledige toepassing van de herziene versie van de eIDAS-verordening wordt* ***niet vóór ten minste 2027 verwacht en vereist de goedkeuring van uitvoeringshandelingen****, terwijl de private sector steeds meer behoefte heeft aan toegang tot betrouwbare gegevens uit bepaalde authentieke bronnen.*
>
> *In dit opzicht steunt het voorstel op de waarborgen die worden geboden door de juridische kaders voor identificatie en authenticatie (met inbegrip van de huidige toepasbare versie van de eIDAS-verordening en de Belgische wetgeving), en laat het zich inspireren door het doel van de herziene eIDAS-verordening. De toegevoegde waarde van het voorstel ligt met name in de mogelijkheid om tegemoet te komen aan een reële en dringende behoefte van burgers en private ondernemingen, die tot op heden niet door andere bestaande maatregelen kan worden vervuld.*" (in vet aangeduid door de Autoriteit)

39. De Autoriteit heeft zich ook vragen gesteld bij de beoogde wijziging van **artikel 6*bis*, § 3, van de wet van 1991**[33], aangezien het gebruik van een geldig identificatiemiddel een voorwaarde is voor de identificatie via een stelsel voor identificatie. Zodra de betrokkene gebruikmaakt van het betrokken stelsel ten aanzien van een (publieke of private) entiteit of een dienst voor elektronische identificatie, wordt hij geïdentificeerd op basis van het door dat stelsel gegarandeerde betrouwbaarheidsniveau. Onder deze omstandigheden **ziet de Autoriteit de bedoeling van het voorstel niet in. Zij heeft de aanvrager verzocht om te verduidelijken welke concrete wettelijke/technische belemmering het voorstel tracht weg te nemen.** Is het bijvoorbeeld de bedoeling dat de dienstverlener van het identificatiemiddel (bijvoorbeeld Itsme) zelf de gegevens kan bijwerken die hij uit de identiteitskaart van de betrokkene heeft gehaald *op het moment dat deze zijn account heeft aangemaakt en zich bij hem via dit identificatiemiddel (eID) heeft geïdentificeerd*? In plaats van, in voorkomend geval, dit aspect door de betrokkene te laten beheren? De aanvrager heeft de Autoriteit hierop geen rechtstreeks antwoord gegeven, maar deze hypothese lijkt in ieder geval te worden beoogd door het voorbeeld dat hij geeft van het mogelijke gebruik van de Itsme-applicatie[34].

---

[33] Zie overwegingen nrs. 14-15.

[34] "*3.3.1. Stap 1: ontvangst van updates door de [dienstverlener van elektronische identificatiemiddelen]*

Bijwerking van de gegevens door de burger via de itsme-applicatie zelf

- ***Waarbij de mogelijkheid tot bijwerking via het Rijksregister****, of via andere kanalen indien nodig, is voorzien.*
- *Een volledige beschrijving van het proces en de mogelijke alternatieven vindt u hier.*
- *Via de rubriek "Meer informatie" kan de gebruiker meer te weten komen over zijn rechten.*

Aanvaarding en activering van het delen van gegevens uit het Rijksregister

- *Optioneel, onmiddellijk na het aanmaken van het itsme®-account.*
- *Op elk ander moment tijdens het gebruik van de itsme-applicatie.*
- *Deactivering blijft mogelijk op dezelfde eenvoudige manier in de itsme-applicatie.*

Kennisgeving van de bijwerking van persoonsgegevens via het Rijksregister

- *De itsme-applicatie geeft aan wanneer een bijwerking van de gegevens heeft plaatsgevonden.*

40. Het voorstel en de door de aanvrager verstrekte antwoorden geven aanleiding tot de volgende opmerkingen van de Autoriteit.

B) Bepaling van de doelstellingen van het voorstel – beginselen

41. Allereerst moet worden opgemerkt dat het **dispositief** van het voorstel, overeenkomstig de beginselen van voorspelbaarheid en legaliteit zoals neergelegd in artikel 8 van het EVRM en artikel 22 van de Grondwet, alsmede overeenkomstig artikel 6, lid 3, 2e alinea, van de AVG, **de doeleinden van de verwerking exhaustief** moet **bepalen**. Wanneer het overigens gaat om de verwerking van gegevens op basis van de **toestemming van de betrokkene**, zoals de CBPL ook heeft benadrukt in haar advies[35], dan mag die toestemming enkel betrekking hebben op een of meer **specifieke doeleinden**. **In dat opzicht is de Autoriteit van oordeel dat het dispositief van het voorstel verder moet worden uitgewerkt, zodat de betrokken specifieke doeleinden duidelijk worden geïdentificeerd[36]**. In het onderhavige geval zijn bijvoorbeeld de volgende formuleringen op zich geen welbepaalde en specifieke doeleinden: bijwerking van gegevens[37]; administratieve vereenvoudiging; nalevingsdoeleinden; identificatie en authenticatie in het algemeen.

42. Ten tweede, en dit punt wordt hieronder nader toegelicht met betrekking tot een van de concrete en welbepaalde doeleinden die in de toelichting van het voorstel en door de aanvrager worden genoemd[38], **moet** het dispositief van het voorstel **een duidelijk onderscheid maken tussen deze doeleinden en de dienst voor identificatie zoals bedoeld in het stelsel voor elektronische identificatie onder de eIDAS-verordening.** In dit verband is het doeleinde van het voorstel ook (net zoals bij de eIDAS2-verordening[39]) om de dienstverleners van elektronische identificatiemiddelen zoals bedoeld in de eIDAS-verordening in staat te stellen **andere diensten aan te bieden**, namelijk het uitwisselen van gegevens tussen de betrokkene en de entiteiten waarvan hij gebruikmaakt, via authentieke bronnen. Het dispositief van het voorstel moet in dit verband bepalen dat, zodra de dienst voor elektronische identificatie aan de betrokkene wordt aangeboden, **dergelijke andere diensten moeten worden onderscheiden** (van de dienst voor elektronische identificatie zoals bedoeld in de

---

- *Deze kennisgeving herinnert de gebruiker aan de mogelijkheid om zijn toestemming in te trekken.*" (in vet aangeduid en vertaald door de Autoriteit).

[35] Overweging nr. 28.

[36] Artikel 5*ter*, § 2, 2°, van de RR-wet gaat hier dieper op in, onverminderd de eventuele analyse die deze bepaling zou vereisen. (Bijvoorbeeld,

[37] Terloops wijst de Autoriteit de aanvrager erop dat krachtens artikel 5, 1., van de AVG gegevens "*zo nodig*" moeten worden geactualiseerd. In ieder geval moet de noodzaak om gegevens te actualiseren worden beoordeeld in het licht van het doeleinde van de verwerking.

[38] Zie overwegingen nrs. 46 e.v.

[39] Zie overweging nr. 38.

eIDAS-verordening) en optioneel moeten blijven, in overeenstemming met het doeleinde van het ontwerp.

43. In dit verband wijst de Autoriteit erop dat het waarschijnlijk **beter** is **om**, in plaats van nieuwe soorten diensten naar Belgisch recht te implementeren, **te wachten op de implementatie van de Europese portemonnees voor digitale identiteit en de attesteringen van attributen[40] zoals bedoeld in de eIDAS2-verordening**, voor zover deze een antwoord kunnen bieden op de bezorgdheden van de aanvrager. Dit is een belangrijke overweging **die in aanmerking moet worden genomen in het kader van de uitvoering van een effectbeoordeling[41]**.

44. Ten derde is de Autoriteit van oordeel dat het voorstel een bepaling moet bevatten **die de verdere verwerking van de** meegedeelde **gegevens voor enig ander doeleinde verbiedt**, in het licht van wat artikel **5*ter*, § 5, eerste lid, van de RR-wet** bepaalt.

45. Dat gezegd zijnde, en meer concreet met betrekking tot de doeleinden, verwijzen het voorstel en de aanvrager in zijn antwoorden voornamelijk naar **twee concrete doeleinden**: de uitvoering van de identificatieverplichtingen in het kader van de bestrijding van het witwassen van geld ("*know your customer*") (hierna "**AML-doelstelling**") en de uitvoering van de eIDAS-verordening zelf (hierna "**eIDAS-doelstelling**").

C) AML-doelstelling (gegevensstroom naar de dienstverlener van elektronische identificatiemiddelen en gegevensstroom naar de onderworpen entiteiten)

46. Wat betreft de uitvoering van de identificatieverplichtingen die voortvloeien uit de wet van 18 september 2017 *tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten* (hierna "**AML-wet**") en de Europese richtlijnen die deze wet omzet, zijn de volgende opmerkingen van belang.

47. Ten eerste merkt de Autoriteit op dat, **hoewel** het **onbetwistbaar** is dat het gebruik van een dienst voor elektronische identificatie met een hoog betrouwbaarheidsniveau **zal bijdragen tot de uitvoering van de** in deze wetgeving neergelegde **verplichtingen** in een digitale omgeving[42], **het**

[40] Overweging nr. 62 van de eIDAS2-verordening luidt overigens als volgt:

"*Veilige elektronische identificatie **en de verlening van attesteringen van attributen** moeten extra flexibiliteit en oplossingen voor de financiëledienstensector bieden om klanten te kunnen identificeren **en specifieke attributen te kunnen uitwisselen** waaraan moet worden voldaan, zoals cliëntenonderzoeksvereisten uit hoofde van een toekomstige verordening tot oprichting van de antiwitwasautoriteit, of uit de wetgeving ter bescherming van investeerders voortvloeiende geschiktheidseisen, ofwel ter ondersteuning van strenge cliëntauthenticatievereisten voor online-identificatie om op accounts in te loggen en transacties op het gebied van betalingsdiensten te initiëren.*" (in vet aangeduid door de Autoriteit)

[41] Zie overweging nr. 27.

[42] Zie met name artikel 13, 1., a), van **Richtlijn (EU) 2015/849** van het Europees Parlement en de Raad van 20 mei 2015 *inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot*

doeleinde van de diensten voor elektronische **identificatie** zoals bedoeld in de eIDAS-verordening **niet gelijkstaat aan de uitvoering van de verplichtingen** inzake identificatie van cliënten zoals neergelegd in de Europese en nationale wetgeving in het kader van de bestrijding van het witwassen van geld. Daarnaast, en zonder hier dieper in te gaan op deze wetgeving, legt de bovengenoemde wet een verplichting op die varieert naargelang het risiconiveau van de cliënt[43] en de situatie waarin de betrokkene zich bevindt. De informatie die wordt verkregen door het gebruik van erkende elektronische identificatiemiddelen wordt daarin beschouwd als een van de middelen om informatie over de cliënt te verkrijgen[44]. Naast de gegevens die zijn opgesomd voor cliënten die geen laag risico vormen[45] (dat wil zeggen, voor een natuurlijke persoon: "*zijn naam, voornaam, geboortedatum en -plaats en, in de mate van het mogelijke, zijn adres*"[46]), bepaalt de wet niet welke "*bijkomende informatie*" in het kader van een hoog risico zou moeten worden verzameld[47, 48].

---

wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie, waarin het volgende is bepaald:

"*De cliëntenonderzoeksmaatregelen omvatten:*

a) de identificatie van de cliënt en de verificatie van zijn identiteit op basis van documenten, gegevens of informatie uit een betrouwbare en onafhankelijke bron, met inbegrip van, voor zover beschikbaar, elektronische identificatiemiddelen, relevante vertrouwensdiensten zoals vastgesteld in Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad (1) of ieder ander identificatieproces dat veilig is, op afstand of langs elektronische weg plaatsvindt en door de relevante nationale autoriteiten is gereglementeerd, erkend, goedgekeurd of aanvaard."

Zie ook meer recentelijk artikel 22, 6., van **Verordening (EU) 2024/1624** van het Europees Parlement en de Raad van 31 mei 2024 *tot voorkoming van het gebruik van het financiële stelsel voor witwassen of terrorismefinanciering* (van toepassing vanaf 10 juli **2027**), waarin is bepaald dat de informatie, documenten en gegevens die vereist zijn voor de verificatie van de identiteit van de cliënt moeten worden verkregen via:

"*a) een ingediend identiteitsdocument, paspoort of gelijkwaardig document, en, in voorkomend geval, informatie uit betrouwbare en onafhankelijke bronnen, ongeacht of de toegang daartoe rechtstreeks is of door de cliënt wordt verstrekt;*

b) het gebruik van elektronische identificatiemiddelen die voldoen aan de vereisten van Verordening (EU) nr. 910/2014 met betrekking tot de betrouwbaarheidsniveaus "substantieel" of "hoog" en relevante gekwalificeerde vertrouwensdiensten als bedoeld in die verordening".

Deze bepaling moet worden gelezen in samenhang met artikel 28, 1., d), en e), van dezelfde verordening, aangezien de toekomstige Autoriteit voor de bestrijding van witwassen en terrorismefinanciering (AMLA) hierover een technische norm moet vaststellen.

Er zij op gewezen dat de verordening voorziet in termijnen (uiterlijk één jaar bij een hoog risico, of vijf jaar) en gevallen waarin de gegevens moeten worden bijgewerkt (termijnen die kunnen worden verlengd wanneer het risiconiveau laag is, zie artikel 33 van de verordening).

In het geval van verscherpte zorgvuldigheidsmaatregelen (hoger risico) voorziet de verordening ook in de mogelijkheid om aanvullende informatie over de cliënt te verzamelen (zie artikel 34 van de verordening).

[43] Zie artikel 26 van de AML-wet.

[44] Zie artikel 27, § 1, eerste lid, 2°, van de AML-wet.

[45] Wat betreft lage risico's, zie artikel 26, § 3, van de AML-wet. De Autoriteit merkt in dit verband op dat de onderworpen entiteit in dit geval niet alleen de ingewonnen informatie "mag" beperken, maar dit ook moet doen, in voorkomend geval, ter uitvoering van het beginsel van minimale gegevensverwerking zoals neergelegd in artikel 5, 1., c), van de AVG.

[46] Artikel 26, § 2, 1°, van de AML-wet.

[47] Artikel 26, § 4, van de AML-wet bepaalt het volgende:

"*Wanneer uit de individuele risicobeoordeling uitgevoerd overeenkomstig artikel 19, § 2, eerste lid, blijkt dat het risico verbonden aan de cliënt en de zakelijke relatie of aan de verrichting hoog is, moet de onderworpen entiteit zich er met verhoogde aandacht van vergewissen dat de op grond van paragraaf 2 ingewonnen informatie haar in staat stelt om de betrokken persoon op onbetwistbare wijze te onderscheiden van elke andere persoon. Indien nodig wint ze daartoe bijkomende informatie in.*"

[48] **Verordening (EU) 2024/1624** van het Europees Parlement en de Raad van 31 mei 2024 *tot voorkoming van het gebruik van het financiële stelsel voor witwassen of terrorismefinanciering* (van toepassing vanaf 10 juli 2027) voorziet in artikel 22, 1., a), met het oog op de identificatie van natuurlijke personen, in de verzameling van alle voor- en achternamen; de geboorteplaats en de volledige geboortedatum; de nationaliteiten, de staatloosheid of de vluchtelingenstatus of de subsidiairebeschermingsstatus, in voorkomend geval, en het nationale identificatienummer, in voorkomend geval; de normale verblijfplaats of, bij gebrek aan een vast woonadres met rechtmatig verblijf in de Unie, het postadres waar de natuurlijke persoon kan worden bereikt en, indien beschikbaar, het fiscaal identificatienummer.

48. Ten tweede, dit gezegd zijnde, bepaalt het positief recht reeds, en terecht, dat **informatie die door de onderworpen entiteit wordt verzameld** via, in wezen, erkende **elektronische identificatiemiddelen** (maar ook vertrouwensdiensten), **verder mag worden verwerkt** voor identificatiedoeleinden in het kader van de AML-wet[49]. In dit verband wijst de Autoriteit de aanvrager erop dat, indien het voorstel voorziet in een **aanvankelijke en bijkomende verzameling van gegevens** – **dus verdergaand dan de verplichte identificatiegegevens zoals vereist op grond van de eIDAS-verordening** (naam of namen, voornaam of voornamen, geboortedatum, nationaal identificatienummer)**[50]** – **met het oog op de uitvoering van de identificatieverplichtingen zoals neergelegd in de relevante artikelen van de AML-wet**, het **dispositief van het voorstel dit doeleinde uitdrukkelijk** moet **vermelden en het onderscheid moet maken tussen deze nieuwe dienst** die de dienstverlener van elektronische identificatiemiddelen kan verlenen, en de dienst voor elektronische identificatie zoals bedoeld in de eIDAS-verordening. Het voorstel zou in een dergelijk scenario immers een bijkomende aanvankelijke verzameling van gegevens toestaan die niet noodzakelijk is voor de uitvoering van de elektronische identificatie krachtens de eIDAS-verordening.

49. In dit opzicht is de Autoriteit echter van oordeel dat de aanvrager **de voorkeur zou kunnen geven aan het gebruik van de Europese portemonnees voor digitale identiteit en de gekwalificeerde elektronische attesteringen van attributen** zoals bedoeld in de eIDAS2-verordening[51], aangezien het hier gaat om nieuwe diensten die zullen vallen onder **volwaardige en geharmoniseerde Europese en Belgische normatieve en technische kaders, met specifieke waarborgen[52]**. Opnieuw gaat het om een belangrijke overweging **die in aanmerking moet worden genomen in het kader van de uitvoering van een effectbeoordeling[53]**.

50. Ten derde merkt de Autoriteit op dat het positief recht **ook reeds bepaalt dat de onderworpen entiteiten toegang kunnen krijgen tot het RR** via de door de Koning aangeduide beroepsorganisaties, zowel met het oog op de identificatie van de personen die niet fysiek aanwezig zijn bij hun identificatie, als voor de bijwerking van de identificatiegegevens van de cliënten[54]. **Het is dan ook aan de aanvrager om aan te tonen dat het noodzakelijk is om een bijkomende toegang tot het RR te voorzien via een andere tussenpersoon (de dienst voor elektronische**

[49] Zie artikel 27, § 1, 2° en 3°, van de AML-wet.

[50] Zie overweging nr. 28.

[51] Zie voetnoot nr. 22.

[52] Zie overweging nr. 51, eerste streepje.

[53] Zie overweging nr. 27.

[54] Zie artikel 28 van de AML-wet.

identificatie)[55]. Deze verantwoording is van groot belang in het kader van de uitvoering van een effectbeoordeling[56].

51. Ten vierde, en zonder afbreuk te doen aan de voorgaande opmerkingen, voorzien de bepalingen van de AML-wet in **verplichtingen** inzake de identificatie van cliënten. Met andere woorden, de verwerking van persoonsgegevens in deze context is **gebaseerd op een wettelijke verplichting**[57] **en niet op de toestemming van de betrokkene**. Het gaat dus om een heel andere situatie (in feite en in rechte) dan die waarop artikel 5*ter* van de RR-wet betrekking heeft, **die een specifiek normatief kader vereist**, waarbij de **rol die wordt toegekend aan de toestemming (controle)** van de betrokkene **specifiek moet worden geregeld door het dispositief van het voorstel**. In het onderhavige geval, en in overeenstemming met de in het voorstel en door de aanvrager aangekondigde bedoelingen, is de Autoriteit van oordeel dat het dispositief van het voorstel, **onverminderd de verplichtingen van de AVG**[58]:

- moet bepalen dat **waarborgen die vergelijkbaar zijn met die welke zijn neergelegd in de eIDAS-verordening inzake transparantie en controle door de betrokkene bij Europese portemonnees voor digitale identiteit**, van toepassing zijn op de dienst die het voorstel invoert. Het gaat er in het bijzonder om regels toe te passen die vergelijkbaar zijn (met de nodige aanpassingen, *mutatis mutandis*) met die van artikel 5*bis*, 4., a)[59] en d)[60],

[55] Dit is onder meer een belangrijk element waarmee rekening moet worden gehouden in het kader van de effectbeoordeling van het ontwerp, zie overweging nr. 27.

