Auditdienst Rijk
Ministerie van Financiën

Deelrapport uitgebracht aan
CIO ministerie van Binnenlandse Zaken en Koninkrijkrelaties

Datum
6 december 2022

Auditdienst Rijk
Korte Voorhout 7
2511 CW Den Haag

Kenmerk
2022-0000299150

Rijksbreed AVG 2022
Deelrapport van bevindingen ministerie van Binnenlandse Zaken en Koninkrijkrelaties

Inleiding
Het rijksbreed AVG-onderzoek 2020 van de Auditdienst Rijk (ADR) heeft het beeld bevestigd dat de verdere inbedding van privacymanagement voor de onderzochte overheidsinstanties nog een uitdaging is. De ADR heeft in april 2022 met als peildatum 01-04-2022 een onderzoek uitgevoerd naar de opzet en waar mogelijk het bestaan van de wijze waarop het ministerie van Binnenlandse Zaken en Koninkrijkrelaties (BZK) en de dienstonderdelen Logius en Rijksdienst voor Identiteitsgegevens (RvIG) de interne organisatie heeft ingericht ten behoeve van een aantoonbare verantwoordingsverplichting, totstandkoming van verwerkersovereenkomsten en -afspraken alsmede de regie en toezicht op de naleving hiervan en welke privacycriteria er in de departementale cloudstrategie worden gehanteerd. Deze onderwerpen zijn belangrijke onderdelen van privacymanagement en dragen ook bij aan het vertrouwen van de burger. Naast het in kaart brengen van de actuele situatie is de doelstelling van het onderzoek om goede voorbeelden en verbeterpunten te identificeren in de inrichting, beheersing en verantwoording van privacybescherming binnen de departementen en op rijksbreed niveau.

Verantwoordingsverplichting en verantwoordingsstructuur
Door middel van een privacybeleid geeft de organisatie op organisatorisch- en strategisch niveau duidelijkheid over de inrichtingskeuzes en hoe zij waarborgt dat de verwerking van persoonsgegevens op een rechtmatige wijze plaatsvindt. Onderdeel hiervan is een heldere verdeling van taken en bevoegdheden, van middelen en rapportagelijnen zodat geborgd kan worden dat op de juiste wijze invulling wordt gegeven aan de eisen van het privacybeleid en de AVG.

Het ontbreken van een privacybeleid leidt ertoe dat de organisatie niet in beeld heeft wat precies wordt verwacht en wie waar verantwoordelijk voor is. Dit brengt het risico met zich mee dat persoonsgegevens onrechtmatig verwerkt kunnen worden. Denk daarbij aan o.a. het verzamelen, bewerken, inzien van gegevens.

Een beperking van dit onderzoek ten aanzien van deel 1, de verantwoordingsverplichting en verantwoordingsstructuur, is dat bij Logius en RvIG de Privacy Officers afwezig of uitdienst waren getreden ten tijde van dit onderzoek. De interviews zijn afgenomen met medewerkers die tijdelijk de taak van Privacy Officer oppakten, maar deze rol niet permanent vervulden.

Privacybeleid
Door de ADR is vastgesteld dat BZK beschikt over een Beleidskader Privacy- & Informatiebescherming en over Richtlijnen Privacy- & Informatiebescherming. Dienstonderdelen hebben de ruimte om aanvullende organisatie-specifieke richtlijnen op te stellen. Dienstonderdelen RvIG en Logius hebben hier ook invulling aan gegeven.

In opzet is vastgelegd dat de privacy-gerelateerde documenten worden geëvalueerd dan wel geactualiseerd om het effect van wijzigingen op de privacy vereisten te monitoren, beoordelen en te behandelen. Het evalueren en actualiseren wordt in gang gezet naar aanleiding van sporadische significante wijzigingen. Een expliciet cyclisch proces heeft de ADR niet altijd kunnen vaststellen.

De manier waarop BZK invulling geeft aan de beginselen inzake verwerking van persoonsgegevens (art. 5 AVG) zoals doelbinding, juistheid, dataminimalisatie en opslagbeperking komt niet expliciet uit het beleidskader en de richtlijnen van BZK naar voren. Wel wordt in het beleidskader en de in opzet beschreven 'richtlijn privacymanagement' aandacht besteed aan onderliggende processen zoals een register van verwerkingsactiviteiten en/of de uitvoering van DPIA's waarin impliciet de beginselen terugkomen.

