AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

De minister van Binnenlandse Zaken en Koninkrijkrelaties,
de heer dr. R.H.A. Plasterk
Postbus 20011
2500 EA Den Haag

Datum	Ons kenmerk	Uw brief van
13 oktober 2017	z2017-06920	30 augustus 2017
	Contactpersoon	Uw kenmerk
		2017-0000387707

Onderwerp
Advies ontwerp Wet generieke digitale infrastructuur

Geachte heer Plasterk,

Bij brief van 30 augustus 2017 heeft u de Autoriteit Persoonsgegevens (AP) gevraagd op grond van het bepaalde in artikel 51, tweede lid, van de Wet bescherming persoonsgegevens (Wbp) te adviseren over de Regels inzake de generieke digitale infrastructuur (hierna: het wetsvoorstel).

De AP voldoet hiermee aan uw verzoek.

Achtergrond van het wetsvoorstel

De afgelopen decennia is het gebruik van de elektronische weg in de contacten tussen burgers, ondernemers en publieke dienstverleners toegenomen en breed geaccepteerd. In bijzondere wetten is soms al de elektronische weg met uitsluiting van de papieren weg voorgeschreven.[1] Hierbij zijn er sterke verschillen tussen de elektronische wegen. Dit hangt onder meer samen met verschillen in tempo waarop bestuursorganen digitaliseren en de invloed van nieuwe technologische ontwikkelingen. Van de overheid mag echter worden verwacht dat zij organisatieoverstijgend opereert, zodat informatie makkelijk vindbaar is en transacties eenvoudig uitvoerbaar zijn. Duidelijk is geworden dat het vrijwel onmogelijk is om alleen op basis van bestuursakkoorden tot de gewenste modernisering te komen.

[1] Bijvoorbeeld de Wet elektronisch berichtenverkeer Belastingdienst, Stb. 2015, 378.

Datum
13 oktober 2017

Ons kenmerk
z2017-06920

Inhoud van het wetsvoorstel

De generieke digitale infrastructuur vormt een dynamisch geheel dat in de toekomst – op basis van technologische ontwikkelingen of nieuwe inzichten – gewijzigd zal worden door het toevoegen van nieuwe (functionaliteiten van) generieke voorzieningen of door het uitfaseren van bestaande voorzieningen. De regering kiest er voor om de wetgeving voor de generieke digitale infrastructuur in tranches tot stand te brengen. Dit wetsvoorstel betreft de eerste tranche.

Het wetsvoorstel regelt:

1. de bevoegdheid van het kabinet om open standaarden[2] te verplichten en
2. de digitale toegang tot publieke dienstverlening voor burgers (natuurlijke personen) en bedrijven (rechtspersonen en natuurlijke personen die handelen in de uitoefening van beroep of bedrijf).

Dit wetsvoorstel is randvoorwaardelijk om zowel aan Europese verplichtingen op het gebied van elektronische identificatie als aan de Europese verplichtingen ten aanzien van het gebruik van standaarden te voldoen.

Ad 1. Open standaarden

ICT-standaarden zijn afspraken vastgelegd in een specificatiedocument. Ze beschrijven hoe gegevens eruit zien, wat ze betekenen en hoe ze kunnen worden uitgewisseld.

De standaarden die op de 'pas toe of leg uit'-lijst[3] staan, zijn open standaarden waarvoor breed draagvlak bestaat. Er is afgesproken dat het Rijk en de medeoverheden deze open standaarden gebruiken en hierbij werken volgens het principe 'pas toe of leg uit'. Bij aanschaf of (ver)bouw van ICT-systemen en -diensten zijn overheden verplicht om de open standaarden die op de 'pas toe of leg uit'-lijst staan te hanteren ('pas toe'). Afwijken van deze verplichting mag alleen in geval van zwaarwegende redenen. Verantwoording hierover moet worden afgelegd in het jaarverslag ('leg uit').

Uit metingen[4] blijkt dat het adoptietempo van open standaarden laag is en dat er in de jaarverslagen zelden wordt uitgelegd waarom een open standaard niet wordt toegepast. Dit heeft nadelige gevolgen voor de interoperabiliteit, veiligheid en kosten(beheersing) van ICT-systemen. Het wetsvoorstel biedt daarom een grondslag om bij algemene maatregel van bestuur een verplicht toe te passen open standaard aan te wijzen.

