Advies nr 18/2017 van 12 april 2017

Betreft: 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)

De Commissie voor de bescherming van de persoonlijke levenssfeer (hierna "de Commissie");

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 29;

Gelet op het verzoek om advies van de heer Jan DEPREST, voorzitter van de Federale Overheidsdienst ICT ontvangen op 10 februari 2017;

Gelet op het verslag van de heer Ivan VANDERMEERSCH;

Brengt op 12 april 2017 het volgend advies uit:

De Commissie vestigt er de aandacht op dat er recent nieuwe Europese regelgeving inzake de bescherming persoonsgegevens werd uitgevaardigd: de algemene Verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (hierna AVG) en de Richtlijn voor Politie en Justitie Deze teksten verschenen in het Europese Publicatieblad van 4 mei 2016[1].

De verordening, meestal GDPR (general data protection regulation) genaamd, is van kracht geworden twintig dagen na publicatie, nl. op 24 mei 2016 en wordt, twee jaar later, automatisch van toepassing: 25 mei 2018. De richtlijn voor politie en justitie moet via nationale wetgeving omgezet worden tegen uiterlijk 6 mei 2018.

Voor de Verordening betekent dit dat vanaf 24 mei 2016, en gedurende de termijn van twee jaar voor de tenuitvoerlegging, op de lidstaten enerzijds een positieve verplichting rust om alle nodige uitvoeringsbepalingen te nemen en anderzijds ook een negatieve verplichting, de zogenaamde “onthoudingsplicht”. Laatstgenoemde plicht houdt in dat er geen nationale wetgeving mag worden uitgevaardigd die het door de Verordening beoogde resultaat ernstig in gevaar zou brengen. Ook voor de Richtlijn gelden gelijkaardige principes.

Het verdient dan ook aanbeveling om desgevallend nu reeds op deze teksten te anticiperen. En het is in de eerste plaats aan de adviesaanvrager(s) om hier rekening mee te houden in zijn (hun) voorstellen of ontwerpen. De Commissie heeft in onderhavig advies, in de mate van het mogelijke en onder voorbehoud van mogelijke bijkomende toekomstige standpunten, alvast gewaakt over de hoger geschetste negatieve verplichting.

I. CONTEXT

1. Het 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, hierna het ontwerp, beoogt uitvoering te geven aan artikel 12 van de - nog uit te vaardigen - wet inzake elektronische identificatie. Het voorontwerp van wet inzake elektronische identificatie, hierna het voorontwerp van wet, maakt het voorwerp uit van advies nr. 48/2016 van 21

---

[1] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)

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

http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L:2016:119:TOC

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC)

september 2016 van de Commissie. Op 16/02/2017 werd een nieuwe versie van het voorontwerp van wet dd. 20 december 2016 meegedeeld, daterend van na het advies van de Commissie.

2. Het ontwerp past in het luik van het voorontwerp van wet dat, voor wat België betreft, de elektronische identificatie voor overheidstoepassingen juridisch onderbouwt, waaronder de erkenning van diensten voor elektronische identificatie. Artikel 12 van het voorontwerp van wet biedt de mogelijkheid toegang te verkrijgen tot digitale overheidstoepassingen op basis van een dienst voor elektronische identificatie, geleverd door spelers die geen openbare instanties zijn.

3. Elektronische identificatie geschiedt via digitale systemen en gaat gepaard met de geautomatiseerde verwerking van persoonsgegevens. De bepalingen van de WVP zijn er dus van toepassing. De analyse beperkt zich tot de artikelen welke betrekking hebben op de verwerking van persoonsgegevens.

II. ONDERZOEK TEN GRONDE

Voorafgaande opmerking

4. Het zijn de beheerders van digitale overheidstoepassingen die de verantwoordelijke voor de verwerking zijn in de zin van art. 1, § 4 WVP. Samen met de verwerkers waarop zij beroep doen, dienen zij de veiligheid van de persoonsgegevens te waarborgen aan de hand van gepaste technische en organisatorische maatregelen (art. 16, § 4 WVP).

