AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Prins Clauslaan 60, 2595 AJ Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Minister van Binnenlandse Zaken en Koninkrijkrelaties

Datum	Ons kenmerk	Uw brief van
14 september 2016	z2015-00357	17 juni 2016

Contactpersoon

Onderwerp
eID

Geachte ,

De Autoriteit Persoonsgegevens (AP, voorheen: het College bescherming persoonsgegevens) heeft bij brief van 7 mei 2015[1] een drietal onderwerpen aangekaart die naar haar mening onvoldoende in beschouwing zijn genomen bij de ontwikkeling van het eID-stelsel[2]. Dit betreft de verantwoordelijkheid voor de verwerking(en), de beveiliging van de verwerking(en) en het gebruik van het burgerservicenummer (BSN).

Van april tot en met juni 2016 hebben er pilots met publieke en private authenticatiemiddelen ten behoeve van (de ontwikkeling van) het eID-stelsel plaatsgevonden. Met betrekking tot deze pilots hebben de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO), Panteia en de Rijksdienst voor wegverkeer (RDW) onderzoeksrapporten opgesteld.[3] De commissie-Kuipers heeft toegezien op de onderzoeken.

[1] Brief College bescherming persoonsgegevens aan Logius / ministerie van Binnenlandse Zaken en Koninkrijkrelaties, *Introductieplateau eID*, z2015-00357, 7 mei 2015.
[2] Met de ontwikkeling van het eID-stelsel werkt de overheid samen met het bedrijfsleven aan de ontwikkeling van een standaard voor de toegang tot online dienstverlening. Het eID-stelsel moet het mogelijk maken dat burgers, consumenten en ondernemers op termijn online zaken kunnen doen met zowel de overheid als het bedrijfsleven. Het eID-stelstel heeft onvermijdelijk gevolgen voor de verwerking van persoonsgegevens van talloze mensen.
[3] Rapport TNO, *Uitkomsten van een onderzoek naar de betrouwbaarheid en veiligheid van de pilots publieke en private middelen in het BSN-domein*, 2016 R10582, 27 mei 2016;
Rapport Panteia, *Gebruikerservaringen pilots publieke en private eID-middelen*, 27 mei 2016;
Rapport RDW, *Evaluatierapport pilot DigiD-RDA, DigiD verstrekt met controle van het identiteitsbewijs*, 23 mei 2016.

Datum
19 augustus 2016

Ons kenmerk
z2015-00357

In haar rapport van 31 mei 2016 heeft de commissie-Kuipers geadviseerd over de uit de pilots te trekken bevindingen en de te nemen vervolgstappen.[4] Tevens heeft het Bureau ICT-toetsing (BIT) van uw ministerie van 5 januari tot 15 april 2016 het programma eID getoetst en op 12 mei 2016 advies hierover uitgebracht.[5]

Na deze evaluatie van de pilots heeft u bij brief van 25 augustus 2016 de Tweede Kamer geïnformeerd over de voortgang van het kabinetsbeleid met betrekking tot de verdere ontwikkeling van de infrastructuur voor (digitaal) inloggen en identificeren (eID beleid). Mede naar aanleiding van de evaluatie van de pilots komt u daarbij tot de conclusie dat kan worden besloten om door te zetten naar een volgende fase binnen het programma eID. Deze stap van verkenningsfase naar uitvoeringsfase is beoogd te starten per 1 oktober 2016.

In uw brief van 14 december 2015 heeft u aangekondigd dat er wettelijke eisen worden gesteld waaraan inlogmiddelen voor gebruik in het BSN-domein moeten voldoen, alsook waaraan hierbij betrokken partijen moeten voldoen. Deze eisen worden, zoals u in eerder genoemde brief heeft aangegeven, gesteld op basis van de wet Generieke Digitale Infrastructuur (Wet GDI). De AP verzoekt u dit wetsvoorstel te zijner tijd ter advisering aan de AP voor te leggen.

De AP acht het evenwel van belang om reeds in dit stadium aandacht te vragen voor een drietal onderwerpen, aangezien het eID-stelsel reeds in technische zin wordt ontwikkeld. Het AP acht het in dit geval van belang dat u reeds in deze fase van ontwikkeling kennis kunt nemen van het advies van de AP ten behoeve van de naleving van de Wet bescherming persoonsgegevens, omdat in een latere fase de noodzakelijke (technische) aanpassingen aan het eID-stelsel op basis van het advies van de AP zeer tijdrovend en kostbaar zullen zijn.

