UHASSELT
KNOWLEDGE IN ACTION

KU LEUVEN

Maastricht University

Faculteit Rechten

master in de rechten

Masterthesis

Digitalisering van het bestuursrecht: Itsme on myID

Matthias Van der Donckt

Scriptie ingediend tot het behalen van de graad van master in de rechten, afstudeerrichting overheid en recht

PROMOTOR :
Prof. dr. Steven VAN GARSSE

COPROMOTOR :
dr. Marie DECOCK

2022
2023

De transnationale Universiteit Limburg is een uniek samenwerkingsverband van twee universiteiten in twee landen: de Universiteit Hasselt en Maastricht University.

UHASSELT
KNOWLEDGE IN ACTION

www.uhasselt.be
Universiteit Hasselt
Campus Hasselt:
Martelarenlaan 42 | 3500 Hasselt
Campus Diepenbeek:
Agoralaan Gebouw D | 3590 Diepenbeek

Faculteit Rechten

master in de rechten

Masterthesis

Digitalisering van het bestuursrecht: Itsme on myID

Matthias Van der Donckt

Scriptie ingediend tot het behalen van de graad van master in de rechten, afstudeerrichting overheid en recht

PROMOTOR :
Prof. dr. Steven VAN GARSSE

COPROMOTOR :
dr. Marie DECOCK

Samenvatting

In deze scriptie wordt op zoek gegaan naar een antwoord op de evaluatieve onderzoeksvraag of het Belgisch wettelijk kader betreffende authenticatie bij online overheidsdiensten voldoende aangepast is aan de ontwikkelingen op het niveau van de Europese Unie. Om tot een antwoord op deze centrale onderzoeksvraag te komen worden vier deelvragen beantwoord die het huidige Belgische en Europese kader betreffende authenticatiesystemen alsook de toepassing van de Algemene Verordening Gegevensbescherming en de evoluties die sinds de invoering ervan hebben plaatsgevonden beschrijven. In de scriptie wordt ter beantwoording van de onderzoeksvragen gebruik gemaakt van de klassiek-juridische methode, aangevuld met een functionele rechtsvergelijking van de recent aangenomen Nederlandse regelgeving.

De hard- en software die de eigenlijke authenticatie van een persoon uitvoeren, vallen in de identificatieketen onder de groep van verificator. In België en Vlaanderen wordt deze rol uitgevoerd door de Federal Authentication Service (FAS) die werd opgericht door de FOD BOSA. Om die taak naar behoren uit te voeren, doet de FAS -naast het gebruik van ouderwetsere methoden zoals tokens en de eID kaartlezer- beroep op private partijen zoals Itsme om burgers op een snelle en gebruiksvriendelijke manier te authenticeren. De wettelijke verankering van de erkenning van authenticatiediensten gebeurt in de wet inzake elektronische identificatie. Ter uitvoering van hun opdracht, krijgen de aanbieders van authenticatiemechanismen de status van onderaannemer van de FOD BOSA. De verdere procedure, voorwaarden en gevolgen van de erkenning worden vastgelegd in het uitvoeringskb. elektronische identificatie. Op Europees niveau worden dia de eIDAS en AVG aan de lidstaten bepaalde verplichtingen opgelegd betreffende deze erkenningsvoorwaarden.

Het antwoord of de Belgische wetgeving voldoende aangepast is aan de evoluties rond de eIDAS verordening is niet eenzijdig positief te beantwoorden. in de eerste plaats valt op dat België sinds de invoering van de eIDAS een voortrekkersrol heeft opgenomen door als enige Europese staat te kiezen voor een (deels) private partner in de ontwikkeling van een betrouwbaar en grensoverschrijdend authenticatiemechanisme voor online overheidsdiensten. Toch zullen de nieuw door de Commissie voorgestelde aanpassingen zodanig ingrijpend zijn dat enkele beleidskeuzes zich opdringen. Zo zal er uitgewerkt moeten worden of identiteitsattributen centraal dan wel decentraal beheerd zullen worden en welke rol authenticatiesystemen in de nieuwe "digitale portefeuille" zullen opnemen.

Ook de evaluatie van het Belgisch wetgevend kader betreffende authenticatiemechanismen aan de beginselen zoals vervat in de AVG brengt enkele problemen aan het licht. Zo zou het Belgisch wettelijk kader duidelijkheid moeten verschaffen over de verwerkingsverantwoordelijkheid van de verschillende actoren in de authenticatieketen, moeten er oplossingen gezocht worden voor problemen die kunnen ontstaan betreffende de doorgifte van gegevens aan derde landen, moet er duidelijke regelgeving komen over welke overheden wanneer gebruik moeten of mogen maken van welke authenticatiesystemen, is er bijkomende regelgeving ter implementatie van het beginsel van minimale gegevensverwerking vereist en kan het beveiligings- en controlesysteem op de actoren strenger en onafhankelijker worden georganiseerd.

Woord vooraf

Met het indienen van deze masterproef komt een einde aan een lange academische vorming die mij de kans gaf mijzelf te ontplooien, bestaande vaardigheden te ontwikkelen en nieuwe competenties te verwerven. Met deze masterscriptie -het summum van de rechtenopleiding- hoop ik jullie als lezer ervan te overtuigen dat deze vaardigheden door vele jaren van intense studie voldoende doorontwikkeld zijn om de graad van Master in de Rechten te kunnen behalen.

Deze masterproef behandelt een aspect van het uiterst interessante en snel ontwikkelende digitaliseringsproces van onze overheden. Het laatste jaar is er in België veel te doen geweest over de monopoliepositie van authenticatiedienst "Itsme" en het al dan niet implementeren van "digitale portefeuilles" en "online datakluizen" door overheden op verschillende niveaus. Met deze scriptie hoop ik u wegwijs te kunnen maken in de huidige regulering van deze initiatieven en u een beeld te geven van enkele van de mogelijke gevaren, tekortkomingen en lacunes die hierin momenteel verscholen liggen.

Graag wil ik in de eerste plaats mijn promotor Prof. Dr. Steven van Garsse bedanken voor de hulp bij het afbakenen van het onderzoek en de vakkundige begeleiding en feedback tijdens het schrijfproces. Ik ben ervan overtuigd dat we ook in de toekomst deze succesvolle samenwerking kunnen verderzetten.

Omdat het doorlopen van deze academische opleiding een lang en intensief project is geweest, en het behalen van dit diploma niet enkel mijn eigen verdienste is geweest, ben ik ook dank verschuldigd aan mijn ouders en vrienden voor de steun die ik altijd ben blijven krijgen en aan mijn broer die de ondankbare taak op zich heeft genomen om de klassieke typ- en schrijffouten in dit werk te verbeteren. In het bijzonder zou ik ook mijn vriendin willen bedanken wiens onvoorwaardelijke steun tijdens de hele opleiding -en niet in het minst tijdens het schrijven van dit onderzoek- onontbeerlijk is geweest voor een positieve afloop.

Ten slotte ben ik ook dank verschuldigd aan de verschillende professoren en tutoren van wie ik het genoegen heb gehad te mogen bijleren, aan mijn medestudenten voor de verschillende leuke momenten en aan alle medewerkers van de UHasselt die een rol hebben gespeeld tijdens mijn studieperiode en in het bijzonder aan al diegenen die de stage in Pretoria hebben mogelijk gemaakt.

Begrippenlijst

Authenticeren: Het proces waarin wordt nagegaan of een bepaald bericht -zoals de identificatie of de handtekening- van een persoon ook effectief van die persoon afkomstig is.

Asymmetrische Cryptografie: zie Public Key Infrastructure (PKI)

Blockchain: datatransactieketen die (meestal via een decentrale database) op een veilige manier transacties tussen partijen mogelijk maakt.

Datakluis: Online platform dat gebruikers moet toelaten op een gecentraliseerde plaats hun data te beheren.

Datamining: het gericht zoeken naar verbanden in gegevensverzamelingen met als doel profielen op te stellen voor wetenschappelijk, journalistiek of commercieel gebruik.

Dataverrijking: Het aanvullen van bestaande data/persoonsgegevens met andere data/persoonsgegevens van diezelfde persoon.

E-government: Elektronische overheid. Het, door gebruik te maken van nieuwe technologieën; het internet en nieuwe media, herdenken en aanpassen van de relatie tussen burgers en ondernemingen enerzijds en de overheid anderzijds met als doel het verbeteren van de dienstverlening en beleidsvoering door de overheid.

ICT: Informatie en Communicatietechnologieën

Identificeren: Het geheel van activiteiten waardoor men de naam en het geografische adres van een persoon (ook wel de primaire identificatiegegevens genoemd) kan vaststellen.

Open data: Gegevens waarop geen of weinig beperkingen rusten en die door de overheid in het kader van haar publieke functie verzameld en openbaar gesteld worden.

Public Key Infrastructure: Methode om via een publieke en private sleutel jezelf digitaal te authenticeren aan een andere partij.

Inhoudsopgave

Inleiding 1

A. Onderzoekscontext 1

a) Onderwerp 1

b) Huidige situatie 2

c) Problemen 3

d) Relevantie 5

e) Beperkingen 5

B. Onderzoeksvraag 5

a) Centrale onderzoeksvraag 5

b) Sub-onderzoeksvragen 5

C. Onderzoeksmethode 6

a) Bibliografie: Selectie en verantwoording 6

b) Methodologische aanpak 7

Hoofdstuk I. Overheidsdigitalisering: E-government en authenticatieprocedures in België en Vlaanderen 9

A. Algemeen 9

B. Rol van authenticatiesystemen in de nationale strategie voor identiteitsbeheer 10

a) algemeen 10

b) Verschillende actoren en hun rol in het identificatiebeleid 11

C. Werking authenticatiemiddelen zoals Itsme en myID 16

a) Algemeen 16

b) FAS 16

c) Itsme 17

d) myID 19

e) De digitale portefeuille 19

D. Conclusie 20

Hoofdstuk II wettelijk kader Elektronische identificatie voor Belgische overheidstoepassingen 21

A. Algemeen 21

B. Wet inzake elektronische identificatie 21

a) Algemeen 21

b) Diensten voor elektronische identificatie aangeboden door private partijen 21

c) Conclusie 23

C. Erkenningsvoorwaarden 23
a) Algemeen 23
b) Betrouwbaarheidsniveaus 24
c) Functionele en technische voorwaarden 24
d) Dienstverleningsbeheer 26
e) Economische, juridische en organisationele voorwaarden 28
D. Erkenningsprocedure 28
E. Gevolgen van erkenning 29
F. Controle- en sanctieregelingen 30
G. FAS gebruikersovereenkomst 30
H. Vergelijking met Nederland 31
a) Algemeen 31
b) Betrouwbaarheidsniveaus 32
c) Reikwijdte 32
d) Privacy en gegevensbescherming 33
e) Identiteitsfraude 34
f) Toezicht en handhaving 35
I. Conclusie 36
Hoofdstuk III. Europees identiteitsmanagement: De eIDAS Verordening 39
A. Algemeen 39
B. Elektronische identificatiemiddelen 40
C. Herziening van de eIDAS verordening 41
a) Tekortkomingen 41
b) Voorstel tot een hernieuwde eIDAS 44
c) Gevolgen voor België 47
D. Conclusie 49
Hoofdstuk IV. Bescherming van persoonsgegevens 53
A. Algemeen 53
B. Toepassingsgebied AVG 54
C. Toelaatbaarheid van de verwerking 56
D. Identificatieplicht voor online overheidsdiensten 57
E. Identificatie en authenticatie door externe authenticatiediensten 58
a) Verantwoordelijkheid van de externe authenticatiedienst 59

b) Beginselen en verplichtingen 63
c) Waarborgen en controle 68
F. Conclusie 71
Conclusie 75
Lijst van geraadpleegde werken 83
A. Wetgeving 83
a) Europa en België 83
b) Nederland 86
B. Rechtspraak 86
C. Rechtsleer 87
D. Overige 90
Bijlage 1: Technische specificaties eIDAS 93

Inleiding

A. Onderzoekscontext

a) Onderwerp

1. De uitbouw van digitale overheidsdiensten is een uitgesproken doelstelling op zowel het Europese als het Belgische en Vlaamse beleidsniveau. Zo presenteerde de Europese commissie op 9 maart 2021 in zijn strategie voor de digitale transformatie de ambitie om tegen 2030 alle essentiële overheidsdiensten en de toegang tot de medische profielen van burgers voor 100% online toegankelijk te maken. Daarnaast zou 80% van de burgers van de Europese Unie gebruik moeten maken van een digitale identiteitskaart.[1] Op nationaal niveau haalde staatssecretaris voor digitalisering Mathieu Michel dan weer herhaaldelijk dat het in België de bedoeling is niet enkel een digitale identiteitskaart maar een hele digitale portefeuille -inbegrepen een digitaal rijbewijs en bankkaart- te lanceren.[2] Op het Vlaamse beleidsniveau ten slotte vat minister van digitalisering Jan Jambon de verschillende intenties goed samen door te willen inzetten op een efficiënte en informatie gedreven overheid die via het "only-once principe" de gebruiksvriendelijkheid van de publieke dienstverlening vergroot.[3]

2. Het is duidelijk dat digitale overheidsdiensten verschillende opportuniteiten bieden: overheden kunnen sneller, klantvriendelijker, ecologischer en innovatiever te werk gaan maar even goed kunnen zij via open data effectiever en transparanter beleid voeren of samenwerkingen met de private sector faciliteren om zo tot oplossingen voor verschillende maatschappelijke problemen te komen.[4] Digitalisering gaat zelfs zo ver dat er sprake is van heuse "smart cities" waarbij informatietechnologie, algoritmen en "the internet of things" gebruikt kunnen worden om steden te besturen van administratie tot openbare dienstverlening en de nutsvoorzieningen.[5]

Toch zijn er ook verschillende aandachtspunten voor een overheid die zijn diensten wenst te digitaliseren: Zo zullen overheden rekening moeten houden met verschillende veiligheids- en privacy vereisten, het gebruiken van correcte informatie, ethiek en natuurlijk ook de bestaande mensrenrechten en -plichten en beginselen van behoorlijk bestuur.[6] Deze scriptie zal zich bezighouden met één van deze aandachtspunten: Hoe kan een online overheidsdienst zeker zijn of iemand die online beweert een zekere persoon te zijn, ook effectief die persoon is? Kunnen wij er als burger zeker van zijn dat onze online gegevens die we gebruiken om onszelf te identificeren op een

[1] EC, "Europa's digitaal decennium: doelstellingen voor 2030", https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_nl, laatst bezocht 5/10/2022.
[2] L. DEWOLF, "Staatssecretaris van Digitalisering Mathieu Michel: "Itsme is sleutel, digitale portefeuille wordt volledig huis"", in *VRTNews,* 30 juni 2022, https://www.vrt.be/vrtnws/nl/2022/06/30/staatssecretaris-van-digitalisering-mathieu-michel-itsme-is-sl/, laatst bezocht: 5/10/2022.
[3] J. JAMBON, "Beleidsnota 2019-2024 – ICT en facilitair management", 8 november 2019, https://publicaties.vlaanderen.be/view-file/32229, laatst bezocht: 5/10/2022.
[4] SERV, "Startnota – De transitie naar een digitale samenleving", Brussel, 3 mei 2017, https://www.serv.be/sites/default/files/documenten/SERV_20170503_startnota_digitalisering_NOT_.pdf, 43-45, laatst bezocht:11/10/2022.
[5] B. KARSTENS, L. KOOL, R. VAN EST, "De slimme stad: grote beloften, weerbarstige praktijk", *Justitiële verkenningen* 2020, Den Haag, Vol. 46, afl. 3, (10) 11.
[6] SERV, "Startnota – De transitie naar een digitale samenleving", Brussel, 3 mei 2017, https://www.serv.be/sites/default/files/documenten/SERV_20170503_startnota_digitalisering_NOT_.pdf, 46-47.

veilige manier gebruikt worden? En is de bestaande regelgeving flexibel genoeg om niet enkel met huidige problemen maar ook met toekomstige evoluties om te gaan?

b) Huidige situatie

3. De digitale transformatie van onze besturen is volop bezig. Dat werd vooral duidelijk tijdens de coronapandemie waar overheidsdiensten ondanks het contact- en samenkomstverbod het gros van hun dienstverlening konden blijven aanbieden dankzij digitale platformen, telewerken, online vergaderingen, beleidsbeslissing op basis van data, … De mogelijkheden die nieuwe technologieën bieden gaan echter nog verder dan het louter implementeren ervan in de publieke dienstverlening (e-gov) of het gebruik van data door de overheid (i-gov): Het stelt overheden in staat verder te evolueren naar een overheidsstructuur gebaseerd op gebruikersverwachtingen en -behoeften (me.gov) waarbij de relatie burger-overheid nog louter online plaatsvindt.[7] Met de wet van 26 januari 2021 verankerde het federale parlement zijn ambitie om tegen 2025 alle communicatie tussen enerzijds particulieren, professionelen, rechtspersonen en mandatarissen die gemachtigd zijn de belastingplichtige te vertegenwoordigen en anderzijds de FOD Financiën online te laten verlopen.[8] Het is een logische volgende stap in het verder digitaliseren van onze overheidsdiensten waarbij het voor de burger steeds belangrijker zal worden om zichzelf digitaal te kunnen identificeren.

4. Om zijn identiteit te bewijzen moet een individu deze kunnen laten authenticeren. Om jezelf te kunnen authenticeren heeft men een authentieke bron nodig dat via een betrouwbaar en gecontroleerd identiteitsregistratieproces de identiteit van een persoon kan registreren. Een voorbeeld van zo'n authentieke bron is het Belgisch rijksregister. Toch zal deze registratie alleen -zeker online- niet voldoende zijn om zichzelf te authenticeren. Men kan niet enkel verwijzen naar een registratieproces dat ooit eens vlak na de geboorte werd doorlopen. Iedere burger krijgt dan ook een identiteitsreferentie in de vorm van een eID dat zowel fysiek als elektronisch onze identiteit moet helpen bewijzen. Via toegangsbeheersystemen kan dit identiteitsbewijs immers gekoppeld worden aan aangepaste authenticatiemiddelen die uiteindelijk onder andere voor toegang tot de online dienstverlening van de overheid kunnen zorgen.[9] Deze authenticatiemiddelen kunnen variëren van eenvoudige username-password accounts (*e.g*. Facebook account) tot meer ingewikkelde PKI systemen (*e.g*. Digitale handtekening).

5. België kent verschillende authenticatiemiddelen (ook wel digitale sleutels genoemd) om in te loggen bij online overheidsdiensten: burgers kunnen onder andere gebruik maken van de eID in combinatie met een kaartlezer, authenticatiesystemen die werken met een combinatie van een gebruikersnaam, wachtwoord en beveiligingscode of van de digitale sleutels van erkende (private)

---

[7] *Ibid*., 45.

[8] Wet van 26 januari 2021 betreffende de dematerialisatie van de relaties tussen de FOD Financiën, de burgers, rechtspersonen en derden bepaalt de wijze waarop de informatie vanaf 1 januari 2025 elektronisch zal worden uitgewisseld, *BS* 10 februari 2021; DROITS QUOTIDIEN LEGAL DESIGN, *FOD Financiën: in 2025zal alle communicatie elektronisch gebeuren*, Wolters Kluwer ImmoSpector, 2021, https://immospector.kluwer.be/newsview.aspx?contentdomains=IMMORES&id=kl2528877&lang=nl.

[9] AGENTSCHAP DIGITAAL VLAANDEREN, *Identity and acces management (IAM)*, Brussel, 2017-2022, https://assets.vlaanderen.be/image/upload/v1648220287/Vo_Informatieclassificatie_-_Minimale_maatregelen_-_IAM_xle0xg.pdf, 18-19.

partners zoals Itsme en myID.[10] Daarnaast werkt de overheid nog aan een eigen initiatief waarbij het online authenticatiemiddel geïntegreerd zou worden in de digitale portefeuille.[11]

Het is het CSAM dat deze online authenticatie en identificatieprocessen op een veilige en betrouwbare manier doet verlopen, onder andere door het aanbieden van de Federal Authentication Service (FAS) die opgericht werd door de FOD BOSA zoals bepaald door de wet elektronische identificatie.[12] Om erkend te worden als authenticatiemechanisme om in te loggen bij de Belgische overheidsdiensten moeten de dienstverleners voldoen aan de voorwaarden zoals vastgelegd in het uitvoeringskb. elektronische identificatie.[13]

6. De verschillende authenticatiemiddelen die worden aangeboden om in te loggen bij verschillende overheidsdiensten hebben verschillende betrouwbaarheidsniveaus (LoA's) waarover op Europees vlak enkele afspraken werden gemaakt in de vorm van de eIDAS verordening. Zo wordt er voorzien in 3 schalen van vertrouwelijkheid oplopend van "laag" naar "substantieel" en uiteindelijk "hoog".[14] Deze authenticatieschalen werden overgenomen door de Belgische federale en Vlaamse overheden.[15] Zowel in Vlaanderen als op federaal niveau zal er om in te loggen bij overheidsdiensten voornamelijk gebruik gemaakt worden van multifactor-authenticatie waarbij twee of meer factoren (klassiek: iets wat je kent zoals een paswoord, iets wat je hebt zoals een eID en iets wat je bent zoals een vingerafdruk) zullen worden gebruikt om de identiteit van burgers te authenticeren. Het voordeel van deze multifactor authenticatieprocessen in vergelijking met single factor authenticatie is dat zij moeilijker te misbruiken zijn door derden die bijvoorbeeld het paswoord van een burger weten te achterhalen.[16]

7. Het is duidelijk dat om tot bovenstaande digitaliseringen te komen, er een verregaande uitwisseling en verwerking van persoonsgegevens nodig is. Het hoeft dan ook niet te verbazen dat elk identificatie- en authenticatieproces onderworpen is aan de nationale en supranationale regelgeving betreffende de bescherming van persoonsgegevens.[17]

c) Problemen

8. Het spreekt voor zich dat wanneer bestuurlijke overheden onderling of met private partners persoonlijke informatie gaan uitwisselen, zij rekening moeten houden met bestaande beschermingsmechanismen zoals het recht op privacy, de bescherming van verwerking van de

---

[10] CSAM, *Mijn digitale sleutels: wat zijn digitale sleutels*, https://iamapps.belgium.be/sma/generalinfo?view=digitalKeys, laatst bezocht: 8 januari 2023.

[11] P.J. VAN LEEMPUTTEN, "overheid werkt aan alternatief voor Itsme", *Datanews knack*, 2022, https://datanews.knack.be/ict/nieuws/overheid-werkt-aan-alternatief-voor-itsme/article-news-1879327.html, laatst bezocht: 8 januari 2023.

[12] Art. 9 §1 wet van 18 juli 2017 inzake elektronische identificatie, *BS* 9 augustus 2017; CSAM, Mijn digitale sleutels: *Wat is CSAM?*, https://iamapps.belgium.be/sma/generalinfo?view=csam, laatst bezocht, 8 januari 2023.

[13] 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, *BS* 8 november 2017.

[14] Art. 8 Verord.Parl.Raad. nr. 910/2014, 23 juli 2014, betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, *Pb.L* 28 augustus 2014, afl. 257, 73. (Hierna eIDAS verordening).

[15] AGENTSCHAP DIGITAAL VLAANDEREN, *Identity and Acces Management (IAM)*, Brussel, 2017-2022, https://assets.vlaanderen.be/image/upload/v1648220287/Vo_Informatieclassificatie_-_Minimale_maatregelen_-_IAM_xle0xg.pdf, 23.

[16] *Ibid*., 24.

[17] F. SCHRAM, "Datamining en fraudebestrijding via gegevensuitwisseling en de juridische gevolgen van onrechtmatige elektronische uitwisseling van informatie tussen verschillende overheidsadministraties", in M. DELANOTTE, B. PEETERS en I. VAN DE WOESTEYNE (eds.), *Digitalisering. Postuniversitaire cyclus Willy Delva*, Mechelen, Wolters Kluwer, 2021, 234-236.

persoonsgegevens en enkele rechtsbeginselen zoals de beginselen van behoorlijk bestuur. De vraag stelt zich echter of deze beschermingsmechanismen in staat zijn om de burger te blijven beschermen in een snel evoluerend digitaal tijdperk. Waar dataverzameling beschermd dient te worden door de -vaak niet aangepaste- privacywetten en grondrechten, kijkt men voor de verwerking van persoonlijke gegevens (zoals het uitwisselen van persoonlijke data, datavergelijking en datamining) voornamelijk naar de verplichtingen vervat in de Algemene Verordening Gegevensbescherming (AVG).[18]

9. Zo voorziet de AVG in enkele verregaande informatie- en beschermingsmaatregelen waardoor het niet zomaar toegelaten is om toegang tot een overheidsdienst af te laten hangen van het uitwisselen van persoonsinformatie.[19] Echter wordt aan de wetgever ook de macht gegeven om quasi alle beschermingsmechanismen van de AVG buiten werking te stellen. Een optie waarvan uiteraard gretig gebruik gemaakt wordt.[20] Het is nog maar de vraag of de overheid bij de ontwikkeling van een eigen authenticatiemiddel aan deze verleiding zal kunnen weerstaan en welke impact dit zal hebben op de bescherming van de persoonsgegevens van zijn burgers. Bovendien duiken bij de toepassing van de AVG vaak enkele praktische problemen op. Zo is het vaak niet duidelijk wie de verzamelaar van data is binnen bepaalde projecten met private partners zoals Itsme wanneer bijvoorbeeld de bestaande apparatuur die de gegevens verzamelt eigendom is van de overheid maar het beheer van de data overgedragen is aan een private partner en op welke manier de vereiste waarborgen kunnen worden geïmplementeerd.[21]

10. Een ander mogelijk probleem dat zou kunnen opduiken, is het feit dat het Belgisch wettelijk kader betreffende de erkenningsvoorwaarden sterk gebaseerd is op de Europese eIDAS verordening die grensoverschrijdende identificatie- en authenticatieprocessen reguleert. Met de herziening van deze verordening wil de Europese Commissie tegemoet komen aan de tekortkomingen die sinds de aanname van de verordening aan de oppervlakte kwamen. Net als staatssecretaris M. MICHEL is het de ambitie van de Commissie om de zogenaamde digitale portefeuille met ingebouwd authenticatiesysteem mogelijk te maken.[22] Daar de herziening van deze verordening er nog niet is doorgekomen, is het nog maar ten zeerste de vraag of ons huidig nationaal wettelijk kader voldoende bescherming biedt om tegemoet te komen aan de technologische ontwikkelingen van de laatste jaren en aan de ambitie om een volledig door de overheid beheerd authenticatiesysteem uit te werken.

---

[18] Zie het onderscheid tussen art. 7 en 8 EU Handvest; F. SCHRAM, "Datamining en fraudebestrijding via gegevensuitwisseling en de juridische gevolgen van onrechtmatige elektronische uitwisseling van informatie tussen verschillende overheidsadministraties", in M. DELANOTTE, B. PEETERS en I. VAN DE WOESTEYNE (eds.), *Digitalisering. Postuniversitaire cyclus Willy Delva*, Mechelen, Wolters Kluwer, 2021, 218.

[19] Art. 25 AVG; GBA, aanbeveling nr. 01/2019 betreffende het opleggen van de verplichte aanmaak van een gebruikersaccount bij Microsoft voor het raadplegen van toepassingen van overheidsdiensten, 6 februari 2019.

[20] F. SCHRAM, "Datamining en fraudebestrijding via gegevensuitwisseling en de juridische gevolgen van onrechtmatige elektronische uitwisseling van informatie tussen verschillende overheidsadministraties", in M. DELANOTTE, B. PEETERS en I. VAN DE WOESTEYNE (eds.), *Digitalisering. Postuniversitaire cyclus Willy Delva*, Mechelen, Wolters Kluwer, 2021, 241.

[21] B. KARSTENS, L. KOOL, R. VAN EST, "De slimme stad: grote beloften, weerbarstige praktijk", *Justitiële verkenningen* 2020, Den Haag, Vol. 46, afl. 3, (10) 15; O. SUSTRONCK, "It's not you, Itsme", *TPP* 2021, nr. 3, (6)7.

[22] EPRS, *Revision of thee IDAS regulation, findings on its implementation and application*, 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf, 1.

d) Relevantie

11. Het is duidelijk dat wanneer het gaat om digitalisering van de bestuurlijke overheden in de relatie met de eigen burger, er nog heel wat onbeantwoorde vragen zijn. Bestaande wetgeving is vaak niet aangepast aan de huidige situatie of niet in staat de snelle evolutie van de digitale wereld te volgen.

e) Beperkingen

12. Het onderzoek in deze scriptie zal zich beperken tot de evaluatie van het specifieke wettelijk kader dat bestaat voor authenticatiemechanismen in België aan de hand van de wetgeving die bestaat op het niveau van de Europese Unie en rechtstreeks van toepassing is op de authenticatieketen. Dat wil zeggen dat de regeling zoals zij bestaat in België bekeken zal worden in het licht van de eIDAS verordening en de bescherming tegen de verwerking van persoonsgegevens. Gezien de beperkte omvang van de scriptie zou het apart bespreken van verdere wetgeving (zoals bijvoorbeeld de grondrechten vervat in het EVRM en de beginselen van behoorlijk bestuur die van toepassing zullen zijn bij een volledig door de overheid gecontroleerd authenticatiemechanisme) te ver afwijken van de centrale onderzoeksvraag. De scriptie beperkt zich ook tot enkel authenticatie voor de toegang tot online overheidsdiensten.

13. Ten slotte is het niet de bedoeling van deze scriptie om een aanbevelend onderzoek uit te voeren. Hoewel de mogelijke tekortkomingen van de bestaande wetgeving tegenover de huidige (en toekomstige) realiteit geëvalueerd zullen worden en er hierbij weliswaar verschillende mogelijke oplossingen zullen worden aangereikt, zullen deze oplossingen niet tegenover elkaar worden afgewogen. Het biedt ruimte aan verdere onderzoeken om te bepalen welke oplossingen het meest geschikt zijn om de in deze scriptie aangehaalde problemen op te lossen.

B. Onderzoeksvraag

a) Centrale onderzoeksvraag

14. De centrale onderzoeksvraag die deze scriptie zal beantwoorden luidt: "*Is het Belgische wetgevend kader om de veiligheid betreffende het gebruik van privaat dan wel overheidsgeorganiseerde authenticatietoepassingen voor het inloggen bij online overheidsdiensten zoals Itsme te garanderen voldoende aangepast aan de ontwikkelingen binnen de Europese Unie?"*

De centrale onderzoeksvraag is een evaluerende onderzoeksvraag waarbij het wettelijk kader dat specifiek verband houdt met de werking van authenticatiemechanismen beoordeeld zal worden in het licht van andere bestaande wetgeving, rechtspraak en technologische ontwikkelingen.[23]

b) Sub-onderzoeksvragen

15. De sub-onderzoeksvragen die beantwoord dienen te worden om tot een conclusie te kunnen komen betreffende de centrale onderzoeksvraag zijn:

1) Hoe wordt authenticatie in het Belgische e-government beleid georganiseerd?

[23] P. SCHOUKENS, K. HENDRICKX, E. TERRYN (red.) and L. KESTEMONT, *Rechtswetenschappelijk schrijven*, Leuven, Acco, 2020, 64.

De eerste sub-onderzoeksvraag is een definiërende onderzoeksvraag waarbij de rol van authenticatiemechanismen in de nationale en Vlaamse identiteitsstrategie kan worden geclassificeerd.[24]

2) Hoe reguleert bestaande nationale en supranationale wetgeving de erkenning van nieuwe en bestaande authenticatiemechanismen?

De tweede sub-onderzoeksvraag is een beschrijvende onderzoeksvraag waarbij op basis van voornamelijk wetgeving en diens voorbereidende teksten de erkenningsvoorwaarden worden beschreven en toegepast op het, in sub-onderzoeksvraag 1) besproken, authenticatiebeleid.[25]

3) Welke rol speelt de gegevensbescherming in het nationale authenticatiebeleid?

De derde sub-onderzoeksvraag is een beschrijvende onderzoeksvraag waarbij op basis van rechtsleer en jurisprudentie wordt nagegaan op welke manier de regelgeving betreffende de bescherming van de persoonsgegevens van invloed is op het in sub-onderzoeksvraag 1) besproken authenticatiebeleid.[26]

4) Welke nieuwe relevante toepassingen, problemen en evoluties hebben er op Europees niveau betreffende in onderzoeksvragen 2) en 3) beschreven wetgevingen plaatsgevonden?

De vierde sub-onderzoeksvraag is een beschrijvende onderzoeksvraag waarbij op basis van rechtsleer, jurisprudentie, een vergelijking met Nederland en eigen inbreng wordt nagegaan of en hoe het nationale authenticatiebeleid hebben geleid of zou kunnen leiden tot problemen in het licht van onder 2) en 3) besproken regelgevingen.[27] Het antwoord op deze sub-onderzoeksvraag zal voldoende informatie verschaffen om uiteindelijk tot een antwoord op de centrale onderzoeksvraag te komen.

C. Onderzoeksmethode

a) Bibliografie: Selectie en verantwoording

16. Aangezien de centrale onderzoeksvraag een bestaand wettelijk kader wenst te evalueren aan de hand van andere (supranationale) wetgeving, is het duidelijk dat over heel de scriptie wetgeving en de voorbereidende documenten daarvan zullen gelden als belangrijkste bronnen. Voor het beantwoorden van de eerste sub-onderzoeksvraag zal verder er invulling worden gegeven aan enkele technische begrippen om zo de materie beter te begrijpen. Omdat het gaat om universeel aanvaarde, doch vaak niet (strikt) juridische begrippen, zal er naast beschrijvingen in bestaande wetgeving en rechtsleer ook gekeken worden naar wetenschappelijk onderzoek uit andere disciplines waaronder voornamelijk IT bronnen. Voor de reële toepassing van deze authenticatiemechanismen, zal er worden gekeken naar het privacy beleid en de gebruikersovereenkomst van de bestaande dienstverleners.

17. Voor het beantwoorden van de tweede sub-onderzoeksvraag die het nationale en Europese wettelijk kader betreffende authenticatiemechanismen zal beschrijven, wordt opnieuw voornamelijk

[24] *Ibid*., 50.
[25] *Ibid*., 45-49.
[26] *Ibid*.
[27] *Ibid*., 64-65.

gekeken naar bestaande wetgeving en wetgevende documenten. De weinig beschikbare binnen- en buitenlandse vakliteratuur zal optimaal moeten worden gebruikt en gecombineerd met -indien deze bestaat- rechtspraak van de bevoegde rechterlijke instanties.

18. De derde sub-onderzoeksvraag, die handelt over Europese en Belgische regelgeving betreffende de bescherming van persoonsgegevens zal worden benaderd vanuit een lezing van de algemene rechtsleer betreffende de inhoud en toepassing van de Algemene Verordening Gegevensbescherming en afgeleide wetgeving. Bovendien moet er worden gekeken naar rechtspraak van de bevoegde rechterlijke instanties zoals het Hof van Justitie, de hoge rechtbanken binnen België en eventueel enkele spraakmakende uitspraken van de Belgische gegevensbeschermingsautoriteit. Voor de specifieke toepassing van deze wetgeving op de authenticatiemechanismen, kan worden teruggegrepen naar gespecialiseerde literatuur zoals bijvoorbeeld de artikel 29 werkgroep.

19. De vierde sub-onderzoeksvraag zal op basis van dezelfde bronnen en nieuwe interpretaties door gezaghebbende instanties nagaan welke evoluties hebben plaatsgevonden na de inwerkingtreding van het Belgisch wettelijk kader.

De centrale onderzoeksvraag ten slotte zal worden beantwoord vanuit een kritische evaluatie van alle voorgaande bronnen. Rechtspraak van gespecialiseerde instanties zoals de gegevensbeschermingsautoriteit zullen daarbij belangrijk zijn. Daar vooral in dit deel van de scriptie het vernieuwende element zit, zal er niet veel Belgische gespecialiseerde literatuur voorhanden zijn. Er zal voor de toepassing van de geëvalueerde wetgeving op de problematiek betreffende de authenticatiemechanismen uitgegaan worden van eigen interpretatie, aangevuld met eventuele buitenlandse bedenkingen en oplossingen. Omdat Nederland tijdens het schrijven van deze scriptie nieuwe wetgeving aan heeft genomen betreffende identificatie en authenticatie voor het gebruik van online overheidsdiensten en zij dit dus -in tegenstelling tot België waar het wettelijk kader al enkele jaren bestaat- deden met alle huidige kennis, vormt zij een ideaal vergelijkingsland voor deze studie. Er zal doorheen de scriptie dan ook aandacht zijn voor de Nederlandse wetgeving en voorbereidende documenten.

b) Methodologische aanpak

20. In deze scriptie wordt gebruik gemaakt van de klassiek-juridische methode waarbij aan de hand van wetgeving, jurisprudentie en literatuur met aanvullende documenten een antwoord wordt gezocht op de verschillende deelvragen. Het begrip wetgeving dient hier ruim te worden geïnterpreteerd en omvat alle nationale en Europese regelgeving met bijhorende parlementaire documenten. De jurisprudentie wordt in deze methode gebruikt als gezaghebbende bron die een vaste gedragslijn kan vaststellen gebaseerd op de interpretatie en herformulering van de bestaande regels. Met literatuur worden uiteraard juridische bronnen bedoeld in de vorm van onderwijsboeken, vakpublicaties en wetenschappelijke artikelen. Omdat het daarnaast de bedoeling van deze scriptie is om een zo getrouw mogelijke waarheid te schetsen van de praktijk rond authenticatiesystemen, zullen ook andere bronnen zoals overeenkomsten tussen betrokken schakels in de authenticatieketen en eerder gegeven interviews via bureauonderzoek worden geraadpleegd.[28]

[28] H. E. B. TIJSSEN, *De juridische dissertatie onder de loep: De verantwoording van methodologische keuzes in juridische dissertaties*, Boom, Juridische Uitgevers, 2009, 70-73.

21. De wettelijke rechtsvergelijking met Nederland betreffende authenticatiemechanismen wordt gedaan volgens de functionele methode. Dit houdt in dat -weliswaar na een korte beschrijving van het te vergelijken rechtstelsel- voor de problemen die tijdens de evaluatie van het Belgische wettelijk kader doorheen deze scriptie aan het licht komen, wordt nagegaan hoe deze worden opgelost door het Nederlandse stelsel.[29] De keuze voor het Nederlandse stelsel als vergelijkingspunt vloeit voort uit het feit dat zij zeer recent, en dus met alle kennis van de evoluties die op Europees niveau rond online authenticatie plaatsvinden, hun wettelijk kader hebben vorm gegeven.

22. De eerste -definiërende- sub-onderzoeksvraag zal in het eerste hoofdstuk worden beantwoord vanuit een beschrijving van enkele niet juridische begrippen zoals "e-government", "authenticatie" en "verificator" aan de hand van zowel juridische bronnen -wanneer zij reeds gedefinieerd werden in de wetgeving, rechtspraak of rechtsleer- of -indien dit niet het geval is- aan de hand van niet-juridische bronnen. Er zal concreet worden beschreven welke rol authenticatiediensten innemen in het federaal en Vlaams identificatiebeleid en hoe deze dienstverleners hun rol vervullen. Op deze manier kunnen de verschillende juridische problemen die kunnen voortvloeien uit authenticatiemechanismen geclassificeerd worden. De classificatie zal gebeuren op basis van de relatie tussen de authenticatiedienst en de burger die van de diensten gebruik maakt.

23. De tweede en derde sub-onderzoeksvragen, die het wettelijk kader dat van toepassing is op de authenticatiemechanismen zullen beschrijven, worden opgenomen in hoofdstukken II (Nationaal kader) en III (eIDAS). Ook zal er voor dit laatste hoofdstuk reeds een antwoord worden gegeven op de vierde onderzoeksvraag en zal er dus worden beschreven welke evolutie er sinds de aanname van de eIDAS heeft plaatsgevonden. Ten slotte zullen er in beide hoofdstukken reeds enkele componenten van de centrale onderzoeksvraag worden behandeld. Zo zal er bijvoorbeeld in hoofdstuk II dieper ingegaan worden op de verschillen in benadering tussen België en Nederland. In hoofdstuk III zal er daarnaast worden nagegaan of de vernieuwingen die nodig geacht worden voor de eIDAS verordening ook geïmplementeerd zouden moeten worden in het nationaal wettelijk kader.

24. Ten slotte zal in hoofdstuk IV de derde sub-onderzoeksvraag beantwoord worden en dit opnieuw in combinatie met een antwoord op elementen van de vierde sub-onderzoeksvraag. De evaluatie die dient te gebeuren voor de centrale onderzoeksvraag zal aldus verspreid zitten over hoofdstukken III en IV.

[29] F. GORLE, G. BOURGEOIS en H. BOCKEN, *Rechtsvergelijking*, Mechelen, Kluwer, 2007, 2-3 en 32-34.

