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 Staatssecretaris van Binnenlandse Zaken en Koninkrijkrelaties,

Postbus 20011
2500 EA Den Haag

Datum	Ons kenmerk	Uw brief van
6 juli 2018	z2018-05537	27 maart 2018

Contactpersoon

070 888 500

Onderwerp
Advies conceptbesluit digitale overheid

Geachte ,

Bij brief van 27 maart 2018 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 het conceptbesluit van (…) houdende wijziging van het Besluit verwerking persoonsgegevens generieke digitale infrastructuur in verband met het stellen van de kaders voor informatieveiligheid en persoonsgegevensverwerking (hierna: het conceptbesluit). De adviesverlening geschiedt thans op grond van artikel 36, vierde lid, van de Algemene verordening gegevensbescherming (AVG).

Met betrekking tot het conceptbesluit was een internetconsultatie opengesteld van 27 maart 2018 tot en met 30 april 2018. De AP heeft u bij brief van 10 april 2018 laten weten dat zij zal adviseren na ommekomst van de internetconsultatie-termijn, opdat de AP eventuele wijzigingen in het conceptbesluit als gevolg van de internetconsultatie in haar advies kan betrekken. Per e-mail van 15 mei 2018 heeft uw ministerie aangegeven dat uitgestelde advisering van de AP bezwaarlijk is.

Op 19 juni 2018 heeft er een overleg plaatsgevonden tussen de AP en uw ministerie over het conceptbesluit. Gespreksonderwerpen waren onder meer de uitgevoerde gegevensbeschermingseffectbeoordelingen (ook wel een privacy impact assessments (PIA's) genoemd) in relatie tot het conceptbesluit en de beveiligingsmaatregelen die worden getroffen in de regelgeving en de technische specificaties. Tevens heeft uw ministerie aangegeven dat de reacties van de internetconsultaties grotendeels zien op de verzwaring van administratieve lasten en niet op de verwerking van persoonsgegevens.

Datum
6 juli 2018

Ons kenmerk
z2018-05537

De AP voldoet hiermee aan uw verzoek om advisering. De AP heeft haar advies gebaseerd op de internetconsultatieversie van het conceptbesluit, zoals is toegestuurd bij brief van 27 maart 2018.

Achtergrond en inhoud van het conceptbesluit

Het wetsvoorstel digitale overheid stelt regels met betrekking tot publieke en private identificatiemiddelen die gebruikt kunnen worden bij het verlenen van toegang tot dienstverlening in het publieke domein. Ingevolge dit wetsvoorstel is op diverse onderdelen uitvoeringsregelgeving nodig. Het onderhavige conceptbesluit behoort tot dit regelgevingscluster.[1] Het conceptbesluit stelt onder meer regels inzake de verwerking, de verstrekking en de bewaartermijn van persoonsgegevens en de informatieveiligheid ten aanzien van de toegang tot elektronische dienstverlening. Het huidige Besluit verwerking persoonsgegevens generieke digitale infrastructuur wordt hiertoe gewijzigd en aangevuld.

Eerdere adviezen AP

De AP en haar voorganger, het College bescherming persoonsgegevens (CBP), hebben eerder de volgende adviezen uitgebracht met betrekking tot (de ontwikkeling en wetgeving van) het eID-stelsel en de uitvoeringswet eIDAS verordening[2]:

- Brief van de AP, *Advies wetsvoorstel Wijziging van de Paspoortwet*, 8 februari 2018[3]
- Brief van de AP, *Advies ontwerp Wet generieke digitale infrastructuur*[4], 13 oktober 2017[5]
- 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

Het conceptbesluit geeft de AP aanleiding tot het maken van de volgende op- en aanmerkingen.

[1] Nota van toelichting, *I Algemeen deel, 1. Inleiding; aanleiding voor het voorstel*, p. 15.
[2] 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).
[3] Deze brief is nog niet gepubliceerd.
[4] Thans de Wet digitale overheid.
[5] Deze brief is nog niet gepubliceerd.

Vooraf

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 AVG en artikel 10 van de Grondwet..

Artikel 8 van het 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 van het VWEU bepaalt dat eenieder in de Europese Unie recht heeft op bescherming van zijn persoonsgegevens.

Op grond van artikel 8 van het EVRM is geen inmenging van enig openbaar gezag toegestaan in de uitoefening van het recht op respect voor zijn privéleven, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Artikel 10, eerste lid, van de Grondwet bepaalt dat een ieder recht heeft op eerbiediging van zijn persoonlijke levenssfeer, behoudens bij of krachtens de wet te stellen beperkingen.

