Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport verificatie- en correctieprocedure Aanmeldpunt Binnenlandse afstand en adoptie

Definitief

Colofon

Titel	Onderzoeksrapport verificatie- en correctieprocedure Aanmeldpunt Binnenlandse afstand en adoptie
Uitgebracht aan	DG Straffen en Beschermen
Datum	22 maart 2021
Kenmerk	2021-0000058454

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

1 Inleiding

1.1 Aanleiding onderzoek en opdrachtgever

Op 3 juni 2020 heeft het ministerie van Justitie en Veiligheid (JenV) een datalekmelding bij de Autoriteit Persoonsgegevens (AP) gedaan in verband met de verwerking van persoonsgegevens door het 'Aanmeldpunt Binnenlandse afstand en adoptie' (hierna: aanmeldpunt). Dit aanmeldpunt van JenV betrof een samenwerkingsverband tussen JenV met Fiom en het Verwey-Jonker Instituut (VJI). Hoewel het bij de inrichting van het aanmeldpunt duidelijk was dat het gevoelige persoonsgegevens zou verwerken, is nagelaten om in de benodigde procedurele en organisatorische waarborgen te voorzien. De verwerking van de gegevens van de aanmelders door Fiom, JenV en VJI heeft daarom niet conform AVG plaatsgevonden. Een maatregel om dit te repareren betreft de inrichting van een verificatie- en correctieprocedure voor de persoonsgegevens en aanmeldverslagen van het aanmeldpunt. JenV heeft deze procedure in het najaar 2020 opgesteld en heeft hiervoor (alsnog) een data protection impact assessment (DPIA) uitgevoerd.

Het is voor JenV van belang dat de verificatie- en correctieprocedure ervoor zorgt dat het vertrouwen van aanmelders wordt hersteld door op een goede wijze om te gaan met de ontvangen (gevoelige) gegevens en dat het onderzoek niet wordt gecompromitteerd met gebruik van in het verleden niet geverifieerde verslagen. Om dit te bewerkstelligen is de ADR gevraagd te onderzoeken op welke wijze de verificatie- en correctieprocedure invulling geeft aan een optimale bescherming van de persoonsgegevens van de aanmelders.
De DG Straffen en Beschermen (DG SenB) is opdrachtgever van dit onderzoek. De DG wenst een onderzoeksrapport te ontvangen. Het rapport bevat geen oordeel en/of conclusies, bijvoorbeeld of de verificatie- en correctieprocedure in overeenstemming is met de AVG.

1.2 Doelstelling en onderzoeksvragen

Het doel van het onderzoek is het geven van inzicht in hoe de verificatie- en correctieprocedure van JenV invulling geeft aan een aantal geselecteerde onderwerpen uit de AVG en hoe de sturing vanuit JenV op de naleving van de procedure is ingericht. Met dit inzicht kan de opdrachtgever bepalen of en welke verbetermogelijkheden er zijn ten aanzien van de verificatie- en correctieprocedure en de sturing hierop om de bescherming van de persoonsgegevens te optimaliseren.

De centrale vraag in dit onderzoek luidt:
Op welke wijze is invulling gegeven aan de geselecteerde onderwerpen uit de AVG in de verificatie- en correctieprocedure en de sturing vanuit JenV op de naleving van de procedure?

De geselecteerde onderwerpen zijn verdeeld over vier onderzoeksvragen. Dit zijn:

1. Hoe is het DPIA-proces vormgegeven en hoe zijn de uitkomsten verwerkt in de verificatie- en correctieprocedure? *(H3)*
2. Op welke wijze is in de verificatie- en correctieprocedure invulling gegeven aan de bescherming van persoonsgegevens? *(H5)*
3. Op welke wijze is in de verificatie- en correctieprocedure invulling gegeven aan de (andere) geselecteerde onderwerpen uit de AVG? *(o.a. H4)*
4. Op welke wijze is de sturing vanuit JenV rondom de verificatie- en correctieprocedure ingericht om de naleving ervan te waarborgen? *(H6)*

1.3 Afbakening en definities

Het object van onderzoek is de verificatie- en correctieprocedure. De procedure omvat de verwerkersovereenkomsten tussen JenV en Fiom en VJI en de verwerkersinstructie. Daarnaast vormt de sturing vanuit JenV op de naleving van de procedure object van onderzoek.

Het onderzoek richt zich op de invulling van de onderwerpen uit de AVG in de verificatie- en correctieprocedure die in overleg met de opdrachtgever zijn geselecteerd. Het onderzoek heeft betrekking op de opzet van procedure, niet op het bestaan en de toekomstige uitvoering ervan. Ook onderzoeken we niet de kwaliteit van de procedure zelf, zoals de uitvoerbaarheid, en de interne instructies van verwerkers als vertaling van de procedure (zie ook hoofdstuk 7).

In het onderzoek hanteren we de term verificatie- en correctieprocedure. Daar waar het specifiek de verwerkersovereenkomst of verwerkersinstructie betreft, is hiernaar verwezen. Ditzelfde geldt voor de opdrachtnemers Fiom en VJI, die in lijn met de AVG zijn aangeduid als verwerkers. Daarnaast gebruiken we de term betrokkene als degene van wie een organisatie persoonsgegevens verwerkt. De betrokkenen in het kader van binnenlandse adoptie en afstand betreffen o.a. afstandsouders, geadopteerden / gewezen afstandskinderen en adoptieouders.

1.4 Leeswijzer

Hoofdstuk 2 betreft de managementsamenvatting. In hoofdstuk 3 gaan we in op de uitgevoerde DPIA (onderzoeksvraag 1). In hoofdstuk 4 behandelen we onder meer de rechtsgronden en doelbinding (onderdeel onderzoeksvraag 3) en in hoofdstuk 5 de bescherming van persoonsgegevens (onderzoeksvraag 2). Hoofdstuk 6 gaat over de sturing vanuit JenV op de naleving van de procedure (onderzoeksvraag 4). In de introductie van elk hoofdstuk staat beschreven welke geselecteerde onderwerpen uit de AVG aan bod komen. Tot slot is in hoofdstuk 7 de verantwoording van het onderzoek opgenomen. In bijlage 1 staat de managementreactie.

2 Managementsamenvatting

JenV heeft vanwege eerdere onvolkomenheden bij de verwerking van persoonsgegevens en aanmeldverslagen door het Aanmeldpunt Binnenlandse adoptie en afstand een verificatie- en correctieprocedure opgesteld. Dit onderzoek heeft als doel inzicht te geven in hoe de verificatie- en correctieprocedure van JenV invulling geeft aan een aantal geselecteerde onderwerpen uit de AVG en hoe de sturing vanuit JenV op de naleving van de procedure is ingericht. Met dit inzicht kan de opdrachtgever bepalen of en welke verbetermogelijkheden er zijn ten aanzien van de verificatie- en correctieprocedure en de sturing hierop om de bescherming van de persoonsgegevens te optimaliseren.

Bevindingen

Uit het onderzoek blijkt dat JenV veel stappen heeft gezet en in de procedure maatregelen heeft opgenomen gericht op het herstellen van de eerdere onvolkomenheden. In de verificatie- en correctieprocedure zijn de geselecteerde onderwerpen uit de AVG meegenomen. De procedure beschrijft onder meer de verantwoordelijkheden van de verwerkersverantwoordelijke (JenV) en verwerkers (Fiom en VJI), het proces rond de uitvoering van de rechten van betrokkenen en instructies gericht op de bescherming en de juistheid van persoonsgegevens.

Uit het onderzoek blijkt tevens een aantal bevindingen omtrent de door de ADR onderzochte onderwerpen en de sturing vanuit JenV op de naleving van de procedure. Deze richten zich met name op de technische beveiligingsmaatregelen voor de bescherming van persoonsgegevens en de sturing op de naleving van de maatregelen in de procedure. Deze bevindingen zijn mede een gevolg van de wijze waarop de DPIA is uitgevoerd, welke bepalend is voor de besluitvorming over de te treffen maatregelen. De belangrijkste bevindingen lichten we hieronder toe.

1. In de reikwijdte van de DPIA zitten beperkingen
Bij de uitvoering van de DPIA is de keuze gemaakt om het proces gericht op het bewaren van de aanmeldverslagen voor het nageslacht niet te beschrijven en slechts deels mee te nemen. Dit schept verwarring rondom het verwerkingsdoel, de bewaartermijn van de persoonsgegevens en vormt een risico voor de transparantie richting de betrokkenen over de verlening van toestemming. Verder is in de DPIA en procedure weinig aandacht voor de risico's die JenV zelf loopt bij de verwerking zoals het bewaren en vernietigen van gegevens. Het is daardoor niet onderbouwd en bekend of de in de procedure vermelde maatregelen hiervoor toereikend zijn.

2. De risico's en maatregelen in DPIA zijn algemeen en beperkt beschreven, waarbij vooral technische beveiligingsmaatregelen nog aandacht vragen
De privacy risico's in de DPIA zijn vrij algemeen, op een hoog abstractieniveau, beschreven en zijn niet toegespitst op de voorgenomen verwerkingen of fases in het verificatie- en correctieproces. Hierdoor is het niet volledig duidelijk wanneer welke risico's zich bij de uitvoering van de verwerkingen in het proces kunnen voordoen bij zowel JenV als de verwerkers.

