Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport
Rijksbreed AVG onderzoek

Overkoepelende rapportage

Definitief

Colofon

Titel	Rijksbreed AVG onderzoek
Uitgebracht aan	Directeur-generaal Overheidsorganisatie en CIO-Rijk
Datum	13 december 2021
Kenmerk	2021-0000256938

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

1 Aanleiding opdracht

Met de Algemene Verordening Gegevensbescherming (AVG) is het belang van privacybescherming nog beter verankerd in de wet. Uitgangspunt hierbij is dat de fundamentele privacyrechten en vrijheden van de betrokkenen gewaarborgd moeten worden. De betrokkenen hebben hiermee meer rechten gekregen om controle uit te kunnen oefenen over de verwerking van hun persoonsgegevens. De Rijksoverheid verwerkt veel (gevoelige en bijzondere) persoonsgegevens van burgers en zal haar informatiehuishouding conform deze wetgeving op orde moeten brengen, houden en zich hierover moeten kunnen verantwoorden.

Het jaarlijks ADR rijksbreed onderzoek naar het stelsel van maatregelen voor de naleving van de Algemene Verordening Gegevensbescherming (AVG) is dit jaar voor het eerst vraaggestuurd uitgevoerd waarbij DGOO en de CIO-Rijk de rol van coördinerende en faciliterende opdrachtgevers vervuld hebben. De opdracht is besproken en geaccepteerd door het CIO Beraad.

1.1 Scope

Gehoor geven aan de burger die een beroep doet op zijn/haar privacyrechten is een belangrijk onderdeel van een gezond privacybeleid en draagt bij aan het vertrouwen van de burger in de Rijksoverheid. Een verkennend onderzoek naar de wijze waarop departementen en de geselecteerde dienstonderdelen burgers in staat stellen om hun recht op inzage[1] en het recht op rectificatie[2] en aanvulling uit te oefenen is daarom gekozen als invalshoek voor dit onderzoek.

Verder hebben wij dit jaar wederom aandacht geschonken aan de kwaliteit van deze registers. Vorig jaar constateerden we bij ons rijksbreed onderzoek dat de status van de verwerkingen in het register van de verwerkingsactiviteiten nog niet overal voldeed aan de vereisten die de AVG voorschrijft. Interdepartementaal is overeengekomen dat de Rijksoverheid aan haar informatieplicht jegens de burger wil voldoen door de registers van verwerkingsactiviteiten, voor zover dat mogelijk is, openbaar te maken. Daarnaast is het register van verwerkingsactiviteiten een middel om te kunnen voldoen aan de aantoonbare verantwoordingsverplichting die artikel 30 van AVG voorschrijft.

Tevens is een follow-up uitgevoerd naar de verbeteracties die departementen hebben ondernomen om de vorig jaar door de ADR gesignaleerde privacyrisico's te mitigeren.
Voor dit verkennend onderzoek hebben wij bij alle departementen een aantal van hun dienstonderdelen geselecteerd waarbij de maatregelen omtrent de eerdergenoemde aspecten nader geanalyseerd zijn.

1.2 Doelstelling

De doelstelling van dit onderzoek is drieledig, namelijk:

1. Het verkrijgen van inzicht in de maatregelen die departementen en een aantal van haar dienstonderdelen hebben getroffen teneinde het faciliteren van de betrokkenen bij het uitoefenen van hun recht op inzage en het recht op rectificatie en aanvulling te borgen.

[1] De AVG geeft mensen het recht om in te zien welke persoonsgegevens van hen worden verwerkt om mensen meer grip te geven op hun persoonsgegevens.
[2] De AVG geeft mensen het recht om onjuiste persoonsgegevens te laten wijzigen of om hun persoonsgegevens aan te vullen.

2. Het verkrijgen van inzicht in de kwaliteit van de registers van verwerkingsactiviteiten die departementen beheren ten einde aantoonbaar een van de verantwoordingsverplichtingen na te leven.
3. Het verkrijgen van inzicht in de activiteiten die departementen ondernomen hebben naar aanleiding van de resultaten uit het Rijksbreed AVG-onderzoek 2019.

Op basis van dit verkennend onderzoek zijn goede voorbeelden en verbeterpunten geïdentificeerd in de beheersing en inrichting van privacybescherming op departementaal en rijksbreed niveau.

1.3 Onderzoeksvragen

Naar aanleiding van hierboven geformuleerde doelstellingen hebben wij per departement de volgende onderzoeksvragen beantwoord:

1. Welke maatregelen heeft de organisatie in opzet en bestaan getroffen ten einde tijdig, juist en volledig te voldoen aan de AVG met betrekking tot de afhandeling van inzageverzoeken en verzoeken tot rectificatie en/of aanvulling van betrokkenen (art. 15 en art.16 AVG)?
2. Welke maatregelen heeft de organisatie in opzet en bestaan getroffen die borgen dat het register van verwerkingsactiviteiten actueel, juist en volledig is teneinde aantoonbaar te voldoen aan de betreffende verantwoordingsverplichting die de AVG voorschrijft (art 30 AVG.).
3. Welke verbeteracties heeft de organisatie ondernomen om de eerder door de ADR gesignaleerde privacyrisico's te mitigeren.

1.4 Rapportage

Elk departement heeft de resultaten van dit onderzoek in de vorm van een deelrapportage ontvangen. Hierin zijn de onderzoeksvragen beantwoord en de bijbehorende verbeterpunten vermeld.

In dit rapport is voor de Directeur-generaal van DGOO, als voorzitter van het ICBR, een rijksbreed beeld van de overkoepelende, geanonimiseerde bevindingen opgenomen. De inhoud hiervan is in het CIO-Beraad van 17 november jl. besproken en vastgesteld. De basis voor de overkoepelende rapportage zijn de deelrapportages per departement. Tevens hebben wij goede voorbeelden en verbetermogelijkheden beschreven. Deze rijksbrede rapportage heeft een anoniem karakter. Voor wat betreft de goede voorbeelden (best practices) hebben wij wel namen van departementen opgenomen.