Hoofdstuk I. Overheidsdigitalisering: E-government en authenticatieprocedures in België en Vlaanderen

A. Algemeen

25. Omgang met de overheid gebeurt steeds meer digitaal. Door gebruik te maken van informatie en communicatie technologieën (ICT), kan de overheid zijn diensten goedkoper, eenvoudiger en neutraler aanbieden aan de burger. Deze omslag richting een "e-government" is al vele jaren aan de gang. Reeds in de jaren 1990 duikt het begrip op en werd het veelvuldig gedefinieerd door verschillende instanties.[30] Zo definieert de Wereldbank e-government als:

> *"The use of information and communications technologies (ICT) to improve the efficiency, effectiveness, transparency and accountability of government."*[31]

Ook Europa -bij monde van de Europese Commissie- definieerde e-government, zij het licht verschillend:

> *"het gebruik van informatie- en communicatietechnologie bij overheidsdiensten in combinatie met organisatorische veranderingen en nieuwe vaardigheden met het oog op een verbetering van de openbare diensten en de democratische processen en een krachtiger ondersteuning van het overheidsbeleid."*[32]

Op nationaal niveau wordt e-government dan weer omschreven als:

> "*een geïntegreerde en continue manier om openbare diensten te verlenen dankzij het optimale gebruik van de informatie- en communicatietechnologieën (ICT). E-government verbetert de kwaliteit en de verlening van overheidsdiensten en versterkt de ondersteuning van het overheidsbeleid en, meer in het algemeen, van het democratische proces."*[33]

In Vlaanderen ten slotte wordt de volgende definitie voor e-government al reeds enige tijd gebruikt:

> *"het gebruik van informatie- en communicatietechnologie bij overheidsdiensten in combinatie met organisatorische veranderingen en nieuwe vaardigheden met het oog op een verbetering van de openbare diensten".*[34]

Uit de verschillende bovenstaande definities komen verschillende kernelementen steeds weer naar voren: Zo wordt duidelijk dat e-government moet worden gezien als: het door gebruik te maken van

---

[30] B. VAN ALSENOY, *Data Protection Law in the EU: Roles, Responsibilities and Liability,* Mortsel, Intersentia, 2019, 347.
[31] WERELDBANK, *The E-government Handbook for developing countries: A project of InFODev and the Center for Democracy & Technology, 2002, 8,* https://documents1.worldbank.org/curated/en/317081468164642250/pdf/320450egovhandbook01public12002111114.pdf, laatst bezocht: 8/12/2022.
[32] Mededeling (Comm.) betreffende de Rol van de elektronische overheid (eGovernment) voor de toekomst van Europa, 26 september 2003, COM(2003)567, https://www.eumonitor.nl/9353000/1/j4nvhdfcs8bljza_j9vvik7m1c3gyxp/vikqh0qi43zz.
[33] FGOV, Het begrip e-government, https://economie.fgov.be/nl/themas/online/het-begrip-e-government, laatst bezocht 9/12/2022.
[34] G. BOURGEOIS, *Beleidsnota bestuurszaken 2004-2009*, 2004, https://overheid.vlaanderen.be/sites/bz.vlaanderen.be/files/documenten/Beleidsnota_bestuurszaken_2004.pdf, 12, laatst bezocht 9/12/2022.

nieuwe technologieën, het internet en nieuwe media, continu herdenken en aanpassen van de relatie tussen burgers en ondernemingen enerzijds en de overheid anderzijds met als doel het verbeteren van de dienstverlening en beleidsvoering door de overheid.[35]

26. Grosso modo kunnen vijf soorten van e-government onderscheiden worden:[36] Vooreerst kunnen overheden de burger voorzien van informatie door deze bijvoorbeeld toegankelijk te maken op hun websites. Daarnaast kunnen overheden online burgerparticipatie organiseren zoals onlangs nog gebeurde in de vorm van de burgerbevraging "Een land voor de toekomst" georganiseerd door huidig minister van Binnenlandse zaken Annelies Verlinden in het kader van de toekomst van de staatsstructuur en democratie in België.[37] Ten derde kunnen overheden hun overheidsopdrachten digitaal aanbieden, digitaal offertes ontvangen en -in principe, mits voldaan is aan alle wettelijke voorwaarden- deze offertes zelfs met behulp van artificiële intelligentie verwerken. Ten vierde houdt e-government ook een uitwisseling van informatie tussen verschillende overheden in wat een integratie van dienstverlening aan de burger via websites of platformen mogelijk maakt. De overheid kan met andere woorden een online "one-stop-shop" organiseren voor burgers die dus niet langer verschillende overheidsinstanties moeten contacteren om van een dienstverlening gebruik te kunnen maken.[38] Ten slotte kan de burger ook online bepaalde verplichtingen naleven en zijn voordelen vanuit de overheid nagaan. Denk hierbij bijvoorbeeld aan de taks-on-web toepassing, uitkeringen vanuit de sociale zekerheid of het aanvragen van een bouwvergunning.[39]

B. Rol van authenticatiesystemen in de nationale strategie voor identiteitsbeheer

a) algemeen

27. Uit bovenstaande voorbeelden blijkt duidelijk dat veel van de -digitale- interacties tussen overheid en burger zeer persoonlijk van aard zijn. Het is dan ook belangrijk dat de burger die gebruik maakt van de overheidsdiensten zich correct en betrouwbaar kan identificeren én dat eventuele andere (persoonlijkheids)kenmerken die de dienst vereist te weten, zoals leeftijd, geslacht, diploma,… kunnen worden geverifieerd.[40] Voor een goed e-government beleid zijn er dus mechanismes nodig die het de overheid mogelijk maken om de burger, die toegang tot de dienstverlening wenst te bekomen, te kunnen identificeren en authenticeren.[41] Onder identificeren wordt het geheel van activiteiten begrepen waardoor men de naam en het geografische adres van een persoon (ook wel de primaire identificatiegegevens genoemd) kan vaststellen. Authenticeren is het proces waarin wordt nagegaan of een bepaald bericht -zoals de identificatie- van een persoon

[35] D. DE BOT, *E-government in het Federale België*, Brussel, Politeia, 2015, 88.
[36] B. VAN ALSENOY*, Data Protection Law in the EU: Roles, Responsibilities and Liability*, Mortsel, Intersentia, 2019, 347.
[37] Zie betreffende dit thema de website van de burgerbevraging: https://demain-toekomst-zukunft.be/.
[38] B. AKGHAR, B. KHAZAEI en J. ALQATAWNA "Importance of service integration in e-government Implementations", in *The 7th International Conference on Information and Communication Systems*, Irbid, 2016, 2-5.
[39] Z. FANG, "E-government in digital era: Concept, Practice and Development", in International Journal of the Computer, The internet and management, 2002, afl 10, nr. 2, 4; B. VAN ALSENOY, *Data protection Law in the EU*, *Roles, Responsibilities and Liability*, Mortsel, Intersentia, 2019, 347-348.
[40] S.S. GARCIA, A.G. OLIVA, E.P. BELLEBONI en I.P. DE LA CRUZ, "Current trends in Pan-European Identity Management Systems", *Technology and Society Magazine* 2012, vol. 31, afl. 3, https://pdfs.semanticscholar.org/ef04/650b114ea77a943e58dde761372493c5b750.pdf?_gl=1*1qxx0n4*_ga*NjU0NzU2MDA0LjE2ODM5Nzc5OTA.*_ga_H7P4ZT52H5*MTY4Mzk3Nzk4OS4xLjEuMTY4Mzk3ODAyOC4wLjAuMA, 2.
[41] B. VAN ALSENOY, *Data protection Law in the EU*, *Roles, Responsibilities and Liability*, Mortsel, Intersentia, 2019, 348.

ook effectief van die persoon afkomstig is. De vraag of een persoon ook effectief is voor wie hij zich uitgeeft wordt met andere woorden beantwoord.[42]

28. Zoals veel Europese landen heeft ook België een identiteitsmanagementstrategie ontwikkeld om vanop afstand personen te kunnen identificeren en authenticeren. Onder identiteitsmanagement worden alle processen en technologieën verstaan die te maken hebben met het creëren, managen en gebruiken van de digitale identiteit.[43] Een belangrijke factor in die strategie was de introductie van de eID die onder andere via het gebruik van hardware zoals een eID reader of software zoals de Itsme app en public key infrastructure (PKI)[44] kan gebruikt worden om jezelf te identificeren en authenticeren voor het gebruik van overheidsdiensten.[45] De overheid krijgt dan een PKI certificaat uitgegeven door een certificaatautoriteit dat bewijst dat de burger zich aan de hand van een geheime private code of paswoord (private sleutel) heeft weten te authenticeren. De overheid gebruikt op zijn beurt een publieke sleutel om de opgevraagde informatie, gegevens of dienst te versleutelen en verzendt deze encryptie naar de burger. De burger die gebruik wil maken van de overheidsdienst kan aan de hand van zijn private sleutel uiteindelijk de versleutelde informatie lezen.[46]

Een tweede belangrijke evolutie in de identiteitsmanagementstrategie kwam er met de invoering van de verplichting voor overheden tot het gebruik van het Rijksregisternummer of het identificatienummer van de Kruispuntbank bij de digitale identificatie van natuurlijke personen die gebruik willen maken van (online) overheidsdiensten.[47] De verplichting kwam er ter bereiking van het doel van de administratieve vereenvoudiging voor de burger en het niet moeten opnieuw doorgeven van gegevens die via een authentieke bron reeds beschikbaar zijn voor de overheid.[48]

b) Verschillende actoren en hun rol in het identificatiebeleid

29. Typisch worden in het identificatiebeleid drie tot zes entiteiten onderscheiden: Minstens zijn er de burger/gebruiker; de credentievoorzieningsservice (credential service provider) en de vertrouwende partij. Conceptueel kunnen daar echter nog de authentieke registers; de integratoren en de verificator (verifier) aan toegevoegd worden. Weliswaar moet er mee worden rekening gehouden dat verschillende entiteiten vervat kunnen zitten binnen één actor. Zo kan een vertrouwende partij bijvoorbeeld zijn eigen verificatiedienst hebben waardoor de entiteiten vertrouwende partij en verificator vervat zitten in één rechtspersoon.[49] In wat hieronder volgt zullen

---

[42] Gegevenbeschermingsautoriteit (GBA), advies over een ontwerpbesluit van de Regering van de Franse Gemeenschap tot het bepalen van de categorieën van persoonsgegevens die worden verwerkt met betrekking tot de doeleinden van de digitale ruimten in toepassing van de artikelen 6 en 11 van het decreet van 25 april 2019 betreffende het digitaal bestuur van het schoolsysteem en de overdracht van digitale gegevens in het leerplichtonderwijs, 5 november 2020, nr. 108/2020, 6; R. DE CORTE, "Elektronische handtekening en identificatie in de virtuele wereld", *P&B*, 2001, afl. 5, (207) 209; A. VEDDER, *Security and Law,* Mortsel, Intersentia, 2019, 162.

[43] A. VEDDER, *Security and Law,* Mortsel, Intersentia, 2019, 161.

[44] Vertaald: "asymmetrische cryptografie".

[45] B. VAN ALSENOY, *Data protection Law in the EU*, *Roles, Responsibilities and Liability*, Mortsel, Intersentia, 2019, 348

[46] D. HAEX en T. AELBRECHT, "De elektronische handtekening toegespitst op vennootschapsrechtelijke documenten: it's all about trust", *RDC-TBH*, 2020, nr. 5, (565) 570.

[47] Art. 4 §1 wet 5 mei 2014 houdende verankering van het principe van de unieke gegevensinzameling in de werking van de diensten en instanties die behoren tot of taken uitvoeren voor de overheid en tot vereenvoudiging en gelijkschakeling van elektronische en papieren formulieren, *BS* 4 juni 2014. (only once wet); Art. III.113/2 Decreet 7 december 2018 Bestuursdecreet, *BS* 19 December 2018.

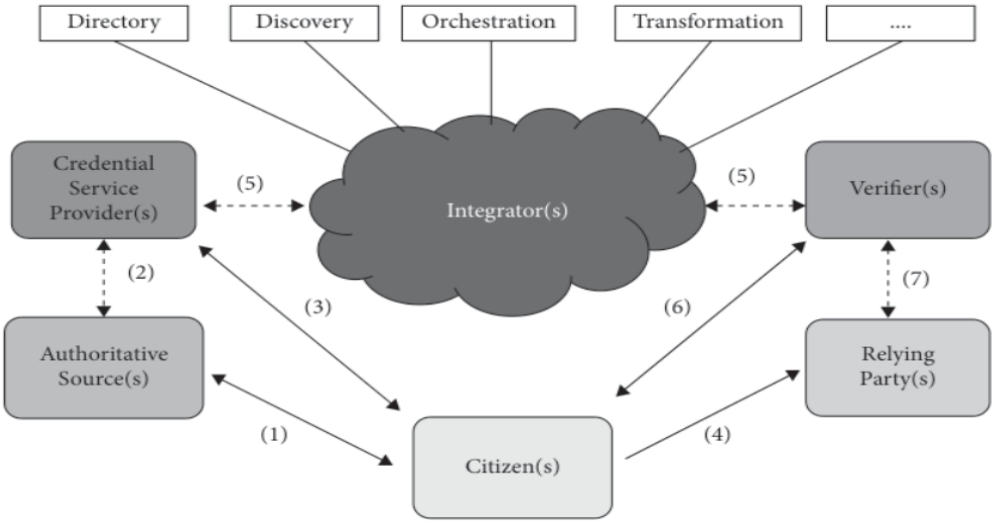
[48] Art. 2 only once wet; D. DE BOT, *E-government in het federale België* . Brussel, Politeia, 2015, 327; J. DE LANDSHEERE, "Only-onceprincipe: het principe van de unieke gegevensverzameling", *NWJ* 2016, (98) 100-103.

[49] B. VAN ALSENOY, *Data protection Law in the EU*, *Roles, Responsibilities and Liability*, Mortsel, Intersentia, 2019, 351.

deze actoren elk apart worden beschreven en zal hun rol in het identificatieproces worden beschreven. Ook zal duidelijk worden waar de authenticatiesystemen zoals Itsme en MyID kunnen worden gesitueerd.

Burger/gebruiker

30. De burger/gebruiker is degene die onderworpen is aan de digitale identiteit. Zoals hierboven (zie *supra* randnummer 27) beschreven hangt een identiteit vast aan bepaalde (persoonlijkheids)kenmerken zoals een geslacht, geboortedatum of telefoonnummer. Minstens één van deze kenmerken zal uiteindelijk binnen een bepaalde context dienen als identificatiemiddel. Denk hierbij bijvoorbeeld aan een studentennummer als identificatiemiddel binnen een universiteit. Vaak zal echter een combinatie van kenmerken (zoals naam, leeftijd en thuisadres) nodig zijn om zich te kunnen identificeren. Het feit dat iemand kan aantonen dat hij bepaalde identificatiemiddelen kent, betekent echter niet dat hij of zij ook de persoon is aan wie deze identificatiemiddelen toebehoren. Voor de effectieve authenticatie is ook de toekenning van authenticatiegegevens vereist.[50] De identificatiemiddelen die toebehoren aan een burger in een overheidscontext zullen vaak reeds door een overheid verzameld zijn en worden opgeslagen in zogenaamde authentieke registers.[51] Het proces van identificatie en authenticatie van burger tot vertrouwende partij wordt duidelijk weergegeven in onderstaande afbeelding. De volle pijlen geven een rechtstreekse interactie tussen de burger en andere entiteiten weer, pijlen met een stippenlijn stellen processen voor waar de burger mogelijks niet meteen bij stilstaat.



[52]

[50] A. VEDDER, *Security and Law,* Mortsel, Intersentia, 2019, 163.
[51] D. DE COCK, B. VAN ALSENOY, B. PRENEEL en J. DUMORTIER, "The Belgian eID approach", in W. FUMY en M. PAESCHKE, *Handbook of eID Security. Concepts, Practical experiences, Technology,* Erlangen, Publicis, 211, (117) 123; B. VAN ALSENOY, *Data protection Law in the EU*, *Roles, Responsibilities and Liability*, Mortsel, Intersentia, 2019, 353.
[52] Bron afbeelding: B. VAN ALSENOY, *Data protection Law in the EU*, *Roles, Responsibilities and Liability*, Mortsel, Intersentia, 2019, 351.

Authentieke registers

31. Authentieke registers zijn dus centrale databanken of opslagplaatsen van informatie over burgers binnen een bepaalde context. Denk hierbij bijvoorbeeld aan het Rijksregister dat de namen, adressen, rijksregisternummers, … van, onder andere, alle Belgen bevat.[53]

Om overheden efficiënter te laten werken en administratieve procedures verder te vereenvoudigen, werd het "only-once-principe" wettelijk in het de Belgische e-government beleid verankerd.[54] Dit principe houdt in dat persoonlijke gegevens van burgers slecht eenmalig door een overheid mogen worden verzameld. na de verzameling moeten overheden zelf de informatie uitwisselen en hergebruiken.[55] Overheden kunnen dus in principe alle informatie die nodig is voor hun werking binnen een bepaalde context samenvoegen in één authentiek register. In de praktijk werkt België echter met gegevensuitwisselingsplatformen (zoals MAGDA in Vlaanderen) die verschillende authentieke registers ontsluiten en benodigde informatie ophalen en doorspelen naar andere overheidsdiensten. Reeds eerder werd aangegeven dat Belgische en Vlaamse overheden voor de identificatie verplicht zijn gebruik te maken van het rijksregisternummer (zie *supra* randnr. 28).

32. Pijl (1) geeft de relatie tussen de burger en de authentieke registers weer en geeft het proces weer waarin de burger zijn gegevens doorgeeft, bewijst, verifieert, rechtzet, … Omgekeerd zal de bron een identificatiemiddel (zoals een rijksregisternummer) toekennen aan de burger. Een deel van de gegevens vervat in de authentieke registers kunnen dan later gebruikt worden om authenticatiegegevens te bekomen.[56]

credentievoorzieningsservice

33. Credenties kunnen worden gedefinieerd als stukjes informatie die doen blijken dat bepaalde beweringen beschouwd kunnen worden als feiten. Credenties worden vaak opgedeeld in drie categorieën: Iets dat je weet (bijvoorbeeld een unieke code, een paswoord, het antwoord op een veiligheidsvraag), iets dat je hebt (zoals een SIM kaart, een bankkaart, een identiteitskaart) en iets dat je bent (bijvoorbeeld biometrische gegevens zoals een vingerafdruk). Vaak zitten zij vervat in tokens die zowel de vorm van hardware -zoals een eID- of software kunnen aannemen.[57]

[53] J. C. BUITELAAR, M. MEINTS en B. VAN ALSENOY, "Conceptual framework for identity management in e-government"*, FIDIS Project,* 2008, nr. 16.1, 45; D. DE BOT, *E-government in het federale België .* Brussel, Politeia, 2015, 474; IBZ, *Rijksregister*, https://www.ibz.rrn.fgov.be/nl/rijksregister/, laatst bezocht 14 december 2022.
[54] Artikel 2 Wet houdende de verankering van het principe van de unieke gegevensinzameling in de werking van de diensten en instanties die behoren tot of taken uitvoeren voor de overheid en tot vereenvoudiging en gelijkschakeling van elektronische en papieren formulieren, *BS* 4 juni 2014. (Hierna only once wet).
[55] D. DE BOT, "De Wet only Once – een wetgevende verankering van het beginsel van unieke gegevensinzameling", *P&I* 2014, nr. 166, (186) 186. D. DE BOT, *E-government in het federale België .* Brussel, Politeia, 2015, 327.
[56] B. VAN ALSENOY, *Data protection Law in the EU*, *Roles, Responsibilities and Liability*, Mortsel, Intersentia, 2019, 354-355.
[57] Gegevenbeschermingsautoriteit (GBA), advies over een ontwerpbesluit van de Regering van de Franse Gemeenschap tot het bepalen van de categorieën van persoonsgegevens die worden verwerkt met betrekking tot de doeleinden van de digitale ruimten in toepassing van de artikelen 6 en 11 van het decreet van 25 april 2019 betreffende het digitaal bestuur van het schoolsysteem en de overdracht van digitale gegevens in het leerplichtonderwijs, 5 november 2020, nr. 108/2020, 6

Een credentievoorzieningsservice is de entiteit die deze credenties zal toekennen en beheren. Het is belangrijk te begrijpen dat de credentievoorzieningsservice zich enkel met de credenties zelf bezighoudt en dus niet per se met de tokens die de credenties bevatten hoewel dit wel mogelijk is.[58]

34. Verschillende credenties hebben een verschillend betrouwbaarheidsniveau[59] dat weergeeft hoeveel vertrouwen de vertrouwende partij erin kan hebben dat de burger ook echt is wie hij zegt dat hij is.[60] Via de eIDAS verordening, die grotendeels gebaseerd werd op het STORK project en ISO standaard 29115, probeert Europa standaarden te implementeren die het mogelijk moeten maken om ook over landsgrenzen heen aan identiteitsmanagement te doen en die bepaalde veiligheidsvereisten introduceren. (zie *infra* randnrs 109 en 126).

35. Zoals bovenstaande afbeelding weergeeft, vinden er zowel interacties plaats tussen de credentievoorzieningsservice en de authentieke registers als tussen de credentievoorzieningsservice en de burger. In het eerste geval gaat het over de data van de authentieke registers die credentievoorzieningsservice nodig heeft om de credenties aan te maken. In het tweede geval gaat het over het uitvaardigen van de credentie aan de burger of de vraag van de burger om een bepaalde credentie stop te zetten of aan te passen zoals bijvoorbeeld bij het vergeten van een paswoord. Ten slotte vindt er ook een interactie plaats tussen de credentievoorzieningsservice en de verificator die, eventueel na tussenkomst van een integrator, nagaat of de opgegeven credentie van een bepaalde burger de juiste is.

Vertrouwende partij

36. De vertrouwende partij is de partij die vertrouwt op de correctheid van de identiteitsinformatie. Zoals eerder aangegeven is het binnen een overheidscontext de overheidsdienst die er op moet kunnen vertrouwen dat het zijn diensten aanbiedt aan de correcte burger. De vertrouwende partij kan zelf zijn authentificatieprocessen organiseren of deze toevertrouwen aan een (externe) derde partij.

Dienstenintegratoren

37. een dienstenintegrator is een platform dat interactie tussen verschillende entiteiten die persoonsgerelateerde diensten aanbieden of nodig hebben mogelijk maakt. Om dit te bewerkstelligen in het kader van authenticatieprocessen zal de dienstenintegrator een lijst van de credentievoorzieningsservices moeten opstellen en bijhouden, zodat hij, wanneer de vertrouwende partij hierom verzoekt, de nodige bronnen ter beschikking heeft om deze van de nodige attesten te voorzien. De dienstenintegrator zal dan de informatie die het krijgt van de credentievoorzieningsservice vertalen naar een format dat begrijpbaar is voor de verificator. Een andere mogelijkheid is dat de dienstenintegrator zelf de nodige identiteitsinformatie zal verzamelen en verifiëren vanuit verschillende bronnen om zo te bepalen of zij in aanmerking komen als

[58] D. DE COCK, B. VAN ALSENOY, B. PRENEEL en J. DUMORTIER, "The Belgian eID approach", in W. FUMY en M. PAESCHKE, *Handbook of eID Security. Concepts, Practical experiences, Technology,* Erlangen, Publicis, 211, (117) 126; A. VEDDER, *Security and Law,* Mortsel, Intersentia, 2019, 163.
[59] De zogenaamde Level of Assurance of LoA
[60] Overweging 16 Verord.Raad.Parl Nr. 910/2014, 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, *Pb.L* 28 augustus 2018, afl. 257, 73. (Hierna eIDAS verordening); A. VEDDER, *Security and Law,* Mortsel, Intersentia, 2019, 167.

authenticatiemiddel.[61] De meest gekende dienstenintegratoren in België zijn de Kruispuntbank voor sociale zekerheid op federaal niveau en het MAGDA platform op Vlaams niveau.[62]

Verificator

38. De verificator ten slotte is de entiteit die de identiteitsinformatie bevestigd aan de vertrouwende partij. De verificator zal met andere woorden de credenties die de gebruiker voorlegt aan de vertrouwende partij verifiëren voordat de gebruiker toegang krijgt tot de gegevens van de dienst van de vertrouwende partij. De verificator zal aan de burger/gebruiker een bepaald authenticatieprotocol voorleggen dat kan variëren afhankelijk van het gewenste betrouwbaarheidsniveau.(zie *supra* randnummer 34). Zo kan het voor sommige diensten voldoende zijn om in te loggen met een e-mailadres en paswoord, terwijl het voor andere diensten -die met gevoeligere informatie werken- nodig zal zijn om via versleutelde informatie een reactieprotocol te doorlopen zoals bijvoorbeeld het invoeren van een bankkaart in een kaartlezer, invoeren van de geheime code en doorgeven van de code die op de kaartlezer verschijnt. Het hoeft niet te verbazen dat in verband met overheidsdiensten het niet voldoende zal zijn om te werken met louter een e-mailadres en paswoord of social media account. Eerder zal er gekozen worden voor systemen die werken met PKI (zie *supra* randnummer 28) en/of digitale handtekeningen. Een typisch voorbeeld van een verificator is een authenticatiedienst zoals de Federal Authentication Service (FAS).[63]

39. Deze laatste entiteit brengt zo het hele identificatie- en authenticatieproces in kaart: De burger -met digitale identiteit- doet beroep op de diensten van de vertrouwende partij, waarop er een interactie ontstaat met de verificator die na het doorlopen van het authenticatieprotocol en eventueel na tussenkomst van een dienstenintegrator zal nagaan bij de credentievoorzieningsservice of de ingevoerde gegevens overeenkomen met de credenties toegewezen aan de burger. De credentievoorzieningsservice zal daaropvolgend de credentie valideren of afwijzen waarna de vertrouwende partij uiteindelijk het resultaat van het authenticatieproces te zien krijgt.

40. Momenteel zijn er in België twee veelgebruikte middelen om jezelf te authenticeren voor het gebruik te kunnen maken van overheidsdiensten zoals MyMinFin: Door gebruik te maken van je eID en een kaartlezer of door beroep te doen op de app Itsme. De werking van de laatste optie wordt in onderstaand deel van deze scriptie uitvoerig besproken. Voor de werking van de eID volstaat het te weten dat deze kaart verschillende functies heeft waaronder dus het online identificeren van personen en het creëren van authenticerende handtekeningen. Hiertoe bezit de kaart vijf certificaten waarvan er dus twee verbonden zijn aan de kaarthouder waarmee hij of zij zichzelf kan authenticeren en rechtsgeldige digitale handtekeningen kan plaatsen.[64] Naast de eID en de Itsme app, is er een nieuw privaat initiatief op de markt gekomen onder de naam MyID dat op gelijkaardige wijze als de Itsme app werkt (doch via het gebruik van QR codes) maar waarvan de functie om in te loggen voor overheidsdiensten op moment van schrijven niet langer beschikbaar is omwille van

[61] B. VAN ALSENOY, *Data protection Law in the EU*, *Roles, Responsibilities and Liability*, Mortsel, Intersentia, 2019, 357.
[62] D. DE BOT, *E-government in het federale België .* Brussel, Politeia, 2015, 820.
[63] B. VAN ALSENOY, "E-Government solutions: Trends and developments in Belgian e-government", in M. MEINTS en H. ZWINGELBERG, *Identity Management Systems – recent developments,* FIDIS, nr. D.3.17, 2009, 41; B. VAN ALSENOY, *Data protection Law in the EU*, *Roles, Responsibilities and Liability*, Mortsel, Intersentia, 2019, 366; D. DE BOT, *E-government in het federale België .* Brussel, Politeia, 2015, 358.
[64] A. VEDDER, *Security and Law,* Mortsel, Intersentia, 2019, 169.

beveiligingsproblemen. Ook de overheid zelf zou bezig zijn aan het creëren van een digitale portefeuille die een eigen (en dus publiek georganiseerde) authenticatiedienst zou bevatten. Ten slotte valt nog op te merken dat er ook gekozen kan worden om in te loggen bij de overheidsdiensten door gebruik te maken van een tokenkaart -deze kunnen echter niet langer aangevraagd worden bij de overheid wat dit systeem dus uitdovend maakt-[65] en een tweestapsverificatie via de eIDkaartlezer en e-mail of sms voor het creëren van een gebruikersnaam en paswoord. Deze systemen worden hier echter niet verder besproken.

C. Werking authenticatiemiddelen zoals Itsme en myID

a) Algemeen

41. Zoals bepaald in de wet van 18 juli 2017 inzake elektronische identificatie, is het de Federale overheidsdienst Beleid en Ondersteuning (BOSA) die binnen het CSAM[66] belast werd met "het aanbieden van elektronische aanmeldingsdiensten voor overheidstoepassingen binnen de authenticatiedienst".[67] De FOD BOSA is in zijn rol ook gemachtigd om gegevens uit het rijksregister te verwerken en te delen.[68] Het is daarnaast de FOD BOSA zelf die instaat voor de organisatie van deze authenticatiedienst.[69] Binnen deze authenticatiedienst mogen private instanties dan hun diensten voor de elektronische identificatie voor toegang tot overheidstoepassing, onder bepaalde voorwaarden (zie hoofdstuk II), aanbieden.[70] De Federale Overheidsdienst BOSA gaf uitvoer aan zijn taak met de oprichting van de FAS (Federal Authentication Service), dat aldus dienst zal doen als verificator. Op gewestelijk niveau maakt ook het Vlaamse toegangsbeheer (ACM) als onderdeel van het Agentschap Digitaal Vlaanderen gebruik van de diensten van de FAS.[71]

b) FAS

42. De FAS is dus de dienst die de burger zal authenticeren voor zij toegang krijgt tot de online overheidsdiensten. Wanneer een burger naar een bepaalde online overheidsdienst gaat, zal hij of zij door de FAS omgeleid worden naar het federaal (of Vlaams) portaal voor authenticatie. Daar biedt zij aan de burger een loginscherm aan dat de nodige authenticatiegegevens van de eindgebruiker opvraagt. Eens die zijn ingegeven zal de FAS de burger terugleiden naar de site van de overheidsdienst samen met een antwoordbericht dat de authenticatie-informatie bevat waarop de overheidsdienst als gebruiker van de FAS kan beslissen om de burger toegang te verlenen tot zijn diensten. De dienst heeft nu wel zekerheid over de authenticiteit van de burger die op zijn diensten beroep doet. De FAS doet beroep op verschillende authenticatiemiddelen, ook bekend als digitale sleutels, waaronder een eenvoudig paswoord/wachtwoordsysteem, software sleutelsystemen zoals

[65] Zie hierover https://www.vlaanderen.be/federaal-token.
[66] CSAM is "een geheel van afspraken en van regels om het identiteits- en toegangsbeheer binnen het e-government te organiseren".
[67] Art. 9 §1 wet van 18 juli 2017 inzake elektronische identificatie, *BS* 9 augustus 2017. (hierna wet elektronische identificatie).
[68] Ibid., art 5 *io.* art 1-3 Kb van 1 februari 2018 tot aanwijzing van instanties conform de wet van 18 juli 2017 inzake elektronische identificatie, *BS* 9 februari 2018.
[69] Art. 9§2 wet elektronische identificatie.
[70] Art. 10 wet elektronische identificatie.
[71] Art. 2 Besluit van de Vlaamse Regering 18 maart 2016 houdende de oprichting van het intern verzelfstandigd agentschap [Digitaal Vlaanderen] en de vaststelling van de werking, het beheer en de boekhouding van het [Eigen Vermogen Digitaal Vlaanderen, *BS* 2 juni 2016.

Itsme, meID en de eID in combinatie met de kaartlezer (hardware).[72] Verschillende sleutels hebben een verschillend beveiligingsniveau en het komt toe aan de overheidsdienst zelf om te bepalen welke van deze authenticatiemiddelen zij wensen in te zetten om de toegang tot hun diensten te controleren.[73] Het zijn bovendien de overheidsdiensten die gebruik maken van het FAS zelf die verantwoordelijk zijn voor de beveiliging van de computers (en paswoorden van deze computers) waarop de toepassing werd geïmplementeerd.[74]

c) Itsme

43. Itsme is dus een erkende dienstverlener binnen de FAS die zorgt voor een digitale sleutel die gebruikt kan worden door verschillende overheidsdiensten[75] ter verificatie van de identiteit van de burger die gebruik wil maken van de dienst. De app werd ontwikkeld door het private consortium Belgium Mobile ID NV, dat bestaat uit zeven private aandeelhouders uit de bank- en telecommunicatiesector[76] en één publieke aandeelhouder: De Federale Participatie- en InvesteringsMaatschappij (FPIM) wat het dus tot een project van publiek-private samenwerking maakt.

44. De Itsme app bevat verschillende functies. Gebruikers kunnen kort samengevat: zichzelf registreren bij dienstverleners -wat een uitwisseling van persoonlijke gegevens, zoals opgeslagen door de Itsme app inhoudt-; inloggen; transacties goedkeuren en documenten digitaal ondertekenen met een gekwalificeerde elektronische handtekening.[77] Om deze diensten te kunnen aanbieden verzamelt en verwerkt Belgium Mobile ID verschillende persoonsgegevens die hieronder kort besproken worden.[78] Alle gebruikers van de Itsme app zijn verplicht de algemene voorwaarden en de privacyverklaring van Itsme te aanvaarden.[79]

Identificatiegegevens

45. Dit zijn de gegevens die het toelaten de gebruiker te identificeren. Het gaat onder andere over alle gegevens die ook terug te vinden zijn op een eID zoals naam, geslacht, adres, geboorteplaats, pasfoto, ID nummer en nummer van het rijksregister. Daarnaast gaat het ook om de contactinformatie van de gebruiker en enkele gebruikersinstellingen zoals een leveringsadres of de hoedanigheid waarin men handelt. Opvallend genoeg behoudt de app zich ook het recht voor om de biometrische gegevens van de gebruiker te verwerken indien de overheid dit wettelijk zou verplichten. De gebruiker zou hiervoor weliswaar zijn expliciete toestemming voor moeten geven.[80]

---

[72] BOSA, *Gebruiksovereenkomst FAS. Versie 6.5*, 2022, 3, https://bosa.belgium.be/sites/default/files/content/documents/DTdocs/FAS/GO_DT_FAS_6.5_20221005_NL.pdf laatst bezocht 15 december 2022.
[73] *Ibid*., 5.
[74] *Ibid*.
[75] Doch ook door niet overheidsdiensten zoals banken, verzekeringsmaatschappijen, verzorgingsinstellingen,…
[76] Belfius, BNP Paribas Fortis, ING, KBC, Orange, Proximus en Telenet.
[77] BELGIAN MOBILE ID, *Algemene voorwaarden itsme app Versie 3.2*, Brussel, 2022, https://www.itsme-id.com/nl-BE/legal/app-terms-and-conditions, 2, Laatst bezocht: 23 maart 2023.
[78] BELGIAN Mobile ID, *Privacybeleid: Itsme app en diensten. Versie 3.1,* Brussel, 2022, https://www.itsme-id.com/nl-BE/legal/app-privacy-policy, 2, laatst bezocht 23 maart 2023.
[79] BELGIAN MOBILE ID, *Algemene voorwaarden itsme app Versie 3.2*, Brussel, 2022, https://www.itsme-id.com/nl-BE/legal/app-terms-and-conditions, 1, Laatst bezocht: 23 maart 2023.
[80] BELGIAN Mobile ID, *Privacybeleid: Itsme app en diensten. Versie 3.1,* Brussel, 2022, https://www.itsme-id.com/nl-BE/legal/app-privacy-policy, 2, laatst bezocht 23 maart 2023.

De identificatiegegevens worden ofwel rechtstreeks van de gebruiker verkregen of via de identiteitscontroleur waar men zich inschreef voor de app (bijvoorbeeld de bank).[81]

Veiligheidsgegevens

46. Veiligheidsgegevens hangen vast aan het toestel dat gebruikt wordt om de app te installeren en de identiteit van de gebruiker aan dat toestel te binden. Het gaat hier bijvoorbeeld om: het merk van het toestel, het operating system, … Deze gegevens worden rechtstreeks van het toestel verzameld.[82]

Transactiegegevens

47. De transactiegegevens zijn de gegevens van de verschillende diensten waarvan de gebruiker gebruik gemaakt heeft. Er wordt onder andere bijgehouden welke dienst (registratie, identificatie, transactie of digitale handtekening) naar welke dienstverlener werd verstuurd, wanneer dit gebeurde en of de transactie geslaagd is of niet.[83] Transactiegegevens worden deels door de app zelf gegenereerd en deels door de dienstverlener/overheidsdienst verstuurde gegevens.

Inschrijvingsgegevens

48. Inschrijvingsgegevens zijn de gegevens die verbonden zijn aan het registratieproces van de Itsme app. De inschrijvingsgegevens bevatten onder andere de instemming met de algemene voorwaarden en het privacybeleid en wanneer deze werd gegeven. De inschrijvingsgegevens worden ofwel rechtstreeks verkregen bij het registreren bij Itsme via de website ofwel via de identiteitscontroleur.[84]

Handtekeninggegevens

49. De handtekeninggegevens tenslotte zijn alle mogelijke gegevens die voor de app nodig zijn om elektronische handtekeningen te kunnen valideren of het kunnen creëren van een gekwalificeerde elektronische handtekening, zoals bepaald onder de eIDAS verordening (zie *infra* hoofdstuk III). Handtekeninggegevens zijn een combinatie van identificatie en transactiegegevens en worden aldus op dezelfde wijze bekomen.[85]

50. De persoonsgegevens zullen door Belgian Mobile ID bij elk van de vier Itsme diensten verwerkt worden, alsook bij het registreren bij Itsme zelf, wanneer deze gegevens bijgewerkt moeten worden of wanneer de gebruiker over de diensten van Itsme of Belgian Mobile ID moet worden geïnformeerd. Alle identificatiegegevens die worden doorgegeven aan de diensten waarop de burger beroep wil doen, worden ook verwerkt door die dienst volgens hun eigen privacybeleid. Volgens het privacybeleid van Itsme zelf treden zij ter uitvoering van de door hen aangeboden vier diensten op als verwerkingsverantwoordelijke. De biometrische authenticatiemethoden die in de app zelf gebruikt worden (zoals de vingerafdruk) zijn verwerkingen die gebeuren op het apparaat en worden niet

[81] *Ibid*., 1, 3.
[82] *Ibid*., 2.
[83] *Ibid*.
[84] *Ibid*.
[85] *Ibid*.

doorgegeven aan Belgian Mobile ID en vallen aldus onder de verantwoordelijkheid van het apparaat waarop de app werd geïnstalleerd.[86]

Alle gegevens worden na het stopzetten van het gebruik van de Belgian Mobile ID diensten of na een inactiviteit van twee jaar nog tien jaar bewaard met als enige uitzondering de transactiegegevens die voor een periode van tien jaar na de transactie zullen worden bewaard.[87]

d) myID

51. myID is een authenticatieapp ontwikkeld door het volledig private U2U consult en werkt op een gelijkaardige wijze als de Itsme app. Het grote verschilpunt is dat myID ter authenticatie werkt met een QR-code in plaats van een gsm-nummer. Een groot voordeel van deze werkwijze ten opzichte van de Itsme app, was het feit dat gebruikers geen Belgisch telefoonnummer nodig hadden om er gebruik van te kunnen maken. Dit speelde uiteraard in het voordeel van bijvoorbeeld Belgen die lange tijd in het buitenland verblijven en geen Belgisch telefoonnummer wensen te houden. Echter werd dit euvel sinds enkele jaren opgelost doordat burgers ook via een internationaal telefoonnummer gebruik kunnen maken van Itsme.

Hoewel de privacyverklaring van myID enkel melding maakt van de verwerking van de naam, het rijksregisternummer en de nationaliteit van de gebruiker alsook de gegevens betreffende het aanmelden en het gebruik van de app, kan men er mijn inziens vanuit gaan dat het verzamelen, verwerken en opslaan van dezelfde gegevens als deze vermeld onder de vorige titel vereist zijn voor het gebruik van de app. Ook U2U consult bewaart zijn gegevens voor een periode van tien jaar, zij het dat bij gebruik van deze app de periode reeds begint te lopen vanaf de actie waarvoor de gegevens verwerkt werden.[88]

52. Gezien de grote gelijkenissen tussen de myID en Itsme applicaties, zullen zij voor de rest van deze scriptie als gelijke producten worden beschouwd tenzij verdere nuancering vereist is.

e) De digitale portefeuille

53. Volgend uit een verplichting die het ontwerp tot herziening van de eIDAS verordening oplegt aan de lidstaten (Zie *infra* hoofdstuk III),[89] verklaarde huidig staatssecretaris voor digitalisering Mathieu Michel dat ook de Belgische federale overheid aan het werken is aan een volledig publiek georganiseerd alternatief voor Itsme en myID.[90] Het alternatief zou kaderen binnen de grotere verplichting tot het voorzien van een volledige "European Digital Identity Wallet" (ook wel digitale portefeuille genoemd) die in de vorm van een app op de smartphone zal kunnen worden gebruikt. Het is de bedoeling de app in de loop van 2023 uit te brengen. Binnen de digitale portefeuille zal de overheid voor iedere burger een digitale identiteit ontwikkelen die het (via blockchaintechnologie)[91]

[86] *Ibid*., 4.
[87] *Ibid*. 5.
[88] U2U consult, *Privacy policy. Versie 2.0.1*, 2022, https://myid.be/privacy.
[89] Art. 1 (7) Voorstel (Comm.) voor een verordening van het Europees parlement en de raad tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit, 3 juni 2021, COM(2021) 281 final 2021/0136 (COD).
[90] Algemene beleidsnota digitalisering, administratieve vereenvoudiging, privacy en regie der gebouwen*, Parl.St.* Kamer 2022-2023, nr. 2934/010, 7.
[91] A. JOUSTEN en X. MINY, "Blockchain et droit Public, menace et/ou atout pour l'Etat?" in A. VANDENBULCKE (ed.), *Les aspects juridiques de la blockchain et de ses applications*, in Limal, Anthemis, 2022, (127) 146.

mogelijk zal maken de burger te identificeren en authenticeren.[92] Het is belangrijk te benadrukken dat het authenticatiesysteem dat mee met de app ontwikkeld zal worden, niet de bedoeling heeft om de andere (privaat georganiseerde) authenticatiesystemen die nu bestaan te vervangen. Wel zal zij een bijkomend alternatief voor deze systemen vormen.[93]

54. Wat de verdere uitwerking van de authenticatiecomponent van deze digitale portefeuille betreft zijn er verder nog maar weinig details bekend. De enige zekerheid lijkt voorlopig te zijn dat het zou gaan om een volledig publieke dienst dat de keuzevrijheid van de burger zou moeten vergroten. Wat de gevolgen daarvan zijn binnen het wettelijk kader voor authenticatiesystemen wordt duidelijk in volgende hoofdstukken.

D. Conclusie

55. In dit eerste hoofdstuk werd een antwoord gezocht op de vraag naar de praktische werking en organisatie van authenticatiemechanismen en hun plaats binnen het nationale en Vlaamse e-gov beleid. Het werd duidelijk dat door de groeiende digitalisatie van het bestuur steeds meer interacties tussen burger en overheid digitaal gebeuren waardoor er een groeiende nood ontstaat aan een correct en betrouwbaar identiteitsbeheer dat toegang verleent tot deze digitale overheidsdiensten.

56. Om aan deze nood tegemoet te komen ontwikkelde België een identiteitsmanagementstrategie die enerzijds overheden verplicht tot het gebruik van het Rijksregisternummer of identificatienummer van de Kruispuntbank voor de identificatie van natuurlijke personen en anderzijds overheden toelaat om via de eID en PKI op een betrouwbare manier deze burger te authenticeren.

Binnen dit identificatie- en authenticatieproces werd een onderlinge interactie tussen drie tot zes entiteiten vastgesteld waardoor de rol van authenticatiemechanismen als onderdeel van de door het CSAM en FOD BOSA opgerichte FAS dat dienst doet als verifier duidelijk werd. Zo zullen authenticatiemechanismen -zoals aangeboden door Itsme- dienst doen als digitale sleutel om de identiteitsinformatie zoals zij werd verstrekt door de burger te gaan verifiëren bij de credentievoorzieningsservice, vaak door middel van een multifactor-authenticatie dat een hoger niveau van betrouwbaarheid aanbiedt dan een single factor authenticatie.

57. Momenteel bestaan er in België (naast de methode van de klassieke eID) twee verschillende authenticatiemechanismen: Het privaat georganiseerde "myID" -dat momenteel weliswaar zijn vergunning is verloren- en het publiek-private "Itsme". Daarnaast heeft huidig staatssecretaris M. MICHEL de ambitie om nog voor het einde van het jaar een bijkomend alternatief uit te werken als onderdeel van de zogenaamde "digitale portefeuille".

58. Ten slotte is het belangrijk te beseffen dat om hun taak als authenticator uit te voeren, de uitgevers van deze mechanismen op grote schaal gevoelige persoonsgegevens zullen moeten verwerken en bewaren.

---

[92] Algemene beleidsnota digitalisering, administratieve vereenvoudiging, privacy en regie der gebouwen*, Parl.St.* Kamer 2022-2023, nr. 2934/010, 8.
[93] *Vr. en Antw*. Kamer 2022-2023, 30 september 2022, nr. 0379, (Vr. 11 S. CREYELMAN, antw. M. MICHEL).

Hoofdstuk II wettelijk kader Elektronische identificatie voor Belgische overheidstoepassingen

A. Algemeen

59. In 2017 erkende de Belgische uitvoerende macht de noodzaak voor burgers om zich online te kunnen identificeren en authenticeren om zo gebruik te kunnen maken van de online overheidsdiensten. Op 8 juni diende toenmalig minister van Ontwikkelingssamenwerking, Digitale agenda, Telecommunicatie en Post Alexander de Croo een wetsontwerp in dat het enerzijds mogelijk moet maken de eIDAS verordening (zie *infra* Hoofdstuk III) volledige uitwerking in de interne rechtsorde te verlenen en anderzijds de Federale Authenticatiedienst wettelijk diende te verankeren en in mogelijkheden moest voorzien om diensten, die elektronische identificatie mogelijk maken met het oog op toegang tot de Belgische overheidsdiensten, te erkennen.[94] In wat volgt in dit hoofdstuk zal de tweede doelstelling van de wet inzake elektronische identificatie verder besproken worden. In hoofdstuk III zal dieper worden ingegaan op de rol van de eIDAS verordening betreffende authenticatiemiddelen.

B. Wet inzake elektronische identificatie

a) Algemeen

60. Zoals reeds eerder beschreven (zie *supra* randnr. 41) is het de wet inzake elektronische identificatie die de FOD BOSA belast met het zorgen voor de beschikbaarheid van een authenticatiedienst en het binnen deze authenticatiedienst aanbieden van elektronische identificatiemiddelen. De FOD BOSA krijgt, om aan zijn verplichtingen te kunnen voldoen, het recht om de identificatienummers van burgers uit het rijksregister te gebruiken.[95] Dit laatste is opvallend omdat ten tijde van de inwerkingtreding van de wet, het -inmiddels opgeheven- sectoraal comité van het rijksregister bevoegd was om machtigingen tot het gebruik van gegevens uit het rijksregister te verlenen.[96] Het is pas sinds de hervormingen doorgevoerd in 2018 dat dit soort bevoegdheden door de minister van binnenlandse zaken of expliciet door of krachtens de wet kan gebeuren.[97]

b) Diensten voor elektronische identificatie aangeboden door private partijen

61. De wet voorziet dat binnen de Federale Authenticatiedienst (FAS), private partijen hun diensten voor elektronische identificatie ter toegang tot online overheidsdiensten kunnen aanbieden eens zij hiervoor een erkenning door de FOD BOSA hebben verkregen.[98] De procedure, voorwaarden en gevolgen van deze erkenning werden door het Kb van 22 oktober 2017 vastgelegd en worden hieronder (zie infra randnr. 68 ev.) besproken.

---

[94] Wetsontwerp (A. DE CROO) inzake elektronische identificatie, *Parl. St.* Kamer 2016-17, nr. 2512/001, 4.
[95] Art. 9 §2 wet inzake elektronische identificatie.
[96] Art. 6 wet 25 maart 2003 t tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *BS* 8 maart 2003; COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (CBPL), advies met betrekking tot het voorontwerp van wet inzake elektronische identificatie, 21 september 2016, nr. 48/2016, 11.
[97] Art. 14 Wet 25 november 2018 houdende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters, *BS* 13 december 2018 *io*. Art. 8 wet 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *BS* 21 april 1984.
[98] Art. 9 §§1-2 wet inzake elektronische identificatie.