Dit heeft mede als gevolg dat de relatie tussen de algemeen geformuleerde risico's en maatregelen niet helder is, oftewel: welke maatregelen de risico's bij de daadwerkelijke verwerking van persoonsgegevens wegnemen en of dit (voor JenV) afdoende is. Volgens ons vormt dit met name een risico ten aanzien van de technische beveiligingsmaatregelen voor de bescherming van persoonsgegevens. De aandacht voor de technische maatregelen gericht op vertrouwelijkheid (encryptie), integriteit (logging) en beschikbaarheid van gegevens (back-up) van de gebruikte

informatiesystemen is nog beperkt. Hierdoor bestaat de kans dat persoonsgegevens niet goed beschermd worden en/of juist zijn.

3. De sturing vanuit JenV op naleving procedure is beperkt door o.a. onduidelijkheid over eisen aan beveiliging bij de verwerkers en implementatie van maatregelen
In de verificatie- en correctieprocedure zijn diverse maatregelen beschreven inzake de sturing vanuit JenV op de naleving van de procedure door de verwerkers. Een belangrijk instrument daarbij is het driehoeksoverleg dat periodiek plaatsvindt tussen JenV en de verwerkers, waarin onder meer de rapportage van de verwerkers over de voortgang en issues bij de uitvoering van de procedure wordt besproken. Daarnaast vormen de nakoming van de afspraken in de procedure en behandeling van inkomende verzoeken onderwerp van gesprek.
Op het gebied van sturing zijn echter ook aandachtspunten:

- De eisen die JenV stelt aan de beveiliging bij de verwerkers zijn niet helder vastgesteld en vastgelegd in de verwerkersovereenkomst.
- Bij JenV ontbreekt vooralsnog een volledig inzicht in de daadwerkelijke aanwezigheid van de vanuit de DPIA voorgenomen maatregelen bij de verwerkers.
- Aangegeven is dat JenV voor de start van de procedure wel een checklist gebruikt om de protocollen met maatregelen van de verwerkers te toetsen aan de procedure en DPIA, maar dit biedt naar ons idee geen garantie dat alle maatregelen daadwerkelijk en juist geïmplementeerd zijn.
- Het is niet duidelijk op welke wijze JenV betrouwbare informatie ontvangt over de daadwerkelijke naleving van (beveiligings)maatregelen tijdens de uitvoering van de procedure om te kunnen bijsturen.

Aanbevelingen

Op basis van onze bevindingen komen we tot een aantal aanbevelingen welke in het rapport nader zijn toegelicht. De belangrijkste aanbevelingen aangaande bovenstaande bevindingen geven wij hieronder weer.

- Breng het gehele verwerkingsproces van persoonsgegevens in kaart. Dat wil zeggen vanaf de opgeslagen persoonsgegevens bij de verwerkers en JenV (uitgangspositie) tot en met het bewaren voor het nageslacht en vernietiging van gegevens bij JenV. Bepaal vervolgens de reikwijdte van de verificatie- en correctieprocedure in dit kader. Zorg dat over het bewaren van de aanmeldverslagen voor het nageslacht zo spoedig mogelijk duidelijkheid komt. We bevelen aan om dit op te nemen in de huidige verificatie- en correctieprocedure zodat er één procedure is voor zowel het verifiëren en corrigeren als de vervolgstappen in het proces. Daarbij is het van belang dat de wijze van bewaren van persoonsgegevens voor het nageslacht transparant naar de betrokkenen wordt gecommuniceerd zodat zij exact weten waarvoor ze toestemming kunnen geven.
- Voer de DPIA uit over het gehele proces om de (resterende) risico’s bij de verwerking van persoonsgegevens door de verwerkers en JenV in beeld te hebben. Leg daarbij de focus op de risico’s ten aanzien van de technische beveiliging om de vertrouwelijkheid, integriteit en beschikbaarheid van de persoonsgegevens te waarborgen. Raadpleeg het beleid en de richtlijnen op het gebied van privacy en informatiebeveiliging en betrek zo nodig interne adviseurs op het juiste niveau in de organisatie.
- Stel op basis van de uitgevoerde DPIA vast welke (beveiligings)maatregelen nog niet (voldoende) aanwezig zijn bij de verwerkers en JenV. Stel in een plan op om deze maatregelen te implementeren en leg deze vast in een overeenkomst.
- Zorg voorafgaand aan en tijdens de procedure voor betrouwbare informatie over de daadwerkelijke aanwezigheid en naleving van de afgesproken (beveiligings)maatregelen door deze bijvoorbeeld (extern) te laten toetsen. Daarbij kunnen de verwerkers en JenV mogelijk steunen op rapportages die reeds aanwezig zijn.

3 Risico’s en maatregelen in de DPIA zijn op hoofdlijnen beschreven

In dit hoofdstuk beschrijven we de wijze waarop invulling is gegeven aan de DPIA (onderzoeksvraag 1). Door middel van een DPIA wordt inzicht verkregen in de verwerking, welke risico’s daarbij spelen en met welke maatregelen deze risico’s beheerst moeten worden. De DPIA vormt daarmee de basis van de invulling van de andere onderwerpen van de AVG die in dit onderzoek aan bod komen.
De bevindingen in dit hoofdstuk hebben betrekking op de invulling van het DPIA-proces en wijze waarop de risico’s en maatregelen daarbij zijn opgesteld. In de volgende hoofdstukken gaan we nader in op hoe de uitkomsten van de DPIA t.a.v. de specifieke AVG onderwerpen verwerkt zijn de verificatie- en correctieprocedure.

3.1 DPIA is met name gericht op verificatie en correctie, niet op gehele verwerkingsproces en de verwerking binnen JenV

Voor de eerdere verwerking van persoonsgegevens door het aanmeldpunt, met als doel om deel te nemen aan het onderzoek van VJI/WODC, is door JenV geen DPIA uitgevoerd. De uitgevoerde DPIA 'Verifiëren en corrigeren verwerkingen Aanmeldpunt van september 2019 tot en met juli 2020' heeft als doel om eerdere onvolkomenheden van de verwerkingen van persoonsgegevens die bij de aanmelding zijn verkregen te corrigeren. Het verwerkingsdoel het bewaren van de aanmeldverslagen voor het nageslacht is later toegevoegd, maar beschouwt JenV als aparte verwerking waarvoor het naderhand een nieuwe DPIA opstelt. Het vragen van toestemming hiervoor maakt echter wel onderdeel uit van de verificatie- en correctieprocedure, omdat de afwezigheid van (schriftelijke) toestemming een onvolkomenheid uit de eerdere verwerking betreft.

In het verifiëren en corrigeren van gegevens voor deelname aan het onderzoek en het bewaren van aanmeldverslagen voor het nageslacht is een scheiding aangebracht, omdat JenV nog niet inzichtelijk heeft hoe en bij welke organisatie die gegevens bewaard zullen worden. Dit heeft als gevolg dat de betrokkenen voorlopig toestemming geven voor iets waarover onduidelijkheid bestaat. Dit lijkt niet in overeenstemming te zijn met de doelstelling van de AVG om transparant te zijn. Dit kan tot onduidelijk en onrust leiden bij betrokkenen. Ook kan de invulling rond het bewaren voor het nageslacht van invloed zijn op de keuzes die gemaakt moeten worden bij de huidige verwerking, zoals het wel of niet pseudonimiseren van de aanmeldverslagen (zie par. 5.3). De onduidelijkheid rond de invulling van het tijdelijk bewaren van de aanmeldverslagen kan ertoe leiden dat deze langer bewaard worden dan is toegestaan volgens de AVG en maatregelen in de huidige procedure niet passend en afdoende zijn.

Daarnaast zijn de DPIA en verificatie- en correctieprocedure voornamelijk gericht op verwerking door de verwerkers en niet zozeer op gegevensverwerking door JenV, zoals het uitwisselen, opslaan en vernietigen van gegevens. De vernietiging van persoonsgegevens in de vorm van kopieën van aanmeldverslagen bij JenV maakt volgens de DPIA wel onderdeel uit van de verwerking. Dit komt verder niet terug in de DPIA bij onder meer de risico’s en maatregelen en het is niet nader beschreven wanneer deze vernietiging moet plaatsvinden. In afwachting van de vernietiging zijn de gegevens bij JenV opgeslagen, maar het is dus nog niet bepaald of en hoe lang gegevens na de procedure bij JenV opgeslagen blijven. JenV heeft gekozen om te focussen om de onvolkomenheden bij de verwerkers te herstellen en minder op de eigen verwerking. JenV loopt daarmee het risico dat de bescherming van de gegevens niet toereikend is en de privacy van betrokkenen niet geheel geborgd is.

3.2 De risico's in DPIA zijn vrij algemeen en beperkt beschreven en beoordeeld

Een onderdeel van de DPIA betreft de inventarisatie en beoordeling van de risico's voor de betrokkenen. De DPIA bevat een aantal risico's bij de verwerking. Een risico is het in onbevoegde handen komen van persoonsgegevens, dat gelet op de ingrijpende persoonlijke verhalen (zeer) schadelijk kan zijn voor de direct betrokkene, de doelgroep van belanghebbenden en derden. Vervolgens zijn drie groepen van oorzaken van dit risico genoemd: onnauwkeurige overdracht, datalekken en herleidbaarheid tot specifieke personen. Een tweede risico betreft 'tijd', waarmee JenV bedoelt dat de verzoeken die tussen het sluiten van het aanmeldpunt en de start van de verificatie- en correctieprocedure binnenkomen niet binnen de termijn conform AVG worden behandeld. Per oorzaak is kort beschreven wat de aard, kans en impact is.