1.5 Leeswijzer

De belangrijkste bevindingen resulterende uit de onderzoeksvragen volgt direct na deze leeswijzer. De onderbouwing hiervan komt aan de orde in de hoofdstukken 1 tot en met 3. In hoofdstuk 1 wordt het resultaat uit het onderzoek naar de maatregelen omtrent de rechten van betrokkenen weergegeven, waaronder een analyse van een selectie AVG-verzoeken. De beantwoording van deelvraag 1 komt hierbij aan de orde. Hoofdstuk 2 bevat een analyse van de aangetroffen maatregelen rond de registers van verwerkingsactiviteiten. Hiermee wordt antwoord gegeven op deelvraag 2. De beantwoording van deelvraag 3 is opgenomen in de bevindingen onder hoofdstuk 3.
Tenslotte geeft hoofdstuk 4 inzicht in de wijze waarop dit onderzoek is uitgevoerd.

2 De verdere inbedding van privacymanagement binnen de Rijksoverheid is noodzakelijk.

Hieronder hebben wij de belangrijkste verbeterpunten die geïdentificeerd zijn in de inrichting, beheersing en verantwoording van privacybescherming binnen de elf onderzochte departementen en twintig hieronder ressorterende dienstonderdelen beknopt weergegeven alsook de constateringen op rijksbreed niveau. Voorafgaand aan het lezen van de centrale hoofdboodschap willen wij u er nogmaals op attenderen dat dit een overkoepelende rapportage betreft waarin de geaggregeerde resultaten feitelijk weergeven zijn. Uit dit verkennend onderzoek blijkt dat de departementen zich in verschillende volwassenheidsfasen van het privacymanagement bevinden. Zo blijkt dat ogenschijnlijk minder complexe aspecten van privacymanagement, zoals de rechten van betrokkenen en het register van verwerkingenregister, zeer divers zijn ingericht. Niet alleen departementen hanteren verschillende aanpakken, ook tussen dienstonderdelen binnen een departement wordt niet eenduidig gehandeld. Daarnaast hebben de departementen te maken met uiteenlopende aantallen van AVG-verzoeken, verwerkingen van persoonsgegevens en beschikbare capaciteit. Een één op één vergelijking van de departementen is daardoor niet altijd direct toepasbaar. In deze rapportage zijn onderliggende verschillen gegeneraliseerd.

2.1.1 Procedures omtrent rechten van betrokken veelal aanwezig, echter dragen de ingerichte processen vaak niet bij aan een adequate afhandeling.

De burger wordt door middel van de verschillende privacyverklaringen op de websites geïnformeerd over zijn/haar rechten in het kader van de AVG en de wijze waarop een AVG-verzoek wordt ingediend. Bij enkele dienstonderdelen wordt de burger proactief ondersteund bij het indienen van een verzoek en/of wordt de burger de mogelijkheid geboden zelf regie te voeren over een beperkt deel van de verwerkte persoonsgegevens. Dit is een positieve ontwikkeling die bijdraagt aan het vergroten van de transparantie en daarmee het vertrouwen in de overheid.

De inbedding van de interne procedures is bij meer dan de helft van de departmenten niet toereikend geweest om de door ons geselecteerde AVG-verzoeken binnen de gestelde termijn en conform de vereisten af te handelen. Uit ons onderzoek blijkt dat 57% van deze verzoeken niet tijdig te zijn afgehandeld. Daarnaast hebben wij veelal geen aantoonbare PDCA-cyclus aangetroffen waarbij systematische en periodieke evaluatie plaatsvindt van de procedure en beheersingsmaatregelen die waarborgen dat deze naar behoren werken.

Binnen de Rijksoverheid zijn meerderen departementen en/of onderdelen samen verantwoordelijk voor bepaalde beleidsterreinen en delen zij in verband met deze taakuitvoering vaak en veel persoonsgegevens. We hebben geconstateerd dat de meeste organisaties geen procedures hebben opgesteld en/of ingericht die borgen dat de ontvangers van persoonsgegevens tijdig worden geïnformeerd over eventuele wijzigingen. Wij vinden het zorgelijk dat een aantal onderdelen geen kennis heeft van deze vereisten. Dit is een belangrijk onderdeel van de AVG omdat anders deze ontvangers besluiten zouden kunnen nemen op basis van onjuiste gegevens. Dit kan vergaande negatieve gevolgen hebben voor de betrokkene.

2.1.2 Juistheid en volledigheid van het register van verwerkingsactiviteiten wordt niet geborgd.

Departementen maken veelal gebruik van een centraal AVG-Register van verwerkingsactiviteiten (Centraal AVG-verwerkingsregister) waarvan de inrichting in lijn is met de vereisten van de AVG. Dit verschaft inzicht in en overzicht over de

verwerkingen van persoonsgegevens waar de organisaties passende beschermingsmaatregelen voor dienen te treffen. Een verwerker dient conform de vereisten ook een AVG-verwerkersregister bij te houden van alle categorieën van verwerkingsactiviteiten die ten behoeve van een verwerkingsverantwoordelijke plaatsvinden. De juistheid en volledigheid van deze registers vormt voor de meeste departementen nog een uitdaging. Er is aandacht nodig voor de inhoudelijke kwaliteit van deze registers en de aantoonbare accordering van de juistheid en volledigheid van de vastlegging door de verwerkingsverantwoordelijke.
Een aantoonbare PDCA-cyclus en een procedure die de actualiteit, juistheid en volledigheid van het AVG-verwerkingsregister borgt is slechts bij een paar onderdelen in opzet aanwezig.