62. Ondanks de expliciete belasting van de Koning met het uitwerken van de erkenning voor diensten inzake elektronische identificatie, worden enkele zaken alsnog door de wet zelf geregeld. Zo bepaalt artikel 10 §5 van de wet dat de erkende aanbieder van de identificatiedienst beschouwd wordt als een onderaannemer van de erkennende overheid (FOD BOSA) en dat zij via de authenticatiedienst (FAS) gemachtigd is om de rijksregisternummers van burgers te gebruiken, zij het uitsluitend voor de aanbieding van de identificatiedienst. Opnieuw valt op dat het hier gaat om een machtiging die -ten tijde van de inwerkingtreding van de wet- niet wettelijk maar via het sectoraal comité diende te gebeuren en die bovendien overbodig is gezien de erkende aanbieders louter via de toekenning van hun status als onderaannemer van BOSA gemachtigd zijn door de bepalingen in de wet tot regeling van een rijksregister de gegevens uit dat rijksregister te gebruiken.[99]

63. Uit de parlementaire voorbereiding blijkt daarnaast dat het gebruik van deze gegevens beperkt zou moeten blijven tot het gebruikers- en toegangsbeheer voor overheidstoepassingen. Terwijl voor andere gebruiksvormen een aparte erkenning zou moeten worden bekomen.[100] Ondanks het advies van de CBPL om expliciet in de wet op te nemen dat "aanbieding van de erkende dienst voor elektronische identificatie" louter het gebruikers- en toegangsbeheer voor overheidstoepassingen inhoudt,[101] koos de wetgever er in de finale teksten voor om het bij de ruim te interpreteren termen te houden. In dezelfde optiek gaf het CPBL het advies om expliciet in de wet te verbieden dat de gegevens voor commerciële doeleinden door de (private) aanbieders van identificatiediensten mogen worden gebruikt. Opnieuw werd het advies echter in de wind geslagen en moeten we ons beperken tot de memorie van toelichting die -opnieuw in brede termen en weinig concreet- stelt dat "*er garanties gevraagd zullen worden om te beletten dat gegevens voor andere doeleinden dan identificatie en authenticatie kunnen worden gebruikt*" en verwijst naar het uitvoeringskb (zie *infra* randnr. 68).[102]

64. Artikel 11 van de wet inzake elektronische identificatie legt ten slotte aan de houder van een elektronisch identificatiemiddel de verplichting op om alle nodige maatregelen te treffen om "*het elektronisch identificatiemiddel onder zijn exclusieve controle te houden, om diefstal, verlies of verspreiding van zijn elektronisch identificatiemiddel te voorkomen en om in geval van diefstal, verlies of verspreiding zijn elektronisch identificatiemiddel onmiddellijk te laten intrekken*." Wanneer het middel vervalt of wordt ingetrokken, mag de houder het niet meer gebruiken. Concreet houdt dit volgens de memorie van toelichting onder meer in dat de gebruiker/burger het middel onder zijn exclusieve controle moet houden en dus maatregelen moet nemen om diefstal of verlies te voorkomen en zijn paswoorden strikt confidentieel dient te houden.[103] In het licht van de werking van diensten zoals Itsme en myID zal deze verplichting dus onder meer inhouden dat burgers er

[99] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (CBPL), advies met betrekking tot het voorontwerp van wet inzake elektronische identificatie, 21 september 2016, nr. 48/2016, 12.
[100] Memorie van toelichting bij Wetsontwerp (A. DE CROO) inzake elektronische identificatie, *Parl. St.* Kamer 2016-17, nr. 2512/001, 15.
[101] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (CBPL), advies met betrekking tot het voorontwerp van wet inzake elektronische identificatie, 21 september 2016, nr. 48/2016, 12.
[102] Memorie van toelichting bij Wetsontwerp (A. DE CROO) inzake elektronische identificatie, *Parl. St.* Kamer 2016-17, nr. 2512/001, 12.
[103] *Ibid*. 16.

voor moeten waken dat zij hun eID en/of gsm waarop de apps reeds geïnstalleerd staan niet verliezen of minstens dat zij hun unieke codes niet delen met derden.[104]

65. Hoewel deze bepaling op het eerste zicht perfect verdedigbare verplichtingen oplegt, duiken er toch enkele moeilijkheden op. Zo wijst de CBPL er -mijn inziens terecht- op dat de verplichtingen die voortvloeien uit artikel 11 niet haalbaar zijn voor delen van de bevolking die, bijvoorbeeld omwille van ziekte of mentale of fysieke onmogelijkheid, al dan niet tijdelijk niet meer in staat zijn om zelf hun betrekkingen met de overheid te regelen. Men kan zich dan ook afvragen of deze mensen in het licht van de verplichting deels mede verantwoordelijk zullen worden gehouden bij misbruik door een derde.[105]

c) Conclusie

66. In het eerste onderdeel van dit hoofdstuk werd dieper ingegaan op de wet die het mogelijk moet maken om diensten van aanbieders van authenticatiemechanismen te laten erkennen. Eens die erkenning is bekomen, zal de aanbieder van de authenticatiedienst beschouwd worden als een onderaannemer van de FOD BOSA en gemachtigd zijn om rijksregisternummers van burgers te gebruiken. Dit was, gezien de verplichting voor overheden om voor de identificatie van burgers gebruik te maken van dit nummer (zie *supra* randnr. 28), uiteraard noodzakelijk.

67. Wat betreft bescherming voor de burger betreffende het gebruik van persoonlijke informatie door een derde partij, liet de wetgever het finaal na om expliciet te verbieden dat aanbieders van authenticatiemechanismen de gegevens voor andere doeleinden dan het gebruikers- en toegangsbeheer mogen verwerken. Er werd daarnaast ook geen verbod over het gebruik voor commerciële doeleinden opgelegd. Opvallend genoeg wordt de burger zelf strenger behandeld en geldt voor eenieder de verplichting om de exclusieve controle te behouden over de persoonlijke identificatiemiddelen. Een verplichting die voor delen van de bevolking wel eens tot problemen zou kunnen leiden.

Wie (voorlopig?) wel ontsnapt aan verdere regulering zijn de overheden zelf die gebruik zullen maken van de erkende authenticatiemechanismen. De verdere uitwerking van het wettelijk kader wordt weliswaar gedelegeerd aan de uitvoerende macht. Die verdere uitwerking wordt in wat hier volgt verder besproken.

C. Erkenningsvoorwaarden

a) Algemeen

68. Met het Kb van 22 oktober 2017 werd verdere uitvoering gegeven aan de artikelen 9 en 10 van de hierboven beschreven identificatiewet. Het Kb werkt een nationale erkenningsregeling uit voor de e-identificatiediensten door de functionele en technische specificaties vast te leggen waaraan deze diensten moeten voldoen om de identiteit van de burger die beroep wenst te doen op overheidsdiensten te verifiëren. Het Kb van 2017 vervangt het eerdere koninklijk besluit van 17 juli

[104] Orb. Antwerpen (afd. Antwerpen) 22 november 2022, *DAOR* 2023/1, nr. 143, (17) 18.
[105] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (CBPL), advies met betrekking tot het voorontwerp van wet inzake elektronische identificatie, 21 september 2016, nr. 48/2016, 12.
[105] Memorie van toelichting bij Wetsontwerp (A. DE CROO) inzake elektronische identificatie, *Parl. St.* Kamer 2016-17, nr. 2512/001, 13.

2014 dat de voorwaarden, procedure en gevolgen van de erkenning van niet-verbonden aanmeldingsmiddelen zoals authenticatie via de eID met kaartlezer regelde.[106]

b) Betrouwbaarheidsniveaus

69. Om via de FAS erkend te kunnen worden als aanbieder van een authenticatiedienst om gebruik te kunnen maken van overheidsdiensten, moet de aanbieder van de aanmeldoptie een "hoog" of minstens "substantieel" betrouwbaarheidsniveau (zie *supra* randnr. 34) kunnen voorleggen.[107] Met dat verschil dat aanbieders van aanmeldopties met een substantieel betrouwbaarheidsniveau hun diensten slechts zullen kunnen aanbieden voor overheidstoepassingen die slechts een laag of substantieel betrouwbaarheidsniveau vereisen. Aanbieders van aanmeldopties met een hoog betrouwbaarheidsniveau kunnen hun diensten aan alle overheidsdiensten aanbieden.[108] Overheden zijn in principe vrij om te bepalen welk betrouwbaarheidsniveau vereist is om toegang te krijgen tot haar online dienstverlening.[109]

Elke dienstverlener kan steeds meerdere authenticatiemechanismen laten erkennen.[110] Omwille van de groeiende concurrentie doet elke dienstverlener er dan ook goed aan om zijn systeem zo te organiseren dat het gebruikt kan worden voor alle overheidstoepassingen en daarbij alle diensten aanbiedt die nodig zijn voor deze toepassingen. Het is dan ook ondenkbaar dat wanneer de overheid met zijn eigen authenticatiesysteem komt, zij een aanmeldoptie met een lager betrouwbaarheidsniveau dan "hoog" zou lanceren. In België kreeg Itsme het betrouwbaarheidsniveau hoog toegekend, myID het betrouwbaarheidsniveau substantieel.[111] Sinds de lancering van myID werd de erkenning als aanmeldoptie voor overheidsdiensten echter weer ingetrokken omwille van veiligheidsproblemen.

c) Functionele en technische voorwaarden

70. De hoge en substantiële betrouwbaarheidsniveaus kunnen slechts worden verkregen indien er voldaan is aan de voorwaarden zoals zij beschreven staan in 2.2 en 2.3.1 van de bijlage bij uitvoeringsverordening nr. 2015/1502 die de technische specificaties van de eIDAS verordening uitwerkt (zie *infra* hoofdstuk III).[112] Deze specifieke voorwaarden zijn als bijlage achter de scriptie terug te vinden.

71. Verder voorziet het Kb er in dat iedere burger vrij is om zelf te bepalen voor welke erkende dienst zij kiezen om zich online te authenticeren. De dienst moet uiteraard wel voorzien in een registratieprocedure die moet voldoen aan de voorwaarden van punt 2.1 van de bijlage bij uitvoeringsverordening 2015/1502.[113] Iedereen is vrij om meerdere diensten tegelijk te gebruiken,

[106] Koninklijk besluit van 17 juli 2014 tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van diensten voor elektronische identificatie voor digitale overheidstoepassingen die gebruik maken van niet-verbonden aanmeldingsmiddelen, *BS* 8 augustus 2014.
[107] Er zijn drie verschillende betrouwbaarheidsniveaus. In oplopende volgorde: Laag, substantieel en hoog.
[108] Art. 2 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, *BS* 8 november 2017. (Hierna Kb. elektronische identificatie).
[109] Art. 4 §1 wet elektronische identificatie.
[110] *Ibid*., art. 3.
[111] AGENTSCHAP DIGITAAL VLAANDEREN, Toegangsbeheer (ACM): nieuw authenticatiemiddel "myID.be", https://www.vlaanderen.be/digitaal-vlaanderen/nieuwsberichten/toegangsbeheer-acm-nieuw-authenticatiemiddel-myidbe.
[112] Art. 5, art. 6 en art. 8 Kb. elektronische identificatie.
[113] *Ibid*. Art. 8.

over te schakelen van de ene dienst naar de andere en het gebruik van een bepaalde authenticatiedienst al dan niet tijdelijk stop te zetten.[114]

72. Wanneer de burger wenst in te loggen bij de online dienstverlening van de overheid, moet de erkende dienst het uniek identificatienummer (het rijksregister- of kruispuntbanknummer) van deze burger doorsturen naar de overheid in kwestie opdat deze de identiteit van de burger kan vaststellen.[115] Deze uitwisseling van gegevens dient te gebeuren volgens bepaalde technische protocollen die vermeld staan in de technische specificaties die op de website van de FOD BOSA gepubliceerd moeten worden.[116]

Het behoort tot de verplichtingen van de erkende dienst om bij elke aanmeldpoging de nodige misbruikcontroles uit te voeren zodat zij minstens dubbele aanmeldingspogingen, wijzigingen van de inhoud van de uitgewisselde gegevens en derde partijen die zich voordoen als de erkende dienst kunnen opsporen en tegengaan. Ieder van deze misbruiken moet altijd leiden tot het mislukken van de aanmeldpoging. Bovendien moeten er voldoende controlemechanismen aanwezig zijn om verdere mogelijke veiligheidsrisico's proactief te kunnen opsporen. Eens gedetecteerd worden deze risico's gerapporteerd aan de FOD BOSA.[117]

73. Wat de verwerking van persoonsgegevens betreft, bepaalt het kb. expliciet dat de nationale en Europese wetgeving betreffende de bescherming van persoonsgegevens alsook de richtlijnen en adviezen van de CBPL van toepassing zijn op de dienstverleners.[118] Opvallend genoeg wordt er nog verwezen naar de oude wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer die inmiddels werd vervangen door de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en de oude Commissie voor de bescherming van de persoonlijke levenssfeer die sinds 2018 werd vervangen door de gegevensbeschermingsautoriteit (GBA).[119]

Naast de -minstens deels overbodige- verwijzing naar andere dwingende rechtsbronnen, preciseert het kb. dat er voldaan moet zijn aan de voorwaarden van het niveau hoog of substantieel betreffende de verwerking van persoonsgegevens zoals opgenomen in punt 2.3.1 van de bijlage bij uitvoeringsverordening 2015/1502.[120]

74. Daarnaast mogen dienstverleners zoals Itsme en myID niet te weten komen tot welke online overheidsdiensten de burger toegang wenst te bekomen. Wel moet er, ter beveiliging van de persoonlijke levenssfeer, een "beveiligd controlespoor" worden geïnstalleerd dat in staat moet zijn de gegevens per transactie te reconstrueren. De dienstverlener moet daartoe het rijksregisternummer of kruispuntbanknummer, de gekozen dienst voor elektronische identificatie en

[114] *Ibid* art 9 en art. 10.
[115] *Ibid*. art. 11 *io*. Verslag over het ontwerp van het Koninklijk besluit tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van diensten voor elektronische identificatie voor overheidstoepassingen, *Parl.St* Fed.R. 2017-2018, nr. 2017/31391, 2.2.
[116] *Ibid*. art. 12 *io*. Art. 7.
[117] *Ibid*. art 13 *io*. Art. 24.
[118] *Ibid*. art. 14.
[119] Wet tot oprichting Gegevensbeschermingsautoriteit, *BS* 10 januari 2018; Wet van 30 juli 2018 tot bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018; E. KINDT en D. STEVENS, "Recente ontwikkelingen in het gegevensbeschermingsrecht" in C. CONINGS, S. GRANATA, M.-C. JANSSENS, E. KINDT, S. ROVER, D. STEVENS, J. VANHERPE en G. VAN OVERWALLE, *Themis 2022-2023 nr. 125 IP- en ICT-recht*, Antwerpen, Intersentia, 2023, (155) 157.
[120] art. 15 Kb. elektronische identificatie.

het tijdstip van de (poging tot) aanmelding gedurende tien jaar vanaf het moment van aanmelding bijhouden.[121]

Uit de informatie uit het privacy beleid van Itsme en myID (zie *supra* randnrs. 50-51), kunnen we afleiden dat beide bestaande diensten ervoor kiezen om "*voor bewijsdoeleinden*" meer gegevens dan de strikt verplichte te bewaren. Bovendien worden alle niet-transactiegegevens van de Itsme gebruikers vaak veel langer bewaard. Belgian Mobile ID kiest er immers voor om de tienjarige termijn voor alle andere persoonsgegevens dan de transactiegegevens pas te laten starten vanaf het stopzetten van het gebruik van de applicatie of na een inactiviteit van 12 jaar.

Het bewaren van meer gegevens dan de strikt noodzakelijke en de bewaring langer dan de voorgeschreven termijn vanuit de optiek dat de gegevens wel eens van pas zouden kunnen komen, zou problematisch kunnen zijn in het licht van de verplichting tot minimale gegevensverwerking zoals vervat in de AVG (zie hierover *infra* randnr. 172 ev.).[122]

75. Ten slotte moeten de dienstverleners garanderen dat de identificatienummers van hun gebruikers enkel voor de elektronische identificatie en dus niet voor andere (commerciële) doeleinden zullen worden gebruikt.[123] In concreto zullen dienstverleners bij hun partners waarmee zij persoonsgegevens delen contractueel afdwingen dat de privacy en veiligheid van de gegevens die zij verwerken, gegarandeerd moet zijn. Ook bij een eventuele verkoop van de applicaties wordt er verzekerd dat de gegevens enkel verwerkt zullen worden zoals beschreven in het privacy beleid.[124]

Gezien de principiële inter partes werking van contracten, is het nog maar de vraag of zo'n contractuele overeenkomst voldoende garantie biedt dat de persoonsgegevens nooit voor commerciële doeleinden zullen worden gebruikt. Het is immers niet zo dat het gebruik van gegevens voor commerciële doeleinden automatisch een schending van een zorgvuldigheidsverplichting uitmaakt waardoor de gebruiker om wiens gegevens het gaat -en die als een derde moet worden beschouwd in deze contractrelatie- zich zou kunnen beroepen op de tegenwerpelijkheid van de verbintenis.[125] Daarnaast zal dergelijke verwerking niet altijd publiek geweten zijn waardoor actie tegen de verwerking niet steeds mogelijk is. Uiteraard kan er in deze gevallen wel nog steeds beroep worden gedaan op de AVG.

d) Dienstverleningsbeheer

76. De dienstverlener moet voor zijn gebruikers en de overheidsdiensten die gebruik maken van zijn applicatie ondersteunende diensten aanbieden in de vorm van een chatdienst, telefonische beschikbaarheid en een webpagina met veel gestelde vragen. Deze diensten moeten in de drie landstalen worden aangeboden alsook in het Engels voor de burger/gebruiker en minstens beschikbaar zijn tussen 8 en 18u tijdens de werkdagen. Voor de erkennende overheid moeten de

[121] *Ibid*. art. 16.
[122] Art. 5 lid 1 c) AVG *io.* Overweging 39 AVG; D. DE BOT, "Algemene beginselen inzake gegevensverwerking] Het derde beginsel - Het beginsel van minimale gegevensverwerking" in D. DE BOT, *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Mechelen, Wolters Kluwer, 2020, (493) 494.
[123] Art. 17 Kb. Elektronische identificatie.
[124] BELGIAN Mobile ID, *Privacybeleid: Itsme app en diensten. Versie 3.1,* Brussel, 2022, https://www.itsme-id.com/nl-BE/legal/app-privacy-policy, 6-7.
[125] Art. 5.103 Nieuw BW; I. CLAEYS, *Verbintenissenrecht*, Gent, Faculteit Recht en Criminologie, 2019, 14.

ondersteunende diensten 24u/7 beschikbaar zijn in de drie landstalen en dit in de vorm van telefonische ondersteuning en een digitaal platform dat aangeeft aan de erkennende overheid dat haar oproep werd geregistreerd en dat zij zo spoedig mogelijk zal worden beantwoord.[126]

77. Elke zes maanden zal de erkennende overheid nieuwe software versies in overweging nemen die in een volgende software uitrol kunnen worden ingepland. De dienstverlener moet garanties inbouwen die ervoor zorgen dat dit uitrolbeheer gevolgd kan worden. Elke nieuwe softwareversie die een significante impact heeft op de gebruiker moet, samen met een impactanalyse, ten minste één maand voor de geplande uitrol ter goedkeuring worden voorgelegd aan de FOD BOSA die de dan impact van de wijzigingen op de gebruiker kan minimaliseren.[127]

Het ontwikkelen en up-to-date houden van de software speelt uiteraard een belangrijke rol bij de beveiliging van de identificatietoepassingen. Mijn inziens is het een goede zaak dat er met de FOD BOSA een instantie is die de impact van nieuwe software controleert. Het Kb. zorgt er op deze manier ook voor dat de overheid de impact van de nieuwe software op de online overheidsdiensten kan controleren. De erkende dienstverleners kunnen deze impact zelf immers onvoldoende inschatten daar zij niet mogen weten voor welke overheidstoepassingen beroep wordt gedaan op hun applicatie (zie *supra* randnr. 74).[128]

78. Gedurende de periode van de erkenning moet de dienstverlener erop toezien dat de applicatie op ononderbroken wijze blijft werken.[129] Hoewel met deze bepaling het belang van de continuïteit van de dienstverlening wordt erkend, voorziet het Kb. niet in een regeling voor de periode volgend op de periode van erkenning. Het kan immers gebeuren dat de erkenning van de dienstverlener wordt ingetrokken (zoals gebeurde bij myID, echter voor de feitelijke uitrol van de applicatie ter gebruik bij het zich online identificeren bij overheidsdiensten) of dat de dienstverlener zelf beslist te stoppen.

In deze gevallen kunnen gebruikers op zeer korte termijn voor voldongen feiten komen te staan waardoor zij mogelijks haastig en niet weloverwogen dienen te veranderen van aanmeldingsdienst. Deze situatie kan enerzijds negatieve gevolgen hebben wat betreft het delen van persoonsgegevens aan andere dienstverleners waarover burgers misschien onvoldoende geïnformeerd zijn maar ook anderzijds vermindert zij het gebruiksgemak dat toch vaak aangehaald wordt als één van de belangrijkste redenen voor de digitale evolutie. De problematiek betreffende deze situaties werd ook opgemerkt door de CBPL.[130] Om uiteindelijk toch -deels- tegemoet te komen aan deze commentaar, verlegt het Kb. de verantwoordelijkheid om te voorzien in de nodige uitdovingsscenario's naar de dienstverleners door hen te verplichten te voldoen aan de voorwaarden in punt 2.4 van de bijlage van uitvoeringsverordening nr. 2015/1502 dat een doeltreffend beëindigingsplan bij stopzetting en

[126] Art. 20 Kb. Elektronische identificatie.
[127] *Ibid*. Art 21 en art. 22.
[128] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (CBPL), advies betreffende ontwerp van koninklijk besluit tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van diensten voor elektronische identificatie voor digitale overheidstoepassingen (CO-A-2017-008), 12 april 2017, nr. 18/2017, 10.
[129] Art. 23 Kb. elektronische identificatie.
[130] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (CBPL), advies betreffende ontwerp van koninklijk besluit tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van diensten voor elektronische identificatie voor digitale overheidstoepassingen (CO-A-2017-008), 12 april 2017, nr. 18/2017, 10-11

overname vereist.[131] Wat er dient te gebeuren in de situatie van het tijdelijk intrekken van een erkenning blijft echter onbeschreven.

79. Ten slotte garandeert het Kb. dat de FOD BOSA controle op de dienstverleners kan blijven uitoefenen. Zo dient de dienstverlener alle informatie betreffende klachtenbehandeling, veiligheidsonderzoeken en incidenten ten allen tijde ter beschikking te stellen aan de FOD BOSA,[132] moet zij de FOD BOSA bij het minste vermoeden van veiligheidsrisico hiervan op de hoogte stellen[133] en moet er een contactpersoon worden aangeduid die vanaf het moment van de erkenning elke zes maanden aan de FOD BOSA over de voorwaarden inzake het dienstverleningsbeheer dient te komen rapporteren.[134]

e) Economische, juridische en organisationele voorwaarden

80. In artikel 27 en 28 voorziet het KB. ten slotte in enkele economische, juridische en organisationele voorwaarden waaraan de dienstverlener dient te voldoen om zijn erkenning te verkrijgen of te behouden. Zo mogen dienstverleners: zich niet in staat van faillissement of vereffening bevinden; mogen zij niet veroordeeld zijn omwille van schendingen van de wetgeving ter bescherming van de persoonlijke levenssfeer en/of wanbedrijven of misdrijven die de professionele integriteit van het bedrijf aantasten; geen zware fouten begaan vastgesteld door de erkennende overheid; moeten zij steeds voldaan hebben aan hun belasting en sociale zekerheidsplichten; zich niet schuldig maken aan valse verklaringen of inlichtingen die zij verplicht zijn te verstrekken en mogen zij niet veroordeeld zijn door de CBPL (nu gegevensbeschermingsautoriteit of GBA) in het kader van diens toezichthoudende bevoegdheden.

Ook hier valt, door gebruik te maken van zeer ruim in te vullen intrekkingsgronden, de ruime bevoegdheid van de FOD BOSA als controleur van de erkende identificatiediensten op.

D. Erkenningsprocedure

81. Elke dienstverlener die erkend wenst te worden als aanbieder van een authenticatiemiddel voor overheidstoepassingen dient daartoe een modelformulier ter erkenningsaanvraag en een referentiedossier in op een elektronische drager bij de FOD BOSA. In dit dossier geeft de dienstverlener aan op welke manier hij zal voldoen aan de hierboven uitvoerig beschreven erkenningsvoorwaarden.[135]

82. Eens de aanvraag volledig is ingediend, beslist de FOD BOSA uiterlijk binnen de drie tot zes maanden over de erkenning. In deze periode consulteert zij bij vertegenwoordigers van het College van voorzitters van de federale en programmatorische overheidsdiensten, bij het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en bij het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut of aan alle voorwaarden is voldaan.[136] Afgekeurde aanvragen kunnen na correctie van de redenen voor weigering opnieuw

[131] Art. 28.1 Kb. elektronische identificatie *io.* Verslag over het ontwerp van het Koninklijk besluit tot vaststelling van de
voorwaarden, de procedure en de gevolgen van de erkenning van diensten voor elektronische identificatie voor overheidstoepassingen, *Parl.St* Fed.R. 2017-2018, nr. 2017/31391, 2.2 in fine.
[132] Art. 24 Kb. elektronische identificatie.
[133] *Ibid*. Art. 25.
[134] *Ibid*. Art. 26.
[135] *Ibid*. art. 29 en art. 30.
[136] *Ibid*. art. 31.§1

worden ingediend en aanvragers kunnen op eigen verzoek of op verzoek van de FOD BOSA worden gehoord over het dossier.[137]

Eens de erkenning wordt toegekend, wordt het authenticatiesysteem opgenomen binnen de FAS. Digitale overheidsdiensten die gebruik maken van de FAS zullen vanaf dan geen keuze meer hebben en moeten de authenticatiedienst aanvaarden in zoverre deze voldoet aan het vereiste beveiligingsniveau voor de betreffende dienst.[138] Het zal belangrijk zijn voor de betreffende overheidsdiensten om hun eventuele bezwaren tegen een nieuwe authenticatietoepassing zeer kenbaar te maken tijdens de hierboven beschreven consultatieronde. Bovendien is het nog maar de vraag of deze regeling te verzoenen is met artikel 28 van de AVG. (zie *infra* randnr. 164).[139]

E. Gevolgen van erkenning

83. Eens erkend, wordt de nieuwe aanmeldingsoptie samen met het beveiligingsniveau weergegeven op het toegangsportaal van de erkennende overheid.[140] Wanneer de gebruiker voor desbetreffende aanmeldingsdienst kiest, wordt hij door de federale authenticatiedienst doorverwezen naar de erkende dienst die dan het identificatienummer van de burger gebruikt en de verificatie terugstuurt via het toegangsportaal.[141] Daarnaast wordt er ook een samenwerkingsovereenkomst gesloten tussen de erkennende overheid en de dienstverlener en wordt er een gezamenlijk plan voor de opstart en de communicatie van de nieuwe dienst opgesteld.[142] De erkenning is geldig voor een periode van drie jaar waarna een nieuwe aanvraag moet worden ingediend.[143]

84. Elk jaar na de erkenning moet de dienstverlener binnen de 15 dagen bevestigen dat zijn authenticatiemechanisme nog steeds voldoet aan de voorwaarden verbonden aan het betrouwbaarheidsniveau substantieel of hoog. De dienstverlener is evenwel verplicht tot extra bevestiging binnen de 15 dagen wanneer de erkennende overheid hierom verzoekt; na kennisname van de wijziging van de erkenningsvoorwaarden; na wijziging van de vereiste elementen om te voldoen aan dit betrouwbaarheidsniveau zoals weergegeven in punt 2.1 en punt 2.3.1 van de bijlage van de uitvoeringsverordening (EU) nr. 2015/1502 of na wijziging van de wetgeving betreffende de bescherming van persoonsgegevens én indien er een wijziging van de dienstverlening of controle over de dienstverlener die impact heeft op de dienstverlener zelf zou plaatsvinden voordat deze wijzigingen effectief plaatsvinden.[144]

Daarnaast moet elke wijziging in gegevens die verstrekt werd op het ogenblik van de erkenningsaanvraag en die een impact kan hebben op de dienstverlening binnen de maand gemeld, beschreven en gemotiveerd worden aan de FOD BOSA. Indien de erkenningsvoorwaarden na deze wijziging niet langer gerespecteerd worden kan de FOD BOSA de erkenning schorsen of intrekken.[145]

---

[137] *Ibid*. Art. 31 §3 en art. 32.
[138] Art. 10 wet elektronische identificatie.
[139] Art. 16§4 WVP en Art. 28(2) AVG; COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (CBPL), advies betreffende ontwerp van koninklijk besluit tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van diensten voor elektronische identificatie voor digitale overheidstoepassingen (CO-A-2017-008), 12 april 2017, nr. 18/2017, 3.
[140] Art 34 Kb. elektronische identificatie.
[141] *Ibid*. art. 33 en art. 35.
[142] *Ibid*. art. 36 en art. 37.
[143] *Ibid*. art. 43.
[144] *Ibid*. art. 39.
[145] *Ibid*. art. 40.

F. Controle- en sanctieregelingen

85. Ter controle van de in het Kb. vermelde erkenningsvoorwaarden, technische specificaties of de samenwerkingsovereenkomst, kan de FOD BOSA gedetailleerde verklaringen tot zelfs een audit opleggen aan de dienstverlener.[146] Daarnaast kan de erkennende overheid de erkenning schorsen voor een maximumtermijn van twaalf maanden bij niet overeenstemming van de erkenningsvoorwaarden, technische specificaties of de samenwerkingsovereenkomst wanneer zij van oordeel is dat de problemen door deze maatregel binnen de redelijke termijn kunnen worden verholpen (cfr. myID) en kan zij om dezelfde redenen of wanneer niet de nodige maatregelen werden getroffen om de schorsing teniet te doen, de erkenning intrekken.[147]

De beslissing tot schorsing of intrekking wordt per aangetekende zending opgestuurd waarna de dienstverlener steeds zal worden gehoord. Eens definitief zal de identificatiedienst verwijderd worden van het toegangsportaal. Indien de overheid van mening is dat er geen redenen tot schorsing meer zijn, kan deze vervroegd worden opgeheven.[148]

86. Eerder werd ook al aangegeven dat de gegevensbeschermingsautoriteit bevoegd is en blijft voor de controle op inbreuken tegen de bescherming op de verwerking van persoonsgegevens.

G. FAS gebruikersovereenkomst

87. Anders dan wat geldt voor de aanbieders van authenticatiediensten, worden de gedragingen van overheden en private partijen die gebruik willen maken van de FAS (hierna voor dit onderdeel "de gebruiker") louter gereguleerd op contractuele basis via de FAS gebruikersovereenkomst. Daarin wordt onder meer bepaald dat de beveiliging van de (digitale en fysieke) omgeving van de gebruiker volledig onder de verantwoordelijkheid van de gebruiker zelf valt, de verplichting voor gebruikers tot het bewaren van authenticaties en pogingen daartoe met bijhorende gegevens zoals datum, tijdstip, identificatienummer en IP-adres gedurende 10 jaar en worden de afspraken omtrent de verantwoordelijkheid van verwerking vastgesteld. (Zie hierover *infra* randnr. 156 ev.). Verder geldt wat betreft de bescherming van persoonsgegevens voor zowel de FOD BOSA als de gebruiker de verplichting tot het bijhouden van een verwerkingsregister dat zij op redelijk verzoek moeten kunnen voorleggen, geldt er een onderlinge informatieverplichting en moeten zij een jaarlijks te actualiseren veiligheidsbeleidplan opstellen en een functionaris voor gegevensbescherming aanwijzen.[149]

88. Net zoals bij het verbod op het gebruik van identificatienummers voor commerciële doeleinden (zie *supra* randnr. 75) zit een belangrijk onderdeel van de bescherming van persoonsgegevens aldus vervat in een contractuele bepaling. Daardoor volgt uit het beginsel van de relativiteit van contracten dat de verplichtingen in het contract in principe niet kunnen worden gevorderd door een derde (burger) wiens gegevens worden beschermd door deze verplichtingen.[150] Toch kan een overeenkomst wel degelijk gevolgen hebben voor derden en zouden burgers zich in sommige gevallen dus ook in hun voordeel kunnen beroepen op het bestaan van de overeenkomst

[146] *Ibid*., art. 44.
[147] *Ibid*., art. 45.
[148] *Ibid*., art. 46.
[149] FOD BOSA, *FAS gebruikersovereenkomst versie 6.7*, 7 februari 2023, https://bosa.belgium.be/sites/default/files/content/documents/DTdocs/FAS/FAS%20Gebruikersovereenkomst.pdf, 4-7.
[150] Art. 5.103 lid 1 Nieuw BW; Cass. 27 mei 1909, *Pas.* I 1909, 272; Cass. 28 maart 2019, nr. C.18.0272.F.

en de gevolgen die zij teweeg brengt.[151] Dit principe van tegenstelbaarheid laat immers toe dat een derde een medecontractant aansprakelijk kan stellen voor contractuele wanprestaties die tegelijk en los van het contract een schending oplevert van de zorgvuldigheidsverplichting uit artikel 1382 oud BW.[152] De contractuele verplichtingen verhogen daarbij de algemene zorgvuldigheidsplicht omdat de contractanten rekening moeten houden met de belangen van derden die op voorzienbare wijze verbonden zijn met de uitvoering van de overeenkomst.[153]

89. Hoewel de contractuele verplichtingen (die eigenlijk een verdieping zijn van de beginselen zoals vervat in de AVG) dus wel degelijk een bepaalde grondslag bieden waarop burgers zich zouden kunnen beroepen, had de wetgever er mijn inziens beter aan gedaan om deze verplichtingen wettelijk te verankeren. De tegenstelbaarheid van verbintenissen en daarmee gepaard gaande verhoogde zorgvuldigheidsplicht vereist immers steeds dat er eerst schade moet worden geleden vooraleer de burger zijn subjectieve rechten kan laten gelden. Een wettelijke verankering van de verplichtingen zou daarentegen de burger reeds in staat stellen op te treden tegen de nalatige gebruiker van de FAS voor er sprake is van schade. Bovendien heeft niet elke burger weet van de gebruikersovereenkomst, noch kan dat van hem verwacht worden. Het zou de transparantie van de werking van overheden aldus ten goede komen. De burger kan zich uiteraard wel beroepen op de AVG en de algemene uitvoeringswetten, doch zij bevatten eerder algemene verplichtingen en dus geen uitgediepte verplichtingen specifiek voor de gevaren die voortvloeien uit de authenticatieketen. Beroep op deze bepalingen zal aldus leiden tot meer discussies voor de rechter en dus minder rechtszekerheid dan het geval zou zijn bij duidelijke wetgeving.

H. Vergelijking met Nederland

a) Algemeen

90. Ook in Nederland werd er recent[154] een wetsvoorstel aangenomen dat voorziet in een kaderwet dat de basis legt voor een verdere digitalisering van het bestuur zoals was vastgelegd in het regeerakkoord van het kabinet Rutte III.[155] Anders dan in België waar de wet elektronische identificatie en het koninklijk uitvoeringsbesluit eerder gericht zijn op aanbieders van authenticatiemechanismen, richt het Nederlandse wetsvoorstel zich voornamelijk tot de Nederlandse overheid zelf.

De Nederlandse overheid koos er bij het opmaken van het voorstel voor om te focussen op de meest urgente onderwerpen betreffende de digitale overheid: De bevoegdheid tot het verplichten van bepaalde standaarden bij het elektronisch verkeer van de overheid; het opstellen van regels betreffende informatieveiligheid; de verantwoordelijkheid voor het beheer van diensten en voorzieningen binnen de digitale overheidsinfrastructuur en ten slotte de online toegang voor burgers

[151] Ibid., lid 2; S. DECLERCQ en E. GOOSSENS, "Derdenwerking van contracten: actuele ontwikkelingen" in S. STIJNS en A. DE BOECK, *Themis 2021-2022 nr. 120: Verbintenissenrecht*, Antwerpen, Intersentia, (43) 44.
[152] Cass. 20 juni 1997, *Arr.Cass* 1997, 673; I. CLAEYS, *Verbintenissenrecht*, Gent, Faculteit Recht en Criminologie, 2019, 14.
[153] Luik 30 september 2005, *JLMB* 2006, 817; I. CLAEYS, *Verbintenissenrecht*, Gent, Faculteit Recht en Criminologie, 2019, 14.
[154] 23 maart 2023.
[155] VVD, CDA, D66 en ChristenUnie, *Regeerakkoord 2017-2021: Vertrouwen in de toekomst*, 10 oktober 2017, https://www.eerstekamer.nl/overig/20171010/vertrouwen_in_de_toekomst/f=/vkicly3bt7yh.pdf, 7.

en bedrijven tot de digitale publieke dienstverlening.[156] Het wetsvoorstel beoogt de regeldruk en administratieve lasten van de Nederlandse burgers te verminderen door de toegang tot digitale dienstverlening door de overheid te uniformeren. Daarnaast maakt het aangenomen voorstel het mogelijk dat burgers met verschillende (publieke en private)[157] middelen kunnen inloggen waardoor er -net zoals in België- keuzevrijheid ontstaat en de beschikbaarheid van werkende authenticatiemiddelen beter wordt gewaarborgd.[158] Momenteel kunnen burgers in Nederland gebruik maken van het door de rijksoverheid aangeboden digiD. Voor bedrijven werd er gekozen voor een publiek-private samenwerking in de vorm van eHerkenning.[159]

b) Betrouwbaarheidsniveaus

91. Net als België (impliciet) erkent Nederland dat authenticatiemechanismen met betrouwbaarheidsniveau "laag" onvoldoende zekerheid bieden om zeker te zijn dat de persoon die wil inloggen effectief de persoon is die hij beweert te zijn. Anders dan België kiest Nederland ervoor om overheden te verplichten gebruik te maken van door de overheid erkende authenticatiesystemen met betrouwbaarheidsniveau "substantieel" dan wel "hoog" afhankelijk van de aard van de online dienst die zij verlenen.[160] Eens een authenticatiemiddel door de bevoegde minister wordt goedgekeurd zijn de overheden verplicht dit middel aan te bieden als optie voor het inloggen.[161] Opvallend genoeg laat Nederland in het wetsvoorstel de ruimte om bij ministeriële regeling af te wijken van deze verplichting in die zin dat het gebruik van "generieke authenticatiemiddelen" onvoldoende kan blijken om in te loggen bij bepaalde overheidsdiensten. De memorie van Toelichting geeft daarbij als voorbeeld dat een advocaat naast zijn identiteit ook een advocatenpas nodig heeft om in te loggen bij elektronische diensten van de Nederlandse Orde van Advocaten.[162] Zo laat de Nederlandse wetgever een opening die het mogelijk maakt om snel te kunnen schakelen naar een systeem dat de facto neerkomt op het gebruik van een digitale portefeuille (zie *supra* randnr. 53 en *infra* randnr. 123). De betrokken overheidsorganisaties moeten daarnaast zelf een audit organiseren die zal bepalen welk betrouwbaarheidsniveau van authenticatie vereist is voor de door hun aangeboden diensten.[163]

c) Reikwijdte

92. De in het vorige randnummer besproken acceptatieplicht voor overheden geldt voor alle zogenaamde "a-besturen" die online diensten aanbieden aan de burger. Concreet gaat het om alle organen van een rechtspersoon die krachtens het publiekrecht werden ingesteld en die niet door de algemene wet bestuursrecht worden uitgesloten.[164] Concreter gaat het om de organen van de staat, provincies en gemeenten en andere rechtspersonen die krachtens het publiekrecht zijn ingesteld

[156] MvT bij wetsvoorstel betreffende Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid), *Parl.St.* tweede kamer 2017-2018, nr. 34972, 3, 1-4.
[157] Ibid., 13.
[158] Ibid., 45.
[159] Ibid., 10.
[160] Art. 6 en art. 7 gewijzigd voorstel van wet betreffende Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid), *Parl.St.* Eerste kamer 2019-2020, nr. 34972, A, 19.
[161] MvT bij wetsvoorstel digitale overheid, 13.
[162] Ibid., 15.
[163] Ibid., 19.
[164] Art. 1:1 lid 1. a) *io.* lid 2 a)-i) Wet van 4 juni 1992, houdende algemene regels van bestuursrecht (Algemene wet bestuursrecht), *StB.* 1992, 315.

zoals bijvoorbeeld de Sociale Verzekeringsbank. Ook andere organen kunnen onder de verplichting vallen als zij worden opgenomen in de bijlage bij het wetsvoorstel of daar bij besluit worden toe aangewezen.[165] Opnieuw zal bij deze beslissing worden gekeken naar de aard van de diensten die worden aangeboden en of er al dan niet gebruik moet worden gemaakt van het BSN nummer.[166]

d) Privacy en gegevensbescherming

93. Waar België er wat betreft privacy en gegevensbescherming voor koos om zich tevreden te stellen met een simpele verwijzing naar de algemeen geldende wetten en verordening die handelen over de bescherming van persoonsgegevens (zie *supra* randnr. 73), gaat Nederland een (klein) stapje verder. Zo voorziet artikel 16 van het voorstel in een wettelijke grondslag die het toelaat aan alle betrokken partijen (denk aan de (aangewezen) overheidsdiensten, de erkende aanbieders van authenticatiemiddelen en andere specifiek betrokken partijen) om elk binnen zijn/haar rol waar noodzakelijk gegevens van burgers te gaan verwerken.[167] Daarnaast wordt er op gewezen dat wat betreft de vereisten van subsidiariteit, doelbinding, proportionaliteit, kenbaarheid, voorzienbaarheid en transparantie de regels verder zullen worden uitgewerkt en aangepast in het besluit verwerking persoonsgegevens dat de specifieke regels betreffende de verwerking van persoonsgegevens "in de generieke digitale infrastructuur" vaststelt.[168]

Hoewel deze aanpassingen nog dienen te gebeuren, geeft de parlementaire voorbereiding wel al een stevige aanzet door te bepalen dat bij de verdere uitwerking van de wet, het zogenaamde "privacy by design" moet worden gerealiseerd. Dit laatste houdt volgens de parlementaire voorbereiding in dat 1) het besluit het principe van minimale gegevensverwerking moet implementeren; 2) dat moet worden vermeden dat er data-hotspots ontstaan door het "onmogelijk te maken om identificatie en vertrouwelijke informatie bij één adressaat te beleggen"; 3) dat gegevens daar waar mogelijk moeten worden gepseudonimiseerd zodat zij niet rechtstreeks kunnen terugleiden naar een persoon of dat er minstens procedurele en systeemtechnische afspraken worden afgedwongen om de bescherming van de persoonsgegevens verder te garanderen met privacy enhancing technologies en ten slotte 4) dat er in maatregelen moet worden voorzien die de impact van beveiligingsincidenten en misbruik zo klein mogelijk maken.[169] Door de verantwoordelijkheid van deze privacy by design bij de regering te leggen, lijkt in Nederland de verwerkingsverantwoordelijkheid minstens deels bij de overheid zelf te worden gelegd.