In navolging op haar eerdere advies van 7 mei 2015 en onverlet het reeds daarin vermelde, alsmede in reactie op uw brief van 25 augustus 2016 en op basis van een (globale) analyse van de voornoemde rapporten betreffende de pilots, adviseert de AP over (1) Privacy by design, (2) Incidentbeheersing en Toezicht, en (3) Beveiliging authenticatie eID.

Advies

1. Privacy by design

Privacy by design houdt in dat een organisatie al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen)aandacht besteedt aan privacy verhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Bovendien wordt al in de ontwikkelingsfase rekening gehouden met dataminimalisatie: het verwerken van zo min mogelijk persoonsgegevens, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking. Op die manier kan een zorgvuldige en verantwoorde omgang met persoonsgegevens (technisch) worden bereikt.

[4] Rapport commissie Kuipers, *Advies van de commissie evaluatie pilots publieke en private authenticatiemiddelen (commissie-Kuipers)*, 31 mei 2016.
[5] Brief BIT aan de minister van Binnenlandse Zaken en Koninkrijkrelaties, *BIT-advies programma eID*, 12 mei 2016.

Uit de bovengenoemde rapporten met betrekking tot de pilots leidt de AP af dat er tot nu toe tijdens de ontwikkeling van het stelsel onvoldoende aandacht is besteed aan (technische) privacyaspecten en daarmee niet volledig voldoet aan het principe van *privacy by design*. Zo stelt het rapport van TNO dat op het gebied van borging, ondersteund door een heldere governance van de stelsels en gegevens, er nog gebreken te bestaan. Ook de uitvraag naar logging heeft tot de conclusie geleid dat hier in de praktijk nog onduidelijkheid over bestaat. [6] Juist in de fase van ontwikkeling is het noodzakelijk dat deze aspecten worden onderkend en ingebouwd in het stelsel, voordat tot verdere ontwikkeling of uitrol wordt overgegaan.

De AP adviseert om alsnog het principe van *privacy by design* nadere toepassing te geven, en daarbij mede aandacht te besteden aan het door TNO uitgebrachte rapport[7], alvorens tot verdere ontwikkeling en/of uitrol van het programma eID over te gaan.

2. Incidentbeheersing en Toezicht

Wanneer fouten worden gemaakt in de gegevensverwerking kan het voor de betrokken burgers lastig zijn om dit te ontdekken en contact op te nemen met de juiste organisatie om het probleem te verhelpen.[8] Dit heeft te maken met de complexiteit van het stelsel, waarbij niet één organisatie een volledig overzicht heeft. Ook organisaties binnen het stelsel zullen hierdoor niet altijd in staat zijn om incidenten op te merken. Er zijn maatregelen denkbaar die de gevolgen van dergelijke incidenten kunnen helpen beperken. Maatregelen zoals betrokkenen via het centrale BSN-koppelregister informeren over belangrijke wijzigingen in zijn of haar account(s), zodat eventuele frauduleuze activiteiten sneller wordt opgemerkt. Betrokkenen laagdrempelig inzage geven in logs, voor zover die worden bijgehouden, kan hier ook aan bijdragen. Ook kan gekeken worden naar technische ontwikkelingen met betrekking tot PKI-systemen, zoals Certificate Transparency, die bedoeld zijn om de impact van vergelijkbare incidenten[9] te beperken.

Uit de onderzoeksrapporten betreffende de pilots blijkt nog van onvoldoende aandacht voor het detecteren en afhandelen van beveiligingsincidenten. Om een zorgvuldige verwerking van persoonsgegevens te waarborgen is het evenwel van belang dat er ook de nodige 'brandoefeningen' worden gehouden, naast het testen of een aantal publieke en private authenticatiemiddelen naar behoren kan functioneren. Hierbij is van belang dat vooraf duidelijk is wie verantwoordelijke is voor welke gegevensverwerking, wie verantwoordelijk is voor de controle op het (feitelijk) functioneren van het stelsel en op welke wijze de controle gaat plaatsvinden. De AP concludeert dat in het stelsel nog onvoldoende aandacht is voor incident-beheersing en toezicht.

