Bijlage 3 Privacyvisie

Recentelijk heb ik de Nota naar aanleiding van het verslag (NnavV) over de wet digitale overheid (WDO) aan uw kamer gezonden, waarin ik de vragen van uw kamer ter voorbereiding van dit wetsvoorstel heb beantwoord.

Als verwerkingsverantwoordelijke bij de inrichting van het eID-stelsel wil ik zorgdragen voor de juiste naleving van de Algemene Verordening gegevensbescherming (AVG) en privacywet- en regelgeving in breed verband. Om deze inrichting te sturen is een Privacyvisie eID opgesteld, waarin de toepasselijke privacyregels zijn geïnventariseerd en waarin stapsgewijs wordt aangegeven hoe deze doorwerken bij de inrichting van het eID-stelsel. Zoals ik u bij de NnavV van de WDO - naar aanleiding van vragen van de leden over de wijze waarop rekening wordt gehouden met de AVG - heb toegezegd zend ik u deze Privacyvisie bij gelegenheid van deze voortgangsrapportage toe.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Privacyvisie eID

Versie 1.0

Datum 10 december 2018
Status

Inhoud

Inleiding

Door het mogelijk te maken dat overheden als onderdeel van hun elektronische dienstverlening de identiteit van burgers beter kunnen vaststellen en de continuïteit daarvan te verhogen wordt de kans dat persoonsgegevens onbedoeld aan anderen ter beschikking worden gesteld en dat daarmee misbruik of fraude wordt gepleegd, aanzienlijk verkleind.

Deze maatregelen, die worden gerealiseerd met het eID stelsel, dragen aldus bij aan het terugdringen van privacyrisico's en verbetering van de bescherming van persoonsgegevens binnen het gehele overheidsdomein.

Deze ingezette beleidslijn voor continu beschikbare en hoogbetrouwbare inlogmethoden en daarbij horende inrichtingskeuzes sluit aan bij de Nederlandse Digitaliseringsstrategie[1], die de strategische doorvertaling van de ambities uit het Regeerakkoord bevat. Deze is recentelijk nog eens herbevestigd in de onlangs aan de Tweede Kamer aangeboden Agenda Digitale overheid (NL DIGIbeter[2]) en de daarop aansluitende kamerbrief over de voortgang van het programma eID[3].

Om de dienstverlening van het eID-stelsel zelf mogelijk te maken worden noodzakelijkerwijs ook persoonsgegevens verwerkt, waaraan privacyrisico's zijn verbonden. Het is daarom essentieel dat het eID-stelsel zelf ook zodanig wordt geregeld en ingericht dat aan het stelsel inherente en geïdentificeerde privacyrisico's zoveel mogelijk worden ondervangen. Bij de inrichting dient het beteugelen van dergelijke risico's uitgangspunt te zijn. Daartoe wordt privacybescherming binnen het eID-stelsel ingericht.

Deze privacyvisie eID beschrijft hoe de bescherming van persoonsgegevens binnen eID wordt aangepakt en ingericht. Daarbij zijn het geldende wettelijk (privacy)kader en de hiervoor genoemde beleidsuitgangspunten randvoorwaardelijk. Deze sturen tezamen de vormgeving van, en de benodigde persoonsgegevensverwerkingen binnen het eID stelsel en zijn daarmee ook richtinggevend voor de wijze waarop de bescherming van persoonsgegevens moet worden ingericht.

Het doel van deze privacyvisie eID is aan te geven welke eisen vanuit het juridisch (privacy)kader in combinatie met de vastgestelde beleidsuitgangspunten aan privacybescherming worden gesteld, en daarmee als vertrekpunt te dienen voor de verdere regeling (in wet en uitvoeringsregelgeving), en de verdere operationele inrichting van het stelsel.

[1] Bijlage bij Kamerstukken II 2017/18, 26 643, nr. 541
[2] Bijlage bij Kamerstukken II 2017/18, 26 643, nr. 549, p., p 41.
[3] Kamerstukken II 2017/18, 26 643, nr. 550.

1. Privacybescherming binnen het eID stelsel

Voor de inrichting van privacybescherming binnen het eID stelsel is een aantal factoren van belang. In de eerste plaats geldt daarbij het juridisch kader voor de bescherming van persoonsgegevens, zoals de Algemene verordening gegevensbescherming (AVG) en de Wet algemene bepalingen burgerservicenummer, waaraan moet worden voldaan. Dit kader stuurt de wijze waarop de bescherming van persoonsgegevens (en ook de beleids- en inrichtingskeuzes van het eID-stelsel) vorm moet krijgen.

Binnen dat juridisch kader gelden de genoemde beleidsdoelstellingen en -uitgangspunten, zoals de inzet van private partijen en gewenste gebruiksvriendelijkheid binnen de context ten behoeve van snelle adoptie van het stelsel binnen de overheid.

Het juridisch kader en de beleidsuitgangspunten hebben tezamen gevolgen voor de inrichting van privacy binnen het stelsel. Zij hebben gevolgen voor de zaken die moeten worden geregeld in wet- en regelgeving, omdat grondslagen voor de verwerking van persoonsgegevens wettelijk moeten worden geregeld.

Hieronder wordt eerst het juridisch kader besproken zoals dat voor eID geldt. Vervolgens worden de beleidskeuzes besproken die richtinggevend zijn voor het eID-stelsel. Daarna komen risico's aan bod die inherent zijn aan de context van het eID stelsel.

Daarna wordt aangegeven – bij de bespreking van het wetsvoorstel digitale overheid en de onderliggende uitvoeringsregelgeving – wat er wettelijk dient te worden geregeld en hoe dat gebeurt. Bij de bespreking van de punten wordt in de visie telkens aangegeven hoe het betreffende punt doorwerkt bij de nadere inregeling c.q. inrichting van het stelsel. Dit beoogt toetsing aan de visie mogelijk te maken.

2. Juridisch privacykader voor eID

Voor het eID stelsel betreft dat naast de Algemene Verordening Gegevensbescherming (AVG) de Uitvoeringswet AVG, die regels stellen aan de systematiek van bescherming van persoonsgegevens. Omdat het eID-stelsel wordt ingezet binnen het BSN-domein is ook wet- en regelgeving ten aanzien van het BSN van belang. Daarnaast is voor het eID-stelsel de eIDAS-verordening en uitvoeringsverordeningen van belang, omdat daarmee regels worden gesteld aan de vormgeving van identificatiemiddelen, die daarmee weer van invloed zijn op de verwerkingen van persoonsgegevens.

2.1. Europees Kader: Algemene Verordening Gegevensbescherming (AVG)

De AVG is sinds 25 mei 2018 rechtstreeks van toepassing. Met de Uitvoeringswet Algemene verordening gegevensbescherming (zie voor een toelichting hierna) is de Wet bescherming persoonsgegevens (Wbp) ingetrokken.

De AVG hanteert voor de bescherming van persoonsgegevens een bepaalde systematiek om op basis van een aantal privacybeginselen te komen tot afgewogen keuzes voor de bescherming van persoonsgegevens. Daarnaast schrijft de AVG aanvullend op een aantal aspecten meer in detail voor hoe persoonsgegevens moeten worden beschermd. In dit kader zijn het meest van belang de “transparantierechten” die aan betrokken worden toegekend en de verplichtingen om *privacy by design* als uitgangspunt te nemen en een PIA uit te voeren om zicht te krijgen op feitelijk spelende privacyrisico’s en daarop maatregelen te treffen.

De AVG wordt hieronder toegelicht.

2.1.1. Systematiek van bescherming van persoonsgegevens: privacybeginselen

De kern van de AVG wordt gevormd door een aantal grondslagen en beginselen dat als uitgangspunt moet worden genomen bij de (inrichting van) verwerking van persoonsgegevens.

2.1.2. Rechtmatige verwerking (verwerkingsgrondslag en doelbinding)

Uit de AVG volgt in de eerste plaats dat de verzameling en verwerking van persoonsgegevens plaatsvindt op een *rechtmatige en behoorlijke wijze* (artikel 5, eerste lid, aanhef en onder a, van de AVG). Verder dienen de doeleinden waarvoor verzameling en verwerking plaatsvindt gerechtvaardigd, welbepaald en uitdrukkelijk omschreven te zijn (*doelbinding*). Voor overheidsorganisaties geldt daarbij dat zij voor de verwerking van persoonsgegevens voor de hen toegekende taken in het kader van die taken over een expliciete verwerkingsgrondslag moeten beschikken.