5. De rol van Fedict (de federale overheidsdienst Informatie- en Communicatietechnologie, sinds 1 maart 2017 overgenomen door de Federale Overheidsdienst Beleid en Ondersteuning[1]), is onder meer een gemeenschappelijke authenticatiedienst ("Federal Authentication Service" of "FAS") uit te baten. Deze dienst is een essentiële basis om administraties, burgers en ondernemingen in de praktijk in staat te stellen informatie- en communicatietechnologie te gebruiken voor digitale overheidstoepassingen.

6. Uit het ontwerp leidt de Commissie af dat wanneer Fedict een erkenning verstrekt aan een dienstverlener, al naar gelang voor een aanmeldoptie met het niveau hoog of het niveau substantieel, de erkende authenticatiedienst automatisch opgenomen wordt binnen dat niveau in de FAS. Concreet zou dit inhouden dat alle digitale overheidstoepassingen die gebruik maken van de FAS dan automatisch deze erkende aanmeldoptie dienen te aanvaarden voor hun toepassingen ingedeeld in het overeenkomstig niveau (substantieel of hoog).

7. De Commissie erkent dat grondige analyse door Fedict waarborgen biedt inzake de veiligheid op een bepaald niveau van de erkende aanmeldopties. Tegelijk stelt de Commissie vast dat de beheerders van digitale overheidstoepassingen formeel slechts één gelegenheid krijgen een standpunt in te nemen in de procedure, meer bepaald in het kader van de consultatie van het College van voorzitters van de Federale en Programmatorische Overheidsdiensten, van het College van

[1] K.B. van 22 februari 2017 *houdende oprichting van de Federale Overheidsdienst Beleid en Ondersteuning.*

afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut, voorafgaand aan de erkenning (artikel 12 voorontwerp van wet). Onvermijdelijk wordt dan de vraag of de beheerders van digitale overheidstoepassingen op basis van een risico-analyse en, in bepaalde sectoren, in overleg met de gebruikers van de diensten alsnog de mogelijkheid behouden te beslissen over welke erkende aanmeldopties zij aanvaarden binnen een bepaalde context. De aard van de te beveiligen gegevens en de potentiële risico's wordt immers expliciet genoemd in artikel 16, § 4 WVP bij het bepalen van de te nemen beveiligingsmaatregelen. De vraag stelt zich overigens of het ontwerp voldoend rekening houdt met artikel 28(2) AVG, dat luidt als volgt:

> *"De verwerker neemt geen andere verwerker in dienst zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke. In het geval van algemene schriftelijke toestemming licht de verwerker de verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken."*

8. De beveiligingsplicht die rust op de verantwoordelijke voor de verwerking houdt eveneens rekening met de stand van de techniek terzake en de kosten voor het toepassen van de maatregelen (art. 16, § 4 WVP). De Commissie stelt evenwel vast dat de beheerder van de digitale overheidstoepassing in het ontwerp geen zekerheid krijgt over de financiële consequenties van de erkenning van een aanmeldoptie. Het ontwerp stelt dat het gebruik van de aanmeldoptie voor de gebruiker gratis is (artikel 42 van het ontwerp). Verder delegeert het de bevoegdheid aan de minister bevoegd voor Digitale Agenda om een vergoedingsmodel vast te leggen om de kosten die worden gemaakt om verbinding te maken met de federale authenticatiedienst te dekken. Minstens zou het ontwerp duidelijkheid moeten verschaffen of voormelde vergoeding de enige vergoeding inhoudt voor het gebruik van die erkende aanmeldoptie, met de zekerheid dat van beheerders van overheidstoepassingen geen bijkomende bijdrage verwacht wordt en dit ongeacht het aantal transacties met hun toepassing. Bij gebrek aan zekerheid hierover is het risico reëel dat beheerders de voorkeur geven aan niet-erkende aanmeldopties – waarvan de kosten vooraf berekenbaar zijn – boven erkende aanmeldopties die een minimum niveau van veiligheid waarborgen, maar waarvan de kosten niet kunnen ingeschat worden. Dit zou het opzet van het ontwerp ondermijnen.