De beschrijving van de risico's en oorzaken is vrij algemeen en beperkt. De risico's zijn niet toegespitst op de voorgenomen verwerkingen, namelijk de diverse uitvoeringsfases in het verificatie- en correctieproces. Dit maakt dat het per verwerking of fase niet (direct) helder is welke risico's zich specifiek voordoen. Daarnaast is het verschil tussen risico en oorzaak en de relatie tussen beide niet altijd helder. Zo vormt herleidbaarheid van gegevens niet direct een oorzaak van het in onbevoegden handen komen van persoonsgegevens. De beoordeling van de risico's (kans maal impact) is vervolgens wat beperkt en niet altijd juist uitgevoerd. Zo is de kans dat een situatie zich voordoet in een enkel geval beoordeeld op basis van de reeds opgestelde procedure als zijnde maatregel, wat niet gewenst is, en komen restrisico's beperkt naar voren. Ook geeft de veel genoemde impact 'is merkbaar voor betrokkene' weinig inzicht in het specifieke risico dat wordt gelopen.

De algemene en beperkte beschrijving en beoordeling van de risico's kent meerdere oorzaken. Allereerst is de DPIA pas uitgevoerd nadat JenV het eerste concept van de verificatie- en correctieprocedure (met maatregelen) heeft opgesteld. Dit heeft als reden dat het projectteam na de datalekmelding eerst inzicht wilde in de stand van zaken en gevolgde procedure rondom de verwerkte persoonsgegevens bij de verwerkers. Het projectteam heeft geen expliciete nulmeting gemaakt van de reeds getroffen maatregelen. Voorafgaand en gaandeweg het opstellen van de procedure zijn de risico's geïnventariseerd en maatregelen bepaald en opgenomen. Het projectteam heeft daarom gekozen om de DPIA algemener te houden en een aantal keer te verwijzen naar de procedure. Daarnaast speelt het gebrek aan ervaring van het projectteam met het opstellen van een DPIA een rol, in combinatie met de onbekendheid met de noodzaak tot het opstellen van een DPIA. Tot slot zijn sommige genoemde aandachtspunten en adviezen van interne adviseurs niet of beperkt meegenomen in de DPIA of missen de punten scherpte, blijkt mede uit onze analyse.

3.3 De risico's en voorgenomen maatregelen zijn niet allemaal direct gekoppeld

De DPIA bevat een aantal voorgenomen maatregelen om de geïnventariseerde risico's te verminderen. Het is onduidelijk of elk risico met een maatregel wordt afgedekt of dat het risico in een bepaalde mate geaccepteerd is. Dit is onder andere het geval bij de risico's op 'het hacken van de inloggegevens' en 'cyberaanval en geautomatiseerde scripts' en 'tijd'. Bij het risico op onnauwkeurige overdracht, dat bij meerdere verwerkingen of uitvoeringsfases aan de orde is, is om die reden alleen verwezen naar de verificatie- en correctieprocedure waarin maatregelen staan.

Door risico's vrij algemeen te benoemen en te beoordelen, deze niet allen direct te koppelen aan maatregelen en adviezen en beleidsstukken beperkt te gebruiken, bestaat de kans dat JenV risico's bij de verwerkingen niet (voldoende) in beeld heeft en de maatregelen hiervoor mogelijk niet tijdig, juist en/of volledig heeft opgesteld en getroffen.

3.4 Betrokkenheid van functionarissen is niet optimaal

Bij het opstellen van de DPIA zijn intern en extern diverse functionarissen en partijen betrokken. De privacy officers en verwerkers zijn in het najaar 2020 door het opgerichte projectteam betrokken bij de inventarisatie van de problematiek, stand van zaken en de opstelling van de procedure. Een eerste versie van de DPIA, opgesteld door het projectteam, is aan de privacy officer (DG SenB) voorgelegd. Volgens het projectteam is deze daarna bij de verwerkers teruggelegd. Een nieuwe versie van de DPIA is vervolgens ter advisering voorgelegd aan de Functionaris Gegevensbescherming (FG) en tot slot bij de adviseur informatiebeveiliging namens Chief Information Security Officer (CISO). Betrokkenen zijn niet apart geraadpleegd bij de DPIA. Hun perspectief, dus welke risico's zij lopen op het gebied van de privacy, zien we wel terug in de DPIA.

De reacties per mail, telefonisch of middels het driehoeksoverleg (verwerkers) zijn door het projectteam verwerkt, maar de mate waarin is niet helemaal duidelijk. Dit komt doordat de reacties en de daadwerkelijke verwerking ervan niet op een gestructureerde wijze gedocumenteerd en dus helemaal herleidbaar zijn. De privacy officers en adviseur informatiebeveiliging hebben beperkt feedback ontvangen wat uiteindelijk met hun reactie is gedaan. Tot slot hebben de betrokken FG, CISO en gemandateerd verwerkingsverantwoordelijke de DPIA (nog) niet ondertekend, waardoor het niet bekend is of zij allen de laatste versie van de DPIA hebben gezien en akkoord bevonden. Daardoor is het mogelijk dat hun perspectieven niet goed geïnterpreteerd en/of onvoldoende meegenomen zijn en risico's blijven bestaan.

Aanbeveling
Het is aan te bevelen om het gehele verwerkingsproces in kaart te brengen. Het proces start bij de reeds verwerkte en opgeslagen persoonsgegevens bij de verwerkers en JenV (uitgangspositie) tot en met het bewaren van het nageslacht bij een organisatie en vernietiging van de gegevens bij JenV. Dit zijn dus verwerkingen vooraf, tijdens en na de huidige procedure. Het is daarbij van belang dat over de wijze van het bewaren voor het nageslacht zo snel mogelijk duidelijkheid komt en dit transparant naar de betrokkenen wordt gecommuniceerd. Ook kan het einde van de verificatie- en correctieprocedure nog scherper worden neergezet (zie par. 5.4).

Vervolgens is het goed om als projectteam met relevante interne en externe functionarissen, zoals de verwerkers en interne adviseurs op het gebied van privacy en informatiebeveiliging, (nogmaals) het bovengenoemde proces door te nemen om te bepalen of de risico's voldoende in beeld zijn. Het kan dan bepaald worden hoe hiermee om te gaan (risicoresponse), of de voorgenomen en getroffen maatregelen passend en afdoende zijn en opwegen tegen de kosten. Vooral de risico's omtrent de bescherming van persoonsgegevens en bijbehorende technische beveiligingsmaatregelen verdienen meer aandacht (zie hoofdstuk 5). JenV kan in overleg met de verwerkers een plan opstellen om aanvullende maatregelen te implementeren.

Wanneer de risicoanalyse tot nieuwe inzichten en maatregelen heeft geleid en/of helderheid is over het bewaren van gegevens voor het nageslacht dienen deze vastgelegd te worden in de procedure. Het is wenselijk om één procedure en DPIA op te stellen voor zowel het verifiëren en corrigeren als de vervolgstappen door JenV. Het is daarbij van belang dat de DPIA het advies van de FG bevat, deze ondertekend wordt en bij voorkeur in een register wordt opgenomen.

4 Vastlegging rechtmatigheid van gegevensverwerking kan accurater

In dit hoofdstuk gaan we in op de rechtmatigheid van de verwerking (onderdeel onderzoeksvraag 3). Dit betreffen de AVG-onderwerpen doelbinding en rechtmatige grondslag, rechten van betrokkene(n), maar ook kwaliteitsmanagement.

4.1 Rechtsgrond is helder, verwerkingsdoel en doelbinding kunnen scherper

De verificatie- en correctieprocedure heeft als doel om de onvolkomenheden van de verwerkingen van persoonsgegevens die bij de aanmelding zijn verkregen te corrigeren. Het verwerkingsdoel is in de DPIA kortweg omschreven als 'voldoen aan de wettelijke verplichting'. Bij de beoordeling van de rechtmatigheid in de DPIA wordt echter verwezen naar de oorspronkelijke doel waarvoor de gegevens zijn verzameld, namelijk deelname aan het onderzoek van VJI/WODC en het bewaren van de gegevens voor het nageslacht. Deze verwerking vindt plaats op grond van schriftelijke toestemming van de betrokkene. Ook bij de beoordeling van de doelbinding lopen het doel van de oorspronkelijke verwerking en huidige verwerking door elkaar. De onduidelijkheid rond de doelen wordt versterkt doordat deze in de DPIA en de verwerkersinstructie soms verschillend geformuleerd zijn. Zo wordt onder meer verwezen naar 'deelname aan onderzoek' en 'selectie van respondenten door de onderzoeker' en wordt bij het bewaren voor het nageslacht niet altijd de tijdelijkheid benoemd.

Het is van belang voor JenV, de verwerkers en bovenal de betrokkenen dat de doelen bekend, eenduidig en welbepaald zijn. In de verwerkersinstructie is weliswaar beschreven dat betrokkenen naast de doelstelling van de verificatie- en correctieprocedure betrokkenen geïnformeerd worden over 'de doelstelling van de beoogde Verwerkingen van Persoonsgegevens'. Als deze doelen niet welbepaald en nadrukkelijk omschreven zijn, voldoet JenV niet aan haar informatieplicht en is de gegeven toestemming ook onrechtmatig.