[2] Onder 'open standaard' wordt verstaan: een afspraak die is vastgelegd in een specificatiedocument dat vrij te verkrijgen (open) is.
[3] Het Forum Standaardisatie beheert deze lijst met open standaarden: https://www.forumstandaardisatie.nl/lijst-open-standaarden.
[4] 1-meting informatieveiligheidstandaarden en de Monitor Open Standaarden Beleid over de jaren 2012, 2013, 2014 en 2015.

Ad 2. Digitale toegang tot publieke dienstverlening voor burgers en bedrijven
Dit wetsvoorstel verplicht publieke dienstverleners[5] voor hun elektronische diensten waarvoor, gelet op de aard ervan veilige toegang in de rede ligt, het betrouwbaarheidsniveau 'substantieel' of 'hoog' te gebruiken. Dit wetsvoorstel strekt er tevens toe dat de digitale toegang tot dienstverlening van bestuursorganen en aangewezen organisaties generiek wordt ingericht zodat burgers en bedrijven met één of meer generieke identificatiemiddelen overheidsbreed en op een passend betrouwbaarheidsniveau toegang kunnen krijgen tot elektronische diensten.

Ingevolge dit wetsvoorstel worden nadere eisen gesteld aan de uitgifte van identificatiemiddelen op de verschillende betrouwbaarheidsniveaus. Hiervoor gelden de relevante bepalingen uit de Europese eIDAS verordening inzake de betrouwbaarheid en het uitgifteproces.[6] De in deze verordening opgenomen classificatie van identificatiemiddelen naar betrouwbaarheidsniveau ('laag', 'substantieel' en 'hoog') wordt hierbij gevolgd. Aanvullende nationale regelgeving is noodzakelijk voor de aanvraag en de uitgifte van Nederlandse publieke identificatiemiddelen. Bij wettelijk voorschrift zal onder meer worden bepaald wie in aanmerking komt voor een publiek identificatiemiddel, hoe het middel wordt uitgegeven, hoe daarbij gebruik moet worden gemaakt van wettelijke registraties, dat er voor het middel dient te worden betaald en wanneer het middel vervalt of wordt ingetrokken.

Voorts codificeert dit wetsvoorstel de huidige taken en verantwoordelijkheden, die nodig zijn om de infrastructuur voor authenticatie in het publieke domein te doen functioneren. De Minister van Economische Zaken krijgt in dit wetsvoorstel taken en verantwoordelijkheden toebedeeld betreffende authenticatie door bedrijven. Hij draagt in dit verband zorg voor een (knooppunt)voorziening met functionaliteiten om authenticatie en soepele dienstverlening binnen de EU mogelijk te maken. De minister van Binnenlandse Zaken en Koninkrijkrelaties (BZK) heeft een zorgplicht voor generieke digitale infrastucturele voorzieningen zoals onder meer het BSN-koppelregister en een machtigingsvoorziening. De minister van BZK is - naast het ontwikkelen en in stand houden van (voorzieningen van) de generieke digitale infrastructuur voor de (semi)publieke sector - verantwoordelijk voor het ontwikkelen van publieke identificatiemiddelen voor burgers op een voldoende hoog betrouwbaarheidsniveau.

Privacy impact assessments

Er zijn privacy impact assessments uitgevoerd ten aanzien van de digitale infrastructuur (eID-stelsel) en de startarchitectuur eIDAS.

[5] Met 'publieke dienstverleners' wordt bedoeld zowel bestuursorganen zoals bedoeld in artikel 1:1, lid 1, onderdeel a, Algemene wet bestuursrecht ('a-organen'), als organisaties die in de bijlage bij het wetsvoorstel zullen worden aangewezen en organisaties die bij besluit van de minister van Binnenlandse Zaken en Koninkrijkrelaties zullen worden aangewezen ('aangewezen organisaties').
[6] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (Pb EU 2014, L 257/73).

Datum
13 oktober 2017

Ons kenmerk
z2017-06920

Eerdere adviezen AP

De AP (eerder het College bescherming persoonsgegevens (CBP) heeft reeds meerdere adviezen uitgebracht betreffende de (ontwikkeling en wetgeving van de) digitale infrastructuur (eID-stelsel) en de uitvoeringswet eIDAS verordening:

- Brief van de AP, *eID*, 14 september 2016:
  autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_eid_aan_bzk.pdf

- Brief van het CBP, *Wetgevingsadvies Besluit verwerking persoonsgegevens DigiD, DigiD Machtigingen, MijnOverheid en BSN-koppelregister*, 3 december 2015:
  autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/z2015-00766_brief.pdf

- Brief van het CBP, *Wetgevingsadvies Uitvoeringswet EU-Verordening elektronische identiteiten en vertrouwensdiensten*, 1 december 2015:
  autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/z2015-00746_brief.pdf

- Brief van het CBP, *Introductieplateau eID*, 7 mei 2015:
  autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_introductieplateau_eid.pdf

Advies wetsvoorstel

Wetgeving in tranches

De wetgeving voor de generieke digitale infrastructuur zal in tranches tot stand worden gebracht.