<u>Doorwerking voor eID</u>
Voor het eID-stelsel betekent dit onder meer dat in een wettelijke verwerkingsgrondslag zal moeten worden voorzien. Op dit moment wordt een grondslag voor de toegang tot elektronische dienstverlening geregeld in artikel X van de Wet elektronisch berichtenverkeer Belastingdienst (EBV). Momenteel wordt met het wetsvoorstel digitale overheid (wetsvoorstel DO) en het onderliggende besluit digitale overheid de hand gelegd aan een meer op de toekomst toegesneden uitwerking. Dit zal bij de bespreking van het wetsvoorstel DO nader worden toegelicht.

2.1.3. Dataminimalisatie
Persoonsgegevens die worden verwerkt moeten toereikend en ter zake dienend zijn, en beperkt zijn tot wat noodzakelijk is voor de doeleinden. Daarbij gaat het om proportionaliteit en subsidiariteit, waardoor een minimum aan verwerking van persoonsgegevens wordt gerealiseerd (artikel 5, eerste lid, onder c, van de AVG). Er mogen niet meer gegevens dan nodig worden verwerkt en er moet goed worden bezien of het doel

niet op een manier kan worden bereikt die minder inbreuk maakt op privacy.

Doorwerking voor eID
Vertaald naar het eID-stelsel betekent dit dat dit als inrichtingsprincipe bij de vormgeving van het eID-stelsel moet worden meegenomen. Dataminimalisatie vormt een wegingsfactor bij de inrichting van het stelsel.

2.1.4. Juistheid van persoonsgegevens
De AVG bepaalt ook dat moet worden voorzien in maatregelen om te zorgen dat persoonsgegevens op een juiste wijze worden verwerkt en dat maatregelen worden getroffen om te zorgen dat gegevens die niet (meer) juist worden verwerkt, gerectificeerd of verwijderd worden (artikel 5, eerste lid, onder d, van de AVG).

Doorwerking voor eID
Ook dit is een belangrijk principe dat bij de vormgeving en inrichting van het eID-stelsel moet worden meegenomen. Het stelt eisen aan het herstelvermogen binnen het stelsel. Daarbij kan het bijvoorbeeld gaan om de reactie op vragen van burgers om vermeende fouten te corrigeren, maar ook om te zorgen dat fouten of optredende incidenten door de verantwoordelijke partijen snel en vroegtijdig kunnen worden opgemerkt en kunnen worden hersteld of – beter nog – kunnen worden voorkomen.

2.1.5. Opslagbeperking (bewaartermijnen)
Een volgend belangrijk uitgangspunt is dat persoonsgegevens niet langer worden verwerkt dan voor een termijn die gelet op het doel van verwerkingen noodzakelijk en daarmee te rechtvaardigen is (artikel 5 eerste lid, onder f, van de AVG).

Doorwerking voor eID
In de uitvoeringsregelgeving zullen bewaartermijnen worden vastgelegd, waarbij de gehanteerde termijnen beargumenteerd en geïmplementeerd moeten worden. Dit gebeurt op dit moment in het wetsvoorstel en – met name in – het besluit digitale overheid. Dit zal daar worden toegelicht.

2.1.6. Beveiliging van persoonsgegevens
Bij de verwerking van persoonsgegevens moeten technische en organisatorische maatregelen worden getroffen, zodanig dat een passende beveiliging gewaarborgd is (artikel 5, eerste lid, onder f, van de AVG). Ten aanzien van de beveiliging van persoonsgegevens werkt artikel 32 van de AVG dit uit. Bepaald wordt dat, waar passend, pseudonimisering en versleuteling dienen te worden ingezet. NB: pseudonimisering is dus niet per definitie verplicht, maar kan als oplossing behulpzaam zijn bij problemen ten aanzien van herleidbaarheid en het voorkomen van kwetsbare gegevensconcentraties.

Ook wordt aangegeven dat maatregelen moeten worden genomen om te zorgen dat op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen kan worden gegarandeerd, en dat de beveiligingsmaatregelen op gezette tijden getest en geëvalueerd worden. Voorts volgt uit dit artikel dat dient te worden voorzien in maatregelen om, bij een fysiek of technisch incident, de beschikbaarheid van en de toegang tot persoonsgegevens tijdig te kunnen herstellen. Voor de inrichting van beveiliging van persoonsgegevens dient rekening te worden gehouden met de zogeheten Richtsnoeren beveiliging

Persoonsgegevens, waarin de AP de wijze waarop beveiliging van persoonsgegevens kan plaatsvinden nader heeft uitgewerkt[4].

Doorwerking voor eID
Voor het eID-stelsel betekent het dat technische en organisatorische maatregelen moeten worden doorgevoerd in de (ICT-) systemen en processen om de gesignaleerde risico's ten aanzien van persoonsgegevens af te dekken. Welke maatregelen dat exact zijn hangt af van de risicoanalyse de daaruit voorkomende risico's en van de weging met overige (ontwerp) beginselen van verwerkingen van persoonsgegevens.

2.1.7. Specifieke aanvullende verplichtingen uit de AVG

Naast de modellering van bescherming van persoonsgegevens aan de hand van deze beginselen, regelt de AVG ter ondersteuning en kadering daarvan ook nog aan aantal meer concrete verplichtingen. De in dit kader meest relevante verplichtingen worden hieronder besproken.

Inregelen faciliteiten voor uitoefening rechten betrokkenen
Transparantie voor betrokkenen heeft in de AVG een belangrijke plaats gekregen. Een van de kernprincipes in de AVG is dat burgers zicht en controle kunnen houden over hun persoonsgegevens en kunnen ingrijpen als dat nodig is (hoofdstuk 3 AVG). De AVG kent aan burgers rechten tot om controle te houden over hun gegevens. Veel rechten (zie bijlage), zoals het inzage- en correctierecht, golden al onder de Wbp, maar een aantal rechten is nieuw of meer in de aandacht gezet, zoals het recht op overdraagbaarheid van gegevens ("dataportabiliteit").

Doorwerking voor eID
Voor het eID stelsel betekenen de toegekende "transparantierechten" dat bij de inrichting rekening zal moeten worden gehouden dat betrokkenen in staat zijn om zicht te hebben en houden over de persoonsgegevens die over hen worden verwerkt. Dat betreft zowel de gegevens die van hen staan geregistreerd bij de aanvraag van middelen als ook het gebruik dat ervan is gemaakt. Ook is belangrijk dat betrokken een overzicht wordt geboden in de middelen die van hem geregistreerd staan. In een stelsel als eID vergt dat voorzieningen om dat overzicht te bieden.

Privacy by design (& by default)
De AVG verplicht expliciet om in het ontwerp (design) van systemen en standaardinstellingen (default) reeds van het begin af aan rekening te houden met bescherming van persoonsgegevens. Er dienen bij het ontwerp technische en organisatorische maatregelen te zijn getroffen die de gegevensverwerking strikt beperken tot de noodzaak en persoonsgegevens mogen in beginsel – systeemtechnisch, d.w.z. zonder bewuste keuze - niet verwerkt/gedeeld worden.

Privacy by design komt er kortgezegd op neer dat bij de inrichting en inregeling van systemen en processen die de noodzakelijke verwerkingen van persoonsgegevens ondersteunen rekening wordt gehouden met de bescherming van persoonsgegevens. In feite betreft dat een weerslag van afweging tussen de genoemde privacybeginselen een invulling van de wijze waarop aan transparantieverplichtingen kan worden voldaan.

[4] http://wetten.overheid.nl/BWBR0033572/2013-03-01

Doorwerking voor eID
Het doorvoeren van Privacy bij Design binnen eID betekent dat bij het ontwerpproces van systemen en processen een afweging moet worden gemaakt tussen de besproken beginselen en verplichtingen.

Privacy Impact Assessment (PIA)
Uiteindelijk gaat het bij de bescherming van persoonsgegevens om het zoveel als mogelijk voorkomen van privacyrisico's en (vooral ook) om het voorkomen van onwenselijke gevolgen ervan voor burgers.

Naar aanleiding van de motie-Franken heeft het kabinet bepaald dat bij de ontwikkeling van beleid en wetgeving waaruit gegevensverwerkingen voortvloeien, bij de bouw van ICT-systemen en de aanleg van grote databestanden een PIA moet worden uitgevoerd. De AVG[5] verplicht tot het voorafgaand uitvoeren van een PIA voor gegevensverwerkingen met een hoog risico voor de rechten en vrijheden van natuurlijke personen. Daarvan wordt in elk geval geacht sprake te zijn als er sprake is van verwerkingen van persoonsgegevens met een hoog risico, zoals bij de inzet van nieuwe technieken of grootschalige gegevensverwerking - voorafgaand daarop – een PIA uit te voeren. Doel er van is om – aanvullend op de inrichting van bescherming van persoonsgegevens op grond van de reeds besproken beginselen, scherper zicht te krijgen op de feitelijk bij de verwerking of in de context spelende privacyrisico's en daarmee – als correctiemechanisme - rekening te houden bij de uiteindelijke (ontwerp) en beveiligingsmaatregelen.