9. Bij al het voorgaande moet overigens genoteerd worden dat de FAS niet alleen wordt gebruikt door overheidsdiensten in strikte zin, maar door andere actoren in bepaalde sectoren die veelvuldig in contact treden met digitale overheidsdiensten (bv. in de sociale sector, de gezondheidssector, de advocatuur, …).

Artikel 8 van het ontwerp

10. Artikel 8 van het ontwerp verwijst voor de registratieprocedure naar de vereisten voor het bewijs en verificatie van de identiteit omschreven in punt 2.1 van de bijlage van de uitvoeringsverordening (EU) nr. 2015/1502.

11. Het is van belang dat erkende authenticatiediensten gebaseerd zijn op degelijke registratieprocedures. Registratieprocedures die gebaseerd zijn op verificatie van de identiteit aan de hand van de eID, voldoen zonder meer aan voormelde vereisten. De overgrote meerderheid van de mensen die nood hebben aan toegang tot overheidsdiensten beschikken over een eID.

12. De uitvoeringsverordening (EU) nr. 2015/1502 legt noch voor het niveau hoog, noch voor het niveau substantieel op dat beroep gedaan wordt op de eID. Om bij de gebruikers een gelijkaardig niveau van vertrouwen te wekken, dient het ontwerp voor registratieprocedures zonder inzet van de eID (dit wil zeggen hetzij door de betrokkene zelf, hetzij via een tussenpersoon) per niveau - hoog dan wel substantieel – specifiekere vereisten te op te leggen dan deze omschreven in punt 2.1 van de bijlage van de uitvoeringsverordening nr. 2015/1502. In het bijzonder is de Commissie van oordeel dat de aansprakelijkheid van de registratie-autoriteit in dergelijke gevallen duidelijk moet worden beschreven in de erkenningsvoorwaarden.

Artikelen 9 en 10 van het ontwerp

13. Het ontwerp garandeert in artikel 9 de keuzevrijheid van de gebruiker om zijn keuze voor de dienst voor elektronische identificatie te wijzigen of stop te zetten. Artikel 10 voegt hieraan toe dat de keuze voor één erkende dienst voor elektronische identificatie de gebruiker niet verhindert ook van andere diensten gebruik te maken.

14. De Commissie wijst erop dat deze keuzevrijheid slechts effectief kan uitgeoefend worden voor zover de overheid bruikbare aanmeldopties aanbiedt voor toegang tot digitale overheidstoepassingen. De Commissie is van oordeel dat het inderdaad niet opgaat gebruikers te binden aan één dienst.

Artikel 11 van het ontwerp

15. Artikel 11 van het ontwerp bepaalt:

> *"De dienst voor elektronische identificatie stuurt de erkennende overheid bij elke aanmelding het uniek identificatienummer van de gebruiker, op basis waarvan de erkennende overheid de identiteit van de gebruiker vaststelt."*

16. Het uniek identificatienummer is hetzij het Rijksregisternummer of het kruispuntbanknummer licht de memorie toe. Artikel 4 § 1 van de wet van 5 mei 2014 betreffende de unieke gegevensinzameling[2] verplicht federale instanties om bij de uitvoering van hun opdrachten het

[2] Wet van 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.*

rijksregisternummer te gebruiken voor de identificatie van natuurlijke personen. Aan personen die niet beschikken over een rijksregisternummer kan een kruispuntbanknummer toegekend worden.