Bij de toepassing van de in voornoemde grondrechtbepalingen opgenomen beperkingsclausules spelen het proportionaliteits- en het subsidiariteitsbeginsel een belangrijke rol. Deze beginselen volgen uit het woord 'noodzakelijk' zoals opgenomen in de bovengenoemde grondslagen. Het proportionaliteitsbeginsel houdt in dat de inbreuken op de belangen van de bij de verwerking van persoonsgegevens betrokkene niet onevenredig mogen zijn in verhouding tot het met de verwerking te dienen doel. Ingevolge het subsidiariteitsbeginsel dient het doel waarvoor de persoonsgegevens worden verwerkt niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige, wijze te kunnen worden verwerkelijkt.

Integraal beeld van gemaakte afwegingen en geboden bescherming

Het eID-stelsel betreft een omvangrijk stelsel van elektronische dienstverlening aan burgers door instellingen van de overheid en in de semi-publieke sector. Door de eIDAS verordening heeft dit stelsel bereik in de gehele Europese Unie. Binnen dit stelsel en door de ketenpartners vindt op grote schaal gegevensverwerkingen plaats.

Er is en wordt diverse wet- en regelgeving opgesteld over het eID-stelsel. Dit conceptbesluit is daarvan een centraal onderdeel, aangezien het ziet op de verwerking en beveiliging van persoonsgegevens. De AP is van oordeel dat de toelichting bij dergelijke wet- en regelgeving een integraal beeld dient te bevatten van

de afwegingen die zijn gemaakt en de wijze waarop de bescherming van persoonsgegevens als geheel vorm krijgt. De nota van toelichting bij het conceptbesluit schiet hierin op een aantal punten nog tekort.

- In de nota van toelichting ontbreekt een weergave van de (belangrijkste) uitkomsten van de uitgevoerde PIA's en de eventuele maatregelen die in lijn daarmee zijn getroffen om de privacyrisico's voor betrokkenen te voorkomen of te verkleinen.

  In de rijksdienst wordt gebruik gemaakt van het *Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA)*[6]. Ingevolge dit model moet binnen de rijksdienst een PIA worden uitgevoerd:
  1. bij de ontwikkeling van beleid en regelgeving die betrekking hebben op verwerkingen van persoonsgegevens of waaruit verwerkingen van persoonsgegevens voortvloeien;
  2. bij voorgenomen verwerkingen van persoonsgegevens die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen.[7]

  Zodra er regelgeving wordt opgesteld betreffende de verwerking van persoonsgegevens dient er dus een PIA te worden uitgevoerd. Deze PIA kan betrekking hebben op het gehele proces of stelsel ten aanzien van de betreffende verwerking van persoonsgegevens. Het is derhalve niet vereist dat er bij elk individueel concept voor bepaalde regelgeving een PIA wordt uitgevoerd. In de nota van toelichting bij dit conceptbesluit is aangegeven dat gedurende het proces om te komen tot elektronische identificatie voor toegang tot dienstverlening in het publieke domein meerdere malen een PIA is uitgevoerd. De uitkomsten daarvan hebben volgens de nota van toelichting tot technische en organisatorische aanpassingen geleid die zijn verwerkt in regelgeving.

  Zo wordt in de PIA over het eID-stelsel van 28 juni 2017[8] het risico geconstateerd dat misbruikbestrijding op stelselniveau nog niet is ingericht. In de PIA wordt aanbevolen om invulling te geven aan de mogelijkheden om op stelselniveau misbruik te kunnen herkennen (detectie) en te herstellen als er misbruik van persoonsgegevens wordt geconstateerd. Misbruikbestrijding en incidentbestrijding op stelselniveau en de gegevens die daarvoor kunnen worden gebruikt moeten volgens de PIA nader worden uitgewerkt.[9] De AP constateert dat in lijn hiermee het conceptbesluit een grondslag bevat voor het verwerken van gegevens door de minister van Binnenlandse Zaken en Koninkrijkrelaties (BZK) ter bestrijding van misbruik (artikel 5e). De nota van toelichting noemt dit evenwel niet.