Een belangrijke maatregel die door de Nederlandse wet wordt aangenomen ter uitvoering van deze privacy by design is het feit dat de erkende authenticatiedienst het BSN-nummer, dat vergelijkbaar is met het Belgisch rijksregisternummer, en de afbeelding van de persoon om wie het gaat weliswaar

[165] MvT bij wet digitale overheid, 16 *io.* bijlage bij artikel 2 gewijzigd voorstel van wet betreffende Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid), *Parl.St.* Eerste kamer 2019-2020, nr. 34972, A, 19.
[166] MvT bij wet digitale overheid, 18.
[167] Art. 16 lid 1-3 gewijzigd voorstel wet digitale overheid; MvT bij wet digitale overheid, 85-86.
[168] Besluit van 17 mei 2016, houdende regels betreffende de verwerking van persoonsgegevens in de voorzieningen voor de generieke digitale infrastructuur DigiD, DigiD Machtigen, MijnOverheid en BSN-Koppelregister (Besluit verwerking persoonsgegevens generieke digitale infrastructuur), *StB* 2016, 195; Art 16 lid 4 gewijzigd voorstel wet digitale overheid.
[169] MvT bij wet digitale overheid, 22.

mag gebruiken ter controle van de identiteitsgegevens van de gebruiker maar ze daarna niet mag bewaren.[170]

94. Ten slotte voorziet de parlementaire voorbereiding nog in een opsomming van de relevante beginselen en verplichtingen uit de AVG en draagt zij de verdere uitwerking ervan over aan de bevoegde minister van Binnenlandse zaken. De verdere uitwerking dient opnieuw nog te gebeuren en kan aldus niet besproken worden in deze scriptie. Wat verder wel opvalt is dat, hoewel het wetsvoorstel er net als België niet in voorzag, er via een novelle alsnog een bepaling werd toegevoegd die het onmogelijk maakt om een erkenning aan private aanbieders van authenticatiemiddelen te verlenen wanneer zij de gegevens die zij daarbij horen te verwerken gebruiken voor commerciële doeleinden.[171]

e) Identiteitsfraude

95. Waar België in de parlementaire voorbereiding amper oog heeft voor misbruik en identiteitsfraude, wijdt Nederland wel enkele pagina's aan het thema. Zo wordt er een onderscheid gemaakt tussen maatregelen die misbruik en fraude moeten opsporen en voorkomen of minstens minimaliseren en maatregelen die, wanneer er toch een dreiging plaatsvindt, de situatie moeten herstellen of de schade moeten beperken.[172]

Net als in België wordt er voor wat betreft de eerste categorie ook gekeken naar de burgers zelf. Zo wordt ook in Nederland aan alle gebruikers expliciet de verplichting opgelegd om alle nodige maatregelen te treffen om misbruik, diefstal, verlies of verspreiding van de identificatiemiddelen te voorkomen.[173]

Wat andere maatregelen voor de overheden en (private) aanbieders van authenticatiemiddelen betreft, werd er opnieuw gekozen voor een delegatie aan de bevoegde minister en dus verdere uitwerking in een uitvoeringsbesluit. Toch koos de Nederlandse wetgever er opnieuw voor om reeds één en ander uit te werken in de parlementaire voorbereiding. Zo suggereert zij dat bij herkenningsmaatregelen moet worden gedacht aan onder andere actieve monitoring, detectie, analyse en proactieve kennisopbouw.[174] Allen maatregelen die we ook terugvinden in het Belgische uitvoeringskb. Voor wat betreft de herstelmaatregelen wordt er gesproken over het (voorlopig) blokkeren van gebruikers, het intrekken of onderbreken van de erkenning van identificatiemiddelen en zelfs het afsluiten van de toegang van overheden die gebruik maken van de erkende authenticatiediensten in geval van beveiligingsgebreken.[175]

Ten slotte wijst de Nederlandse wetgever er nog op dat misbruik zich kan manifesteren over verschillende componenten van authenticatieketen heen en dat een innige samenwerking tussen de verschillende actoren die een rol spelen in het authenticatieproces dan ook onontbeerlijk is om misbruik effectief te kunnen aanpakken.[176] Om deze samenwerking mogelijk te maken wordt in het wetsvoorstel aan de bevoegde minister de mogelijkheid gelaten om bij overheden en aanbieders van

[170] Art. 16 lid 2 gewijzigd voorstel wet digitale overheid; MvT bij wet digitale overheid, 85.
[171] Amendement bij wetsvoorstel digitale overheid, *Parl.St.* 7 juni 2022, https://www.eerstekamer.nl/9370000/1/j9vvkfvj6b325az/vltnc0d2jclp/f=y.pdf, 1.
[172] Ibid., 28-29.
[173] Art. 10 lid 1 gewijzigd voorstel wet digitale overheid.
[174] MvT bij wet digitale overheid, 29.
[175] Ibid., 30.
[176] Ibid., 31.

authenticatiemiddelen informatie op te vragen die het mogelijk moet maken om effectieve maatregelen te treffen om misbruik tegen te gaan.[177]

96. Ook hier zien we dus heel wat verschillen met België dat in zijn wettelijk kader enkel voorziet in maatregelen die weerslag hebben op de aanbieders van de authenticatiediensten. Bovendien lijkt België de rol van overheden die gebruik maken van authenticatiemechanismen en de rol die zij kunnen spelen wat betreft het tegengaan van misbruik en identiteitsfraude te miskennen door hierover geen waarborgen op te nemen in het wettelijk kader.

f) Toezicht en handhaving

97. Ook voor het toezicht kiest de Nederlandse wetgever voor een opdeling tussen verschillende actoren. Zo geldt voor de dienstverlening door bestuursorganen die verplicht worden gebruik te maken van de authenticatietools het principe dat zij zelf moeten toezien op een goede naleving van de toepasselijke normen zoals de acceptatieplicht, betrouwbaarheids- en beveiligingsvereisten betreffende de toegang tot de online dienstverlening. Voor bestuursorganen en wettelijk aangewezen organisaties geldt daarnaast het gewoonlijke bestuurlijk toezicht en de verplichting voor provincies tot het informeren van de minister over de mate van naleving van de verplichtingen door gemeentelijke overheden. Voor nationale overheidsorganen en aangewezen organisaties kunnen daarnaast toezichthouders worden aangewezen.[178] Voor nationale uitvoeringsorganisaties (zoals de belastingdienst) betekent dit bijvoorbeeld dat het de minister die verantwoordelijk is voor deze organisatie zal zijn die de controle dient uit te oefenen. Bovendien moeten de besturen aan de minister de verklaring van een auditor kunnen voorleggen dat verklaart dat de overheid aan de verplichtingen voldoet.[179] Deze audit moet jaarlijks worden herhaald.[180] Niet naleving van de verplichtingen kan (zoals hierboven reeds aangegeven) aanleiding geven tot repressieve sancties.

98. Wat betreft de controle op het authenticatiemechanisme zelf zullen de contractuele en wettelijke vereisten betreffende betrouwbaarheid en veiligheid worden gecontroleerd door de minister van Binnenlandse Zaken aan de hand van jaarlijkse externe auditrapporten. Daarnaast zal ook steeds contractueel worden afgedwongen dat de bevoegde minister en zijn ambtenaren ten allen tijde ook zelf een audit mogen uitvoeren. Ook hier kan, indien de nodige vereisten niet worden nageleefd, overgegaan worden op repressieve sancties zoals de intrekking van de toelating of het beëindigen van de toelating tot aansluiting van het authenticatiemechanisme op de publieke infrastructuur.[181] Daarnaast wordt ook hier door de minister een toezichthouder aangewezen (de Memorie wijst zelf naar het Agentschap Telecom) die aan de hand van rapportages en verklaringen toezicht houdt op het naleven van de voorwaarden door de erkende authenticatiedienstverlener. Ook eigen onderzoek door de toezichthouder blijft mogelijk indien nodig.[182]

[177] Art. 19 lid 1 gewijzigd voorstel wet digitale overheid.
[178] Art. 17 gewijzigd voorstel wet digitale overheid; MvT bij wet digitale overheid, 32.
[179] Art. 4 lid 2 gewijzigd voorstel wet digitale overheid.
[180] Art. 3 lid 4 gewijzigd voorstel wet digitale overheid; MvT bij wet digitale overheid, 33.
[181] Art. 9 lid 2 gewijzigd voorstel wet digitale overheid; MvT wet digitale overheid, 34.
[182] MvT wet digitale overheid, 34.

I. Conclusie

99. In dit tweede hoofdstuk werd een antwoord gezocht op een onderdeel van de tweede onderzoeksvraag naar de regulatie door de nationale wetgeving betreffende de erkenning van nieuwe en bestaande authenticatiemechanismen.

100. Met de wet elektronische identificatie maakte de wetgever het mogelijk om authenticatiemechanismen ontwikkeld door private dienstverleners te erkennen. De aanbieders worden daarbij gezien als onderaannemers van de FOD BOSA en krijgen daarmee ook toestemming tot het gebruik van de rijksregisternummers van de Belgische burgers.

101. In de wet werd het grootste gedeelte van de verdere uitwerking gedelegeerd aan de uitvoerende macht die in het Kb. elektronische identificatie de concrete erkenningsvoorwaarden voor een authenticatiemechanisme vastlegde. Dit Kb. bepaalt dat een authenticatiemechanisme om erkend te worden moet voldoen aan het betrouwbaarheidsniveau substantieel of hoog zoals vastgesteld volgens de technische vereisten uitgewerkt in de bijlage van de uitvoeringsverordening van de Europese eIDAS Verordening.

102. In het laatste gedeelte van dit hoofdstuk werd ook het net aangenomen wettelijk kader in Nederland besproken. Deze vergelijking leidde tot enkele opvallende gelijkenissen en verschilpunten tussen de twee landen.

103. Een eerste groot verschilpunt betreft het feit dat waar Nederland kiest voor een kaderwet en uitvoeringsbesluit dat zowel gedragingen van de aanbieders van authenticatiemechanismen als de overheden die gebruik (moeten) maken van deze mechanismen reguleert, de wettelijke focus in België volledig op die eerste ligt. Een mogelijke verklaring van dit verschil zou in de complexe federale structuur van ons land kunnen liggen waar de regeling van gedragingen van lokale besturen door de federale uitvoerende macht grondwettelijk niet toegelaten is.[183] In België wordt dan ook gebruik gemaakt van een contractuele overeenkomst tussen de FAS en de overheden die van diens diensten gebruik wil maken, wat leidt tot een verminderd beschermingsniveau en niveau van rechtszekerheid voor de burger.

De opvallendste Nederlandse regulering betreffende de online overheden betreft het feit dat zij zullen worden verplicht gebruik te maken van de erkende authenticatiemechanismen. In België en Vlaanderen geldt deze verplichting enkel voor die overheden die ervoor kiezen om gebruik te maken van de diensten van de FAS.

104. Wat de cyberveiligheid betreft, kiezen beide systemen voor een regeling van zowel preventie, als opvolging en rapportering waarbij er door de aanbieders van authenticatiemechanismen systemen moeten worden geïnstalleerd die misbruik kunnen voorkomen. Wanneer er toch een dreiging wordt opgemerkt moet dit worden gerapporteerd aan een toezichthoudende instantie. In België is dit de erkennende overheid FOD BOSA. Daarnaast moet er in België elke zes maanden de mogelijkheid worden bekeken tot het implementeren van nieuwe software waarbij de FOD BOSA opnieuw een controlerende bevoegdheid heeft gekregen die het mogelijk maakt de impact voor

[183] Art. 39 GW *io.* art. 6, §1, VIII BWHI.

online overheidsdiensten in te schatten. Deze mogelijkheid hebben de authenticatiemechanismen zelf immers niet.

Het grootste verschilpunt hier ligt hem opnieuw in het feit dat de regulering in Nederland ook voorziet in de mogelijkheid tot ingrijpen indien er zich veiligheidsproblemen voordoen op het niveau van de besturen die online diensten aanbieden. In België bestaat deze mogelijkheid vooralsnog niet.

105. Ook op vlak van de bescherming van persoonsgegevens vallen opvallende verschillen tussen de twee wetgevingen waar te nemen: Waar Nederland reeds in de voorbereidende documenten wijst op het belang van een goede gegevensbescherming en een opsomming geeft van de beginselen waarmee de bevoegde minister rekening mee zal moeten houden bij het uitwerken van het uitvoeringsbesluit, blinkt België vooral uit in het gebrek aan een dergelijke regulering. Weliswaar geldt er voor de authenticatiediensten (net als in Nederland waar het overigens wel gewoon om een algemeen geldend wettelijk verbod gaat.)[184] een verbod op het gebruik van de persoonsgegevens voor commerciële doeleinden. In de praktijk kunnen aanbieders van authenticatiemechanismen dit enkel contractueel met hun partners afdwingen waardoor de rechtsbescherming van de burger in het gedrang dreigt te komen.

Verder geldt in beide landen het principe dat aanbieders van authenticatiemechanismen niet behoren te weten van welke overheidsdiensten de burger wenst gebruik te maken en geldt er in België een maximumbewaartermijn van tien jaar vanaf de aanmeldingspoging. Uit de privacyverklaring die werd besproken in hoofdstuk I blijkt echter dat de aanbieders van Itsme deze termijn niet al te strikt opnemen.

Een verklaring voor de gebrekkige Belgische implementatie van de beginselen van de AVG in vergelijking met Nederland is uiteraard het feit dat de Europese wetgeving ten tijde van het opstellen van de wet en het besluit nog zeer nieuw was.

106. Wat ten slotte het toezicht op de naleving van de erkenningsvoorwaarden betreft valt op dat in België zeer veel verantwoordelijkheid bij de FOD BOSA wordt gelegd. In Nederland daarentegen wordt een veel gedifferentieerder systeem van bestuurlijk toezicht en de mogelijkheid tot toezicht door onafhankelijke organisaties geïmplementeerd. Daarnaast komt er ook veel verantwoordelijkheid bij de bevoegde minister van Binnenlandse Zaken te liggen die er als rechtstreeks verantwoordelijke in vergelijking met een overheidsdienst een groot politiek belang bij heeft dat er geen grootschalige lekken ontstaan. Bovendien is het nog maar de vraag of een overheidsdienst zoals de FOD BOSA in staat zal zijn om -eventueel onder politieke druk- op een objectieve manier te oordelen over een door de overheid opgericht authenticatiesysteem. Deze bedenking geldt uiteraard parallel voor de situatie in Nederland.

[184] Art. 8 lid 1 gewijzigd voorstel digitale overheid.

Hoofdstuk III. Europees identiteitsmanagement: De eIDAS Verordening

A. Algemeen

107. De eIDAS Verordening omvat, als opvolger van de richtlijn harmonisatie van de interne markt voor elektronische handtekeningen en identificatiediensten, twee aparte materies: Enerzijds de onderlinge erkenning door lidstaten van elektronische identificatiemiddelen en anderzijds een lijst met vertrouwensdiensten.[185]

Wat het eerste luik betreft, faciliteren de bepalingen van de verordening het gebruik van identificatiemiddelen doch enkel voor toepassingen in de publieke sector en in grensoverschrijdende situaties. Wat het tweede luik betreft worden vertrouwensdiensten gedefinieerd als elektronische diensten die gewoonlijk tegen betaling worden aangeboden en die (limitatief) 1) het aanmaken, verifiëren en valideren van elektronische handtekeningen 2) het aanmaken, verifiëren en valideren van certificaten voor authenticatie van websites of 3) het bewaren van elektronische handtekeningen, zegels of certificaten die betrekking hebben op deze diensten, inhoudt.[186]

108. De eIDAS verordening is -zoals alle verordeningen- rechtstreeks toepasselijk in de interne rechtsorde waardoor tegenstrijdige nationale bepalingen niet langer toepasselijk zijn. Toch behouden lidstaten het recht om aanvullende maatregelen te nemen, zolang deze niet in strijd zijn met de verordening.[187] Daar waar het eerste luik enkel van toepassing is op de publieke sector, is luik twee wel van toepassing op de marktdiensten. Dit neemt echter niet weg dat bepalingen betreffende het eerste luik ter inspiratie kunnen dienen voor een nationale regeling voor elektronische identificatie voor wat betreft e-banking of dat, wat het tweede luik betreft er op nationaal niveau en dus voor nationale toepassingen bijkomende vertrouwensdiensten worden gecreëerd.[188] Omdat in dit werk de nationale regelgeving geëvalueerd wordt in het licht van de Europese regelgeving, zal er in dit hoofdstuk enkel ingegaan worden op de artikelen die van invloed kunnen zijn op de Belgische strategie en regeling.

Met de invoering van de twee luiken van de eIDAS, werd het eerste grensoverschrijdende kader voor digitale identiteiten en zogenaamde "trust services" opgezet dat het mogelijk maakt voor EU burgers om toegang te krijgen tot publieke diensten over heel Europa door gebruik te maken van elektronische identificatiemiddelen uitgegeven door hun thuisland en erkend door alle lidstaten.[189] Het spreekt voor zich dat voor het beantwoorden van de centrale onderzoeksvraag, dit hoofdstuk zich voornamelijk zal focussen op het eerste luik.

109. Specifiek stelt de eIDAS zich het vergroten van het vertrouwen in elektronische transacties binnen de interne markt tot doel. Voornamelijk wilde de Europese regelgever dit bereiken door het tegelijk wegnemen van twijfels betreffende rechtszekerheid onder burgers en het verhogen van de

[185] H. GRAUX, "De eIDAS-Verordening en de begeleidende Belgische wetgeving : nieuwe marsorders voor elektronische handtekeningen en andere vertrouwensdiensten", *CDJ* 2016, nr. 3, (53) 56.
[186] Art. 3.16 eIDAS verordening.
[187] K. LENAERTS en P. VAN NUFFEL, *Europees recht*, Mortsel, Intersentia, 2023, 640-643.
[188] H. GRAUX, "De eIDAS-Verordening en de begeleidende Belgische wetgeving : nieuwe marsorders voor elektronische handtekeningen en andere vertrouwensdiensten", *CDJ* 2016, nr. 3, (53) 56.
[189] EPRS, *Revision of the eIDAS regulation, findings on its implementation and application,* 2022, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)699491, 1.

gebruiksvriendelijkheid.[190] Dit beoogt de eIDAS door te voorzien in een gemeenschappelijke grondslag waardoor ook de doeltreffendheid van online publieke diensten binnen de EU kon verhogen.[191] Daarnaast wilde de EU met de eIDAS uiteraard ook belemmeringen betreffende het grensoverschrijdende aspect van elektronische authenticatie voor overheidsdiensten wegnemen door een veilige authenticatie te garanderen voor EU burgers, samenwerking tussen lidstaten betreffende deze veiligheid te stimuleren en de ontwikkelingen van de digitale interne markt te waarborgen.[192]

B. Elektronische identificatiemiddelen

110. De eIDAS maakt het mogelijk voor lidstaten om elektronische identificatiemiddelen aan te melden bij de Europese Commissie. De verordening is uitgesproken technologie neutraal en laat staten toe om beroep te doen op private partners[193] maar er moet wel worden voldaan aan enkele -zeer makkelijk te halen- vereisten vastgelegd in artikel 7 zoals bijvoorbeeld de voorwaarden dat de identificatiemiddelen moeten kunnen worden gebruikt om in te loggen bij ten minste één dienst geleverd door een openbare instantie[194] en dat het systeem een identificatiemiddel moet kunnen koppelen aan een natuurlijke of rechtspersoon.[195] Om landen die niet in staat waren om zelf een online identificatiemiddel op te starten mee in het digitale verhaal te krijgen, voorziet de eIDAS ook in de mogelijkheid voor staten om identificatiemiddelen ontwikkeld door privébedrijven aan te melden, doch enkel in zoverre dat de uitgifte van de dienst gebeurt in samenwerking met de aanmeldende lidstaat.[196]

111. Naast de eisen vermeld in artikel 7, zijn er relatief weinig kwaliteitsvereisten die worden opgelegd aan de identificatiemechanismen. Het staat de staten immers vrij gebruik te maken van zeer zwakke systemen (username + paswoord) of zeer sterke systemen die bijvoorbeeld gebruik maken van biometrische gegevens. Weliswaar werden, om het mogelijk te maken een lijn te trekken tussen de betrouwbaarheid van de verschillende systemen, drie categorieën van betrouwbaarheidsniveaus gaande van laag over substantieel tot hoog en lijsten met de technische specificaties die bij elk van deze niveaus hoort, opgesteld (zie bijlage 1).[197] Er bestaat geen

[190] EUROPESE COMMISSIE, *Verslag van de Commissie aan het Europees Parlement en de Raad over over de evaluatie van Verordening (EU) Nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (eIDAS)*, Brussel, 2021, 2; H. JACQUEMIN en N. GILLARD, "Regulation 910/2014/EU – eIDAS Regulation", in S. GIJRATH, S. VAN DER HOF, A. R. LODDER en G-J ZWENNE, *Concise European Data Protection, E-Commerce and IT Law*, Alpen aan den Rijn, Wolters Kluwer, 2018, 517.
[191] Overweging 1 en 2 eIDAS verordening.
[192] Overweging 12 en 19 eIDAS verordening.
[193] Overweging 13 en 27 eIDAS verordening; W.Y. HU, F.M.J. VAN DEN BROEK, B.P.F. JACOBS, "Attribuut-gebaseerde elektronische handtekeningen en de eIDAS-verordeninging" in P.T.J WOLTERS, *Digitalisering en conflictoplossing reeks OO&R deel 130*, Alpen aan den Rijn, Wolters Kluwer, 2021, (293) 293.
[194] Art. 7 b) eIDAS verordening; H. JACQUEMIN en N. GILLARD, "Regulation 910/2014/EU – eIDAS Regulation", in S. GIJRATH, S. VAN DER HOF, A. R. LODDER en G-J ZWENNE, *Concise European Data Protection, E-Commerce and IT Law*, Alpen aan den Rijn, Wolters Kluwer, 2018, 533.
[195] Art. 7 d) eIDAS verordening.
[196] H. GRAUX, "De eIDAS-Verordening en de begeleidende Belgische wetgeving : nieuwe marsorders voor elektronische handtekeningen en andere vertrouwensdiensten", *CDJ* 2016, nr. 3, (53) 57.
[197] Art. 8 eIDAS verordening; Uitvoeringsverord.Comm Nr. 2015/1502, 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, 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, *Pb.L* 9 september 2015, afl 235, 7.

verplichting om alle systemen die aan de verplichtingen zouden voldoen aan te melden, noch om überhaupt een systeem aan te melden.[198]

Daarentegen verplicht de verordening door middel van een systeem van wederzijdse erkenning wél dat wanneer lidstaten om gebruik te maken van een online dienst een verplichte authenticatie oplegt, zij ook de aangemelde identificatiemiddelen van andere lidstaten moet ondersteunen in zoverre deze buitenlandse systemen het niveau substantieel of hoog behalen en daarbij eenzelfde level van betrouwbaarheid kunnen voorleggen als de systemen van de lidstaat die de verplichte authenticatie oplegt.[199] Authenticatiesystemen met een betrouwbaarheidsniveau laag of die een lager betrouwbaarheidsniveau hebben dan de eigen systemen hoeven dus niet geaccepteerd te worden.

112. Wetende dat België momenteel twee systemen heeft aangemeld: de Belgische eID en de Itsme applicatie en dat deze systemen beide het betrouwbaarheidsniveau "hoog" hebben verkregen, zouden deze systemen alle Belgen toegang moeten kunnen verlenen tot alle e-gov applicaties binnen het gecreëerde netwerk doch -uiteraard- enkel in zoverre zij het recht hebben om van deze diensten gebruik te maken.[200] Het valt te verwachten dat eens MyID zijn securityproblemen oplost, ook zij in de Europese lijst met erkende systemen zal worden opgenomen, zij het met betrouwbaarheidsniveau substantieel.

C. Herziening van de eIDAS verordening

a) Tekortkomingen

113. Zoals staatssecretaris Michel in België deed in 2022, sprak Ursula Von der Leyen zich reeds in 2020 uit voor verschillende initiatieven betreffende een algemene digitale identiteit voor EU burgers.[201] Volgens een evaluatie van de Commissie slaagt de eIDAS er immers slechts gedeeltelijk in zijn doel (het mogelijk maken voor EU burgers om met nationaal geaccepteerde elektronische identificatiemiddelen gebruik te kunnen maken van publieke dienstverlening over de grenzen heen) te bereiken.[202]

114. Zo constateerde de Commissie dat, ondanks het feit dat de verordening erin geslaagd is een eID netwerk te creëren, slechts 59% van de Europese burgers toegang heeft tot een eID en dat er technische problemen zouden zijn met het infrastructuurnetwerk van de eIDAS. Daarnaast heeft de keuze om de lidstaten vrij te laten in de technologiekeuze voor de implementatie van de eIDAS, ondanks de veelheid aan begeleidende regeling met de nodige technologische standaarden en vereisten -waar België overigens wel dankbaar gebruik van maakte-, geleid tot een versnipperde

[198] Overweging 14; H. GRAUX, "De eIDAS-Verordening en de begeleidende Belgische wetgeving : nieuwe marsorders voor elektronische handtekeningen en andere vertrouwensdiensten", *CDJ* 2016, nr. 3, (53) 57.
[199] Art. 6 eIDAS Verordening; H. JACQUEMIN en N. GILLARD, "Regulation 910/2014/EU – eIDAS Regulation", in S. GIJRATH, S. VAN DER HOF, A. R. LODDER en G-J ZWENNE, *Concise European Data Protection, E-Commerce and IT Law*, Alpen aan den Rijn, Wolters Kluwer, 2018, 531.
[200] Overweging 14 eIDAS Verordening.
[201] U. VON DER LEYEN, *State of the Union 2020*, Brussel, 2020, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655, 8.
[202] H. JACQUEMIN en N. GILLARD, "Regulation 910/2014/EU – eIDAS Regulation", in S. GIJRATH, S. VAN DER HOF, A. R. LODDER en G-J ZWENNE, *Concise European Data Protection, E-Commerce and IT Law*, Alpen aan den Rijn, Wolters Kluwer, 2018, 517.

markt en een veelheid aan verschillende interpretaties door de nationale toezichthoudende organen.[203]

115. Een tweede zwakte die naar boven kwam bij het evalueren van de verordening was het veranderde eID-ecosysteem waarbij -zoals ook het geval is in België- steeds meer beroep wordt gedaan op privaat georganiseerde dienstverleners die instaan voor de online authenticatie. Door het toenemend aantal online transacties dreigen ook steeds meer Europese burgers, die geen toegang hebben tot een veilige online identiteit, uit de boot te vallen. Het blijft dan ook belangrijk om te voorzien in gemeenschappelijke normen voor alle lidstaten en de focus van de verordening op aangemelde eID regelingen en op de toegang tot online overheidsdiensten te verbreden.[204]

116. Een derde groep tekortkoming die aan het licht kwam, bestaat erin dat onder de lidstaten -ondanks de aanwezige bijlagen in de uitvoeringsverordeningen- geen eensgezindheid zou bestaan over welke systemen nu precies een hoge, dan wel substantiële of lage betrouwbaarheid bezitten. Bovendien zou -in het kader van de AVG- de burger/gebruiker van de dienst onder de huidige regelgeving te weinig in staat zijn om zijn rechten wat betreft gegevensminimalisering en de controle op welke gegevens met welke partners worden gedeeld, uit te oefenen. Onder het huidige systeem is het immers zo dat steeds een minimale dataset volledig wordt doorgestuurd om de authenticatie van de gebruiker mogelijk te maken. Ten slotte zou er duidelijkheid moeten komen over de rol van de nationale instanties die de aanbieders van authenticatiediensten dienen te controleren.[205] Het is duidelijk dat, aangezien ook België zich volledig gebaseerd heeft op de technische vereisten zoals zij vermeld staan in de verordening, ook in onze nationale regelgeving dezelfde tekortkomingen aanwezig zijn zoals overigens uit het vorige hoofdstuk al bleek.

117. Een laatste algemene tekortkoming van de eIDAS is het feit dat door de gebrekkige implementatie door de lidstaten, de eIDAS verordening slechts tot een geringe toegevoegde waarde voor de digitale Europese markt leidt.[206] De gebrekkige implementatie zou er komen door het gebrek aan verplichting tot het registreren van eID regelingen waardoor vele lidstaten geen maatregelen getroffen hebben, of ervoor kozen om de systemen die ze ontwikkelden niet (wederkerig) te laten erkennen door andere lidstaten.[207] Echter is het duidelijk dat België met zijn drie erkende authenticatiesystemen eerder een voortrekkersrol opneemt dan een achterblijver is ten opzichte van de rest van Europa.

118. Naast de besproken tekortkomingen wijst de Commissie ook op de snel veranderende digitale omgeving. Daar waar het in 2014 nog voldoende was om in de verordening te focussen op veilige grensoverschrijdende toegangsmogelijkheden voor online overheidsdiensten, verwachten burgers en bedrijven -gestuwd door de corona digitaliseringsgolf waarbij verschillende openbare diensten plots online georganiseerd moesten worden- tegenwoordig meer. Zo verwachten burgers en bedrijven -aldus de Commissie- een hoge mate van gemak en veiligheid voor allerlei online activiteiten zoals

[203] EUROPESE COMMISSIE, *Verslag van de Commissie aan het Europees Parlement en de Raad over over de evaluatie van Verordening (EU) Nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (eIDAS)*, Brussel, 2021, 3-4.
[204] *Ibid*., 4-5.
[205] *Ibid*., 5.
[206] *Ibid*., 6.
[207] EPRS, *Revision of the eIDAS regulation, findings on its implementation and application,* 2022, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)699491, 3.

het inschrijven bij buitenlandse universiteiten, inschrijven op online aanbestedingen, het indienen van belastingaangiften, …

Door die toegenomen digitalisering en hogere eisen van de gebruikers, zou de vraag naar online authenticatiemiddelen en tools voor het uitwisselen van persoonsgegevens met betrouwbaarheidsniveau "hoog" exponentieel zijn toegenomen wat geleid heeft tot een paradigmaverschuiving van het gebruik van starre online identiteiten naar tools die verschillende verifieerbare gegevens, certificaten en attributen met betrekking tot de identiteit van een gebruiker kunnen integreren. Volgens de commissie zouden de huidige eID middelen die mogelijk zijn onder de eIDAS niet aan deze vereisten kunnen voldoen. Daarnaast zou de particuliere sector voornamelijk buiten de verordening gebruik maken van authenticatiediensten ontwikkeld door bijvoorbeeld Google en Facebook die, zoals hierboven reeds beschreven, slechts een lage betrouwbaarheid kunnen garanderen en dus geen link kunnen garanderen naar een door een overheid geverifieerde eID. De reden dat er -ondanks de toegenomen vraag naar authenticatiemechanismen met betrouwbaarheidsniveau hoog- meer en meer gebruik gemaakt wordt van diensten zoals Facebook en Google, ligt voornamelijk aan het complexe aanmeldingsproces voor particuliere aanbieders voor online diensten om zich aan te sluiten op het door de eIDAS gecreëerde netwerk.[208]

119. Met een nieuwe en sterkere eIDAS wil de commissie inspelen op deze veranderende noden en vermelde tekortkomingen door te voorzien in betrouwbare authenticatiemiddelen met aan de overheid gekoppelde eID's maar ook andere door de overheden of private sector verleende credenties -zoals bijvoorbeeld een lidkaart, rijbewijs, inentingscertificaat, diploma, medische attesten,…- die allen volledig door de gebruiker kunnen worden beheerd en die in de hele EU worden erkend en gebruikt kunnen worden om toegang te krijgen tot openbare en particuliere diensten.[209]

120. Mijn inziens kan de redenering van de Commissie, wanneer we naar de situatie in België kijken, niet integraal gevolgd worden. Itsme slaagt er immers reeds enkele jaren in zowel in de overheids- als de private sector authenticatiediensten te leveren die gekoppeld zijn aan de eID van de Belgische burgers. Bovendien zijn zij er ook in geslaagd om bij de uitvoering van deze dienst het door de eIDAS opgelegde betrouwbaarheidsniveau "hoog" te bereiken. Bovendien zagen we tijdens de coronacrisis dat Itsme met de "corona app" in staat is zeer snel aan nieuwe maatschappelijke noden wat betreft authenticatie en certificaten te voldoen en werkt de app op een gebruiksvriendelijke manier binnen heel Europa. Het is dus nog maar de vraag of een groot deel van de doelen van de Commissie niet al bereikt kunnen worden onder het huidige kader van de eIDAS.

Langs de andere kant lijkt de doelstelling om verschillende credenties, certificaten en authenticatiemogelijkheden onder te brengen onder één dienst georganiseerd door een selecte club dienstverleners om zo het gebruiksgemak hoog te houden en fragmentatie binnen Europa tegen te gaan wel valabel. Bovendien is het opvallend dat in de evaluatie van de huidige eIDAS Facebook en Google expliciet genoemd worden als voorbeelden van hoe online identificatie niet hoort te gebeuren maar in de praktijk toch vaak als identificatietool blijkt te worden gebruikt. Mijn inziens kan de hervorming van de eIDAS dan niet volledig los gezien worden van de strijd van de EU tegen het

[208] EUROPESE COMMISSIE, *Verslag van de Commissie aan het Europees Parlement en de Raad over over de evaluatie van Verordening (EU) Nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (eIDAS)*, Brussel, 2021, 6.
[209] *Ibid*., 7.

gebruik van persoonlijke data van EU burgers door private (buiten de EU gevestigde) ondernemingen. Het zal in het verdere verloop van dit hoofdstuk duidelijk worden of er -met deze doelstelling in het achterhoofd- überhaupt nog plaats zal zijn voor privaat georganiseerde authenticatiediensten of dat het organiseren van een digitale portefeuille een zuiver overheidsgestuurde dienst moet worden.

b) Voorstel tot een hernieuwde eIDAS

121. De hervorming van de eIDAS staat dus al even op de Europese agenda en past volledig binnen de nieuwe digitale strategie waarbij Europa zich tot doel stelt wereldleider te worden inzake de digitale evolutie door middel van toegankelijke technologie, in een open economie en een duurzame democratische samenleving.[210] Tegen 2030 zou er binnen Europa een brede uitrol van een betrouwbare en volledig door de burger gecontroleerde online identiteit moeten hebben plaatsgevonden waarbij 80% van de EU burgers toegang hebben tot een online ID oplossing.[211] In wat verder onder deze titel volgt, wordt dieper ingegaan op de voorgestelde hervorming en de mogelijke gevolgen voor België en andere Europese landen. Uiteraard zal er, gezien de afbakening van deze scriptie, opnieuw enkel gekeken worden naar de artikelen die betrekking hebben op de online identificatie voor overheidstoepassingen.

122. Op 3 juni 2021 deed de Commissie uiteindelijk een voorstel tot herziening van de huidige eIDAS verordening aan het Europees parlement en de Raad.[212] De doelstellingen van deze vernieuwde verordening kunnen worden samengevat als het creëren van een wettelijk kader dat met oog op grensoverschrijdend gebruik toelaat om toegang tot sterk beveiligde elektronische identiteitsoplossingen aan te bieden die gebruikt kunnen worden door zowel openbare en particuliere dienstverleners als burgers en rechtspersonen en verbonden zijn met een reeks attributen waarmee zeer specifieke identiteitsgegevens -enkel diegene die voor de welbepaalde dienst nodig zijn- kunnen worden gedeeld.[213] Zo zou iemand die bijvoorbeeld zijn of haar meerderjarigheid moet bewijzen, niet langer een (digitale) kaart met al zijn gegevens moeten overhandigen maar zou die persoon er via zijn digitale portefeuille voor kunnen kiezen enkel zijn leeftijd te delen. In vergelijking met de huidige eIDAS, wordt het dus duidelijk dat er een shift heeft plaatsgevonden van het gebruik van rigide digitale identiteiten naar de wil tot het louter delen van specifieke attributen die met onze identiteit verbonden zijn en een bijkomende focusuitbreiding van authenticatie voor online diensten aangeboden door de overheden naar online diensten aangeboden door particuliere partners.[214]

Naast de bovenvermelde vernieuwingen wil de commissie met haar voorstel tot vernieuwing ook inzetten op een geharmoniseerde beveiliging van de online identificatietools om zo de bestaande versnippering tegen te gaan. Hiertoe nam de Commissie gelijktijdig met hun voorstel tot vernieuwing van de eIDAS een aanbeveling aan die lidstaten en andere belanghebbenden uitnodigt om samen

[210] EUROPESE COMMISSIE, *Shaping Europe's digital future,* Luxemburg, Publications office of the European Union, 2020, 2,6.
[211] Mededeling (Comm.) aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het comité van de regio's Digitaal kompas 2030: de Europese aanpak voor het digitale decennium, 9 maart 2021, COM(2021) 118 final, 13-14.
[212] Voorstel (Comm.) voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit, 3 juni 2021, COM(2021) 281 final. (Hierna: Voorstel wijziging eIDAS verordening).
[213] Toelichting bij voorstel wijziging eIDAS verordening, 1.
[214] S. BERTILLE DEMBELE, "La protection de l'identité numérique post mortem", *RDTI* 2018, nr. 3, (5) 7.

met de Commissie te werken aan een "toolbox" om uiteenlopende benaderingen te voorkomen en de toekomstige uitvoering van het Europese kader betreffende online identificatie niet opnieuw in het gedrang te brengen.[215]

123. Een eerste aanpassing in het voorstel is de invoering van een verplichting voor de lidstaten om binnen het jaar na de inwerkingtreding van de nieuwe verordening een "Europese portemonnee voor digitale identiteit" uit te geven. Dit kan door de lidstaat zelf, krachtens een mandaat door de lidstaat of door privépartners op zelfstandige basis maar weliswaar na erkenning door de betrokken lidstaat.[216] De Europese portemonnee voor digitale identiteit wordt gedefinieerd als:

> *"een product en dienst die de gebruiker in staat stelt identiteitsgegevens, inloggegevens en attributen met betrekking tot zijn/haar identiteit op te slaan, op verzoek aan vertrouwende partijen te verstrekken, voor online en offline authenticatie voor een dienst overeenkomstig artikel 6 bis te gebruiken, en gekwalificeerde elektronische handtekeningen en zegels aan te maken"*[217]

Waarbij "attributen" -volledig in lijn met wat hierboven werd uiteengezet worden gedefinieerd als:

> *"een eigenschap, kenmerk of kwaliteit van een natuurlijke of rechtspersoon of een entiteit, in elektronisch formaat"*[218]

Elke digitale overheidsdienst die op basis van nationaal recht online authenticatie vereist alsook elke particuliere dienst waarvoor ofwel wettelijk een sterke authenticatie ofwel contractueel een sterke authenticatie voor zover het gaat om enkele belangrijke gebieden zoals sociale zekerheid, financiële dienstverlening, onderwijs,… vereist is, is verplicht om de Europese portemonnee voor digitale identiteit te aanvaarden als authenticatiemiddel.[219]

124. De portemonnees voor digitale identiteit moeten in het voorstel -net zoals bij de huidige eIDAS- voldoen aan een aantal bijzondere techniciteiten zoals een gemeenschappelijke interface, een ingebouwd authenticatiemechanisme, het waarborgen dat verleners van attributieattesten geen info verkrijgen over het gebruik van deze attributen én dat er voldaan wordt aan de voorwaarden om veiligheidsniveau hoog te halen zoals zij beschreven staan in het ongemoeid gelaten artikel 8 van de huidige eIDAS verordening en de uitvoeringsverordening.[220] Wel zou de commissie -indien het voorstel effectief omgezet wordt in een verordening- binnen de zes maanden na de inwerkingtreding met een nieuwe uitvoeringsverordening naar buiten komen die geüpdatete technische specificaties zou bevatten.[221] Het is aan de lidstaten zelf om te voorzien in valideringsmechanismen die de authenticiteit en veiligheid van de Europese portemonnees voor digitale identiteit, de geldigheid van de attesteringen van de attributen en de geldigheid van de aan de portemonnee gekoppelde persoonsidentificatiegegevens kunnen verifiëren.[222]

---

[215] *Ibid*., 2-3.
[216] Art 1 (6), art 6bis lid 1 en lid 2 en art. 7 lid 1 voorstel wijziging eIDAS verordening.
[217] *Ibid*., art 3.42.
[218] *Ibid*., art. 3.43.
[219] *Ibid*., art 12 ter lid 1 en 2.
[220] Art. 6bis lid 4 en lid 6 voorstel wijziging eIDAS verordening.
[221] *Ibid*., Art. 6bis lid 11
[222] *Ibid*., art 6bis lid 5.

Daarnaast stapt de Commissie in haar voorstel af van het principe van volledige technologie neutraliteit en wordt van de lidstaten verwacht dat zij een gemeenschappelijk mechanisme implementeren voor de authenticatie van gebruikers. Opnieuw zal de Commissie zes maanden na de inwerkingtreding van de nieuwe eIDAS zelf met een uitvoeringsverordening komen met technische en operationele specificaties om deze laatste verplichting concreter vast te leggen.[223]

125. Zoals reeds eerder aangehaald is het de bedoeling dat de burger volledige controle blijft behouden over zijn digitale identiteit. Dit houdt onder meer in dat de ontwikkelaar van de portefeuille -publiek dan wel privaat georganiseerd- geen informatie mag verzamelen betreffende het gebruik die niet noodzakelijk zijn voor het leveren van zijn diensten. Bovendien mogen de identificatiegegevens -tenzij op uitdrukkelijke vraag van de gebruiker- niet gecombineerd worden met andere persoonsgegevens die de afgever zou bezitten omdat hij naast het uitgeven van de portefeuille ook andere diensten aan de gebruiker levert. De identificatiegegevens moeten ter uitvoering van dit verbod dan ook "fysiek en logisch" gescheiden worden van de andere gegevens.[224] Wanneer het gaat om particuliere dienstverleners, dienen zij een aparte juridische identiteit op te richten voor de verschillende diensten.[225] Met deze bepalingen probeert het Hof duidelijk het principe van de minimale gegevensverwerking zoals vervat in de AVG (zie *infra* randnr. 172 ev.) concreet uit te werken voor de toepassing op de digitale portefeuilles.

126. Een volgende opvallende wijziging die voorgesteld wordt, is de verplichte certificering voor de Europese portefeuilles voor digitale identiteit. Zo moeten de aangemelde portefeuilles een certificering krijgen die aantoont dat zij voldoen aan bepaalde cyberbeveiligingsstandaarden -iets wat in de oude eIDAS zelfs niet wordt vermeld- in overeenstemming met verordening 2019/881, een certificaat dat zij de gegevens beschermen in overeenstemming met de AVG én moeten zij een certificaat bekomen dat uitgegeven wordt door door de staat op te richten -publieke dan wel private- organen waaruit moet blijken dat de portefeuilles voldoen aan de technische vereisten zoals uitgewerkt in het nieuwe voorstel en in een nog voor te stellen uitvoeringsverordening.[226]

Dat de organen van de EU het belang van een goede cybersecurity inzien, bewijst ook de onlangs (14 december 2022) aangenomen NIS 2 richtlijn die een hoger en gemeenschappelijk cyberbeveiligingsniveau binnen de EU beoogt. Na implementatie van deze richtlijn zullen onder andere instellingen van het openbaar bestuur en (middel)grote ondernemingen binnen bepaalde sectoren (waaronder digitale infrastructuur en digitale aanbieders) moeten voldoen aan strengere beveiligings- en rapportageverplichtingen. Eén van de te implementeren maatregelen is het gebruik van multi-factor authenticatie "waar nodig".[227]

127. Ter uitvoering van de idee van de Europese digitale portemonnee, was het oorspronkelijke plan dat elke burger een unieke en permanente identificatiecode toegewezen zou krijgen die via de

[223] *Ibid*. art. 6ter lid 2 en lid 4.
[224] *Ibid*., art 6bis lid 7.
[225] *Ibid*., *io*. 45 septies lid 4 voorstel wijziging eIDAS verordening.
[226] *Ibid*., art 6 quater lid 1-4 en art. 12bis.
[227] Art. 21 lid 2 Richtl.Europese Raad en parl. nr. 2022/2555, 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn), Pb.L 27 december 2022, afl. 333, 80.

portefeuille app gedeeld zou worden met publieke en private dienstverleners.[228] Echter is op dit idee zoveel kritiek gekomen van de lidstaten die het idee hadden dat een unieke identificatiecode zou leiden tot dataconcentratie en het de deur zou openzetten voor overheden en bedrijven om alles waarvoor de digitale portefeuille gebruikt wordt te kunnen opvolgen en zou kunnen leiden tot profiling, dat de unieke identificatiecode voor haar burgers optioneel is geworden voor de lidstaten.[229] Verder is het ook hier wachten op verdere details tot de Commissie met haar uitvoeringsverordening naar buiten komt.

c) Gevolgen voor België

128. België koos er -net als 19 andere Europese landen zoals Nederland, Zweden en Duitsland-[230] voor om mee te gaan in het eIDAS verhaal door te voorzien in twee elektronische identificatiemogelijkheden met betrouwbaarheidsniveau "hoog". België onderscheidt zich echter van deze landen door enerzijds te kiezen voor een systeem dat uitgebaat wordt door een -deels- privaat consortium waar andere landen kiezen voor een louter overheidsgereguleerd authenticatiemechanisme en anderzijds door verder te gaan dan het merendeel van deze 16 landen door te voorzien in een systeem dat niet enkel gebruikt kan worden ter authenticatie van personen voor online overheidsdiensten maar ook voor bepaalde private onlinediensten. Mijn inziens kan België op vlak van digitale identiteit wat betreft de huidige situatie dan ook gezien worden als een voortrekker binnen Europa.

Toch is het duidelijk dat de Europese Unie met de eIDAS 2.0 en de invoering van de digitale portefeuille nog een stap verder wil gaan dan wat momenteel in België mogelijk is.