17. Alhoewel artikel 12, § 2, van het voorontwerp van wet de Koning belast met het bepalen van de procedure, de voorwaarden en de gevolgen van de erkenning, worden er enkele aspecten op ondubbelzinnige wijze in artikel 12, § 5, van het voorontwerp van wet geregeld. In de eerste plaats wordt uitdrukkelijk bepaald dat de aanbieder van een erkende dienst voor elektronische identificatie door het feit van erkenning - in hoedanigheid van onderaannemer van Fedict - gemachtigd is om het Rijksregisternummer te gebruiken. Het voorontwerp van wet voert bijgevolg een wettelijke uitzondering in op artikel 8 van de wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen* die bepaalt dat de machtiging om het Rijksregisternummer te gebruiken wordt verleend door het sectoraal comité van het Rijksregister.

18. De omschrijving van het doeleinde waarvoor de erkende dienst voor elektronische identificatie het uniek identificatienummer mag gebruiken komt aan bod in artikel 17 van het ontwerp.

Artikel 12 van het ontwerp

19. Artikel 12 van het ontwerp bepaalt:

> *"De informatie-uitwisseling tussen de dienstverlener en de erkennende overheid in het kader van de dienst voor elektronische identificatie geschiedt overeenkomstig de technische protocollen zoals uiteengezet in de technische specificaties."*

20. De Commissie is van oordeel dat de technische specificaties gepaste vereisten moeten omschrijven voor de beveiliging van de informatie-uitwisseling (conform artikel 16, § 4 WVP[3]).

Artikel 13 van het ontwerp

21. Het ontwerp legt de dienstverlener op om maatregelen te nemen inzake beveiliging van de aanmeldoptie. Drie specifieke veiligheidsrisico's worden genoemd.

> *"§ 1. Bij iedere informatie-uitwisseling tussen de erkennende overheid en de dienstverlener alsook tussen de dienstverlener en de gebruiker voert de dienst voor elektronische identificatie controles uit om ten minste de onderstaande misbruiken tegen te gaan:*
>
> *1. een nieuwe verzending van eenzelfde boodschap of aanmeldingspoging;*
>
> *2. een wijziging van de inhoud van de uitgewisselde informatie; en*
>
> *3. een derde partij die zich voordoet als de operationele dienst of als dienstverlener.*

---

[3] Art. 16, § 4 WVP bepaalt "*Om de veiligheid van de persoonsgegevens te waarborgen, (moeten de verantwoordelijke van de verwerking, en in voorkomend geval zijn vertegenwoordiger in België, alsmede de verwerker, de gepaste technische en organisatorische maatregelen treffen die nodig zijn voor de bescherming van de persoonsgegevens) tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.*"

§ 2. De in paragraaf 1 vermelde misbruiken worden gedetecteerd en leiden tot het falen van de aanmelding.

§ 3 De dienst voor elektronische identificatie omvat voldoende controlemechanismen om eventuele veiligheidsrisico's proactief op te sporen. De dienstverlener rapporteert hierover overeenkomstig de procedure omschreven in onderafdeling 5 van afdeling 2."

22. De term "veiligheidsrisico's" omvat "*aanvallen; inbraak, zowel fysisch als elektronisch; reputatie- en imagoschade en alle mogelijke schade die een negatieve impact kan hebben op de dienstverlening*" (artikel 1, 13° van het ontwerp).

23. Waar artikel 33 AVG) inzake melding van "inbreuken in verband met persoonsgegevens" van toepassing is, zal de dienstverlener eveneens bepaalde meldingen dienen te maken aan de toezichthoudende autoriteit, naast de plicht tot melding aan de erkennende overheid (artikel 25 van het ontwerp). De Commissie stelt vast dat het begrip "veiligheidsrisico" minstens ten dele overlapt met de notie van "inbreuk in verband met persoonsgegevens", namelijk een "*inbreuk op de beveiliging* (in de zin van incident) *die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens"* (art. 4, 12° AVG).

24. De verwijzing naar reputatie- en imagoschade in de definitie van veiligheidsrisico maakt duidelijk dat de doelstelling van het ontwerp onder meer is het vertrouwen van de gebruikers en de overheidsdiensten die gebruik maken van de dienst te vrijwaren.