---

[6] Zie eerdergenoemd Rapport TNO, 27 mei 2016, p. 111.

[7] Rapport TNO, 27 mei 2016, p. 111 "Op het gebied van borging, ondersteund door een heldere governance van de stelsels en gegevens, blijken echter nog gebreken te bestaan. (...) De uitvraag van de onderzoekers naar logging heeft echter tot de conclusie geleid dat hier in de praktijk nog onduidelijkheid over bestaat. (...) Een beperking binnen dit onderzoek was dat privacy-borging alleen beoordeeld kon worden op basis van documentatie en normenkaders.'.

[8] Zie eerdergenoemd Rapport commissie Kuipers, 31 mei 2016, p. 30 onder 'Voorbeeld Stop-ID'.
Rapport commissie Kuipers, *Advies van de commissie evaluatie pilots publieke en private authenticatiemiddelen (commissie-Kuipers)*, 31 mei 2016.

[9] Zoals ten aanzien van Diginotar waarbij maatregelen om incidenten te detecteren en de gevolgen van incidenten te beperken onvoldoende bleken te zijn.

De AP adviseert om in het ontwerp van het stelsel nadrukkelijk rekening te houden met het detecteren en afhandelen van beveiligingsincidenten, de inrichting van het interne toezicht en tevens tot het houden van 'brandoefeningen'.

3. Beveiliging authenticatie eID

Binnen het eID-stelsel kunnen betrokkenen gebruik maken van verschillende authenticatiemiddelen. DigiD zal één van deze authenticatiemiddelen worden. In de meeste gevallen waarin DigiD thans wordt gebruikt, wordt het beveiligingsniveau basis (gebruikersnaam en wachtwoord) gehanteerd.

Artikel 13 Wet bescherming persoonsgegevens vereist dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen dienen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau te garanderen gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen dienen er mede op gericht te zijn om onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

De AP is van oordeel dat het huidige lage beveiligingsniveau van DigiD, gelet op de stand van de techniek en de gevoelige en/of bijzondere persoonsgegevens (waaronder het BSN) die in het kader van DigiD worden verwerkt[10], onvoldoende is. De AP is van oordeel dat voor een authenticatiemiddel als DigiD ook nu reeds minimaal twee-factor authenticatie nodig is. Artikel 13 Wbp bepaalt bovendien dat een passend beveiligingsniveau (onder meer) afhankelijk is van de stand van de techniek. Dit betekent dat het (gehele) eID-stelsel, waar het authenticatiemiddel DigiD onderdeel van gaat uitmaken, in technische zin flexibel moet zijn, zodat snel en eenvoudig nieuwe en/of aanvullende beveiligingsmaatregelen kunnen worden getroffen wanneer een zich ontwikkelende stand van de techniek dat vereist.

De AP adviseert om het beveiligingsniveau van DigiD in het kader van de inrichting van het nieuwe stelsel te verhogen naar minimaal twee-factor authenticatie en tevens het eID-stelsel dusdanig te ontwerpen dat snel en eenvoudig nieuwe en/of aanvullende (technische) beveiligingsmaatregelen kunnen worden getroffen wanneer een zich ontwikkelende stand van de techniek dat vereist.

Verdere ontwikkeling eID

De AP vertrouwt erop dat dit advies, alsmede haar eerdere advies van 7 mei 2015, worden betrokken in de verdere ontwikkeling van het eID-stelsel. Wellicht ten overvloede wijst de AP erop dat deze brief niet kan worden beschouwd als een goedkeuring van het eID-stelsel als geheel, dan wel van onderdelen daarvan.

[10] DigiD geeft vaak toegang tot gevoelige en/of bijzondere persoonsgegevens en iedere keer dat juist wordt ingelogd met DigiD, wordt het BSN van de betrokkene vanuit Logius gestuurd naar de betreffende afnemer. Het BSN is een bijzonder persoonsgegeven.

Datum
19 augustus 2016

Ons kenmerk
z2015-00357

Deze brief zal door de AP middels de daarvoor geëigende kanalen worden openbaar gemaakt. Een afschrift van deze brief zendt de AP aan de minister van Economische Zaken.

Hoogachtend,

Autoriteit Persoonsgegevens,
Voor deze,

Mr. W.B.M. Tomesen
Vicevoorzitter