129. Volgend uit het voorstel van de Commissie kwam ook staatssecretaris Michel met het initiatief om, tegen einde 2023, voor elke Belg een digitale portefeuille te voorzien die ook uitgerust zou moeten zijn met een authenticatiemechanisme (zie *supra* randnrs. 53 en 54). Hoewel het zeker niet onmogelijk is om dit praktisch op nationaal niveau uit te werken en in een nieuw nationaal wettelijk kader te voorzien dat voldoende waarborgen bevat betreffende de veiligheid van de digitale identiteitsgegevens van de burgers, moet er ook rekening gehouden worden met de huidige ontwikkelingen op Europees niveau.

De bedoeling van zowel de huidige eIDAS als de toekomstige, is immers om minstens te voorzien in erkende authenticatiemechanismes dat burgers van de lidstaten toelaat om zich binnen heel Europa online te kunnen identificeren bij online overheidsdiensten. Hoewel het in algemene lijnen duidelijk is wat de Europese Commissie met haar verplichte digitale portemonnee voor ogen heeft, mag de Belgische federale overheid niet vergeten dat wanneer zij zelf een digitale portefeuille wil uitwerken die binnen het nieuwe (toekomstige?) eIDAS systeem wordt erkend, deze zal moeten voldoen aan bepaalde -nog uit te werken- technische en operationele specificaties en cyberveiligheidsvereisten

---

[228] *Ibid*, art 11 bis lid 2; EDRI, *eIDAS policy paper*, 25 januari 2021, https://www.europarl.europa.eu/cmsdata/244763/eIDAS-policy%20paper-EW+EDRi.pdf, 1; M. KIROVA, *Overview of pre-notified and notified eID schemes under eIDAS*, laatste bijwerking: D. GATTWINKEL 24 januari 2023, https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS.

[229] *Vr. en Antw.* Tweede kamer (ndl.) 2022-2023, 16 februari 2023, nr. 54-6, 4 (LEIJTEN antw. VAN HUFFELEN).

[230] EU, "Stelsels voor elektronische identificatie aangemeld overeenkomstig artikel 9, lid 1, 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", *Pb.L* 21 augustus 2020, afl 276, 2.

én dat er een initiatief zal komen om een gemeenschappelijk mechanisme uit te bouwen (zie *supra* randnr. 122). Door voor het einde van dit jaar een eigen initiatief te ontwikkelen -al lijkt die deadline gezien het gebrek aan parlementaire activiteiten stilaan onhaalbaar te worden-, loopt de federale overheid mijn inziens dan ook het risico om (als het voorstel van de commissie wordt omgezet in een decreet) over enkele jaren zijn huiswerk opnieuw te moeten maken.

In Nederland hebben ze dit goed begrepen. Daar wordt met de wet digitale overheid (die werd aangenomen op 21 maart 2023) een duidelijke opsplitsing gemaakt tussen een implementatie van identificatiemechanismen en de implementatie van een digitale portefeuille zoals wordt voorgesteld in eIDAS 2.0. Dat laatste zullen ze pas doen eens deze verordening van kracht is.[231] Wel werd er reeds een nationaal proefproject opgestart dat het mogelijk moet maken om op een meer geïnformeerde manier deel te nemen aan de besprekingen over de implementatie van de digitale portefeuille.[232]

130. Een groot voordeel dat een overheid wél heeft in de ontwikkeling van de digitale portefeuille tegenover private ontwikkelaars is dat zij reeds veel data over de identiteitsattributen van gebruikers beheert. Het zal dan ook veel makkelijker zijn om een gecentraliseerd model te ontwikkelen.

131. Zoals hierboven beschreven (zie *supra* randnr. 123) is het onder het nieuwe voorstel ook nog steeds mogelijk dat deze digitale portefeuille uitgewerkt wordt door private partijen waarna de applicatie erkend dient te worden door de nationale overheid. Omdat België momenteel het enige Europese land is dat gebruikt maakt van authenticatiemechanismen die uitgebaat worden door private partners, is het ietwat onduidelijk in hoeverre er ook effectief nog plaats zal zijn voor deze diensten onder een nieuwe eIDAS verordening. De bestaande authenticatietools zullen mijn inziens twee mogelijke opties hebben binnen de huidige Belgische en Europese evolutie:

Vooreerst is er natuurlijk de optie dat de huidige aanbieders van authenticatiediensten naast de kernidentiteit ook de nodige identiteitsattributen zelf, gecentraliseerd gaan beheren. Zij zouden die zelf bij hun gebruikers kunnen opvragen of zij zouden deze (deels) kunnen verkrijgen in samenwerking met de bevoegde overheden en eventuele andere instanties die momenteel deze data beheren. Vanuit deze gecentraliseerde portefeuille kunnen burgers dan de nodige gegevens uitwisselen met derde partijen. Binnen dit scenario kan men zich wel de vraag stellen of het in het kader van cybersecurity en identiteitsfraude wel veilig is om zoveel gegevens van burgers vanuit één centrale plek te beheren. Bij de minste veiligheidsproblemen liggen immers meteen alle persoonsgegevens van de slachtoffers op straat. Bovendien kan men zich in het kader van de AVG en de toelaatbaarheid van gegevensverwerking (zie infra randnr. 147) vragen stellen bij de manieren waarop de authenticatietools aan de nodige gegevens betreffende de identiteitsattributen zouden geraken. In ieder geval zou voor wat dit laatste betreft een volledig nieuw wettelijk kader moeten worden uitgewerkt.

Daarnaast zouden de huidige authenticatiemechanismen als één van de mogelijke authenticatiemechanismen bij een door de overheid ontwikkelde gecentraliseerde of gedecentraliseerde digitale portefeuille met de benodigde identiteitsattributen kunnen fungeren. Zij

[231] Verslag van de vergadering van 21 februari 2023, *Parl.St.* Eerste Kamer (Ndl) 2022-2023, nr. 20, https://www.eerstekamer.nl/handelingen/ek/20230221/wet_digitale_overheid, 2.
[232] *Vr. en Antw.* Tweede kamer (ndl.) 2022-2023, 16 februari 2023, nr. 54-6, 4 (LEIJTEN antw. VAN HUFFELEN).

zouden met andere woorden een soort hybride model kunnen creëren waarbij de authenticatieapps wel het beheer van de kernidentiteit op zich blijven nemen (en dus in staat blijven om aan de overheidsdiensten de burger te authenticeren) én daarbij in interactie kunnen treden met andere data-platformen die op hun beurt verantwoordelijk blijven voor het beheer van de in hun bezit zijnde identiteitsattributen. De authenticatietools zouden daarbij als het ware dienen als een soort doorgeefluik tussen deze dataplatformen en de overheidsdienst die de nodige data opvraagt zonder dat deze data door de authenticatietool wordt opgeslagen. In deze situatie zouden dus de hierboven besproken rollen van authenticator en integrator gecombineerd worden door één partij. Het is echter nog maar de vraag of bestaande authenticatiemechanismen in dit scenario, door de integratie van een door de overheid ontwikkeld authenticatiemiddel binnen deze portefeuille niet weggeconcurreerd zullen worden. Het spreekt in ieder geval voor zich dat ook in dit geval het huidige wetgevend kader wat betreft de erkenning van privaat georganiseerde authenticatiemechanismen bij een dergelijke uitbreiding van functies ontoereikend zal worden en er een apart dan wel geïntegreerd kader moet komen voor wat betreft de uitwisseling van de persoonsgegevens tussen de authenticator en de externe dataplatformen. Wat de authenticatiefunctie zelf betreft, verandert er in dit scenario in de praktijk weliswaar niets waardoor het huidige kader voor dat aspect -op de verwijzingen naar de huidige eIDAS na- voldoende lijkt. Een bijkomend probleem voor de authenticatiediensten is het feit dat zij, om binnen heel Europa erkend te kunnen worden, opnieuw zullen moeten voldoen aan de nog uit te werken technische en operationele specificaties.

132. Ondanks de vele uitdagingen, sprak Itsme zich reeds in 2020 uit in het voordeel van het tweede scenario en maakt het zich sterk dat de app zo is ontwikkeld dat zij snel zou kunnen schakelen naar het hierboven beschreven hybride systeem.[233]

Op 4 mei 2023 lanceerde Vlaams minister president Jan Jambon met "Athumi" het proefproject van het Vlaams datanutsbedrijf rond een datakluis die het voor burgers mogelijk zou moeten maken om zelf te bepalen welke persoonlijke gegevens online worden uitgewisseld met overheidsdiensten en bedrijven. De datakluis zou gegevens van burgers gecentraliseerd bewaren, burgers zouden er via authenticatiesystemen zoals Itsme toegang tot krijgen.[234] Hoewel er nog onvoldoende informatie beschikbaar is om het initiatief grondig te beoordelen, lijkt Vlaanderen met dit proefproject in ieder geval de kaart van de tweede optie te hebben getrokken.

D. Conclusie

133. In dit derde hoofdstuk werd ingegaan op het huidige kader dat op Europees niveau bestaat betreffende het identificatiebeleid. Op basis van voorbereidende documenten die een herziening van deze wetgeving beogen werd ingegaan op de zwaktes in deze wetgeving en de evoluties die binnen Europa plaatsvinden. Er werd daarnaast beschreven in welke mate België reeds aangepast was aan

[233] BELGIAN MOBILE ID, *de toekomst van digitale identiteit*, 1 juni 2020, https://www.itsme-id.com/nl-BE/business/blog/future-of-digital-id, laatst bezocht 9 maart 2023.
[234] Art. 5 Decreet 2 december 2022 houdende machtiging tot oprichting van het privaatrechtelijk vormgegeven extern verzelfstandigd agentschap Vlaams Datanutsbedrijf in de vorm van een naamloze vennootschap, *BS* 14 december 2022; AGENTSCHAP DIGITAAL VLAANDEREN, *Het Vlaams Datanutsbedrijf gaat officieel van start onder de naam 'athumi'*, persbericht 5 mei 2023, https://www.vlaanderen.be/digitaal-vlaanderen/nieuwsberichten/het-vlaams-datanutsbedrijf-gaat-officieel-van-start-onder-de-naam-athumi; C. MICHIELS, "Vlaanderen lanceert Athumi: bepalen we binnenkort zelf wat er met onze online data gebeurt?" in *VRTNieuws* 4 mei 2023, https://www.vrt.be/vrtnws/nl/2023/05/04/vlaanderen-lanceert-athumi-bepalen-we-binnenkort-zelf-wat-er-me/.

het oude wettelijke kader, of de zwaktes in het Europees beleid ook hier terug te vinden zijn en in hoeverre België reeds in staat zou zijn om mee te gaan in de voorgestelde evoluties. Op die manier kan (deels) een antwoord worden geformuleerd op sub-onderzoeksvragen 2 en 4.

134. Concluderend kan worden gesteld dat de Europese Unie met de eIDAS verordening wilde voorzien in een gemeenschappelijke Europese grondslag die de doeltreffendheid van de online overheidsdiensten binnen Europa moest verhogen. Door de implementatie van een gemeenschappelijk identificatiebeleid dat het op een veilige manier mogelijk zou maken om zich grensoverschrijdend te kunnen authenticeren wilde de EU de gebruiksvriendelijkheid van zijn burgers verhogen en rechtsonzekerheid wegnemen.

Om dit te bereiken voorziet de verordening in een soort minimumharmonisatie waarbij lidstaten zelf of via samenwerking met een private partner de mogelijkheid hebben om, rekening houdend met enkele technische specificaties, een gepast authenticatiemiddel uit te werken. Indien de lidstaten een middel laten erkennen, zijn zij verplicht om buitenlandse systemen die minstens een betrouwbaarheidsniveau van "substantieel" hebben te accepteren voor de eigen online overheidsdiensten zolang deze geen hoger betrouwbaarheidsniveau vereisen dan hetgeen waar het buitenlandse authenticatiemiddel in kan voorzien. In eerdere hoofdstukken werd reeds uitvoerig besproken dat België ijverig op de kar is gesprongen en met Itsme en de eID twee systemen met een hoog betrouwbaarheidsniveau heeft aangemeld.

135. Toch blijken er enkele zwaktes in de regulering te zitten: Zo zouden niet alle lidstaten even gretig als België mee in het eIDAS verhaal instappen, gelden er door de minimumvereisten verschillende standaarden over de landen heen waardoor er vertrouwensproblemen en discussies over de toegekende betrouwbaarheidsniveaus ontstaan. Bovendien wordt er steeds meer gebruik gemaakt van private (maar daarom niet altijd erkende) aanbieders van authenticatiediensten zoals Facebook en Google. Hoewel België ook gebruik maakt van de standaarden zoals zij vervat zitten in de uitvoeringsverordeningen van de eIDAS, werd in hoofdstuk II aangetoond dat er ook wordt voorzien in bijkomende beschermingsmechanismen. Toch werden zelfs in die bijkomende regulering nog heel wat zwaktes aangetroffen.

136. Met de eIDAS 2.0 wil de Europese Unie inspelen op deze zwaktes en de evoluties die plaatsvinden in de digitalisering van openbare dienstverlening implementeren. Zo bevat het voorstel tot verordening de verplichting voor lidstaten om een digitale portefeuille te ontwikkelen dat naast de kernidentiteit ook toegang heeft tot zogenaamde attributen. De digitale portefeuille zou het mogelijk moeten maken om niet steeds alle identiteitsgegevens door de sturen naar de online overheidsdienst maar slechts die gegevens die relevant zijn voor de gevraagde dienst. De digitale portefeuille moet ook een ingebouwde authenticatiedienst bevatten en voldoen aan nieuw -in overleg- vast te stellen technische vereisten. Daarnaast zouden om erkend te kunnen worden ook een aantal certificaten nodig zijn die een hoog niveau van cyberveiligheid en gegevensbescherming garanderen. Op die manier wordt dan ook afgestapt van de huidige technologieneutraliteit. Ten slotte zullen vanuit Europa bepaalde overheidsdiensten verplicht worden om gebruik te maken van de digitale portefeuille.

137. Voor België zijn deze ontwikkelingen dubbel. Enerzijds toont het via Itsme aan dat veel van de zorgen binnen de Commissie misschien niet volledig terecht zijn. Zo werd een systeem ontwikkeld

dat voldoet aan alle kwaliteitsnormen om een betrouwbaarheidsniveau "hoog" te behalen en dat reeds via de vaccinatieapp in België tijdens de coronacrisis bewezen heeft om op een betrouwbare en gebruiksvriendelijke manier snel te kunnen inspelen op maatschappelijke noden en dat het een systeem heeft ontwikkeld dat een attribuut (het al dan niet gevaccineerd zijn) kan voorleggen wanneer nodig.

Langs de andere kant valt er wel wat te zeggen voor de voorgestelde hervormingen: Zo zou het louter kunnen delen van attributen kunnen leiden tot een betere implementatie van het beginsel van minimale gegevensverwerking, werd in het vorige hoofdstuk reeds aangehaald dat de Belgische keuze om geen verplichting aan (bepaalde) overheden op te leggen om de erkende authenticatiemechanismen te gebruiken eerder een zwakte in het beleid is, is het in het veranderde digitale klimaat een goed idee om meer te gaan nadenken over cybersecurity en is de doelstelling om te komen tot een grotere harmonisatie binnen Europa uiteraard ook te verdedigen.

138. Hoewel de huidige staatssecretaris voorstander is om binnen Europa wat betreft het identificatiebeleid met België een voortrekkersrol te blijven spelen, lijkt het mijn inziens in het licht van de rechtszekerheid in België toch verstandiger om te wachten op de definitieve hervormingen binnen Europa. Wel kan België dankzij de unieke ervaring van de ontwikkelaars van de Itsme app een prominente rol aannemen ter ontwikkeling van de "toolbox". Daarnaast zou de staatssecretaris net als de Nederlandse overheid een proefproject kunnen starten in eigen land om de gevolgen van een flexibelere digitale identiteit beter te kunnen inschatten. De ontwikkelaars van de Itsme app gaven in ieder geval aan daar reeds klaar voor te zijn.

139. Een beslissing die België (of Europa?) in ieder geval zal moeten nemen is die in de keuze tussen een meer gecentraliseerde opslag van persoonsgegevens of een eerder gedecentraliseerde opslag van gegevens. Het nadeel van de eerste optie bestaat hem er uiteraard in dat deze situatie veel gevoeliger zou zijn voor grootschalige datalekken en misbruik. In de tweede situatie kan men zich de vraag stellen of privaat georganiseerde diensten omwille van redenen van gebruiksgemak niet zullen worden weggeconcurreerd door alternatieven ontwikkeld door de overheid die over reeds heel veel data beschikt en deze via dienstenintegratoren makkelijk onderling kan uitwisselen. Bovendien zal er aanvullende wetgeving nodig zijn die de modaliteiten wat betreft de nodige data uitwisseling tussen de aanbieders van de digitale portefeuille en de externe dataplatformen regelt. Hoewel het standpunt van België in deze discussie niet gekend is, sprak Nederland zich wel reeds uit voor datadecentralisatie.[235] Ook de ontwikkelaars van Itsme zelf spraken dezelfde voorkeur reeds uit.

[235] *Vr. en Antw.* Tweede kamer (ndl.) 2022-2023, 16 februari 2023, nr. 54-6, 4 (LEIJTEN antw. VAN HUFFELEN).

Hoofdstuk IV. Bescherming van persoonsgegevens

A. Algemeen

140. Artikelen 16 VWEU en 8 van het Handvest van de Grondrechten van de EU omvatten het recht op de bescherming van persoonsgegevens. De EU koos er in 1995 voor om dit recht te waarborgen door aan de lidstaten de Databeschermingsrichtlijn op te leggen. Omdat de lidstaten de regels vervat in deze richtlijn te weinig naleefden en opvolgden, koos de EU er met de Algemene Verordening Gegevensbescherming (hierna AVG) in 2016 voor om een meer dwingende en gedetailleerde verordening op te leggen.[236] Hoewel de AVG reeds in 2016 in werking is getreden, werd zij pas twee jaar later, en dus na de inwerkingtreding van de wet en het KB elektronische identificatie, effectief van toepassing in de lidstaten. De verordening houdt in de eerste plaats de principes van de oude databeschermingsrichtlijn in stand maar legt ook nieuwe verplichtingen en straffen op aan overheden en bedrijven die persoonsgegevens verwerken.[237] Op deze manier zullen overheden en bedrijven steeds een inschatting moeten maken van de risico's die verbonden zijn aan het verwerken van persoonsgegevens, zullen zij moeten kunnen aantonen dat zij de nodige maatregelen hebben getroffen om deze risico's te beperken en moeten zijn de verplichtingen uit de verordening naleven.[238]

141. In de parlementaire voorbereiding van het aangenomen wetsvoorstel digitale overheid in Nederland wordt de bevoegde minister van Binnenlandse Zaken opgedragen de specifieke rechten en verplichtingen in de AVG (zoals de transparantieverplichting, de verplichting tot dataminimalisatie, het recht op inzage en rectificatie, …) en hun specifieke werking in de keten die leidt tot authenticatie bij online overheidsdiensten, uit te werken.[239] De Nederlandse wetgever gaat daarmee in tegen het advies van de Nederlandse Autoriteit Persoonsgegevens, die zelfs aanraadde om de toepassing van de rechten en verplichtingen op te nemen in de wet zelf.[240] Hoewel het nog wachten is op deze verdere uitwerking, valt het te betreuren dat in België niet minstens dezelfde inspanningen werden geleverd. Het is immers zo dat de bepalingen van de AVG weliswaar rechtstreekse werking hebben maar toch zijn veel rechten en plichten die erin zijn vervat eerder algemeen opgesteld. Een verdere verdieping van deze beginselen en hun uitwerking op alle actoren in de authenticatieketen (en dus ook de overheden die gebruik maken van de authenticatiedienst) zou heel wat verwarring en discussie kunnen vermijden.

142. In wat in dit hoofdstuk nog volgt, wordt eerst het toepassingsgebied van de AVG beknopt besproken. Verder wordt voornamelijk ingegaan op de eerder algemene principes en verplichtingen van de AVG waar de overheid, bij het implementeren van een (nieuw) wettelijk kader betreffende elektronische identificatie, rekening mee zal moeten houden of had moeten houden.

---

[236] A. WILLEMS, "De beoordeling van de wetgevende kaders in Europa, China en de Verenigde Staten rond het gebruik van persoonsgegevens ter bestrijding van globale gezondheidscrisissen. Lessen uit de COVID-19-pandemie", *TPR* 2021, afl 4, (1729) 1735.
[237] M. GAWRONSKI, *Guide to the GDPR*, Alphen aan den Rijn, Kluwer Law International, 2019, 3
[238] *Ibid*., 4.
[239] MvT wet digitale overheid, 24-27.
[240] AUTORITEIT PERSOONSGEGEVENS, Advies wet ontwerp Wet generieke digitale infrastructuur, 13 oktober 2017, nr. z2017-06929, https://www.eerstekamer.nl/overig/20180619/advies_autoriteit_persoonsgegevens/document, 6.

B. Toepassingsgebied AVG

143. Zodra er sprake is van een (deels) automatische verwerking van persoonsgegevens of van een manuele verwerking waarbij de persoonsgegevens in een bestand worden opgenomen of daartoe bestemd zijn, is de AVG van toepassing.[241] De AVG is daarnaast van toepassing op alle verwerkers met vestigingen binnen de Europese Unie, zelfs als de verwerking daarbuiten gebeurt.[242] Dit betekent dat alle Belgische bedrijven die persoonsgegevens automatisch verwerken dan wel handmatig verwerken en opnemen in een bestand, verplicht zijn om te voldoen aan de bepalingen van de AVG. Als er sprake is van een handmatige verwerking maar geen (bedoeling tot) opname in een bestand, is de AVG niet van toepassing.[243]

144. De AVG definieert persoonsgegevens als:

"*alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon*"[244]

Deze definitie moet dermate ruim worden geïnterpreteerd dat het alle informatie in elke mogelijke vorm die verband kan houden met een persoon, zelf als deze informatie foutief of niet bewezen zou zijn, kan omvatten.[245] De gegevens kunnen daarnaast zowel direct (vb. naam, geslacht, leeftijd…) als indirect betrekking hebben op een persoon. Directe persoonsgegevens zijn die gegevens die direct betrekking hebben op een geïdentificeerde of identificeerbare persoon, zonder dat er verdere informatie nodig is om deze persoon te identificeren (vb. naam, telefoonnummer, sommige e-mailadressen, …). Indirecte persoonsgegevens zijn deze gegevens die op zichzelf genomen geen directe informatie verschaffen over een persoon maar in combinatie met andere gegevens wel kunnen worden gebruikt om een persoon te identificeren (vb. iemands beroep in combinatie met zijn werkgever).[246] Gegevens kunnen slechts indirect betrekking hebben op een persoon als zij een impact hebben op deze persoon of wanneer zij gebruikt worden ter beoordeling, beïnvloeding of behandeling van deze persoon.[247]

---

[241] Art. 2 AVG; *Vr. en Antw.* Kamer 2019/2020, 16 december 2020, nr. 55-031 (Vr. 12 S. MATHEÏ, Antw. M. Michel), 486; M. CAPRONI en S. DE SMEDT, *Praktische gids, Privacy in de onderneming*, Mechelen, Wolters Kluwer, 2019, 17; A. FOCQUET en E. DECLERCK, *gegevensbescherming in de praktijk*, Antwerpen, Intersentia, 2019, 5, 15.

[242] Art. 3 AVG; A. WILLEMS, "De beoordeling van de wetgevende kaders in Europa, China en de Verenigde Staten rond het gebruik van persoonsgegevens ter bestrijding van globale gezondheidscrisissen. Lessen uit de COVID-19-pandemie", TPR 2021, afl 4, (1729) 1735.

[243] *Vr. en Antw.* Kamer 2019/2020, 16 december 2020, nr. 55-031 (Vr. 12 S. MATHEÏ, Antw. M. Michel), 486; I. DE POORTER, "De 'GDPR' of algemene Verordening Gegevensbescherming (AVG) – Een algemene inleiding" in INSTITUUT FINANCIEEL RECHT, *Financieel recht: een dwarsdoorsnede*, Antwerpen, Intersentia, 2019, (449) 460; M. KRZYSZTOFEK, *GDPR, Personal data protection in the European Union*, Alphen aan den Rijn, Kluwer, 2021, 30

[244] Art 4 1) AVG; A. FOCQUET en E. DECLERCK, *gegevensbescherming in de praktijk*, Antwerpen, Intersentia, 2019, 6.

[245] I. DE POORTER, "De 'GDPR' of algemene Verordening Gegevensbescherming (AVG) – Een algemene inleiding" in INSTITUUT FINANCIEEL RECHT, *Financieel recht: een dwarsdoorsnede*, Antwerpen, Intersentia, 2019, (449) 453; A. FOCQUET en E. DECLERCK, *gegevensbescherming in de praktijk*, Antwerpen, Intersentia, 2019, 6, 9; F. HENRY en I. VERHELST "Protection des données à caractère personnel dans les relations individuelles et collectives de travail" in H., JACQUEMIN, *Le règlement général sur la protection des données (RGPD/GDPR): premières applications et analyse sectorielle*, Luik, Anthemis, 2020, 69; RAAD VAN EUROPA, *Handboek Europese gegevensbeschermingswetgeving,* Luxemburg, Bureau voor Publicaties van de Europese Unie, 2021, 100.

[246] ARTIKEL 29 WERKGROEP, *advies over het begrip persoonsgegeven*, 20 juni 2007, nr 4/2007, 13-14; D. DE BOT, *De toepassing van de algemene verordening gegevensbescherming in de Belgische context*, Mechelen, Wolters Kluwer, 2020, 115.

[247] A. FOCQUET en E. DECLERCK, *gegevensbescherming in de praktijk*, Antwerpen, Intersentia, 2019, 9.

Als de gegevens anoniem of geanonimiseerd zijn en er geen persoon meer uit afgeleid kan worden, is de AVG niet van toepassing.[248] Als er echter spraken is van een loutere pseudonimisering (waarbij identificatie met behulp van aanvullende gegevens opnieuw mogelijk is)[249], blijft de AVG wel van toepassing.[250]

145. Daarnaast moet ook het begrip "verwerking" ruim worden begrepen. Het verwijst naar alle mogelijke manieren waarop persoonsgegevens kunnen worden gebruikt, doorgegeven, bewaard of ter beschikking worden gesteld.[251]

146. Het spreekt voor zich dat wanneer het gaat om de online identificatie en authenticatie van personen, waarbij het delen en verifiëren van de identiteit van een persoon aan de hand van identificatoren centraal staat, er sprake is van een verwerking van persoonsgegevens. Zowel de overheden die om authenticatie vragen als de verificatoren zelf zullen zich aldus aan de principes en verplichtingen van de AVG moeten houden. De personen van wie de gegevens verwerkt worden, ontlenen dan weer bepaalde rechten (zoals het recht op informatie, inzage en rectificatie van de gegevens) aan de verordening. Bovendien is het niet ondenkbaar dat, wanneer men evolueert naar een digitale portemonnee, er bij het delen van identiteitsattributen gebruik gemaakt zal worden van zogenaamde "bijzondere categorieën van persoonsgegevens". Deze gegevens worden gedefinieerd als:

> "*Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid*."[252]

Concreet kan er bijvoorbeeld gedacht worden aan het online uitwisselen van het medisch dossier van een patiënt met het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering (RIZIV) of het sinds de verplichte invoering steeds belangrijker wordende digitale vingerafdruk op de eID.[253] Al heeft het Grondwettelijk Hof over dit laatste wel gezegd dat het beeld van de vingerafdruk meteen na afname moet verwijderd worden, niet permanent mag worden opgeslagen in een centrale databank doch

---

[248] M. CAPRONI en S. DE SMEDT, *Praktische gids, Privacy in de onderneming*, Mechelen, Wolters Kluwer, 2019, 30; A. FOCQUET en E. DECLERCK, *gegevensbescherming in de praktijk*, Antwerpen, Intersentia, 2019, 10-12; I. DE POORTER, "De 'GDPR' of algemene Verordening Gegevensbescherming (AVG) – Een algemene inleiding" in INSTITUUT FINANCIEEL RECHT, *Financieel recht: een dwarsdoorsnede*, Antwerpen, Intersentia, 2019, (449) 454.
[249] ARTIKEL 29 WERKGROEP, *advies over het begrip persoonsgegeven*, 20 juni 2007, nr 4/2007, 18-19.
[250] Overweging 26 AVG; D. DE BOT, *De toepassing van de algemene verordening gegevensbescherming in de Belgische context*, Mechelen, Wolters Kluwer, 2020, 210; I. DE POORTER, "De 'GDPR' of algemene Verordening Gegevensbescherming (AVG) – Een algemene inleiding" in INSTITUUT FINANCIEEL RECHT, *Financieel recht: een dwarsdoorsnede*, Antwerpen, Intersentia, 2019, (449) 457.
[251] Art. 4 2) AVG; HvJ 6 november 2003, nr. C-101/01, ECLI:EU:C:2003:596, Lindqvist/Zweden, §25; HVJ 13 mei 2014, nr. C-131/12, ECLI:EU:C:2014:317, Google Spain/AEPD §28; HvJ 9 maart 2017, nr. C-398/15, ECLI:EU:C:2017:197, Manni/Italië, §35; D. DE BOT, *De toepassing van de algemene verordening gegevensbescherming in de Belgische context*, Mechelen, Wolters Kluwer, 2020, 134; A. FOCQUET en E. DECLERCK, *gegevensbescherming in de praktijk*, Antwerpen, Intersentia, 2019, 14; RAAD VAN EUROPA, *Handboek Europese gegevensbeschermingswetgeving,* Luxemburg, Bureau voor Publicaties van de Europese Unie, 2021, 117-120.
[252] Art. 9 lid 1 AVG; RAAD VAN EUROPA, *Handboek Europese gegevensbeschermingswetgeving,* Luxemburg, Bureau voor Publicaties van de Europese Unie, 2021, 115; A. WILLEMS, "De beoordeling van de wetgevende kaders in Europa, China en de Verenigde Staten rond het gebruik van persoonsgegevens ter bestrijding van globale gezondheidscrisissen. Lessen uit de COVID-19-pandemie", *TPR* 2021, afl 4, (1729) 1736.
[253] Art. 6 §2 8° Wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten.

enkel in de eID zelf en dat de digitale afdrukken niet mogen worden uitgewisseld met andere overheidsinstanties.[254] Toch is het mijn inziens niet ondenkbaar dat in de evolutie naar een digitale identiteit, waarbij we steeds meer lijken af te stappen van de fysieke identiteitskaart, politiediensten uiteindelijk identiteiten zullen kunnen controleren via biometrische gegevens opgeslagen in de digitale portefeuille.

C. Toelaatbaarheid van de verwerking

147. Nu werd vastgesteld dat de AVG van toepassing is op verschillende actoren in het authenticatieproces, moet worden nagegaan of de verwerking van persoonsgegevens wel toegelaten is. Is zij niet toegelaten, is de verwerking altijd onrechtmatig in de zin van de AVG. De gronden waarop de toelaatbaarheid van de verwerking gebaseerd moet zijn om rechtmatig te zijn staan opgesomd in artikel 6 van de AVG.[255] De grote uitzondering op deze regel zijn de zogenaamde "bijzondere categorieën van persoonsgegevens" waarvoor een principieel verwerkingsverbod geldt.[256] De verschillende toestemmingsgronden die zouden kunnen dienen voor de verwerking van persoonsgegevens in de authenticatiecontext zijn de toestemming, de noodzakelijkheid voor het uitvoeren van een contract, en de noodzakelijkheid voor het invullen van een taak van het algemeen belang of openbaar gezag.[257] Ook een combinatie van deze toelatingsgronden zou mogelijk kunnen zijn.

148. De eerste en meest voor de hand liggende grond die gebruikt zou kunnen worden om de verwerking van persoonsgegevens toe te staan, is die van de noodzakelijkheid voor het invullen van een taak van het algemeen belang of openbaar gezag. Omdat er geen eenduidige definitie voorhanden is over de inhoud van het begrip "algemeen belang", komt het aan de wetgever toe te bepalen welke belangen als "algemeen" kunnen worden beschouwd.[258] Vaak zal dit gebeuren door op wettelijke basis een dienst of instelling op te richten aan wie specifieke taken worden toegekend die kunnen worden beschouwd als taken van algemeen belang. Dat kan ook door het toevoegen van een bijkomende taak aan een reeds bestaande instelling.[259] Voor wat betreft de authenticatiemechanismen werd deze taak in België toevertrouwd aan de FOD BOSA die hieraan uitvoering gaf via de FAS (zie *supra* randnr. 41). Uit het specialiteitsbeginsel vloeit wel voort dat deze delegatie duidelijk moet worden afgebakend, wat via het kb. elektronische identificatie is gebeurd.

---

[254] GwH 14 januari 2021, nr. 02/2021, 68-75; zie over het gebruik van biometrie in de authenticatie ook: Gegevensbeschermingsautoriteit (GBA), advies uit eigen beweging over het verwerken van biometrische gegevens in het raam van authenticatie van personen, 9 april 2008, nr. 17/2008.

[255] RAAD VAN EUROPA, *Handboek Europese gegevensbeschermingswetgeving,* Luxemburg, Bureau voor Publicaties van de Europese Unie, 2021, 140; A. WILLEMS, "De beoordeling van de wetgevende kaders in Europa, China en de Verenigde Staten rond het gebruik van persoonsgegevens ter bestrijding van globale gezondheidscrisissen. Lessen uit de COVID-19-pandemie", *TPR* 2021, afl 4, (1729) 1741.

[256] D. DE BOT, *De toepassing van de algemene verordening gegevensbescherming in de Belgische context Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Mechelen, Wolters Kluwer, 2020, 400-401.

[257] Art 6 lid 1 a), b) en e) AVG.

[258] Art. 6 lid 3 AVG; A. WILLEMS, "De beoordeling van de wetgevende kaders in Europa, China en de Verenigde Staten rond het gebruik van persoonsgegevens ter bestrijding van globale gezondheidscrisissen. Lessen uit de COVID-19-pandemie", *TPR* 2021, afl 4, (1729) 1735.

[259] D. DE BOT, *De toepassing van de algemene verordening gegevensbescherming in de Belgische context Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Mechelen, Wolters Kluwer, 2020, 431-432.

Bijkomstig mag niet worden vergeten dat de toelaatbaarheidsgrond slechts stand houdt in de mate waarin de toegewezen overheid (FOD BOSA) met een taak van algemeen belang werd belast én de verwerkingen noodzakelijk zijn voor de uitvoering van deze taak.

149. Het feit dat een taak van het algemeen belang werd toegewezen aan een publieke rechtspersoon staat er niet aan in de weg dat de taak ook kan worden toegewezen aan private rechtspersonen (zoals Belgian Mobile ID). De overheid gebruikt daarvoor overigens steeds vaker privaatrechtelijke technieken zoals het administratieve contract. Zoals eerder werd besproken maakte ook de FAS gebruik van deze techniek door middel van de onderaannemingsovereenkomst. Ook overheden die gebruik maken van de diensten van de FAS kunnen zich mijn inziens beroepen op de taak van algemeen belang van de fod BOSA om hun verwerkingsactiviteiten in verband met de authenticatie te verantwoorden.

150. Voor andere doeleinden dan deze die in de wet (en het Kb.) staan, zullen de verschillende verwerkers andere toelaatbaarheidsgrondslagen nodig hebben. Daarbij komen voor de aanbieders van authenticatiediensten al snel de uitvoering van het contract en de toestemming die de gebruiker moet geven in beeld.[260] Omdat deze scriptie zich beperkt tot een evaluatie van de bestaande wetgeving wordt hier echter niet verder op ingegaan.

D. Identificatieplicht voor online overheidsdiensten

151. In tegenstelling tot Nederland, waar er sinds kort een duidelijke lijst opgesteld is die bepaalt welke dienstverleners van de overheid verplicht een authenticatietool moeten voorzien en of deze van het betrouwbaarheidsniveau substantieel dan wel hoog moet zijn, bestaat er in België geen gelijkaardige regeling. Overheden zijn dus vrij om zelf te bepalen wanneer er een verplichte identificatie moet plaatsvinden (zie *supra* randnr. 69). Het feit dat overheden zo vrij worden gelaten wat betreft hun identificatiebeleid heeft in de praktijk al enkele keren tot schendingen van enkele belangrijke beginselen van de AVG geleid.

152. Zo wees de gegevensbeschermingsautoriteit (GBA) er in 2019 reeds op dat een verplichte identificatie voor de toegang tot online overheidsdiensten niet altijd en zomaar kan worden opgelegd. Zo moet zij in de eerste plaats om rechtmatig te zijn, voorzien zijn in een rechtsgrond en noodzakelijk zijn voor de uitvoering van een taak van openbaar gezag.[261] Daarnaast moet er ook rekening worden gehouden met de informatieplicht[262] en het toestemmingsprincipe.[263] Dat laatste principe wordt geschonden indien er wordt gekozen toegang tot de dienst afhankelijk te maken van het aanvaarden van de standaardvoorwaarden van een privaat platform van een verwerker, er gebruik wordt gemaakt van nudging ten voordele van de minder privacyvriendelijke optie of indien de privacyvriendelijke opties verborgen worden.[264] Ten slotte mag een overheid die er voor wil kiezen een online identificatieplicht op te leggen niet vergeten te voldoen aan het principe van minimale

[260] Gegevensbeschermingsautoriteit (GBA), *Aanbeveling betreffende de verwerking van biometrische gegevens*, 1 december 2021, nr. 01/2021, 20.
[261] Art. 5 lid 1 a) io. Art. 6 lid 1 e) en lid 3 b) AVG; GBA nr. 02/2019, *Aanbeveling betreffende het opleggen van de verplichte aanmaak van een gebruikersaccount bij Microsoft voor het raadplegen van toepassingen van overheidsdiensten*, 6 februari 2019, 3.
[262] Art. 13 en 14 AVG.
[263] Art. 6 *io*. Art. 7 AVG.
[264] GBA nr. 02/2019, *Aanbeveling betreffende het opleggen van de verplichte aanmaak van een gebruikersaccount bij Microsoft voor het raadplegen van toepassingen van overheidsdiensten*, 6 februari 2019, 4.

gegevensverwerking en de proportionaliteitsvereiste.[265] De GBA bevestigde zijn aanbeveling in latere rechtspraak waarbij het de overheid veroordeelde omdat het de toegang tot fisconetplus -dat een onderdeel is van MyMinFin- afhankelijk stelde van het vrijgeven van persoonsgegevens in de vorm van een Microsoft account.[266]

153. Concreet oordeelt de GBA in bovenstaande aanbeveling en beslissing dat -rekening houdend met bovenstaande principes- het niet voor elke overheidsdienst noodzakelijk is om een identificatieplicht op te leggen. Ze maakt daarbij een onderscheid tussen toepassingen die louter toegang geven tot publieke informatie en toepassingen die toegang geven tot gepersonaliseerde diensten zoals tax-on-web. Enkel in de tweede situatie kan er een noodzaak tot identificatie- en authenticatieplicht ontstaan. De afweging dient door de betrokken overheid steeds gemotiveerd, schriftelijk en in concreto te gebeuren. Kiest de overheid er uiteindelijk voor om toch een identificatie- en authenticatieplicht op te leggen, wordt het aangeraden om gebruik te maken van de authenticatiediensten van de FAS of de diensten die daarin geïntegreerd zijn (zoals Itsme).[267] Systemen zoals Microsoft, Facebook en Google bieden immers niet dezelfde waarborgen wat betreft de bescherming van persoonsgegevens.[268] Om erkend te worden bij de FAS moet er echter voldaan zijn aan de voorwaarden om veiligheidsniveau substantieel of hoog te behalen (zie *supra* randnr. 69). Wanneer niet erkende diensten worden uitgesloten zijn er in België geen alternatieven van veiligheidsniveau laag. Langs de andere kant kan men zich echter ook de vraag stellen of het verstandig is om wanneer het gaat om "gepersonaliseerde diensten", gebruik te maken van authenticatiemechanismen met dergelijke geringe betrouwbaarheid.

154. Ondanks het feit dat de gegevensbeschermingsautoriteit en de AVG voldoende kapstokken lijken aan te reiken om te bepalen welke overheidsdiensten gebruik kunnen maken van verplichte online identificatie en authenticatie, doet de wetgever er waarschijnlijk goed aan om het voorbeeld van Nederland te volgen en lijsten op te stellen van (soorten) overheidsdiensten die aan bovenstaande voorwaarden voldoen. Het is immers niet ondenkbaar dat -zeker voor lokale besturen- het niet steeds duidelijk is waar de grenzen tussen gepersonaliseerde diensten en publieke informatie liggen. Bovendien is onder het huidige systeem het afdwingen van bovenstaande voorwaarden van de gegevensbeschermingsautoriteit geen sinecure. Veel mensen zijn immers niet op de hoogte van deze rechtspraak, hebben onvoldoende kennis of kiezen zonder al te veel nadenken voor de snelle inlogmethode.

E. Identificatie en authenticatie door externe authenticatiediensten

155. Naast het verplichte gebruik van online identificatie, rijzen er ook enkele problemen betreffende het gebruik van externe dienstverleners als authenticatiedienst en de verenigbaarheid met de AVG. Hoewel noch de AVG noch de eIDAS verordening private partners uitsluit als aanbieder van een authenticatiedienst, is de AVG immers ook op hen van toepassing. Over het algemeen

[265] Art. 5 lid 1 c) io. Art. 25 AVG.
[266] GBA geschillenkamer, beslissing ten gronde nr. 82/2020 betreffende klacht wegens het noodzakelijk moeten aanmaken van een Microsoft account voor het downloaden van een document bij de FOD Financiën, 23 december 2020; GBA, *Het afstaan van gegevens kan geen voorwaarde zijn voor toegang tot fiscale informatie,* Persbericht 4 juni 2020.
[267] O. SUSTRONCK, "It's not you, Itsme", *TPP* 2021, nr. 3, (6) 7.
[268] GBA nr. 02/2019, *Aanbeveling betreffende het opleggen van de verplichte aanmaak van een gebruikersaccount bij Microsoft voor het raadplegen van toepassingen van overheidsdiensten*, 6 februari 2019, 5.

kunnen er vragen gesteld worden betreffende de verantwoordelijkheid die deze dienstverleners dragen, hoe zij aan de verplichtingen en de beginselen in de AVG moeten voldoen en welke waarborgen de overheid zal moeten inbouwen met betrekking tot deze dienstverleners.[269] Deze drie thema's worden in wat volgt achtereenvolgens besproken.

a) Verantwoordelijkheid van de externe authenticatiedienst

156. Welke verantwoordelijkheden de verlener van een private authenticatiedienst moet dragen in overeenstemming met de AVG, hangt af van de kwalificatie die deze authenticatiedienst krijgt onder de verordening. De vraag stelt zich dus of de private authenticatiedienst beschouwd moet worden als een verwerker dan wel als een (gezamenlijke) verwerkingsverantwoordelijke. De AVG definieert een verwerker als:

> "*een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt*"[270]

Verwerkingsverantwoordelijke wordt daarentegen gedefinieerd als:

> "*een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen*"[271]

Het Hof van Justitie bepaalde hierover reeds dat de kwalificatie voornamelijk een feitenkwestie is waarbij het begrip verantwoordelijke, ter bescherming van de betrokkene wiens gegevens worden verwerkt, ruim begrepen moet worden en dat er gekeken moet worden naar wie de doelen en de middelen van de verwerking vaststelt.[272] Het is ook mogelijk dat de rol na verloop van tijd omslaat van verwerker naar verwerkingsverantwoordelijke. Dat is over het algemeen het geval "*wanneer keuzes die een hoog risico vormen voor de algemene rechten en vrijheden van de betrokkenen*" worden overgelaten aan de verwerkers zoals bijvoorbeeld het geval is bij een verplichte aanvaarding van de algemene voorwaarden van de authenticatiedienst, de keuze of de verwerker al dan niet datamining en -verrijking kan toepassen op de eigen platformen of het bepalen wanneer de betrokkene moet geïdentificeerd worden. Ten slotte kan er ook sprake zijn van controleverlies wanneer het authenticatiemechanisme van de private partij aangeprezen wordt als het meest gebruiksvriendelijke.[273]

---

[269] O. SUSTRONCK, "It's not you, Itsme", *TPP* 2021, nr. 3, (6) 7.
[270] Art. 4 lid 1 8) AVG.
[271] *Ibid*., art 4 lid 1 7).
[272] Richtsnoer.EDPB nr. 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG, 7 juli 2021, 11; HvJ 13 mei 2014, nr. C-131/12, ECLI:EU:C:2014:317, Google Spain/AEPD, 34; HvJ 5 juni 2018, nr. C-210/16, ECLI:EU:C:2018:388, Wirtschaftsakademie Schleswig-Holstein, 28; HvJ 29 juli 2019, nr. C-40/17, ECLI:EU:C:2019:629, Fashion ID, 80; T. BALTHAZAR en P. RAEMAEKERS, *Gegevensbescherming in de zorg - een praktische gids bij de GDPR*, Brugge, Die Keure, 2018, 33.
[273] GBA nr. 02/2019, *Aanbeveling betreffende het opleggen van de verplichte aanmaak van een gebruikersaccount bij Microsoft voor het raadplegen van toepassingen van overheidsdiensten*, 6 februari 2019, 8.