Het voordeel hiervan kan zijn dat elk onderdeel van de wetgeving 'behapbaar' blijft. Tevens kan de ervaring die wordt opgedaan met het eerste onderdeel, worden meegenomen bij het wetgevingstraject van het volgende onderdeel. Daarentegen brengt de gefaseerde totstandkoming van wetgeving ook risico's met zich mee voor het overzicht van het geheel en de samenhang tussen de verschillende onderdelen en daarmee voor een adequate bescherming van de persoonsgegevens van de betrokkenen.

De AP merkt op dat het van belang is om bij de afwegingen omtrent de bescherming van persoonsgegevens in elke tranche zo veel mogelijk de volledige scope van de generieke digitale infrastructuur te betrekken.

Lagere regelgeving

In lagere regelgeving zullen nadere regels worden gesteld met betrekking tot de verwerking van persoonsgegevens, waaronder regels omtrent dataminimalisatie, juistheid van persoonsgegevens, beveiliging, bewaartermijnen, verstrekking van persoonsgegevens en rechten van betrokkenen.

Deze regels omtrent de verwerking van persoonsgegevens hangen evenwel nauw samen met de regels omtrent de inrichting van de generieke digitale infrastructuur zoals in dit wetsvoorstel worden gesteld.

Deze nauwe samenhang bemoeilijkt het adviseren over een deel van de wetgeving, terwijl het samenhangende deel nog onbekend is. In de Memorie van Toelichting van dit wetsvoorstel is bovendien niet gemotiveerd waarom de nadere regels omtrent de verwerking van persoonsgegevens niet in deze wet in formele zin worden gesteld, maar pas bij lagere regelgeving.

De AP adviseert om in de Memorie van Toelichting van dit wetsvoorstel te motiveren waarom de betreffende regels met betrekking tot de verwerking van persoonsgegevens bij lagere regelgeving worden gesteld en niet in deze wet in formele zin. Tevens adviseert de AP om het toekomstige advies over de lagere regelgeving niet los te zien van dit advies over het wetsvoorstel. De AP ziet de lagere regelgeving te zijner tijd ter nadere advisering graag tegemoet.

Beginselen van proportionaliteit en subsidiariteit
Wetsvoorstellen dienen te voldoen aan artikel 8 van het Handvest van de grondrechten van de Europese Unie (Handvest), artikel 16 van het Verdrag betreffende de werking van de Europese Unie (VWEU), artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), de Algemene verordening gegevensbescherming (AVG)[7] en, in Nederland, artikel 10 van de Grondwet en.

Artikel 8 Handvest bepaalt onder meer dat persoonsgegevens eerlijk en voor bepaalde doeleinden moeten worden verwerkt, en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet.
Artikel 16 VWEU bepaalt dat eenieder in de Europese Unie recht heeft op bescherming van zijn persoonsgegevens.
Artikel 8 EVRM eist dat iedere inmenging op het recht op respect voor privéleven op een wettelijke grondslag berust.
De AVG stelt regels inzake de bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen in verband met de verwerking van persoonsgegevens
Artikel 10 Grondwet scherpt verlangt voor elke beperking van het recht op eerbiediging van de persoonlijke levenssfeer een grondslag in de formele wet.

Voor een wettelijke beperking van het voornoemde grondrecht gelden ook materiële eisen. Het voorschrift zal voldoende nauwkeurig moeten zijn en adequate en effectieve waarborgen moeten bevatten tegen ongeoorloofde inbreuken. Voorts is een inmenging op het recht op respect voor privéleven slechts toegestaan indien deze in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of goede zeden of voor de bescherming van de rechten en vrijheden van anderen (artikel 8 EVRM).