2.1.3 *Verbetertrajecten beperkt opgestart, voldoende privacycapaciteit blijft een aandachtspunt, realisatie blijft achter.*

Een deel van de dienstonderdelen heeft activiteiten ondernomen voor (her)inrichting en verdere inbedding van privacymanagement en privacygovernance om de door ons eerder gesignaleerde privacyrisico's te mitigeren. Een beperkt deel van de onderdelen monitort de voortgang van deze acties en rapporteert hierover.
De meeste activiteiten blijken nog in uitvoering te zijn of zijn nog niet opgepakt. Aangegeven is dat de doelstellingen van de verbetertrajecten vanaf medio 2021 aantoonbaar gerealiseerd zullen zijn. Naast herprioritering in verband met de impact van de Corona-maatregelen wordt ook de schaarse privacycapaciteit om de verbeterplannen uit te voeren als reden voor de vertraging aangevoerd. Dat laatste wordt met name veroorzaakt door de groeiende behoefte aan privacydeskundigheid bij de verschillende vraagstukken en werkzaamheden omtrent de bescherming van persoonsgegevens.

2.1.4 *Inrichting privacymanagement en privacygovernance binnen de Rijksoverheid nog in ontwikkeling.*

De onderzochte onderwerpen lenen zich voor een meer uniforme en eenduidige aanpak, dit zou de werkbaarheid ten goede komen. Duidelijkheid en uniformiteit dragen niet alleen bij aan de dienstverlening aan de burger, maar ook aan heldere uitvoering van privacymanagement. Hierdoor krijgen de departementen meer grip op de privacybeheersing en kunnen hier aantoonbaar rekenschap over geven. Om de burger ten dienste te zijn, is eenduidige informatievoorziening wenselijk. Op dit moment zien we dat ogenschijnlijk simpele privacyaspecten, zoals het voldoen aan verzoeken van betrokkenen en het implementeren van een verwerkingenregister, zeer verschillend opgepakt worden.

De in deze rapportage geconstateerde aandachtspunten lijken, in ieder geval deels, veroorzaakt te worden door de beperkte beschikbaarheid van privacydeskundigheid en de gekozen prioriteitsstelling. Wij merken op dat door de verschillende privacy incidenten binnen de Rijksoverheid dit onderwerp bij een aantal onderdelen beschouwd wordt als een punt van zorg. Meer inspanning en ondersteuning bij de inbedding van privacy management binnen de departementen kan bijdragen aan de borging van de kwaliteit van de privacybescherming binnen het Rijk.

Met het nieuwe Besluit CIO-stelsel Rijksdienst heeft BZK een eerste aanzet gedaan om duiding te gegeven aan het inrichten van een regierol met betrekking tot privacymanagement. Echter maakt dit nog geen onderdeel uit van het CIO-stelsel. Het besluit bepaalt dat de CIO een oordeel vormt en de departementsleiding adviseert over alle aspecten van digitalisering en informatievoorziening. Dit omvat aspecten zoals informatiebeveiliging, privacy en de ontwikkeling en het beheer van informatiesystemen, in elk stadium van het uitvoeringsproces, beleidsontwikkeling of het bedrijfsvoeringproces. De precieze invulling hiervan in relatie tot de functie van CIO-Rijk en CISO-Rijk moet nog plaatsvinden, maar kan wel bijdragen aan een meer gelijke aanpak en een gedeelde visie over de invulling van privacy-management. Vanwege de groeiende belangstelling voor het onderwerp privacy binnen de samenleving en daarmee de Tweede Kamer zal aandacht besteed moeten worden aan de formalisatie van de rijksbrede privacygovernance.

3 Rechten van betrokkenen

Doelstelling en risico:
De verwerkingsverantwoordelijke dient in staat te zijn om de juiste uitvoering te geven aan de rechten van betrokkenen. Hiertoe dienen de betrokkenen tijdig en volledig geïnformeerd te worden over de rechten waarop zij zich kunnen beroepen. De ontvangen AVG-verzoeken moeten tijdig en adequaat afgehandeld worden. Wanneer de gegevens onjuist, onnauwkeurig, niet volledig, verouderd of niet op integere wijze verkregen zijn, kan verwerking niet of niet meer zijn toegestaan. Ook kunnen de gebruikers verkeerde conclusies over de betrokkene trekken met mogelijk negatieve consequenties of naar het oordeel van betrokkene ongewenste verwerking van zijn of haar persoonsgegevens.
Onderzoekskader RBO AVG 2020

3.1 Procedures voor het afhandelen van AVG-verzoeken zijn vaak in opzet aanwezig, aantoonbare inbedding van adequate procedures vraagt nog aandacht.

3.1.1 De overheid informeert de burger over privacyrechten

De burger wordt door middel van de diverse privacyverklaringen op de websites geïnformeerd over zijn/haar rechten in het kader van de AVG. Ook wordt hierin aangegeven op welke wijze AVG-verzoeken kunnen worden ingediend, maar in veel gevallen beperkt de informatievoorziening zich tot het hoogstnoodzakelijke en wordt de burger niet proactief ondersteund bij het indienen van een verzoek. Enkele privacyverklaringen verwijzen wel naar de voorbeeldbrieven van de Autoriteit Persoonsgegevens (AP). Bij een aantal onderdelen wordt verwezen naar het Algemeen Contact formulier van de Rijksoverheid wat vaak verwarrend en/of ontmoedigend kan werken.

Best-practice: We hebben webformulieren aangetroffen die de burger wel op een eenvoudige en gebruiksvriendelijke manier ondersteunen bij het indienen van een AVG-verzoek. Voorbeelden hiervan zijn bij het Ministerie van Defensie en de Huurcommissie aanwezig.