157. Het spreekt voor zich dat de verantwoordelijkheid over de verwerking van persoonsgegevens niet te lichtzinnig uit handen gegeven mag worden. Bovenstaande elementen moeten dan ook zorgvuldig door de overheid die een identificatieplicht wil opleggen worden afgewogen. Doet zij dit niet, zou dit gepaard kunnen gaan met controleverlies over wat er met de data van zijn burgers zou kunnen gebeuren.[274] Indien er immers niet voldoende waarborgen worden ingebouwd, zouden privébedrijven zoals Facebook en Google de verkregen data immers (door de burger ongewild) kunnen gebruiken voor commerciële doeleinden. In sommige gevallen kan het dus beter zijn om privébedrijven bewust louter de status "verwerker" toe te kennen zodat zij de betrokken gegevens enkel in opdracht van de betrokken overheid mogen verwerken en dus niet voor haar eigen (commerciële) doeleinden.[275] Het spreekt mijn inziens dan ook voor zich dat het gebruik van ongereguleerde private actoren -zoals gebeurde in bovenstaande zaak voor de gegevensbeschermingsautoriteit (zie *supra* randnr. 152)- in de toekomst best vermeden kan worden door overheden te verplichten enkel private diensten erkend door de FAS te gebruiken.

158. Minstens zou er toch steeds duidelijkheid moeten bestaan over wie er verwerkingsverantwoordelijke is en wie louter verwerker zodat ook voor de gebruiker van de authenticatieapplicatie duidelijk is wie er verantwoordelijk is voor de verwerking van zijn gegevens. Hoewel in de eigen privacyverklaring Itsme zichzelf "in overeenstemming met de Belgische privacywetgeving" aanwijst als verwerkingsverantwoordelijke wanneer het gaat om het inloggen bij (overheids)diensten (zie *supra* randnr. 50), kan dit niet rechtstreeks uit de wet of het kb. elektronische identificatie, noch uit de wet bescherming persoonsgegevens en ook niet uit de onderaannemingsovereenkomst tussen de FAS en de aanbieders van de authenticatieservice afgeleid worden.

159. Uit het louter bestaan van de onderaannemingsovereenkomst (zie *supra* randnr. 62) en de -weliswaar beperkte- veiligheidsmechanismen die de wetgever en de uitvoerende macht hebben willen invoeren met oa. het verbod op het gebruik van het unieke identificatienummer voor commercieel gebruik (zie *supra* randnr. 75), zou zelfs integendeel kunnen worden afgeleid dat het de FAS zelf is die beschouwd moet worden als verantwoordelijke van de verwerking.

Ook zonder de onderaannemingsovereenkomst kan met enige zekerheid worden gesteld dat de FOD BOSA als erkennende overheid -minstens deels- beschouwd moet worden als een verwerkingsverantwoordelijke. Dat zij er zelf ook zo over denkt blijkt overigens uit de contractuele gebruikersovereenkomst tussen de FAS en overheden die van diens diensten gebruik willen maken waarin de FOD BOSA wordt aangewezen als verwerkingsverantwoordelijke in de relatie tussen de FAS en de aanbieders van authenticatiediensten.[276] Omdat de ontwikkelaars van authenticatiediensten zoals geïmplementeerd in de FAS zelf echter geen contractuele partij zijn in deze gebruikersovereenkomst, is het nog maar de vraag of aan deze bepaling enige waarde gehecht kan worden.

[274] O. SUSTRONCK, "It's not you, Itsme", *TPP* 2021, nr. 3, (6) 8.
[275] M. GAWRONSKI, *Guide to the GDPR*, Alphen aan den Rijn, Kluwer Law International, 2019, 81.
[276] FOD BOSA, *FAS gebruikersovereenkomst versie 6.7*, 7 februari 2023, https://bosa.belgium.be/sites/default/files/content/documents/DTdocs/FAS/FAS%20Gebruikersovereenkomst.pdf, 6.

160. Daarnaast mag niet uit het oog worden verloren dat de wetgever zelf heeft nagelaten een strikte controle over de gegevens te bewaren en daarbij -ondanks het advies van de CBPL- ervoor heeft gekozen om het gebruiken van persoonsgegevens voor commerciële doeleinden niet expliciet in de wet te verbieden. Het feit dat dit verbod in het koninklijk besluit later wél werd ingevoerd doch enkel voor het unieke identificatienummer lijkt een argument voor het terugwinnen van deze controle niet te kunnen rechtvaardigen.

Verder is het ook zo dat gebruikers van de Itsme diensten de algemene voorwaarden en de privacyverklaring moeten aanvaarden voor ze er gebruik van kunnen maken. Ten slotte moet er wel op gewezen worden dat hoewel Itsme als aanmeldingsoptie voor velen waarschijnlijk als de meest gebruiksvriendelijke optie zal aanvoelen, digitale Vlaamse overheden sinds kort gestopt zijn met nudging richting deze aanbieder als "snelste optie". Tegenwoordig wordt er op het aanmeldportaal van authenticatie Vlaanderen enkel nog verwezen naar de kaartlezer als "veiligste optie" en naar de beveiligingscode via de mobiele app als "gemakkelijkste keuze". Het federaal aanmeldportaal van de CSAM bevat geen nudging.

161. Wat wel als een oplossing voor het vraagstuk over de verwerkingsverantwoordelijkheid zou kunnen gelden is het idee dat zowel de erkennende overheid als de authenticatiedienst als de gebruikers van de FAS beschouwd moeten worden als gezamenlijke verwerkingsverantwoordelijken. Dit begrip wordt in de AVG gedefinieerd als:

> "*Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen*"[277]

Uit de definitie volgt dat twee of meer organisaties het gezamenlijk eens moeten zijn over zowel de doeleinden als de middelen van de verwerking om beschouwd te kunnen worden als gezamenlijke verwerkingsverantwoordelijken. Ook wanneer verwerkers optreden in verschillende fasen van de verwerking kan er sprake zijn van een gezamenlijke verwerkingsverantwoordelijkheid waarbij verschillende verantwoordelijkheden zullen worden toegekend aan de verwerkers afhankelijk van hun rol in een bepaalde fase van het verwerkingsproces.[278] Indien er sprake is van een medeverantwoordelijkheid, moet er in een onderlinge regeling voorzien worden waarin de specifieke verantwoordelijkheden van iedere partij, hun rol en hun verhouding tegenover de burger worden vastgelegd.[279] Uit wat hierboven beschreven staat wordt echter duidelijk dat de verschillende betrokken instanties niet op één lijn staan wat betreft de onderlinge verdeling van verantwoordelijkheden en dat indien er sprake is van gezamenlijke verantwoordelijkheid verdere (wettelijke) afspraken vereist zijn.

162. De term gezamenlijke verwerkingsverantwoordelijke moet overigens ook onderscheiden worden van de -niet in de AVG gedefinieerde- parallelle verantwoordelijkheid die ontstaat wanneer

[277] Art. 26 lid 1 AVG.
[278] HvJ 29 juli 2019, nr. C-40/17, ECLI:EU:C:2019:629, Fashion ID, 100; . P. CRADDOCK, "Arrêt « Fashion ID »: qui est le « responsable du traitement » des données sur un site Internet incorporant un renvoi à un réseau social?", *JTDE* 2019, nr. 10, (404) 406.
[279] Ibid., lid 2; Richtsnoer.EDPB nr. 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG, 7 juli 2021, 21; T. BALTHAZAR en P. RAEMAEKERS, *Gegevensbescherming in de zorg - een praktische gids bij de GDPR*, Brugge, Die Keure, 2018, 37.

twee of meer verantwoordelijken de gegevens van eenzelfde persoon verwerken maar voor eigen vastgestelde doeleinden en middelen en zonder controle over hoe de andere de gegevens gebruikt.[280]

In het licht van wat hierboven reeds werd aangehaald zal er mijn inziens eerder sprake zijn van een gezamenlijke verantwoordelijkheid dan een parallelle. Voor wat betreft gebruikers van de FAS kan hiervoor ondersteuning worden gezocht in de FAS gebruikersovereenkomst waarin de gebruikers aangewezen worden als verwerkingsverantwoordelijke voor wat betreft de verwerking van gegevens in hun online overheidstoepassing. Doch kan hierover in de huidige stand van zaken -en zeker wat betreft de aanbieders van de authenticatiediensten zoals Itsme- geen zekere conclusie aan verbonden worden. De wetgever zou er dan ook goed aan doen om het statuut van private authenticatiemechanismen in een eventuele revisie van de huidige wetgeving uit te klaren.

163. Eén van de verplichtingen die de AVG oplegt aan de verwerkingsverantwoordelijke is het principe van de zogenaamde "Gegevensbescherming door ontwerp en door standaardinstellingen" (privacy by design). Dit principe verplicht de verwerkingsverantwoordelijke om -rekening houdend met de stand van de techniek- te voorzien in passende technische en organisationele maatregelen die de gegevensbeschermingsmechanismen op een doeltreffende wijze moeten waarborgen en dat er voldaan is aan het principe van de minimale gegevensbescherming.[281] Het is daarnaast duidelijk dat zelfs als de erkennende overheid louter beschouwd kan worden als een gezamenlijke verwerkingsverantwoordelijke, zij nog steeds gehouden zal zijn tot het afsluiten van bijkomende protocollen wanneer er elektronische gegevensuitwisselingen plaatsvinden tussen verschillende overheden.[282] Dit is bij authenticatie via het FAS en de overheid die zijn diensten online aanbiedt, altijd het geval. Het valt dan ook te betreuren dat bij het opstellen van het wettelijk kader, de rol en verantwoordelijkheid van de verschillende overheden -in tegenstelling tot het kader in Nederland- niet werd opgenomen.

Ook moet de verwerkingsverantwoordelijke "passende technische en organisationele maatregelen" nemen om de persoonsgegevens te beschermen.[283] De wetgevende of uitvoerende macht kunnen mijn inziens inspiratie halen uit de verplichte certificaten zoals voorgesteld door de Commissie betreffende een nieuwe eIDAS om in ieder geval aanbieders van authenticatiemechanismen te verplichten hun verantwoordelijkheid hierover op te nemen (zie *supra* randnr. 126).

164. Een ander probleem dat het gebrek aan regulering betreffende de verantwoordelijkheid voor de verschillende gegevensverwerkingen creëert ligt vervat in artikel 28 lid 2 van de AVG. Dat artikel bepaalt immers dat verwerkers geen andere verwerkers in dienst mogen nemen zonder voorafgaande toestemming van de verwerkingsverantwoordelijke. Eerder (zie *supra* randnr. 82) werd echter reeds beschreven dat eens een authenticatiedienst wordt erkend binnen de FAS, de online overheidsdiensten deze authenticatiedienst moeten accepteren. Het is nog maar de vraag of

[280] HvJ 5 juni 2018, nr. C-210/16, ECLI:EU:C:2018:388, Wirtschaftsakademie Schleswig-Holstein, 25-44; M. GAWRONSKI, *Guide to the GDPR*, Alphen aan den Rijn, Kluwer Law International, 2019, 38.
[281] Art. 25 AVG; L. VANELVEN, "Les obligations du responsible du traitement" in A. BEELEN en A. JASPAR, *La protection des données pour les institutions publiques*, Limal, Anthemis, 2020, (65) 71.
[282] Art.20 wet verwerking persoonsgegevens; art. 8 decreet 18 juli 2018 betreffende het elektronisch bestuurlijk gegevensverkeer, *BS* 29 oktober 2008 (e-gov decreet); VLAAMSE TOEZICHTCOMMISSIE VOOR DE VERWERKING VAN PERSOONSGEGEVENS, advies wetgeving VTC betreffende het voorontwerp van decreet samenwerkingsakkoord vaccinaties COVID-19, februari 2021, nr. 2021/13, 7, 11.
[283] Art. 32 lid 1 AVG; ARTIKEL 29 WERKGROEP, *Advies over de recente ontwikkelingen op het gebied van het internet van de dingen*, 16 september 2014, nr. 8/2014, 20.

dat wanneer een online overheidsdienst moet gezien worden als een (gezamenlijke) verwerkingsverantwoordelijke, deze verplichting niet ingaat tegen het vermelde verbod van de AVG.[284]

b) Beginselen en verplichtingen

Algemeen

165. Elke overheidsdienst waarbij er persoonsgegevens worden verwerkt -wat bij een online identificatieplicht per definitie het geval zal zijn- moet voldoen aan de beginselen en verplichtingen zoals vervat in de AVG (zie *supra* randnr. 74). Zoals hierboven reeds beschreven zullen overheden vooral rekening moeten houden met de beginselen van proportionaliteit en minimale gegevensverwerking in de beslissing of er al dan niet een identificatieplicht moet worden ingesteld.

166. Naast de overheden die een verplichting tot identificatie opleggen en de erkennende overheid als mogelijke verwerkingsverantwoordelijken, moet uiteraard ook de (private) aanbieder van de authenticatiedienst zich houden aan de beginselen van de AVG. Zoals reeds eerder gezegd gaat deze scriptie niet in op alle verplichtingen die gelden voor verwerkers en verantwoordelijken. Beginselen zoals bijvoorbeeld het recht van inzage en rectificatie zijn immers direct van toepassing op de verwerkers van gegevens, zijn voldoende duidelijk en maken geen deel uit van de hier te evalueren Belgische wetgeving. Wél belangrijk om te signaleren is de situatie die ontstaat wanneer deze bedrijven niet kunnen garanderen dat de beginselen van de AVG effectief worden gevolgd.[285] Dat kan met name het geval zijn wanneer de private authenticatieservice is buitenlandse handen is en gegevens worden doorgegeven aan derde landen.[286]

167. Ten slotte moet ook de regulerende overheid zelf bij het aanmaken van wetgeving rekening houden met de gevolgen van (het gebrek aan) die wetgeving op het vlak van de bescherming tegen de verwerking van persoonsgegevens. De beste manier om dit te doen is door middel van één of meerdere gegevensbeschermingseffectenbeoordelingen.[287].

Doorgeven van gegevens

168. Van doorgifte van gegevens is sprake wanneer er voldaan is aan drie cumulatieve criteria: Vooreerst moet de onderneming die de gegevens doorgeeft onder het territoriaal toepassingsgebied van de AVG vallen (zie *supra* randnr. 143). Daarnaast moet het deze onderneming zijn die de persoonsgegevens doorgeeft, en dus niet bijvoorbeeld de persoon om wiens gegevens het gaat zelf. Ten slotte moet de ontvangende onderneming gevestigd zijn in een derde land, ongeacht of deze onderneming al dan niet binnen het territoriaal toepassingsgebied van de AVG valt.[288] Van een doorgifte van gegevens zal ook sprake zijn wanneer de opslag van persoonsgegevens gebeurt op

[284] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (CBPL), advies betreffende ontwerp van koninklijk besluit tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van diensten voor elektronische identificatie voor digitale overheidstoepassingen (CO-A-2017-008), 12 april 2017, nr. 18/2017, 3.
[285] O. SUSTRONCK, "It's not you, Itsme", *TPP* 2021, nr. 3, (6) 8-9.
[286] M. GAWRONSKI, *Guide to the GDPR*, Alphen aan den Rijn, Kluwer Law International, 2019, 99.
[287] Art. 35 lid 1 *io.* Overwegingen 90 en 91 AVG; ARTIKEL 29 WERKGROEP GEGEVENSBESCHERMING, *Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679*, 4 april 2017, 9.
[288] EUROPEES COMITE VOOR GEGEVENSBESCHERMING (EDPB) nr. 05/2021, Guidelines on the interplay between the application of article 3 and the provisions on international transfers as per chapter V of the GDPR 2.0, 14 februari 2023, 7.

een externe serveropslag of cloudtoepassing als die beheerd wordt door een andere onderneming.[289] Het louter posten van persoonsgegevens op het internet is dit niet.[290]

Concreet zal er in het geval van authenticatiemechanismen sprake zijn van een doorgifte van gegevens wanneer het bedrijf van de authenticatiedienstverlener in handen komt van een bedrijf gevestigd in een derde land of het de persoonsgegevens (tijdelijk) opslaat op een cloud of server beheerd door een onderneming uit een derde land.

169. Terzake bouwt de AVG enkele veiligheidswaarborgen in. Zo mogen persoonsgegevens niet buiten de EU (en Noorwegen, Ijsland en Liechtenstein als landen waar het vrij verkeer van persoonsgegevens geldt) worden overgedragen tenzij in dat land eenzelfde graad van bescherming geldt als dat van de AVG.[291] De AVG voorziet zelf de gronden waarop een dergelijke veilige doorgifte mogelijk is. Zo kan een doorgifte naar een derde land plaatsvinden wanneer de Commissie hierover na onderzoek aan de hand van een aantal factoren,[292] zoals de rechtsstatelijkheid van een land en de al dan niet aanwezigheid van effectieve controleorganen, een adequaatheidsbesluit neemt.[293] Een tweede grond waaronder het doorgeven van persoonsgegevens naar derde landen mogelijk zou zijn, is wanneer er "passende waarborgen" worden genomen en de betrokkenen over afdwingbare rechten en afdoende rechtsmiddelen beschikken.[294] Praktisch kan dat onder andere geregeld worden door middel van bilaterale verdragen, bindende bedrijfsvoorschriften en contractclausules die werden vastgesteld door een toezichthoudend orgaan of de commissie.[295] Dat laatste gebeurde voor de Commissie overigens bij een uitvoeringsbesluit.[296]

170. Hoewel er dus zeker manieren zijn om een samenwerking met een authenticatiedienst die in handen is van een bedrijf uit een derde land -een risico dat met private bedrijven die kunnen worden overgenomen niet kan worden uitgesloten-, zijn er toch nog steeds enkele gevaren. Zo oordeelde het Hof van Justitie in de zaak Schrems II dat hoewel het (vorige) uitvoeringsbesluit van de Europese Commissie wel degelijk geldig is, de modelclausules door hun contractuele aard niet bindend zijn voor de autoriteiten van een derde land.[297] Daardoor kunnen deze bedrijven niet garanderen dat nationale overheden zich geen toegang verschaffen tot de verwerkte persoonsgegevens op grond

[289] EDPB nr. 01/2020, Aanbevelingen inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen versie 2.0, 18 juni 2021, nr. 01/2020, 12.
[290] HvJ 6 november 2003, nr. C-101/01, ECLI:EU:C:2003:596, Lindqvist/Zweden, 68-69; RAAD VAN EUROPA, *Handboek Europese gegevensbeschermingswetgeving,* Luxemburg, Bureau voor Publicaties van de Europese Unie, 2021, 300.
[291] Art. 44 AVG; M. GAWRONSKI, *Guide to the GDPR*, Alphen aan den Rijn, Kluwer Law International, 2019, 99.
[292] Art 45 lid 2 AVG.
[293] Ibid., lid 1 en lid 3; HvJ 16 juli 2020, nr. C-311/18, ECLI:EU:C:2020:559, Schrems II; RAAD VAN EUROPA, *Handboek Europese gegevensbeschermingswetgeving,* Luxemburg, Bureau voor Publicaties van de Europese Unie, 2021, 301; A. WILLEMS, "De beoordeling van de wetgevende kaders in Europa, China en de Verenigde Staten rond het gebruik van persoonsgegevens ter bestrijding van globale gezondheidscrisissen. Lessen uit de COVID-19-pandemie", *TPR* 2021, afl 4, (1729) 1744.
[294] RAAD VAN EUROPA, *Handboek Europese gegevensbeschermingswetgeving,* Luxemburg, Bureau voor Publicaties van de Europese Unie, 2021, 306; A. WILLEMS, "De beoordeling van de wetgevende kaders in Europa, China en de Verenigde Staten rond het gebruik van persoonsgegevens ter bestrijding van globale gezondheidscrisissen. Lessen uit de COVID-19-pandemie", *TPR* 2021, afl 4, (1729) 1745.
[295] Ibid., art 46 lid 1-3; S. DEPREZ, *Gegevensbescherming*, Hoegaarden, LeA uitgevers, 2022, 164; M. GAWRONSKI, *Guide to the GDPR*, Alphen aan den Rijn, Kluwer Law International, 2019,
[296] Uitvoeringsbesluit.Comm. nr. 2021/914, 4 juni 2021 betreffende standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad (Voor de EER relevante tekst), *Pb.L* 7 juni 2021, afl 199, 31.
[297] HvJ 16 juli 2020, ECLI:EU:C:2020:559, nr. C-311/18, Schrems II, 125

van de nationaal geldende rechtsregels.[298] Dat was ook de reden waarom in de zaak Schrems II, het Hof van Justitie de standaardclausules van de Commissie weliswaar goedkeurde maar met dien verstande dat wanneer de waarborgen van de AVG niet kunnen worden nageleefd, de exporteur van de gegevens het doorsturen van gegevens moet opschorten of beëindigen.[299]

Over het adequaatheidsbesluit van de Europese Commissie over de Verenigde Staten (het zogenaamde "Privacy shield[300]") dat terzake ook in vraag werd gesteld oordeelde het Hof dat hoewel wél bindend voor de nationale autoriteiten, het privacy shield meer toegang tot en gebruik van de persoonsgegevens toeliet voor deze autoriteiten dan strikt noodzakelijk was.[301]

171. Vooral voor mogelijke aanbieders van authenticatiediensten uit landen waar geen adequaatheidsbesluit geldt (waar de Verenigde Staten er dus één van is, evenals china, Zuid Korea, Japan…),[302] leert de zaak Schrems dat zelfs via de methode van standaardclausules er nog steeds inherente risico's verbonden zijn aan een samenwerking met private aanbieders. Zo zou in principe het recht van het bestemmingsland steeds grondig geanalyseerd moeten worden om na te gaan of er voldoende waarborgen betreffende de bescherming van persoonsgegevens kunnen gegeven worden.[303] Dit gebeurt liefst door een externe audit en er zal rekening moeten gehouden worden met een exitstrategie voor wanneer de zaken toch dreigen mis te lopen zoals bijvoorbeeld bij een faillissement.[304] Is dat niet het geval, zullen er aanvullende maatregelen genomen moeten worden door bijvoorbeeld de gegevens zodanig te versleutelen dat zij onbereikbaar zijn voor de overheidsinstanties van dat derde land.[305] Of private bedrijven voldoende gemotiveerd en capabel zullen zijn om grootmachten zoals Amerika voor te blijven op vlak van versleutelingstechnologieën lijkt nog maar de vraag. In dat opzicht is een (deels) staatsgecontroleerde authenticatiedienst die niet of moeilijker in buitenlandse handen kan komen wel meer bestendig voor eventuele problemen wat betreft het kunnen garanderen dat de beginselen van de AVG worden gevolgd. Minstens is het een goed idee om burgers enkele verschillende authenticatiemogelijkheden aan te bieden zodat zij snel kunnen schakelen wanneer ze het gevoel krijgen dat de bescherming van hun persoonsgegevens in het gedrang komt.

---

[298] O. SUSTRONCK, "It's not you, Itsme", *TPP* 2021, nr. 3, (6) 9

[299] HvJ 16 juli 2020, nr. C-311/18, ECLI:EU:C:2020:559, Schrems II, 136-137; M. BEUDELS, "Schrems II: volgend hoofdstuk in het verhaal van de internationale gegevensdoorgiften", *TPP* 2021, nr. 1, (18) 22.

[300] Uitvoeringsverordening.Comm. nr. 2016/1250, 12 juli 2016 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de gepastheid van de door het EU-VS-privacyschild geboden bescherming.

[301] HvJ 16 juli 2020, nr. C-311/18, ECLI:EU:C:2020:559, Schrems II, 176-184.

[302] Momenteel is er een adequaatheidsbesluit voor Andorra, Argentinië, Australië, Guersney, Israel, Canada, Nieuw Zeeland, Zwitserland, het eiland man en de Faeröer eilanden.

[303] M. BEUDELS, "Schrems II: volgend hoofdstuk in het verhaal van de internationale gegevensdoorgiften", *TPP* 2021, nr. 1, (18) 25; J. CLEMENS, "De Raad van State opent de deur voor doorgiften van persoonsgegevens naar de Verenigde Staten na Schrems II", *TPP* 2022, nr. 1, (24) 28; W. DEBEUCKELAERE, "En wat nu (weer) gedaan? Verbazing en verwarring na Schrems II", *TPP* 2020, nr. 4, 38.

[304] VLAAMSE TOEZICHTCOMMISSIE VOOR DE VERWERKING VAN PERSOONSGEGEVENS (VTC), advies betreffende informatieveiligheid en GDPR-conformiteit 4 platformen onderwijs – Amazon Web Services, 8 september 2020, nr. 2020/05, 7.

[305] RvS 12 mei 2021, nr. 250.599, 18; EUROPEES COMITE VOOR GEGEVENSBESCHERMING, Aanbeveling over de Europese essentiële garanties voor surveillancemaatregelen, 10 november 2020, nr. 02/2020;EPDB, Aanbevelingen inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen versie 2.0, 18 juni 2021, nr. 01/2020, 33.

Beginsel van minimale gegevensverwerking en proportionaliteit

172. Het beginsel van minimale gegevensverwerking houdt in dat persoonsgegevens "toereikend, ter zake dienend en beperkt moeten zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt".[306] Hoewel de benaming en de definitie van het beginsel doet vermoeden dat de persoonsgegevens moeten worden beperkt tot het minimum dat nodig is voor de verwerkingsdoeleinden, wordt in de overwegingen van het voorstel van de verordening verduidelijkt dat er slechts voor gezorgd moet worden dat de verzamelde gegevens niet "excessief" zijn en dat de opslagtermijn tot een minimum moet worden beperkt.[307] Dat laatste wordt overigens nog eens bevestigd in overweging 39 van de uiteindelijke verordening dat bevestigt dat bewaartermijnen vervat zitten in het beginsel van minimale gegevensverwerking en proportionaliteit.[308]

173. Zoals eerder in deze scriptie besproken (zie supra randnr. 74) werd in België de bewaringstermijn vastgelegd in het Kb. elektronische identificatie. De uitvoerende macht nam dus zelf de verantwoordelijkheid op om de bewaringstermijn te bepalen. Omdat de bewaring zelf beschouwd kan worden als een verwerking van persoonsgegevens en dus proportioneel moet zijn, mogen deze gegevens volgens het beginsel van minimale gegevensverwerking niet langer worden bewaard wanneer daar geen reden meer toe is. Men kan zich dan ook de vraag stellen of de bewaringstermijn zoals zij in België is verankerd in overeenstemming is met het beginsel van minimale gegevensverwerking.

174. Het eerste dat opvalt is dat het Kb. spreekt over het "moeten" bewaren van de gegevens gedurende een periode van tien jaar vanaf het moment van de poging tot aanmelding. Op deze manier wordt aan de aanbieders van authenticatiemechanismen louter een minimumbewaringstermijn opgelegd die het mogelijk moet maken een controlespoor te reconstrueren dat optreden tegen eventuele misbruiken makkelijker maakt. Hoewel de uitvoerende macht zeker goede bedoelingen had met de invoering van deze bepaling, maakt Itsme van dit feit gretig gebruik door veel gegevens langer dan door de wet vereist te bewaren en de termijn pas in te laten gaan vanaf het moment van het stopzetten van het gebruik van de app of de gegevens pas te verwijderen na een inactiviteit van twaalf jaar.

175. Het uitgangspunt om de bewaartermijn te bepalen is nochtans eenvoudig: gegevens zullen zo lang moeten worden bewaard als de rechtsvorderingen waarvoor ze relevant kunnen zijn, niet zijn verjaard.[309] Dat zal in het geval van authenticatie en eventueel misbruik van deze systemen de termijn voor het ontvankelijk kunnen instellen van een rechtsvordering zijn. De termijn die daarvoor geldt in België is tien jaar vanaf het moment van het ontstaan van de burgerrechtelijke vordering

[306] Art 5 lid 1 c) AVG; Gegevenbeschermingsautoriteit (GBA), advies over een ontwerpbesluit van de Regering van de Franse Gemeenschap tot het bepalen van de categorieën van persoonsgegevens die worden verwerkt met betrekking tot de doeleinden van de digitale ruimten in toepassing van de artikelen 6 en 11 van het decreet van 25 april 2019 betreffende het digitaal bestuur van het schoolsysteem en de overdracht van digitale gegevens in het leerplichtonderwijs, 5 november 2020, nr. 108/2020, 7; P. CORNETTE, "Autres impactes du RGPDsur l'IT" in A. BEELEN en A. JASPAR, *La protection des données pour les institutions publiques*, Limal, Anthemis, 2020, (189) 196; RAAD VAN EUROPA, *Handboek Europese gegevensbeschermingswetgeving,* Luxemburg, Bureau voor Publicaties van de Europese Unie, 2021, 149.
[307] Overweging 30 voorstel AVG.
[308] D. DE BOT, *De toepassing van de algemene verordening gegevensbescherming in de Belgische context Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Mechelen, Wolters Kluwer, 2020, 494.
[309] Ibid., 495.

die hier gelijk zal lopen met het moment van de poging tot misbruik.[310] Er lijkt dan ook geen reden te bestaan waarom de aanbieders van authenticatiesystemen de gegevens langer dan deze termijn zouden moeten bewaren. De wetgever (of bevoegde minister) zou er mijn inziens dan ook goed aan doen om een maximumbewaringstermijn van tien jaar op te leggen.

Op strafrechtelijk vlak wordt een algemene en ongedifferentieerde bewaarplicht voor identiteitsgegevens ter bestrijding van criminaliteit overigens toegestaan door het Hof van Justitie omdat een bewaring van deze gegevens geen ernstige inbreuk op het privéleven van de betrokkenen zou uitmaken.[311] Problematischer zou het zijn geweest wanneer er ook zo'n bewaarplicht voor verkeers- en locatiegegevens zou bestaan. Zo'n algemene en ongedifferentieerde bewaarplicht zou immers enkel mogelijk zijn voor een beperkte periode en wanneer er voldoende aanwijzingen zijn voor een actuele of waarschijnlijke bedreiging van de nationale veiligheid.[312]

176. Eerder werd ook reeds besproken dat authenticatiediensten in België meer gegevens lijken te bewaren dan strikt noodzakelijk zou zijn voor het kunnen aanbieden van hun diensten. Hoewel dit in het licht van de betekenis van het beginsel van minimale gegevensverwerking zoals blijkt uit de voorbereidende documenten niet per se een schending van de verordening hoeft te zijn, doet de wetgever er mijn inziens toch goed aan om wanneer er op dergelijk grote schaal gegevens worden verwerkt ook hier wetgevend in te grijpen en uit te werken welke soorten gegevens mogen of moeten worden bewaard en welke niet.

177. Een maatregel die -hoewel zo niet benoemd of gemotiveerd- wel degelijk het beginsel implementeert is de bepaling die stelt dat in België (net zoals in Nederland) authenticatiediensten niet mogen verwerken op welke overheidsdiensten beroep wordt gedaan (zie *supra* randnr. 74). In Nederland bestaat daarnaast de verplichting tot het verwijderen van de gelaatsfoto en BSN nummer na registratie (zie *supra* randnr. 93), een maatregel die mijn inziens ook in België makkelijk geïmplementeerd zou kunnen worden.

178. Op Europees niveau werd eerder al aangehaald dat de invoering van flexibele digitale identiteiten, die het mogelijk maken enkel die identiteitsattributen door te sturen die noodzakelijk zijn voor de gewenste overheidsdienst een stap voorwaarts zou zijn in de implementatie van het beginsel van minimale gegevensverwerking (zie *supra* randnr. 125).

179. Ten slotte werd er in deze scriptie ook reeds meerdere malen voor gepleit om lijsten op te stellen van overheden die verplicht gebruik zouden moeten maken van de erkende overheidsdiensten. Zoals ook reeds eerder werd aangehaald mag dit er in het licht van het beginsel van minimale gegevensverwerking echter niet toe leiden dat overheidsdiensten die louter informatie verschaffen verplichte authenticatie gaan opleggen aan de burger.

[310] Art. 2262 bis §1 lid 1 oud BW.
[311] HvJ 6 oktober 2020, C-511/18, C512/18 en C-520/18, ECLI:EU:C:2020:791, La Quadrature du Net, 157.
[312] C. DE TERWANGNE, "L'illégalité nuancée de la surveillance numérique : la réponse des juridictions belge et française à l'arrêt La Quadrature du Net de la Cour de justice de l'Union européenne", *RTDH* 2022, nr. 129, (3) 5; L. KEUNEN, "De vernietiging van de Dataretentiewet 2.0: naar een gerichte bewaring met ruime toegang?",(noot onder HvJ 6 oktober 2020, C-511/18, C512/18 en C-520/18, La Quadrature du Net) *RW* 2021-2022, nr 37, (5) 7.

c) Waarborgen en controle

180. Uit het integriteits- en vertrouwelijkheidsbeginsel van de AVG volgt ten slotte dat de erkennende overheid (FAS) of de overheid die gebruikt maakt van andere authenticatiesystemen dan diegenen die door de FAS werden erkend, als verwerkingsverantwoordelijken erop moeten toezien dat er passende technische en organisatorische maatregelen worden getroffen om de veiligheid van de verwerkte gegevens te garanderen.[313] Daaronder wordt in de eerste plaats verstaan dat zij erop moeten toezien dat de beginselen en veiligheidsmaatregelen van de AVG correct worden geïmplementeerd en nageleefd. Met betrekking tot private dienstverleners bestaat er daarnaast echter ook een bijkomend risico dat deze dienstverleners zouden kunnen overgaan tot het verzamelen van persoonsgegevens, dataverrijking en datamining.[314]

Omdat het daarnaast bij authenticatie over het uitwisselen van gegevens op grote schaal gaat en er -toch wat betreft beveiliging van deze gegevens- steeds nieuwe technologieën worden gebruikt, zijn de overheden ook gehouden tot een gegevensbeschermingseffectenbeoordeling.[315] Een diepgaande privacy impact analyse wordt overigens door de Nederlandse Autoriteit Persoonsgegevens ook aanbevolen wanneer bepaalde applicaties (zoals Itsme) door meerdere overheden op grote schaal worden gebruikt.[316] Indien de federale overheid zijn plannen tot het oprichten van een eigen, in de digitale portefeuille geïntegreerde, authenticatiemechanisme doorzet, zal een nieuwe gegevensbeschermingseffectenbeoordeling moeten plaatsvinden.

181. Nog volgens de AVG, is het aan de lidstaten zelf om te voorzien in onafhankelijke overheidsinstanties die instaan voor het toezicht op de toepassing van de verplichtingen in de AVG.[317] Dat toezicht gebeurt in België op federaal niveau door de gegevensbeschermingsautoriteit (GBA) dat bevoegd is voor het toezicht op de naleving van de beginselen van de verwerking van persoonsgegevens wat naast de toepassing van de AVG ook andere beschermingswetten inhoudt zoals bijvoorbeeld de camerawetgeving.[318] De GBA is bevoegd voor zowel instanties uit de publieke als de private sector.[319] Voor verwerkingsactiviteiten die werden aangenomen op het Vlaamse niveau is de Vlaamse Toezichtcommissie (VTC) bevoegd weliswaar met dien verstande dat de bevoegdheid zich enkel uitstrekt tot de Vlaamse overheden en dus niet de private sector waar de GBA voor

[313] Art. 5 lid 1 f) *io.* Art. 24 lid 1 en art. 32 AVG.
[314] GBA nr. 02/2019, *Aanbeveling betreffende het opleggen van de verplichte aanmaak van een gebruikersaccount bij Microsoft voor het raadplegen van toepassingen van overheidsdiensten*, 6 februari 2019, 7; O. SUSTRONCK, "It's not you, Itsme", *TPP* 2021, nr. 3, (6) 9.
[315] Art. 35 lid 1 AVG; ARTIKEL 29 WERKGROEP GEGEVENSBESCHERMING, *Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679*, 4 april 2017, 9.
[316] AUTORITEIT PERSOONSGEGEVENS, advies nr. z2021-08230 Google G suite for education, 8 juni 2021.
[317] Art. 51 lid 1 AVG; RAAD VAN EUROPA, *Handboek Europese gegevensbeschermingswetgeving,* Luxemburg, Bureau voor Publicaties van de Europese Unie, 2021, 226.
[318] Art 4 lid 1 wet tot oprichting gegevensbeschermingsautoriteit, *BS* 10 januari 2018; E. KINDT en D. STEVENS, "Recente ontwikkelingen in het gegevensbeschermingsrecht" in C. CONINGS, S. GRANATA, M.-C. JANSSENS, E. KINDT, S. ROVER, D. STEVENS, J. VANHERPE en G. VAN OVERWALLE, *Themis 2022-2023 nr. 125 IP- en ICT-recht*, Antwerpen, Intersentia, 2023, (155) 160.
[319] E. KINDT en D. STEVENS, "Recente ontwikkelingen in het gegevensbeschermingsrecht" in C. CONINGS, S. GRANATA, M.-C. JANSSENS, E. KINDT, S. ROVER, D. STEVENS, J. VANHERPE en G. VAN OVERWALLE, *Themis 2022-2023 nr. 125 IP- en ICT-recht*, Antwerpen, Intersentia, 2023, (155) 164.

bevoegd blijft.[320] Daarnaast is het ook zo dat de GBA naast de VTC bevoegd blijft voor de Vlaamse overheden.[321] Voor beide organen wordt die onafhankelijkheid wettelijk vastgesteld.[322]

182. Ondanks de bevoegdheid van de GBA, werd eerder reeds vastgesteld dat in de eerste plaats de FOD BOSA bevoegd is om het naleven van de erkenningsvoorwaarden -die vaak verband houden met de beginselen ter bescherming van de persoonsgegevens maar er niet volledig mee samenvallen- door de authenticatiedienstverleners te controleren en eventueel te bestraffen (zie *supra* randnr. 85). Toch zal ook de GBA bevoegd zijn om deze dienstverleners te controleren op het naleven van de wetgeving rond gegevensbescherming.[323] Bij overtredingen kunnen er sancties opgelegd worden zoals verplicht door de AVG.[324] Deze sancties kunnen gaan van waarschuwingen en verplichtingen tot het stopzetten van de verboden activiteit tot het opleggen van administratieve geldboeten die kunnen oplopen tot 20 miljoen euro of 4% van de omzet van het bedrijf.[325]

183. Moeilijker wordt het echter wanneer het gaat om controle op de overheden die gebruik willen maken van de authenticatiemechanismen en op de FOD BOSA zelf. Weliswaar zullen zowel de GBA als de VTC onderzoek kunnen uitvoeren naar en bindende adviezen of waarschuwingen kunnen uitbrengen over de samenwerking van overheden met authenticatiedienstverleners. Toch zijn zij in hun controlerende bevoegdheid tegenover de overheid meer beperkt dan tegenover private partijen. Zo kan de GBA tegenover overheden slechts een administratieve boete opleggen wegens overtredingen van de beginselen ter bescherming van persoonsgegevens als die overheid goederen of diensten aanbiedt op een markt.[326] De bevoegdheid van de VTC is zo mogelijk nog beperkter daar zij geen enkele boetebevoegdheid hebben.[327] Het beperken van de mogelijkheid om aan overheden een geldboete op te leggen is overigens volledig in overeenstemming met de bepalingen van de AVG.[328]

184. Concreet komt het er mijn inziens dan ook op neer dat overheden die gebruik maken van aanbieders authenticatiemechanismen weliswaar gecontroleerd maar niet beboet zullen kunnen worden over de manier waarop zij dat doen. Dat wil ook zeggen dat, zolang er geen verplichting tot het louter gebruik van authenticatiemechanismen erkend door de FOD BOSA wordt ingevoerd, overheden niet geldelijk kunnen bestraft worden voor het gebruik van (buitenlandse) mechanismen die niet voldoen aan de standaarden van de AVG. Controle met administratieve geldboeten op de FAS zelf zullen daarnaast wel mogelijk zijn daar de FAS aanbieder is van de authenticatieservice die

[320] Art. 10/1 §1 lid 1 decreet betreffende het elektronische bestuurlijke gegevensverkeer, *BS* 29 oktober 2008; D. DE BOT, *De toepassing van de algemene verordening gegevensbescherming in de Belgische context Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Mechelen, Wolters Kluwer, 2020, 980; S. DEPREZ, *Gegevensbescherming*, Hoegaarden, LeA uitgevers, 2022, 272.
[321] Wetsontwerp tot oprichting van de Gegevensbeschermingsautoriteit, *Parl.St*. Kamer 2016/17, nr. 2648/001, 7; Brussel (Marktenhof) 26 oktober 2022, Computerr. 2023/40.
[322] Art. 43 en 44 wet tot oprichting gegevensbeschermingsautoriteit, Art. 10/1 §1 lid 2 en art. 10/2 §2 decreet betreffende het elektronische bestuurlijke gegevensverkeer.
[323] Cour adm. Luxembourg 12 juli 2005, *DAOR* 2006/79, (289) 306; C-E. CLESSE en M. VERWILGHEN, "Les sanctions de la violation de la vie privée" in S. GILSON en P. NILLES, *Technologies, surveillance et vie privée du travailleur*, 371; D. DE BOT, *De toepassing van de algemene verordening gegevensbescherming in de Belgische context*, Mechelen, Wolters Kluwer, 2020, 20; I. VERHELST, W. VAN LOON, en S. CONIX, "gegevensbescherming in de HR-praktijk: een stand van zaken na één jaar GDPR", *Or.* 2019, nr. 5, p. 164.
[324] Art. 58 lid 2 AVG.
[325] Art. 83 lid 5 AVG; Art. 100 §1 wet tot oprichting gegevensbeschermingsautoriteit; M. KRZYSZTOFEK, *GDPR, Personal data protection in the European Union*, Alphen aan den Rijn, Kluwer, 2021, 32.
[326] Art. 221 §2 wet 30 juli 2018 tot bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.
[327] O. SUSTRONCK, "It's not you, Itsme", *TPP* 2021, nr. 3, (6) 9.
[328] Art. 83 lid 7 AVG.

kan worden gebruikt door de federale en Vlaamse overheden. Geldboeten zijn natuurlijk niet zaligmakend maar ze kunnen toch een nuttige stok achter de deur blijven bij herhaalde inbreuken tegen de bescherming van de persoonsgegevens. Helaas werd er bewust voor gekozen deze sanctiemaatregelen zo min mogelijk te gebruiken tegen overheidsdiensten zelf.

Eerder werd reeds gewezen op de verschillende aanpak van Nederland inzake de controle van overheden in de authenticatieketen en de grotere politieke en bestuurlijke verantwoordelijkheid die daar zou gelden bij grootschalige datalekken. Deze aanpak zou de afwezigheid van sanctiemaatregelen voor nalatige overheden in België gedeeltelijk kunnen opvangen.

185. Met bovenstaande in het achterhoofd wordt het dan ook interessant te volgen wat de wetgever zal doen met de controleproblematiek eens zij zelf een nieuwe volledig publiek georganiseerde authenticatiedienst als deel van de digitale portefeuille naar buiten zal brengen. Te verwachten valt dat ook deze authenticatiedienst als onderdeel van de FAS vooreerst onder het toeziend oog van de FOD BOSA als erkennende overheid zal vallen. Het zal dan nog maar de vraag zijn in hoeverre de FOD dan geneigd zal zijn om streng toe te zien op het nakomen van de erkenningsvoorwaarden die ook gelden voor private aanbieders. Zeker wanneer in rekening wordt genomen dat de wetgever via artikel 23 van de AVG over een zeer uitgebreide mogelijkheid beschikt om de rechten en verplichtingen zoals zij in de AVG worden beschermd te beperken.

Die beperkingen moeten dan wel in een Unierechtelijke of nationale bepaling worden voorzien en moet de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laten. Bovendien moet de beperking noodzakelijk en proportioneel zijn ter waarborging van één van de in artikel 23 AVG limitatief opgesomde doelen waaronder -naast de klassiekers waar nu al gebruik van wordt gemaakt zoals het onderzoek en de vervolging van strafbare feiten[329]- vooral de grondslag "*andere belangrijke doelstellingen van algemeen belang van de Unie of van een lidstaat, met name een belangrijk economisch of financieel belang van de Unie of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid*"[330] voldoende ruim lijkt om de bepalingen van de AVG die bescherming moeten bieden voor wat betreft verwerkingen in de digitale portefeuille verder te beperken.