Aanbeveling
Het is aan te bevelen om het verwerkingsdoel (en de relatie met de oorspronkelijke doel) nauwkeurig, in duidelijke en eenvoudige taal en consequent op te nemen in de verificatie- en correctieprocedure en communicatie richting de betrokkene, zodanig dat het precies duidelijk is waarvoor betrokkene toestemming geeft.

4.2 Toestemming opgenomen in de procedure, gebruik bijzondere persoonsgegevens en wijze van toestemming vragen nog aandacht

In de verwerkersinstructie komt de vraag voor toestemming voor de verwerking voor de doeleinden op meerdere plaatsen aan de orde. Bij het op orde brengen van de persoonsgegevens dienen de verwerkers te controleren of reeds schriftelijk toestemming is gegeven voor het gebruik van de persoonsgegevens voor de selectieprocedure van en de contactgegevens bij deelname aan het onderzoek. Via het informatieve bericht bij aanvang van de procedure informeert JenV de betrokkenen over o.a. de inhoud en het verdere verloop van het verificatie- en correctieprocedure en vraagt, mits dit nog niet is gebeurd, schriftelijke toestemming voor beide doelen. De betrokkenen ontvangen in dit bericht tevens informatie over hun rechten in deze procedure, waaronder het recht om de toestemming in te trekken.

In de verwerkersinstructie is niet genoemd dat betrokkenen in de berichtgeving worden gewezen op de verwerking van bijzondere persoonsgegevens. De betrokkenen moeten echter op de hoogte zijn dat en welke bijzondere persoonsgegevens (mogelijk) zijn of worden verwerkt om hier toestemming voor te kunnen geven. Het projectteam geeft aan bezig te zijn met het opstellen van dit bericht over toestemming. Het team is voornemens om daarin een toelichting op te nemen wat bijzondere persoonsgegevens zijn en het verwerken van bijzondere persoonsgegevens expliciet te benoemen bij het vragen van toestemming.
De wijze waarop betrokkenen hun toestemming kunnen aangeven is nog niet beschreven. Dit zal volgens het projectteam middels het beantwoorden van de informatiemail of schriftelijk door middel van een ondertekende brief zijn. In de verwerkersinstructie zijn wel eisen aan de toestemming vermeld, zoals ondubbelzinnigheid en gebruik van eenvoudige taal. Het informatiebericht waarin om toestemming wordt gevraagd is nog in opzet en hebben we daarom niet bekeken. De toestemming voor het gebruik van bijzondere persoonsgegevens en de wijze waarop dit gegeven kan worden verdienen nog aandacht in de procedure.

4.3 Processen voor de rechten van betrokkenen bevatten nog enkele onduidelijkheden

Betrokkenen kunnen de rechten die zij hebben op basis van de AVG doen gelden. Het interne proces hiervoor is in de verificatie- en correctieprocedure opgenomen. Betrokkenen zijn op de hoogte van hun rechten door de privacyverklaring die JenV als verwerkingsverantwoordelijke op de openbare website heeft geplaatst. Het projectteam geeft aan tevens een privacyverklaring voor de verificatie- en correctieprocedure op te stellen voor het project, welke ook op de websites van de verwerkers komt te staan.

De betrokkenen kunnen bij zowel JenV als de verwerker die de aanmelding heeft verzorgd verzoeken indienen. Het is niet heel duidelijk beschreven wie welke ingediende verzoeken moet beantwoorden of afhandelen. In de DPIA staat dat JenV alle verzoeken afhandelt, maar het projectteam geeft aan dit alleen voor verzoeken te doen die JenV of Fiom ontvangen. In het protocol inzake inzageverzoeken in de verwerkersovereenkomst is daarentegen opgenomen het uitgangspunt is dat JenV de beantwoording doet, daar waar in de verwerkersinstructie staat dat verwerkers de verzoeken inwilligen, wat enigszins verwarrend is. Verder schrijft het protocol voor dat JenV als verwerkingsverantwoordelijke de betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek het resultaat verstrekt of aangeeft waarom hier geen gevolg aan is gegeven. Deze eis inclusief termijn is niet terug te vinden in de verwerkersinstructie en/of bij het proces voor de andere rechten van betrokkenen. Hieruit is op te maken dat de beschrijving van de behandeling van alle verzoeken in de procedure niet geheel eenduidig is.

Het projectteam geeft aan de behandeling van verzoeken bij de verwerkers tot aan de start van de verificatie- en correctieprocedure conform protocol zijn verlopen. Het houdt hiervan een (anoniem) register bij. Doordat betrokkenen hun verzoeken bij meerdere organisaties kunnen indienen, kan het voor hen onduidelijk zijn bij welke organisatie zij terecht kunnen voor de uitoefening van hun rechten. Ook kan het zorgen dat het overzicht bij JenV van verzoeken en de status ervan niet volledig is, waardoor de kans bestaat dat een verzoek niet of niet juist is/wordt opgepakt. De afspraak dat binnenkomende verzoeken met alle betrokken organisaties worden besproken in het driehoeksoverleg en o.a. het (in opzet zijnde) informatiebericht naar betrokkenen hierover ondervangen dit grotendeels.

Aanbeveling
We raden aan om in de verificatie- en correctieprocedure en specifiek de verwerkersinstructie nader te specificeren bij welke organisatie betrokkenen hun verzoeken inzake álle rechten kunnen indienen en hoe JenV en de verwerkers hiermee dienen om te gaan. Het is wenselijk om de beantwoording van de verzoeken bij de verwerkingsverantwoordelijke te beleggen, zodat diegene het

overzicht kan bijhouden en de volledigheid kan bewaken tijdens en na de procedure. Daarnaast is het goed om intern na te gaan of de (voorgestelde) communicatie hierover naar betrokkenen helder en eenduidig is.

4.4 Maatregelen voor de verificatie en correctie van persoonsgegevens zijn gedetailleerd beschreven

Het is van belang dat de gegevensverwerking correct en in overeenstemming met de wens van betrokkenen is. De verificatie- en correctieprocedure heeft mede als doel om de juistheid en volledigheid van de reeds verzamelde persoonsgegevens te bepalen dan wel te herstellen. Dit is mede nodig om te zorgen dat de selectie van betrokkenen gebaseerd is op de juiste persoonsgegevens en aanmeldverslagen. Diverse maatregelen zijn opgesteld om opzettelijk en met name onzorgvuldig menselijk handelen te voorkomen. De verwerkersinstructie bevat vooral organisatorische maatregelen zoals gedetailleerde instructies om de juistheid te waarborgen. Zo geeft de verwerkersinstructie invulling aan de behandeling van verzoeken rond de correctie en vernietiging van gegevens. Dit geldt ook voor (het kenbaar maken van) de gewenste wijze van correspondentie door betrokkenen.

Een organisatorische maatregel betreft de vastlegging van de medewerkers die bevoegd zijn om de persoonsgegevens te kunnen inzien, wijzigen en vernietigen. De verwerkers beschikken over diverse (documenten met) persoonsgegevens zoals de contactgegevens, aanmeldverslagen, eventueel aangeleverde stukken, intakeformulieren, e-mails en journaals. De opslag van contactgegevens en eventueel aangeleverde stukken geschiedt vanwege het pseudonimiseren in een andere map dan de aanmeldverslagen. Slechts enkele medewerkers hebben (in opzet) toegang tot deze mappen. Het is uit de documentatie echter niet op te maken welke informatie exact in welke map staat, wat wel helder dient te zijn. Ook zijn beperkte technische maatregelen vastgelegd om onjuist gebruik van gegevens door medewerkers en de gevolgen daarvan te herkennen, zoals logging. Ook andere technische (beveiligings)maatregelen de juistheid of integriteit van de gegevens te waarborgen behoeven nog extra aandacht (zie par. 5.2).

Een ander aandachtspunt betreft de vaststelling van de identiteit van betrokkenen. Identificatie vindt plaats aan de hand van de NAW-gegevens bij het laatste contact. De verwerkers controleren middels diverse bronnen of deze gegevens juist zijn. Daarnaast sturen ze als extra verificatie een informatiebericht waarop betrokkenen moeten reageren, alvorens ze het aanmeldverslag versturen. De wijze van identificatie bij een verzoek is verder niet beschreven. De kans blijft echter bestaan dat degene die een verzoek indient of reageert op correspondentie niet de betreffende betrokkene is, waardoor het aanmeldverslag met bijzondere gegevens uiteindelijk mogelijk naar de verkeerde persoon wordt verstuurd. De verwerkers zullen overigens later in de procedure bij de communicatie gebruik maken van encryptie, waardoor e-mailberichten met bijvoorbeeld aanmeldverslagen niet te openen zijn zonder aanvullende mail of sms-code.

Aanbeveling
Het is aan te bevelen om nader te bepalen in hoeverre JenV een risico loopt omtrent de identificatie van betrokkenen en in hoeverre het gewenst is om hiervoor extra maatregelen in de eerste fase van de procedure in te regelen. Daarnaast kan meer aandacht gegeven worden aan de technische beveiligingsmaatregelen om onjuistheid van gegevens tegen te gaan (zie hoofdstuk 5).