25. Het bijhouden van logbestanden is een maatregel om te kunnen rapporteren over de mate waarin veiligheidsrisico's zich gerealiseerd hebben – concreet wanneer de detectie van misbruik geleid heeft tot het falen van de aanmelding (artikel 13, § 2 ontwerp). De Commissie stelt evenwel vast dat de verplichting om controlesporen bij te houden uitsluitend geldt voor transacties, zijnde elke succesvolle aanmelding door middel van een erkende dienst voor elektronische identificatie. Deze controlesporen dienen 10 jaar lang bewaard te worden (artikel 16, § 2 van het ontwerp), een termijn die aldus de memorie gebaseerd is op de gemeenrechtelijke verjaringstermijnen.

26. De Commissie is van oordeel dat de erkennende overheid in een samenwerkingsovereenkomst afspraken moet maken met de dienstverleners over het bewaren van controlesporen van gefaalde meldingen met het oog op het beheersen van veiligheidsrisico's.

Artikel 14 van het ontwerp

27. Artikel 14 van het ontwerp luidt als volgt:

"De dienstverlener wendt de persoonsgegevens enkel aan voor de dienstverlening. De dienstverlener zal de persoonsgegevens verwerken in overeenstemming met de bepalingen van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, de uitvoeringsbesluiten en de richtlijnen en aanbevelingen van de Commissie voor de bescherming van de persoonlijke levenssfeer als ook de Europese Verordening (EU)

> *2016/679 van het Europees parlement en de raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG."*

28. De eerste zin legt een beperking op aan verwerking van persoonsgegevens door dienstverleners die, op het eerste zicht, strenger is dan artikel 4, § 1, 2° WVP. Het ontwerp beoogt dienstverleners toe te laten om aanmeldopties die zij ontwikkeld hebben voor toegang tot hun eigen diensten ook in te zetten voor hun gebruikers als aanmeldoptie voor toegang tot digitale overheidstoepassingen. De dienstverleners beschikken over persoonsgegevens van hun gebruikers die zij gebruiken voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (cf. artikel 4, § 1, 2° WVP), desgevallend gaat het om één of meer commerciële doelstellingen. Per definitie zullen de dienstverleners in dit geval de persoonsgegevens die zij verwerken bij elk gebruik van de aanmeldoptie niet uitsluitend gebruiken voor de "*dienst die de identiteit garandeert van de gebruiker die toegang zoekt tot digitale overheidstoepassingen op basis van een aanmeldoptie*", maar ook voor hun eigen doeleinden.

29. Om coherent te zijn met het opzet van het ontwerp vraagt de Commissie deze bepaling te herschrijven, zodat duidelijk wordt dat enkel de persoonsgegevens uitsluitend verzameld in het kader van de levering van de dienst voor elektronische identificatie vervolgens ook uitsluitend voor de dienstverlening mogen aangewend worden.

30. De expliciete verwijzing in de tweede zin van het artikel naar de WVP en de AVG dient louter ter bewustmaking van de dienstverleners. Het spreekt voor zich dat de dienstverleners de regelgeving van toepassing op hun activiteit - met name de wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen* die het gebruik van het Rijksregisternummer regelt - dienen na te leven, ongeacht of er hiernaar expliciet verwezen wordt.

Artikel 15 van het ontwerp

31. Artikel 15 van het ontwerp verwijst naar de mechanismen ter bescherming van de persoonsgegevens zoals omschreven in punt 2.3.1 van de bijlage van de uitvoeringsverordening (EU) nr. 2015/1502, maar laat na te specifiëren dat de dienstverlener de keuze heeft tussen het niveau substantieel of hoog (vergelijk met art. 5, 6 en 8 van het ontwerp).