Aanbeveling: Ondersteun pro-actief burgers bij het indienen van een AVG-verzoek bijvoorbeeld door het beschikbaar stellen van een begeleidende (contact)formulier als optie voor het indienen van een verzoek en door het verduidelijken van de informatievoorziening op de websites.

3.1.2 Procedures voor het afhandelen van de AVG-verzoeken vaak in opzet aanwezig

De meeste onderdelen beschikken over een procedure voor het afhandelen van AVG verzoeken met al dan niet onderliggende werkinstructies en modelbrieven die de verantwoordelijke functionarissen ondersteunen bij de uitvoering. Desalniettemin dient opgemerkt te worden dat een deel van deze procedures een hoog abstractieniveau kent en ook niet volledig is, waardoor een tijdige en effectieve afhandeling niet altijd geborgd kan worden. Dit blijkt onder andere uit het feit dat een aantal procedures niet in gaat op het afhandelen van rectificatieverzoeken. Een uitzondering hierop is bijvoorbeeld de uitgewerkte handreiking Rechten van betrokkenen van het Ministerie van VWS.

Best-practice: Een aantal onderdelen stelt de burger in staat zelf regie te voeren over een beperkt deel van de verwerkte persoonsgegevens. Dit is een positieve ontwikkeling die bijdraagt aan het vergroten van de transparantie en daarmee het vertrouwen in de overheid. Hierbij wordt door middel van een DigiD-account inzage verschaft tot het eigen dossier en wordt de mogelijkheid geboden om bepaalde

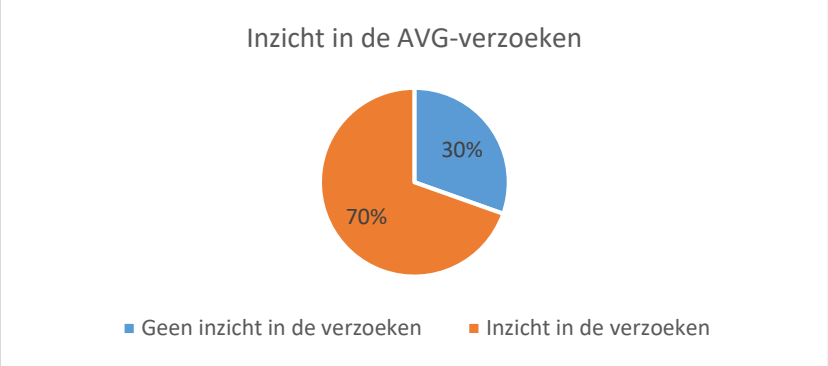
wijzigingen en aanvullingen zelf te doen. Voorbeelden hiervan zijn de Belastingdienst en de Rijksdienst voor Ondernemers.

<u>Aanbeveling:</u> Draag zorg voor procedures met een leidraad die toeziet op een tijdige afhandeling van AVG-verzoeken. In deze leidraad dient aandacht te zijn voor het aantoonbaar monitoren van de status van de afhandeling en het periodiek beoordelen daarvan.

3.1.3 Aantoonbare inbedding van procedures voor de afhandeling van de AVG-verzoeken is nog niet gerealiseerd.

In de praktijk worden de AVG-verzoeken vaak niet geheel in overeenstemming met de in opzet aanwezige procedures afgehandeld. Momenteel worden bij een aantal onderdelen de AVG-verzoeken door medewerkers van het primaire proces afgehandeld die niet altijd over voldoende privacy kennis beschikken. Het is niet duidelijk of zij de AVG-verzoeken als zodanig herkennen en conform de vereisten afdoen. Wij hebben geconstateerd dat een aantal van de onderdelen een overzicht heeft waarin de verzoeken vastgelegd worden en de status gemonitord kan worden. Echter is het inzicht in status van deze verzoeken niet bij alle onderdelen aanwezig waardoor het aantal en de tijdigheid en effectiviteit van afhandeling hiervan mogelijk niet gemonitord kan worden. Een aantoonbare PDCA-cyclus waarbij systematisch en periodiek een evaluatie plaatsvindt van de procedure en beheersingsmaatregelen die waarborgen dat deze naar behoren werken is nergens aangetroffen. Wel hebben wij bij een aantal onderdelen rapportages aangetroffen waaruit opgemaakt kan worden dat de tijdigheid van de afhandeling van verzoeken en het aantal binnengekomen verzoeken periodiek wordt verantwoord.

<u>Aanbeveling:</u> Zorg dat alle onderdelen een overzicht hanteren waarin AVG-verzoeken kunnen worden vastgelegd voor monitoring op een tijdige afhandeling.



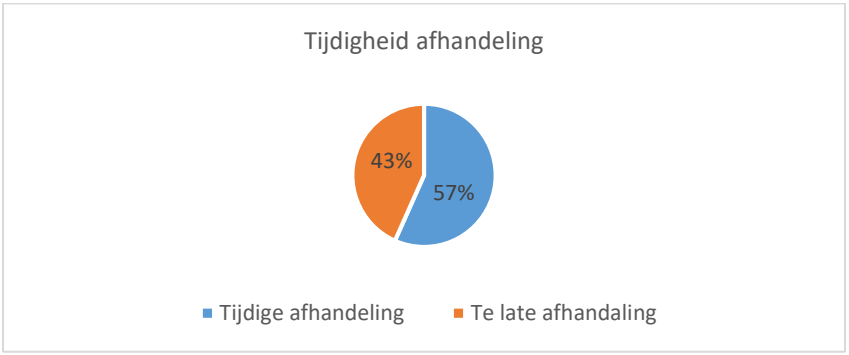
Figuur 1: Verdeling dienstonderdelen met en zonder inzicht in de AVG-verzoeken.