5 (Beveiligings)maatregelen voor bescherming van persoonsgegevens vragen meer aandacht

In dit hoofdstuk bespreken we de wijze waarop in de procedure invulling is gegeven aan de bescherming van persoonsgegevens (onderzoeksvraag 2). Hierbij komen tevens andere onderwerpen terug, zoals bewaartermijnen, verwerkers en doorgifte.

5.1 Inzicht in verwerkingssystemen en mate van beveiliging is gering

De verwerkers hebben de persoonsgegevens opgeslagen in Microsoft SharePoint en gebruiken dit systeem en/of Zivver voor mailverkeer met betrokkenen en om onderling persoonsgegevens inclusief verslagen uit te wisselen. Het is onduidelijk of de basisbeveiliging van beide applicaties en systemen op orde is. In de DPIA is aangegeven dat Microsoft SharePoint AVG-proof is, maar de onderbouwing daarvan ontbreekt. Het is ook niet helder in hoeverre dit voor Zivver geldt, waarover is gesteld dat dit 'een beveiligde omgeving is'. Tijdens dit onderzoek is vanwege diverse nadelen besloten niet (langer) gebruik te maken van Microsoft SharePoint en is het onduidelijk in welke systemen Fiom en VJI hun gegevens (gaan) opslaan. Bij JenV bevinden de kopieën van de aanmeldverslagen van Fiom en overzicht van meldingen zich op een L-schijf. Het is onbekend in hoeverre de omgeving bij JenV passend beveiligd is en hier ook de verslagen na de procedure worden opgeslagen.

5.2 Technische beveiligingsmaatregelen zijn beperkt vastgesteld en vastgelegd

In de verificatie- en correctieprocedure zijn diverse maatregelen opgenomen om de persoonsgegevens te beschermen. De verwerkersinstructie bevat gedetailleerde organisatorische maatregelen bij de verschillende uitvoeringsfases richting de verwerkers om de vertrouwelijkheid en integriteit van de gegevens te borgen. Zo is in de verwerkersinstructie opgenomen dat verwerkers zorg dienen te dragen dat betrokken medewerkers correct geautoriseerd zijn en in het bezit zijn van een verklaring omtrent gedrag (VOG) en getekende geheimhoudingsverklaring. Ook zijn instructies opgenomen voor de vernietiging en wijziging van gegevens (zie ook par. 4.4) en informatie-uitwisseling tussen betrokken partijen en betrokkenen.

In de verwerkersovereenkomst tussen JenV en Fiom zijn in de bijlage aanvullende organisatorische en technische maatregelen beschreven. Genoemde maatregelen zijn onder meer dat gegevens per mail via end-to-end encryptie met sms-code verstuurd worden, toegangscontrole op het systeem zit en waar mogelijk een wachtwoord op documentatie komt. Deze bijlage met maatregelen ontbreekt vooralsnog in de verwerkersovereenkomst met VJI. Daarbij zijn deze maatregelen niet in de DPIA genoemd en lijken mede daardoor na aanlevering door Fiom door JenV overgenomen te zijn, zonder expliciete afweging of deze maatregelen noodzakelijk zijn gezien de risico's. In de DPIA is wel vermeld dat JenV en Fiom zich bij de gegevensverwerkingen zullen houden aan de Baseline Informatiebeveiliging Overheid (BIO 2020). In de verificatie- en correctieprocedure wordt niet verwezen naar deze richtlijn waardoor het niet direct blijkt hoe hier concreet invulling aan is gegeven.

Doordat de risico's en bijbehorende (beveiligings)maatregelen in de DPIA algemeen en beperkt zijn beschreven (zie hoofdstuk 3), is het mogelijk dat JenV en de verwerkers onvoldoende maatregelen hebben vastgesteld en getroffen die een passend beveiligingsniveau waarborgen. We constateren dat het niet volledig inzichtelijk in welke mate de beveiligingsmaatregelen bij de verwerkers en JenV een permanente basis de vertrouwelijkheid, integriteit en beschikbaarheid van de

verwerkingssystemen garanderen. Zo zijn in de DPIA en in de procedure geen maatregelen opgenomen om de beschikbaarheid van persoonsgegevens te borgen, zoals de aanwezigheid van een back-up. Meer technische maatregelen ten behoeve van de integriteit van de persoonsgegevens, zoals het gebruik van logging om gebruikersactiviteiten te achterhalen en toegangscontrole mogelijk te maken, zijn ook niet beschreven. Deze punten zijn mede aangegeven door de adviseur informatiebeveiliging, maar beperkt verwerkt en vragen dus meer aandacht.

Aanbeveling
In lijn met eerdere aanbevelingen raden we aan om het gehele verwerkingsproces in kaart te brengen om met functionarissen, zoals de verwerkers en adviseurs op het gebied van privacy en informatiebeveiliging, de technische risico's ten aanzien van de beveiliging en bescherming van persoonsgegevens te kunnen inventariseren. Daarbij is inzicht in de gebruikte verwerkingssystemen bij de verwerkers en JenV nodig. Het is vervolgens goed om met dit volledige inzicht als JenV te bepalen welke aanvullende maatregelen genomen moeten worden. Daarbij kan gebruik worden gemaakt van richtlijnen zoals de BIO[1].

Het is belangrijk dat JenV de aanvullende voorwaarden of eisen aan de beveiliging (beheersingscriteria) voor de verwerkers opstelt. Deze dienen helder in de verwerkersovereenkomst en eventueel in de verwerkersinstructie vastgelegd te worden. Dit geldt uiteraard ook voor de reeds vastgestelde eisen en maatregelen.

5.3 Pseudonimisering dient meerdere en tegenstrijdige doelen

Een maatregel die JenV treft is de pseudonimisering van gegevens van de betrokkenen in de aanmeldverslagen. Daarvoor moeten de verwerkers de contactgegevens en de aanmeldverslagen in aparte mappen opslaan. Beide bestanden zijn voorzien van een code om de verslagen bij eventuele selectie voor het onderzoek van VJI/WODC te kunnen herleiden naar de betrokkenen en hun contactgegevens. In de verwerkersinstructie is opgenomen dat informatie die direct herleidbaar is tot de betrokkene en gegevens die direct of indirect herleidbaar zijn tot derden in de verslagen moeten worden verwijderd.

De DPIA impliceert dat met het pseudonimiseren de kans op herleidbaarheid en daarmee in het onbevoegden handen komen van persoonsgegevens wordt beperkt. Het projectteam geeft echter aan dat het pseudonimiseren niet zozeer een beveiligingsmaatregel is, maar voornamelijk als doel heeft om als onderzoeker een objectieve selectie te kunnen maken op basis van een gepseudonimiseerd verslag. Bij het bewaren voor het nageslacht zou dit wel een beveiligingsmaatregel zijn. Binnen JenV speelt echter ook de (terechte) vraag of het pseudonimiseren van de verslagen wenselijk is indien deze bewaard worden voor het nageslacht, om de kennis over afstand en adoptie voor een breed publiek beschikbaar en levend te houden. Betrokkenen willen mogelijk hun verhaal juist niet anoniem doen.

Dit is enigszins tegenstrijdig en kan leiden tot onduidelijkheid in de verificatie- en correctieprocedure. JenV wil dit oplossen door ruimte te bieden om betrokkenen hun verslagen niet gepseudonimiseerd te gebruiken. Dit is momenteel nog niet in de verwerkersinstructie opgenomen, maar JenV is voornemens hiervoor een aparte procedure op te stellen voor een eenduidige verwerking. Hierbij dient rekening te worden gehouden met het feit dat oorspronkelijke verslagen worden gewist. Indien andere gegevens van de betrokkene naast direct herleidbare contactgegevens zoals een naam zijn verwijderd uit het verslag, kunnen deze niet meer achterhaald worden indien de betrokkene dit later wenst. Bovendien moet het helder zijn welke persoonsgegevens als direct en indirect herleidbaar beschouwd moeten worden.

[1] De NEN-ISO 27001/27002 en daaraan gerelateerde overheidsnormen - zoals de Baseline Informatieveiligheid Overheid (BIO) - zijn de standaard baselines om te komen tot een 'adequate' beveiliging.

Aanbeveling
Het is aan te bevelen om aan betrokkenen helder te maken waarom hun verslag gepseudonimiseerd is of wordt (voor zover dit niet de planning is). Daarnaast kan een beschrijving van de wijze van pseudonimiseren en anonimiseren voor de verwerkers voor meer eenduidigheid zorgen. Het moet helder zijn welke soort persoonsgegevens van de betrokkene in het oorspronkelijke verslag de verwerkers moeten verwijderen (anonimiseren) of versleutelen (pseudonimiseren) en hoe zicht dit verhoudt tot de eventuele wens van de betrokkene om hun verhaal niet anoniem te doen.

5.4 Het bewaren en vernietigen van gegevens is nog niet welbepaald

Zoals eerder aangegeven zijn de bewaartermijnen voor het tijdelijk opslaan van persoonsgegevens inclusief aanmeldverslagen ten behoeve van het (tijdelijk) bewaren voor het nageslacht zijn nog niet bepaald (zie par. 4.1). De verificatie- en correctieprocedure gaat wel in op het bewaren en vernietigen van gegevens tot aan het VJI/WODC onderzoek. De verwerkersinstructie beschrijft gedetailleerd de verschillende situaties waarbij persoonsgegevens vernietigd worden, bijvoorbeeld wanneer response uitblijft, geen toestemming wordt gegeven of deze wordt ingetrokken. De instructie schrijft ook voor dat verwerkers de persoonsgegevens van betrokkenen die worden gebruikt voor de selectie voor het onderzoek pas verwijderen als het onderzoek van VJI/WODC is afgerond. Dit lijkt niet verenigbaar met het doel, want na de selectie en overdracht van de gegevens van de geselecteerde personen hebben de verwerkers geen doel meer om deze te bewaren. Het is niet helder wat JenV precies onder de afronding van het onderzoek verstaat.