Artikel 16 van het ontwerp

32. Artikel 16, § 1 van het ontwerp bepaalt:

> *"De dienstverlener neemt geen kennis van de digitale overheidstoepassingen waartoe de gebruiker door middel van de dienst voor elektronische identificatie toegang verzoekt."*

33. Deze bepaling moet samen gelezen worden met artikelen 33 en 35 van het ontwerp.

> *Art. 33. Bij de aanmelding van de gebruiker bij de digitale overheidstoepassing, verbindt de federale authenticatiedienst de gebruiker door naar de erkende dienst voor elektronische identificatie waarvoor de gebruiker heeft gekozen.*
> *Art. 35. De aanbieder van een erkende dienst voor elektronische identificatie gebruikt het uniek identificatienummer voor het aanbieden van de erkende dienst voor elektronische identificatie via het toegangsportaal van de erkennende overheid.*

34. Hieruit blijkt dat de federale authenticatiedienst (geregeld in artikel 11 van het voorontwerp van wet) er als tussenpersoon voor zorgt dat de dienstverlener niet op de hoogte gesteld wordt van tot welke digitale overheidstoepassing de gebruiker wenst toegang te krijgen. Uit artikel 35 van het ontwerp volgt dat de dienstverlener na een geslaagde aanmelding dit feit - gekoppeld aan het uniek identificatienummer - meedeelt aan de federale authenticatiedienst, die dit feit op zijn beurt doorspeelt aan de digitale overheidstoepassing.

35. Artikel 16, § 2 van het ontwerp bepaalt:

> *"De dienstverlener installeert een beveiligd controlespoor zodat de gegevens per specifieke transactie kunnen worden gereconstrueerd met het oog op de beveiliging van de gegevens en de bescherming van de persoonlijke levenssfeer. Hiertoe bewaart de dienstverlener voor iedere aanmelding de volgende informatie gedurende een termijn van tien jaar te rekenen vanaf het moment van de aanmelding in kwestie:*
> *1. de naam en voornaam van de gebruiker die zich aanmeldt;*
> *2. het unieke identificatienummer van de gebruiker;*
> *3. de dienst voor elektronische identificatie van de dienstverlener waarmee de gebruiker zich aanmeldt; en*
> *4. het tijdstip van de aanmelding"*

36. Het belang van logbestanden werd eerder reeds aangehaald in randnummer 25. Wat de inhoud van de controlesporen van geslaagde aanmeldingen betreft, gaat de Commissie ervan uit dat de verplichte vermelding van "*de naam en voornaam van de gebruiker die zich aanmeldt"* veronderstelt dat elke aanmeldoptie de naam en voornaam van de gebruiker verwerkt bij elke aanmeldpoging. Dienstverleners die gebruik maken van andere gegevens (e-mail adres, gsm-nummer, bankrekeningnummer, ...) om hun gebruikers te identificeren in het aanmeldproces, worden verplicht bijkomend telkens de naam en voornaam op te nemen in het controlespoor. De Commissie acht de formulering van het ontwerp op dit punt disproportioneel. Hier gaat het ontwerp verder dan het bewaren van de identificator die de gebruiker feitelijk gebruikt heeft om zich aan te melden. Bovendien kan de federale authenticatiedienst de naam en voornaam van de betrokkene achterhalen aan de hand van het uniek identificatienummer. Het uniek identificatienummer volstaat voor deze doelstelling.

Artikel 17 van het ontwerp

37. Artikel 17 van het ontwerp bepaalt:

> *"De dienstverlener neemt maatregelen om te garanderen dat het unieke identificatienummer van de gebruiker enkel gebruikt wordt voor de finaliteit elektronische identificatie via het toegangsportaal van de erkennende overheid"*

38. De dienstverlener die erkend wensen te worden moeten bijgevolg garanties bieden dat zij de persoonsgegevens die zij verzamelden met het oog op het doeleinde waarvoor zij erkend zijn, niet voor andere commerciële doeleinden zullen gebruiken.

39. Gelet op het feit dat het voorontwerp van wet het gebruik van het Rijksregisternummer regelt, dient uit de aanhef de overbodige verwijzing naar "*de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, artikel 8, § 1, tweede lid*" geschrapt te worden. Deze verwijzing dient ook geschrapt te worden in het verslag aan de Koning.