3.2 Borging van de tijdigheid en adequaatheid van de afhandeling van AVG-verzoeken vraagt nog inzet

3.2.1 Tijdigheid van de afhandeling van AVG-verzoeken is voor de meeste onderdelen nog een uitdaging.

In dit verkennend onderzoek hebben wij een ad random selectie geregistreerde AVG-verzoeken nader geanalyseerd. Dienstonderdelen die geen inzicht hebben in de door hun ontvangen AVG-verzoeken of die dat indirect ook niet konden geven zijn niet meegenomen in deze exercitie. Uit deze analyse blijkt dat de AVG-verzoeken geregeld niet binnen het initieel gestelde termijn van 30 dagen worden afgedaan. Over het algemeen wordt bij de meeste departementen vaak gebruik gemaakt van de optie om de afhandeltermijn te verlengen tot drie maanden, terwijl niet altijd duidelijk is of voldaan wordt aan de criteria die hieraan verbonden zijn. Bijvoorbeeld dat de verlenging gerelateerd is aan de complexiteit van het AVG-verzoek of de grote hoeveelheid ontvangen verzoeken. Bij een deel van de onderdelen is de inbedding van de interne procedures niet toereikend geweest om een deel van geselecteerde AVG-verzoeken binnen de uiterste termijn van drie maanden af te

doen. Daarbij wordt de burger in sommige gevallen ook niet schriftelijk op de hoogte gesteld van de verlenging. Bij kleine departementen worden de beperkt aantal ontvangen AVG-verzoeken vaak wel tijdig afgehandeld.



Figuur 2: De tijdigheid van de afhandeling van de geselecteerde AVG-verzoeken

3.2.2 *De AVG-verzoeken worden niet altijd in overeenstemming met de vereisten beantwoord.*

Uit de analyse is gebleken dat het overgrote deel van de inzageverzoeken schriftelijk wordt afgedaan. De interdepartementaal - of zelfontwikkelde modelbrieven bieden handvaten die bijdragen aan een correcte en eenduidige afhandeling, maar worden niet consistent gebruikt. Verder blijkt dat een beperkt deel van de verzoeken terecht niet wordt gezien als een beroep op de inzage recht. De burger wordt dan door een aantal onderdelen proactief geïnformeerd over de vereisten die gesteld worden aan een verzoek, maar ook over de beperkingen die het inzagerecht kent. Wij hebben in ons onderzoek een te beperkt aantal rectificatieverzoeken ontvangen om algemene resultaten te kunnen rapporteren. Aangegeven is dat deze verzoeken veelal in het primaire proces worden afgedaan.

<u>Aanbeveling:</u> Richt een controle- en monitoringsproces in teneinde de juistheid en tijdigheid van de afhandeling van AVG-verzoeken te borgen.

3.3 Inbedding van de kennisgevingsplicht vraagt dringend aandacht.

Binnen de Rijksoverheid zijn meerdere departementen en/of onderdelen samen verantwoordelijk voor bepaalde beleidsterreinen, zij delen grote hoeveelheden persoonsgegevens. Het is noodzakelijk dat de organisaties elkaar tijdig informeren wanneer verzoeken tot rectificatie, gegevenswissing of verwerkingsbeperking hebben geleid. Dit is een belangrijk onderdeel van de AVG omdat de risico bestaat dat op basis van verkeerde of onvolledige informatie mogelijk verkeerde besluiten genomen worden. Dit kan zeer vergaande negatieve gevolgen hebben voor de betrokkene.

We hebben geconstateerd dat de meeste organisaties geen procedures hebben opgesteld en/of ingericht die borgen dat de ontvangers van persoonsgegevens tijdig worden geïnformeerd over eventuele wijzigingen. Wij vinden het ook zorgelijk dat een aantal onderdelen geen kennis heeft van deze vereisten. Met het oog op de recente ontwikkelingen vragen wij dringend aandacht voor dit onderwerp.

<u>Aanbeveling:</u> Behandel de kennisgevingsplicht in de interne procedures en ontwikkel een stelsel van maatregelen om deze na te kunnen komen. Stel een leidraad op ter ondersteuning van het maken van de afweging wanneer afgeweken wordt van de kennisgevingsplicht.

4 Register van verwerkingsactiviteiten

Doelstelling en risico:
Voor de aantoonbare naleving van de AVG dient de verwerkingsverantwoordelijke onder andere een register van verwerkingsactiviteiten bij te houden. Het doel van dit register is inzicht te hebben in de verwerkingen van persoonsgegevens en de stromen van persoonsgegevens binnen de organisatie en bij de partijen die namens de organisatie persoonsgegevens verwerken. Het register draagt bij aan de verantwoordingsplicht van de aantoonbare naleving van de AVG. Het niet hebben van een overzicht van verwerkingen leidt tot een mogelijk incompleet beeld van de verwerkte categorieën persoonsgegevens en de getroffen maatregelen voor de relevante verwerkingen, processen en technische systemen. Het risico is dan aannemelijk dat de organisatie zich niet bewust is van de persoonsgegevens die zij verwerkt of aanvullende maatregelen die zij zou moeten treffen.
Onderzoekskader RBO AVG 2020

4.1 Registers van verwerkingsactiviteiten rijksbreed in gebruik, verwerkingen nog niet volledig vastgesteld.

4.1.1 Inrichting van het centrale register in lijn met de vereisten.

Alle ministeries hebben een centraal register van verwerkingsactiviteiten (hierna te noemen het centraal AVG-verwerkingsregister) voor het verkrijgen van inzicht in en overzicht van de verwerkingen binnen hun departement. Het centraal AVG-verwerkingsregister voorziet in de mogelijkheid voor de vastlegging van de vereisten uit de AVG. Dit betreft een tool die rijksbreed beschikbaar is gesteld en periodiek wordt geüpdatet en onderhouden door een centrale beheersorganisatie. Bij alle ministeries is het gebruik hiervan voorgeschreven voor het hele departement, met uitzondering van één ministerie. Het gebruik van een standaard tool draagt bij aan uniforme wijze waarop de burger geïnformeerd wordt over de verwerkingen.