Doorwerking voor eID
Bij onrechtmatige of onbedoelde verwerking van persoonsgegevens binnen het eID-stelsel kan gedacht worden aan verlies (beschikbaarheid) van de toegang tot een groot aantal overheidsdienstverleners. Bij een grootschalige ontwikkeling als het eID-stelsel is het maken en regelmatig onderhouden van een PIA zonder meer aan de orde gezien een aantal indicaties van een hoog risico die de AVG geeft: er is sprake van grootschalige verwerking van persoonsgegevens. Er is sprake van technieken die voor het eerst in onderlinge samenhang en grootschalig worden ingezet. En de gewenste functionaliteit van het stelsel en de context, namelijk de identiteitsvaststelling voor een groot aantal (overheids)organisaties die daarvan afhankelijk zijn en er op moeten kunnen vertrouwen, stelt hoge eisen aan veiligheid, privacybescherming en misbruikbestrijding. Voor het eID-stelsel is het uitvoeren van een PIA derhalve verplicht. In de ontwikkeling van het eID stelsel zijn daarom ook bij herhaling PIA's uitgevoerd. De PIA eID en de doorvertaling daarvan komt aan de orde bij de bespreking van de in de risico's die spelen bij eID (hoofdstuk 4).

Een PIA is een hulpmiddel
Overigens is en wordt binnen eID het "instrument" PIA ingezet als hulpmiddel voor bewustwording en planmatige inrichting van privacybescherming en het gedurende de ontwikkeling finetunen daarvan. Beoogd wordt om inzicht te geven in de gegevensverwerkingen die plaatsvinden, en daarmee bij te dragen aan de transparantie over de werking van eID. Naar de toekomst toe zullen daarom PIA's uitgevoerd blijven worden en zal op basis daarvan door de tijd bijstelling

[5] Art. 35 AVG.

plaatsvinden. PIA's zullen regulier onderdeel uit (moeten) maken van het proces.

2.1.8. Sluitstuk AVG: register- en verantwoordingsplicht

De AVG vereist dat organisaties (zowel verantwoordelijken als verwerkers) aantoonbare controle hebben over de persoonsgegevens die zij verwerken. Dit betekent dat een register moet worden bijhouden van alle verwerkingen van persoonsgegevens die plaatsvinden. De AVG schrijft concreet voor welke gegevens ten aanzien van verwerkingen moeten worden bijgehouden. Ook moet actief aandacht worden besteed aan, en maatregelen geïmplementeerd waaruit blijkt dat de organisatie de AVG-beginselen voor verwerking van persoonsgegevens naleeft.

Doorwerking voor eID

Om binnen eID aantoonbaar verantwoording te kunnen afleggen, bijvoorbeeld aan de Autoriteit Persoonsgegevens (de AP), moeten daarom verwerkingen geïnventariseerd zijn, en moeten er voor daadwerkelijke naleving operationele maatregelen, zoals beveiligingsmaatregelen zijn getroffen en worden onderhouden. Er moet kunnen worden uitgelegd hoe rekening houdend met de AVG ontwerpkeuzes zijn gemaakt en welke maatregelen zijn getroffen; dit gebeurt in de al eerder genoemde PIA.

Naleving van de AVG betekent overigens – ook voor eID - geen eenmalige handeling maar een doorlopend en continu proces. Processen zullen in de regel doorlopend in meer of mindere mate wijzigen. Bij nieuwe verwerkingen zal de naleving van privacyregels standaard onderdeel moeten vormen van de inrichting, en geadviseerd wordt om ten minste jaarlijks een actualisatie uit te voeren op al bestaande de verwerkingen van persoonsgegevens. Dit betekent dat de aspecten voor de verantwoordingsplicht moeten worden nagelopen. Opzet, bestaan en werking van de beheersmatige processen rond de AVG dienen dus te worden ingericht.

2.2. Europees kader: Europese eIDAS-verordening (910/2014)

De Europese eIDAS-verordening (910/2014) heeft tot doel om het vertrouwen in elektronische transacties en daarmee de elektronische handel binnen in de interne Europese markt te vergroten. De verordening voorziet in een gemeenschappelijke grondslag voor veilige elektronische interactie tussen burgers, bedrijven en overheden.

De verordening schept een kader voor wederzijdse (onderlinge) erkenning door nationale lidstaten van elektronische identificatiemiddelen. Het doel is om te komen tot eenduidige betrouwbaarheidseisen zodat burgers hun authenticatiemiddel ook in andere lidstaten kunnen gebruiken. Áls middelen aan de gestelde eisen voldoen, kunnen zij genotificeerd worden en dan moeten zij in de hele EU geaccepteerd worden.

Het uiteindelijke doel is om ook Nederlandse identificatiemiddelen te notificeren en burgers in staat te stellen om met hun Nederlandse eID middel bij organisaties elders in Europa te kunnen inloggen. Om deze reden wordt bij de ontwikkeling van deze middelen rekening gehouden met de uitvoeringsverordeningen die daaraan regels stellen. Naast eIDAS-uitvoeringsbesluiten die zien op samenwerking tussen lidstaten en het

notificatieproces zijn er uitvoeringsverordeningen die direct van invloed zijn om de inrichting van identificatiemiddelen en de persoonsgegevens die daarbij (moeten) worden verwerkt. Deze verordeningen zullen hieronder worden toegelicht.

2.2.1. Betrouwbaarheidsniveaus "Laag", "substantieel" en "hoog"

In de eIDAS-verordening worden – in artikel 8 – de criteria voor de betrouwbaarheidsniveaus gegeven.

Het betrouwbaarheidsniveau laag "betreft een elektronisch identificatiemiddel in het kader van een stelsel voor elektronische identificatie, dat een beperkte mate van vertrouwen in iemands opgegeven of beweerde identiteit biedt, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van misbruik of wijziging van identiteit te verkleinen";

Het betrouwbaarheidsniveau substantieel betreft "een elektronisch identificatiemiddel in het kader van een stelsel voor elektronische identificatie, dat een substantiële mate van vertrouwen in iemands opgegeven of beweerde identiteit biedt, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van misbruik of wijziging van identiteit te verkleinen";

Het betrouwbaarheidsniveau hoog betreft "een elektronisch identificatiemiddel in het kader van een stelsel voor elektronische identificatie, dat een hogere mate van vertrouwen in iemands opgegeven of beweerde identiteit biedt dan een elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van misbruik of wijziging van identiteit te voorkomen".

De technische specificaties en procedures waarnaar het artikel verwijst, en die richtinggevend zijn voor de vormgeving van identificatiemiddelen en authenticatiediensten, worden uitgewerkt in de eIDAS-uitvoeringsverordening 1502, die in paragraaf 2.3.1. zal worden besproken.

<u>Doorwerking voor eID</u>
Bij de vormgeving en inrichting van identificatiemiddelen moet ervoor gezorgd worden naar deze naar de eIDAS-indeling geclassificeerd kunnen worden.

2.2.2. Specifieke privacy bepalingen in de eIDAS-verordening

In de eIDAS verordening zelf is in artikel 5 expliciet opgenomen dat de verwerkingen van persoonsgegevens binnen de eIDAS context in overeenstemming moeten plaatsvinden met de Europese privacywetgeving (AVG).[6] Het tweede lid van artikel 5 voegt daaraan nog toe dat het gebruik van pseudoniemen in elektronische transacties niet mag worden verboden.

[6] De eIDAS-verordening dateert uit 2014 en verwijst nog naar Richtlijn 95/46/EG.

Doorwerking voor eID
Geen specifieke doorwerking anders dan dat het belang van naleving van het Europese privacykader onderstreept wordt.

2.3. Europees kader: eIDAS-Uitvoeringsverordeningen

2.3.1. Uitvoeringsverordening 2015/1502 (betrouwbaarheidsniveaus)

In de eIDAS uitvoeringsverordening 1502 wordt, door het stellen van technische specificaties en procedures, bepaald op welke wijze de vereisten en criteria van artikel 8 van Verordening (EU) nr. 910/2014 worden toegepast op elektronische identificatiemiddelen en authenticatiediensten.