[56] Zie overweging nr. 27.

[57] Artikel 6, 1., c), van de AVG.

[58] Deze punten zijn ook relevant in het kader van de uitvoering van een effectbeoordeling, zie overweging nr. 27.

[59] "*4. Met een Europese portemonnee voor digitale identiteit kunnen gebruikers op […] gebruiksvriendelijke, transparante en voor hen traceerbare wijze:*

a) veilig, met volledige controle door de gebruiker, persoonsidentificatiegegevens aanvragen, verkrijgen, selecteren, combineren, opslaan, verwijderen, delen en aanbieden, en, indien van toepassing, in combinatie met elektronische attesteringen van attributen, zich online en, indien passend, in offlinemodus authenticeren bij vertrouwende partijen, om toegang te krijgen tot publieke en private diensten, waarbij ervoor wordt gezorgd dat een selectieve verstrekking van gegevens mogelijk is;"

[60] "*4. Met een Europese portemonnee voor digitale identiteit kunnen gebruikers op […] gebruiksvriendelijke, transparante en voor hen traceerbare wijze:*

d) toegang krijgen tot een log van alle transacties die met de Europese portemonnee voor digitale identiteit worden uitgevoerd via een gemeenschappelijk dashboard waarmee de gebruiker:

i) een actuele lijst van vertrouwende partijen waarmee de gebruiker een verbinding tot stand heeft gebracht en, indien van toepassing, alle uitgewisselde gegevens kan bekijken;

ii) gemakkelijk kan verzoeken om het wissen door een vertrouwende partij van persoonsgegevens overeenkomstig artikel 17 van Verordening (EU) 2016/679;

iii) gemakkelijk aan de bevoegde nationale gegevensbeschermingsautoriteit een vertrouwende partij kan aangeven, wanneer een vermeend onrechtmatig of verdacht verzoek om gegevens is ontvangen;"

5., a), iv), ix), x), b), d), e)[61], 10.[62], 14. (zonder evenwel een tegengesteld verzoek van de gebruiker toe te staan, aangezien dit vreemd is aan de doelstellingen van het voorstel)[63], 15.[64], 16., a) (zonder mogelijkheid tot uitdrukkelijke toestemming, aangezien deze niet onder het voorstel valt)[65], van de eIDAS-verordening;

- moet overwegen om in het licht van **artikel 5*ter*, § 3, tweede lid, van de RR-wet** toe te staan dat de betrokkene **actie** kan **ondernemen bij de bron van de gegevens, namelijk <u>bij het RR</u>** zelf;

- moet bepalen dat de **artikelen 4, 11), en 7, van de AVG van toepassing zijn op de verschillende keuzes van de betrokkenen in het kader van**: de uitvoering van de **aanvankelijke verzameling** van de nodige gegevens door de dienstverlener van

---

[61] "*5. Europese portemonnees voor digitale identiteit moeten in het bijzonder:*

a) gemeenschappelijke protocollen en interfaces ondersteunen:

[…]

iv) opdat de gebruiker met de Europese portemonnee voor digitale identiteit kan communiceren en om een EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit te kunnen weergeven;

[…]

x) om het aan de bevoegde nationale gegevensbeschermingsautoriteit te melden wanneer van een vertrouwende partij een vermeend onrechtmatig of verdacht verzoek om gegevens is ontvangen;

[…]

b) verleners van vertrouwensdiensten van elektronische attesteringen van attributen geen informatie verstrekken over het gebruik van die elektronische attesteringen;

[…]

d) aan de voorwaarden van artikel 8 voldoen wat het betrouwbaarheidsniveau „hoog" betreft, met name betreffende de vereisten voor het bewijzen en verifiëren van identiteit, en het beheer en de authenticatie van elektronische identificatiemiddelen;

e) bij elektronische attestering van attributen met een ingebed openbaarmakingsbeleid, het passende mechanisme toepassen om de gebruiker ervan in kennis te stellen dat de vertrouwende partij of de gebruiker van de Europese portemonnee voor digitale identiteit die om die elektronische attestering van attributen verzoekt tot die attestering toegang heeft;"

[62] "*10. Aanbieders van Europese portemonnees voor digitale identiteit zorgen ervoor dat gebruikers gemakkelijk om technische ondersteuning kunnen verzoeken en technische problemen of andere incidenten die negatieve gevolgen hebben voor het gebruik van Europese portemonnees voor digitale identiteit kunnen melden.*"

[63] "*14. Gebruikers hebben volledige controle over het gebruik van en de gegevens in hun Europese portemonnee voor digitale identiteit. De aanbieder van de Europese portemonnee voor digitale identiteit verzamelt geen informatie over het gebruik van de Europese portemonnee voor digitale identiteit die niet noodzakelijk is voor de verlening van de diensten in verband met Europese portemonnees voor digitale identiteit, noch combineert hij of zij persoonsidentificatiegegevens of enige andere persoonsgegevens die zijn opgeslagen of betrekking hebben op het gebruik van de Europese portemonnee voor digitale identiteit met persoonsgegevens van andere door die aanbieder of derden aangeboden diensten als die niet noodzakelijk zijn voor de verlening van de diensten in verband met Europese portemonnees voor digitale identiteit, tenzij de gebruiker uitdrukkelijk anders heeft gevraagd. Persoonsgegevens met betrekking tot de verstrekking van de Europese portemonnee voor digitale identiteit worden logisch gescheiden van andere door de aanbieder van de Europese portemonnee voor digitale identiteit opgeslagen gegevens. Indien de Europese portemonnee voor digitale identiteit wordt verstrekt door private partijen overeenkomstig lid 2, punten b) en c), is artikel 45 nonies, lid 3, van overeenkomstige toepassing.*"

[64] "*15. Het gebruik van Europese portemonnees voor digitale identiteit is vrijwillig. De toegang tot publieke en private diensten, de arbeidsmarkt en vrij ondernemerschap van natuurlijke of rechtspersonen die de Europese portemonnees voor digitale identiteit niet gebruiken, wordt niet beperkt of belemmerd. Het blijft mogelijk om via andere bestaande identificatie- en authenticatiemiddelen toegang te krijgen tot publieke en private diensten.*"

[65] "*16. Het technische kader van de Europese portemonnee voor digitale identiteit:*

a) mag het aanbieders van elektronische attesteringen van attributen of andere partijen na de afgifte van de attestering van attributen, niet mogelijk maken gegevens te verkrijgen waarmee kan worden gevolgd, gekoppeld of gecorreleerd of waarmee kennis van transacties of gebruikersgedrag anderszins kan worden verkregen, tenzij de gebruiker daar uitdrukkelijk toestemming voor heeft gegeven;"

elektronische identificatiemiddelen, volgens het identificatieniveau dat vereist is voor de AML-doelstelling *in concreto* (laag, normaal of hoog risico), ongeacht de bron van deze aanvankelijke verzameling (de identiteitskaart of het RR[66]); de **mededeling** van de nodige gegevens aan de onderworpen entiteit, volgens het identificatieniveau dat vereist is voor de AML-doelstelling *in concreto* (laag, normaal of hoog risico); de **bijwerking** van de nodige gegevens door de dienstverlener van elektronische identificatiemiddelen, volgens het identificatieniveau dat vereist is voor de AML-doelstelling *in concreto* (laag, normaal of hoog risico); de **mededeling van de nodige bijgewerkte gegevens** aan de onderworpen entiteit, volgens het identificatieniveau dat vereist is voor de AML-doelstelling *in concreto* (laag, normaal of hoog risico).

52. Ten vijfde **moet het dispositief van het voorstel zodanig worden aangepast dat het alleen betrekking heeft op gegevens** uit het RR, het Register van de Identiteitskaarten en het Register van de Vreemdelingenkaarten **die nodig zijn voor de uitvoering van de identificatieverplichtingen zoals bedoeld in de AML-wet, volgens van het risiconiveau*, in concreto***. De Autoriteit ziet ***bijvoorbeeld*** niet in waarom, in deze context, de foto (en zelfs foto's, aangezien het Register van de Identiteitskaarten ook oude foto's bevat) van de houder van de identiteitskaart zou(den) moeten worden meegedeeld aan de onderworpen entiteiten. Een dergelijk gegeven lijkt *a priori* en van meet af aan onevenredig.

53. Ten zesde **ziet** de Autoriteit **geen reden om af te wijken van de logica die is vastgelegd in de artikelen 5 en 5*ter* van de RR-wet**, waarin wordt bepaald dat **de minister van Binnenlandse Zaken een machtiging moet verlenen aan elke instantie** (de onderworpen entiteiten) **die betrokken is** bij de gegevensstroom, om toegang te krijgen tot de betrokken gegevens. Het feit dat de betrokken dienstverlener van elektronische identificatiemiddelen zelf over een machtiging moet beschikken, is in dit verband niet doorslaggevend. Ter herinnering: deze voorwaarde geldt ook voor overheidsinstanties die in het kader van hun taken van algemeen belang toegang willen krijgen tot het RR, het Register van de Identiteitskaarten of het Register van de Vreemdelingenkaarten. Deze voorwaarde is met name belangrijk vanuit het oogpunt van de verantwoordelijkheid die op het RR rust als verwerkingsverantwoordelijke[67].

54. Ten zevende **moet artikel 5*quater*, § 3**, van de RR-wet zoals voorgesteld, geïnspireerd op artikel 5*ter*, § 3, van de RR-wet, **worden aangevuld**, aangezien het enkel betrekking heeft op de situatie waarin de contractuele relatie tussen de betrokkene en de dienstverlener van *elektronische*

[66] Een reeks gegevens waarop het voorstel betrekking heeft, wordt niet opgenomen op de elektronische identiteitskaart.

[67] Zie in dit verband bijvoorbeeld advies nr. 34/2024 van 15 april 2024 *betreffende een wetsvoorstel tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten (CO-A-2024-139)*, overwegingen nrs. 16 en 17.

identificatiemiddelen wordt stopgezet. **Het dispositief van het voorstel moet echter ook voorzien in de stopzetting van de contractuele relatie tussen de betrokkene en de entiteit die** via de dienstverlener van elektronische identificatiemiddelen **gegevens en updates ontvangt**. In de logica van het voorstel en van het huidige artikel 5*ter* van de RR-wet betekent dit dat de onderworpen entiteit verplicht is om de stopzetting van de contractuele relatie aan de dienstverlener van elektronische identificatiemiddelen te melden, en dat deze daaruit de consequenties op het vlak van gegevensbescherming trekt[68].

55. Ten achtste wijst de Autoriteit de aanvrager op de **noodzaak voor de onderworpen entiteit om het referentierepertorium dat zou worden gebruikt** voor de automatische bijwerking van gegevens, **realtime aan te passen** op basis van de keuzes die de betrokkene maakt[69]. Indien de betrokkene aanvankelijk een laag risico vertoont, bestaat er immers geen legitieme reden om van meet af aan gegevens te verzamelen (en in voorkomend geval updates te ontvangen) die pas in de toekomst nodig ***zouden kunnen*** zijn, mocht het risiconiveau van de betrokkene evolueren. Omgekeerd geldt dat wanneer het risiconiveau van een betrokkene daalt, de consequenties daarvan op het vlak van gegevensbescherming rechtstreeks moeten worden getrokken[70].

56. Ten negende merkt de Autoriteit op dat het voorstel niet voorziet in de toepassing van **artikel 5*ter*, § 5, eerste lid, van de RR-wet**, dat bepaalt dat de Koning een **tarief** vaststelt ten gunste van de bevoegde dienst van het RR[71]. Nochtans is het essentieel om **de (financiële) impact van het ontwerp voor het RR** te evalueren, gelet op de uitbreiding van zijn opdrachten, **om te waarborgen dat het RR**, als verwerkingsverantwoordelijke, **materieel in staat is om de verplichtingen na te komen die op hem rusten krachtens de AVG**, in het bijzonder met betrekking tot **de *verantwoordingsplicht*[72]**.

57. Ten tiende herinnert de Autoriteit tot slot aan haar vaste adviespraktijk volgens welke een overheidsinstantie (of een private entiteit) in principe **verantwoordelijk** is **voor de verwerking** van gegevens die noodzakelijk is voor de vervulling van de taak van algemeen belang die haar is opgedragen (of die binnen de reikwijdte valt van het openbaar gezag dat haar is verleend)[73] of die

[68] Dit houdt in ieder geval in dat de mededeling van gegevens aan de onderworpen entiteit wordt stopgezet en dat, indien dezelfde gegevens niet voor andere doeleinden door de dienstverlener van elektronische identificatiemiddelen worden verwerkt, deze gegevens worden gewist en het referentierepertorium wordt aangepast.

[69] Hoewel het hier niet gaat om een analyse van artikel 5*ter* van de RR-wet, is deze opmerking ook hier relevant. In een situatie waarin bijvoorbeeld een defect product moet worden teruggeroepen of waarin een geschil ontstaat, is een bijgewerkt adres nodig op het moment dat deze gebeurtenissen zich voordoen.

[70] Zie voetnoot nr. 68.

[71] Dit punt moet ook worden gelezen in samenhang met overweging nr. 53 (betreffende de machtigingen van de minister van Binnenlandse Zaken).

[72] Artikelen 5, 2., en 24 van de AVG. Dit is onder andere nog een belangrijk element dat in aanmerking moet worden genomen in het kader van de effectbeoordeling van het ontwerp, zie overweging nr. 27.

[73] Artikel 6, 1., e), van de AVG.

noodzakelijk is om te voldoen aan de wettelijke verplichting die op haar rust[74], krachtens de betrokken norm[75, 76]. De Autoriteit is van oordeel dat het voorstel, wat betreft de geautomatiseerde verzameling en bijwerking van de betrokken gegevens, **een gezamenlijke actie** inhoudt **van de drie categorieën van actoren waarop het betrekking heeft, ten dienste van de AML-doelstelling**, zodanig dat zij als gezamenlijke verwerkingsverantwoordelijken zullen optreden.

D) eIDAS-doelstelling (gegevensstroom naar de dienstverlener van elektronische identificatiemiddelen)

58. Wat betreft de doelstelling van de **uitvoering van de eIDAS-verordening** met betrekking tot **de gegevensstroom** van het RR, het Register van de Identiteitskaarten en het Register van de Vreemdelingenkaarten **naar de dienstverleners van elektronische identificatiemiddelen**, is de Autoriteit van oordeel dat **in de memorie van toelichting van het voorstel** eerst en vooral **duidelijk moet worden aangegeven welk probleem men beoogt op te lossen**. Dit probleem moet in aanmerking worden genomen als uitgangspunt in het kader van een effectbeoordeling[77]. Er moet immers worden vastgesteld dat België op dit moment **volgens het positief recht**, ook zonder de nieuwe regels van het voorstel, reeds beschikt over twee stelsels voor identificatie met een **hoog betrouwbaarheidsniveau[78]**.

---

[74] Artikel 6, 1., c), van de AVG.

[75] Zie met name: advies nr. 143/2023 van 29 september 2023 *betreffende een voorontwerp van decreet tot instemming met het samenwerkingsakkoord tussen het Waals Gewest en de Franse Gemeenschap tot aanwijzing van de dienstintegrator van het Waals Gewest en de Franse Gemeenschap en een ontwerp van samenwerkingsakkoord met betrekking tot de oprichting van de gemeenschappelijke dienst van de Waalse Regeringen en de Franse Gemeenschap, genaamd "Banque Carrefour d'échange de données" (niet onderworpen aan instemming) (CO-A-2023-375), en betreffende een voorontwerp van decreet houdende instemming met het samenwerkingsakkoord tussen het Waals Gewest en de Franse Gemeenschap tot aanwijzing van de dienstintegrator van het Waals Gewest en de Franse Gemeenschap en een ontwerp van samenwerkingsakkoord met betrekking tot de oprichting van de gemeenschappelijke dienst van de Waalse Regeringen en de Franse Gemeenschap, genaamd "Banque Carrefour d'échange de données" (niet onderworpen aan instemming) (CO-A-2023-376)*, overwegingen nrs. 7 e.v.; advies nr. 83/2023 van de Autoriteit van 27 april 2023 *over een Voorontwerp van ordonnantie tot wijziging van de ordonnantie van 4 april 2019 betreffende het elektronisch uitwisselingsplatform voor gezondheidsgegevens (CO-A-2023-147)*, overweging nr. 11; 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*, overwegingen nrs. 42 e.v.; advies nr. 227/2022 van 29 september 2022 *betreffende een voorontwerp van decreet over open data en het hergebruik van overheidsinformatie (CO-A-2022-209)*, overwegingen nrs. 17-23; advies nr. 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 nrs. 55 e.v.; 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 *over een voorontwerp van decreet tot oprichting van het gecentraliseerde platform voor geautomatiseerde gegevensuitwisseling "E-Paysage"*, 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.

[76] Advies nr. 154/2023 van 20 oktober 2023 *over een Gezamenlijk decreet en ordonnantie houdende het Wetboek voor governance en gegevensbeheer en de aanduiding van de cartografische databank URBIS (CO-A-2023-407)*, overweging nr. 167.

[77] Zie overweging nr. 27.

[78] Zie overweging nr. 28.

59. De Autoriteit ziet niet in welk probleem het voorstel beoogt op te lossen, bijvoorbeeld wat betreft de **verificatie van de geldigheid** van de identiteitskaart[79]. Bij verlies, diefstal of vernietiging van de identiteitskaart **worden de certificaten** immers **herroepen, en deze status kan (en moet) altijd worden geverifieerd** (bijvoorbeeld via een *OCSP client* – "*Online Certificate Status Protocol*")[80,81]. Bovendien hebben de certificaten een geldigheidsdatum die overeenkomt met de geldigheidsdatum van de identiteitskaart zelf.

60. Wat betreft de **bijwerking van de gegevens** afkomstig van de identiteitskaart, **met betrekking tot de gegevens *die nodig zijn voor de identificatie in het kader van een dienst voor elektronische identificatie zoals bedoeld in de eIDAS-verordening*** (want voor bijkomende gegevens verandert het doeleinde van de verwerking[82]), worden de bovengenoemde stelsels voor identificatie in het positief recht geacht een hoog betrouwbaarheidsniveau te bieden, zodanig dat het theoretisch moeilijk voorstelbaar is dat zij geen actuele identificatiegegevens verstrekken. Een naamswijziging of overlijden leidt bijvoorbeeld tot de **annulering van de identiteitskaart, wat inhoudt dat deze wordt vernietigd en de elektronische functies worden ingetrokken**[83].

---

[79] Zie overweging nr. 15.