186. Moest de wetgever in de mogelijkheid voorzien dat de authenticatiedienst van de digitale portefeuille via deze bepaling aan bijvoorbeeld de informatieverplichtingen kan ontsnappen (zoals dat in andere dossiers ook veelvuldig gebeurt)[331], zou dit meteen ook een bijkomende hindernis vormen voor een effectief toezicht door de gegevensbeschermingsautoriteit.

[329] Art 23 lid 1 d)
[330] *Ibid.,* e).
[331] F. SCHRAM, "Datamining en fraudebestrijding via gegevensuitwisseling en de juridische gevolgen van onrechtmatige elektronische uitwisseling van informatie tussen verschillende overheidsadministraties", in M. DELANOTTE, B. PEETERS en I. VAN DE WOESTEYNE (eds.), *Digitalisering. Postuniversitaire cyclus Willy Delva*, Mechelen, Wolters Kluwer, 2021, 241.

F. Conclusie

187. In dit laatste hoofdstuk werd getracht een antwoord te formuleren op sub-onderzoeksvragen 3) en 4). Er werd ingegaan op het toepassingsgebied van de Algemene Verordening Gegevensbescherming en geconcludeerd dat zowel de Belgische wetgever als de aanbieders van authenticatiediensten als de overheden die gebruik willen maken van deze authenticatiediensten rekening dienen te houden met de beginselen en verplichtingen van deze verordening. Omdat deze scriptie zich beperkt tot een evaluatie van het Belgisch wettelijk kader werd niet op alle beginselen ingegaan, doch enkel op diegene waar mogelijks een (aangepast) optreden van de wetgevende of uitvoerende macht in België is vereist.

188. de toelaatbaarheid van de verwerking voor de actoren in de authenticatiesystemen werd voorzien in de wet en het kb. elektronische identificatie in combinatie met de privaatrechtelijke onderaannemingsovereenkomst voor private ontwikkelaars van authenticatiesystemen (zie *supra* randnr 149) ter uitvoering van een taak van het algemeen belang (zie *supra* randnr. 148).

189. Toch werd vastgesteld dat het gebruik van authenticatiediensten door overheden die online diensten aanbieden niet onbeperkt kan worden toegestaan. Zo oordeelde de GBA dat enkel overheidstoepassingen die gepersonaliseerde diensten aanbieden de aanwezigheid van een voorafgaande authenticatie kunnen verantwoorden. Voor andere overheidsdiensten zou dit een schending uitmaken van het principe van minimale gegevensverwerking. In de loop van deze scriptie werd er reeds meerdere malen voor gepleit dat de Belgische wetgevende of uitvoerende macht lijsten van overheidsdiensten die verplicht gebruik zouden moeten maken van een authenticatiemechanisme. Een extra argument voor deze aanbeveling wordt gevonden in de moeilijkheid die zou kunnen ontstaan voor lokale besturen om uit te maken of zij gepersonaliseerde dan wel louter informatieve diensten aanbieden.

190. Een tweede probleem dat opduikt tijdens de evaluatie van het bestaande wetgevende kader in het licht van de AVG betreft de verwarring die er heerst betreffende het statuut van de verwerkingsverantwoordelijke. Dat is nochtans belangrijk, niet enkel omwille van het gebrek aan rechtszekerheid en transparantie voor de burger over wie hij moet aanspreken in het geval er iets misgaat maar ook omwille van het mogelijke controleverlies over wat er met de data van deze burgers (weliswaar binnen de beperkingen opgelegd door de AVG) zou kunnen gebeuren. De vaststelling van de verwerkingsverantwoordelijke is volgens het Hof van Justitie een dynamische feitenkwestie waarin gekeken moet worden wie de doelen en middelen van de verwerking vaststelt en in welke mate er controleverlies over wat er gebeurt met de gegevens optreedt. Hoewel er verschillende documenten zijn die elkaar tegenspreken over wie op welke domeinen beschouwd kan worden als verwerkingsverantwoordelijke, kan er mijn inziens worden geconcludeerd dat zowel de erkennende overheid als de aanbieder van authenticatiediensten als overheden die hiervan gebruik maken elk binnen bepaalde (best door de wetgever vast te stellen) domeinen een gezamenlijke dan wel parallelle verantwoordelijkheid dragen.

191. Een van de verantwoordelijkheden die wordt opgelegd aan de verwerkingsverantwoordelijke door de AVG is het ontwikkelen van een strategie over de zogenaamde privacy by design. Eerder werd reeds beschreven dat de Nederlandse wetgever dit opnieuw beter begrepen heeft dan België

door aan de bevoegde minister de opdracht te geven deze strategie voor de betrokken actoren verder uit te werken. (Zie *supra* randnr. 93).

192. Een bijkomend probleem van het gebrek aan duidelijkheid betreffende de verantwoordelijkheid ligt vervat in de AVG zelf. Zo wordt bepaald dat verwerkers zelf geen verwerkers in dienst mogen nemen zonder toestemming van de verwerkingsverantwoordelijke. Wanneer wordt besloten dat overheden die gebruik maken van authenticatiemechanismen (parallelle of mede-) verantwoordelijken zijn, zou de acceptatieverplichting die in België geldt en de beperkte invloed die deze overheden maar hebben op het erkenningsproces van de aanbieders van authenticatiediensten (zie *supra* randnr. 82) in strijd kunnen worden beschouwd met deze bepaling. Ook de Europese Unie lijkt zich mijn inziens nog over dit probleem te zullen moeten buigen, daar ook zij een soortgelijke acceptatieverplichting (van in het buitenland erkende authenticatiemiddelen) opleggen in de huidige eIDAS verordening en ze daarmee nog een stap verder zouden willen gaan in het besproken voorstel tot hervorming.

193. Een derde grote probleem dat zou kunnen ontstaan uit het bestaande Belgische wettelijke kader, is de problematiek rond het doorgeven van gegevens wanneer een bedrijf dat erkende authenticatiediensten aanbiedt, verkocht of overgenomen wordt door een bedrijf dat gevestigd is in een derde land of de persoonsgegevens daar opslaat. De AVG verbiedt immers de overdracht van persoonsgegevens naar een derde land dat niet dezelfde standaarden ter bescherming tegen verwerking van deze gegevens kan bieden als de AVG zelf tenzij er een adequaatheidsbesluit geldt of er passende waarborgen worden genomen die voldoende afdwingbaar zijn.

Vooral wanneer er geen adequaatheidsbesluiten voorhanden zijn, zou zo een overname problematisch kunnen zijn. De methode van de passende waarborgen vereist immers dat er een grondige analyse betreffende de bescherming van de over te dragen persoonsgegevens en de mogelijkheid tot afdwingen van die bescherming dient te gebeuren. Bovendien moet er voorzien worden in een regeling die het mogelijk maakt om wanneer het misloopt alsnog de verwerking door de overnemende partij stop te zetten én mogen de gegevens in het derde land niet bereikbaar zijn voor diens autoriteiten. Dat laatste kan onmogelijk blijken wanneer in het derde land wetgeving wordt aangenomen die inzage in de gegevens onder bepaalde voorwaarden wel mogelijk maakt of wanneer het land gebruik kan maken van zeer geavanceerde technologie waar de afweersystemen van het overnemende bedrijf niet tegen opgewassen zijn.

194. Een vierde beginsel waar de Belgische wetgever rekening mee dient te houden, betreft het beginsel van de minimale gegevensverwerking en proportionaliteit. Dit beginsel kan immers verbonden worden aan het verschil in bewaartermijn dat voorgeschreven wordt in het kb elektronische identificatie en de bewaartermijn die Itsme zelf hanteert en reeds eerder in deze scriptie werd besproken. De overheid koos ervoor om slechts een minimumtermijn voor bewaring op te leggen waar het beginsel van minimale gegevensverwerking mijn inziens eerder een maximumtermijn vereist. Deze zou gelijkgesteld kunnen worden met de verjaringstermijn voor het instellen van een ontvankelijke rechtsvordering door de aanbieder van het authenticatiemechanisme tegen personen die trachten misbruik te maken van dit mechanisme.

195. Verder werd betreffende dit beginsel vastgesteld dat de Belgische overheid zich in vergelijking met Nederland eerder terughoudend opstelt en er misschien goed aan doet iets

krachtdadiger op te treden. Zij zou dit bijvoorbeeld kunnen doen door vast te stellen welke persoonsgegevens mogen worden bewaard en welke niet.

196. Ten slotte werd er in dit hoofdstuk nog gewezen op de eerder beperkte bevoegdheid die, de door de AVG verplichte, onafhankelijke controleorganen in de vorm van de GBA en VTC hebben in de controle van overheidsinstanties die deel uitmaken van de authenticatieketen. Zo zou het gebrek aan effectieve sanctiemogelijkheden kunnen leiden tot een verminderde toepassing van de beginselen van de AVG.

Conclusie

197. In deze scriptie werd op zoek gegaan naar een antwoord op de vraag of het Belgisch wettelijk kader betreffende authenticatie bij online overheidsdiensten voldoende aangepast is aan de ontwikkelingen op het niveau van de Europese Unie. Om tot een antwoord op deze centrale onderzoeksvraag te komen werden vier deelvragen beantwoord.

198. In het eerste hoofdstuk werd de organisatie van authenticatie op het Belgisch federaal en Vlaams niveau nagegaan. Het werd duidelijk dat door het groeiende aantal persoonlijke interacties tussen overheid en burger, authenticatie van burgers binnen het e-government beleid steeds belangrijker wordt. Om te kunnen nagaan of een persoon die online zegt een bepaalde identiteit te hebben ook effectief die persoon is, werd in België een identiteitsmanagementstrategie ontwikkeld waarin een belangrijke rol is weggelegd voor de eID kaart die samen met hard- of software binnen de PKI gebruikt kan worden om een authenticatiecertificaat te genereren dat gebruikt kan worden om zich aan de online overheidsdienst te authenticeren. Overheden zijn langs hun kant omwille van het only-once principe dan weer verplicht om ter identificatie van de burger gebruik te maken van het Rijksregisternummer. (zie *supra* randnrs. 27-29).

199. De hard- en software die de eigenlijke authenticatie van een persoon uitvoeren, vallen in de identificatieketen onder de groep van verificator (zie *supra* randnrs. 38-39). In België en Vlaanderen wordt deze rol uitgevoerd door de FAS dat werd opgericht door de FOD BOSA. Om die taak naar behoren uit te voeren, doet de FAS -naast het gebruik van ouderwetsere methoden zoals tokens en de eID kaartlezer- beroep op private partijen zoals Itsme (en binnenkort myID?) om burgers op een snelle en gebruiksvriendelijke manier te authenticeren. (zie *supra* randnrs. 40 en 42).

200. Het tweede hoofdstuk van deze scriptie ging dieper in op de nationale regulering betreffende deze authenticatiediensten. De wettelijke verankering van de erkenning van authenticatiediensten gebeurt in de wet inzake elektronische identificatie. Ter uitvoering van hun opdracht, krijgen de aanbieders van authenticatiemechanismen de status van onderaannemer van de FOD BOSA (zie *supra* randnr. 62). De verdere procedure, voorwaarden en gevolgen van de erkenning werden vastgelegd in het uitvoeringskb. elektronische identificatie.

201. Het Kb. legt aan het mechanisme de vereiste op om te voldoen aan de eisen die overeenkomen met betrouwbaarheidsniveaus substantieel of hoog en zoals vastgelegd in de uitvoeringsverordening van de eIDAS. Eens erkend, moeten alle overheidsdiensten die gebruik maken van de FAS de authenticatiemechanismen die overeenkomen met of hoger zijn dan het betrouwbaarheidsniveau dat, op beslissing van de betreffende overheid zelf, vereist is voor de specifieke online overheidsdienst. (Zie *supra* randnrs. 69 en 82). Verder moeten er bepaalde beveiligingsstandaarden zoals softwareupdates worden gevolgd (zie *supra* randnr. 77), moet er regelmatig gerapporteerd worden aan de FOD BOSA (zie *supra* randnr. 79) en moet de wetgeving betreffende de bescherming van persoonsgegevens worden gevolgd (zie *supra* randnrs. 73-75). De controle op deze vereisten komt toe aan de FOD BOSA die de erkenning kan schorsen of intrekken en de GBA die bevoegd blijft voor inbreuken op de privacy en gegevensbeschermingswetgeving (zie *supra* randnrs. 85-86).

202. Burgers die gebruik maken van de diensten van de FAS moeten zorg dragen voor hun identificatiemiddelen door ze te behoeden van verlies en diefstal (zie *supra* randnr. 64). De gedragingen van online overheden die gebruik maken van de diensten van de FAS worden -behoudens het accepteren van erkende authenticatiemechanismen- niet wettelijk gereguleerd (zie *supra* randnrs. 87-89).

203. Op Europees niveau wordt het authenticatiebeleid gereguleerd door de eIDAS verordening. De verordening maakt het onder andere voor EU burgers mogelijk om toegang te krijgen tot online overheidsdiensten over heel Europa door gebruik te maken van nationaal erkende authenticatiemechanismen (zie *supra* randnr. 108). Onder dit kader kunnen staten zonder verplichting en op een technologie neutrale manier authenticatiemechanismen ontwikkelen of laten ontwikkelen door een private partij en die daarna aanmelden onder de eIDAS verordening. Wel wordt er een systeem van wederzijdse erkenning opgesteld waarbij onderscheid gemaakt tussen de verschillende aangemelde systemen in de vorm van drie toegekende betrouwbaarheidsniveaus gaande van laag over substantieel tot hoog (zie *supra* randnrs. 110-111).

204. Het antwoord op de derde sub-onderzoeksvraag ("Welke rol speelt de gegevensbescherming in het nationale authenticatiebeleid?") werd gegeven in het laatste hoofdstuk. Uit het toepassingsgebied van de Algemene Verordening Gegevensbescherming vloeit voort dat inzake authenticatie zowel de overheden die gebruik maken van authenticatiesystemen als de aanbieders van authenticatiesystemen zelf zich zullen moeten houden aan de principes en verplichtingen van de AVG (zie *supra* randnrs. 143-146).

De eerste verplichting waar altijd rekening mee moet worden gehouden is die van de toelaatbaarheid van de verwerking welke voor de actoren in de authenticatiesystemen uiteraard werd voorzien in de wet en het kb. elektronische identificatie in combinatie met de privaatrechtelijke onderaannemingsovereenkomst voor private ontwikkelaars van authenticatiesystemen (zie *supra* randnr 149) ter uitvoering van een taak van het algemeen belang (zie *supra* randnr. 148). Eens de verwerking toelaatbaar is, moet er door de verwerkers rekening worden gehouden met algemene beginselen zoals het beginsel van de minimale gegevensverwerking, beginsel van rechtmatigheid, behoorlijkheid en transparantie en het beginsel van juistheid. Het komt aan de wetgevende overheid toe om die beginselen die voor verwarring zouden kunnen zorgen wat betreft hun concrete implementatie, verder te verdiepen in de nationale regelgeving (zie *supra* randnr. 141). Voor wat betreft de controle op deze beginselen moet er voorzien worden in een onafhankelijke instantie en is er een bijzondere rol weggelegd voor de verwerkingsverantwoordelijke (zie *supra* randnrs. 180-181).

205. Sinds de implementatie van de eIDAS verordening en de AVG zijn er voor beide wetgevingen echter enkele nieuwe strategieën en inzichten ontwikkeld. Het onderzoeken van deze evoluties leidde tot een antwoord op de vierde sub-onderzoeksvraag.

206. Voor wat de eIDAS verordening betreft, stelde de Commissie vast dat door een groeiende digitalisering, er een nood is ontstaan aan flexibele digitale identiteiten en authenticatiesystemen met een groot gebruiksgemak, sterke beveiliging en hoge betrouwbaarheid (zie *supra* randnrs. 118-119). Hiertoe ontwikkelde de Commissie in haar voorstel voor een eIDAS 2.0 een wettelijke grondslag waarin het mogelijk moet worden gemaakt voor staten om te voorzien in een grensoverschrijdend

systeem waarbij burgers zelf kunnen kiezen welke attributen verbonden zijn aan zijn identiteit. Daarnaast worden er vernieuwde verplichtingen opgelegd voor wat betreft beveiliging van deze identiteiten en de authenticatiemechanismen hieraan verbonden. Het is daarbij de bedoeling om via een "toolbox" waarin lidstaten hun opvattingen over online identificatie en authenticatiesystemen kunnen kenbaar maken, tot een geharmoniseerd systeem te komen (zie *supra* randnrs. 123-124) . De portefeuilles voor digitale identiteit zullen ook verplicht enkele certificaten moeten behalen die aangeven dat zij voldoen aan technische vereisten die garanderen dat zij in overeenstemming zijn met bepaalde cybersecurity standaarden opgelegd door verordening 2019/881 en verplichtingen opgelegd door de AVG (zie *supra* randnr. 126). Verdere uitwerking van deze ideeën zou volgen in nog op te stellen uitvoeringsverordeningen.

207. Ook voor wat betreft de toepassing van de AVG kwamen er nieuwe inzichten die van invloed kunnen zijn op het kader zoals het momenteel in België bestaat. Zo wees in 2019 de gegevensbeschermingscommissie er reeds op dat de verplichting door een overheidsdienst opgelegd aan een burger om zich te identificeren niet in alle gevallen legitiem is. Concreet zal dat enkel het geval zijn wanneer de overheidsdienst een persoonlijke dienst aan de burger verleent. Wanneer er een dienst wordt aangeboden die identificatie en authenticatie verantwoordt, zou er best worden gekozen voor de diensten aangeboden door de FAS.

208. Een tweede probleem dat is opgedoken is dat voor een correcte toepassing van de AVG het duidelijk zou moeten zijn welke verwerker van persoonsgegevens in de authenticatieketen wanneer beschouwd moet worden als verwerkingsverantwoordelijke. Dat is belangrijk omdat het de verantwoordelijke is die de controle over de betreffende gegevens uitoefent en het ook deze verantwoordelijke zal zijn die moet worden aangesproken in het geval van een onrechtmatige verwerking. Het Hof van Justitie stelde betreffende deze problematiek dat de status van verwerkingsverantwoordelijke een feitenkwestie is waarbij gekeken moet worden naar wie de doelen en middelen van de verwerking vaststelt (zie *supra* randnrs. 156-157).

209. Een derde probleem dat opduikt bij het gebruik van privaat georganiseerde authenticatiediensten en de verenigbaarheid met de AVG is het feit dat zij kunnen worden overgenomen door buitenlandse investeerders. Dit creëert voornamelijk problemen wanneer er daarbij een doorgifte van persoonsgegevens aan een derde land plaats zou vinden wat door de AVG enkel wordt toegestaan mits de aanwezigheid van een adequaatheidsbesluit, een bilateraal verdrag, bindende bedrijfsvoorwaarden of standaardcontractclausules overeenkomstig met het betreffende uitvoeringsbesluit van de Europese Commissie (zie *supra* randnr. 169). Uit de zaak Schrems II werd echter duidelijk dat zelfs de aanwezigheid van één van deze middelen op zich onvoldoende is om te garanderen dat de doorgifte van gegevens in overeenstemming met de AVG gebeurt. Om wel in overeenstemming te zijn zou het recht van het bestemmingsland grondig moeten worden gecontroleerd, moet er een exitstrategie bestaan voor wanneer het bedrijf failliet blijkt te gaan en moeten er maatregelen genomen worden om ervoor te zorgen dat de gegevens uit de handen blijven van de autoriteiten van het derde land (zie *supra* randnr. 171).

210. Ten slotte kunnen er wat betreft de toepassing van de AVG op de authenticatieketen nog vragen gesteld worden bij de noodzakelijkheid tot optreden van de wetgever wanneer het gaat om het naleven van het principe van minimale gegevensverwerking dat onder andere bepaalt dat

gegevens niet langer dan noodzakelijk mogen worden bewaard (zie *supra* randnr. 173) en wanneer het gaat om de verplichting tot het organiseren van een effectief en onafhankelijk toezicht op de naleving van de verplichtingen die voortvloeien uit de AVG door de verschillende schakels in de authenticatieketen (zie *supra* randnrs. 180-181).

211. Uit de antwoorden van bovenstaande vragen kan uiteindelijk een antwoord worden geformuleerd op de centrale onderzoeksvraag "Is het Belgische wetgevend kader om de veiligheid betreffende het gebruik van privaat dan wel overheidsgeorganiseerde authenticatietoepassingen voor het inloggen bij online overheidsdiensten zoals Itsme te garanderen voldoende aangepast aan de ontwikkelingen binnen de Europese Unie?". Een functionele rechtsvergelijking met Nederland laat daarnaast ook toe om reeds enkele voorzichtige aanbevelingen te formuleren op de ontdekte problemen in de Belgische regelgeving. Een diepgaandere analyse over deze en eventuele aanvullende aanbevelingen is echter nodig en kan daardoor voer zijn voor een volgend aanvullend onderzoek.

212. De evaluatie van de Belgische wetgeving betreffende authenticatiemechanismen werd in een eerste deel uitgevoerd door middel van een toetsing aan de Europese eIDAS verordening. Het antwoord of de Belgische wetgeving voldoende aangepast is aan de evoluties rond deze verordening is niet eenzijdig positief te beantwoorden. Zo viel in de eerste plaats op dat België sinds de invoering van de eIDAS meteen een voortrekkersrol heeft opgenomen door als enige Europese staat te kiezen voor een (deels) private partner in de ontwikkeling van een gebruiksvriendelijk authenticatiemechanisme dat gebruikers toeliet om zichzelf grensoverschrijdend en met de hoogst mogelijke betrouwbaarheid te identificeren bij online overheidsdiensten (zie *supra* randnrs. 112 en 128). Bovendien bewees Itsme om binnen het bestaande kader zeer snel aan veranderende sociale noden te kunnen voldoen. Het Belgisch kader is daardoor zodanig goed opgesteld dat de samenwerking met Itsme die daaruit voortvloeide mijn inziens in staat bleek om grotendeels te weerstaan aan de kritiek van de Europese Commissie betreffende de huidige eIDAS verordening en de implementatie hiervan in Europa. Itsme gaf ook reeds aan snel te kunnen schakelen naar een systeem waarbij gebruikers zelf kunnen kiezen welke identiteitsattributen zij bij de authenticatie wensen door te sturen naar de online overheidsdiensten (zie *supra* randnr. 132).

213. Toch zullen de door de Commissie voorgestelde aanpassingen zodanig ingrijpend zijn dat enkele beleidskeuzes zich zullen opdringen. Zo zal er uitgewerkt moeten worden of identiteitsattributen centraal dan wel decentraal beheerd zullen worden en welke rol authenticatiesystemen in de nieuwe digitale portefeuille zullen opnemen.

In navolging van de progressie op Europees niveau, verklaarde staatssecretaris M. MICHEL dat België voor het einde van 2023 zelf met een bijkomend alternatief voor Itsme zou komen in de vorm van een digitale portefeuille. Het feit dat de Commissie pleit voor een zo homogeen mogelijk systeem verspreid over heel Europa en er daarbij nog enkele fundamentele knopen door te hakken zijn, is mijn inziens voldoende reden om te wachten tot de Europese regelgeving concreter wordt. België is, gezien zijn uitzonderlijke expertise betreffende het thema, weliswaar uitstekend geplaatst om een prominente rol te spelen bij het geven van input voor de zogenaamde "toolbox". Opvallend genoeg lijkt het uiteindelijk eerder Vlaanderen te zijn dat met de lancering van datakluis "Athumi" -weliswaar een proefproject- lijkt te kiezen voor een gecentraliseerd systeem en daarmee zichzelf dreigt te

vergalopperen. Een gecentraliseerde datakluis heeft immers als nadeel bijzonder gevoelig te zijn voor cyberaanvallen en bijhorende identiteitsfraudes. Ook Nederland erkent deze problematiek en sprak zich op Europees niveau al uit tegen gecentraliseerde systemen (zie *supra* randnrs. 131, 132 en 139).

214. Waar België mijn inziens wel reeds op zou kunnen inspelen zijn de verplichtingen tot certificaten waarin de hernieuwde eIDAS zal voorzien. Zo zou in het huidige kader reeds dergelijke verplichting kunnen worden opgenomen. Voor wat betreft cybersecurity zou er daarbij gekeken kunnen worden naar de cyberbeveiligingsverordening die voorziet in de oprichting van een Europees agentschap voor cyberbeveiliging (ENISA) dat bevoegd is dergelijke Europese cyberbeveiligingscertificaten uit te reiken (zie *supra* randnr. 126). Voor een certificaat betreffende de correcte implementatie van de AVG zou er kunnen worden gekeken naar de GBA (zie *supra* randnr 181).

215. Meer valt er te zeggen over de evaluatie van het Belgisch wetgevend kader betreffende authenticatiemechanismen aan de beginselen zoals vervat in de AVG. Reeds eerder werden enkele problemen aangehaald waar de Belgische wetgever bij het opstellen van het wettelijk kader rekening mee dient te houden.

216. Vooreerst moet het kader voorzien in een wettelijke grondslag dat voorziet in een reden die de verwerking van persoonsgegevens door verschillende actoren in de authenticatieketen mogelijk maakt. Dit gebeurde uitdrukkelijk door de wet elektronische identificatie dat aan de FOD BOSA en de FAS de uitvoering van een taak van algemeen belang opdroeg (zie *supra* randnrs. 42, 60, 61 en 148). Via het onderaannemingscontract wordt dan weer voorzien in een grondslag die een verwerking door de erkende aanbieders van authenticatiemiddelen toelaat (zie *supra* randnrs. 100 en 149). Voor overheden die identificatie en authenticatie van de burger vraagt, ligt de grondslag in de only-once wet, het bestuursdecreet en de gebruikersovereenkomst die overheden die gebruik maken van de FAS dienen te accepteren. (zie *supra* randnrs. 29 en 87).

217. Toch lijkt er, volgende uit de rechtspraak van de gegevensbeschermingsautoriteit dat de eis tot identificatie door online overheden beperkt, een grote tekortkoming aanwezig in het Belgisch kader. Het zou mijn inziens (voornamelijk voor lokale overheden) immers moeilijk kunnen zijn om in te schatten welke online diensten beschouwd moeten worden als persoonlijke dienst -en dus identificatie verantwoorden- en welke als louter informatief. Het zou dan ook duidelijker zijn om, zoals Nederland gedaan heeft, lijsten op te stellen met welke overheidsdiensten en publieke instellingen voor welke diensten verplicht worden om gebruik te maken van de authenticatiediensten. Om een wildgroei aan eigen of ongecontroleerde buitenlandse authenticatiesystemen te voorkomen kan daarbij de verplichting worden opgelegd enkel gebruik te maken van de diensten van de FAS. Een dergelijke verplichting zou weliswaar een samenwerking tussen de verschillende federale niveaus in België vereisen (zie *supra* randnr. 154).

218. Een tweede tekortkoming werd waargenomen door het gebrek aan duidelijkheid betreffende de verantwoordelijkheid van de verschillende verwerkingen van persoonsgegevens die plaatsvinden gedurende de authenticatie. Een lezing van de wetgeving, de onderaannemingsovereenkomst, gebruiksocereenkomt en privacyverklaring van Itsme leidt immers tot tegenstrijdige of minstens verwarrende berichtgeving hieromtrent. Bovendien gaf de wetgever voor een groot stuk de controle

over de persoonsgegevens uit handen (zie *supra* randnr. 159-160). De wetgever zou er mijn inziens dan ook goed aan doen om zoals Nederland (zie *supra* randnr. 93) hieromtrent duidelijkheid te verschaffen of minstens vast te leggen tot waar de (parallelle of gedeelde?) verantwoordelijkheid van de overheidsinstellingen zelf gaat. Dit gebeurde overigens wel reeds gedeeltelijk in de FAS gebruikersovereenkomst waarbij de verantwoordelijkheid voor de verwerking van gegevens in de online overheidstoepassing bij de overheid in kwestie wordt gelegd (zie *supra* randnr. 162). Binnen de eigen verantwoordelijkheden, zal het ook aan de erkennende overheid toekomen om in bijkomende protocollen die voorzien in passende technische en organisationele maatregelen af te sluiten (zie *supra* randnr. 163).

Ten slotte lijkt de verplichting voor online overheidsdiensten om alle erkende authenticatiediensten van de FAS te moeten aanvaarden haaks te staan op het verbod in artikel 28 lid 2 AVG. Mogelijks moet de wetgever dan ook overwegen deze overheden meer inspraak te geven betreffende het (behoud van) erkenningen. Dit zou kunnen door bijvoorbeeld te voorzien in een noodprocedure wanneer een overheid vaststelt dat de bepalingen van de AVG worden geschonden.

219. Wat betreft de geschetste problematiek over het doorgeven van gegevens moet er uiteraard worden toegegeven dat de Belgische wetgever niet kan voorzien of een privaat bedrijf overgenomen zal worden door een buitenlandse investeerder uit een derde land. Het is dan ook moeilijk om op deze potentiële situatie in te spelen. Toch is dit risico inherent aan een samenwerking met private partijen en moet er mijn inziens tot op zekere hoogte rekening mee worden gehouden. De overheid deed dit reeds door te voorzien in de mogelijkheid tot het uitvoeren van een audit in combinatie met een (tijdelijke) intrekking van de vergunning van authenticatiedienstverleners wanneer zij van oordeel zou zijn dat de veiligheid van de gegevens van de burger niet meer gegarandeerd kan worden (zie *supra* randnr. 85). Bovendien heeft de overheid nog steeds een (minderheids)aandeel in Belgium Mobile ID NV en behoudt zij zo inspraak of minstens inzage in eventuele gesprekken met potentiële overnemers (zie *supra* randnr. 43). Door in de toekomst zelf te voorzien in een publiek beheerde authenticatiedienst, verzekert zij daarnaast een authenticatiedienst die niet in buitenlandse handen kan vallen en dat burgers redelijk makkelijk zullen kunnen overschakelen wanneer een erkenning wordt ingetrokken of wanneer burgers zelf het idee hebben dat de veiligheid van hun gegevens in gevaar zou zijn.

Als Itsme of myID alsnog in handen zou komen van een bedrijf uit een derde land zullen evenwel aanvullende maatregelen zoals een analyse van het rechtssysteem van het derde land nodig zijn (zie *supra* randnr. 171). Wat deze verdere aanvullende maatregelen precies zouden moeten inhouden kan onderwerp zijn voor een eventueel verder onderzoek. Wel voorziet het Belgische kb in de mogelijkheid tot intrekking van de vergunning wanneer het bedrijf zich in staat van faillissement bevindt wat zou kunnen helpen om gegevens uit de handen van nationale autoriteiten te houden (zie *supra* randnr. 80).

220. Een vierde problematiek die ontstaat tussen het Belgisch kader en de AVG is de implementatie van het beginsel van de minimale gegevensverwerking. Dat vereist immers dat de termijn gedurende wanneer gegevens mogen opgeslagen blijven moet beperkt blijven tot een minimum. Dat minimum wordt aangenomen overeen te komen met de verjaringstermijn voor het ontvankelijk kunnen instellen van een rechtsvordering (zie *supra* randnrs. 173 en 175). Het kb.

elektronische identificatie voorziet echter in een minimumbewaringstermijn van tien jaar vanaf het moment van (poging tot) aanmelding (zie *supra* randnr. 74). Hoewel de keuze voor een verplichte termijn van tien jaar in het licht van de verjaringstermijnen in België te verdedigen valt, zou er mijn inziens beter worden gekozen voor een absolute termijn waarbij gegevens na het verlopen van de tien jaar automatisch worden gewist. Uit de privacyvoorwaarden van Itsme blijkt immers dat gegevens momenteel langer worden bewaard dan noodzakelijk (zie *supra* randnr. 50).

221. Ook valt op dat authenticatiediensten in België meer gegevens lijken te bewaren dan strikt noodzakelijk zou zijn voor het kunnen aanbieden van hun diensten (zie *supra* randnrs. 45-49). Hoewel dit in het licht van de betekenis van het beginsel van minimale gegevensverwerking zoals blijkt uit de voorbereidende documenten niet per se een schending van de verordening hoeft te zijn, doet de wetgever er mijn inziens toch goed aan om wanneer er op dergelijk grote schaal gegevens worden verwerkt ook hier wetgevend in te grijpen en uit te werken welke soorten gegevens mogen worden bewaard en welke niet.

222. Een maatregel die wel degelijk het beginsel implementeert is de bepaling die stelt dat in België (net zoals in Nederland) authenticatiediensten niet verwerken op welke overheidsdiensten beroep wordt gedaan. In Nederland bestaat daarnaast de verplichting tot het verwijderen van de gelaatsfoto en BSN nummer na registratie (zie *supra* randnr. 93), een maatregel die mijn inziens ook in België makkelijk geïmplementeerd zou kunnen worden.

223. Wat betreft controle ten slotte viel in deze scriptie vast te stellen dat hoewel België en Vlaanderen door de oprichting en bevoegdverklaring van de GBA en VTC lijken te voldoen aan de verplichting tot het oprichten van een onafhankelijke controle-instantie, de grootste controleur van de authenticatiediensten toch voornamelijk de FOD BOSA zelf is. Voor de aanbieders van authenticatiediensten lijkt de controle op het eerste zicht echter goed georganiseerd: Zo wordt er voorzien in een systeem van opvolging dat verzekert dat de authenticatiediensten nog steeds voldoen aan de voorwaarden die door de wet en het kb. worden opgelegd, bestaat er een verplichting tot het melden van problemen moesten die zich voordoen, worden de beheerders verplicht tot het verlenen van inzage aan de FOD BOSA in bepaalde documenten en kan er ten allen tijde overgegaan worden tot een audit van het systeem (zie *supra* randnrs.79 en 84). Ook in Nederland bestaat een vergelijkbaar controlemechanisme (zie surpa randnr. 98.).

224. Voor wat betreft het toezicht op overheden valt op dat beide controle-instellingen niet in staat zullen zijn om bestraffende sancties op te leggen aan overheidsinstanties betrokken in de authenticatieketen (zie *supra* randnrs. 182 en 183). Vooral met een volledig publiek authenticatie alternatief in het vooruitzicht, kunnen er toch vragen gesteld worden over de doeltreffendheid van het bestaande controlemechanisme zeker omdat de AVG nog voorziet in de mogelijkheid om de verplichtingen die zij zelf oplegt te beperken voor overheidsinstellingen (zie *supra* randnr. 184-185).

225. Een mogelijke oplossing voor dit probleem kan opnieuw gevonden worden in Nederland waar er wordt voorzien in een grote toezichtsverantwoordelijkheid voor de Minister van Binnenlandse zaken en het expliciet van toepassing verklaren van het systeem van bestuurlijk toezicht door hogere overheden op lagere overheden. Bovendien geldt voor deze besturen ook een informatieplicht bij problemen aan deze minister en moet er een jaarlijkse audit worden gehouden waarvan de resultaten opnieuw moeten worden meegedeeld aan deze minister (zie *supra* randnr. 97). Dit systeem creëert

naar mijn mening een verhoogd politiek besef voor de gevaren die gepaard gaan met het verwerken van data, gecombineerd met een verhoogde politieke verantwoordelijkheid voor de bevoegde minister. Dit zou mijn inziens kunnen leiden tot een striktere opvolging dan het geval is in België waar ministers zich kunnen wegsteken achter de ambtenaren van de FOD BOSA.

226. Concluderend kan mijn inziens dan ook worden gesteld dat hoewel België lang een voortrekker is geweest wat betreft de implementatie van authenticatiesystemen en dit in vergelijking met heel wat landen in Europa misschien nog steeds is, er toch heel wat opmerkingen te maken vallen over het wettelijk kader zoals dat op de dag van vandaag bestaat. Het valt vooral op dat de wetgeving wat betreft de implementatie van de AVG veel leemtes bevat waarmee het parlement en de regering bij het maken van deze regulering geen rekening mee heeft kunnen houden. Dat is voor veel van de beschreven situaties, gezien de snelle evolutie in de digitalisering, ook niet geheel verwonderlijk. Toch zijn de in deze scriptie aanbevolen aanpassingen mijn inziens niet onoverkomelijk en snel te implementeren. Dat ligt anders voor wat betreft de evoluties rond de eIDAS verordening. België bewijst daar vooral goed en waarschijnlijk zelfs voor op schema te liggen in vergelijking met andere landen in Europa. Op enkele kleine implementaties -zoals het verplichten van bepaalde certificaten- na lijkt het verstandiger om de definitieve teksten op Europees niveau af te wachten alvorens nieuwe systemen te gaan uitrollen. Wel kan er optimaal gebruik worden gemaakt van de ervaring die België reeds opdeed in verband met authenticatiesystemen en kan er -net zoals in Nederland- overwogen worden om reeds enkele proefprojecten op te starten om door middel van bijkomende bevindingen te wegen op het Europees beleid.

227. Voor volgende scripties zal het daarnaast interessant zijn om op te volgen hoe deze Europese evoluties zich de komende maanden zullen concretiseren in wetteksten en in welke mate deze te verzoenen zijn met de bepalingen uit de AVG. Ook de verdere uitwerking en concretisering in Nederland zou kunnen leiden tot nieuwe inzichten voor wat betreft het (toekomstig) Belgisch kader. Ten slotte zou het interessant kunnen zijn om in samenwerking met specialisten in de cybersecurity een interdisciplinair onderzoek uit te werken over hoe men via wettelijke verplichtingen tot een optimale beveiliging van persoonsgegevens beheerd door overheden zou kunnen komen.

Lijst van geraadpleegde werken

A. Wetgeving

a) Europa en België

- Verdrag betreffende de Werking van de Europese Unie, *Pb.L* 26 oktober 2012, afl.326, 47.
- Handvest van de Grondrechten van de Europese Unie, *Pb.L* 18 december 2000, afl 361, 1.
- Verord.Raad.Parl Nr. 910/2014, 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, *Pb.L* 28 augustus 2018, afl. 257, 73.
- Verord.Parl.Raad Nr. 2019/881, 17 april 2019 inzake inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening), *Pb.L* 7 juni 2019, afl. 151, 15.
- Uitvoeringsverord.Comm. Nr. 2015/1501, 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, *Pb.L* 9 september 2015, afl. 235, 1.
- Uitvoeringsverord.Comm Nr. 2015/1502, 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, 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, *Pb.L* 9 september 2015, afl 235, 7.
- Verordening EP en Raad Nr. 2016/679, 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.
- Uitvoeringsverordening.Comm. nr. 2016/1250, 12 juli 2016 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de gepastheid van de door het EU-VS-privacyschild geboden bescherming.
- Uitvoeringsbesluit.Comm. nr. 2021/914, 4 juni 2021 betreffende standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad (Voor de EER relevante tekst), *Pb.L* 7 juni 2021, afl 199, 31.
- Richtl.Europese Raad en parl. nr. 2022/2555, 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn), *Pb.L* 27 december 2022, afl. 333, 80.
- EUROPEES COMITE VOOR GEGEVENSBESCHERMING, Aanbeveling over de Europese essentiële garanties voor surveillancemaatregelen, 10 november 2020, nr. 02/2020, 16p.

- Mededeling (Comm.) aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het comité van de regio's Digitaal kompas 2030: de Europese aanpak voor het digitale decennium, 9 maart 2021, COM(2021) 118 final.
- Voorstel (Comm.) voor een verordening van het Europees parlement en de raad tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit, 3 juni 2021, COM(2021) 281 final 2021/0136 (COD).
- EUROPEES COMITE VOOR GEGEVENSBESCHERMING (EDPB), Aanbevelingen inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen versie 2.0, 18 juni 2021, nr. 01/2020, 55p.
- Richtsnoer.EDPB nr. 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG, 7 juli 2021, 61p.
- EDPB nr. 05/2021, Guidelines on the interplay between the application of article 3 and the provisions on international transfers as per chapter V of the GDPR 2.0, 14 februari 2023.
- Bijzondere wet 8 augustus 1980 tot hervorming der instellingen, *BS* 15 augustus 1980.
- Wet 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *BS* 21 april 1984.
- Wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten, *BS* 3 september 1991.
- Wet 25 maart 2003 t tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *BS* 8 maart 2003.
- Wet 5 mei 2014 houdende verankering van het principe van de unieke gegevensinzameling in de werking van de diensten en instanties die behoren tot of taken uitvoeren voor de overheid en tot vereenvoudiging en gelijkschakeling van elektronische en papieren formulieren, *BS* 4 juni 2014.
- (Oud) Burgerlijk Wetboek 21 maart 1804, *BS* 3 september 1807.
- Wet van 18 juli 2017 inzake elektronische identificatie, *BS* 9 augustus 2017
- Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, *BS* 10 januari 2018.
- Wet 30 juli 2018 tot bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018.
- Wet van 25 november 2018 houdende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters, *BS* 13 december 2018.
- Wet van 26 januari 2021 betreffende de dematerialisatie van de relaties tussen de FOD Financiën, de burgers, rechtspersonen en derden bepaalt de wijze waarop de informatie vanaf 1 januari 2025 elektronisch zal worden uitgewisseld, *BS* 10 februari 2021.
- Wet 20 april 2022 houdende boek 5 "verbintenissen" van het Burgerlijk Wetboek, *BS* 1 juli 2022.
- Decreet 18 juli 2018 betreffende het elektronisch bestuurlijk gegevensverkeer, *BS* 29 oktober 2008.
- Decreet 7 december 2018 Bestuursdecreet, *BS* 19 December 2018.

- Decreet 2 december 2022 houdende machtiging tot oprichting van het privaatrechtelijk vormgegeven extern verzelfstandigd agentschap Vlaams Datanutsbedrijf in de vorm van een naamloze vennootschap, *BS* 14 december 2022.
- Koninklijk besluit van 17 juli 2014 tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van diensten voor elektronische identificatie voor digitale overheidstoepassingen die gebruik maken van niet-verbonden aanmeldingsmiddelen, *BS* 8 augustus 2014.
- 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, *BS* 8 november 2017.
- Koninklijk besluit van 1 februari 2018 besluit tot aanwijzing van instanties conform de wet van 18 juli 2017 inzake elektronische identificatie, *BS*, 9 februari 2018.
- Besluit van de Vlaamse Regering 18 maart 2016 houdende de oprichting van het intern verzelfstandigd agentschap [Digitaal Vlaanderen] en de vaststelling van de werking, het beheer en de boekhouding van het [Eigen Vermogen Digitaal Vlaanderen, *BS* 2 juni 2016.
- Wetsontwerp (A. DE CROO) inzake elektronische identificatie, *Parl. St.* Kamer 2016-17, nr. 2512/001.
- Wetsontwerp tot oprichting van de Gegevensbeschermingsautoriteit, *Parl.St*. Kamer 2016/17, nr. 2648/001.
- Gegevensbeschermingsautoriteit (GBA) advies uit eigen beweging over het verwerken van biometrische gegevens in het raam van authenticatie van personen, 9 april 2008, nr. 17/2008.
- COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (CBPL), advies met betrekking tot het voorontwerp van wet inzake elektronische identificatie, 21 september 2016, nr. 48/2016.
- COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (CBPL), advies betreffende ontwerp van koninklijk besluit tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van diensten voor elektronische identificatie voor digitale overheidstoepassingen (CO-A-2017-008), 12 april 2017, nr. 18/2017.
- VLAAMSE TOEZICHTCOMMISSIE VOOR DE VERWERKING VAN PERSOONSGEGEVENS (VTC), advies betreffende informatieveiligheid en GDPR-conformiteit 4 platformen onderwijs – Amazon Web Services, 8 september 2020, nr. 2020/05.
- Gegevenbeschermingsautoriteit (GBA), advies over een ontwerpbesluit van de Regering van de Franse Gemeenschap tot het bepalen van de categorieën van persoonsgegevens die worden verwerkt met betrekking tot de doeleinden van de digitale ruimten in toepassing van de artikelen 6 en 11 van het decreet van 25 april 2019 betreffende het digitaal bestuur van het schoolsysteem en de overdracht van digitale gegevens in het leerplichtonderwijs, 5 november 2020, nr. 108/2020.
- VLAAMSE TOEZICHTCOMMISSIE VOOR DE VERWERKING VAN PERSOONSGEGEVENS, advies wetgeving VTC , betreffende het voorontwerp van decreet samenwerkingsakkoord vaccinaties COVID-19, februari 2021, nr. 2021/13.
- Gegevensbeschermingsautoriteit (GBA), *Aanbeveling betreffende de verwerking van biometrische gegevens*, 1 december 2021, nr. 01/2021.

