



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.

Eenzijds 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 identificeren¹.
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.....	4
II.2. Het voorstel – Wijziging van de RR-wet en van de wet van 1991	6
II.2.1. Dispositief en motivering van het voorstel	6
II.2.2. Twee categorieën van gegevensstromen en betrokken actoren	10
II.2.3. Verband tussen het voorstel en artikel 5ter van de RR-wet	11
II.2.4. Elektronische identificatie in de eIDAS-verordening ten aanzien van de doelstellingen van het voorstel.....	14
II.2.5. De waarborg die de erkenning krachtens het KB van 2017 vormt	16
II.2.6. Doelstellingen van het voorstel en verwerkte gegevens	18
A) Aanvullende informatie verstrekt door de aanvrager	18
B) Bepaling van de doelstellingen van het voorstel – beginselen	25
C) AML-doelstelling (gegevensstroom naar de dienstverlener van elektronische identificatiemiddelen en gegevensstroom naar de onderworpen entiteiten)	26
D) eIDAS-doelstelling (gegevensstroom naar de dienstverlener van elektronische identificatiemiddelen)	33
E) Andere specifieke doeleinden	35
II.3. Conclusie – redenen	35

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 authenticeren. 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. (definitie³), 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 Digitalisering⁴) een Europese portemonnee voor digitale identiteit uitbouwt en ter beschikking stelt⁵.
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 bevatten⁶. Zoals de aanvrager overigens in een ander antwoord aan de Autoriteit aangeeft, is het normatief kader van de hervormde eIDAS-verordening nog niet van toepassing⁷.

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. 5^{quater}. § 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 onvermijdelijk 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 6bis, § 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 **5ter**, § 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 certificatediensten;

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]²⁰.

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 5ter van de RR-wet.

25. Bovendien, **in tegenstelling tot artikel 5ter 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 **beperkte 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 5ter 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 uitgevoerd¹⁴. De Autoriteit heeft het RR bevestigd over de

¹³ Namelijk de gegevens bedoeld in artikel 6bis, § 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>
[2 k) de in artikel 374/1 van het Burgerlijk Wetboek bedoelde vermelding]"³⁰.

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 blijft¹⁵. 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; geslacht¹⁶. 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-verordening¹⁸.

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-verordening²³, en dat deze portemonnee gepaard gaat met een reeks aanvullende waarborgen op het gebied van transparantie en controle door de betrokkene²⁴.
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 private sector 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.

II.2.5. De waarborg die de erkenning krachtens het KB van 2017 vormt

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 *reikt 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 over²⁸, 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-verordening²⁹. **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 relevant³⁰, 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 ontwikkelingen³¹.

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-verordening³², 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 "wachregister" 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 certificatediensten (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 6bis, § 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-applicatie³⁴.

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 advies³⁵, 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 gegevens³⁷; 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 genoemd³⁸, **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-verordening³⁹) 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

o *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 **5ter, § 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 omgeving⁴², **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 financiële dienstensector 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 cliënt⁴³ 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 verkrijgen⁴⁴. Naast de gegevens die zijn opgesomd voor cliënten die geen laag risico vormen⁴⁵ (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 gereguleerd, 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-wet⁴⁹. 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-verordening⁵¹, 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 cliënten⁵⁴. **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 effectbeoordeling⁵⁶.

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 5ter, § 3, tweede lid, van de RR-wet** toe te staan dat de betrokkene **actie kan ondernemen bij de bron van de gegevens, namelijk bij het RR** 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 RR⁶⁶); 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 5ter 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 verwerkingsverantwoordelijke⁶⁷.
54. Ten zevende **moet artikel 5quater, § 3**, van de RR-wet zoals voorgesteld, geïnspireerd op artikel 5ter, § 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 trekt⁶⁸.

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 maakt⁶⁹. 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 getrokken⁷⁰.
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 RR⁷¹. 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 rust⁷⁴, 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 effectbeoordeling⁷⁷. 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 identiteitskaart⁷⁹. 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 verwerking⁸²), 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.rn.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,
(get.) Cédrine Morlière, directeur