[80] Zie met name FOD Binnenlandse Zaken, AD Identiteit en Burgerzaken, Bevolking en Identiteitskaarten, "Algemene onderrichtingen betreffende de elektronische identiteitskaarten van Belg", bijgewerkt op 5 juli 2023, beschikbaar op

https://www.ibz.rrn.fgov.be/sites/default/files/documents/nl/identiteitsdocumenten/eid/onderrichtingen/AO-eID-NL-05072023.pdf, laatst geraadpleegd op 05/02/2025. Zie ook artikel 6 van het koninklijk besluit van 26 maart 2003 *betreffende de identiteitskaarten* (nog niet van kracht volgens de geconsolideerde wetgeving beschikbaar via de FOD Justitie; zie hierover artikel 12 van het koninklijk besluit van 10 december 2019 *tot wijziging van het koninklijk besluit van 25 maart 2003 betreffende de identiteitskaarten en het koninklijk besluit van 19 april 2014 aangaande de identiteitskaarten afgegeven door de consulaire beroepsposten; de minister van Binnenlandse Zaken is bevoegd om de inwerkingtreding van deze bepaling te bepalen*). Zie ook certipost, "Belgisch Certificaatbeleid & Verklaring met betrekking tot de Praktijk voor eID PKI-infrastructuur Citizen CA", v. 5.0, 03/09/2024, beschikbaar op

https://repository.eid.belgium.be/downloads/citizen/nl/CPS_CitizenCA_BRCA34.pdf, laatst geraadpleegd op 10/02/2025, pp. 31-34.

[81] **Wat betreft de certificaten**, zie https://repository.eid.belgium.be/index.php?lang=nl;

https://repository.eid.belgium.be/index.php?item=status&lang=nl; https://stage-pki.belgium.be/; laatst geraadpleegd op 05/02/2025. Certificatieautoriteiten (**certipost**, zowel "Citizen CA" als "Belgium Root CA") die actief zijn in een systeem van *public key infrastructure* zoals dat van de eID, leveren met name de diensten die nodig zijn om de geldigheid van de uitgegeven certificaten te verifiëren. Bovendien, in de context van "Citizen CA", "[*moeten*] *vertrouwende partijen* [...], *om de status van certificaten te controleren, gebruikmaken van online hulpmiddelen die de CA ter beschikking stelt via het archief, alvorens deze certificaten te vertrouwen. De CA werkt de OCSP, de webinterface voor verificatie van de certificaatstatus, de CRL's en de Delta-CRL's dienovereenkomstig bij. CRL's worden regelmatig bijgewerkt, met een minimuminterval van drie uur.*", certipost, "Belgisch Certificaatbeleid & Verklaring met betrekking tot de Praktijk voor eID PKI-infrastructuur Citizen CA", v. 5.0, 03/09/2024, beschikbaar op

https://repository.eid.belgium.be/downloads/citizen/nl/CPS_CitizenCA_BRCA34.pdf, laatst geraadpleegd op 10/02/2025, p. 32.

Het **RR** en de gemeenten spelen zelf ook rechtstreeks een rol in het kader van deze PKI (in het kader van "**Citizen CA**") als registratieautoriteiten en lokale registratieautoriteiten. Zij zijn met name verantwoordelijk voor de geldigheidsverklaring van de identiteit van de burgers, de registratie van de gegevens die gecertificeerd moeten worden, en de Autoriteit voor de Schorsing en de Herroeping, oftewel de entiteit die de certificaten schorst en/of herroept. Zie certipost, "Belgisch Certificaatbeleid & Verklaring met betrekking tot de Praktijk voor eID PKI-infrastructuur Citizen CA", v. 5.0, 03/09/2024, beschikbaar op

https://repository.eid.belgium.be/downloads/citizen/nl/CPS_CitizenCA_BRCA34.pdf, laatst geraadpleegd op 10/02/2025, p. 16. Wat betreft "Belgium Root CA", zie FOD Beleid en Ondersteuning, DG Digitale Transformatie, "Belgian Certificate Policy & Practice Statement for eID PKI Infrastructure Belgium Root CA", v3.0.5, beschikbaar op https://stage-pki.belgium.be/resources/BRCA%20CPS%20V3.05.pdf, laatst geraadpleegd op 10/02/2025.

[82] Zie *mutatis mutandis*, overwegingen nrs. 47, 48. Voor de betrokken gegevens, zie overweging nr. 28.

[83] Zie de "Algemene onderrichtingen betreffende de elektronische identiteitskaarten van Belg", aangehaald in voetnoot nr. 80, pp. 76-77. Afgezien van de loutere hypothese van identificatie, wanneer er ook sprake is van elektronische handtekeningen, wordt het gekwalificeerd handtekeningcertificaat niet geactiveerd op de identiteitskaart van minderjarige personen, en wanneer

Zoals zojuist is opgemerkt, is de informatie over ingetrokken certificaten beschikbaar en moet deze worden geverifieerd.

61. De Autoriteit merkt overigens op dat, indien het betrouwbaarheidsniveau van de identificatie in het gedrang zou komen door het ontbreken van alle of een deel van de in het voorstel voorziene gegevensstromen – wat, gelet op het bovenstaande, *a priori* echter niet het geval lijkt te zijn –, men zich kan afvragen of het doeltreffend is om de oplossing van dit probleem volledig te laten afhangen van de toestemming van de betrokkenen.

62. Voor wat **verder** gaat **dan de identificatiegegevens van de betrokkene in het kader van de eIDAS-verordening**, verwijst de Autoriteit *mutatis mutandis* naar de voorgaande uiteenzettingen die betrekking hebben op de gegevensstroom naar de dienstverlener van elektronische identificatiemiddelen.

E) Andere specifieke doeleinden

63. Indien het voorstel andere specifieke doeleinden beoogt, namelijk andere diensten voor gegevensuitwisseling die zouden kunnen worden uitgevoerd door dienstverleners van elektronische identificatiemiddelen zoals bedoeld in de eIDAS-verordening, zou enerzijds moeten worden nagedacht over het beoogde doeleinde, zoals de Autoriteit dat heeft gedaan met betrekking tot de AML-doelstelling, en zouden anderzijds het dispositief en de memorie van toelichting van het ontwerp *mutatis mutandis* moeten worden aangepast (**overwegingen nrs. 46-57**). De Autoriteit schort haar analyse hierover op.

II.3. Conclusie – redenen

OM DEZE REDENEN,
is de Autoriteit de volgende mening toegedaan:

1. Hoewel de bedoeling van het amendement lovenswaardig is aangezien deze zou kunnen passen binnen het streven om de eIDAS2-verordening in Belgisch recht om te zetten, lijkt het niettemin voorbarig om op dit moment een bijzonder wettelijk gevolg toe te kennen aan "*de officiële 'Belgische digitale portefeuille' applicatie*". Enerzijds wordt deze applicatie niet gedefinieerd in het dispositief van het amendement, anderzijds kan zij wettelijk nog niet bestaan als portemonnee voor digitale identiteit in de zin van de eIDAS2-verordening, aangezien het daarin neergelegd normatief en technisch kader nog niet volledig

de vrederechter jegens een persoon de handtekeningsonbekwaamheid of de onbekwaamheid om zich met behulp van de elektronische identiteitskaart te authenticeren, beslist, worden de gekwalificeerde handtekenings- of authenticeringscertificaten op de identiteitskaart ingetrokken (zie artikel 6, § 7, derde en vierde lid, van de wet van 1991).

geïmplementeerd en van toepassing is (**overwegingen nrs. 5-**Error! Reference source not found.);

2. Het voorstel moet verduidelijken welke dienstverleners erkend zijn "*door een overheidsdienst die door of krachtens een wet, een decreet of een ordonnantie de opdracht heeft om een dienst voor gebruikers- en toegangsbeheer aan te bieden*", alsook welke overheidsdiensten daarbij eventueel betrokken zijn en welk normatief kader van toepassing is. Zo niet, dient de verwijzing ernaar te worden weggelaten. De Autoriteit spreekt zich hierover niet uit (**overwegingen nrs. 19-**Error! Reference source not found.);

3. Het wordt aanbevolen om een effectbeoordeling uit te voeren met betrekking tot het ontwerp (**overwegingen nrs. 22-28**), waarbij in het bijzonder rekening wordt gehouden met de in dit advies opgeworpen vragen (overwegingen nrs. 43 en 49, noodzaak van het voorstel in het licht van de eIDAS2-verordening; overweging nr. 50, bijkomende toegang tot het RR; overweging nr. 51, keuze van de betrokkene en transparantie; overweging nr. 52, betrokken gegevens; overweging nr. 53, machtigingen van de minister van Binnenlandse Zaken; overweging nr. 54, stopzetting van de contractuele relatie; overweging nr. 56, financiële impact voor het RR; overweging nr. 58, probleem dat moet worden opgelost in het kader van de eIDAS-doelstelling), volgens de doelstellingen van het voorstel (overweging nr. 63);

4. Opdat de door de aanvrager bedoelde erkenning daadwerkelijk de waarborg kan bieden die zij krachtens het voorstel en de motivering ervan geacht wordt te bieden, moet worden nagegaan of en in welke mate deze in het kader van het voorstel kan en moet worden opgelegd, en moet het KB van 2017 worden aangepast aangezien het niet is opgesteld met het voorstel in gedachten (**overwegingen nrs. 33-34**);

5. Het dispositief van het voorstel moet de welbepaalde en specifieke doeleinden die het nastreeft in het kader van de nieuwe gegevensuitwisselingen die het mogelijk maakt, expliciteren en onderscheiden van de dienst voor identificatie zoals bedoeld in de eIDAS-verordening, en de verdere verwerking van de verzamelde gegevens beperken zoals artikel 5*ter* van de RR-wet (**overwegingen nrs. 39-45**);

6. Indien de aanvrager voornemens is de AML-doelstelling in het voorstel te behouden, terwijl enerzijds de onderworpen entiteiten reeds toegang hebben tot het RR en anderzijds de Europese portemonnees voor digitale identiteit en de elektronische attesteringen van attributen het nagestreefde doeleinde kunnen bereiken (**overweging nr. 49**), moet het worden aangepast om: een onderscheid te maken tussen de nieuwe dienst en de dienst voor

elektronische identificatie zoals bedoeld in de eIDAS-verordening (**overweging nr. 48**); de noodzaak van een bijkomende toegang tot het RR aan te tonen (**overweging nr. 50**); de rol van de toestemming te verduidelijken en bijkomende specifieke waarborgen te bieden, in het licht van de eIDAS2-verordening en artikel 5*ter* van de RR-wet, met betrekking tot de controle waarover de betrokkene beschikt en met betrekking tot de transparantie (**overweging nr. 51**); de betrokken gegevens te beperken (**overweging nr. 52**); ook voor de onderworpen entiteiten de vereiste te voorzien om een machtiging van de minister van Binnenlandse Zaken te verkrijgen (**overweging nr. 53**); ook rekening te houden met de stopzetting van de contractuele relatie met de onderworpen entiteit, en de consequenties hiervan in het kader van het ontwerp vast te leggen (**overweging nr. 54**); te evalueren of een vergoeding van het RR noodzakelijk is om te waarborgen dat het materieel in staat is om zijn verplichtingen als verwerkingsverantwoordelijke na te komen (**overweging nr. 56**);

7. Wat de eIDAS-doelstelling betreft, moet in de memorie van toelichting duidelijk worden aangegeven welk probleem het voorstel beoogt op te lossen, aangezien de Autoriteit dit niet concreet kan vaststellen. Volgens het positief recht bieden de door België aangemelde diensten voor elektronische identificatie immers reeds een hoog betrouwbaarheidsniveau (**overwegingen nrs. 58-61**);

8. Indien het voorstel andere welbepaalde en specifieke doeleinden beoogt, dient hierover te worden nagedacht in het licht van **punt 6** hierboven, en dient het dispositief dienovereenkomstig te worden aangepast (**overweging nr. 63**).

Voor de Autorisatie- en Adviesdienst,
Cédrine Morlière, directeur

Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 14/2025 du 27 février 2025

Objet: Demande d'avis *concernant une proposition de loi relative au partage de données provenant de sources authentiques avec les prestataires de services d'identification électronique agréés (DOC56 0330/001) et un amendement y lié (DOC56 0330/002)* (CO-A-2025-003)

Mots-clés : identification et authentification électroniques ; registre national ; accès par le secteur privé ; prestataires de services d'identification électronique ; portefeuille européen d'identité numérique ; Règlement EIDAS.

Version originale

Introduction

La Proposition soumise pour avis modifie la loi du 8 août 1983 *organisant un registre national des personnes physiques* et la loi du 19 juillet 1991 *relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour* afin de permettre un accès plus large du secteur privé, dans le contexte des services d'identification électroniques, aux données disponibles dans le Registre National et dans les Registres des cartes d'identité et cartes d'étranger. Elle entend également permettre à l'application « *portefeuille numérique belge* » de valoir certificat d'inscription dans les registres de la population.

Concrètement, la Proposition permettrait la mise en place de nouveaux services d'échanges de données issues des sources authentiques précitées, via les prestataires de services d'identification électronique, sur la base du consentement de la personne concernée et ce, à des finalités spécifiques que son dispositif doit expliciter. Le présent avis détaille à quelles conditions (spécification de la finalité, garanties quant au contrôle de la personne concernée, etc.) elle pourrait y aboutir, en particulier s'agissant de la mise en œuvre des obligations d'identification des clients par les entreprises assujetties à la législation de prévention contre le blanchiment d'argent.

Pour les textes normatifs émanant de l'Autorité fédérale, de la Région de Bruxelles-Capitale et de la Commission communautaire commune, les avis sont en principe disponibles en français et en néerlandais sur le site Internet de l'Autorité. La « Version originale » est la version qui a été validée collégialement.

Toutefois d'une part, ces entités ont déjà accès au Registre National. Et, plus largement d'autre part, les portefeuilles européens d'identité numérique et les attestations d'attributs prévus par la récente réforme du Règlement EIDAS devraient permettre d'accomplir les objectifs poursuivis par la Proposition. De telle sorte que ceux-ci pourraient y être préférés, s'agissant d'un cadre normatif juridique, technique et harmonisé au niveau européen, certes pas encore complètement mis en œuvre et d'application. Ce cadre prévoit en outre des garanties spécifiques dont le contrôle total de l'utilisateur sur le portefeuille européen d'identité numérique et une transparence accrue.

Notamment et plus largement à l'aune des finalités spécifique qui seraient envisagées, l'Autorité recommande dans ce contexte, la réalisation d'une analyse d'impact.

L'Autorité considère par ailleurs qu'il est prématuré à ce stade, à défaut pour la réforme juste évoquée d'être pleinement d'application, de reconnaître dès maintenant, un effet légal au « *portefeuille numérique belge* ». L'Autorité n'en reste pas moins consciente de l'intérêt et de la nécessité de mettre en place un portefeuille européen d'identité numérique au niveau belge, conformément au Règlement EIDAS2, dans les délais impartis.

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent.e.s : Mesdames Cédrine Morlière et Griet Verhenneman et Messieurs Yves-Alexandre de Montjoye, Bart Preneel et Gert Vermeulen;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après « LCA »);

Vu l'article 43 du règlement d'ordre intérieur selon lequel les décisions du service d'autorisation et d'avis 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 la demande du Président de la Chambre des Représentants, Monsieur Peter De Roover (ci-après, « le demandeur »), reçue le 7 janvier 2025;

Vu la demande d'informations complémentaires adressée au demandeur le 24 janvier 2025;

Vu la réponse communiquée par le demandeur le 2 février 2025;

Émet, le 27 février 2025, l'avis suivant :

I. Objet et contexte de la demande d'avis

1. Le demandeur a introduit auprès de l'Autorité une demande d'avis concernant une proposition de loi *relative au partage de données provenant de sources authentiques avec les prestataires de services d'identification électronique agréés (DOC56 0330/001)* (ci-après, « **la Proposition** »), ainsi qu'un amendement y lié (DOC56 0330/002) (ci-après, « **l'Amendement** ») (CO-A-2025-003).

2. En substance, la Proposition entend permettre des accès supplémentaires aux données du Registre National (ci-après, « **RN** ») et des Registres des cartes d'identité et des cartes d'étranger par des acteurs privés, moyennant le consentement de la personne concernée. Les prestataires de services d'identification électroniques recevraient automatiquement des mises à jour de données à caractère personnel issues de ces sources de données, afin d'une part, de disposer eux-mêmes de données d'identification à jour à propos des personnes recourant à leurs services, et d'autre part, de communiquer tout ou partie de ces données aux acteurs privés auprès desquels ces personnes s'identifient via ces mêmes services[1].

3. A cette fin, la **Proposition** insère un article 5*quater* dans la loi du 8 août 1983 *organisant un registre national des personnes physiques* (ci-après, la « **Loi RN** ») et modifie l'article 6*bis*, § 3, de la loi du 19 juillet 1991 *relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour* (ci-après, la « **Loi de 1991** »).

4. L'**Amendement** quant à lui, concerne un portefeuille d'identité numérique (« *Digital Identity Wallet* ») et modifie l'article 6, § 1er, de la Loi de 1991.

II. Examen

Le présent avis est structuré comme suit :

[1] Sur la question de savoir si la Proposition entend bien permettre un accès aux Registres des cartes d'identité et des cartes d'étrangers au-delà des prestataires de services d'identification électronique, voir le considérant n° 11.

II.1. L'Amendement – Le portefeuille d'identité numérique

5. L'Amendement concerne un **portefeuille d'identité numérique** (« *Digital Identity Wallet* ») et modifie l'article 6, § 1er, de la Loi de 1991, en insérant entre ses premier et deuxième alinéas, l'alinéa suivant : « *Les documents d'identité numériques mobiles figurant dans l'application officielle 'portefeuille numérique belge' valent certificat d'inscription dans les registres de la population* ». Sur la base d'une recherche via Internet, ce portefeuille est *a priori* **l'application pour appareil mobile myGov** (voir https://mygov.be/[2]). Notamment, la page « Conditions d'utilisation » du site internet mygov.be précise ce qui suit :

> « *MyGov.be est une application ou app que vous pouvez installer sur votre appareil mobile. L'objectif de MyGov.be est de faciliter l'accès aux services publics, en fournissant un moyen simple et sûr de vous identifier. Cette application vous permet également de demander et recevoir facilement des documents officiels via le* ***Guichet****, de les conserver en lieu sûr et de communiquer en toute sécurité avec l'administration publique via la fonction* ***My eBox****, la version mobile de My ebox.*
> *MyGov.be est aussi une* ***clé numérique*** *qui vous permet de vous authentifier en ligne. Vous pouvez démontrer avec un niveau de confiance élevé et fiable qu'il s'agit bien de vous. Vous trouverez de plus amples informations sur les clés numériques ici : https://csam.be/fr/profil-egov.html.*
> *À l'avenir, cette application permettra d'apposer une* ***signature électronique*** *qualifiée* ».

[2] Dernièrement consulté le 22/01/2025.

6. En **droit européen**, les portefeuilles européens d'identité sont visés par les articles 3, 42. (définition[3]), et 5*bis* à 5*septies* du Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 *sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE* (ci-après, « **Règlement EIDAS** »), tels qu'insérés par le Règlement (UE) n° 2024/1183 du Parlement Européen et du Conseil du 11 avril 2024 *modifiant le Règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique* (ci-après, « **le Règlement EIDAS2** »).

7. En **droit belge**, la loi du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral* (ci-après, « **la Loi intégrateur de services** ») prévoit que l'intégrateur de services fédéral (soit, le Service public fédéral en charge de la Digitalisation[4]) développe et met à disposition un portefeuille européen d'identité numérique[5].