Artikel 21 en 22 van het ontwerp

40. Artikel 21 en 22 bevatten een regeling rond de uitrol van nieuwe versies van de software door de erkende dienstverlener. Hierrond moet de erkende dienstverlener afspraken maken met de erkennende overheid.

41. Artikel 22 van het ontwerp bepaalt:

> *"De dienstverlener legt elke nieuwe softwareversie die een significante impact heeft op de gebruiker, vergezeld door een impactanalyse, ten laatste één maand voor de datum van inplanning van de uitrol ter goedkeuring voor bij de erkennende overheid."*

42. Wijzigingen in de technische specificaties van de erkende aanmeldopties kunnen een impact hebben op de digitale overheidstoepassingen die ervan gebruik maken via de FAS. Daar de erkende dienstverleners niet mogen weten voor welke digitale overheidstoepassingen beroep gedaan wordt op de door hen geleverde aanmeldoptie, moet de erkennende overheid erover waken dat er geen impact is voortvloeiende uit technische wijzigingen. De Commissie is van oordeel dat het ontwerp hiertoe de nodige waarborgen moet inbouwen.

Artikel 23 van het ontwerp

43. Artikel 23 van het ontwerp bepaalt:

> *"*De dienstverlener bouwt mechanismen in die de dienstverlening op ononderbroken wijze kunnen garanderen gedurende de duur van de erkenning.*"*

44. Het ontwerp erkent het belang van continuïteit van de dienstverlening gedurende de periode van erkenning, daarentegen bevat het geen regeling voor de periode die volgt op het beëindigen van de erkenning. Hierbij gaat het zowel om situaties waarbij de dienstverlener zelf beslist de dienst stop te zetten als deze waarin de erkenning geschorst of ingetrokken wordt. Abrupte stopzetting van een kan in bepaalde omstandigheden onvermijdelijk zijn. Toch is de Commissie van oordeel dat de

erkennende overheid in de erkenningsvoorwaarden dient vast te leggen dat uitdovingsscenario's de regel zijn. Zodoende worden gebruikers van aanmeldopties niet plots voor voldongen feiten gesteld en kunnen zij geleidelijk overstappen naar andere diensten. Ook de beheerder van de digitale overheidstoepassing krijgt zo de kans overgangsmaatregelen te treffen indien nodig. Welk uitdovingsscenario aangewezen is hangt af van de context.

Artikel 27 van het ontwerp

45. Artikel 27 van het ontwerp somt gevallen op waarin de aanvrager van de erkenningsprocedure kan uitgesloten worden of de dienstverlener de erkenning kan verliezen, onder meer in geval deze "*bij rechterlijke beslissing die in kracht van gewijsde is gegaan, veroordeeld is geweest voor een inbreuk op de wetgeving inzake de bescherming van de persoonlijke levenssfeer*."

46. Hierbij wordt uit het oog verloren dat de Commissie ingevolge van de AVG (artikelen 58.2 en 83) de bevoegdheid zal hebben administratieve sancties op te leggen. In dergelijke gevallen is een schorsing of intrekking van de erkenning eveneens aan de orde. De Commissie is van oordeel dat een verwijzing naar deze bevoegdheid dient toegevoegd.

Terminologische bemerking

47. Het ontwerp gebruikt op verschillende plaatsen de term 'privacy', terwijl het Koninklijk Besluit de verwerking van persoonsgegevens beoogt te omkaderen, blijkens de verwijzing in artikel 14 naar de WVP en de AVG. Gezien het ontwerp een regeling betreft inzake de verwerking van persoonsgegevens, verzoekt de Commissie de terminologie hieraan aan te passen.

OM DEZE REDENEN,
de Commissie

een **gunstig** advies op voorwaarde dat rekening wordt gehouden met haar opmerkingen onder de punten 7, 8, 9, 12, 20, 26, 20, 31, 36, 39, 42, 44, 46 en 47.

De Wnd. Administrateur, De Voorzitter,

(get.) An Machtens (get.) Willem Debeuckelaere