Het bewaren van de journaals, een chronologisch overzicht van uitgevoerde verwerkingen en communicatie per unieke code, bij de verwerkers na de procedure lijkt eveneens geen directe relatie te hebben met het doel van de verwerking. Dit geldt ook voor de kopieën van de aanmeldverslagen die JenV momenteel in opslag heeft, waarvan ook niet duidelijk is of dit verenigbaar is met het doel waarvoor toestemming is of wordt gegeven.

Het is daarnaast op te merken dat in de verificatie- en correctieprocedure weinig aandacht is voor de beveiliging van fysieke opslag en vernietiging van geretourneerde aanmeldverslagen en andere documentatie met persoonsgegevens die per post zijn ontvangen. Dit betreft nog een aandachtspunt in de procedure, net zoals de controle op de vernietiging van fysiek en digitaal opgeslagen gegevens. In de procedure is opgenomen dat de verwerkers binnen een maand na de procedure de gegevens moeten vernietigen en de opdrachtgever op de hoogte moeten stellen van het tijdstip en de wijze van de vernietigingen. De opdrachtnemers hoeven echter niet nader aan te tonen dat gegevens op alle locaties vernietigd zijn en dit wordt verder niet gecontroleerd.

Aanbeveling
We bevelen aan om persoonsgegevens waaronder de journaals en kopieën van verslagen te verwijderen wanneer de opslag niet verenigbaar blijkt te zijn met het doel. Daarnaast is het gewenst dat de verwerker aantoont dat alle gegevens correct (in lijn met voorschriften) zijn vernietigd.

6 Interne organisatie en sturing op naleving procedure kennen nog gebreken

In dit hoofdstuk behandelen we de sturing op de naleving van de verificatie- en correctieprocedure en de inrichting van de interne organisatie (onderzoeksvraag 4). Dit betreft de onderwerpen interne organisatie en toezicht, meldplicht datalekken, verwerkingsregister en privacybeleid.

6.1 Sturing vanuit JenV op naleving procedure is nog beperkt ingeregeld

Door JenV is voorafgaand aan het aanmeldproces niet onderzocht en beoordeeld of de verwerkers voldoende garanties bieden voor de naleving van de AVG. Dit is ook niet expliciet gedaan bij de verificatie- en correctieprocedure. JenV heeft ervoor gekozen de verwerkers ook het verificatie- en correctieproces uit te laten voeren, omdat zij de tevens persoonsgegevens hebben verzameld en deze dus al in bezit hebben. Overhandiging van gegevens aan een derde partij zonder toestemming is bovendien niet wenselijk.

In de verwerkersinstructie is opgenomen dat de verwerkers in de voorbereidingsfase onder meer vastleggen op welke wijze zij maatregelen die voortkomen uit DPIA en zijn opgenomen in de procedure hebben doorgevoerd in hun protocol. JenV toetst de protocollen bij de start van de procedure middels een checklist, welke is gebaseerd op de (beperkt uitgevoerde) DPIA en procedure. Het is daarmee echter niet helder of de genoemde maatregelen voorafgaand aan de procedure geïmplementeerd zijn, zoals het inregelen van autorisaties. Met andere woorden, het biedt geen garantie dat alle maatregelen daadwerkelijk geïmplementeerd zijn en naar behoren werken.

De rapportage- en verantwoordingslijnen tijdens de uitvoering van de verificatie- en correctieprocedure richting de verwerkingsverantwoordelijke zijn helder. Beide verwerkers stellen periodiek een rapportage op waaruit de voortgang blijkt. Zo rapporteren ze over de verrichte werkzaamheden, knelpunten en de beschikbare capaciteit in relatie tot de voortgang. In de procedure is tevens opgenomen dat JenV en de verwerkers periodiek een driehoeksoverleg hebben om de rapportage te bespreken. Ook de naleving van de instructie, de voortgang en genomen maatregelen naar aanleiding van inbreuken in verband met persoonsgegevens, de status van bezwaren, klachten en verzoeken van betrokkenen en de reacties op communicatieactiviteiten komen aan de orde. Dit driehoeksoverleg vindt ook al voorafgaand aan de procedure plaats. Binnen JenV wordt aangesloten bij de formele rapportage- en verantwoordingslijnen, te weten projectteam, afdelingshoofd, DG.

Door het gebruik van een rapportage en bespreking daarvan in het driehoeksoverleg kan JenV sturing geven op de naleving van de procedure tijdens de uitvoering. De (periodieke) controle op de naleving van de afgesproken (beveiligings)maatregelen is hiermee echter niet volledig ingeregeld. Een procedure of plan voor het evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking bij de verwerkers is niet aangetroffen, evenmin als bij JenV. De verantwoording door de verwerker op de organisatorische en technische maatregelen is daarmee nog beperkt.

Aanbeveling
Zoals eerder aangegeven raden we aan om eisen op te stellen voor de beveiliging van persoonsgegevens aan de hand van richtlijnen zoals de BIO en uiteraard het beleid omtrent privacy en informatiebeveiliging van JenV. Het is noodzakelijk bij de start van de procedure betrouwbare informatie is over de daadwerkelijke

aanwezigheid van afgesproken (beveiligings)maatregelen bij de verwerkers. Het is aan te bevelen om dit door een externe partij te laten toetsen (zoals een IT-auditor) op basis van bijvoorbeeld de BIO (ISO27001 of ISO27001, aangevuld met ISO27018 en ISO27017). Daarbij kunnen de verwerkers en JenV mogelijk steunen op rapportages die reeds aanwezig zijn. Dit geldt ook in zekere mate voor JenV.

6.2 Verantwoordelijkheden bij de procedure zijn over het algemeen belegd en gedocumenteerd

De verantwoordelijkheden bij de verificatie- en correctieprocedure zijn op meerdere plekken beschreven in de verwerkersovereenkomsten en –instructie. De minister van Rechtsbescherming is verwerkingsverantwoordelijke, al is het niet concreet benoemd aan wie (op welk niveau) deze rol gemandateerd is en of dit conform het privacybeleid is. De taken, verantwoordelijkheden en bevoegdheden zijn over het algemeen duidelijk beschreven in de procedure waarbij ook de onderlinge relaties tussen de verantwoordelijke(n) en verwerkers inzichtelijk zijn gemaakt. Wat betreft de vastlegging van verantwoordelijkheden bij de uitvoering van rechten van betrokkenen is nog verbetering mogelijk (zie par. 4.3).
Verder is in dit kader op te merken dat de verwerkersovereenkomsten tussen JenV en de verwerkers de minimale wettelijke eisen bevatten, met de opmerking dat de vastlegging van de eisen rond de technische en organisatorische maatregelen beter kan (zie o.a. par 6.2). Daarnaast is een gedocumenteerde procedure aanwezig voor de melding van inbreuken op persoonsgegevens (datalekken) bij JenV en de verwerkers, welke in de verwerkersovereenkomst is opgenomen.

6.3 Raadpleging privacy- en beveiligingsbeleid en opname verwerkingsregister zijn aandachtspunten

Het projectteam heeft bij de opstelling van de verificatie- en correctieprocedure geen gebruik gemaakt van het privacybeleid van JenV en bepaald of de procedure hiermee in overeenstemming is. Het team was wel bekend met (het bestaan van) het beleid, maar wist niet dat en hoe hieraan invulling gegeven moest worden bij het project. Het informatiebeveiligingsbeleid van JenV is ook niet geraadpleegd bij het opstellen van de procedure. Kennis van privacy- en informatiebeveiligingsbeleid had ontstane knelpunten mogelijk deels kunnen voorkomen. De DPIA en verificatie- en correctieprocedure zijn overigens wel voorgelegd aan privacy officers van DG SenB, adviseur informatiebeveiliging en de FG, waarvan aangenomen kan worden dat zij het beleid kennen en dit hebben meegenomen in hun adviezen.

Daarnaast is de verwerking in het kader van de verificatie- en correctieprocedure niet opgenomen in het verwerkingsregister van JenV. Dit gebeurt volgens JenV pas wanneer de uitkomsten van dit onderzoek en dat van de Commissie zijn verwerkt in de procedure. Het is nog niet helemaal helder welke verwerking exact wordt opgenomen. Volgens het projectteam is dit de verificatie- en correctieprocedure en het (tijdelijk) bewaren voor het nageslacht, terwijl dit laatste in feite een andere verwerking is waarvoor apart een DPIA wordt opgesteld. Hoe zich dit verhoudt tot het oorspronkelijke en huidige verwerkingsdoel dient helder te worden.