8. L'article 5*quinquies* du Règlement EIDAS prévoit notamment une obligation d'information de la Commission par les Etats membres en cas de fourniture et certification d'un portefeuille européen d'identité numérique, ainsi qu'une obligation de publication d'une liste de ces portefeuilles par la Commission. L'Autorité a interrogé le demandeur quant aux points suivants, le cadre normatif en la matière n'apparaissant pas totalement défini et d'application : la Commission a-t-elle été informée de ce « *portefeuille numérique belge* » précité et dans la négative pourquoi ? ; où est accessible la liste des portefeuilles européens d'identité numérique certifiés ? ; outre la Loi intégrateur de services, des règles de droit belge exécutant le Règlement EIDAS, et dans l'affirmative lesquelles, encadrent-elles le « portefeuille numérique belge » en le nommant, précisant les rôles et responsabilités de la (des) partie(s) qui l'offre(nt), etc. ? Le demandeur a répondu ce qui suit : « *Wij hebben geen contact gehad met de Europese Commissie* » et a renvoyé vers une page internet qui ne semble pas reprendre la liste recherchée[6]. Comme le demandeur l'indique par ailleurs dans une autre réponse communiquée à

---

[3] A savoir, « *un moyen d'identification électronique qui permet à l'utilisateur de stocker, de gérer et de valider en toute sécurité des données d'identification personnelle et des attestations électroniques d'attributs afin de les fournir aux parties utilisatrices et aux autres utilisateurs des portefeuilles européens d'identité numérique, et de signer au moyen de signatures électroniques qualifiées ou d'apposer des cachets au moyen de cachets électroniques qualifiés* ».

[4] Article 3 de la Loi intégrateur de services.

[5] Selon l'article 4, 3., de la Loi intégrateur de services, il a pour mission « *d'élabore*[r] *les modalités techniques et les conditions visant à développer, connecter et mettre à disposition les canaux d'accès aux banques de données, y compris les services web, les applications mobiles, le portefeuille européen d'identité numérique et les portails en ligne, de la manière la plus efficace et la plus sûre possible* ».

Selon l'article 4, 14., de la même loi, il « *développe et met à disposition un portefeuille européen d'identité numérique visé à l'article 3, point 42, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 relatif à l'identification électronique et aux services de confiance pour les transactions électroniques dans le marché intérieur et abrogeant la directive 1999/93/CE, modifiée par le règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) no 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique, et par l'intermédiaire du portefeuille européen d'identité numérique, afin de donner accès aux données contenues dans les banques de données et d'attester les données* ».

[6] Voir

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_fr, dernièrement consulté le 06/02/2025.

l'attention de l'Autorité, le cadre normatif du Règlement EIDAS réformé n'est pas encore en application[7].

9. Dans ces conditions, bien que l'intention de l'Amendement puisse être louable en ce que celle-ci pourrait s'inscrire dans l'objectif de la mise en œuvre du Règlement EIDAS2 en droit belge, **il apparaît néanmoins prématuré d'accorder dès maintenant, un effet légal particulier à « *l'application officielle 'portefeuille numérique belge'* » qui d'une part, n'est d'ailleurs pas définie dans le dispositif de l'Amendement** (ne serait-ce que par renvoi précis aux dispositions pertinentes du Règlement EIDAS ainsi qu'aux règles de droit belge l'exécutant), **et d'autre part, ne peut encore exister légalement comme portefeuille d'identité numérique au sens du Règlement EIDAS**. Ce qui n'exclut pas que l'Autorité soit bien consciente de la nécessité de préparer l'exécution du Règlement EIDAS en droit belge.

II.2. La Proposition – Modification de la Loi RN et de la Loi de 1991

II.2.1. Dispositif et motivation de la Proposition

10. L'article 5*quater* proposé de la Loi RN est principalement rédigé comme suit :

> « *Art. 5quater. § 1er. Sans préjudice de l'article 5, une personne majeure peut également* ***autoriser*** *la communication par les services du Registre national de ses informations visées à l'article 3, alinéa 1er, ainsi que des modifications apportées à ces informations,* ***à des fournisseurs de service d'identification électronique de niveau élevé ou substantiel*** *tels que visés dans le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, agréés par arrêté royal ou par un service public qui, par ou en vertu d'une loi, d'un décret ou d'une ordonnance, a pour mission de fournir un service de gestion des utilisateurs et des accès,* ***exclusivement à des fins d'identification et d'authentification d'une personne physique souhaitant recourir aux services de ces fournisseurs pour l'identification, l'authentification ou un service de signature électronique, et en vue de l'exécution de ces services****.*
>
> *§ 2. Les conditions visées à l'article* ***5ter, § 2, 1° et 3° à 6°,*** *s'appliquent à la communication des modifications visées au § 1er.*

[7] Voir le considérant n° 38.

> *§ 3. La* ***cessation de la relation contractuelle entre la personne physique et les fournisseurs d'un service d'identification électronique*** *entraîne la cessation de toute communication de données issues du Registre national. Le service d'identification électronique est tenu de signaler aux services du Registre national la cessation de ladite relation contractuelle.*
>
> *Les fournisseurs d'un service d'identification électronique* ***ne peuvent communiquer les données obtenues conformément au § 1er à des tiers que moyennant le consentement*** *de la personne physique* » (mis en gras par l'Autorité).

11. Les développements de la Proposition précisent qu'il s'agit « *de faire parvenir* ***automatiquement*** *à des prestataires de services bien précis des mises à jour et des compléments d'information extraits de sources authentiques telles que le Registre national,* ***qu'ils pourraient partager avec les entreprises qui sont soumises à une obligation d'identification, par exemple,*** *et ce, selon des conditions bien définies et moyennant un contrôle effectué par le citoyen* » (mis en gras par l'Autorité). Sur ce point, les développements indiquent encore et notamment, ce qui suit : « *La réutilisation de données provenant de sources authentiques permettra* ***aux entreprises*** *de* ***s'acquitter de l'obligation qui leur incombe de compléter et de mettre à jour régulièrement les données****. Leurs* ***obligations en matière d'identification seront également*** *facilitées dès lors qu'elles disposeront d'un outil leur permettant de suivre les modifications apportées ou les éléments ajoutés à ces données d'identification. L'accès à ces données sera* ***également synonyme de simplification administrative****. Grâce à cet accès, les entreprises ne devront plus redemander constamment* ***certaines données****, ce qui occasionne des* ***tracas administratifs****. Enfin, l'accès à ces données* ***contribuera à la lutte contre la fraude (à l'identité)*** *et cet accès sera lui-même à l'abri des fraudes et sécurisé* » (mis en gras et souligné par l'Autorité).

12. Les développements précisent encore ce qui suit : « *Il n'est actuellement pas possible de partager des données provenant du Registre national. Bien que les articles 5, 5ter et 8 de la loi sur le Registre national prévoient déjà des possibilités de partager des données ou des modifications apportées à celles-ci avec des parties privées,* ***ces possibilités ne suffisent pas. Le ministre de l'Intérieur ou le SPF Intérieur n'autorise par exemple pas le partage de données (art. 5) ou ce partage n'est possible qu'en respectant toute une série de conditions restrictives et d'interprétations strictes (art. 5ter et art. 8, § 3 et § 5)****. C'est pourquoi nous entendons insérer un article 5quater dans la loi sur le Registre national* » (mis en gras par l'Autorité).

13. Et le demandeur indique ce qui suit dans le formulaire de demande d'avis :

« *Het blijft voor de burger altijd mogelijk om handmatig gegevens bij te werken bij de verschillende entiteiten of bedrijven die persoonsgegevens actueel willen en moeten houden, met name voor identificatiedoeleinden en naleving van wettelijke verplichtingen.*
Dit houdt echter in dat de burger actie moet ondernemen bij elke entiteit of elk bedrijf waar zijn/haar identificatiegegevens moeten worden bijgewerkt, wat lastig kan zijn en het risico op fouten of het niet tijdig handelen vergroot.
Deze actie kan eruit bestaan:

- ***Zich fysiek te begeven naar kantorennetwerk van (elke) derde partij, zoals banken**, die hierbij een correcte uitlezing en validatie van de gegevens van een (e)ID document dienen te verrichten;*
  o Naast de inspanning die hierbij wordt gevraagd van de betrokkenen, vergt dit ook een aanzienlijke werklast van de derde partijen in kwestie;
- ***Een foto of scan van het eID document maken en doorsturen**, hetgeen:*
  o enerzijds leidt tot complexiteit in de handelingen zoals die worden vereist van de betrokkene;
  o anderzijds onvermijdelijk leidt tot een verminderde betrouwbaarheid van de dusdanig bekomen gegevens: fouten in de overname van identiteitsgegevens via optische tekstherkenning zijn onvermijdelijk, en sterk afhankelijk van de kwaliteit van de scan en/of foto van het document;
- ***Het opsturen van een papieren document welke de identiteit van de gebruiker kan staven op basis van kopie van een ID document, een factuur van een nutsbedrijf of officiële instanties of andere**. Naast de hoge werklast zowel aan de kant van de betrokkene als van derde partijen, leidt dit ook overmijdelijk tot een verminderde betrouwbaarheid van deze identiteitsgegevens.*
- ***Online uitlezen van het eID document op websites van derden**. Dit vereist het gebruik van een kaartlezer en kennis van de persoonlijke pincode, hetgeen voor een groter deel van betrokkenen een complexiteit meebrengt die onoverkomelijk is gebleken sinds de initiële uitgifte van de eID kaarten in 2004.*

Samenvattend kan men stellen dat voor elk van deze alternatieve manieren deze:

- *ineffectief en onnauwkeurig zijn: identificatieprocessen worden hier vaak uitgevoerd met onnauwkeurige gegevens. Zo bieden scans van bijvoorbeeld papieren documenten zoals een identiteitskaart of factuur geen garantie voor de juistheid van de gegevens. Hierdoor is het voor betrokken entiteiten moeilijk om aan hun verplichtingen te voldoen, wat onder andere een groter risico op witwassen met zich meebrengt;*
- *duur, tijdrovend en onhandig zijn voor de burgers: het stelt digitale dienstverleners niet in staat om het bijwerken van verwerkte gegevens gebruiksvriendelijk en snel te*

maken voor burgers, wat leidt tot een slechte ervaring. Burgers moeten verschillende identificatieprocessen doorlopen met verschillende entiteiten, op verschillende tijdstippen, terwijl hun gegevens centraal beschikbaar en geverifieerd zijn vanuit authentieke bronnen. Verlopen gegevens kunnen uiteindelijk leiden tot het blokkeren van essentiële diensten (zoals het verlies van toegang tot bankrekeningen);

• niet aangepast zijn aan de digitaliseringstrend in een post-COVID-19 tijdperk: zowel burgers als entiteiten moeten vaak hun identiteit verifiëren aan de hand van papieren documenten (bijv. via scans) en persoonlijke identificatie;

• kostbaar en tijdrovend zijn voor entiteiten en bedrijven die gegevens die al beschikbaar zijn uit authentieke bronnen opnieuw moeten verzamelen ».

14. Modifié par la Proposition, **l'article 6*bis*, § 3, de la Loi de 1991** prévoirait en outre ce qui suit :

« *Aux conditions visées à l'article 5quater, § 2, de la loi du 8 août 1983 organisant un Registre national des personnes physiques,* ***les fournisseurs*** *visés à l'article 5quater, § 1er, de la même loi* ***sont habilités à connaître les informations visées au § 1er*** **[8]**, *moyennant le respect de l'autorisation visée à l'alinéa 1er* » (mis en gras par l'Autorité).

15. Le commentaire des articles de la Proposition justifie cette disposition comme suit :

« *Dès lors qu'il est possible de vérifier la validité de la carte d'identité grâce à laquelle les personnes concernées peuvent être identifiées, nous estimons qu'il serait judicieux de modifier l'article 6bis de la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour afin de* ***permettre aux prestataires de services d'identification électronique agréés d'accéder aux informations pertinentes à propos de la carte d'identité****, moyennant une autorisation préalable. Les prestataires de services agréés pourront ainsi* ***vérifier, conformément au règlement EIDAS, la validité du document d'identité sur la base duquel ils identifient la personne concernée et mettre à jour les données de la carte d'identité conformément au RGPD****. En outre, cette modification s'inscrit pleinement dans les récentes recommandations formulées par les organismes européens compétents à propos de la* ***fiabilité de l'identification en ligne*** *(ENISA, mars 2024)* » (mis en gras et souligné par l'Autorité).

[8] Voir la note de bas de page n° 13.

II.2.2. Deux catégories de flux de données et d'acteurs concernés

16. La Proposition prévoit par conséquent deux catégories de flux de données. Dans le cadre d'une **première catégorie de flux de données**, il s'agit tout d'abord de permettre aux **prestataires de services d'identification électronique agréés** de recevoir des données et des mises à jour des données extraites du RN et des Registres des cartes d'identité et cartes d'étranger. Ces « *acteurs pourront ainsi s'assurer que les données dont ils disposent sont toujours complètes et à jour, et ce, dans des conditions bien définies et de manière contrôlée par le citoyen* ». Sont concernés des fournisseurs de **service d'identification électronique de niveau élevé ou substantiel** tels que visés dans le règlement EIDAS, agréés.

17. Concernant l'agrément, il existe en droit positif belge un arrêté royal du 22 octobre 2017 *fixant les conditions, la procédure et les conséquences de l'agrément de services d'identification électronique pour applications publiques* (ci-après, « **l'AR de 2017** »). Cet arrêté exécute la loi du 18 juillet 2017 *relative à l'identification électronique (ci-après,* « **la Loi de 2017** »).

18. A l'heure de rédiger le présent avis, la Belgique a notifié deux **schémas d'identification** de niveau de garantie **élevé**, soit l'**eID** (la carte d'identité électronique)[9] et **Itsme** (une application mobile)[10]. L'Autorité a interrogé le demandeur afin d'identifier quels étaient les prestataires actuellement agréés et où leur liste était disponible. Elle l'a également interrogé quant à l'identification des prestataires qui seraient également agrées « *par un service public qui, par ou en vertu d'une loi, d'un décret ou d'une ordonnance, a pour mission de fournir un service de gestion des utilisateurs et des accès* ». Celui-ci a notamment répondu ce qui suit : « *En raison des exigences strictes de l'Arrêté Royal EIDAS, une seule entité a été accréditée à ce jour. Le prestataire de services d'identification électronique accrédité dans le cadre de l'Arrêté Royal EIDAS à ce jour est Belgian Mobile ID (pour la fourniture des moyens d'identification électronique itsme®)* ».

19. L'Autorité est d'avis que **la Proposition doit clarifier quels sont les prestataires qui sont agréés** « *par un service public qui, par ou en vertu d'une loi, d'un décret ou d'une ordonnance, a pour mission de fournir un service de gestion des utilisateurs et des accès* », ainsi que les éventuels services publics concernés, et le cadre normatif y applicable, ou omettre la référence à ceux-ci. L'Autorité ne se prononce pas à leur sujet dès lors qu'elle n'est pas en mesure de visualiser ni les entités ni le service public visé par la disposition en projet.

[9] Voir https://ec.europa.eu/digital-building-blocks/sites/display/EIDCOMMUNITY/Belgium+-+eID, dernièrement consulté le 13/01/2025.

[10] Voir https://ec.europa.eu/digital-building-blocks/sites/display/EIDCOMMUNITY/Belgium+-+Itsme, dernièrement consulté le 13/01/2025.

20. Une **deuxième catégorie de flux de données** consiste à **permettre la communication des données issues du RN, voire également des Registres des cartes d'identité et cartes d'étranger**, **aux entreprises** auprès desquelles la personne concernée s'identifie au moyen du service d'identification électronique concerné. Si l'article 3 du Projet ne semble permettre un accès aux données issues des Registres des cartes d'identité et des cartes d'étranger qu'aux prestataires de services d'identification électronique, les réponses communiquées par le demandeur laissent néanmoins entendre que ces données également, pourraient être communiquées à d'autres acteurs privés (soit les entités auprès desquelles la personne concernée s'identifie aux fins de l'exécution des contrats concernés)[11].

II.2.3. Relation entre la Proposition et l'article 5ter de la Loi RN

21. S'agissant des conditions dans lesquelles l'accès au RN pourra être octroyé, la Proposition justifie de sa conformité au RGPD en précisant notamment qu'il prévoit le recours aux *opt-in* et consentement du citoyen, il est sans préjudice de l'article 5 de la Loi RN (nécessitant l'autorisation du ministre de l'Intérieur), et il prévoit l'application des conditions visées à l'article **5*ter*,** § 2, 1° et 3° à 6°, de la **Loi RN**, **dans la filiation duquel il s'inscrit**. En effet sur ce dernier point, le commentaire de l'article 2 de la Proposition précise que le nouvel article 5*quater* de la loi RN « *fait suite à l'article 5ter de la loi sur le Registre national qui poursuit une finalité identique, à savoir l'obtention de mises à jour automatiques du Registre national* ».

22. Cette dernière disposition a été insérée dans la Loi RN par une **loi du 25 novembre 2018** *portant des dispositions diverses concernant le Registre national et les registres de population*. Elle étend de manière inédite, pour des finalités qui ne sont **pas liées à l'intérêt général**, les possibilités d'accéder au RN **par le secteur privé**. L'avant-projet de cette loi a été l'objet d'un avis de la Commission de la Protection de la Vie Privée n° 19/2018 du 28 février 2018 *concernant un avant-projet de loi portant des dispositions diverses « Intérieur » (CO-A-2018-002)* (ci-après, « **l'avis de la CPVP** »).

23. L'Autorité observe cependant et avant tout, que l'article **5*quater*** en projet de la Loi RN a une **portée plus large** que l'article 5*ter* de la Loi RN, évoqué dans les développements du Projet, et **va plus loin** dans l'accessibilité aux données issues du RN et des Registres des cartes d'identité et cartes d'étranger. L'article **5*ter*** ne concerne que les données visées à **l'article 3, al. 1er, 1°, 5° et 6°** de la Loi RN (soit, les nom et prénom, résidence principale et lieu et date de décès ou, en cas de déclaration d'absence, la date de la transcription de la décision déclarative d'absence).

[11] La photo en effet, ne se trouve pas dans le RN mais bien dans le Registre des cartes d'identité. Voir les considérants nos 14 et 37.

24. Or s'agissant de **l'accès au RN**, la Proposition vise ***l'ensemble* des données visées à l'article 3, al. 1er, de la Loi RN**[12]. La Proposition, en son article 3, modifiant l'article 6*bis* de la Loi de 1991, « *habilite* » **également** les fournisseurs de services d'identification électronique « *à connaître* » des informations reprises aux fichier central des cartes d'identité et au fichier central des étrangers, soit **les Registres des cartes d'identité et des cartes d'étranger**[13]. L'hypothèse visée par l'article 5*ter* de la Loi RN n'a pas été assortie d'une telle possibilité.

---

[12] Ces données sont les suivantes :

«1° les nom et prénoms;

2° le lieu et la date de naissance;

3° le sexe;

4° la nationalité;

5° la résidence principale;

6° (le lieu et la date du décès ou, en cas de déclaration d'absence, la date de la transcription de la décision déclarative d'absence); <L 2007-05-09/44, art. 52, 021; En vigueur : 01-07/2007>

7° [4 ...]4

8° l'état civil;

9° la composition du ménage.