Het betreft in de eerste plaats de inschrijving van een identificatiemiddel (waaronder de aanvraag, de registratie en het bewijs en verificatie van identiteit). Vervolgens komt het beheer van elektronische identificatiemiddelen aan de orde, waaronder het ontwerp en de lifecycle (uitgifte, beheer, verlenging en beëindiging) van identificatiemiddelen. Hierna volgen de waarborgen voor authenticatie(mechanisme). Voorts komen de elementen die zien op het beheer van organisatie aan bod, waaronder algemene eisen aan organisaties, de informatievoorziening aan gebruikers van identificatiemiddelen, informatiebeveiliging, administratie, faciliteiten en personeel en technische controles. Ten slotte wordt beschreven op welke wijze de naleving en controle daarop moet plaatsvinden.

Doorwerking voor eID
De doorwerking wordt hieronder toegelicht onder splitsing van het BSN- en het bedrijvendomein, waarvoor op dit moment gekozen is.

Doorwerking voor toegelaten middelen in het BSN-domein
In de Nederlandse uitvoeringspraktijk zal moeten worden getoetst of identificatiemiddelen en authenticatiediensten aan de eIDAS-criteria voldoen. Voor toelating van identificatiemiddelen tot het BSN-domein wordt daartoe een *Controleprotocol eID BSN domein* opgesteld, dat als beleidsregel zal worden vastgesteld ingevolge art. 9 lid 5 van de wet digitale overheid. Deze beleidsregel strekt tot vaststelling van een controleprotocol waarmee in de Nederlandse uitvoeringspraktijk kan worden getoetst aan de Europese niveaus van betrouwbaarheid van elektronische identiteitsmiddelen (eID) zoals uitgewerkt in de eIDAS-uitvoeringsverordening 1502. Het is wenselijk deze beleidsregel vast te stellen teneinde de conformiteit van de recentelijk ontwikkelde DigiD-varianten[7] op een hoger betrouwbaarheidsniveau met de betrouwbaarheidsniveaus “substantieel” en “hoog” als bedoeld in deze Europese regelgeving, te kunnen vaststellen. Ook kan het worden gebruikt voor de beoordeling van private inlogmiddelen die kunnen worden toegelaten als inlogmiddel bij dienstverlening waarbij het burgerservicenummer wordt gebruikt (het zgn. BSN-domein).

[7] Thans opgenomen in de Regeling voorzieningen GDI

Doorwerking voor erkende middelen in het Bedrijvendomein
In het bedrijvendomein zullen voor de uitvoeringspraktijk eveneens regels worden opgesteld. Dit vindt plaats bij AMvB en – als nadere uitvoering – bij ministeriele regeling. Inhoudelijk zullen de regels ten aanzien van uitgifte van identificatiemiddelen en authenticatiediensten niet verschillen, echter op een aantal aspecten, zoals uitgifte van middelen aan rechtspersonen en vertegenwoordiging van rechtspersonen zullen aanvullende zaken geregeld moeten worden.

De eIDAS uitvoeringsverordening maakt bij de kwalificaties laag, substantieel en hoog geen onderscheid tussen de mate van zekerheid van identiteitsvaststelling tussen burgers en bedrijven. Materieel wordt dezelfde mate van zekerheid beoogd, en is het doel ook gelijkwaardig. Het betrouwbaarheidsniveau is in alle gevallen bedoeld om belangen van de dienstverlening die ermee wordt ontsloten te beschermen. In het burgerdomein zullen dat in de regel persoonlijke (financiële) en privacybelangen zijn. Maar ook in het bedrijvendomein waar natuurlijk financiële en bedrijfsbelangen beschermd moeten worden, kan het gaan om toegang tot persoonsgegevens.

Het ligt daarom ook in de rede om de eisen die in Nederland aan middelen in de twee domeinen gesteld worden gelijkluidend te laten zijn.

2.3.2. Uitvoeringsverordening 2015/1501 (Interoperabiliteit binnen Europa)

Een belangrijk uitgangspunt van de eIDAS-verordening is om binnen Europa grensoverschrijdend gebruik van identificatiemiddelen mogelijk te maken. Uitvoeringsverordening 1502, regelt een aantal aspecten om deze interoperabiliteit mogelijk te maken. Er wordt bepaald dat lidstaten knooppunten moeten inrichten om een eigen identificatielandschap te ontsluiten voor genotificeerde middelen uit andere lidstaten, en moeten zorgen dat hun eigen middelen in andere lidstaten gebruikt kunnen worden voor diensten waarvoor inloggen op betrouwbaarheidsniveau substantieel of hoog wordt vereist.

2.3.3. Specifieke privacybepalingen in uitvoeringsverordening 1501

De uitvoeringsverordening 1502 heeft expliciet aandacht voor de borging van de bescherming van persoonsgegevens bij de inrichting van de nationaal knooppunt (eIDAS-knooppunt). In artikel 6 van de uitvoeringsverordening wordt vereist dat de “de bescherming van privacy en vertrouwelijkheid van de door de knooppunten uitgewisselde gegevens en de handhaving van de integriteit van die gegevens wordt gewaarborgd door middel van de best beschikbare technische oplossingen en beschermingsmethoden” (art. 6 lid 1). Het tweede lid stelt direct eisen en beperkingen aan de functionaliteit en het bewaren van gegevens door het eIDAS knooppunt door de bepalen dat deze knooppunten geen gegevens mogen opslaan. Uitzondering vormt de opslag van gegevens om ingeval van incidenten reconstructie van uitwissing van berichten (authenticatieverklaringen) mogelijk te maken. Het betreft in ieder geval gegevens over de identificatie van het knooppunt, identificatie van het

bericht en datum en tijd van het bericht. De bewaartermijnen mogen daarbij nationaal bepaald worden.

Doorwerking voor eID
Bij de inrichting en vormgeving van het eIDAS-knooppunt dient het bepaalde in dit artikel in acht genomen te worden. Functionaliteit, de logging en het bewaren ervan dient te stroken met het artikel.

2.3.4. Persoonsidentificatiegegevens ("Minimale dataset")

Een belangrijk punt voor identificatiemiddelen om gebruikt te kunnen worden in andere lidstaten is dat zij voldoende persoonsgegevens (attributen) leveren die natuurlijke personen (of rechtspersonen) op unieke wijze vertegenwoordigen. Overheidsorganisaties buiten Nederland hebben (immers) niet de beschikking over het BSN aan de hand waarvan zijn benodigde gegevens kunnen achterhalen. En datzelfde geldt vice versa voor Nederlandse overheidsorganisaties. De uitvoeringsverordening bepaalt daarom in artikel 11 dat een zogeheten minimaal pakket persoonsidentificatiegegevens (ook wel minimale dataset, MDS) moet worden geleverd. Voor natuurlijke personen is in de bijlage bij uitvoeringsverordening 1501 bepaald dat de volgende attributen verplicht moeten worden geleverd: huidige familienaam of familienamen, huidige voornaam of voornamen, geboortedatum en een door de lidstaat toe te kennen unieke identificatiecode ("uniqueness ID"). Daarnaast mogen aanvullend voornamen of familienamen bij geboorte, geboorteplaats, huidig adres en geslacht als aanvullend attribuut worden opgenomen.

Doorwerking voor eID
Om in Europa gebruikt te kunnen worden dient de minimale gegevensset te kunnen worden geleverd. Bij de (technische) vormgeving moet worden ingeregeld dat identificatiemiddelen deze set kunnen leveren.

2.4. Nationaal kader: Uitvoeringswet AVG (UAVG)

Met de UAVG wordt uitvoering gegeven aan de AVG. De AVG is een Europese verordening. Dat betekent dat voor de lidstaten nog maar beperkt ruimte is voor de nationale wetgever om op het terrein van de verwerking van persoonsgegevens zelf iets (afwijkends) te regelen. Daar waar de verordening nog wel ruimte laat voor nationale keuzes, is gekozen om zo dicht mogelijk te blijven bij de Wbp (beleid-neutrale implementatie). In dit verband is het meest relevant dat artikel 87 van de AVG een grondslag geeft om bij nationaal recht specifieke voorwaarden te stellen voor de verwerking van nationale identificatienummers, in Nederland onder meer het BSN.

2.4.1. Regeling van het BSN in de Uitvoeringswet AVG

De Uitvoeringswet AVG regelt het gebruik van wettelijk voorgeschreven nummers, beleidsneutraal en overeenkomend met het voorheen geldende artikel 24 van de Wbp. De nu geldende regels voor verwerking van het BSN worden dus gecontinueerd. Dit betekent dat voor verwerking van het BSN een wettelijke grondslag nodig is. Voor overheidsorganen betreft artikel 10 van de Wabb. Voor de verwerking van het BSN door private partijen betekent de regeling dat dient te worden voorzien in een specifieke wettelijke grondslag. Hieronder wordt dit nader toegelicht.