Aanbeveling
We raden aan om bij de verificatie- en correctieprocedure en eventuele nieuwe risicoanalyse na te gaan of deze in overeenkomst is met het privacy- en informatiebeleid, al dan niet met behulp van interne functionarissen zoals de privacy officers en adviseur informatiebeveiliging / CISO. Daarbij zouden JenV en specifiek DG SenB meer kunnen doen om de basiskennis van privacy en informatiebeveiliging bij medewerkers te vergroten. Tot slot is het van belang dat de reikwijdte en doelen van de verwerking helder zijn (zie hoofdstuk 3) en de juiste verwerking zo spoedig mogelijk opgenomen wordt in het verwerkingsregister van JenV.

7 Verantwoording onderzoek

7.1 Onderzoeksvragen en referentiekader

Ten behoeve van het onderzoeksdoel is de volgende centrale vraag opgesteld:
Op welke wijze is invulling gegeven aan de geselecteerde onderwerpen uit de AVG in de verificatie- en correctieprocedure en de sturing vanuit JenV op de naleving van de procedure?

Om tot de beantwoording van deze centrale vraag te komen, zijn de volgende vier onderzoeksvragen geformuleerd:

1. Hoe is het DPIA-proces vormgegeven en hoe zijn de uitkomsten verwerkt in de verificatie- en correctieprocedure? *(H3)*
2. Op welke wijze is in de verificatie- en correctieprocedure invulling gegeven aan de bescherming van persoonsgegevens? *(H5)*
3. Op welke wijze is in de verificatie- en correctieprocedure invulling gegeven aan de (andere) geselecteerde onderwerpen uit de AVG? *(o.a. H4)*
4. Op welke wijze is de sturing vanuit JenV rondom de verificatie- en correctieprocedure ingericht om de naleving ervan te waarborgen? *(H6)*

In overleg met de opdrachtgever zijn een aantal AVG-onderwerpen geselecteerd die relevant zijn voor het vraagstuk. De ADR heeft onderzocht hoe in de verificatie- en correctieprocedure invulling is gegeven aan de volgende geselecteerde onderwerpen:

- Beoordelen privacy risico's en uitvoeren DPIA
- Privacybeleid
- Verwerkingsregister
- Doelbinding en rechtmatige grondslag
- Kwaliteitsmanagement
- Rechten van betrokkene(n)
- Bewaartermijnen persoonsgegevens
- Meldplicht datalekken
- Verwerkers
- Doorgifte van persoonsgegevens
- Bescherming van persoonsgegevens
- Interne organisatie / toezicht

Deze onderwerpen zijn toebedeeld aan de bovenstaande onderzoeksvragen. Sommige onderwerpen komen bij meerdere onderzoeksvragen aan bod. In de inleiding van elk hoofdstuk is daarom aangegeven op welke onderwerpen de bevindingen betrekking hebben.

De geselecteerde AVG onderwerpen zijn weergegeven in het referentiekader. Het referentiekader betreft (een selectie van) het ADR Privacy Framework. Het uitgangspunt van dit kader is de AVG en de UAVG. Daarnaast is er rekening gehouden met de adviezen die de Autoriteit Persoonsgegevens (AP) en de European Data Protection Board (EDPB) hebben uitgebracht. Verder zijn inzichten meegenomen uit het Privacy Control Framework van NOREA, de Privacy Baseline van CIP-Overheid en de handreiking AVG die interdepartementaal is opgesteld. Voor dit onderzoek zijn daarnaast een aantal aanvullende, relevante onderwerpen uit de Privacy Baseline van CIP-overheid toegevoegd.

7.2 Werkzaamheden en afbakening

Om de onderzoeksvragen te beantwoorden hebben we ons referentiekader met de geselecteerde AVG-onderwerpen naast de verificatie- en correctieprocedure en aanvullende documentatie gelegd. De uitkomsten van deze documentenstudie vormen input voor de interviews die we met intern betrokkenen bij het opstellen van de procedure hebben gevoerd. Dit betreffen het projectteam JenV, de privacy officers en adviseur informatiebeveiliging. De uitvoering is daarmee conform de overeengekomen werkzaamheden in de opdrachtbevestiging.

Het object van onderzoek is de verificatie- en correctieprocedure. Voor de eenduidigheid wordt deze term in dit onderzoek gehanteerd, maar de procedure omvat de volgende documenten:

- De "Verwerkingsovereenkomsten verificatie en correctie" van het ministerie van Justitie en Veiligheid met Fiom en het VJI (versies 15-12-2020);
- De "Verwerkingsinstructie verificatie en correctie" als bedoeld in art. 4.1. in de verwerkingsovereenkomsten met Fiom en VJI (versie 15-12-2020);

Daarnaast vormt de sturing vanuit JenV op de naleving van de verificatie- en correctieprocedure object van onderzoek. Dit betreft de wijze waarop JenV intern en extern stuurt op de naleving van de procedure en hierop toezicht houdt.

De ADR onderzoekt hoe in (de verschillende fasen van) de verificatie- en correctieprocedure invulling is gegeven aan de geselecteerde AVG-onderwerpen. Het onderzoek richt zich op de opzet van de verificatie- en correctieprocedure, niet op de uitvoering of het daadwerkelijke bestaan van de maatregelen in de procedure. De ADR onderzoekt daarnaast niet specifiek naar kwaliteitsaspecten van de procedure, zoals de efficiëntie, uitvoerbaarheid of belasting voor betrokkenen.

Interne instructies of procedures van de verwerkers, als vertaling van de verificatie- en correctieprocedure van JenV, maken geen onderdeel uit van het onderzoek. De ADR bekijkt ook niet op welke manier de verwerkers hun informatiebeveiliging zelf hebben vormgegeven, maar alleen hoe de sturing, beheersing en toezicht is ingericht vanuit JenV om de persoonsgegevens te beschermen. Mede daarom zijn de verwerkers niet betrokken bij het onderzoek.

7.3 Gehanteerde standaard en kwaliteitsborging

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zouden we wellicht andere zaken hebben geconstateerd en gerapporteerd.

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

7.4 Verspreiding rapport

De opdrachtgever, mr. W.F. Saris MPA, is eigenaar van dit rapport. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Hoewel het rapport de context van het onderzoek zo goed mogelijk probeert te beschrijven, is het mogelijk dat iemand die de context niet (volledig) kent de uitkomsten anders interpreteert dan bedoeld.

In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de Auditdienst Rijk (ADR) een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt.

De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van rapporten die de ADR heeft uitgebracht en plaatst dit overzicht op www.rijksoverheid.nl.

8 Ondertekening

Den Haag, 22 maart 2021

w/g

mw. N.J.C. Klijn MSc

Projectleider

Auditdienst Rijk

Bijlage 1 Managementreactie

Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Auditdienst Rijk
per e-mail

Directoraat-Generaal
Straffen en Beschermen
Directie Sanctietoepassing en Jeugd

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv
Contactpersoon
M 06 539 387 23
l.r.l.poffe@minvenj.nl

Projectnaam
project Binnenlandse afstand en adoptie

Ons kenmerk
3253184

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 18 maart 2021
Onderwerp Beleidsreactie onderzoeksrapport verificatie- en correctieprocedure Binnenlandse afstand en adoptie

Bijgevoegd treft u de beleidsreactie aan op het onderzoeksrapport verificatie- en correctieprocedure Binnenlandse afstand en adoptie.

Met vriendelijke groet,

W. F. Saris
De Directeur-generaal Straffen en Beschermen

De beleidsreactie op het onderzoeksrapport verificatie- en correctieprocedure Binnenlandse afstand en adoptie.

Directoraat-Generaal Straffen en Beschermen
Directie Sanctietoepassing en Jeugd

Datum
18 maart 2021

Ons kenmerk
3253184

In het kader van de toegezegde zorgvuldigheid voor het herstellen van fouten met betrekking tot het Aanmeldpunt binnenlandse afstand en adoptie door middel van de verificatie- en correctieprocedure is, zoals gemeld in de brief van de Minister voor Rechtsbescherming van 15 oktober aan de Tweede Kamer (TK 2020 -2021, 31 265, nr. 74), de Auditdienst Rijk (ADR) gevraagd om onderzoek naar deze procedure te doen. Daarnaast heeft de Commissie van onafhankelijke deskundigen inzake afstand en adoptie onder andere de taak gekregen aanbevelingen te doen die betrekking hebben op de inrichting en uitvoering van deze verificatie- en correctieprocedure.

Met dit rapport heeft de ADR invulling gegeven aan haar opdracht om inzicht te geven in de vraag hoe de verificatie- en correctieprocedure van het ministerie van Justitie en Veiligheid invulling geeft aan een aantal geselecteerde onderwerpen uit de AVG en hoe de sturing vanuit het ministerie van Justitie en Veiligheid op de naleving van de procedure is ingericht. Gelet op dit onderzoek door de ADR is ervoor gekozen om de DPIA eerst af te stemmen met de deskundigen binnen het ministerie van Justitie en Veiligheid en met Fiom en het Verwey-Jonker Instituut (VJI) en daarna formeel vast te stellen.

De ADR schrijft in haar onderzoeksrapport verificatie- en correctieprocedure Aanmeldpunt Binnenlandse afstand en adoptie dat uit zijn onderzoek blijkt "dat JenV veel stappen heeft gezet en in de procedure maatregelen heeft opgenomen gericht op het herstellen van eerdere onvolkomenheden. In de verificatie- en correctieprocedure zijn de geselecteerde onderwerpen uit de AVG meegenomen." Daarnaast constateert de ADR dat op een aantal punten verdere verfijning en borging is aan te brengen. Deels is deze verfijning en borging reeds tijdens het onderzoek door de ADR door het ministerie van Justitie en Veiligheid uitgevoerd. Aan de hand van de vier belangrijkste aanbevelingen van de ADR wordt hieronder beschreven met welke acties deze opgevolgd worden.