Volgens de jurisprudentie van het Europese Hof voor de Rechten van de Mens betekent dit dat de beperking van de persoonlijke levenssfeer moet worden gerechtvaardigd door een 'pressing social need' en in overeenstemming moet zijn met de beginselen van proportionaliteit (de beperking mag niet

[7] De AVG is vanaf 25 mei 2018 van toepassing.

onevenredig zijn in verhouding tot het nagestreefde doel) en de subsidiariteit (het nagestreefde doel moet niet op een voor de burger minder ingrijpende wijze kunnen worden bereikt). Deze vereisten moeten in hun onderlinge samenhang gelezen worden.

Het wetsvoorstel regelt het kader met betrekking tot de digitale dienstverlening van overheidsorganisaties. Wanneer burgers gebruik maken van deze digitale dienstverlening, worden er persoonsgegevens van hen verwerkt. Dit levert een inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer op.

Volgens de Memorie van Toelichting van het wetsvoorstel zullen de beginselen van proportionaliteit en subsidiariteit nader worden ingevuld in de uitvoeringsregelgeving.[8] Het wetsvoorstel bevat evenwel bepalingen omtrent de inrichting van de generieke digitale infrastructuur en de partijen die daarin een rol spelen. Deze inrichting en partijen vormen de basis van de wijze waarop en door wie persoonsgegevens worden verwerkt. Bovendien bevat het wetsvoorstel en de bijbehorende Memorie van Toelichting bepalingen en overwegingen omtrent de verwerking van persoonsgegevens, waaronder het burgerservicenummer (bsn)[9].[10]

De AP adviseert om in de Memorie van Toelichting van het wetsvoorstel expliciet te motiveren op welke wijze het wetsvoorstel en de genoemde gegevensverwerkingen voldoen aan het proportionaliteits- en subsidiariteitsbeginsel.

Geldigheid AVG

Volgens de Memorie van Toelichting bij het wetsvoorstel bevat het wetsvoorstel bepalingen die een aanvulling zijn op de waarborgen van de AVG. Daarbij is opgemerkt dat de bepalingen van de AVG gelden voor alles wat het wetsvoorstel en het daarop gebaseerde besluit niet regelt over de verwerking van persoonsgegevens in het kader van de toegang tot elektronische dienstverlening.[11]

De AP merkt voor de goede orde op dat de AVG van toepassing is ten aanzien van de verwerkingen van persoonsgegevens zoals wordt geregeld bij of krachtens dit wetsvoorstel. Dit wetsvoorstel en het betreffende besluit kunnen de normen van de AVG, voor zover die daar ruimte voor bieden, slechts verdiepen.

Voor zover dat met het bovenstaande tekstgedeelte in de Memorie van Toelichting ook is bedoeld, adviseert de AP om dit tekstgedeelte in die zin te verduidelijken. Voor zover de toetsing aan de AVG niet overeenkomstig de opmerking van de AP heeft plaatsgevonden, adviseert de AP dit alsnog te doen en de wijze waarop die toetsing heeft plaatsgevonden in de Memorie van Toelichting nader toe te lichten.

[8] Par. 5., *Dataminimalisatie*, p. 19.
[9] Artikel 14 van het wetsvoorstel.
[10] Zo is in de Memorie van Toelichting van het wetsvoorstel (p. 56) bijvoorbeeld aangegeven dat een authenticatiedienst een kopie van het overlegde identificatiemiddel bewaart, waarop de gelaatsfoto en het bsn zijn verwijderd. Uit de Memorie van Toelichting blijkt evenwel niet waarom het noodzakelijk is om een kopie van het identificatiemiddel te bewaren en waarom vervolgens niet kan worden volstaan met (nog) minder persoonsgegevens op de betreffende kopie.
[11] p. 17

Cryptografische maatregelen

In de Memorie van Toelichting van het wetsvoorstel is aangegeven dat het BSN-koppelregister een rol speelt bij het activeren van een middel en bij een daadwerkelijke authenticatie van een gebruiker ten behoeve van een specifiek(e) bestuursorgaan of aangewezen organisatie. Deze functies zijn zodanig ingericht, dat het BSN-koppelregister alleen bij de eenmalige activering van een nieuw middel kan herleiden tot een individuele gebruiker en zijn bsn. Bij de functies authenticeren en informeren is dit volgens de Memorie van Toelichting niet nodig en is herleiding vanuit privacy-overwegingen onmogelijk gemaakt door cryptografische maatregelen.[12]

Uit het wetsvoorstel of de bijbehorende Memorie van Toelichting blijkt evenwel niet welke cryptografische maatregelen worden getroffen. De AP kan daarom niet beoordelen of herleiding tot een natuurlijk persoon daadwerkelijk onmogelijk is. Daarbij merkt de AP op dat er rekening mee moet worden gehouden dat technische implementaties die thans voldoende zijn om herleiding te voorkomen, in de toekomst wellicht niet meer voldoen.