  Daarnaast volgt uit de eerdergenoemde PIA dat door middel van polymorfe pseudonimisering binnen het stelsel compartimentering zou moeten worden ingeregeld, waardoor grote gegevensconcentraties worden vermeden. Het risico bestaat volgens de PIA dat compartimentering grotendeels teniet wordt gedaan, doordat een aantal belangrijke leveranciers voor overheidspartijen in feite meerdere rollen invullen. In de PIA wordt daarom voorgesteld om eisen te stellen aan dienstverleners en leveranciers,

[6] *Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA)*, september 2017.
[7] *Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA)*, september 2017, p. 6.
[8] *Gegevensbeschermingseffectbeoordeling (GEB) eID-stelsel*, versie 1.0, 28 juni 2017.
[9] *Gegevensbeschermingseffectbeoordeling (GEB) eID-stelsel*, versie 1.0, 28 juni 2017, p. 6 en 36.

ten aanzien van combinaties van rollen en cumulatie van partijen binnen één leverancier. Minimaal zouden er garanties voor functiescheiding (Chinese muren) moeten komen, aldus de PIA.[10] De AP constateert dat in dit conceptbesluit weliswaar toepassing van functiescheiding is voorgeschreven, maar dat deze norm zich richt tot bestuursorganen en aangewezen organisaties. Uit de nota van toelichting blijkt niet of deze abstracte bewoordingen ook beogen de door de PIA bedoelde functiescheiding binnen de grote leveranciers te bewerkstelligen. Indien dat niet het geval is rijst de vraag hoe dan anderszins gewaarborgd is dat deze maatregelen zijn of zullen worden genomen.[11]

Verder wordt in de eerdergenoemde PIA aangegeven dat het niet uitgesloten is dat een organisatie, zeker als de rollen van authenticatiedienst en middelenuitgever daarin worden verenigd – aan de hand van ontvangen en doorgeleide authenticatieverzoeken naar dienstverleners – uit de logging kan herleiden welke dienstverlening door de gebruiker is afgenomen. In de PIA wordt daarom aanbevolen om expliciet nadere afspraken te maken dat deze logging niet voor andere doeleinden mag worden gebruikt dan de authenticatiedienstverlening en binnen het stelsel toezicht op naleving van deze afspraken te organiseren.[12] Het conceptbesluit verplicht bestuursorganen en aangewezen organisaties om te loggen met het doel om onbevoegde informatieverwerking en systeemtechnische fouten bij de toegang tot hun elektronische dienstverlening te kunnen ontdekken.[13] Een concreet verbod op misbruik of een zorgplicht en/of andere concrete voorschriften om misbruik van logging te voorkomen en/of toezicht te vergemakkelijken bevat het conceptbesluit echter niet. Ook blijkt uit de nota van toelichting niet of en zo ja hoe deze problematiek elders in de regelgeving voldoende is of zal worden ondervangen.

- De PIA over het eID-stelsel van 28 juni 2017 bevat op het punt van informatiebeveiliging de conclusie dat misbruikbestrijding op stelselniveau (nog) niet is ingevuld. Er wordt aanbevolen om maatregelen te treffen om op stelselniveau misbruik te kunnen herkennen (detectie) en te herstellen.[14] De AP constateert dat artikel 16 tot en met 24 van het conceptbesluit weliswaar regels met betrekking tot informatieveiligheid bij de toegang tot elektronische dienstverlening bevat, maar deze regels zien op bestuursorganen en aangewezen organisaties in de zin van de Wet digitale overheid. Daarmee is nog niet een volledig detectie- en herstelmechanisme bij misbruik op stelselniveau ingericht. Het voornemen is de detectie van misbruik (deels) uit te werken in technische specificaties door een notificatieplicht aan de burger wanneer op zijn naam een nieuw identificatiemiddel wordt aangevraagd. De AP acht dit een belangrijke maatregel ter bestrijding van misbruik, aangezien op deze wijze een controlemogelijkheid voor externe en onafhankelijke personen wordt geschapen. De AP is dan ook van oordeel dat deze maatregel ook in regelgeving dient te worden geborgd. Om voorts te kunnen beoordelen of het door de PIA opgemerkte punt dat misbruikbestrijding op stelselniveau niet is ingevuld, voldoende door het geheel aan wetgeving, toekomstige uitvoeringswetgeving en technische specificaties wordt gedekt, is het van belang dat in de nota van toelichting voldoende

[10] *Gegevensbeschermingseffectbeoordeling (GEB) eID-stelsel*, versie 1.0, 28 juni 2017, p. 43.
[11] Artikel 19, eerste lid, van het conceptbesluit.
[12] *Gegevensbeschermingseffectbeoordeling (GEB) eID-stelsel*, versie 1.0, 28 juni 2017, p. 37.
[13] Artikel 23, eerste lid, van het conceptbesluit.
[14] *Gegevensbeschermingseffectbeoordeling (GEB) eID-stelsel*, versie 1.0, 28 juni 2017, p. 6 en 36.

inzicht in het geheel aan beveiligingsmaatregelen wordt geboden. De essentie van voor het geheel belangrijke technische maatregelen hoort daarbij door vastlegging in de regelgeving te zijn geborgd.