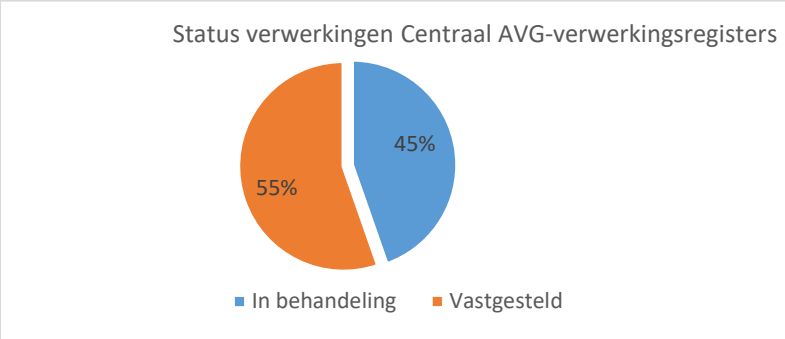
Bij één departement is het niet voorgeschreven om het centrale tool te gebruiken waardoor er gebruik gemaakt wordt van decentrale registers. Hierdoor is er geen volledig en centraal inzicht in de verwerkingen binnen dit departement waardoor er uitdagingen zijn in de ondersteuning van de beheersing van en toezicht op de verwerkingen. Dit departement is voornemens om in 2021 een andere tool aan te schaffen die naast de registratie van verwerkingen ook andere elementen van privacy management ondersteunt. Deze tool zal niet worden voorgeschreven voor de onderdelen. Hierdoor blijft de kans bij dit departement bestaan dat er geen centraal inzicht is in de verwerkingen. Naast dit departement heeft ook een ander departement aangegeven in 2021 over te overstappen naar een nieuwe tool voor het vastleggen van de verwerkingen binnen het departement. Hierbij dient oog te blijven voor de uniforme wijze waarop de burger geïnformeerd wordt over de verwerkingen.

4.1.2 Vaststelling verwerkingen bij meeste departementen nog niet gereed.

De centrale AVG-verwerkingsregisters geven inzicht in een groot deel van de verwerkingen binnen de departementen. De volledigheid van de AVG-verwerkingsregisters is nog een aandachtspunt bij meerdere departementen. Momenteel bevindt een beperkt aantal van de onderzochte onderdelen zich nog in een transitiefase waarbij de verwerkingen van een decentraal register overgezet worden naar het centraal AVG-verwerkingsregister van het betreffende departement.

Uit de analyse van de verwerkingen uit de centrale AVG-verwerkingsregisters blijkt dat een groot deel hiervan nog niet is vastgesteld. Dit is een aandachtspunt bij veel van de departementen.

Van de 4.341 verwerkingen in de centrale AVG-verwerkingsregisters waarin wij inzage hebben gekregen[3] is iets meer dan de helft vastgesteld. De overige verwerkingen zijn nog in behandeling (bijv. concept, in bewerking of ter review). Zoals eerder aangegeven heeft een aantal onderdelen eigen decentrale registers. Ook hiervan is een groot deel van de verwerkingen nog niet vastgesteld.



Figuur 3: Status van de verwerkingen in de centrale AVG-registers bij de departementen

Een aantoonbare accordering van de juistheid en volledigheid van de vastlegging van een verwerking door de verwerkingsverantwoordelijke hebben wij bij meerdere departementen niet (volledig) vast kunnen stellen. Wel maakt een deel van de departementen gebruik van authenticatieformulieren waarvan de geaccordeerde versie opgenomen worden in hun centraal AVG-verwerkingsregister. Doordat een aanzienlijk deel van de verwerkingen nog niet vastgesteld is, mede door een tekort aan privacy capaciteit en prioriteitstelling, wordt hier nog niet structureel uitvoering aan gegeven.

<u>Best-practice:</u> De twee onderzochte onderdelen van het Ministerie van Buitenlandse Zaken hebben wel voor de meeste verwerkingen het authenticatieformulier opgenomen in het AVG-verwerkingsregister. Hiermee onderschrijft de verwerkingsverantwoordelijke aantoonbaar de juistheid en volledigheid van de verwerkingen in het register.

4.1.3 *Deel van de verwerkingen is openbaar, geen duidelijke criteria voor publicatie.*

De meeste departementen hebben een deel van de verwerkingen ook (openbaar) gepubliceerd (op www.avgregisterrijksoverheid.nl) en geven daarmee (deels) invulling aan de informatieplicht die de AVG voorschrijft. Dit is in lijn met de afspraak van het CIO Beraad om deze informatie openbaar te maken tenzij daar reden voor zijn om het niet te doen. Bij vier departementen zijn er geen of een zeer beperkt aantal verwerkingen gepubliceerd op deze website.
Er zijn rijksbreed geen eenduidige criteria afgesproken met betrekking tot welke verwerkingen gepubliceerd worden, hierdoor wordt de uniforme weergave van de informatie niet geborgd.

<u>Aanbeveling:</u> Draag zorg voor richtlijnen en/of instructies voor het inhoudelijk vullen van het verwerkingsregister. Neem hierin ook de criteria voor het vaststellen en publiceren van de verwerkingen op.

Borging van de juistheid en volledigheid van het register van verwerkingsactiviteiten is vaak niet ingericht. Meerdere departementen hebben instructies opgesteld die bijdragen aan het uniform vastleggen van verwerkingen in het AVG-verwerkingsregister.

[3] Bij enkele departementen is niet volledig toegang verkregen tot het centraal AVG-verwerkingsregister.

Best-practice: De ministeries van Financiën, OCW en SZW hebben uitgewerkte instructies opgesteld die een juiste en volledige vastlegging van de informatie borgen.