Taken, bevoegdheden en verantwoordelijkheden
BZK heeft in opzet de taken, bevoegdheden en verantwoordelijkheden inzake privacy- en informatiebescherming vastgelegd in het beleidskader en de aanvullende richtlijnen. Vastgelegd is dat indien een aparte Privacy Officer is aangesteld, deze soortgelijke taken heeft als de CISO maar dan op het gebied van de bescherming van persoonsgegevens. Wat precies soortgelijke taken op het gebied van de bescherming van persoonsgegevens inhouden is niet concreet vastgelegd. Gezien er ten tijde van het onderzoek geen formele Privacy Officer was aangesteld bij RvIG of wel aangesteld was maar langdurig niet beschikbaar bij Logius, kon hier geen antwoord op worden gegeven.

Privacy bewust werken en opleiden
In opzet is vastgelegd dat BZK beschikt over een bewustwordingsprogramma waarbij periodiek informatie, kennis en handelingsperspectief m.b.t. informatiebeveiliging en privacy naar de medewerker wordt gebracht. Er wordt binnen het dienstonderdeel of directie de noodzaak bepaald om extra aandacht te geven aan IB en privacy. Hierbij kan deze extra aandacht zich richten op het hele onderdeel, of specifieke functionarissen binnen het onderdeel. Door de ADR is verschillende informatie ontvangen waaruit blijkt dat zowel op BZK-breed niveau als op het niveau van de onderliggende dienstonderdelen in de praktijk aan bovenstaande invulling wordt gegeven. Dit geldt ook voor het onboardingsprogramma waar privacy onderdeel van is. Het is echter niet altijd bekend wie en hoeveel medewerkers hebben deelgenomen aan bepaalde trainingen en cursussen m.u.v. het onboardingsprogramma.

Inrichting verantwoordingsstructuur
BZK heeft vastgelegd dat de CIO jaarlijks middels een overkoepelend verantwoordingsverslag verantwoording aflegt aan de Bestuursraad van het departement over de staat van informatiebeveiliging en privacy. Dit is door de ADR ook in bestaan vastgesteld. CIO-BZK stelt sjablonen ter beschikking die gebruikt moeten worden bij de deelverantwoordingen van de directies en dienstonderdelen gebaseerd op de implementatie en naleving van de BZK-brede richtlijnen die onderdeel zijn van het beleidskader. De verantwoording is hoofdzakelijk geënt op informatiebeveiliging waarbij privacy een onderdeel is.

Door de ADR is vastgesteld dat dienstonderdelen Logius en RvIG deelverantwoordingen over 2021 hebben aangeleverd. Inzake privacy worden onderwerpen bevraagd zoals volledigheid en actualiteit register, verwerkersovereenkomsten, DPIA's, datalekken, rechten van betrokken en informatieplicht. Het volwassenheidsniveau ten opzichte van het beleidskader wordt geplot in een spin-/radardiagram waardoor er geen specifieke gekwantificeerde informatie beschikbaar is (vb. aantal DPIA's, aantal inzageverzoeken etc.). Er wordt niet bij alle directies en dienstonderdelen een spin-/radardiagram gehanteerd. De ADR heeft niet kunnen vaststellen welke opvolgende maatregelen het management van het dienstonderdeel heeft genomen n.a.v. eerdere bevindingen over de staat van privacy (Act-gedeelte van PDCA).

Three Lines Model
BZK heeft in opzet de algemene taken en verantwoordelijkheden van de actoren (met uitzondering van de eerdergenoemde Privacy Officer) van impliciet het Three Lines Model in het Beleidskader beschreven. Het inrichten door de eerste lijn, het monitoren door de tweede lijn en het toetsen door de derde lijn – als expliciete koppeling naar het Three Lines Model – is minder concreet in opzet beschreven. Dienstonderdeel Logius heeft hier in de praktijk wel concreter invulling aan gegeven al is door de ADR geconstateerd dat verantwoordelijkheden en werkzaamheden van de eerste en tweede lijn soms door elkaar lopen. In het bijzonder bij de IB-specialisten die zowel het lijnmanagement bijstaan bij de uitvoering van het beleid (1e lijn) als toezien op de uitvoering van het beleid (2e lijn).