- Tenslotte blijkt uit de nota van toelichting niet of en zo ja op welke punten het conceptbesluit de uitkomst is vanuit het oogpunt van de bescherming van persoonsgegevens overwogen alternatieven.[15] In de nota van toelichting bij het concept besluit is onder het kopje *Proportionaliteit en subsidiariteit* aangegeven dat deze beginselen leidend zijn geweest bij de totstandkoming van dit besluit.[16] De AP heeft in het advies bij het conceptwetsvoorstel digitale overheid hier ook aandacht voor gevraagd.[17] Het is van belang dat uit de toelichting blijkt dat er een zorgvuldige belangenafweging is gemaakt en dat daarbij alternatieven zijn onderzocht (subsidiariteitsbeginsel). Bij de verwerking van persoonsgegevens moet de privacy van de betrokkenen immers zo min mogelijk worden geschaad.

De AP adviseert de nota van toelichting en het conceptbesluit aan te vullen.

Toezicht door de AP

Volgens de nota van toelichting geschiedt toezicht op de naleving van de bepalingen in het conceptbesluit over de verwerking van persoonsgegevens door de AP. Voor wat betreft het bepaalde inzake informatieveiligheid is het toezicht op de dienstverleners belegd bij de minister van BZK, aldus de nota van toelichting.[18] Voor de goede orde merkt de AP op dat zij ook toezicht houdt op de beveiliging van persoonsgegevens ingevolge artikel 51, eerste lid, van de AVG j° artikel 6, tweede lid, van de Uitvoeringswet algemene verordening gegevensbescherming j° artikel 32 van de AVG. De AP adviseert om de nota van toelichting bij het conceptbesluit daarop aan te passen.

Bewaartermijnen in verband met het bedrijfs- en organisatiemiddel

Artikel 5, eerste lid, aanhef en onder e, van de AVG bepaalt:
Persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is (…).
Overweging 39 geeft het volgende aan: (…) *De persoonsgegevens dienen toereikend en ter zake dienend te zijn en beperkt te blijven tot wat noodzakelijk is voor doeleinden waarvoor zij worden verwerkt. Dit vereist met name dat ervoor wordt gezorgd dat de opslagperiode van de persoonsgegevens tot een strikt minimum wordt beperkt.* (…)

Het voorgestelde artikel 14c bevat verschillende bewaartermijnen ten aanzien van persoonsgegevens die worden verwerkt in het kader van het bedrijfs- en organisatiemiddel. De nota van toelichting bij het conceptbesluit bevat hierover de volgende toelichting:
Wat betreft de bewaartermijnen voor de persoonsgegevens die worden verwerkt ten behoeve van het bedrijfs- en organisatiemiddel (artikel 14c) is van belang, dat de gegevens voor vijf doelen worden verwerkt, te weten een functioneel doel (het laten werken van de systemen), een verantwoordingsdoel (zodat kan worden aangetoond dat de werkzaamheden

[15] De AP heeft ook ten aanzien van het conceptbesluit verwerking persoonsgegevens DigiD, DigiD Machtigingen, MijnOverheid en BSN-Koppelregister geadviseerd om in de nota van toelichting de subsidiariteit te onderbouwen. Brief van het CBP, *Wetgevingsadvies Besluit verwerking persoonsgegevens DigiD, DigiD Machtigingen, MijnOverheid en BSN-koppelregister*, 3 december 2015, p. 8.
[16] Nota van toelichting, *Proportionaliteit en subsidiariteit*, p. 22.
[17] Brief van de AP, *Advies ontwerp Wet generieke digitale infrastructuur*, 13 oktober 2017, p. 6.
[18] Nota van toelichting, *7 Toezicht en handhaving*, p. 24.

correct zijn uitgevoerd), het doel van foutopsporing (zodat problemen, zo nodig in samenwerking met ketenpartners, kunnen worden opgelost), het doel calamiteitenbestrijding (opdat de werking van het systeem kan worden hersteld na een probleem) en de bestrijding van misbruik. Dat vertaalt zich voor de verschillende gegevens die in het kader van het bedrijfs- en organisatiemiddel worden verwerkt in de aangegeven bewaartermijnen.[19]

Deze toelichting is evenwel geen onderbouwing van de lengte van de bewaartermijnen. De AP adviseert om alsnog de lengte van de bewaartermijnen met betrekking tot persoonsgegevens die worden verwerkt in het kader van het bedrijfs- en organisatiemiddel te onderbouwen in de nota van toelichting.