[1 9° /1 [4 les actes et décisions relatifs à la capacité juridique et les décisions d'administration de biens ou de la personne visées à l'[6 article 1250]6, alinéa 1er, du Code judiciaire; le nom, le prénom et l'adresse de la personne qui représente ou assiste un mineur, un interdit, un interné ou une personne placée sous statut de minorité prolongée, ou de l'administrateur de biens ou de la personne dont il est fait mention dans la décision visée à l'[6 article 1250]6, alinéa 1er, du Code judiciaire.]4]1

(10° la mention du registre dans lequel les personnes visées à l'article 2 sont inscrites [5 ou mentionnées]5; 11° la situation administrative des personnes visées à l'article 2, alinéa 1er, 3°.) <L 1994-05-24/39, art. 9, 005; En vigueur : 01-02-1995>

(12° s'il échet l'existence du certificat d'identité et de signature, dans le sens de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification;

13° la cohabitation légale.) <L 2003-03-25/30, art. 3, 013; En vigueur : 07-04-2003>

(14° la situation de séjour pour les étrangers visés à l'article 2.) <L 2006-12-27/30, art. 166, 018; En vigueur : 01-04-2007>

[3 15° la mention des ascendants au premier degré, que le lien de filiation soit établi dans l'acte de naissance, par décision judiciaire, par reconnaissance ou par une adoption;

16° la mention des descendants en ligne directe au premier degré, que le lien de filiation soit établi dans l'acte de naissance, par décision judiciaire, par reconnaissance ou par une adoption;

17° [4 le cas échéant, les coordonnées communiquées uniquement sur une base volontaire par les citoyens, telles que déterminées par le Roi, par arrêté délibéré en Conseil des ministres; le Roi détermine également les modalités de communication de ces données aux services du Registre national des personnes physiques et de modification de ces données par le citoyen;]4]3 ».

[13] Soit les données visées dans l'article 6*bis*, § 1er, de la Loi de 1991 :

« *1° [4 pour chaque titulaire: le numéro d'identification du Registre national des personnes physiques, la photo du titulaire correspondant à celle de la dernière carte ainsi que les photos du titulaire figurant sur les cartes d'identité qui lui ont été délivrées au cours des quinze dernières années, l'image électronique de la signature du titulaire ainsi que l'historique des images électroniques des signatures, la langue demandée pour l'émission de la carte et le numéro d'ordre de la carte. Le Roi fixe la date à partir de laquelle l'historique des photos et l'historique des images électroniques des signatures sont enregistrées et conservées dans le fichier central des cartes d'identité et dans le fichier central des cartes d'étrangers;]4*

2° pour chaque (carte) émise : <L 2007-05-15/42, art. 12, 013; En vigueur : 18-06-2007>
a) la date de demande avec la date d'émission du document de base, la date d'émission, la date de péremption de la carte et, le cas échéant, la date de destruction;

b) la date de délivrance et la commune qui l'a délivrée;

c) le numéro d'ordre de la carte;

d) le numéro de séquence (première, deuxième, troisième, etc. carte);

e) l'information dont il ressort que la carte est valable, périmée ou détruite et, dans ce cas, la raison;

f) le type de (carte); <L 2007-05-15/42, art. 12, 013; En vigueur : 18-06-2007>

g) indication de la présence ou de l'absence de la fonction " signature électronique ";

h) la date de la dernière mise à jour;

25. En outre, **contrairement à l'article 5*ter* de la Loi RN**, lu en combinaison avec l'article 5 de cette même loi, dans l'hypothèse duquel chaque organisme doit être autorisé par le ministre de l'Intérieur à accéder aux données du RN, la Proposition prévoit un **rôle d'autorisation plus limité au ministre de l'Intérieur**, qui devra uniquement autoriser l'accès par les prestataires de service d'identification électroniques (et non les entreprises qui accèderont par l'intermédiaire de ces prestataires, aux données issues du RN et des Registres précités).

26. L'Autorité a interrogé le demandeur d'avis quant à la réalisation éventuelle préalable d'une **analyse d'impact**. Elle l'a également interrogé quant à la question de savoir s'il disposait de données relatives à la mise en œuvre de l'article 5*ter* de la Loi RN (nombre d'entreprises concernées ; de personnes concernées ; etc.), s'agissant d'un précédent avancé dans la discussion du Projet. Celui-ci a notamment précisé ne pas disposer de chiffres en la matière en renvoyant vers le RN, et l'Autorité comprend de la réponse communiquée qu'une analyse d'impact n'a pas en tant que telle, été réalisée[14]. L'Autorité a interrogé le RN au sujet de la mise en œuvre de l'article 5*ter* de la Loi RN et celui-ci a répondu **qu'à ce jour, aucune demande d'autorisation n'avait été introduite sur la base de l'article 5*ter* de la Loi RN**.

27. Afin d'assurer un débat parlementaire efficace à propos du Projet, compte-tenu de l'extension envisagée dans l'accessibilité du secteur privées aux données issues du RN et des Registres des cartes d'identité et cartes des étrangers, **l'Autorité recommande au demandeur la réalisation d'une analyse d'impact, et ce, également à l'aune des questionnements posés dans le présent avis**.

II.2.4. L'identification électronique dans le Règlement EIDAS au regard des objectifs de la Proposition

28. Les **finalités poursuivies par la Proposition manquent de clarté**. L'Autorité souligne qu'en substance, **l'identification électronique** dans le cadre du Règlement EIDAS a pour objectif d'établir et de confirmer (authentification), avec un certain degré de fiabilité (faible, substantiel ou élevé), l'identité d'une personne, sur la base de données la représentant de manière univoque conformément

---

i) la date de la dernière mise à jour relative à la résidence principale.

(j) les autres mentions, imposées par les lois;) <L 2007-05-15/42, art. 12, 013; En vigueur : 18-06-2007> [3 k) la mention visée à l'article 374/1 du Code civil.] 3 ».

[14] Le demandeur a répondu ce qui suit :

« *En ce qui concerne le champ d'application de la proposition de loi, l'article 5quater étend le champ d'application de l'article 5ter pour répondre au besoin plus large du secteur privé d'accéder à des données de meilleure qualité au moyen d'un processus pratique et sûr. Ce champ d'application élargi est nécessaire pour éviter l'utilisation de méthodes moins précises et moins sûres pour que les citoyens fournissent leurs données à des entités privées, telles que les processus sur papier ou l'utilisation d'une copie des documents d'identité/ passeport combinée à des processus manuels de mise à jour des données à l'initiative du citoyen* ».

au droit applicable. Le Règlement EIDAS a défini **l'ensemble minimal de données d'identification personnelle nécessaire pour représenter de manière univoque une personne** (physique ou morale), et s'agissant des personnes physiques, il s'agit des données **obligatoires** suivantes : nom(s) de famille actuel(s) ; prénom(s) actuel(s) ; date de naissance ; un identifiant unique créé par l'État membre expéditeur conformément aux spécifications techniques aux fins de l'identification transfrontalière et qui soit aussi persistant que possible dans le temps[15]. L'ensemble minimal de données ***peut*** également contenir un ou plusieurs des attributs supplémentaires suivants : prénom(s) et nom(s) de famille à la naissance ; lieu de naissance ; adresse actuelle ; sexe[16]. Sur ce point, l'Autorité souligne que l'addition de données facultatives doit être **justifiée conformément au principe de minimisation des données consacré dans l'article 5, 1., c), du RGPD[17]**. Au passage et sans analyser ce sujet, l'Autorité observe que d'après la documentation technique disponible en ligne à propos **d'Itsme, les « *attributs* » (ou « *claims* »)** qui peuvent être communiqués à propos de l'utilisateur sont plus nombreux et paraissent partant, aller au-delà de la simple identification au sens du règlement EIDAS[18].

29. L'identification électronique au sens du Règlement EIDAS **n'a pas pour objectif de permettre la communication directe de données à caractère personnel issues d'une source authentique de données,** par un « *fournisseur de service d'identification électronique* »[19], à des entreprises à l'égard desquelles la personne concernée a recours à ce fournisseur (en fait, à un schéma d'identification donné), **aux fins de l'exécution par cette entreprise, d'obligations légales et**

---

[15] Voir l'article 12, 3., d), du Règlement EIDAS ainsi que l'annexe du Règlement d'exécution (UE) n° 2015/1501 de la Commission du 8 septembre 2015 *sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement (UE) no 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur*.

[16] *Ibid*.

[17] En Belgique, **les noms, prénoms, date de naissance et numéro RN permettent par définition, de représenter de manière univoque une personne concernée**. Les prénom(s) et nom(s) de famille à la naissance, lieu de naissance, adresse actuelle et sexe ne sont pas nécessaires. Et logiquement, l'Autorité souligne que le Règlement EIDAS est sans préjudice du RGPD (voir l'article 2, 4., du Règlement EIDAS.

[18] Sans entrer dans les détails, parmi les données **facultatives dans le cadre d'EIDAS**, sont reprises pour la Belgique : le genre (« *User's gender. Possible values are: female male unknown n/a. If the value mentioned on the user's ID document is different from those (local language, letter code...), then we apply a best-effort mapping to one of those values* ») ainsi que l' « *official_gender* » (« *User's gender unaltered, exactly as mentioned on their ID document* ») ; le lieu de naissance (ville et pays) ; l'adresse. **Au-delà** des données visées par le Règlement EIDAS, sont aussi et notamment disponibles : la nationalité (selon deux formats, soit comme indiquée sur le document d'identité et selon la forme ISO 3166-1 alpha-3) ; le numéro d'identification du document d'identité ; des informations à propos de l'appareil de l'utilisateur (OS, modèle, etc.) ; la date de délivrance du document d'identité ainsi que sa date d'échéance ; le type de document d'identité et le pays qui l'a délivré ; et la **photo** (à savoir, « *User's ID picture, represented as a URL string. This URL points to an image file (for example, a JPEG, JPEG2000, or PNG image file). This image is the raw (unprocessed) image contained on the ID document. Accessing this URL has to be done with your bearer token. Example:* […] »). Voir

https://belgianmobileid.github.io/doc/authentication/#user-data, https://belgianmobileid.github.io/doc/identification/#user-data, https://belgianmobileid.github.io/doc/confirmation/#user-data et https://belgianmobileid.github.io/doc/claims/, dernièrement consultés le 23/01/2025. Les attributs disponibles varient selon le document officiel à partir duquel le compte Itsme a été créé.

[19] Dans le règlement EIDAS, il convient de distinguer les éléments sollicités dans le schéma d'identification, soit un moyen d'identification – un élément matériel et/ou immatériel ; et une authentification – un processus.

L'article 1er, 1°, de l'AR de 2017 définit le « *service d'identification électronique* » comme « *le service garantissant l'identité de l'utilisateur qui tente d'accéder **à des applications publiques** sur la base d'une option d'identification* » (mis en gras par l'Autorité).

autres finalités qui lui sont propres, au-delà de la pure confirmation de l'identité revendiquée par la personne concernée sur la base des données d'identification prédéfinies[20, 21].

30. A ce sujet, **il n'est pas ici question de portefeuilles européen d'identité numérique** ou encore **d'attestations électroniques d'attributs[22]**. A noter sur ce point que les objectifs poursuivis par le portefeuille européen d'identité vont plus loin que la simple identification visée par le Règlement EIDAS[23], et que ce portefeuille est assorti d'une série de garanties additionnelles en matière de transparence et de contrôle par la personne concernée[24].

31. En outre en droit belge, l'article 1er, 1°, de **l'AR de 2017** définit le « *service d'identification électronique* » comme « *le service garantissant l'identité de l'utilisateur qui tente d'accéder* ***à des applications publiques*** *sur la base d'une option d'identification* » (mis en gras par l'Autorité)[25]. Contrairement au portefeuille européen d'identité numérique qui semble bien avoir pour finalité de permettre **l'identification électronique à l'égard du secteur privé en général**, **dans la logique de la réforme du Règlement EIDAS**, tel ne semble pas être le cas de la Loi de 2017 et de l'AR de 2017.

32. Dans ce contexte, **l'Autorité a posé plusieurs questions au demandeur[26]** dont les réponses sont prises en considérations dans les développements suivants.

II.2.5. La garantie que constitue l'agrément en vertu de l'AR de 2017

[20] Voir le considérant n° 28 s'agissant des **données minimales concernées**.

[21] Remarque : sans analyser cette hypothèse, l'Autorité observe que le FAS (« *Federal Authentication Service* ») semble bien « *retirer* » « *des attributs liés à un utilisateur auprès d'une ou de plusieurs sources fiables disponibles au sein d'autres institutions publiques (p.ex. Registre national, BCSS et BCE)* », Voir https://bosa.belgium.be/fr/services/federal-authentication-service-fas#anchor-3, dernièrement consulté le 23/01/2025. Mais celui-ci est fourni par une autorité publique et afin d'accéder à des applications publiques. Il s'agit par conséquent d'un contexte distinct.

[22] Voir les articles 3, 43) – 46), et 45*ter* à 45*nonies* du Règlement EIDAS, et l'Annexe VI de ce même Règlement qui définit une **liste minimale d'attributs** (dont l'adresse, l'âge, le sexe, l'état civil, la composition de famille, les diplômes, etc.).

[23] Voir le considérant n° 6.

[24] Voir notamment à ce sujet, le considérant n° 51.

[25] Le concept de « *prestataire de services* » renvoie à « *la personne qui offre un service d'identification électronique agréé* ».

[26] L'objectif poursuivi par la Proposition ne pourrait-il en fait pas être rencontré via le portefeuille belge (européen) d'identité numérique et les attestations électroniques d'attributs ? Quelle est sa plus-value à cet égard ? L'objectif est-il bien de permettre, par l'intermédiaire du prestataire de service d'identification électronique utilisé par la personne concernée, de communiquer des données issues du RN aux entreprises auprès desquelles cette personne s'identifie, aux fins de la satisfaction, par ces entreprises, de leurs obligations légales et lesquelles ? Une illustration concrète des scénarios envisagés peut-elle être communiquée ? Pourrait-il être confirmé ou infirmé que l'agrément visé par l'AR de 2017 concerne les services d'identifications utilisés pour accéder à des applications publiques (et non à des services fournis par des entités privées). En cas de confirmation, sur la base de quelles règles les prestataires de service seraient-ils agréés s'agissant de l'accès à des services offerts par le secteur privé ? L'Autorité a aussi invité le demandeur à justifier la raison pour laquelle il était envisagé de permettre l'accès à des données allant au-delà de l'ensemble minimal de données obligatoires d'identification personnelle nécessaire pour représenter de manière univoque une personne prévue par le règlement EIDAS (voir le considérant n° 28) alors qu'il n'est question que d'identification ?

33. Dès lors que la Proposition présente l'agrément en vertu de l'AR de 2017 comme une garantie importante dans son contexte, l'Autorité a interrogé le demandeur quant à l'applicabilité de cet arrêté royal dans le cadre de l'identification dans le secteur privé. Celui-ci a communiqué les éléments suivants :

> « *L'accréditation des fournisseurs de services d'identification électronique dans le cadre de l'Arrêté Royal EIDAS concerne l'autorisation de fournir des services* ***dans le cadre d'applications publiques****.* ***Toutefois,*** *il est essentiel de noter que les moyens d'identification électronique couverts par l'accréditation* ***sont fournis à la fois dans le cadre de services au secteur public et au secteur privé****. Ce point est d'ailleurs souligné par l'Arrêté Royal EIDAS lui-même, qui exige que ces prestataires de services exploitent déjà ces services conformément aux exigences du Règlement EIDAS, avant l'accréditation (voir l'article 28 de l'Arrêté Royal EIDAS). En particulier, les moyens d'identification électronique sont eux-mêmes soumis à des exigences strictes en vertu du Règlement EIDAS.*
>
> ***D'une certaine manière, l'accréditation prévue par l'Arrêté Royal EIDAS agit comme une couche supplémentaire*** *pour les fournisseurs de services d'identification électronique. Cette couche supplémentaire* ***reste*** *néanmoins* ***pertinente*** *(en plus des exigences existantes en vertu du règlement EIDAS lui-même)* ***pour la fourniture*** *des moyens d'identification électronique par les fournisseurs de services d'identification électronique accrédités* ***dans le secteur privé****. L'Arrêté Royal EIDAS impose des* ***exigences supplémentaires qui s'appliquent à l'ensemble de l'organisation des prestataires de services****. Ces derniers sont notamment soumis à des exigences d'audit appliquées à l'ensemble de leur organisation et doivent présenter des garanties strictes* ***applicables à tous leurs processus et services, qu'ils soient fournis aux autorités publiques ou à des entités privées*** *; c'est par exemple le cas de leur obligation de se conformer strictement - et d'être audités sur leur conformité - au GDPR, aux exigences de sécurité, etc. La supervision par les autorités belges des fournisseurs de services d'identification électronique accrédités dans le cadre de l'Arrêté Royal EIDAS* ***s'étend donc au-delà de la portée de leurs services dans le cadre d'applications publiques*** » (mis en gras par l'Autorité)[27].

[27] Le demandeur a également communiqué ce qui suit :

« *Le statut et le rôle spécifiques des prestataires de services d'identification électronique agréés dans le secteur privé et le fait qu'ils présentent des garanties supplémentaires, leur permettant notamment de traiter des données spécifiques dans le cadre de la loi sur les registres nationaux, ont déjà été reconnus par le législateur belge à plusieurs reprises.*

En 2018, juste après l'introduction du statut des fournisseurs de services d'identification électronique, la loi sur le registre national a été modifiée pour autoriser spécifiquement ces prestataires de services à traiter le numéro de registre national à des fins d'identification et d'authentification dans le cadre des services qu'ils offrent aux entités privées (voir article 8, §5 de la loi sur le registre national). Les fournisseurs de services d'identification électronique sont, dans ce contexte, également autorisés à transférer le numéro de registre national aux entités privées utilisant leurs services d'identification et d'authentification, aux mêmes fins d'identification et d'authentification (voir les commentaires sur l'article 8§5 dans Proposition de loi portant des dispositions diverses concernant le Registre national et les registres de population, Commentaires des articles, Doc., Ch., 2017-2018, n° 3256/001, pp. 26-27).

34. L'Autorité prend acte de cette réponse. **Pour que l'agrément visé par la Proposition puisse constituer la garantie effective qu'il est supposé offrir en vertu de celle-ci et de sa motivation, l'Autorité est d'avis qu'il convient** :

- Que le demandeur **vérifie** si un agrément tel que visé par l'AR de 2017 peut bien être imposé dans l'offre de services d'identification dans le secteur privé au motif que le prestataire de service concerné se voit accorder l'accès à des sources authentiques de données ;

- Que le demandeur établisse avec certitude que l'AR de 2017 est bien juridiquement également applicable à la prestation de services d'identification électronique dans le secteur privé par les prestataires agréés et dans quelle mesure. L'Autorité ne pouvant pas le confirmer et en doutant[28], bien que certaines conditions de l'agrément soient relatives à l'activité du prestataire en général. En outre, la Proposition entend aller au-delà de la simple identification au sens du Règlement EIDAS[29]. **Dès lors que l'AR de 2017 n'a pas initialement été rédigé dans l'optique de la Proposition** (application aux applications du secteur privé pour l'identification et l'échange de données additionnelles), **il devrait être adapté** afin de s'appliquer également et de manière certaine, dans la mesure pertinente voulue[30], à la prestation de services visés par la Proposition, dans le secteur privé ;

En 2020, le législateur belge a transposé la cinquième directive anti-blanchiment (directive UE 2018/843 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme) en adoptant la loi du 20 juillet 2020. Dans le cadre de cette transposition, le législateur belge a reconnu que notamment les États membres doivent encourager le secteur privé à utiliser volontairement des moyens d'identification électronique reconnus dans le cadre d'un schéma notifié, c'est-à-dire notamment des moyens d'identification électronique accrédités dans le cadre de l'Arrêté Royal EIDAS (voir notamment les commentaires dans la proposition de loi portant des dispositions diverses relatives à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, Exposés des motifs, Doc, Ch., 2019-2020, n°1324/001, pp. 10-11). Le législateur a donc explicitement reconnu que l'utilisation des moyens d'identification électronique fournis par des prestataires de services d'identification électronique agréés est considérée comme suffisante pour satisfaire aux obligations de KYC liées à la vérification des personnes à identifier dans le cadre des obligations de lutte contre le blanchiment d'argent et le financement du terrorisme (voir l'article 27, §1, 2° de la loi belge relative à la lutte contre le blanchiment de capitaux) ».