Uit ons onderzoek blijkt dat de vereiste informatie in het centrale AVG-verwerkingsregisters en in de decentrale registers niet altijd eenduidig, volledig en samenhangend is. Wij hebben een selectie van de verwerkingen uit de AVG-verwerkingsregisters (centraal en decentraal) geanalyseerd. Hieruit is gebleken dat veel van de vereiste informatie is vastgelegd. Wel is aandacht nodig voor de inhoudelijke kwaliteit daarvan. De volgende aandachtspunten zijn geconstateerd:

- De rechtsgronden zijn vaak in algemene termen opgenomen. Bij veel van de verwerkingen ontbreekt de onderbouwing.
- De categorieën van persoonsgegevens worden op verschillende aggregatieniveaus in de registers opgenomen. Daarnaast blijkt dat bij meerdere verwerkingen de categorieën niet juist en/of volledig zijn opgenomen.
- De noodzaak voor het verwerken van de bijzondere persoonsgegevens blijkt niet altijd uit de vastlegging.
- Bij veel verwerkingen blijkt dat de bewaartermijnen niet opgenomen zijn of dat ze onjuist zijn. Ook worden ze meestal niet onderbouwd wat de beheersing en transparantie niet ondersteunt.
- In de AVG-verwerkingsregisters is vaak niet vastgelegd dat gebruik wordt gemaakt van verwerkers. Ook komt het geregeld voor dat ten onrechte verwerkers worden genoemd, terwijl dit geen verwerkers zijn volgens de definitie uit de AVG.

Een deel van de onderdelen heeft aandacht voor de kwaliteit van de informatie in de AVG-verwerkingsregisters. Ook hebben een aantal onderdelen aangegeven dat ze bezig zijn met een verbeterslag op de inhoud en consistentie van de vastleggingen. Aangegeven wordt dat een gebrek aan capaciteit en prioriteitstelling bij het primaire proces binnen de organisatieonderdelen ertoe leidt dat de benodigde verbeterslagen niet kunnen worden doorgevoerd of dat weinig vooruitgang wordt geboekt.

Afhankelijk van het privacybeleid van het departement dienen in het AVG-verwerkingsregister relevante bijlagen opgenomen te worden die de in het register opgenomen informatie verder staaft. Dit zijn onder andere vastgestelde data protection impact assessments (dpia's), verwerkersovereenkomsten of –afspraken en risicoanalyses (bijv. pre-pia's). Bij geen van de departementen zijn alle vereiste dpia's en verwerkersovereenkomsten of -afspraken opgenomen in de centraal AVG-verwerkingsregisters. Deels wordt dit veroorzaakt doordat de betreffende documenten nog niet gereed of actueel zijn. Een aantal departementen geeft aan bezig te zijn met het implementeren van een GRC-tool waarin onder andere dergelijke documenten opgenomen en beheerd zullen worden.

Aanbeveling: Draag zorg voor een register dat een juist, volledig en actueel beeld geeft van de verwerkingen van persoonsgegevens waarbij aandacht geschonken wordt aan de volledige samenhang tussen de vastgelegde gegevens en de verwerkingen.

4.2 Vastleggen verwerkingen in de rol van verwerker niet volledig en eenduidig.

Meerdere onderdelen verwerken ook persoonsgegevens voor andere overheidsdiensten. Een verwerker dient conform de vereisten ook een AVG-*verwerkers*register bij te houden van alle categorieën van verwerkingsactiviteiten die ten behoeve van een verwerkingsverantwoordelijke plaatsvinden. Uit ons onderzoek blijkt dat deze vastleggingen nog aandacht behoeven.
De huidige rijksbrede tool (centraal AVG-verwerkingsregister) kent een module om aan deze verplichting te voldoen. Echter is deze module door een zeer beperkt aantal departementen daadwerkelijk in gebruik genomen. Momenteel worden de verwerkingen in de rol van verwerker, indien ze wel vastgelegd worden, op diverse

manieren geregistreerd waarbij niet altijd de juistheid en volledigheid van de informatie wordt geborgd. Bij sommige dienstonderdelen blijkt dat deze verwerkingen opgenomen zijn in het centrale AVG-verwerkingsregister zonder dat duidelijk aangegeven is onder welk verantwoordelijkheidsgebied[4] dit verwerkt wordt.

<u>Aanbeveling:</u> Draagzorg voor het registeren van verwerkingen in de verantwoordelijkheid van een verwerker.

4.3 Inrichting PDCA-cyclus om actualiteit te borgen nog in ontwikkeling.

Een procedure die de actualiteit, juistheid en volledigheid van het AVG-verwerkingsregister borgt, is bij een paar onderdelen in opzet aanwezig. Met een enkele uitzondering is er nog geen aantoonbare PDCA-cyclus geïmplementeerd om de actualiteit van de registers te borgen.
Een van de uitzonderingen is het ministerie van Sociale Zaken en Werkgelegenheid waar de verwerkingen periodiek worden gereviewd en waar wijzigingen gemeld worden aan de Functionaris Gegevensbescherming.

<u>Aanbeveling:</u> Zie toe op een actualisatieprocedure die borgt dat het register periodiek aantoonbaar geanalyseerd (PDCA-cyclus) wordt zodat deze een accuraat beeld geeft van de verwerkingen en zodat hiermee de juiste maatregelen getroffen kunnen worden om de verwerkingen te beschermen.