De AP adviseert om in het wetsvoorstel en/of de Memorie van Toelichting nader te specificeren welke crytografische maatregelen worden getroffen. Tevens adviseert de AP om in het wetsvoorstel te bepalen dat er regelmatig wordt beoordeeld of de getroffen technische implementatie nog steeds voldoende zijn om herleiding tot een natuurlijke persoon te voorkomen.

Technische scheiding en privacy by design

In de Memorie van Toelichting van het wetsvoorstel is aangegeven dat de functie authenticeren en informeren vanuit het oogpunt van veiligheid en privacybescherming technisch van elkaar zijn gescheiden (privacy by design).[13]

Uit het wetsvoorstel of de bijbehoren de Memorie van Toelichting blijkt evenwel niet op welke wijze deze functies van elkaar gescheiden worden. De AP kan daarom niet beoordelen of er daadwerkelijk sprake is van een technische scheiding die een onderdeel kan zijn van privacy by design. De AP merkt daarbij op dat privacy by design meer omvat dan alleen het scheiden van functies. Het betreft het geheel van privacyverhogende maatregelen waaraan al tijdens de ontwikkeling van producten en diensten aandacht wordt besteed, waaronder dataminimalisatie.

De AP adviseert om in het wetsvoorstel en/of de Memorie van Toelichting nader te specificeren op welke wijze de functie authenticeren en informeren van elkaar zijn gescheiden. Tevens adviseert de AP om in de Memorie van Toelichting te verduidelijken dat de technisch scheiding slechts een onderdeel is van privacy by design.

[12] p. 46
[13] p. 46

Voorschriften privaat identificatiemiddel
Artikel 8, lid 3, van het wetsvoorstel bepaalt dat een toelatingsbesluit van een privaat identificatiemiddel een omschrijving bevat van het betrouwbaarheidsniveau van het identificatiemiddel en de duur waarvoor de toelating is verleend, de verplichtingen van de houder van de toelating en, indien van toepassing, de prijs die de houder van de toelating betaalt of de subsidie die de minister van BZK aan de houder verstrekt. Deze omschrijving (voorschriften) hebben volgens de Memorie van Toelichting van het wetsvoorstel onder meer betrekking op de beveiliging en privacybescherming.[14]

In het wetsvoorstel of de bijbehorende Memorie van Toelichting is de inhoud van de voorschriften niet nader uitgewerkt. De AP kan daarom over de inhoud van de voorschriften niet adviseren.

De AP adviseert om in het wetsvoorstel en/of de Memorie van Toelichting de voorschriften die verbonden zijn aan het toelatingsbesluit nader te specificeren en te motiveren.

Uitzondering erkenning dienst of middel
Artikel 10, lid 7, van het wetsvoorstel bepaalt dat de minister van Economische Zaken een dienst of bedrijfs- of organisatiemiddel kan erkennen, indien deze niet aan de voor die dienst of dat middel gestelde regels voldoet, doch onverkorte toepassing van die regels tot een onaanvaardbaar resultaat zou leiden. Volgens de Memorie van Toelichting van het wetsvoorstel kan dit bijvoorbeeld aan de orde zijn in geval aan vrijwel alle eisen wordt voldaan en nog enige tijd nodig is om aan alle eisen te voldoen.[15]

De AP gaat ervan uit dat deze uitzondering niet leidt tot een gegevensverwerking die in strijd is met de AVG.

Verklaring van een auditor
Artikel 13, lid 2, van het wetsvoorstel bepaalt dat bestuursorganen en aangewezen organisaties een verklaring van een auditor dienen te overleggen waaruit blijkt dat zij voldoen aan de in artikel 13, lid 1, van het wetsvoorstel bedoelde regels met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische dienstverlening die zij in stand houden. De verklaring dient te worden overgelegd aan de minister van BZK. Volgens de Memorie van Toelichting bij het wetsvoorstel gaat het hier om een verplichting om *regulier* een verklaring van een auditor te overleggen.[16]

Er is evenwel niet nader gespecificeerd wanneer en hoe vaak een auditverklaring dient te worden overgelegd om te kunnen spreken van 'regulier'.