Ces considérations ne sont toutefois pas déterminantes en l'occurrence. D'une part, les certificats (d'authentification et de signature) repris sur la carte d'identité belge comportant le numéro de RN, le traitement de ce dernier est nécessité par toute solution basée sur ces certificats. Une adaptation de la Loi RN était par conséquent nécessaire afin de permettre l'identification et la signature électroniques sur la base des certificats concernés (le traitement du numéro de RN est nécessaire à la vérification des certificats). Etant entendu dans ce contexte, que la finalité d'utilisation du numéro de RN est exclusivement limitée par l'article 8, §§ 5 et 3 de la Loi RN. D'autre part, que le législateur encourage le recours aux services agréés concernés n'est pas décisif quant à la détermination du champ d'application des règles de l'AR de 2017.

[28] Voir notamment les articles 1er, 1° (définition du service d'identification électronique) ; 2, § 1er (la conséquence de l'agrément est l'autorisation de mettre le service à disposition à des fins d'utilisation sur des applications publiques) ; 4 (relation avec l'option d'identification avec laquelle l'accès à l'application publique est demandé) ; 16, § 1er (ne vise que les applications publiques consultées) ; 20 (concernant le support à fournir) ; 33 et 34 (conséquences opérationnelles de l'agrément en relation avec des applications publiques) ; 41 (indemnisation des prestataires de services), etc. L'AR de 2017 **ne prévoit par ailleurs pas explicitement que ses conditions s'appliquent également à la fourniture de service dans le cadre des applications du secteur privé, ni n'exclut que le prestataire agréé offre dans d'autres conditions des services d'identification électronique** dans ce même cadre, **qui ne répondraient pas aux conditions de l'agrément**. Quid par exemple de l'applicabilité des exigences liées à la disponibilité du service, sa réactivité, à la gestion du déploiement, etc. ?

[29] Voir les considérants nos 35 et 41-42.

[30] Cela nécessite également de s'interroger sur l'éventualité de l'hypothèse des prestataires qui ne souhaiteraient pas offrir leurs services dans le cadre de l'identification à des applications publiques – quelles règles relatives à l'agrément doivent rester d'application dans ce cas ?

- Que les règles et le processus d'agrément prévoient la prise en compte et l'évaluation de la mise en œuvre des principes et garanties applicables en matière de protection des données, en particulier à l'aune des développements ultérieurs[31].

II.2.6. Finalités poursuivies par la Proposition et données traitées

A) Informations complémentaires communiquées par le demandeur

35. S'agissant de **l'objectif** poursuivi par la Proposition, le demandeur a précisé ce qui suit :

> « *L'objectif de la proposition est double :* ***(i) améliorer la sécurité des échanges de données et répondre à la nécessité d'une meilleure qualité des données dans le secteur privé, notamment pour des raisons de conformité et (ii) réduire la charge administrative pesant sur les citoyens et les entités privées****.*
>
> *La proposition donne la possibilité aux fournisseurs de services d'identification électronique de mettre à jour, si nécessaire, les données collectées au moment de l'identification des citoyens (y compris les données obtenues à partir de la carte d'identité des citoyens), à condition qu'ils aient reçu un consentement valide au sens du RGPD de la part des citoyens concernés et que ce consentement soit toujours valide au moment de la mise à jour. Cela concerne les données dont la source authentique est le registre national (cf. proposition de nouvel article 5quater dans le cadre de la loi relative au registre national du 8 août 1983) et le registre des cartes d'identité (cf. proposition de modification de l'article 6bis, paragraphe 3, de la loi relative au registre de la population et à la carte d'identité du 19 juillet 1991) . Cela garantit que les citoyens ne partagent pas de données obsolètes lorsqu'ils doivent s'identifier auprès d'entités privées et qu'ils décident d'utiliser leur moyen d'identification électronique pour ce faire. Toute utilisation* ***ultérieure*** *des moyens d'identification électronique pour identifier les citoyens et tout transfert de données à caractère personnel liées à ces moyens d'identification électronique se feront toujours avec le consentement du citoyen concerné et* ***peuvent être requis pour différentes raisons, notamment la nécessité d'identifier et d'authentifier avec suffisamment de certitude la personne avec laquelle une entité privée est en contact et avec laquelle elle est susceptible de passer un contrat, ou l'obligation légale de collecter certaines données concernant le citoyen dans le cas d'une entité soumise au cadre juridique relatif à la lutte contre le blanchiment d'argent, par exemple****.*

[31] Voir le considérant n° 51.

*La proposition vise à **réduire les contraintes imposées aux citoyens pour la mise à jour de leurs données et à supprimer autant que possible la nécessité d'actions proactives de la part des citoyens pour mettre à jour manuellement leurs données**. En pratique, les citoyens doivent constamment mettre à jour et fournir à nouveau leurs données aux entreprises, car les modifications apportées aux données personnelles (par exemple, un changement d'adresse) ne sont pas transmises automatiquement ni facilement accessibles au secteur privé (comme indiqué ci-dessous).*

Cela conduit à diverses inefficacités et à divers risques, notamment:

1.Premièrement, tout partage de données comporte des risques de sécurité et de confidentialité lorsqu'il n'est pas effectué par le biais de canaux sécurisés
2.De plus, cette façon de travailler nécessite toujours une initiative de la part d'un acteur qui est souvent le citoyen lui-même.
3.En l'absence d'initiative, les informations ne sont pas mises à jour et des informations incorrectes (incomplètes ou non actualisées) sont susceptibles de circuler parce que les mises à jour ou les modifications ne sont pas communiquées à temps. Il en résulte une insécurité juridique. Les entreprises ne peuvent pas respecter leurs obligations d'identification, ni l'obligation générale du RGPD de ne travailler qu'avec des données correctes, avec tous les risques que cela comporte (fraude à l'identité, exclusion numérique, etc.). Pensez à une entreprise qui n'est pas informée à temps d'un changement d'adresse de son client.

*En outre, **les processus utilisés pour mettre à jour les données sont inefficaces, coûteux et longs, tant pour les citoyens que pour les entités privées**. En cas de modification de leurs données, les citoyens doivent également suivre différentes procédures auprès de différentes entités (par exemple, en cas de changement d'adresse, ils sont tenus d'informer toutes les entreprises avec lesquelles ils entretiennent une relation durable de ce changement), à différents moments. Des données non mises à jour peuvent en fin de compte conduire au blocage de services essentiels, comme la perte d'accès à un compte bancaire. En particulier, ceci peut également conduire à l'impossibilité d'utiliser un moyen d'identification électronique valide. Ceci est d'autant plus problématique que les citoyens ont parfois l'impression que ce lien entre leur moyen d'identification électronique et source authentique est déjà mis en place et tendent à ne pas mettre leur moyen d'identification électronique à jour proactivement.*

Pour les citoyens qui ne donneraient pas leur consentement pas à fournir des mises à jour, ces mesures supplémentaires - mais plus lourdes et moins efficaces - restent applicables pour mettre à jour leurs données.

Enfin, nous notons que la proposition concerne, pour la majorité des données à caractère personnel en jeu, ***des données à caractère personnel qui sont déjà traitées par les fournisseurs de services d'identification électronique pour la même finalité d'identification. Par conséquent, l'impact sur la quantité de données personnelles des citoyens traitées devrait rester limité*** » (mis en gras par l'Autorité).

36. Le demandeur a en outre communiqué une **illustration concrète** de la mise en œuvre de la Proposition sur la base de l'application Itsme.

37. S'agissant de la justification de l'accès à des données allant **au-delà de l'ensemble minimal de données obligatoires d'identification personnelle** nécessaire pour représenter de manière univoque une personne prévue par le règlement EIDAS[32], le demandeur a indiqué ce qui suit :

> « *L'accès à un ensemble plus large de données d'identification est* ***essentiel pour soutenir la fourniture de services d'identification sûrs et fiables qui répondent aux différents besoins dans tous les secteurs****. La facilitation de l'accès à ces données est également conforme à la tendance législative générale au niveau de l'UE (comme le règlement 2022/668 de l'UE, c'est-à-dire le Règlement sur la gouvernance des données, et le règlement 2023/2854 de l'UE, c'est-à-dire le Règlement sur les données) et à la stratégie 2030 de l'UE pour une économie fondée sur les données, qui s'efforcent de fournir aux citoyens de l'UE un cadre juridique et une infrastructure plus fiables et plus sûrs pour contrôler leurs données en étant en mesure de les partager dans tous les secteurs (à la fois avec des entités publiques et privées).*
>
> ***En particulier****,* ***l'accès aux données suivantes contenues dans le registre national peut être justifié comme suit*** *:*
>
> - *le nom et les prénoms, le lieu et la date de naissance, le lieu de résidence principale et la nationalité (article 3, 1°, 2°, 4°, 5°) :*
>
> *Ces informations sont requises pour l'identification (y compris la vérification de l'identité) par la* ***directive AML UE 2015/849*** *(telle que modifiée par la directive AML 2018/843), qui a été transposée dans la* ***loi belge du 17 sept. 2017*** *(telle que modifiée par la loi du 20 juillet 2020), en ajoutant le lieu de naissance comme éléments supplémentaires. Cette obligation légale s'applique à des secteurs très divers, notamment les entités financières et le secteur*

[32] Voir les considérants nos 23 et 28.

des assurances, mais aussi la comptabilité, le secteur des jeux de hasard, les services postaux, le secteur diamantaire, etc. (cf. art. 5 de la loi belge relative à la lutte contre le blanchiment d'argent). En particulier, les lignes directrices de la BNB sur l'application de la lutte contre le blanchiment d'argent au secteur financier exigent que ces données soient tenues à jour, ce qui correspond aux obligations générales du GDPR.
En outre, ***la création d'un certificat*** *qualifié pour les personnes physiques doit inclure les noms et prénoms, la date de naissance et, dans certains cas, la nationalité, conformément aux normes EIDAS et ETSI.*

- ***le lieu et la date du décès ou, en cas de déclaration d'absence, la date du transfert de la décision contenant la déclaration d'absence (article 3, 6°)*** *:*

Conformément au ***règlement EIDAS****, les fournisseurs de moyens d'identification électronique sont tenus de fonder l'identification hautement fiable des personnes physiques sur des procédures qui démontrent la validité continue de cette identification. L'utilisation de ces informations est donc cruciale pour s'assurer qu'aucune autre utilisation des moyens d'identification électronique n'est faite après le décès du citoyen ;*

- ***le sexe, l'état civil, la composition de la famille, la cohabitation légale, l'état de résidence pour l'étranger, l'inscription du registre dans lequel sont inscrites les personnes inscrites au registre de la population ou des étrangers, au "registre d'attente" ou au registre des consuls ; la situation administrative des personnes inscrites au registre des consuls (article 3, 3°, 8°, 9°, 10°, 11°, 13°, 14°)*** *;*

Conformément à la législation sur la lutte contre le blanchiment d'argent et aux lignes directrices des autorités de régulation financière, il s'agit ***d'informations supplémentaires que les entités obligées peuvent être amenées à demander dans le cadre de leur processus KYC****, soit dans le cadre des "informations supplémentaires à demander en cas de mesure de vigilance renforcée", soit pour effectuer une évaluation précise des risques liés à la lutte contre le blanchiment d'argent dans le cadre de la relation avec la personne à identifier. Il s'agit de données qui peuvent fournir, entre autres, des informations sur l'origine des fonds, la propriété des biens.*

- *les actes et décisions relatifs à la* ***capacité juridique et les décisions d'administration des biens ou de la personne visés à l'article 1250, premier alinéa, du Code judiciaire ; e (article 3, 9°/1) et le cas échéant, l'existence du certificat d'identité et de signature, tel que prévu par la loi du 9 juillet***

2001 établissant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification *(article 3, 12°) :*

Ces informations sont nécessaires pour déterminer si le citoyen a effectivement la capacité juridique de passer un contrat en tant qu'adulte et d'interagir numériquement avec d'autres entités privées.

En particulier, l'accès aux données suivantes ***contenues dans le registre des cartes d'identité*** *peut être justifié comme suit :*

- *Pour la* ***réglementation EIDAS*** *et* ***l'identification de la personne pour laquelle les moyens d'identification électronique sont délivrés, ainsi que pour la création d'un certificat qualifié*** *pour les personnes physiques, il doit y avoir un moyen d'identifier de manière unique la personne et de la relier au document d'identité reconnu et valide utilisé à l'origine pour l'identification. Pour ce faire, les données suivantes doivent au moins être collectées par ces entités :*
  - *la date de la demande suivie de la date de délivrance du document de base, de la date de délivrance, de la date d'expiration et, le cas échéant, de la date de destruction ;*
  - *le numéro séquentiel de la carte ;*
  - *les informations indiquant que la carte est valide, expirée ou détruite et, le cas échéant, le motif ;*
  - *le numéro d'identification du registre national des personnes physiques,*

- *Les informations supplémentaires suivantes sont également requises pour l'identification (y compris la vérification de l'identité) par la* ***directive AML UE 2015/849*** *(telle que modifiée par la directive AML 2018/843), qui a été transposée dans la* ***loi belge du 17 sept. 2017*** *(telle que modifiée par la loi du 20 juillet 2020),* ***y compris la photo du sujet en tant 'qu'élément de supplémentaire, mais aussi la capacité juridique et le lieu de résidence.*** *Cette obligation légale s'applique à des secteurs très divers, notamment les entités financières et le secteur des assurances, mais aussi la comptabilité, le secteur des jeux de hasard, les services postaux, le secteur diamantaire, etc. (cf. art. 5 de la loi belge relative à la lutte contre le blanchiment d'argent). Ces éléments de données comprennent :*
  - *la photographie du titulaire correspondant à la photographie de la dernière carte.*
  - *le type de carte ;*
  - *l'indication de l'existence ou de l'absence de la fonction " signature électronique " ;*
  - *la date de la dernière mise à jour ;*

- *Date de la dernière mise à jour concernant la résidence principale.*
- *l'éventuelle mention relative à l'exercice de l'autorité parentale telle que prévue à l'article 374/1 du Code civil* » (mis en gras par l'Autorité).

38. Sur la **possibilité d'accomplir les objectifs poursuivis par la Proposition dans le cadre du Règlement EIDAS tel que récemment réformé**, le demandeur a répondu ce qui suit :

> « *Les attestations d'attributs sont de* ***nouveaux services*** *prévus par les prochaines modifications du règlement EIDAS. Toutefois, cette version révisée du règlement EIDAS n'est* ***pas encore pleinement mise en œuvre et applicable.*** *La pleine application de la version révisée du règlement EIDAS n'est* ***pas attendue avant au moins 2027 et nécessite l'adoption d'actes d'exécution****, alors que le secteur privé a de plus en plus besoin d'accéder à des données fiables provenant de certaines sources authentiques.*
>
> *À cet égard, la proposition s'appuie sur les garanties fournies par les cadres juridiques mis en œuvre pour l'identification et l'authentification (y compris la version actuelle applicable du règlement EIDAS ainsi que la législation belge), tout en s'inspirant de la raison d'être de la version révisée d'EIDAS. La valeur ajoutée de la proposition réside notamment dans la possibilité de répondre à un besoin réel et urgent des citoyens et des entreprises privées qui ne peut être satisfait, à ce jour, par d'autres mesures existantes* » (mis en gras par l'Autorité).

39. L'Autorité s'est aussi interrogée à propos de la modification envisagée de **l'article 6*bis*, § 3, de la Loi de 1991**[33], le recours à un moyen d'identification valide étant une prémisse de l'identification via un schéma d'identification. Une fois que la personne concernée a recours au schéma concerné à l'égard d'une entité (publique ou privée), ou d'un service d'identification électronique, elle est identifiée sur la base du niveau de fiabilité garanti par ce schéma. Dans ces conditions, **l'Autorité ne perçoit pas la portée de la Proposition**. **Elle a interrogé le demandeur afin qu'il clarifie l'obstacle légal/technique concret que celle-ci tente de lever**. L'objectif est-il par exemple que le prestataire du service d'identification (par exemple, Itsme) puisse lui-même mettre à jour les données qu'il a extraites de la carte d'identité de la personne concernée, *lorsque celle-ci a créé son compte et s'est identifiée auprès de lui via ce moyen d'identification (eID)* ? Plutôt que, le cas échéant, de laisser la personne concernée gérer cet aspect ? Le demandeur n'a pas fourni de réponse directe sur ce point, à l'Autorité, mais cette hypothèse semble en tout cas être visée par l'illustration qu'il fournit de l'utilisation qui pourrait être faite de l'application Itsme[34].

---

[33] Voir les considérants nos 14-15.

[34] « *3.3.1. Étape 1 : réception des mises à jour par le [prestataire de services d'identification électronique]*

Mise à jour des données par le citoyen à partir de l'application itsme elle-même

- ***Dans lequel la possibilité de mises à jour par le biais du registre national****, ou par d'autres canaux si nécessaire, est prévue.*

40. La Proposition et les réponses communiquées par le demandeur appellent, les commentaires suivants de la part de l'Autorité.

B) Détermination des finalités de la Proposition – principes

41. Il convient de rappeler premièrement, qu'il incombe au **dispositif** de la Proposition, conformément aux principes de prévisibilité et de légalité consacrés dans les articles 8 CEDH et 22 de la Constitution, ainsi que conformément à l'article 6, 3., al. 2, du RGPD, **de déterminer exhaustivement les finalités du traitement**. S'agissant du traitement de données fondés sur le **consentement de la personne concernée en outre**, comme la CPVP l'a rappelé dans son Avis[35], le consentement ne peut porter que sur une ou plusieurs finalités **spécifiques**. **A cet égard d'emblée, l'Autorité considère que le dispositif de la Proposition doit être développé afin d'identifier clairement les finalités spécifiques concernées[36]**. En l'occurrence, et par exemple, ne constituent pas en elles-mêmes des finalités déterminées et spécifiques : la mise à jour de données[37] ; la simplification administrative ; les fins de conformités ; en général, l'identification et l'authentification.

42. Deuxièmement, et ce point est évoqué plus précisément ci-après concernant une des finalités concrètes et déterminées évoquées dans le commentaire de la Proposition et par le demandeur[38], le dispositif de celle-ci **devrait clairement distinguer ces finalités du service d'identification impliqué dans le schéma d'identification électronique visé par le Règlement EIDAS**. Sur ce point, l'objectif de la Proposition est également (comme le Règlement EIDAS2[39]) de permettre aux prestataires de services d'identification électronique visés par le Règlement EIDAS **d'offrir d'autres services**, d'échanges de données entre la personne concernée et les entités aux services desquelles elle recourt, via des sources authentiques. Le dispositif de la Proposition doit prévoir à cet égard, que

---

- *Une description complète du processus et des alternatives possibles est fournie ici.*
- *Grâce à la rubrique "Plus d'informations", l'utilisateur peut s'informer davantage sur ses droits.*

Acceptation et activation du partage des données du registre national

- *En option, immédiatement après la création du compte itsme®.*
- *A tout autre moment lors de l'utilisation de l'application itsme*
- *La désactivation reste possible de la même manière simple dans l'application itsme.*

Notification de la mise à jour des données personnelles via le registre national

- *L'application itsme indique lorsqu'une mise à jour des données a été effectuée*
- *Cette notification rappelle à l'utilisateur la possibilité de retirer son consentement* » (mis en gras par l'Autorité).

[35] Considérant n° 28.