Artikel 46 van de UAVG regelt dat een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, bij de verwerking van persoonsgegevens slechts gebruikt wordt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald. In feite is dit een kapstokbepaling, op basis waarvan in andere wetten invulling kan worden gegeven aan dergelijke nummers.

In de praktijk bestaat soms de wens het BSN ook voor andere doelen te gebruiken dan ter uitvoering van de wet waarin het voorschrift over het nummer is opgenomen. Dit is alleen gerechtvaardigd als aan twee vereisten is voldaan. Ten eerste geldt het algemene vereiste dat persoonsgegevens alleen verder mogen worden verwerkt als dat verenigbaar is met de doeleinden waarvoor ze zijn verkregen. Ten tweede bepaalt artikel 46 van de Uitvoeringswet dat verwerking van persoonsnummers voor andere doeleinden dan de uitvoering van de betreffende wet alleen mogelijk is voor zover dat bij de wet is bepaald. Dit is een aanvullende eis op die van verenigbaarheid omdat het gebruik van persoonsnummers extra risico's met zich kan brengen voor de bescherming van de persoonlijke levenssfeer, zoals bijvoorbeeld identiteitsfraude.

Eventuele andere gebruiksdoelen dienen derhalve door de formele wetgever zelf te worden vastgesteld. Er komt ten aanzien van de verdere verwerking van het BSN geen eigen afweging toe aan de verwerkingsverantwoordelijke. Hiermee is in de Uitvoeringswet gebruik gemaakt van de nationale ruimte die de verordening biedt om specifieke voorwaarden te stellen aan de verwerking van een nationaal identificatienummer op grond van artikel 6, tweede lid, en 87 van de verordening.

2.5. Wet algemene bepalingen burgerservicenummer en sectorale wetgeving

Voor de overheid is het gebruik van een uniek persoonsnummer, het burgerservicenummer (BSN), geregeld in artikel 10 Wet algemene bepalingen burgerservicenummer (Wabb). Overheidsorganen kunnen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun publieke taak gebruikmaken van het BSN, zonder dat daarvoor nadere regelgeving vereist is. Vanzelfsprekend moet die publieke taak er dan wel zijn, ingevolge een aan hen opgedragen wettelijke taak of anderszins.

Voor instellingen die geen beroep kunnen doen op artikel 10 Wabb dient het gebruik te zijn voorgeschreven in sectorale wetgeving. Zo geldt bijvoorbeeld voor de zorgsector de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (voorheen: Wet gebruik burgerservicenummer in de Zorg), in het onderwijs de wet BSN in het onderwijs. Daarnaast is in bepaalde situaties het gebruik van het BSN specifiek aangewezen. Zo moeten banken het BSN gebruiken voor uitwisseling van gegevens met de Belastingdienst.

Doorwerking voor eID
Het eID stelsel beoogt toegang te verlenen tot elektronische dienstverlening van (semi)overheidsorganisaties en aangewezen (private) organisaties die voor deze dienstverlening gebruik maken van het BSN. Binnen het eID stelsel wordt het BSN gebruikt. Voor eID betekent het bovenstaande dat partijen die het BSN verwerken over een publieke taak (ingeval van overheden) dan wel een expliciete wettelijke grondslag (ingeval van aangewezen organisaties en andere private partijen) moeten

beschikken. Dit betekent dat, waar dat noodzakelijk is voor de werking van het stelsel, daarvoor grondslagen moeten worden gecreëerd en dat inkadering van de verwerking moet plaatsvinden. Dit wordt nader toegelicht bij de bespreking van het wetsvoorstel DO.

3. Beleidsuitgangspunten eID

3.1. Beleidsagenda Digitale Overheid (*NL DIGIbeter*)

Recentelijk is de beleidsagenda Digitale Overheid (*NL DIGIbeter*) vastgesteld. Hierin wordt de beleidsagenda voor de digitale overheid in breder verband geschetst, waarbij ook de uitgangspunten voor de ontwikkeling van identificatiemiddelen aan de orde komt[8]. Deze uitgangspunten bepalen de beleidsrichting voor eID en daarmee ook de operationele inrichting op onderdelen. In het verlengde daarvan zijn zij mede van invloed op de vormgeving van privacybescherming binnen het eID-stelsel.

Kort samengevat komen de in dit kader – voor deze privacy visie relevante - beleidsuitgangspunten in *NL DIGIbeter* op het volgende neer.

3.2. Verhogen van betrouwbaarheid en continuïteit identificatiemiddelen

Voor de ontwikkeling van de digitale overheid is modernisering van elektronische identificatiemiddelen (eID-middelen) en meer betrouwbare identiteitsvaststelling voor elektronische transacties tussen overheid en burgers en bedrijven daarbij van vitaal belang.[9] Het kabinet wil daarnaast voor het publieke domein de continuïteit verhogen door de afhankelijkheid van DigiD als exclusief authenticatiemiddel te verminderen, door gebruikers op het moment dat een middel onverhoopt niet werkt in staat te stellen andere authenticatiemiddelen te gebruiken. Om dit mogelijk te maken, is ervoor gekozen om toegang tot digitale overheidsdienstverlening via meer dan één inlogmiddel te realiseren, waarbij tevens de inzet van private authenticatiemiddelen wordt voorzien.

NL DIGIbeter:
Het Nederlandse identiteitsstelsel moet zeer betrouwbaar en praktisch zijn en niet fraudegevoelig. Daarbij wordt gewerkt met innovatieve oplossingen die dit waarborgen. In de komende jaren dient DigiD te worden verbreed, waarbij de strategie is om de groep rechthebbenden op DigiD te verbreden en ervoor te zorgen dat meer mensen DigiD op het betrouwbaarheidsniveau 'substantieel' gaan gebruiken. Ook zal DigiD op betrouwbaarheidsniveau 'hoog' worden aangeboden.

[8] NL DIGIbeter, Agenda Digitale Overheid, p 41.
https://www.digitaleoverheid.nl/nldigibeter/
[9] Zie Tweede Kamerbrief van 21 december 2016, 2016-0000790934.

Ook is als uitgangspunt opgenomen dat een of meer private eID-middelen toe worden gelaten en dat het mogelijk wordt gemaakt dat ook eID-middelen uit andere EU-lidstaten in Nederland gebruikt kunnen worden. Dit betekent dat er dan naast DigiD ook alternatieve inlogmiddelen zijn.

Om deze beleidsdoelen, hogere betrouwbaarheid en continuïteit, te realiseren is het eID-stelsel opgezet. Het stelsel moet burgers en bedrijven in staat stellen op een veilige en betrouwbare manier digitaal zaken te doen met organisaties in het publieke domein. Binnen het publieke domein, ook wel het Burger Service Nummer domein (BSN-domein) genoemd, omdat het primair (semi) overheidsorganisaties zijn die het BSN mogen en moeten gebruiken, kunnen zowel publieke als private leveranciers authenticatiemiddelen aanbieden. Daarbij geldt als uitgangspunt dat de bestaande voorzieningen, zoals machtigingsvoorzieningen (DigiD Machtigen) gebruikt kunnen blijven worden.

Om de betrouwbaarheid te kunnen garanderen, moeten leveranciers van middelen vooraf toegelaten worden. Daarvoor dienen zij aan Europese eIDAS-eisen te voldoen die beogen de veiligheid en betrouwbaarheid van identificatiemiddelen te waarborgen. Daarbij wordt onderscheid gemaakt in verschillende eisen voor de zogeheten betrouwbaarheidniveaus “laag”, “substantieel” en “hoog”, die deze verordening onderkent. Hoe hoger het betrouwbaarheidsniveau, hoe hoger de mate van zekerheid van identiteitsvaststelling is.

Doorwerking voor eID
Dit beleidsuitgangspunt stuurt de vormgeving van eID in die zin dat burgers moeten kunnen beschikken over meerdere alternatieve inlogmiddelen. Dit bepaalt in belangrijke mate de vormgeving van het stelsel.

3.3. Notificeren identificatiemiddelen binnen EU (eIDAS)

NL DIGIbeter: om bedrijven te ondersteunen bij zakendoen over de grens wordt de wederzijdse erkenning van elektronische identificatie geregeld (eIDAS verordening 2014/910). Ook wordt gezorgd dat burgers en bedrijven DigiD en eHerkenning kunnen gebruiken als zij binnen de Europese Unie een dienst afnemen van publieke dienstverlener.