Aanbevelingen
Op basis van deze bevindingen doet de ADR de volgende aanbevelingen:
- Borg het actualiseren en evalueren van beleidsstukken omtrent privacy, naast significante wijzigingen, middels een concreet cyclisch proces tenminste eens per drie jaar.
- Breid het Beleidskader Privacy- & Informatiebescherming uit met de manier waarop BZK invulling geeft aan de beginselen inzake verwerking van persoonsgegevens en koppel dit aan de reeds bestaande onderliggende processen zoals het register van verwerkingsactiviteiten en de uitvoering van DPIA's.
- Beschrijf en documenteer expliciet de taken, bevoegdheden en verantwoordelijkheden van een Privacy Officer.
- Kwantificeer als onderdeel van de PDCA-cyclus de uitvraag en verantwoording inzake privacy om explicieter verantwoording af te

kunnen leggen over de staat van privacy binnen de directies en dienstonderdelen.
- Besteed bij de uitvraag omtrent de staat van IB en privacy tevens aandacht aan de opvolging van eerdere verbetermaatregelen (Act-gedeelte).
- Expliciteer de invulling en uitvoering van het Three Lines Model.

Verwerkersovereenkomsten en verwerkersafspraken

Bij de verwerking van persoonsgegevens door derden zijn maatregelen noodzakelijk om te borgen dat op de juiste wijze met persoonsgegevens wordt omgegaan en deze worden beschermd. Dit moet worden vastgelegd in een concrete overeenkomst of een andere rechtshandeling zodat er een verbintenis ontstaat tussen de verwerker en de verwerkingsverantwoordelijke.

Wanneer niet voldaan wordt aan de plicht de vereiste afspraken te maken, bestaat de kans dat de verwerkersverantwoordelijke grip op data van betrokkenen kwijtraakt, wat er mede voor kan zorgen dat er privacyrisico's ontstaan voor een betrokkene.

Geselecteerde dienstonderdelen en verwerkingen
Als steekproef voor dit onderdeel heeft de ADR een selectie gemaakt van vijf verwerkingen uit het register van verwerkingsactiviteiten. Deze verwerkingen vinden plaats bij de dienstonderdelen Rijksdienst voor Identiteitsgegevens (RvIG) en Logius:

1. M3299 – Toekennen BSN (RvIG)
2. M4448 – Uitvoering Wet Basis Registratie Personen (RvIG)
3. M1088 – DigiD machtigen (Logius)
4. M1533 – SC Burgerondersteuning eerste lijn (Logius)
5. M1931 – Mijn Overheid (Logius)

Garanties naleving AVG door verwerkers / DPIA
Vastgesteld is dat bij BZK en de geselecteerde dienstonderdelen in opzet is beschreven dat alleen verwerkers ingeschakeld mogen worden die voldoende garanties kunnen bieden dat zij aan de wettelijke vereisten voor gegevensbescherming voldoen. Zo dient er bijvoorbeeld bij de inkoop van diensten en producten ten behoeve van de informatievoorziening betrouwbaarheidseisen (bv vanuit de AVG) tijdig worden vastgesteld. Daarnaast dient er een DPIA te worden uitgevoerd om privacyrisico's in kaart te brengen.

Procedure opstellen verwerkersovereenkomsten
Vastgesteld is dat BZK en de geselecteerde dienstonderdelen niet beschikken over een expliciet in opzet beschreven proces waarin de taken, bevoegdheden en verantwoordelijkheden omtrent de totstandkoming van verwerkersafspraken en/of -overeenkomsten zijn beschreven. Aangegeven door Logius is dat het opstellen van verwerkersovereenkomsten onderdeel is van het reguliere inkoopproces. Logius geeft aan dat er in de praktijk niet altijd een eenduidige manier is en er verschillende wegen zijn (met verschillende actoren) betreft het opstellen van verwerkersovereenkomsten.

Verwerkersovereenkomsten met verwerkers
De ADR heeft van de geselecteerde verwerkingen van RvIG en Logius uit het register van verwerkingsactiviteiten alle verwerkersovereenkomsten met de vermelde verwerkers ontvangen. De ADR heeft geconstateerd dat alle verwerkersovereenkomsten zijn opgesteld conform rijksbreed format en de benodigde vereisten uit de AVG bevatten.