[36] L'article 5*ter*, § 2, 2°, de la Loi RN est plus élaboré à ce sujet, sans préjudice de l'analyse éventuelle que nécessiterait cette disposition. (Par exemple,

[37] Au passage, l'Autorité attire l'attention du demandeur sur le fait qu'en vertu de l'article 5, 1., du RGPD, les données doivent être « *si nécessaire* », tenues à jour. En tout état de cause, la nécessité de tenir des données à jour devra être évaluée à l'aune de la finalité poursuivie par le traitement.

[38] Voir les considérants nos 46 et s.

[39] Voir le considérant n° 38.

dès l'offre de son service d'identification électronique à la personne concernée, **de tels autres services doivent être distingués** (du service d'identification électronique visé par le Règlement EIDAS) et demeurer optionnels, conformément à l'objectif du Projet.

43. A cet égard, l'Autorité souligne d'emblée que plutôt que de mettre en œuvre des nouveaux types de services de droit belge, il serait probablement **préférable d'attendre la mise en œuvre des portefeuilles européens d'identité numérique et des attestations d'attributs[40] visés par le Règlement EIDAS2**, dans la mesure où ceux-ci peuvent répondre aux préoccupations du demandeur. Il s'agit d'une considération importante **à prendre en considération dans le cadre de la réalisation d'une analyse d'impact[41]**.

44. Troisièmement, l'Autorité est d'avis que la Proposition doit prévoir une disposition **interdisant le traitement ultérieur des données** qui seraient communiquées, **à toute autre fin**, à l'aune de ce que prévoit l'article **5*ter*, § 5, al. 1er, de la Loi RN**.

45. Cela étant précisé, concrètement s'agissant des finalités, la Proposition et le demandeur dans ses réponses évoquent principalement **deux finalités concrètes** : la mise en œuvre des obligations d'identification dans le cadre de la lutte contre le blanchiment d'argent (« *know your customer* ») (ci-après, « **Finalité AML** ») et la mise en œuvre du Règlement EIDAS lui-même (ci-après, « **Finalité EIDAS** »).

C) Finalité « AML » (flux de données vers le prestataire de service d'identification électronique et flux de données vers les entités assujetties)

46. S'agissant de la mise en œuvre des obligations d'identification découlant de la Loi du 18 septembre 2017 *relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces* (ci-après, « **Loi AML** ») et des directives européennes que celle-ci transpose, les commentaires suivants s'imposent.

47. Premièrement, l'Autorité relève que **s'il** est effectivement **incontestable** que le recours à un service d'identification électronique de garantie élevé **contribuera à la mise en œuvre des obligations**

[40] Le considérant n° 62 du Règlement EIDAS2 s'énonce d'ailleurs comme suit :

« *L'identification électronique sécurisée **et la fourniture d'attestations d'attributs** devraient offrir davantage de souplesse et de solutions au secteur des services financiers en ce qui concerne l'identification des clients **et l'échange des attributs spécifiques nécessaires pour** respecter, par exemple, les obligations de vigilance à l'égard de la clientèle prévues par un futur règlement établissant l'autorité de lutte contre le blanchiment de capitaux et les exigences en matière d'adéquation découlant du droit en matière de protection des investisseurs, ou pour permettre le respect d'exigences en matière d'authentification forte du client pour l'identification en ligne à des fins de connexion au compte et d'exécution de transactions dans le domaine des services de paiement* » (mis en gras par l'Autorité).

[41] Voir le considérant n° 27.

consacrées dans cette législation dans l'environnement numérique[42], **l'objectif des services d'identification** électronique visés par le Règlement EIDAS **n'équivaut pas à la mise en œuvre des obligations** d'identification des clients consacrées dans les législations européenne et nationale dans le cadre de la lutte contre le blanchiment d'argent. D'ailleurs, et sans pouvoir entrer ici dans l'analyse approfondie de cette législation, la loi précitée consacre une obligation à degré variable dépendant du niveau de risque du client[43] et de l'hypothèse dans laquelle se trouve la personne concernée, les informations obtenues par l'utilisation de moyens d'identification électroniques agréés y apparaissent comme un moyen parmi d'autres d'obtenir des informations au sujet du client[44], et, au-delà des données énumérées s'agissant des clients ne constituant pas un risque faible[45] (soit, s'agissant d'une personne physique, « *son nom, son prénom, ses lieu et date de naissance et, dans la mesure du possible, son adresse* »[46]), la loi ne définit pas quelles sont les « *informations complémentaires* » qui pourraient devoir être collectées dans le cadre d'un risque élevé[47, 48].

---

[42] Voir d'ailleurs notamment l'article 13, 1., a), de la **Directive (UE) n° 2015/849** du Parlement européen et du Conseil du 20 mai 2015 *relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n o 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission*, selon lequel :

« *Les mesures de vigilance à l'égard de la clientèle comprennent:*

a) l'identification du client et la vérification de son identité, sur la base de documents, de données ou d'informations obtenus d'une source fiable et indépendante, y compris, le cas échéant, les moyens d'identification électronique et les services de confiance pertinents prévus par le règlement (UE) n o 910/2014 du Parlement européen et du Conseil (1), ou tout autre processus d'identification sécurisé, électronique ou à distance, réglementé, reconnu, approuvé ou accepté par les autorités nationales concernées ».

Voir également plus récemment, l'article 22, 6., du **Règlement (UE) n° 2024/1624** du Parlement européen et du Conseil du 31 mai 2024 *relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme* (applicable à partir du 10 juillet **2027**), qui prévoit que les informations, documents et données nécessaires à la vérification de l'identité du client doivent être obtenues via :

« *a) la présentation d'un document d'identité, du passeport ou d'un document équivalent et, lorsqu'il y a lieu, l'obtention d'informations en provenance de sources fiables et indépendantes, consultées directement ou fournies par le client;*

b) l'utilisation de moyens d'identification électronique qui satisfont aux exigences du règlement (UE) no 910/2014 en ce qui concerne les niveaux de garantie «substantiel» ou «élevé» et les services de confiance qualifiés pertinents prévus par ledit règlement ».

Cette disposition est à lire en combinaison avec l'article 28, 1., d), et e), du même Règlement, une norme technique devant être adoptée en la matière par la future Autorité de lutte contre le blanchiment de capitaux et le financement du terrorisme (ALBC).

Il convient de noter que le Règlement prévoit des délais (1 an au plus tard si risque élevé, ou 5 ans) et hypothèses dans lesquelles doivent être mises à jour les données (délais susceptibles d'être allongés lorsque le degré de risque est peu élevé, voir l'article 33 du Règlement).

Dans l'hypothèse des mesures de vigilances renforcées (risque plus élevé), le Règlement prévoit également la possibilité de collecter des informations supplémentaires sur le client (voir l'article 34 du Règlement).

[43] Voir l'article 26 de la Loi AML.

[44] Voir l'article 27, § 1er, al. 1er, 2°, de la Loi AML.

[45] Concernant les risques faibles, voir l'article 26, § 3, de la Loi AML. L'Autorité relève sur ce point que dans ce cas, l'entité assujettie ne « peut » pas seulement limiter le nombre d'informations recueillies mais le devra bien, le cas échéant, en exécution du principe de minimisation des données consacré dans l'article 5, 1., c), du RGPD.

[46] Article 26, § 2, 1°, de la Loi AML.

[47] L'article 26, § 4, de la Loi AML prévoit ce qui suit :

« *Lorsqu'il ressort de l'évaluation individuelle des risques réalisée conformément à l'article 19, § 2, alinéa 1er, que le risque associé au client et à la relation d'affaires ou à l'opération est élevé, l'entité assujettie s'assure avec une attention accrue que les informations qu'elle recueille en application du paragraphe 2 lui permettent de distinguer de façon incontestable la personne concernée de toute autre. Au besoin, elle recueille à cette fin des informations complémentaires* ».

[48] Le **Règlement (UE) n° 2024/1624** du Parlement européen et du Conseil du 31 mai 2024 relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (applicable à partir du 10 juillet 2027), prévoit en son article 22, 1., a), afin d'identifier les personnes physiques, la collecte de tous les prénoms et les

48. Deuxièmement, cela étant dit, le droit positif prévoit déjà et à juste titre, que **les informations collectées par l'entité assujettie** via en substance, **les services d'identification électroniques** agréés (mais aussi, les services de confiance), **peuvent être traitées ultérieurement** aux fins de l'identification dans le cadre de la Loi AML[49]. A cet égard, l'Autorité attire l'attention du demandeur sur le fait que si la Proposition entend fonder une **collecte initiale et additionnelle de données**, **au-delà des données obligatoires d'identification nécessitées par le Règlement EIDAS** (nom(s), prénom(s), date de naissance, numéro d'identification national)**[50]**, et ce, **aux fins de la mise en œuvre des obligations d'identifications consacrés aux articles pertinents de la Loi AML**, le **dispositif de la Proposition** doit **explicitement prévoir cette finalité et distinguer ce nouveau service** que pourrait prester le prestataire de service d'identification électronique, du service d'identification électronique visé par le Règlement EIDAS. En effet, la Proposition permettrait dans un tel scénario une collecte initiale supplémentaire de données, qui ne sont pas nécessaires à l'accomplissement de l'identification électronique en vertu du Règlement EIDAS.

49. A cet égard cependant, l'Autorité est d'avis que le demandeur **pourrait privilégier le recours aux portefeuilles européens d'identité numérique et aux attestations électroniques d'attributs qualifiées** visées par le Règlement EIDAS2[51], s'agissant de nouveaux services qui feront l'objet de **cadres normatifs et techniques européens et belges aboutis et harmonisés, comportant des garanties spécifiques[52]**. Une fois de plus, il s'agit d'une réflexion importante **à prendre en considération dans le cadre de la réalisation d'une analyse d'impact[53]**.

50. Troisièmement, l'Autorité relève que le droit positif **prévoit également déjà, que les entités assujetties peuvent avoir accès au RN**, via les associations professionnelles désignées par le Roi, s'agissant de l'identification des personnes qui ne sont pas présentes lors de leur identification, mais encore, de la mise à jour des données d'identification relatives aux clients[54]. **Il appartient par conséquent au demandeur de démontrer la nécessité de prévoir un accès additionnel, via**

noms, du lieu et de la date complète de naissance, des nationalités ou de l'apatridie et du statut de réfugié ou du statut conféré par la protection subsidiaire, le cas échéant, ainsi que le numéro d'identification national, le cas échéant, du lieu de résidence habituelle ou, en l'absence d'adresse fixe correspondant à une résidence légale dans l'Union, l'adresse postale à laquelle la personne physique peut être jointe et, s'il est disponible, le numéro d'identification fiscale.

[49] Voir l'article 27, § 1er, 2° et 3°, de la Loi AML.

[50] Voir le considérant n° 28.

[51] Voir la note de bas de page n° 22.

[52] Voir le considérant n° 51, premier tiret.

[53] Voir le considérant n° 27.

[54] Voir l'article 28 de la Loi AML.

un autre intermédiaire (le service d'identification électronique), au RN[55]. C'est une démonstration importante dans le cadre de la réalisation d'une analyse d'impact[56].

51. Quatrièmement, et sans préjudice des commentaires précédents, les dispositions de la Loi AML prévoient en matière d'identification des clients des **obligations**. Autrement dit, le traitement des données à caractère personnel dans ce contexte est **fondé sur une obligation légale[57] et non sur le consentement de la personne concernée**. Il s'agit par conséquent d'une hypothèse très différente (en fait et en droit) de celle visée par l'article 5*ter* de la Loi RN, **qui nécessite un encadrement normatif spécifique**, où le **rôle reconnu à l'accord (au contrôle)** de la personne concernée doit **spécifiquement être encadré par le dispositif de la Proposition**. En l'occurrence, et conformément aux intentions annoncées dans la Proposition et par le demandeur, l'Autorité est d'avis que le dispositif de celle-ci devrait, **sans préjudice des obligations consacrées dans le RGPD[58]** :

- Prévoir que des **garanties similaires à celles consacrées dans le Règlement EIDAS en matière de transparence et de contrôle de la personne concernée dans le cas des portefeuilles européens d'identité numérique** s'appliquent au service mis en place par la Proposition. Il s'agit en particulier de rendre applicable des règles similaires (une adaptation étant nécessaire, *mutatis mutandis*) à celles consacrées dans l'article 5*bis*, 4., a)[59] et d)[60], 5.,

[55] Il s'agit parmi d'autres, d'un élément important à prendre en considération dans le cadre de l'analyse d'impact du Projet, voir le considérant n° 27.

[56] Voir le considérant n° 27.

[57] Article 6, 1., c), du RGPD.

[58] Ces points également, sont pertinents dans le cadre de la réalisation d'une analyse d'impact, voir le considérant n° 27.

[59] « *4. Les portefeuilles européens d'identité numérique permettent à l'utilisateur, d'une manière conviviale, transparente et qui garantit la traçabilité pour l'utilisateur:*

a) de demander, d'obtenir, de sélectionner, de combiner, de stocker, de supprimer, de partager et de présenter en toute sécurité, sous le seul contrôle de l'utilisateur, des données d'identification personnelle et, lorsqu'il y a lieu, en combinaison avec les attestations électroniques d'attributs, de s'authentifier à l'égard de parties utilisatrices, en ligne et, le cas échéant, en mode hors ligne, en vue d'accéder à des services publics et privés, tout en veillant à ce qu'une divulgation sélective de données soit possible ».

[60] « *4. Les portefeuilles européens d'identité numérique permettent à l'utilisateur, d'une manière conviviale, transparente et qui garantit la traçabilité pour l'utilisateur:*

d) d'accéder à un journal de toutes les transactions effectuées avec le portefeuille européen d'identité numérique, au moyen d'un tableau de bord commun qui permet à l'utilisateur:

i) de consulter une liste à jour des parties utilisatrices avec lesquelles l'utilisateur a établi une connexion et, le cas échéant, de toutes les données échangées;

ii) de demander facilement l'effacement par une partie utilisatrice de données à caractère personnel en vertu de l'article 17 du règlement (UE) 2016/679;

iii) de signaler facilement une partie utilisatrice à l'autorité nationale chargée de la protection des données compétente, lorsqu'une demande de données présumée illégale ou suspecte est reçue; ».

a), iv), ix), x), b), d), e)[61], 10.[62], 14. (sans pour autant permettre la demande contraire de l'utilisateur, s'agissant d'une hypothèse étrangère aux objectifs de la Proposition)[63], 15.[64], 16., a) (sans possibilité d'autorisation expresse toutefois, ne s'agissant pas d'une hypothèse visée par la Proposition)[65], du Règlement EIDAS ;

- Envisager de permettre à l'aune de **l'article 5*ter*, § 3, al. 2, de la Loi RN**, que la personne concernée puisse **agir à la source des données, à savoir <u>auprès du RN</u>** lui-même ;

- Prévoir que les **articles 4, 11), et 7 du RGPD s'appliquent aux divers choix de la personnes concernées dans le cadre de** : la mise en œuvre de la **collecte initiale** des données nécessaires par le prestataire de service d'identification électronique, selon le niveau

---

[61] « *5. En particulier, les portefeuilles européens d'identité numérique:*

a) prennent en charge des protocoles et interfaces communs:

[…]

iv) pour permettre à l'utilisateur d'autoriser une interaction avec le portefeuille européen d'identité numérique et d'afficher un label de confiance de l'UE pour le portefeuille européen d'identité numérique;

[…]

x) pour signaler une partie utilisatrice à l'autorité nationale chargée de la protection des données compétente lorsqu'une demande de données présumée illégale ou suspecte est reçue;

[…]

b) ne fournissent aux prestataires de services de confiance chargés de la fourniture d'attestations électroniques d'attributs aucune information concernant l'utilisation de ces attestations électroniques;

[…]

d) satisfont aux exigences énoncées à l'article 8 quant au niveau de garantie élevé, tel qu'il est appliqué en particulier aux exigences concernant la preuve et la vérification d'identité, et à la gestion des moyens d'identification électronique et à l'authentification;

e) dans le cas de l'attestation électronique d'attributs intégrant des politiques de divulgation, mettent en œuvre le mécanisme approprié pour informer l'utilisateur que la partie utilisatrice ou l'utilisateur du portefeuille européen d'identité numérique qui demande cette attestation électronique d'attributs a l'autorisation d'accéder à cette attestation; ».

[62] « *10. Les fournisseurs de portefeuilles européens d'identité numérique garantissent que les utilisateurs peuvent facilement demander une assistance technique et signaler des problèmes techniques ou tout autre incident ayant une incidence négative sur l'utilisation des portefeuilles européens d'identité numérique* ».

[63] « *14. Les utilisateurs exercent un contrôle total sur l'utilisation de leur portefeuille européen d'identité numérique et des données qui y figurent. Le fournisseur du portefeuille européen d'identité numérique ne collecte pas les informations sur l'utilisation du portefeuille européen d'identité numérique qui ne sont pas nécessaires à la fourniture des services liés au portefeuille européen d'identité numérique, et il ne combine pas non plus des données d'identification personnelle ou d'autres données à caractère personnel stockées ou relatives à l'utilisation du portefeuille européen d'identité numérique avec des données à caractère personnel provenant de tout autre service offert par ce fournisseur ou de services tiers qui ne sont pas nécessaires à la fourniture des services liés au portefeuille européen d'identité numérique, à moins que l'utilisateur n'ait fait expressément la demande contraire. Les données à caractère personnel relatives à la fourniture du portefeuille européen d'identité numérique sont maintenues séparées, de manière logique, de toute autre donnée détenue par le fournisseur du portefeuille européen d'identité numérique. Si le portefeuille européen d'identité numérique est fourni par des parties privées conformément au paragraphe 2, points b) et c), du présent article, les dispositions de l'article 45 nonies, paragraphe 3, s'appliquent mutatis mutandis* ».

[64] « *15. L'utilisation des portefeuilles européens d'identité numérique a lieu sur une base volontaire. Les personnes physiques ou morales qui n'utilisent pas les portefeuilles européens d'identité numérique ne sont en aucune façon limitées ou désavantagées dans l'accès aux services publics et privés, l'accès au marché du travail et la liberté d'entreprise. Il reste possible d'accéder aux services publics et privés par d'autres moyens d'identification et d'authentification existants* ».

[65] « *16. Le cadre technique du portefeuille européen d'identité numérique:*

a) ne permet pas aux fournisseurs d'attestations électroniques d'attributs ou à toute autre partie, après la délivrance de l'attestation d'attributs, d'obtenir des données permettant de suivre, de relier ou de corréler les transactions ou le comportement de l'utilisateur, ou de prendre connaissance des transactions ou du comportement de l'utilisateur d'une autre manière, sauf autorisation expresse de l'utilisateur ».

d'identification requis par la Finalité AML *in concreto* (risque faible, normal ou élevé), et peu importe la source de cette collecte initiale (la carte d'identité ou le RN[66]) ; la **communication** des données nécessaires à l'entité assujettie, selon le niveau d'identification requis par la Finalité AML *in concreto* (risque faible, normal ou élevé) ; la **mise à jour** des données nécessaires par le prestataire de service d'identification électronique, selon le niveau d'identification requis par la Finalité AML *in concreto* (risque faible, normal ou élevé) ; la **communication des données nécessaires mises à jour** à l'entité assujettie, selon le niveau d'identification requis par la Finalité AML *in concreto* (risque faible, normal ou élevé).