De AP is ingenomen met deze bepaling met betrekking tot het overleggen van een verklaring van een auditor. De AP adviseert om vanuit het oogpunt van rechtszekerheid in de wettekst op te nemen dat een verklaring van een auditor *regulier* dient te worden overgelegd. Tevens adviseert de AP om in de wettekst

[14] p. 50
[15] p. 51
[16] p. 54

dan wel in de Memorie van Toelichting te definiëren of te motiveren wat onder 'regulier' wordt verstaan. Voorts adviseert de AP om vanuit het oogpunt van transparantie in de wettekst de verplichting op te nemen dat de auditrapportages openbaar worden gemaakt.

Verwerking persoonsgegevens authenticatiedienst
In de Memorie van Toelichting van het wetsvoorstel is aangegeven dat een authenticatiedienst geen integrale kopie van het overgelegde identificatiemiddel bewaart, maar een kopie waarop de gelaatsfoto en het bsn zijn verwijderd. Hierdoor ontstaat er volgens de Memorie van Toelichting bij de authenticatiediensten geen verzameling van persoonsgegevens ("hotspot"), waardoor de privacy van de gebruikers wordt beschermd.[17]

Naar het oordeel van de AP neemt deze maatregel niet weg dat er nog steeds een verwerking van persoonsgegevens plaatsvindt. In die zin behoeft het bovenstaande aanpassing.

Overgangsrecht
Ingevolge het wetsvoorstel zullen alleen identificatiemiddelen met een betrouwbaarheidsniveau substantieel en hoog worden erkend. Middelen op een lager betrouwbaarheidsniveau, zoals het bestaande DigiD, zullen niet worden toegelaten of erkend.

Het wetsvoorstel voorziet in overgangsrecht voor bepaalde middelen en diensten van ten hoogste 18 maanden vanaf de inwerkingtreding van het wetsvoorstel.[18]

Het is voor de AP onduidelijk of deze overgangstermijn ook geldt voor identificatiemiddelen met een laag betrouwbaarheidsniveau. Bovendien ontbreekt er een onderbouwing van de duur van de overgangstermijn.

De AP adviseert om in de Memorie van Toelichting van het wetsvoorstel expliciet aan te geven of de overgangstermijn ook geldt ten aanzien van identificatiemiddelen met een laag betrouwbaarheidsniveau. Indien dit het geval is, dan adviseert de AP tevens om in de Memorie van Toelichting de duur van de overgangstermijn te onderbouwen in het licht van dat lage betrouwbaarheidsniveau.

Dictum

De AP adviseert u niet tot indiening van het voorstel over te gaan, dan nadat daarin met het vorenstaande rekening zal zijn gehouden.

[17] p. 56
[18] artikel 22

AUTORITEIT
PERSOONSGEGEVENS

Datum
13 oktober 2017

Ons kenmerk
z2017-06920

Uniforme toepassing AVG

Tot slot wil de AP u nog op het volgende wijzen. Zoals ook vermeld in de Memorie van Toelichting van het conceptwetsvoorstel is vanaf 25 mei 2018 de AVG van toepassing. Uw voorstel is door de AP reeds aan de AVG getoetst en de toets aan de AVG leidt thans niet tot een ander oordeel dan onder de huidige Wbp. In dat kader acht de AP het echter wel van belang het volgende op te merken. De AVG beoogt in de gehele Europese Unie een uniforme toepassing van de regels inzake bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen in verband met de verwerking van persoonsgegevens te bewerkstelligen. Hiertoe is het onder meer noodzakelijk dat de toezichthoudende autoriteiten in de lidstaten van de EU gezamenlijk bijdragen aan de ontwikkeling van een uniforme uitleg van bepalingen van de AVG. Gelet op de omstandigheid dat de AVG pas vanaf 25 mei 2018 van toepassing is, kunnen inzichten met betrekking tot de toepassing van de AVG – door bijvoorbeeld benodigde afstemming met andere toezichthouders – in de toekomst invloed hebben op het oordeel van de AP.

Wij adviseren u voorts om bij het opstellen van nieuwe wet- en regelgeving geen bepalingen op te nemen die een juiste toepassing en verwezenlijking van de werking van de AVG en, voor zover van toepassing, EU-richtlijn 2016/680 in gevaar kunnen brengen.

Hoogachtend,
Autoriteit persoonsgegevens,

Mr. W.B.M. Tomesen
Vicevoorzitter