Reservekopieën

In de nota van toelichting bij het concept besluit is aangegeven dat reservekopieën van gegevens worden gemaakt om DigiD, DigiD Machtigen en MijnOverheid te kunnen herstellen na een calamiteit. Het doel van de reservekopieën is om het gehele productiesysteem terug te kunnen zetten in geval van een calamiteit. Omdat gegevens in de reservekopieën volgens de nota van toelichting niet raadpleegbaar of beschikbaar zijn, wordt het maken van de reservekopieën gezien als eerste stap in het vernietigingsproces. De reservekopieën worden maximaal vier maanden bewaard, aldus de nota van toelichting.[20]

Het conceptbesluit bevat geen bepaling waarin deze bewaartermijn van vier maanden is neergelegd. De AP adviseert om deze bewaartermijn alsnog op te nemen in het conceptbesluit en om de lengte van deze bewaartermijn te onderbouwen in de nota van toelichting.

Toepassen ISO/NEN normen

De artikelen 16 tot en met 19 van het conceptbesluit bevatten regels omtrent informatiebeveiliging. In de nota van toelichting is toegelicht dat deze bepalingen doelvoorschriften zijn, die ruimte laten voor eigen invulling.[21] Ingevolge het voorgestelde artikel 21 voldoen dienstverleners aan de artikelen 16 tot en met 19, indien zij de voor hen bepaalde ISO/NEN normen[22] aantoonbaar toepassen bij de inrichting van hun beheerssysteem inzake informatieveiligheid van de toegang tot hun elektronische dienstverlening. Volgens de nota van toelichting levert het volgen van de relevante ISO/NEN normen evenwel slechts een *vermoeden* op dat aan de eisen van de artikelen 16 tot en met 19 van het conceptbesluit wordt voldaan.[23]

De AP adviseert om het conceptbesluit in overeenstemming te brengen met de nota van toelichting, door met toepassing van Ar 3.10, tweede lid, van de Aanwijzingen voor de regelgeving, in het conceptbesluit op te nemen dat het toepassen van de betreffende ISO/NEN normen een weerlegbaar rechtsvermoeden oplevert dat aan de informatiebeveiligingseisen als bedoeld in de artikelen 16 tot en met 19 van het conceptbesluit wordt voldaan.

---

[19] Nota van toelichting, *Onderdeel M*, p. 33.
[20] Nota van toelichting, *Onderdeel j*, p. 32.
[21] Nota van toelichting, *Onderdeel O, Artikel 21*, p. 35.
[22] Het betreft ISO/NEN 27001 voor bestuursorganen en aangewezen organisaties (artikel 21, eerste lid, van het conceptbesluit) en ISO/NEN 7510 voor aangewezen organisaties als bedoeld in onderdeel 3 van de bijlage bij artikel 2, tweede lid, onder a, van de Wet digitale overheid (artikel 21, tweede lid, van het conceptbesluit).
[23] Nota van toelichting, *Onderdeel O, Artikel 21*, p. 35.

Datum
6 juli 2018

Ons kenmerk
z2018-05537

Tekstueel

In het voorgestelde artikel 14c is abusievelijk een bewaartermijn opgenomen van '18 maanden jaar'. Het woord 'jaar' dient te worden geschrapt.

Tevens bevat de nota van toelichting bij het conceptbesluit onder *Onderdeel M* een tekstgedeelte dat geen betrekking heeft op dit onderdeel maar op *Onderdeel L*. Het betreft het tekstgedeelte *Daarnaast wordt de kortere bewaartermijn* (…) *verwerkt door de minister van BZK*. Dit tekstgedeelte dient te worden geplaatst onder *Onderdeel L*.

Dictum

De AP adviseert de voordracht te doen nadat met het vorenstaande rekening zal zijn gehouden.

Hoogachtend,
Autoriteit Persoonsgegevens,

Mr. A. Wolfsen
Voorzitter