52. Cinquièmement, **le dispositif de la Proposition doit être adapté de manière telle qu'il ne vise que les données** issues du RN et des Registres des cartes d'identité et cartes d'étranger **nécessaires à la mise en œuvre des obligations d'identification visées par la Loi AML, selon le niveau de risque**, ***in concreto***. ***Par exemple***, l'Autorité ne voit pas pour quelle raison dans ce contexte, la photo (et même, les photos, le Registre des cartes d'identité contenant également d'anciennes photos) du titulaire de la carte d'identité devrai(en)t être communiquées aux entités assujetties. Une telle donnée apparaît *a priori* et d'emblée, disproportionnée.

53. Sixièmement, l'Autorité **ne perçoit pas de raison de s'écarter de la logique acquise dans les articles 5 et 5*ter* de la Loi RN** nécessitant une **autorisation du ministre de l'Intérieur, pour chaque organisme concerné** (les entités assujetties) par le flux de données, en vue d'accéder aux données concernées. Le fait que le prestataire du service d'identification électronique concerné doive lui-même disposer d'une autorisation n'est pas déterminant à cet égard. Il s'agit pour rappel d'une condition également applicable aux autorités publiques qui dans l'exercice de leurs missions d'intérêt public, entendent accéder au RN ou aux Registres des cartes d'identité et cartes d'étranger. Cette condition est notamment importante sous l'angle de la responsabilité qui incombe au RN en tant que responsable du traitement[67].

54. Septièmement, **l'article 5*quater*, § 3,** de la loi RN tel que proposé, inspiré de l'article 5*ter*, § 3, de la Loi RN, **devrait être complété** dès lors qu'il ne vise que l'hypothèse de la cessation de la relation contractuelle entre la personne concernée et le prestataire de service *d'identification électronique*. **Or le dispositif de la Proposition doit également encadrer la cessation de la relation contractuelle entre la personne concernée et l'entité qui reçoit les données et mises à jour** via le prestataire de service d'identification électronique. Dans la logique de la Proposition et de l'actuel article 5*ter* de la Loi RN, cela implique que l'entité assujettie soit obligée de notifier la cessation de la

[66] Une série de données visées par la Proposition ne sont pas reprises sur la carte d'identité électronique.

[67] En ce sens, voir par exemple l'Avis n° 34/2024 du 15 janvier 2024 *concernant une Proposition de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour (CO-A-2024-139)*, considérants nos 16 et 17.

relation contractuelle au prestataire du service d'identification électronique, et que celui-ci en tire les conséquences sur le plan de la protection des données[68].

55. Huitièmement, l'Autorité attire l'attention du demandeur sur la **nécessité pour l'entité assujettie, d'adapter en temps réel le répertoire des références qui serait utilisé** pour la mise à jour automatique des données, en fonction des choix opérés par la personne concernée[69]. En effet, si initialement, la personne concernée présente un risque faible, il n'y a pas de raison légitime de collecter d'emblée (et le cas échéant, de recevoir les mises à jour) les données qui ***pourraient*** être nécessaires à l'avenir, si le niveau de risque de la personne concernée évoluait. Inversement, si le niveau de risque que présente une personne concernée est abaissé, les conséquences doivent en être tirées directement sur le plan de la protection des données[70].

56. Neuvièmement, l'Autorité observe que la Proposition ne prévoit pas l'application de **l'article 5*ter*, § 5, al. 1er, de la Loi RN**, prévoyant la fixation par le Roi d'un **tarif** au profit du service compétent du RN[71]. Or il est fondamental d'évaluer **l'impact (financier) du Projet pour le RN,** au regard de l'extension de ses missions, **afin de garantir que celui-ci**, en tant que responsable du traitement, **soit matériellement capable d'exécuter les obligations qui lui incombent en vertu du RGPD**, en particulier au titre de **l'*accountability*[72]**.

57. Dixièmement enfin, l'Autorité rappelle sa pratique d'avis constante selon laquelle une autorité publique (ou une entité privée) est en principe **responsable du traitement** de données nécessaire à la mise en œuvre de la mission d'intérêt public qui lui incombe (ou qui relève de l'autorité publique dont elle

[68] En tout état de cause, cela implique la cessation de la communication des données à l'entité assujettie, et dans le cas où les mêmes données ne sont pas traitées à d'autres fins par le prestataire de service d'identification électronique, la suppression de ces données et l'adaptation du répertoire de références.

[69] Bien qu'il ne s'agisse pas ici d'analyser l'article 5*ter* de la Loi RN, ce commentaire y est également pertinent. S'agissant par exemple d'une situation dans laquelle un produit défectueux doit être rappelé, ou d'une situation dans laquelle naît un litige, c'est au moment de ces événements, qu'une adresse à jour est nécessaire.

[70] Voir la note de bas de page n° 68.

[71] Ce point doit également être lu en combinaison avec le considérant n° 53 (concernant les autorisations du ministre de l'Intérieur).

[72] Articles 5, 2., et 24 du RGPD. C'est encore, parmi d'autres, un élément important à prendre en considération dans le cadre de l'analyse d'impact du Projet, voir le considérant n° 27.

est investie)[73], ou nécessaire à l'obligation légale qui la lie[74], en vertu de la norme concernée[75, 76]. L'Autorité est d'avis que la Proposition implique, dans la collecte et mise à jour automatisée des données concernées, **une action conjointe des trois catégories d'acteurs impliqués** par elle, **au service de la Finalité « AML »,** de telle sortes que ceux-ci agiront comme responsables conjoints du traitement.

D) Finalité « EIDAS » (flux de données vers le prestataire de service d'identification électronique)

58. S'agissant de la finalité de **mise en œuvre du Règlement EIDAS** en ce qui concerne **le flux de données** du RN et des Registres des cartes d'identité et carte d'étranger **vers les prestataires de services d'identification électronique**, l'Autorité est d'avis qu'avant tout, **l'exposé des motifs de la Proposition devrait expliciter clairement le problème que celui-ci entend solutionner**. Ce problème est à prendre en considération comme point de départ, dans le cadre d'une analyse d'impact[77]. En effet, force est de constater qu'à ce jour **en droit positif**, même en l'absence des nouvelles règles prévues par la Proposition, la Belgique dispose déjà de deux schémas d'identification présentant un niveau de **garantie élevé[78]**.

59. L'Autorité ne perçoit pas le problème que la Proposition entend résoudre, par exemple s'agissant de la **vérification de la validité** de la carte d'identité[79]. En effet, en cas de perte, vol ou destruction de la

[73] Article 6, 1., e), du RGPD .

[74] Article 6, 1., c), du RGPD .

[75] Voir notamment : avis n° 143/2023 du 29 septembre 2023 *concernant un avant-projet de décret portant assentiment à l'accord de coopération entre la Région wallonne et la Communauté française désignant l'intégrateur de services de la Région wallonne et de la Communauté française et un projet d'accord de coopération relatif à la création du service commun aux Gouvernements Wallon et de la Communauté française, dénommé Banque Carrefour d'échange de données (non soumis à assentiment) (CO-A-2023-375), et concernant un avant-projet de décret portant assentiment à l'accord de coopération entre la Région wallonne et la Communauté française désignant l'intégrateur de services de la Région wallonne et de la Communauté française et un projet d'accord de coopération relatif à la création du service commun aux Gouvernements Wallon et de la Communauté française, dénommé Banque Carrefour d'échange de données (non soumis à assentiment) (CO-A-2023-376)* considérants nos 7 et s. ; avis de l'Autorité n° 83/2023 du 27 avril 2023 *concernant un avant-projet d'ordonnance modifiant l'ordonnance du 4 avril 2019 portant sur la plate-forme d'échange électronique des données de santé (CO-A-2023-147)*, considérant n° 11 ; 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. ; l'avis n° 227/2022 du 29 septembre 2022 *concernant un avant-projet de décret relatif aux données ouvertes et à la réutilisation des informations du secteur public (CO-A-2022-209)*, considérants nos 17-23 ; 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.

[76] Avis n° 154/2023 du 20 octobre 2023 *concernant un avant-projet de décret et ordonnance conjoints portant le code bruxellois de la gouvernance et de la donnée (CO-A-2023-407)*, considérant n° 167.

[77] Voir le considérant n° 27.

[78] Voir le considérant n° 28.

[79] Voir le considérant n° 15.

carte d'identité, les **certificats sont <u>révoqués</u> et ce statut peut (et doit) notamment toujours être vérifié** (par exemple, via un client OSCP-« *Online Certificate Status Protocol* »)[80,81]. En outre, les certificats ont une date de validité qui correspond à la date de validité de la carte d'identité elle-même.

60. En ce qui concerne la **<u>mise à jour</u> des données** provenant de la carte d'identité, **concernant les données *nécessaires à l'identification dans le cadre d'un service d'identification électronique visé par le Règlement EIDAS*** (car pour les données supplémentaires, la finalité du traitement change[82]), de nouveau, les schémas d'identification précités sont en droit positif, supposés offrir un niveau de garantie élevé, de manière telle qu'il est théoriquement difficilement envisageable qu'ils ne fournissent pas des données d'identification à jour. Le changement de nom et le décès par exemple, entraînent une **annulation de la carte d'identité, qui implique une destruction de celle-ci et une révocation des fonctions électroniques**[83]. Comme cela vient d'être rappelé, l'information selon laquelle des certificats sont révoqués est disponible doit être vérifiée.

---

[80] Voir notamment SPF Intérieur, DG Identité et Affaires citoyennes, Population et Documents d'identité, « Instructions générales relatives aux cartes d'identité électronique Belges », à jour le 5 juillet 2023, disponible sur

<u>https://www.ibz.rrn.fgov.be/fileadmin/user_upload/fr/cartes/eid/instructions/IG-eID-FR-05072023.pdf</u>, dernièrement consulté le 05/02/2025). Voir également l'article 6 de l'arrêté royal du 26 mars 2003 *relatif aux cartes d'identité* (non encore en vigueur selon la législation consolidée disponible via le SPF Justice ; voir sur ce point l'article 12 de l'arrêté royal du 10 décembre 2019 *modifiant l'arrêté royal du 25 mars 2003 relatif aux cartes d'identité et l'arrêté royal du 19 avril 2014 relatif aux cartes d'identité délivrées par les postes consulaires de carrière ; le ministre de l'Intérieur est compétent pour déterminer l'entrée en vigueur de cette disposition*). Voir aussi certipost, « Politique belge de Certification et Déclaration de Pratique pour l'infrastructure PKI eID Citizen CA », v. 5.0, 03/09/2024, disponible sur

<u>https://repository.eid.belgium.be/downloads/citizen/fr/CPS_CitizenCA_BRCA34.pdf</u>, dernièrement consulté le 10/02/2025, pp. 29-32.

[81] **Quant aux certificats**, voir <u>https://repository.eid.belgium.be/index.php?lang=fr</u> ;

<u>https://repository.eid.belgium.be/index.php?item=status&lang=fr</u> ; <u>https://stage-pki.belgium.be/</u> ; dernièrement consultés le 05/02/2025. Les autorités de certification (**certipost**, à la fois « Citizen CA » et « Belgium Root CA ») actives dans un schéma de *public key infrastructure* tel que celui de l'eID, fournissent notamment les services nécessaires à la vérification de la validité des certificats émis. Et, dans le contexte de « Citizen CA », « [l]*es parties se fiant au certificat doivent utiliser les ressources en ligne que la CA met à leur disposition via son référentiel afin de vérifier l'état des certificats avant de s'y fier. La CA met à jour en conséquence l'OCSP, le service de vérification du statut de la certification par interface web, les CRL et les Delta CRL. Les CRL sont actualisées fréquemment, au minimum toutes les trois heure* », certipost, « Politique belge de Certification et Déclaration de Pratique pour l'infrastructure PKI eID Citizen CA », v. 5.0, 03/09/2024, disponible sur

<u>https://repository.eid.belgium.be/downloads/citizen/fr/CPS_CitizenCA_BRCA34.pdf</u>, dernièrement consulté le 10/02/2025, p. 30.

Le **RN** et les communes jouent eux-mêmes également et directement un rôle dans le contexte de cette PKI (dans le cadre de « **Citizen CA** ») comme autorité d'enregistrement et autorités d'enregistrement locales. Ils sont notamment responsables de la validation de l'identité des citoyens, de l'enregistrement des données à certifier, et sont responsables de l'autorité de suspension et de révocation, soit l'entité qui suspend et/ou révoque les certificats. Voir certipost, « Politique belge de Certification et Déclaration de Pratique pour l'infrastructure PKI eID Citizen CA », v. 5.0, 03/09/2024, disponible sur

<u>https://repository.eid.belgium.be/downloads/citizen/fr/CPS_CitizenCA_BRCA34.pdf</u>, dernièrement consulté le 10/02/2025, p. 16. Pour ce qui concerne « Belgium Root CA », voir SPF Stratégie et Appui, DG Transformation digitale, « Belgian Certificate Policy & Practice Statement for eID PKI Infrastructure Belgium Root CA», v3.0.5, disponible sur <u>https://stage-pki.belgium.be/resources/BRCA%20CPS%20V3.05.pdf</u>, dernièrement consulté le 10/02/2025.

[82] Voir *mutatis mutandis*, les considérants nos 47, 48. A propos des données concernées, voir le considérant n° 28.

[83] Voir les « Instructions générales relatives aux cartes d'identité électronique Belges », citée à la note de bas de page n° 80, pp. 75-76. Au-delà de la simple hypothèse de l'identification, lorsqu'il est également question de signature électronique, le certificat qualifié de signature n'est pas activité sur la carte d'identité des personnes mineures, et lorsque le juge de paix décide de l'incapacité de signer ou de s'authentifier d'une personne au moyen de la carte d'identité électronique, les certificats qualifiés de signature ou d'authentification figurant sur la carte d'identité sont révoqués (voir l'article 6, § 7, als 3 et 4, de la Loi de 1991).

61. L'Autorité relève par ailleurs que si le niveau de fiabilité de l'identification était mis en péril par l'absence de tout ou partie des flux de données prévus par la Proposition – ce qui n'apparaît toutefois *a priori* pas être le cas, compte-tenu de ce qui vient d'être rappelé –, l'on pourrait s'interroger sur l'efficacité de laisser reposer entièrement la solution de ce problème sur le consentement des personnes concernées.

62. Pour ce qui va **au-delà des données d'identification de la personne concernée dans le cadre du Règlement EIDAS**, l'Autorité se réfère *mutatis mutandis*, aux développements précédents qui incluent le flux de données à destination du prestataire de service d'identification électronique.

E) Autres finalités spécifiques

63. Si la Proposition entendait prévoir d'autres finalités spécifiques, à savoir d'autres services d'échanges de données que pourraient mettre en œuvre les prestataires de service d'identification électronique visés par le Règlement EIDAS, il conviendrait d'une part, de mener une réflexion au sujet de la finalité envisagée telle que celle menée par l'Autorité concernant la Finalité « AML », et d'autre part, d'adapter *mutatis mutandis*, le dispositif et l'exposé des motifs du Projet (**considérants nos 46-57**). L'Autorité réserve son analyse à ce sujet.

II.3. Conclusion – motifs

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

1. Bien que l'intention de l'Amendement puisse être louable en ce que celle-ci pourrait s'inscrire dans l'objectif de la mise en œuvre du Règlement EIDAS2 en droit belge, il apparaît néanmoins prématuré d'accorder dès maintenant, un effet légal particulier à « *l'application officielle 'portefeuille numérique belge'* » qui d'une part, n'est pas définie dans le dispositif de l'Amendement, et d'autre part, ne peut encore exister légalement comme portefeuille d'identité numérique au sens du Règlement EIDAS2 dès lors que le cadre normatif et technique consacré par celui-ci n'est pas encore pleinement mis en œuvre et d'application (**considérants nos 5-9**) ;

2. La Proposition doit clarifier quels sont les prestataires qui sont agréés « *par un service public qui, par ou en vertu d'une loi, d'un décret ou d'une ordonnance, a pour mission de fournir un service de gestion des utilisateurs et des accès* », ainsi que les éventuels services publics concernés, et le cadre normatif y applicable, ou omettre la référence à ceux-ci. L'Autorité ne se prononce pas à leur sujet (**considérants nos 19-20**) ;

3. Il est recommandé de réaliser une analyse d'impact à propos du Projet (**considérants nos 22-28**), prenant en particulier en considération les questionnements soulevés dans le présent avis (considérants nos 43 et 49, nécessité de la Proposition au regard du Règlement EIDAS2 ; considérant n°50, accès supplémentaire au RN ; considérant n° 51, choix de la personne concernée et transparence ; considérant n° 52, données concernées ; considérant n° 53, autorisations du ministre de l'Intérieur ; considérant n° 54, cessation de la relation contractuelle ; considérant n° 56, impact financier pour le RN ; considérant n° 58, problème à résoudre dans le cadre de la Finalité « EIDAS »), selon les finalités poursuivies par la Proposition (considérant n° 63);

4. Pour que l'agrément visé par le demandeur puisse constituer la garantie effective qu'il est supposé offrir à la lecture de la Proposition et de sa motivation, il convient de vérifier si et dans quelle mesure celui-ci peut et doit être imposé dans le cadre de la Proposition, et l'AR de 2017 devrait être adapté dès lors qu'il n'a pas été pensé dans l'optique poursuivie par la Proposition (**considérants nos 33-34**) ;

5. Le dispositif de la Proposition doit expliciter, et distinguer du service d'identification visé par le Règlement EIDAS, les finalités déterminées et spécifiques qu'il entend poursuivre dans le cadre des nouveaux échanges de données qu'il permet, et limiter le traitement ultérieur des données collectées à la manière de l'article 5*ter* de la Loi RN (**considérants nos 39-45**) ;

6. Si le demandeur entend maintenir la Finalité « AML » dans la Proposition, alors que d'une part, les entités assujetties disposent déjà d'un accès au RN, et que d'autre part, les portefeuilles européens d'identité numérique et les attestations électroniques d'attributs sont susceptibles de rencontrer l'objectif poursuivi (**considérant n° 49**), celle-ci doit être adaptée afin de : distinguer le nouveau service créé et le service d'identification électronique visé par le Règlement EIDAS (**considérant n° 48**) ; démontrer la nécessité de prévoir un accès additionnel au RN (**considérant n° 50**) ; clarifier le rôle joué par le consentement, et prévoir des garanties spécifiques additionnelles, à l'aune du Règlement EIDAS2 et de l'article 5*ter* de la Loi RN, quant au contrôle dont dispose la personne concernée et quant à la transparence, (**considérant n° 51**) ; cibler de manière limitative les données concernées (**considérant n° 52**) ; prévoir la nécessité de disposer d'une autorisation du ministre de l'Intérieur pour les entités assujetties également (**considérant n° 53**) ; prendre également en considération la cessation de la relation contractuelle avec l'entité assujettie, et y attacher les conséquences dans le cadre du Projet (**considérant n° 54**) ; évaluer si une rémunération du RN est nécessaire afin de garantir sa capacité matérielle d'exécuter ses obligations en tant que responsable du traitement (**considérant n° 56**) ;

7. S'agissant de la Finalité « EIDAS », l'exposé des motifs doit expliciter le problème que la Proposition entend résoudre, l'Autorité ne pouvant le percevoir concrètement, dès lors qu'en droit positif, les services d'identification électroniques notifiés par la Belgique offrent déjà un niveau de garantie élevé (**considérants nos 58-61**) ;

8. Si la Proposition entendait prévoir d'autres finalités déterminées et spécifiques, il conviendrait de mener à l'égard de celles-ci, la réflexion impliquée par le **point n° 6** plus haut, et d'adapter le dispositif en conséquence (**considérant n° 63**).

Pour le Service d'Autorisation et d'Avis,
(sé.) Cédrine Morlière, Directrice