Door - zoals aangegeven in de vorige paragraaf – voor de toelating en erkenning van middelen aan te haken op de Europese eIDAS-eisen zal het eID-stelsel burgers uiteindelijk in staat te stellen om ook grensoverschrijdend digitale diensten af te nemen van andere Europese lidstaten. Daarvoor is het nodig dat het stelsel kan samenwerken met stelsels uit andere EU-lidstaten. Een voorziening die dit mogelijk maakt zal ingericht moeten worden (eIDAS-knooppunt).

Doorwerking voor eID
De beleidskeuze om identificatiemiddelen te notificeren brengt met zich mee dat identificatiemiddelen die worden ontwikkeld of toegelaten de minimale dataset moeten kunnen leveren. Daarmee dient bij de inrichting van het stelsel rekening te worden gehouden (vergelijk ook de doorwerking van paragraaf 2.3.4.).

3.4. Snelle en efficiënte adoptie van het stelsel binnen het overheidsdomein

Om als privacy maatregel effect te kunnen hebben en uiteindelijk snel een belangrijke bijdrage te kunnen leveren in breder verband (privacybescherming bij dienstaanbieders) is het belangrijk dat het eID-stelsel werkbaar is in termen van gebruikersgemak. Dat heeft een belangrijk effect op het gebruik en adoptiesnelheid.

Dat geldt zowel voor burgers als voor overheidsorganisaties die er gebruik van (moeten gaan) maken. Hogere veiligheid van identificatiemiddelen betekent vaak een complexere hanteerbaarheid en waardoor (minder-digitaalvaardige) burgers eerder zullen afhaken en andere wegen zullen zoeken die uiteindelijk risicovoller kunnen zijn. Een hogere betrouwbaarheid draagt in dat geval per saldo niet bij aan een verbetering van privacy. Voor overheidsorganisaties geldt dat zij vaak te maken hebben met bestaande processen en informatiesystemen en dat aanpassing de nodige tijd kost. Hoe complexer aansluiting op het eID stelsel is, hoe lager de adoptiesnelheid kan en waarschijnlijk zal zijn.

Doorwerking voor eID
Bovenstaande betekent dat bij de inrichting van privacybeschermende maatregelen niet alleen van belang is hoe die maatregelen privacybeschermend werken binnen het stelsel zelf, maar ook wat zij betekenen voor de werkbaarheid en adoptie binnen het bredere overheidsdomein en de beoogde privacybescherming daarin.

Om snel effectief te kunnen zijn binnen het overheidsdomein en met betrouwbare identiteitsvaststelling een bijdrage te kunnen leveren aan privacybescherming in het brede overheidsdomein, is beleidsmatig een snelle adoptie van het stelsel van belang en gewenst. Gebruiksvriendelijkheid c.q. laagdrempelige toepasbaarheid is voor zowel burgers als overheden een belangrijk uitgangpunt. Dat geldt zowel voor het gebruik door burgers als de wijze waarop aansluiting op het stelsel door overheidsorganisaties kan worden gerealiseerd.

4. Resterende privacy risico's eID-stelsel

4.1. Privacy risico's als sturende factor bij de inrichting van privacybescherming

De AVG verplicht tot het uitvoeren van een privacy impactanalyse (PIA) voor gegevensverwerkingen met een – te verwachten - hoog risico voor de rechten en vrijheden van natuurlijke personen. De PIA vormt daarbij in die gevallen een wezenlijk en sturend onderdeel bij de inrichting van privacybescherming.

Bij een grootschalige ontwikkeling als het eID-stelsel is een PIA nodig gezien een aantal indicaties van een hoog risico die de AVG geeft: er is sprake van grootschalige verwerking van persoonsgegevens. De gewenste

functionaliteit van het stelsel en de context, namelijk de identiteitsvaststelling voor een groot aantal (overheids)organisaties die daarvan afhankelijk zijn en er op moeten kunnen vertrouwen, stelt hoge eisen aan veiligheid, privacybescherming en misbruikbestrijding. Op grond van de AVG en eerder kabinetsbeleid is een PIA voor het eID-stelsel derhalve verplicht.

4.2. PIA als instrument om risico's in kaart te brengen

Een PIA heeft tot doel om van voorgenomen regelgeving of projecten waarbij persoonsgegevens worden verwerkt, de privacyrisico's op een gestructureerde en gestandaardiseerde wijze in kaart te brengen, om op basis hiervan maatregelen te treffen om deze risico's te voorkomen of verkleinen en transparante afwegingen mogelijk te maken tussen de privacyrisico's van verschillende alternatieven.

De beoogde functie van de PIA is aldus om, naast richting die reeds voor privacybescherming bepaald wordt door de geldende wet en regelgeving, de feitelijk spelende risico's een (bij) sturende rol te laten spelen.

Daarmee draagt een PIA bij aan de nakoming van de verantwoordingsplicht tot naleving van de 'beginselen inzake verwerking van persoonsgegevens' zoals vastgelegd in de AVG. De PIA beoogt ook bij te dragen aan verdere verhoging van het privacybewustzijn bij de vele organisaties die het eID-stelsel mede ontwikkelen en implementeren.

4.3. PIA op het eID stelsel

Voor het eID-stelsel is in 2017 een PIA dan ook uitgevoerd, op het conceptueel kader van het eID-stelsel. Op dat moment werd – en ook nu nog wordt - gewerkt aan de (detail)uitwerking van zowel functionaliteit van het eID-stelsel als de kaders daaromheen. Het eID-stelsel en de bescherming van persoonsgegevens zijn daardoor dan ook nog niet "af". Het feit dat sprake is van een tussentijdse doorkijk betekent onvermijdelijk dat bepaalde zaken nog moeten worden uitgewerkt. Sprake is van een continu (verbeter)proces.

Het juridisch kader en de beleidsuitgangspunten sturen de inrichting van de bescherming van persoonsgegevens. Door op grond daarvan privacybescherming in te richten worden privacyrisico's afgedekt. Daarnaast spelen er gezien bepaalde beleidskeuzes en de context waarin het eID stelsel wordt gebruikt nog een aantal feitelijk resterende risico's, waarmee bij de regeling en inrichting van het eID stelsel rekening moet worden gehouden. Deze zijn grofweg onder te verdelen in inherente risico's aan het stelsel zelf, risico's aan de inzet van private partijen en risico's die kleven aan de context waarin het eID-stelsel wordt ingezet. Deze worden hier kort besproken. Het is belangrijk dat hiervoor bij de feitelijke inrichting van het eID stelsel aandacht is.

Voor een volledige weergave van de risico's wordt verwezen naar de eerder uitgevoerde PIA op het eID stelsel.[10] Opgemerkt wordt dat (rest)risico's door de tijd kunnen en zullen veranderen. Dit betekent dat PIA's periodiek moeten worden herhaald om de risico's te actualiseren en de te nemen maatregelen daarop te laten aansluiten. Dit sluit ook aan bij de insteek van de AVG; privacybescherming is vormgegeven als een doorlopende activiteit. Bij de verdere inrichting en vormgeving zal hier rekening mee worden gehouden.

4.4. Opvolging PIA en de Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens heeft – in het kader van haar adviserende rol ten aanzien van de wet en regelgeving expliciet aandacht gevraagd voor de (de opvolging van een aantal in de) in de PIA gesignaleerde risico's en de daarbij gedane aanbevelingen[11]. Dat geldt zowel voor de zaken die wettelijk geregeld dienen te worden – zoals wettelijke grondslagen en inkadering – als bij de operationele inrichting van het stelsel.

4.5. Inherente Privacyrisico's aan het eID stelsel zelf

Risico's verlies van het middel/gebruik middel door anderen.
Een gevolg van de centrale rol van het eID stelsel bij overheidsidentificatie is dat bij onrechtmatige of onbedoelde verwerking of verlies van persoonsgegevens (beschikbaarheid) onbevoegde toegang kunnen krijgen tot een groot aantal overheidsdienstverleners die op het stelsel zijn aangesloten. Verlies van eID-inlogmiddelen kan ongeoorloofde wijziging van gegevens bij dienstverleners (integriteit) betekenen, of ongeoorloofde afname van dienstverlening door derden. Gelet op de schaalgrootte en context waarin het stelsel wordt gepositioneerd kunnen de negatieve gevolgen in potentie groot zijn, en doorwerken tot ver buiten het eID stelsel zelf. Verlies van controle over hun eID-middelen of een inbreuk op de goede werking kan voor gebruikers leiden tot (blootstelling aan) identiteitsdiefstal of –fraude en bijbehorende financiële verliezen. Omdat beoogd wordt dat ook zorgverleners gebruik kunnen maken van het stelsel zal ook verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens aan de orde kunnen zijn.