Breng het gehele proces vanaf de ontvangen aanmeldingen tot en met het bewaren voor het nageslacht en vernietiging gegevens bij JenV in kaart. Bepaal vervolgens de reikwijdte van de verificatie- en correctieprocedure in dit kader. We bevelen aan om [duidelijkheid over het bewaren van de aanmeldverslagen voor het nageslacht] op te nemen in de huidige verificatie- en correctieprocedure zodat er één procedure is voor zowel het verifiëren en corrigeren als de vervolgstappen in het proces. Draag daarbij zorg dat het bewaren voor het nageslacht transparant naar de betrokkenen wordt gecommuniceerd zodat zij exact weten waarvoor ze toestemming kunnen geven.

Wij begrijpen deze aanbeveling, zo dat de ADR ook het proces voorafgaande aan de verificatie- en correctieprocedure, dat wil zeggen vanaf de inrichting van het

Directoraat-Generaal Straffen en Beschermen
Directie Sanctietoepassing en Jeugd

Datum
18 maart 2021

Ons kenmerk
3253184

Aanmeldpunt, evenals het proces na afronding van de verificatie- en correctieprocedure in kaart gebracht wil zien. De stappen voorafgaande en ten vervolge op de verificatie- en correctieprocedure zullen in de eerste plaats onderdeel uitmaken van de overwegingen in de verwerkersovereenkomst en de toelichtende paragrafen van de verwerkingsinstructie. In de tweede plaats voorzien de procedure en de berichten aan de aanmelders in een uitgebreide en heldere uitleg over de aanleiding, de stappen in de procedure, hun rechten in de procedure, de wijze waarop in de procedure wordt omgegaan met de persoonsgegevens en met welk doel hun persoonsgegevens worden verwerkt. Expliciet wordt daarbij benoemd dat de aanmelder te allen tijde over het gebruik van haar/zijn gegevens gaat en - indien dit gebruik van de persoonsgegevens wijzigt - aan haar/hem opnieuw een verzoek om toestemming wordt voorgelegd.

Met de ADR deel ik de noodzaak om helderheid te geven aan de betrokkenen omtrent het bewaren voor het nageslacht voor de langere termijn voor zover dat nu mogelijk is. In het verzoek om toestemming voor verwerking van de persoonsgegevens staat concreet en helder omschreven aan wie, waarvoor, voor hoe lang en voor welke verwerkingen toestemming voor het gebruik van welke persoonsgegevens wordt gevraagd. Ten aanzien van het tijdelijk bewaren van gespreksverslagen door het ministerie van Justitie en Veiligheid voor het nageslacht, betekent dit dat aan aanmelders zal worden uitgelegd waarom het bewaren 'tijdelijk' is, wat we nu kunnen vertellen over het einddoel en dat hen opnieuw om toestemming zal worden gevraagd als dit definitief vorm heeft gekregen. De aanmelder heeft een vrije keuze deze toestemming(en) te verlenen en wordt gewezen op het recht om een eerder gegeven toestemming weer in te trekken.

Voer de risicoanalyse/DPIA uit over het gehele proces om de (resterende) risico's bij de verwerking van persoonsgegevens door de verwerkers en JenV in beeld te hebben.

Wij begrijpen de aanbeveling zo dat de DPIA mede betrekking moet hebben zowel op de risico's verbonden aan de gevolgen van het Aanmeldpunt (inclusief de verwerkingen die plaatsvinden bij het ministerie van Justitie en Veiligheid met betrekking tot het bewaren van persoonsgegevens die van Fiom zijn ontvangen en verwerkingen die voorafgaande aan de verificatie- en correctieprocedure worden uitgevoerd op grond van bijvoorbeeld inzageverzoeken), als op de risico's voor de uiteindelijke verwerking ten behoeve van het nageslacht. Hierbij zijn reeds beheersmaatregelen genomen met protocollen voor het behandelen van tussentijdse inzageverzoeken, klachten en verzoeken tot vernietiging van persoonsgegevens. Deze protocollen vinden inmiddels, na afstemming met de verwerkers, toepassing.

Daarnaast zijn andere aspecten uit de periode van het Aanmeldpunt wel in ogenschouw genomen maar in de DPIA niet inhoudelijk behandeld omdat ze

Directoraat-Generaal Straffen en Beschermen
Directie Sanctietoepassing en Jeugd

Datum
18 maart 2021

Ons kenmerk
3253184

alleen zien op het ministerie van Justitie en Veiligheid en dus geen betrekking hebben op de verwerkingen door Fiom of VJI. Het gaat hier met name om de persoonsgegevens die het ministerie van Justitie en Veiligheid van Fiom heeft ontvangen. Dat wil niet zeggen dat een DPIA niet beoogd is, alleen dat deze – met het oog op een zo spoedige mogelijke start van de verificatie- en correctieprocedure – geen prioriteit heeft gekregen. Voor deze aspecten wordt nu een afzonderlijke DPIA gemaakt als basis voor een beheerreglement voor de persoonsgegevens die al bij het ministerie van Justitie en Veiligheid voorhanden zijn en voor de persoonsgegevens die aan het einde van de verificatie- en correctieprocedure aan het ministerie van Justitie en Veiligheid zullen worden overgedragen. Voor een toekomstige derde partij die het bewaren voor het nageslacht structureel voor haar rekening neemt, zal het uitvoeren van een DPIA en het nemen van maatregelen op grond hiervan een eis zijn.

Stel op basis van de uitgevoerde risicoanalyse/DPIA vast welke concrete (beveiligings)maatregelen nog niet (voldoende) aanwezig zijn (binnen het eigen departement en de verwerkers) en stel in overleg met de verwerkers een plan op om deze maatregelen te implementeren.

De derde aanbeveling heeft betrekking op het in overleg met de verwerkers zorgdragen dat de (beveiligings)maatregelen op grond van de uitgevoerde risicoanalyse/DPIA goed zijn geïmplementeerd. In de komende periode tot aan de start van de procedure gaat het ministerie van Justitie en Veiligheid de volgende stappen nemen. In de eerste plaats zal in samenwerking met de Functionaris Gegevensbescherming worden nagegaan of (beveiligings)maatregelen uit de risicoanalyse/DPIA zijn ingevoerd en welke nog aandacht behoeven. In de tweede plaats gaat het ministerie van Justitie en Veiligheid na of de medewerkers afdoende zijn geïnstrueerd op gedragsregels voor de gebruiksmiddelen en de beveiligingsmaatregelen. Tenslotte gaan, in de derde plaats, zowel de verwerkers als het ministerie van Justitie en Veiligheid afzonderlijk van elkaar de (beveiligings)maatregelen in de praktijk testen. Daarbij wordt niet alleen gekeken naar de werking van de (beveiligings)maatregelen maar ook naar het gebruiksgemak voor de aanmelders. Mede op basis hiervan schrijven de verwerkers een instructie voor de aanmelders.

Zorg voorafgaand aan de start van de procedure voor betrouwbare informatie over de daadwerkelijke aanwezigheid en werking van afgesproken (beveiligings)maatregelen door deze bijvoorbeeld (extern) te laten toetsen. Daarbij kunnen de verwerkers en JenV mogelijk steunen op rapportages die reeds aanwezig zijn.

De ADR wijst het ministerie van Justitie en Veiligheid in haar laatste aanbeveling op het toetsen en de daadwerkelijke aanwezigheid en werking van de afgesproken (beveiligings)maatregelen. Lopende het onderzoek van de ADR heeft het ministerie van Justitie en Veiligheid de verschillende (beveiligings)maatregelen bij

de verwerkers en haarzelf nagelopen en beoordeeld op de werking en het gebruiksgemak. Het meest kritische proces, namelijk het terugleggen c.q. verzenden van de gespreksverslagen door de verwerkers naar de aanmelders en terug (met de te hanteren termijnen en andere eisen vanuit de AVG) is hierbij leidend geweest. Uit de beoordeling is één optie voldoende betrouwbaar gebleken om een beveiligd mailverkeer naar de aanmelders en terug te garanderen met een volledige grip op het proces voor verwerker én aanmelder. Gelet op de overzichtelijkheid van het aantal aanmelders, de uitgebreide voorbereiding van de procedure met verwerkers en de belangen van aanmelders bij een spoedige start van de procedure heeft het ministerie van Justitie en Veiligheid ervoor gekozen om de verwerkers zelf aanvullend te vragen om inzicht te geven in de aanwezigheid en werking van de genomen (beveiligings)maatregelen. De verwerkers is gevraagd om inzicht te geven in de genomen en de werking van organisatorische, technische, procedurele en beheersmaatregelen. Deze uitvraag is gebaseerd op de Baseline Informatiebeveiliging Overheid 2020. Deze inzichten zullen samen met de DPIA onderdeel uitmaken van de overeenkomst met de verwerkers. Daarnaast beoordeelt JenV voor aanvang van de procedure aan de hand van een checklist de protocollen van de verwerkers.

Directoraat-Generaal Straffen en Beschermen
Directie Sanctietoepassing en Jeugd

Datum
18 maart 2021

Ons kenmerk
3253184

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00