[4] Verwerkersverantwoordelijke of verwerker

5 Opvolging aanbevelingen voorgaand jaar

5.1 Verbetertrajecten deels opgestart, voldoende privacycapaciteit blijft een aandachtspunt.

5.1.1 Inbedding privacymanagement vraagt nog inzet

In ons onderzoek hebben wij de CIO-offices op kerndepartementen gevraagd naar de verbetertrajecten die door de eerder onderzochte onderdelen mogelijk opgestart zijn teneinde de eerder door ons gesignaleerde privacyrisico's te mitigeren. Een deel van de onderdelen heeft activiteiten ondernomen voor (her)inrichting en verdere inbedding van privacymanagement en privacygovernance waarbij ook de bevindingen uit het voorgaand onderzoek meegenomen zijn. Dit traject betreft vaak een veranderproces dat meer tijd en aandacht kost.

Aanbeveling: Draag zorg voor voldoende capaciteit voor de verdere inbedding van privacymanagement waaronder de controle- en monitoringsactiviteiten.

5.1.2 Deels inzicht in de voortgang van de verbetertrajecten.

De voortgang van de gestarte verbetertrajecten wordt bij een deel van de onderdelen periodiek gemonitord en de resultaten worden soms verantwoord in voortgangsrapportages.

Uit de verschillende voortgangsrapportages blijkt dat de meeste activiteiten nog in uitvoering zijn of nog niet opgepakt zijn. Verder hebben wij hieruit vastgesteld en is in interviews ook aangegeven dat de doelstellingen van de verbetertrajecten vanaf medio 2021 aantoonbaar gerealiseerd zullen zijn.

Aangegeven is dat naast herprioritering in verband met de impact van de Corona-maatregelen ook de schaarse privacycapaciteit om de verbeterplannen uit te voeren reden is voor de vertraging. Dat laatste wordt met name veroorzaakt door de groeiende behoefte aan privacydeskundigheid bij de verschillende vraagstukken en taken omtrent de bescherming van persoonsgegevens.

Best-practice: Bij het ministerie van Financiën wordt de opvolging van de aanbevelingen uit relevante ADR en AR onderzoeken centraal gecoördineerd en gemonitord. Dit vergroot het inzicht in de te nemen maatregelen en de mogelijke overlap hiertussen wat bijdraagt aan het efficiënter inzetten van de schaarse capaciteit.

6 Verantwoording onderzoek

6.1 Werkzaamheden en afbakening

Het object van onderzoek betreft de beheersing van privacybescherming conform de AVG op het niveau van de eindverantwoordelijke van de geselecteerde verwerkingen. Uitgaande van de beschikbare capaciteit zijn naast het kerndepartement maximaal twee dienstonderdelen per departement betrokken bij dit onderzoek.
De scope van dit onderzoek is de opzet (is er een beschrijving van de maatregelen?) en bestaan van maatregelen (functioneren de maatregelen op het moment van onderzoek conform de opzet?) die de departementen en de door de ADR geselecteerde dienstonderdelen getroffen hebben teneinde de burger te faciliteren bij het uitoefenen van de hierboven beschreven rechten die voortvloeien uit de AVG. Tevens hebben wij de inrichting van het register van verwerkingsactiviteiten onderzocht alsook de in opzet en bestaan getroffen maatregelen om aan de hieraan gerelateerde vereisten uit de AVG te voldoen.

De werkzaamheden zijn uitgevoerd conform het vastgestelde in de opdrachtbevestiging. Voor het onderzoek is op elk departement een selectie gemaakt van verzoeken en risicovolle verwerkingen per departement. Aan de hand van de selectie is onderzocht op welke wijze de verwerkingsverantwoordelijke invulling heeft gegeven aan de in, opzet beschreven, maatregelen en aan de gestelde kwaliteitscriteria voor het register teneinde invulling te kunnen geven aan de aantoonbare verantwoordingsverplichting.
Tenslotte heeft het onderzoek naar de opvolging van aanbevelingen bestaan uit een kwalitatief onderzoek naar de werkzaamheden die door het departement of dienstonderdeel uit zijn gevoerd om het oorspronkelijke risico en/of gap weg te nemen.

Voor dit onderzoek is gebruikgemaakt van de in bijlage A opgenomen onderzoekskader waarin de relevante maatregelen uit het ADR Privacyframework zijn opgenomen alsook maatregelen die betrekking hebben op de opvolging van de verbeteractiviteiten. Het uitgangspunt van het ADR Privacyframework is de AVG en de UAVG, rekening houdend met de adviezen die de Autoriteit Persoonsgegevens (AP) en de European Data Protection Board (EDPB) hebben uitgebracht. Verder is bij het ADR Privacyframework gekeken naar het Privacy Control Framework van NOREA en naar de Privacy Baseline van CIP-Overheid.

6.2 Gehanteerde Standaard

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.
Naast deze standaarden gelden voor de onderzoeken van de ADR ook de regels die opgenomen staan in de Audit Charter. De Audit Charter geeft duidelijkheid aan alle betrokkenen over wat de auditfunctie inhoudt, hoe deze functie concreet wordt ingevuld en wat de aard en reikwijdte van de dienstverlening is die wordt geleverd aan de opdrachtgevers. Hier zijn ook de afspraken opgenomen met betrekking tot geheimhouding en vertrouwelijkheid.
Wij benadrukken dat op grond daarvan, verkregen (vertrouwelijke) gegevens uitsluitend voor de vervulling van deze opdracht worden gebruikt.

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.

6.3 Verspreiding rapport

De opdrachtgever, DGOO, is eigenaar van dit rapport.
Het opdrachtgeverschap intendeert in dit verkennend onderzoek een centraal belegde faciliterende rol bij DGOO en vloeit niet voort uit een formele verantwoordingslijn. De politieke leiding van een departement is immers zelf eindverantwoordelijk voor de naleving van de AVG en zal vanuit het eigen departement hier verantwoording over afleggen.

Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht is 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 door de ADR uitgebrachte rapporten en plaatst dit overzicht op www.rijksoverheid.nl.

7 Ondertekening

Den Haag, 13 december 2021

Projectleider Rijksbreed onderzoek Privacy

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