- Algemene beleidsnota digitalisering, administratieve vereenvoudiging, privacy en regie der gebouwen*, Parl.St.* Kamer 2022-2023, nr. 2934/010.
- *Vr. en Antw.* Kamer 2019/2020, 16 december 2020, nr. 55-031 (Vr. 12 S. MATHEÏ, Antw. M. Michel), 486
- *Vr. en Antw*. Kamer 2022-2023, 30 september 2022, nr. 0379, (Vr. 11 S. CREYELMAN, antw. M. MICHEL).

b) Nederland

- Wet van 4 juni 1992, houdende algemene regels van bestuursrecht (Algemene wet bestuursrecht), *StB.* 1992, 315.
- Besluit van 17 mei 2016, houdende regels betreffende de verwerking van persoonsgegevens in de voorzieningen voor de generieke digitale infrastructuur DigiD, DigiD Machtigen, MijnOverheid en BSN-Koppelregister (Besluit verwerking persoonsgegevens generieke digitale infrastructuur), *StB* 2016, 195.
- Gewijzigd voorstel van wet betreffende Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid), *Parl.St.* Eerste kamer 2019-2020, nr. 34972, A.
- MvT bij wetsvoorstel betreffende Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid), *Parl.St.* tweede kamer 2017-2018, nr. 34972, 3.
- AUTORITEIT PERSOONSGEGEVENS, Advies wet ontwerp Wet generieke digitale infrastructuur, 13 oktober 2017, nr. z2017-06929, https://www.eerstekamer.nl/overig/20180619/advies_autoriteit_persoonsgegevens/document.
- *Vr. en Antw.* Tweede kamer (ndl.) 2022-2023, 16 februari 2023, nr. 54-6, 4 (LEIJTEN antw. VAN HUFFELEN).

B. Rechtspraak

- HvJ 6 november 2003, nr. C-101/01, ECLI:EU:C:2003:596, Lindqvist/Zweden.
- HvJ 13 mei 2014, nr. C-131/12, ECLI:EU:C:2014:317, Google Spain/AEPD.
- HvJ 9 maart 2017, nr. C-398/15, ECLI:EU:C:2017:197, Manni/Italië.
- HvJ 5 juni 2018, nr. C-210/16, ECLI:EU:C:2018:388, Wirtschaftsakademie Schleswig-Holstein.
- HvJ 29 juli 2019, nr. C-40/17, ECLI:EU:C:2019:629, Fashion ID.
- HvJ 16 juli 2020, nr. C-311/18, ECLI:EU:C:2020:559, Schrems II, noot CLEMENS., J.
- HvJ 6 oktober 2020, C-511/18, C512/18 en C-520/18, ECLI:EU:C:2020:791, La Quadrature du Net.
- GwH 14 januari 2021, nr. 02/2021.
- Cass. 27 mei 1909, *Pas.* I 1909, 272.
- Cass. 20 juni 1997, *Arr.Cass* 1997, 673.
- Cass. 28 maart 2019, nr. C.18.0272.F.
- RvS 12 mei 2021, nr. 250.599.
- Luik 30 september 2005, *JLMB* 2006, 817.

- Brussel (Marktenhof) 26 oktober 2022, Computerr. 2023/40.
- Orb. Antwerpen (afd. Antwerpen) 22 november 2022, *DAOR* 2023/1, nr. 143, 17-20.
- Cour adm. Luxembourg 12 juli 2005, *DAOR* 2006/79, 289-307.
- GBA, aanbeveling nr. 01/2019 betreffende het opleggen van de verplichte aanmaak van een gebruikersaccount bij Microsoft voor het raadplegen van toepassingen van overheidsdiensten, 6 februari 2019.
- GBA geschillenkamer, beslissing ten gronde nr. 82/2020 betreffende klacht wegens het noodzakelijk moeten aanmaken van een Microsoft account voor het downloaden van een document bij de FOD Financiën, 23 december 2020.
- AUTORITEIT PERSOONSGEGEVENS*,* advies nr. z2021-08230 Google G suite for education, 8 juni 2021.

C. Rechtsleer

- ARTIKEL 29 WERKGROEP, *advies over het begrip persoonsgegeven*, 20 juni 2007, nr 4/2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_nl.pdf, 28p.
- ARTIKEL 29 WERKGROEP, *Advies over de recente ontwikkelingen op het gebied van het internet van de dingen*, 16 september 2014, nr. 8/2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_nl.pdf, 27p.
- ARTIKEL 29 WERKGROEP GEGEVENSBESCHERMING, *Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679*, 4 april 2017, https://overheid.vlaanderen.be/sites/default/files/media/VTC/wp248%20rev.01_nl_0.pdf, 29p.
- BALTHAZAR, T. en RAEMAEKERS, P., *Gegevensbescherming in de zorg - een praktische gids bij de GDPR*, Brugge, Die Keure, 2018, 151p.
- BEELEN, A., en JASPAR, A., *La protection des données pour les institutions publiques*, Limal, Anthemis, 2020, 256p.
- BERTILLE DEMBELE, S., "La protection de l'identité numérique post mortem", *RDTI* 2018, nr. 3, 5-24.
- BEUDELS, M., "Schrems II: volgend hoofdstuk in het verhaal van de internationale gegevensdoorgiften", *TPP* 2021, nr. 1, 18-27.
- BUITELAAR, J. C., MEINTS, M. en VAN ALSENOY, B., "Conceptual framework for identity management in e-government"*, FIDIS Project,* 2008, nr. 16.1, 143p.
- CAPRONI, M. en DE SMEDT S., *Praktische gids, Privacy in de onderneming*, Mechelen, Wolters Kluwer, 2019, 323p.
- CLAEYS, I., *Verbintenissenrecht*, Gent, Faculteit Recht en Criminologie, 2019, 27p.
- CLEMENS, J., "De Raad van State opent de deur voor doorgiften van persoonsgegevens naar de Verenigde Staten na schrems II", *TPP* 2022, nr. 1, 24-31.
- CLESSE, C-E. en VERWILGHEN, M., "Les sanctions de la violation de la vie privée" in GILSON, S. en NILLES, P., *Technologies, surveillance et vie privée du travailleur*, 371p.
- P. CRADDOCK, "Arrêt « Fashion ID »: qui est le « responsable du traitement » des données sur un site Internet incorporant un renvoi à un réseau social?", *JTDE* 2019, nr. 10, 404-406.

- DEBEUCKELAERE, W., "En wat nu (weer) gedaan? Verbazing en verwarring na Schrems II", *TPP* 2020, nr. 4, 38.
- DE COCK, D., VAN ALSENOY, B., PRENEEL, B., en DUMORTIER, J., "The Belgian eID approach", in FUMY, W., en PAESCHKE, M., *Handbook of eID Security. Concepts, Practical experiences, Technology,* Erlangen, Publicis, 211, 117-139.
- DE BOT, "De Wet only Once – een wetgevende verankering van het beginsel van unieke gegevensinzameling", *P&I* 2014, nr. 166, 186-188.
- DE BOT, D., *E-government in het Federale België*, Brussel, Politeia, 2015, 1184p.
- DE BOT, D., *Gegevensverwerking in de publieke sector. Een verkennend onderzoek van de relatie tussen privacy-, gegevensbeschermings-, administratief en grondwettelijk recht aan de hand van de uitwisseling van gegevens tussen besturen*, Brussel, Politeia, 2016, 655.
- DE BOT, D., *De toepassing van de algemene verordening gegevensbescherming in de Belgische context Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Mechelen, Wolters Kluwer, 2020, 1394p.
- DECLERCQ, S., en GOOSSENS, E., "Derdenwerking van contracten: actuele ontwikkelingen" in STIJNS, S., en DE BOECK, A., *Themis 2021-2022 nr. 120: Verbintenissenrecht*, Antwerpen, Intersentia, 43-78.
- DE CORTE, R., "Elektronische handtekening en identificatie in de virtuele wereld", *P&B*, 2001, afl. 5, 207-234.
- DE LANDSHEERE, J., "Only-onceprincipe: het principe van de unieke gegevensverzameling", *NWJ* 2016, nr. 336, 98-103.
- DE POORTER, I., "De 'GDPR' of algemene Verordening Gegevensbescherming (AVG) – Een algemene inleiding" in INSTITUUT FINANCIEEL RECHT, *Financieel recht: een dwarsdoorsnede*, Antwerpen, Intersentia, 2019, 449-492.
- DEPREZ, S., *Gegevensbescherming*, Hoegaarden, LeA uitgevers, 2022, 346p.
- C. DE TERWANGNE, "L'illégalité nuancée de la surveillance numérique : la réponse des juridictions belge et française à l'arrêt La Quadrature du Net de la Cour de justice de l'Union européenne", *RTDH* 2022, nr. 129, 3-28.
- DROITS QUOTIDIEN LEGAL DESIGN, *FOD Financiën: in 2025zal alle communicatie elektronisch gebeuren*, Wolters Kluwer ImmoSpector, 2021, https://immospector.kluwer.be/newsview.aspx?contentdomains=IMMORES&id=kl2528877&lang=nl.
- FOCQUET, A. en DECLERCK, E., *gegevensbescherming in de praktijk*, Antwerpen, Intersentia, 2019, 218 p.
- GAWRONSKI, M., *Guide to the GDPR*, Alphen aan den Rijn, Kluwer Law International, 2019, 345 p, https://wkldigitalbooks-integra-co-in.bib-proxy.uhasselt.be/Customer/Home/BookDetails?TitleGUID=B264AF7E-6C5E-4CA7-9F01-56E002CDFAC2
- GORLE, F., BOURGEOIS, G., en BOCKEN, H., *Rechtsvergelijking*, Mechelen, Kluwer, 2007, 359p.

- GRAUX, H., "De eIDAS-Verordening en de begeleidende Belgische wetgeving : nieuwe marsorders voor elektronische handtekeningen en andere vertrouwensdiensten", *CDJ* 2016, nr. 3, 53-62.
- HAEX, D., en AELBRECHT, T., "De elektronische handtekening toegespitst op vennootschapsrechtelijke documenten: it's all about trust", *RDC-TBH*, 2020, nr. 5, 565-582.
- HENRY, F en VERHELST, I., "Protection des données à caractère personnel dans les relations individuelles et collectives de travail" in H., JACQUEMIN, *Le règlement général sur la protection des données (RGPD/GDPR): premières applications et analyse sectorielle*, Luik, Anthemis, 2020, 59-126.
- HU, W.Y., VAN DEN BROEK, F.M.J. en JACOBS, B.J.F., "Attribuut-gebaseerde elektronische handtekeningen en de eIDAS-verordeninging" in WOLTERS, P.T.J., *Digitalisering en conflictoplossing reeks OO&R deel 130*, Alpen aan den Rijn, Wolters Kluwer, 2021, 293-317.
- JACQUEMIN, H., en GILLARD, N., "Regulation 910/2014/EU – eIDAS Regulation", in S. GIJRATH, S. VAN DER HOF, A. R. LODDER en G-J ZWENNE, *Concise European Data Protection, E-Commerce and IT Law*, Alpen aan den Rijn, Wolters Kluwer, 2018, 1039p.
- JOUSTEN, A. en MINY, X., "Blockchain et droit Public, menace et/ou atout pour l'Etat?" in VANDENBULCKE, A., (ed.), *Les aspects juridiques de la blockchain et de ses applications*, in Limal, Anthemis, 2022, 127-167.
- KEUNEN, L., "De vernietiging van de Dataretentiewet 2.0: naar een gerichte bewaring met ruime toegang?",(noot onder HvJ 6 oktober 2020, C-511/18, C512/18 en C-520/18, La Quadrature du Net) *RW* 2021-2022, nr 37, 5-8.
- KINDT, E. en STEVENS, D., "Recente ontwikkelingen in het gegevensbeschermingsrecht" in CONINGS, C., GRANATA, S., JANSSENS, M-C., KINDT, E., ROVER, S., STEVENS, D., VANHERPE, J., en VAN OVERWALLE, G., *Themis 2022-2023 nr. 125 IP- en ICT-recht*, Antwerpen, Intersentia, 2023, 155-194.
- KRZYSZTOFEK, M., *GDPR, Personal data protection in the European Union*, Alphen aan den Rijn, Kluwer, 2021, 348p.
- LENAERTS, K., en VAN NUFFEL, P., *Europees recht*, Mortsel, Intersentia, 2023, 809p.
- RAAD VAN EUROPA, *Handboek Europese gegevensbeschermingswetgeving,* Luxemburg, Bureau voor Publicaties van de Europese Unie, 2021, 466 p.
- SCHOUKENS, P., HENDRICKX K., TERRYN, E., (red.) and KESTEMONT L., *Rechtswetenschappelijk schrijven*, Leuven, Acco, 2020, 143p.
- SCHRAM, F., "Datamining en fraudebestrijding via gegevensuitwisseling en de juridische gevolgen van onrechtmatige elektronische uitwisseling van informatie tussen verschillende overheidsadministraties", in DELANOTTE, M., PEETERS, B., en VAN DE WOESTEYNE, I. (eds.), *Digitalisering. Postuniversitaire cyclus Willy Delva*, Mechelen, Wolters Kluwer, 2021, 436p.
- SUSTRONCK, O., "It's not you, Itsme", *TPP* 2021, nr. 3, 6-10.
- TIJSSEN, H. E. B., *De juridische dissertatie onder de loep: De verantwoording van methodologische keuzes in juridische dissertaties*, Boom, Juridische Uitgevers, 2009, 253p.
- VAN ALSENOY, B., *Data protection Law in the EU*, *Roles, Responsibilities and Liability*, Mortsel, Intersentia, 2019, 694p.

- VEDDER, A., Security and Law, Mortsel, Intersentia, 2019, .344p.
- VERHELST, I., VAN LOON, W. en CONIX, S., "gegevensbescherming in de HR-praktijk: een stand van zaken na één jaar GDPR", *Or.* 2019, nr. 5, p. 153-178.
- WILLEMS, A., "De beoordeling van de wetgevende kaders in Europa, China en de Verenigde Staten rond het gebruik van persoonsgegevens ter bestrijding van globale gezondheidscrisissen. Lessen uit de COVID-19-pandemie", *TPR* 2021, afl 4, 1729-1830.

D. Overige

- AGENTSCHAP DIGITAAL VLAANDEREN, *Identity and acces management (IAM)*, Brussel, 2017-2022, https://assets.vlaanderen.be/image/upload/v1648220287/Vo_Informatieclassificatie_-_Minimale_maatregelen_-_IAM_xle0xg.pdf, 31p.
- AGENTSCHAP DIGITAAL VLAANDEREN, Toegangsbeheer (ACM): nieuw authenticatiemiddel "myID.be", https://www.vlaanderen.be/digitaal-vlaanderen/nieuwsberichten/toegangsbeheer-acm-nieuw-authenticatiemiddel-myidbe.
- AGENTSCHAP DIGITAAL VLAANDEREN, *Het Vlaams Datanutsbedrijf gaat officieel van start onder de naam 'athumi'*, persbericht 5 mei 2023, https://www.vlaanderen.be/digitaal-vlaanderen/nieuwsberichten/het-vlaams-datanutsbedrijf-gaat-officieel-van-start-onder-de-naam-athumi.
- AKGHAR, B., KHAZAEI, B.,en ALQATAWNA, J., "Importance of service integration in e-government Implementations", in The 7th International Conference on Information and Communication Systems, Irbid, 2016, 1-7.
- BELGIAN Mobile ID, *de toekomst van digitale identiteit*, 1 juni 2020, https://www.itsme-id.com/nl-BE/business/blog/future-of-digital-id, laatst bezocht 9 maart 2023.
- BELGIAN MOBILE ID, *Algemene voorwaarden itsme app Versie 3.2*, Brussel, 2022, https://www.itsme-id.com/nl-BE/legal/app-terms-and-conditions, 11p., Laatst bezocht: 16 december 2022.
- BELGIAN Mobile ID, *Privacybeleid: Itsme app en diensten. Versie 3.1,* Brussel, 2022, https://www.itsme-id.com/nl-BE/legal/app-privacy-policy, 9p., laatst bezocht 16 december 2022.
- BOSA, *Gebruiksovereenkomst FAS. Versie 6.5*, 2022, https://bosa.belgium.be/sites/default/files/content/documents/DTdocs/FAS/GO_DT_FAS_6.5_20221005_NL.pdf, laatst bezocht 15 december 2022, 12p.
- BOURGEOIS, G., *Beleidsnota bestuurszaken 2004-2009*, 2004, https://overheid.vlaanderen.be/sites/bz.vlaanderen.be/files/documenten/Beleidsnota_bestuurszaken_2004.pdf, 12, laatst bezocht 9/12/2022.
- Mededeling (Comm.) betreffende de Rol van de elektronische overheid (eGovernment) voor de toekomst van Europa, 26 september 2003, COM(2003)567, https://www.eumonitor.nl/9353000/1/j4nvhdfcs8bljza_j9vvik7m1c3gyxp/vikqh0qi43zz
- CSAM, *Mijn digitale sleutels: wat zijn digitale sleutels,* https://iamapps.belgium.be/sma/generalinfo?view=digitalKeys, laatst bezocht: 8 januari 2023.

- DEWOLF, L., "Staatssecretaris van Digitalisering Mathieu Michel: "Itsme is sleutel, digitale portefeuille wordt volledig huis"", in *VRTNews,* 30 juni 2022, https://www.vrt.be/vrtnws/nl/2022/06/30/staatssecretaris-van-digitalisering-mathieu-michel-itsme-is-sl/, laatst bezocht 5/10/2022.
- EC, "Europa's digitaal decennium: doelstellingen voor 2030", https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_nl, laatst bezocht 5/10/2022.
- EDRI, *eIDAS policy paper*, 25 januari 2021, https://www.europarl.europa.eu/cmsdata/244763/eIDAS-policy%20paper-EW+EDRi.pdf, 6p.
- EPRS, *Revision of the eIDAS regulation, findings on its implementation and application,* 2022, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)699491, 12p.
- EUROPESE COMMISSIE, *Shaping Europe's digital future,* Luxemburg, Publications office of the European Union, 2020, 9p.
- EUROPESE COMMISSIE, *Verslag van de Commissie aan het Europees Parlement en de Raad over over de evaluatie van Verordening (EU) Nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (eIDAS)*, Brussel, 2021, 9p.
- EU, "Stelsels voor elektronische identificatie aangemeld overeenkomstig artikel 9, lid 1, 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", *Pb.L* 21 augustus 2020, afl 276, 2.
- FANG, Z., "E-government in digital era: Concept, Practice and Development", in *International Journal of the Computer, The internet and management*, 2002, afl 10, nr. 2, 1-22.
- FGOV, *Het begrip e-government*, https://economie.fgov.be/nl/themas/online/het-begrip-e-government, laatst bezocht 9/12/2022.
- FOD BOSA, *FAS gebruikersovereenkomst versie 6.7*, 7 februari 2023, https://bosa.belgium.be/sites/default/files/content/documents/DTdocs/FAS/FAS%20Gebruikersovereenkomst.pdf, 11p.
- S.S. GARCIA, A.G. OLIVA, E.P. BELLEBONI en I.P. DE LA CRUZ, "Current trends in Pan-European Identity Management Systems", *Technology and Society Magazine* 2012, vol. 31, afl. 3, https://pdfs.semanticscholar.org/ef04/650b114ea77a943e58dde761372493c5b750.pdf?_gl=1*1qxx0n4*_ga*NjU0NzU2MDA0LjE2ODM5Nzc5OTA.*_ga_H7P4ZT52H5*MTY4Mzk3Nzk4OS4xLjEuMTY4Mzk3ODAyOC4wLjAuMA, 7p.
- GBA, *Het afstaan van gegevens kan geen voorwaarde zijn voor toegang tot fiscale informatie,* Persbericht 4 juni 2020, https://www.gegevensbeschermingsautoriteit.be/burger/het-afstaan-van-gegevens-kan-geen-voorwaarde-zijn-voor-toegang-tot-fiscale-informatie.
- IBZ, *Rijksregister*, https://www.ibz.rrn.fgov.be/nl/rijksregister/, laatst bezocht 14 december 2022
- JAMBON, J., "Beleidsnota 2019-2024 – ICT en facilitair management", 8 november 2019, https://publicaties.vlaanderen.be/view-file/32229, laatst bezocht: 5/10/2022.

- M. KIROVA, *Overview of pre-notified and notified eID schemes under eIDAS*, laatste bijwerking: D. GATTWINKEL 24 januari 2023, https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS.
- MICHIELS, C., "Vlaanderen lanceert Athumi: bepalen we binnenkort zelf wat er met onze online data gebeurt?" in *VRTNieuws* 4 mei 2023, https://www.vrt.be/vrtnws/nl/2023/05/04/vlaanderen-lanceert-athumi-bepalen-we-binnenkort-zelf-wat-er-me/.
- SERV, "Startnota – De transitie naar een digitale samenleving", Brussel, 3 mei 2017, https://www.serv.be/sites/default/files/documenten/SERV_20170503_startnota_digitalisering_NOT_.pdf, laatst bezocht: 5/10/2022.
- U2U consult, *Privacy policy. Versie 2.0.1*, 2022, https://myid.be/privacy.
- VAN LEEMPUTTEN, P.J., "overheid werkt aan alternatief voor Itsme", *Datanews knack*, 2022, https://datanews.knack.be/ict/nieuws/overheid-werkt-aan-alternatief-voor-itsme/article-news-1879327.html, laatst bezocht: 8 januari 2023.
- VON DER LEYEN, U., *State of the Union 2020*, Brussel, 2020, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655, 15p.
- VVD, CDA, D66 en ChristenUnie, *Regeerakkoord 2017-2021: Vertrouwen in de toekomst*, 10 oktober 2017, https://www.eerstekamer.nl/overig/20171010/vertrouwen_in_de_toekomst/f=/vkicly3bt7yh.pdf, 73.
- WERELDBANK, *The E-government Handbook for developing countries: A project of InFODev and the Center for Democracy & Technology, 2002, 41p,* https://documents1.worldbank.org/curated/en/317081468164642250/pdf/320450egovhandbook01public12002111114.pdf, laatst bezocht: 8/12/2022.

Bijlage 1: Technische specificaties eIDAS

BIJLAGE

Technische specificaties en procedures voor de betrouwbaarheidsniveaus laag, substantieel en hoog betreffende op grond van een aangemeld stelsel voor elektronische identificatie uitgegeven elektronische identificatiemiddelen

1. Definities

Voor de toepassing van deze bijlage wordt verstaan onder:

1. „gezaghebbende bron": elke bron, ongeacht de vorm ervan, waarvan kan worden verwacht dat deze nauwkeurige gegevens, informatie of bewijsmateriaal biedt op basis waarvan een identiteit kan worden aangetoond;

2. „authenticatiefactor": een factor waarvan is bevestigd dat deze gebonden is aan een persoon en die onder een van de volgende categorieën valt:

   a) „op bezit gebaseerde authenticatiefactor": een authenticatiefactor waarvan de betrokkene moet aantonen dat deze in zijn bezit is;

   b) „op kennis gebaseerde authenticatiefactor": een authenticatiefactor waarvan de betrokkene moet aantonen dat hij ervan kennis draagt;

   c) „inherente authenticatiefactor": een authenticatiefactor die op een fysiek kenmerk van een natuurlijke persoon is gebaseerd en waarbij de betrokkene moet aantonen dat hij dat fysieke kenmerk bezit;

3. „dynamische authenticatie": een elektronisch proces, dat met gebruikmaking van cryptografie of een andere techniek de middelen biedt om op verzoek een elektronisch bewijs op te maken dat de betrokkene de controle heeft over of in het bezit is van de identificatiegegevens, en dat verandert telkens als authenticatie plaatsvindt tussen de betrokkene en het systeem dat diens identiteit verifieert;

4. „beheerssysteem voor informatiebeveiliging": een geheel van processen en procedures die zijn ontworpen om de informatieveiligheidsrisico's tot een aanvaardbaar niveau te beperken.

2. Technische specificaties en procedures

Aan de hand van de in deze bijlage beschreven elementen van de technische specificaties en procedures wordt bepaald op welke wijze de vereisten en criteria van artikel 8 van Verordening (EU) nr. 910/2014 worden toegepast op elektronische identificatiemiddelen die zijn uitgegeven op grond van een stelsel voor elektronische identificatie.

2.1. *Inschrijving*

2.1.1. Aanvraag en registratie

Betrouwbaarheids-niveau	Vereiste elementen
Laag	1. De aanvrager moet bekend zijn met de voorwaarden die aan het gebruik van het elektronische identificatiemiddel zijn verbonden. 2. De aanvrager moet bekend zijn met de aanbevolen veiligheidsvoorzorgen die aan het gebruik van het elektronische identificatiemiddel zijn verbonden. 3. De relevante identiteitsgegevens die voor het bewijs en de verificatie van de identiteit vereist zijn, moeten zijn verzameld.
Substantieel	Hetzelfde als niveau laag.
Hoog	Hetzelfde als niveau laag.

2.1.2. Bewijs en verificatie van identiteit (natuurlijke persoon)

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. De persoon kan worden verondersteld in het bezit te zijn van bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt. 2. Het bewijs kan worden verondersteld echt te zijn, dan wel volgens een gezaghebbende bron te bestaan, en het bewijs lijkt geldig te zijn. 3. Een gezaghebbende bron weet dat de opgegeven identiteit bestaat en er kan worden verondersteld dat de persoon die de identiteit opgeeft, dezelfde persoon is.
Substantieel	Niveau laag plus een van de onder de punten 1 tot en met 4 vermelde alternatieven. 1. Er is geverifieerd dat de persoon in het bezit is van bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt; en het bewijs is gecontroleerd op de echtheid ervan; of het bestaan ervan is volgens een gezaghebbende bron bekend en het heeft betrekking op een werkelijk bestaande persoon; en er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat het bewijsstuk verloren, gestolen, geschorst, ingetrokken of verlopen is. of 2. Er is een identiteitsdocument overgelegd tijdens een registratieproces in de lidstaat waar het document is afgegeven, en het document lijkt betrekking te hebben op de persoon die het heeft overgelegd; en er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat documenten verloren, gestolen, geschorst, ingetrokken of verlopen zijn. of 3. Indien procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.2 voor het betrouwbaarheidsniveau substantieel, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad ([1]) of een daaraan gelijkwaardige instantie. of 4. Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel of hoog, is het, rekening houdend met het risico van een wijziging van de persoonsidentificatiegegevens, niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau substantieel of hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie.

Betrouwbaarheidsniveau	Vereiste elementen
Hoog	Er moet zijn voldaan aan de vereisten van punt 1 of punt 2. 1. Niveau substantieel plus een van de onder a) tot en met c) vermelde alternatieven. a) Indien is geverifieerd dat de persoon in het bezit is van een bewijs dat voorzien is van een foto of biometrische gegevens, dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt, wordt het bewijs gecontroleerd op geldigheid aan de hand van een gezaghebbende bron; en de door de aanvrager opgegeven identiteit wordt geverifieerd door vergelijking van één of meer fysieke kenmerken van de persoon met een gezaghebbende bron. of b) Indien procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.2 voor het betrouwbaarheidsniveau hoog, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie; en er zijn maatregelen getroffen om aan te tonen dat de resultaten van de eerdere procedures nog steeds geldig zijn. of c) Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau hoog, is het, rekening houdend met het risico van een wijziging van de persoonsidentificatiegegevens, niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie. en er zijn maatregelen getroffen om aan te tonen dat de resultaten van deze eerdere uitgifteprocedure van een aangemeld elektronisch identificatiemiddel nog steeds geldig zijn. OF 2. Indien de aanvrager geen erkend identiteitsdocument met een foto of biometrische kenmerken overlegt, worden dezelfde procedures toegepast die op nationaal niveau van toepassing zijn in de lidstaat van de verantwoordelijke instantie voor de verkrijging van een dergelijk bewijsstuk met foto of biometrische kenmerken.

([1]) Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 (PB L 218 van 13.8.2008, blz. 30).

2.1.3. Bewijs en verificatie van identiteit (rechtspersoon)

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. De opgegeven identiteit van de rechtspersoon wordt aangetoond aan de hand van een bewijsstuk dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan.

Betrouwbaarheidsniveau	Vereiste elementen
	2. Het bewijsstuk lijkt geldig en kan worden verondersteld echt te zijn dan wel volgens een gezaghebbende bron te bestaan, indien de rechtspersoon op vrijwillige basis in de gezaghebbende bron is opgenomen op basis van een regeling tussen de rechtspersoon en de gezaghebbende bron. 3. De rechtspersoon bevindt zich volgens een gezaghebbende bron niet in een toestand die verhindert dat zij als die rechtspersoon optreedt.
Substantieel	Niveau laag plus een van de onder de punten 1 tot en met 3 vermelde alternatieven. 1. De opgegeven identiteit van de rechtspersoon wordt aangetoond aan de hand van een bewijsstuk dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, inclusief de naam, de rechtsvorm en (indien van toepassing) het registratienummer van de rechtspersoon; en het bewijsstuk wordt gecontroleerd om te bepalen of het echt is dan wel volgens een gezaghebbende bron bestaat, indien de rechtspersoon in de gezaghebbende bron is opgenomen omdat dat voor de rechtspersoon verplicht is om in de betrokken sector actief te mogen zijn; en er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de rechtspersoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat documenten verloren, gestolen, geschorst, ingetrokken of verlopen zijn. of 2. Indien de procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.3 voor het betrouwbaarheidsniveau substantieel, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie. of 3. Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel of hoog, is het niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau substantieel of hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie.
Hoog	Niveau substantieel plus een van de onder de punten 1 tot en met 3 vermelde alternatieven. 1. De opgegeven identiteit van de rechtspersoon wordt aangetoond aan de hand van een bewijsstuk dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, inclusief de naam en de rechtsvorm van de rechtspersoon en ten minste één in een nationale context gebruikte unieke identificatiecode die de rechtspersoon vertegenwoordigt; en het bewijs is gecontroleerd om de geldigheid ervan volgens een gezaghebbende bron te bepalen. of

Betrouwbaarheidsniveau	Vereiste elementen
	2. Indien de procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.3 voor het betrouwbaarheidsniveau hoog, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie; en er zijn maatregelen getroffen om aan te tonen dat de resultaten van deze eerdere procedure nog steeds geldig zijn. of 3. Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau hoog, is het niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie; en er zijn maatregelen getroffen om aan te tonen dat de resultaten van deze eerdere uitgifteprocedure van een aangemeld elektronisch identificatiemiddel nog steeds geldig zijn.

2.1.4. Koppeling tussen de elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen

Indien van toepassing gelden de volgende voorwaarden voor de koppeling tussen het elektronische identificatiemiddel van een natuurlijke persoon en het elektronische identificatiemiddel van een rechtspersoon:

1. Het moet mogelijk zijn een koppeling te schorsen en/of te herroepen. De verschillende koppelingsstadia (o.a. activering, schorsing, hernieuwing, herroeping) worden beheerd volgens op nationaal niveau erkende procedures.

2. De natuurlijke persoon wiens elektronische identificatiemiddel is gekoppeld aan het elektronische identificatiemiddel van de rechtspersoon kan volgens op nationaal niveau erkende procedures de uitoefening van de koppeling delegeren aan een andere natuurlijke persoon. De delegerende natuurlijke persoon blijft echter aansprakelijk.

3. De koppeling wordt op de volgende wijze uitgevoerd:

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Er is geverifieerd dat het bewijs van de identiteit van de natuurlijke persoon die namens de rechtspersoon optreedt, heeft plaatsgevonden op het niveau laag of hoger. 2. De koppeling is tot stand gebracht volgens op nationaal niveau erkende procedures. 3. De natuurlijke persoon bevindt zich volgens een gezaghebbende bron niet in een toestand die verhindert dat hij namens die rechtspersoon optreedt.
Substantieel	Punt 3 van niveau laag, plus: 1. er is geverifieerd dat het bewijs van de identiteit van de natuurlijke persoon die namens de rechtspersoon optreedt, heeft plaatsgevonden op het niveau substantieel of hoog;

Betrouwbaarheidsniveau	Vereiste elementen
	2. de koppeling is tot stand gebracht volgens op nationaal niveau erkende procedures, wat ertoe heeft geleid dat de koppeling in een gezaghebbende bron is geregistreerd; 3. de koppeling is geverifieerd op basis van informatie uit een gezaghebbende bron.
Hoog	Punt 3 van niveau laag en punt 2 van niveau substantieel, plus: 1. er is geverifieerd dat het bewijs van de identiteit van de natuurlijke persoon die namens de rechtspersoon optreedt, heeft plaatsgevonden op het niveau hoog; 2. de koppeling is geverifieerd op basis van een in een nationale context gebruikte unieke identificatiecode die de rechtspersoon vertegenwoordigt, en op basis van uit een gezaghebbende bron afkomstige informatie die op unieke wijze een natuurlijke persoon vertegenwoordigt.

2.2. *Beheer van elektronische identificatiemiddelen*

2.2.1. Kenmerken en ontwerp van elektronische identificatiemiddelen

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Het elektronische identificatiemiddel maakt gebruik van ten minste één authenticatiefactor. 2. Het elektronische identificatiemiddel is zodanig ontworpen dat de uitgever ervan redelijke stappen onderneemt om te verifiëren dat het slechts wordt gebruikt door of onder controle van de persoon aan wie het toebehoort.
Substantieel	1. Het elektronische identificatiemiddel maakt gebruik van ten minste twee authenticatiefactoren die tot verschillende categorieën behoren. 2. Het elektronische identificatiemiddel is zodanig ontworpen dat het kan worden verondersteld slechts te worden gebruikt door of onder controle van de persoon aan wie het toebehoort.
Hoog	Niveau substantieel, plus: 1. Het elektronische identificatiemiddel biedt bescherming tegen kopiëring en vervalsing en tegen aanvallers met een hoog aanvalspotentieel. 2. Het elektronische identificatiemiddel is zodanig ontworpen dat het door de persoon aan wie het toebehoort op betrouwbare wijze kan worden beschermd tegen gebruik door anderen.

2.2.2. Uitgifte, uitreiking en activering

Betrouwbaarheidsniveau	Vereiste elementen
Laag	Na de uitgifte wordt het elektronische identificatiemiddel uitgereikt via een mechanisme waarmee het kan worden verondersteld alleen de beoogde persoon te bereiken.
Substantieel	Na de uitgifte wordt het elektronische identificatiemiddel uitgereikt via een mechanisme waarmee kan worden verondersteld dat alleen de persoon aan wie het toebehoort in het bezit ervan wordt gesteld.
Hoog	Bij het activeringsproces wordt geverifieerd dat slechts de persoon aan wie het elektronische identificatiemiddel toebehoort ervan in het bezit wordt gesteld.

2.2.3. Schorsing, herroeping en reactivering

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Het is mogelijk het elektronische identificatiemiddel snel en doeltreffend te schorsen en/of te herroepen. 2. Er bestaan maatregelen om ongeoorloofde schorsing, herroeping en reactivering te voorkomen. 3. Een elektronisch identificatiemiddel mag slechts worden gereactiveerd indien nog steeds wordt voldaan aan dezelfde betrouwbaarheidsvereisten als die welke voorafgaand aan de schorsing of herroeping van kracht waren.
Substantieel	Zelfde als niveau laag.
Hoog	Zelfde als niveau laag.

2.2.4. Verlenging en vervanging

Betrouwbaarheidsniveau	Vereiste elementen
Laag	Rekening houdend met het risico dat de persoonsidentificatiegegevens zijn gewijzigd, moet voor verlenging of vervanging aan dezelfde betrouwbaarheidsvereisten zijn voldaan als voor het initiële proces van bewijs en verificatie van de identiteit, of moet worden uitgegaan van een geldig elektronisch identificatiemiddel met hetzelfde of een hoger betrouwbaarheidsniveau.
Substantieel	Zelfde als niveau laag.
Hoog	Niveau laag, plus: Als voor verlenging of vervanging wordt uitgegaan van een geldig elektronisch identificatiemiddel, worden de identiteitsgegevens geverifieerd aan de hand van een gezaghebbende bron.

2.3. *Authenticatie*

Dit onderdeel is met name gericht op dreigingen die gepaard gaan met het gebruik van het authenticatiemechanisme. Het vermeldt de vereisten voor elk van de betrouwbaarheidsniveaus. In dit onderdeel wordt ervan uitgegaan dat de controles in overeenstemming zijn met de risico's op het desbetreffende niveau.

2.3.1. Authenticatiemechanisme

In onderstaande tabel worden voor elk betrouwbaarheidsniveau de vereisten weergegeven voor het authenticatiemechanisme, door middel waarvan de natuurlijke persoon of rechtspersoon het elektronische identificatiemiddel gebruikt om zijn identiteit te bevestigen tegenover een vertrouwende partij.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Alvorens persoonsidentificatiegegevens worden vrijgegeven, worden het elektronische identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd. 2. Indien als onderdeel van het authenticatiemechanisme persoonsidentificatiegegevens worden opgeslagen, wordt die informatie beveiligd ter bescherming tegen verlies en schending, met inbegrip van offlineanalyse. 3. Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een laag aanvalspotentieel.

Betrouwbaarheidsniveau	Vereiste elementen
Substantieel	Niveau laag, plus: 1. Alvorens persoonsidentificatiegegevens worden vrijgegeven, worden het elektronische identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd door middel van dynamische authenticatie. 2. Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een gematigd aanvalspotentieel.
Hoog	Niveau substantieel, plus: Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een hoog aanvalspotentieel.

2.4. *Beheer en organisatie*

Alle deelnemers die een dienst verlenen op het gebied van elektronische identificatie in een grensoverschrijdende context (hierna „aanbieders" genoemd) beschikken over gedocumenteerde methoden en beleid voor het beheer van informatiebeveiliging, benaderingen voor risicobeheersing en andere erkende controlemethoden, zodat zij de bevoegde bestuursorganen van de lidstaten op het gebied van stelsels voor elektronische identificatie garanties kunnen bieden dat in doeltreffende praktijken is voorzien. In onderdeel 2.4 wordt ervan uitgegaan dat alle vereisten/elementen in overeenstemming zijn met de risico's op het desbetreffende niveau.

2.4.1. Algemene bepalingen

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Aanbieders die een operationele dienst aanbieden die onder deze verordening valt, zijn een overheidsinstantie of een rechtspersoon die door het nationale recht van een lidstaat als zodanig wordt erkend, over een gevestigde organisatie beschikt en volledig operationeel is op alle gebieden die voor de verlening van de diensten relevant zijn. 2. De aanbieders voldoen aan al hun wettelijke verplichtingen in verband met het verrichten en leveren van de dienst, onder meer wat betreft de soorten informatie die mogen worden gevraagd, de wijze waarop het bewijs van de identiteit wordt geleverd, welke informatie mag worden bewaard en hoe lang deze mag worden bewaard. 3. De aanbieders kunnen aantonen dat zij in staat zijn het risico van de aansprakelijkheid voor schade op zich te nemen en over voldoende financiële middelen beschikken om hun activiteiten en de dienstverlening voort te zetten. 4. De aanbieders zijn verantwoordelijk voor het naleven van alle verplichtingen die zij aan andere entiteiten hebben uitbesteed en voor het voldoen aan het beleid inzake het stelsel, op dezelfde wijze als wanneer zij deze taken zelf vervulden. 5. Stelsels voor elektronische identificatie die niet volgens nationaal recht zijn opgezet, moeten over een doeltreffend beëindigingsplan beschikken. Dat plan omvat voorzieningen voor de ordelijke stopzetting van de dienstverlening of de voortzetting daarvan door een andere aanbieder, voor de wijze waarop de betrokken autoriteiten en eindgebruikers worden ingelicht, alsook voor de wijze waarop de administratie wordt beschermd, bewaard en vernietigd overeenkomstig het voor het stelsel geldende beleid.
Substantieel	Zelfde als niveau laag.
Hoog	Zelfde als niveau laag.

2.4.2. Gepubliceerde mededelingen en informatie voor de gebruikers

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Er bestaat een gepubliceerde beschrijving van de dienst met alle toepasselijke voorwaarden en vergoedingen, inclusief eventuele gebruiksbeperkingen. De beschrijving van de dienst omvat een privacyverklaring. 2. Er dient te worden voorzien in passend beleid en passende procedures om de gebruikers van de dienst tijdig en op betrouwbare wijze te informeren over elke wijziging van de beschrijving van de dienst, alle toepasselijke voorwaarden en de privacyverklaring. 3. Er dient te worden voorzien in passend beleid en passende procedures om verzoeken om informatie volledig en correct te beantwoorden.
Substantieel	Zelfde als niveau laag.
Hoog	Zelfde als niveau laag.

2.4.3. Beheer van informatiebeveiliging

Betrouwbaarheidsniveau	Vereiste elementen
Laag	Er bestaat een doeltreffend beheerssysteem voor informatiebeveiliging dat zorg draagt voor het beheer en de beheersing van informatiebeveiligingsrisico's.
Substantieel	Niveau laag, plus: Het beheerssysteem voor informatiebeveiliging voldoet aan beproefde normen en beginselen voor het beheer en de beheersing van informatiebeveiligingsrisico's.
Hoog	Zelfde als niveau substantieel.

2.4.4. Bijhouden van de administratie

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Relevante informatie wordt vastgelegd en bewaard met behulp van een doeltreffend documentenbeheersysteem, met inachtneming van de toepasselijke wetgeving en goede praktijken op het gebied van gegevensbescherming en gegevensbewaring. 2. De gegevens moeten worden bewaard voor zover dat is toegestaan door het nationale recht of een andere nationale bestuurlijke regeling, en beschermd gedurende de termijn die noodzakelijk is met het oog op financiële controle en onderzoek van beveiligingsinbreuken; na afloop van de bewaringstermijn worden de gegevens veilig vernietigd.
Substantieel	Zelfde als niveau laag.
Hoog	Zelfde als niveau laag.

2.4.5. Faciliteiten en personeel

Onderstaande tabel bevat de vereisten inzake faciliteiten alsmede inzake personeelsleden en eventuele subcontractanten die taken uitvoeren die onder deze verordening vallen. Aan elk van de vereisten moet worden voldaan in verhouding tot het risiconiveau waarmee het desbetreffende betrouwbaarheidsniveau gepaard gaat.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Er zijn procedures om te waarborgen dat personeelsleden en subcontractanten voldoende zijn opgeleid en gekwalificeerd en dat zij ervaren zijn in de vaardigheden die vereist zijn voor de taken die zij vervullen. 2. Er zijn voldoende personeelsleden en subcontractanten om de dienstverlening voldoende te waarborgen overeenkomstig het beleid en de procedures. 3. De voor de dienstverlening gebruikte faciliteiten staan onder permanente controle en worden permanent beschermd tegen schade door milieu-invloeden, ongeoorloofde toegang en andere factoren die de veiligheid van de dienst kunnen aantasten. 4. De voor de dienstverlening gebruikte faciliteiten zijn zodanig ingericht dat de toegang tot zones met persoonsgegevens, cryptografische gegevens en andere gevoelige informatie beperkt is tot bevoegde personeelsleden of subcontractanten.
Substantieel	Zelfde als niveau laag.
Hoog	Zelfde als niveau laag.

2.4.6. Technische controles

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Er is voorzien in proportionele controles ter beheersing van de risico's voor de veiligheid van de diensten, waarbij de vertrouwelijkheid, integriteit en beschikbaarheid van de verwerkte informatie worden beschermd. 2. De elektronische communicatiekanalen die voor de uitwisseling van persoonsgegevens en gevoelige gegevens worden gebruikt, worden beschermd tegen afluisteren, manipuleren en herafspelen. 3. De toegang tot gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, is beperkt tot de uitoefening van taken en toepassingen waarvoor de toegang strikt noodzakelijk is. Er wordt op toegezien dat dergelijk materiaal niet permanent in onversleutelde staat wordt opgeslagen. 4. Er zijn procedures die waarborgen dat de veiligheid duurzaam wordt gehandhaafd en dat een respons mogelijk is op wijzigingen van het risiconiveau, incidenten en veiligheidsinbreuken. 5. Alle media die persoonsgegevens, cryptografische informatie of andere gevoelige informatie bevatten, worden veilig opgeslagen, vervoerd en verwijderd.
Substantieel	Zelfde als niveau laag, plus: Gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, wordt beschermd tegen ongeoorloofde manipulatie.
Hoog	Zelfde als niveau substantieel.

2.4.7. Compliance en audit

Betrouwbaarheidsniveau	Vereiste elementen
Laag	Er vinden periodieke interne audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn, teneinde de naleving van het desbetreffende beleid te waarborgen.

Betrouwbaarheids-niveau	Vereiste elementen
Substantieel	Er vinden periodieke onafhankelijke interne of externe audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn, teneinde de naleving van het desbetreffende beleid te waarborgen.
Hoog	1. Er vinden periodieke onafhankelijke externe audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn, teneinde de naleving van het desbetreffende beleid te waarborgen. 2. Indien een stelsel wordt beheerd door een overheidsinstantie, vinden audits plaats overeenkomstig het nationaal recht.