<u>Doorwerking voor eID</u>
Het is van belang om te voorzien in een vangnet, waarmee misbruik stelselbreed kan worden aangepakt als het onverhoopt toch plaatsvindt (herstelvermogen). In alle gevallen van misbruik is het van belang om dit tijdig te onderkennen en daarom te voorzien in mogelijkheden om misbruik snel te kunnen herkennen. Verder moet worden voorzien in mogelijkheden om, als het misgaat, misbruik te kunnen herstellen (dat wil zeggen: maatregelen nemen om misbruik te stoppen) en hulp te kunnen bieden aan burgers, bedrijven en overheden die daarvan het slachtoffer zijn geworden. Rekening zal moeten worden gehouden met het feit dat misbruik van persoonsgegevens kan plaatsvinden. Ontwerpmaatregelen moeten er erop gericht zijn incidenten zo snel mogelijk te ontdekken, de

[10] https://www.rijksoverheid.nl/documenten/rapporten/2017/06/28/gegevensbescherm ingseffectbeoordeling-eid-stelsel
[11] Advies conceptbesluit digitale overheid, Autoriteit Persoonsgegevens, brief van 11 juli 2018, kenmerk z201 8-05537

gevolgen daarvan zoveel mogelijk te beperken (compartimentering) en snel te herstellen. Juridisch – in de wet digitale overheid en uitvoeringsregelgeving – moeten de grondslagen worden geregeld.

4.6. Risico's aan de inzet van private partijen

Een feitelijk risico dat speelt bij de inzet van private partijen binnen het eID stelsel, is dat private partijen inzicht zouden krijgen in de zaken die burgers met de overheid afwikkelen. Het is noodzakelijk voor deze partijen om voor de vervulling van bepaalde taken persoonsgegevens te kunnen verwerken. Door afspraken te maken kan dit risico beperkt worden. Het heeft echter de voorkeur om – voor zover dat mogelijk is – in het ontwerp ervoor te zorgen dat partijen niet de beschikking (hoeven te) hebben over persoonsgegevens.

Doorwerking voor eID
Essentieel is daarom, zeker bij de voorgenomen inzet van private leveranciers van inlogmiddelen dat de gegevensverwerking zodanig wordt ontworpen en ingericht, dat geen van de bij authenticatie betrokken partijen (inclusief dienstverleners) kan zien welke andere websites door de houder van het middel worden bezocht. Dit is niet alleen belangrijk voor de bescherming van persoonsgegevens als zodanig, maar doet tevens recht aan het uitgangspunt dat de betrokken partijen geen inzicht in of bemoeienis moeten kunnen hebben met zaken die gebruikers in het publieke domein afwikkelen.

Uit de EIDAS-verordening, noch uit de huidige juridische kaders, volgt een strikt voorschrift voor de specifiek te nemen technische maatregelen en de sterkte ervan. Het uitgangspunt *'privacy by design'* vanuit de AVG kan eveneens op verschillende manieren worden vormgegeven in proces en techniek. Los daarvan er een belang om een sterke – toekomstbestendige - bescherming van de privacy van authenticatiemomenten in de techniek te implementeren, mede vanuit het oogpunt van voorziene doorontwikkelingen van het stelsel, waarbij ook private ondernemingen een belangrijkere rol gaan spelen. Het is dan essentieel dat private partijen met mogelijk meerdere belangen in hun dienstverlening aan de burger, deze belangen strikt gescheiden weten binnen het eID-stelsel.

4.7. Privacyrisico's binnen de context waarin het eID-stelsel wordt gebruikt

Herleidbaarheid, datalekken en betrouwbaarheidsniveau's.
Binnen het eID-stelsel zelf worden in de logging geen bijzondere of strafrechtelijke persoonsgegevens verwerkt. Wel kunnen, door voor de werking noodzakelijke logging, patronen in andere persoonsgegevens die in het eID-stelsel worden verwerkt een indicatie of voorspeller zijn van (bijzondere) persoonsgegevens, bijvoorbeeld als wordt ingelogd bij specifieke zorgverleners of bij bijvoorbeeld de reclassering.

De noodzaak van het al dan niet voorkomen van herleidbaarheid van persoonsgegevens, en het risico van de gevolgen van datalekken te minimaliseren zal met name afhangen van het risico dat door de herleidbaarheid gelopen wordt.

Denkbaar is dat er verschil is in noodzaak tussen de herleidbaarheid van handelingen die min of meer generiek en gemeengoed zijn en daarmee niet of nauwelijks onderscheidend zijn (zoals het doen van belastingaangifte) en de herleidbaarheid van het feit dat bij een specifieke en gespecialiseerde zorgverlener is ingelogd (de logging kan dan als voorspeller raken aan een bijzonder persoonsgegeven). Voor de maatregelen die dat vergt wat betreft beveiliging – zoals versleuteling - kan dat verschil maken.

Hoewel het betrouwbaarheidsniveau (substantieel of hoog) dat is vereist in veel gevallen zal samenhangen met de noodzaak om de herleidbaarheid van de logging verder te voorkomen, is dat niet noodzakelijkerwijs gekoppeld. Zo is het denkbaar dat voor een generiek proces een hoge mate van zekerheid gewenst wordt voor het achterliggende proces.

Doorwerking voor eID

Dit betekent dat bij de vormgeving van het eID stelsel aandacht moet zijn voor het voorkomen van herleidbaarheid van persoonsgegevens. Daarbij kan gedacht worden aan dataminimalisatie en rollenscheiding – elke partij verwerkt slechts die data die nodig zijn voor diens rol/taken en het vermijden van gegevensconcentraties – het ontwerp wordt zodanig ingericht dat het niet nodig is om potentieel identificeren en vertrouwelijke informatie bij één rol neer te leggen; Waar mogelijk moet het gebruik van privacybeschermende technieken, zoals versleuteling waardoor herleidbaarheid wordt teruggedrongen worden overwogen. In zijn algemeenheid heeft het de voorkeur om de bescherming van persoonsgegevens technisch af te dwingen boven procedurele afspraken.

Binnen het stelsel is het van belang dat privacy op een gelijk niveau (dus integraal) wordt beschermd. Het is daarom van belang dat partijen binnen het stelsel, hun privacybeschermende maatregelen afstemmen op de eisen die voortvloeien, bijvoorbeeld uit de PIA op het eID stelsel. Eventueel individueel nog op te stellen door deze partijen PIA's zullen op deze PIA moeten aansluiten.

5. Juridisch inregelen privacybescherming: grondslagen en kadering in Wet DO

Het wettelijk privacykader zoals dat is besproken, vereist dat voor het verwerken van persoonsgegevens grondslagen aanwezig zijn. Zoals eerder al ter sprake gekomen bij de bespreking van de regelgeving ten aanzien van het burgerservicenummer, worden persoonsgegevens binnen het eID stelsel verwerkt in het kader van wettelijke taken van overheidsorganisaties en andere betrokken – private – partijen.

5.1. Wet Digitale Overheid

Het wetsvoorstel Digitale overheid dient de grondslagen voor de verwerkingen van persoonsgegevens te bevatten die voor een goede werking van het eID-stelsel noodzakelijk zijn. De Wet Digitale overheid bevat daartoe op dit punt bepalingen die een aanvulling zijn op de waarborgen van de AVG.

Deze regels, waartoe de AVG ruimte biedt, zijn noodzakelijk om een goede uitvoering van de AVG te bewerkstelligen. Er worden regels gesteld inzake grondslagen, doelen, waarborgen en beveiliging alsmede worden taken, verantwoordelijkheden en bevoegdheden voor de betrokken ministers vastgelegd. Ook bevat het verplichtingen voor bestuursorganen en aangewezen organisaties en voor private partijen. De grondslag om persoonsgegevens te verwerken vloeit voort uit deze bepalingen, in samenhang met artikel 6, eerste lid, onder e, van de AVG. In het wetsvoorstel zijn grondslagen neergelegd voor de verwerking van persoonsgegevens door partijen die een rol hebben in het eID stelsel, voor zover dat noodzakelijk is voor de uitvoering en het verlenen van veilige toegang tot elektronische dienstverlening. Krachtens het wetsvoorstel zullen nadere regels worden gesteld, waaronder over de verstrekking van persoonsgegevens en de bewaartermijnen die in acht moeten worden genomen.

In het wetsvoorstel is – gelet op de geldende BSN-wet- en regelgeving - opgenomen dat het BSN door de genoemde betrokken partijen mag worden verwerkt voor zover dat, in het kader van veilige toegang en het voorkomen van misbruik, noodzakelijk is voor de goede uitvoering van hun taken en verplichtingen ingevolge deze wet (artikel 16 lid 1; ministers), voor een goede elektronische dienstverlening (artikel 16 lid 1; dienstverleners), voor de goede uitvoering van de wet (artikel 16 lid 2; private partijen) en voor de goede werking van het bedrijfs- en organisatiemiddel en goede toegang met dat middel tot elektronische dienstverlening (artikel 16 lid 3; private partijen).

5.1.1. Besluit Digitale Overheid

In dit verband met de regeling van het bieden van verwerkingsgrondslagen en het inkaderen van de verwerkingen van persoonsgegevens zal het Besluit verwerking persoonsgegevens GDI worden uitgebreid en gewijzigd, en zal het worden ongedoopt tot het Besluit digitale overheid. De Wet regelt de verwerkingsgronden in meer algemene zin. In het besluit digitale overheid wordt dit meer in detail uitgewerkt. Reden voor het regelen van de verwerking van persoonsgegevens bij algemene maatregel van bestuur is het feit, dat het wetsvoorstel het karakter heeft van een kaderwet waarin hoofdzaken zijn geregeld en het om redenen van flexibiliteit opportuun is gedetailleerde (technische) uitwerking in de uitvoering vorm te geven.

In het Besluit digitale overheid zal tevens worden aangesloten bij hetgeen reeds is neergelegd in bestaande regelgeving op het gebied van de verwerking van persoonsgegevens ter zake van GDI-voorzieningen. Bij de nadere uitwerking zullen onder meer de beginselen van proportionaliteit en subsidiariteit leidend zijn. Het wetsvoorstel en de daarop gebaseerde

algemene maatregel van bestuur werken, waar mogelijk, nodig en passend, de normen van de AVG uit.

Deze nationale normen met betrekking tot grondslagen, doelen, waarborgen en beveiliging zijn noodzakelijk om een goede uitvoering van de AVG te bewerkstelligen.[12] 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, gelden de bepalingen van de AVG. Binnen de kaders van de wettelijke grondslagen die worden geboden in de Wet digitale overheid en de nadere uitwerking met kaders voor de verwerkingen moet privacybescherming daarom conform de AVG worden ingeregeld.

5.1.2. Regeling Betrouwbaarheidsniveaus

Zoals aangegeven is het eID-stelsel op zichzelf een privacy maatregel, omdat het bijdraagt aan de betere bescherming van (persoons)gegevens die worden gebruikt bij overheidsdienstverlening in breder verband. In aanvulling op de eigenstandige verantwoordelijkheid die overheidsorganisaties al hebben, zorgen authenticatiemiddelen op de hogere betrouwbaarheidsniveaus ervoor dat identiteitsvaststelling, een fundamentele beveiligingsmaatregel, wordt verbeterd.

Om te zorgen dat overheidsorganisaties werken met de inzet van deze hogere betrouwbaarheidsniveaus, wordt in de Wet digitale overheid een verplichting opgenomen om deze te gebruiken voor dienstverlening die digitaal wordt aangeboden en waarvoor identiteitsvaststelling benodigd is[13]. Vanuit de Tweede Kamer is eerder aangedrongen op verplichtstelling van ten minste 2-factor authenticatie en ook de Autoriteit Persoonsgegevens heeft hier meermaals op aangedrongen.

Voor dienstverlening waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is, wordt bepaald dat gebruik gemaakt dient te worden van middelen die ten minste het voor de betreffende dienstverlening vereiste betrouwbaarheidsniveau hebben: «wie het meerdere mag, mag het mindere». Een gebruiker kan derhalve voor alle diensten met een middel op betrouwbaarheidsniveau hoog terecht, ook als het bestuursorgaan of de aangewezen organisatie voor de desbetreffende dienst slechts een middel met een lager betrouwbaarheidsniveau vereist en een publiek middel op niveau laag wordt geaccepteerd door het bestuursorgaan of de aangewezen organisatie. Middelen op een lager betrouwbaarheidsniveau dan substantieel of hoog, zullen niet worden toegelaten en op termijn worden uitgefaseerd.

Een bestuursorgaan of aangewezen organisatie bepaalt in beginsel zelf welk betrouwbaarheids-niveau hij passend acht voor welke soort dienstverlening. Bij het bepalen van het betrouwbaarheidsniveau moeten

[12] Bij algemene maatregel van bestuur wordt bijvoorbeeld geconcretiseerd welke bewaartermijnen gelden, omdat de AVG hieromtrent geen concrete eisen stelt. Het uitgangspunt van de AVG is dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk voor het doel van uw verwerking. Hoe lang gegevens mogen worden bewaard, vergt telkens een afweging en verschilt dus per geval waardoor uitwerking in nationale regels geboden is.

[13] Dit wordt voorzien in artikel 6 van het wetsvoorstel digitale overheid

dienstverleners zich evenwel houden aan de bij ministeriële regeling te stellen criteria inzake betrouw-baarheidsniveaus voor authenticatie bij elektronische diensten; er zullen regels worden gesteld op basis waarvan een bestuursorgaan of aangewezen organisatie kan vaststellen voor welke elektronische dienst tenminste het betrouwbaarheidsniveau substantieel of hoog geldt. Doel van deze regeling, die in lijn zal zijn met de eIDAS-verordening en de in de praktijk reeds gehanteerde Handreiking betrouwbaarheidsniveaus[14], is dienstverleners te helpen een eenduidige, efficiënte en bewuste keuze te maken in de betrouwbaarheidsniveaus van hun digitale diensten. In de regeling zullen criteria worden opgenomen («classificatiemodel») die relevant zijn voor het door de dienstverlener (kunnen) inschalen van het benodigde betrouwbaarheidsniveau zoals aard en rechtsgevolg van de desbetreffende dienst.

Om organisaties ruimte te bieden is in het wetsvoorstel een gefaseerde invoering voorzien, waarbij redelijke overgangstermijnen zullen worden gehanteerd.

5.2. Kadering op basis van eIDAS: eisen aan middelen

5.2.1. Controleprocotol (BSN domein) en AMVB (Bedrijvendomein)

Aan de hand van de in de bijlage van de eIDAS-uitvoeringsverordening 1502 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.

Het Controleprotocol eID haakt daarbij (voor het BSN domein) aan. Bij algemene maatregel van bestuur wordt de eIDAS verordening ingevuld voor het bedrijvendomein.

Er wordt invulling gegeven aan de beoogde eIDAS waarborgen voor de betrouwbaarheidsniveaus substantieel en hoog. Het betreft in de eerste plaats de inschrijving van een identificatiemiddel (waaronder de aanvraag, de registratie en het bewijs en verificatie van identiteit). Vervolgens komt het beheer van elektronische identificatiemiddelen aan de orde, waaronder het ontwerp en de lifecycle (uitgifte, beheer, verlenging en beëindiging) van identificatiemiddelen. Hierna volgen de waarborgen voor authenticatie(mechanisme). Voorts komen de elementen die zien op het beheer van organisatie aan bod, waaronder algemene eisen aan organisaties, de informatievoorziening aan gebruikers van identificatiemiddelen, informatiebeveiliging, administratie, faciliteiten en personeel en technische controles.

[14] https://www.forumstandaardisatie.nl/nieuws/nieuwe-versie-handreiking-betrouwbaarheidsniveaus

6. Privacyvisie als ijkpunt voor operationele inrichting van bescherming van persoonsgegevens binnen het stelsel

6.1. Inrichting op basis van juridisch kader, beleid en (rest)risico's

De vormgeving en inrichting van het eID stelsel wordt gestuurd door het in het eerste hoofdstuk besproken juridisch (privacy)kader en de vastgestelde beleidsuitgangspunten ten aanzien van eID. In het vorige hoofdstuk is aan de orde geweest wat daarvoor – aan verwerkingsgrondslagen en kadering in de wet DO en uitvoeringsregelgeving moet worden geregeld.

De operationele inrichting van het eID-stelsel en de daarbij te maken keuzes dienen aan te sluiten op en invulling te geven aan het besproken juridisch kader, de beleidsuitgangspunten en de kadering die in de Wet DO is afgesproken.

Bij de bespreking in de voorgaande hoofdstukken is – waar opportuun – aangegeven hoe besproken punten doorwerken in de operationalisering van het eID stelsel. Daarmee worden handvatten geboden voor toetsing van de inrichting aan deze Privacyvisie eID.