Controle en monitoring verwerkersovereenkomsten/-afspraken
Door de ADR is vastgesteld dat er binnen BZK geen formeel proces is ingericht dan wel in de bestaande processen voor contractmanagement is verankerd dat erop toeziet dat bij gewijzigde omstandigheden afgesloten verwerkersovereenkomsten worden aangepast. Logius heeft aangegeven dat het wel een gebruikelijke werkwijze is binnen Logius dat contractmanagement wordt benaderd indien verwerkersovereenkomsten aangepast moeten worden. Tevens is in opzet vastgelegd dat periodiek een risicobeoordeling moet plaatsvinden op bestaande verwerkersovereenkomsten, vastgelegd en gemonitord moet worden middels ISMS. De manier waarop dit uitgevoerd wordt is niet in opzet vastgelegd in een procesbeschrijving. Bij twee van de geselecteerde verwerkingen zijn er hernieuwde DPIA's uitgevoerd waar nieuwe risico's zijn gesignaleerd. Dit inzicht heeft echter (nog) niet geleid tot het aanpassen van de benodigde maatregelen voor deze nieuwe risico's uiteengezet in de verwerkersovereenkomsten en/of afspraken.

Toezicht en controle op naleving van de afspraken met verwerkers
BZK heeft in opzet beschreven dat de opdrachtgever door middel van periodieke rapportages geïnformeerd moet worden over het functioneren van de uitvoering van het proces, de informatievoorziening of dienst. Een explicietere koppeling naar een procedure t.a.v. de gemaakte afspraken met verwerkers inzake privacy ontbreekt echter in opzet. Wel is door de ADR geconstateerd dat in de praktijk sommige verwerkers periodieke rapportages aanleveren die tevens worden beoordeeld. Bijvoorbeeld vanuit RvIG met DICTU. De rapportages zijn echter hoofdzakelijk geënt op informatiebeveiliging en in mindere mate op privacy.

Aanbevelingen
Op basis van deze bevindingen doet de ADR de volgende aanbevelingen:
- Documenteer het proces betreft het opstellen van verwerkersafspraken en verwerkersovereenkomsten inclusief de taken, bevoegdheden en verantwoordelijkheden van de betrokken actoren.
- Richt een proces in voor de controle en monitoring van afgesloten verwerkersovereenkomsten zodat tijdig verwerkersovereenkomsten onderbouwd kunnen worden verlengd, beëindigd of nieuwe kunnen worden afgesloten.
- Om bovenstaande te kunnen realiseren, inventariseer en creëer overzicht in alle afgesloten verwerkersovereenkomsten en veranker dit in bestaande processen van contractmanagement.
- Documenteer en breid het proces inzake het periodiek aanleveren van rapportages door verwerkers uit met privacycriteria om explicieter invulling te kunnen geven aan de toezicht en controle op de gemaakte afspraken.

Privacycriteria in departementale cloudstrategie

Gezien overheidsorganisaties een transitie naar de cloud overwegen of in transitie zijn naar de cloud, leeft bij de privacy professionals van de departementen de behoefte om inzicht te krijgen in de criteria omtrent de bescherming van persoonsgegevens in de verschillende departementale cloudstrategieën. Naar aanleiding hiervan heeft de ADR een inventarisatie gehouden van de privacycriteria in deze departementale strategieën.

Cloudbeleid en strategie BZK
Vastgesteld is dat BZK beschikt over een in opzet beschreven cloudvisie en -strategie. Het document beschrijft de visie waarin de redenen voor een ontwikkeling naar de cloud worden besproken (waarom) evenals de bijbehorende strategie (hoe en waarmee). Hiermee geeft het document richting en handvatten voor architecten, adviseurs en managers binnen BZK en de uitvoeringsorganisaties ten aanzien van de Cloud First strategie van BZK. Het document dient gelezen te worden in relatie met het beveiligingsbeleid van BZK, de datastrategie en de open source strategie van de overheid.

Clouddiensten binnen BZK
Door de ADR is vastgesteld dat de verschillende onderdelen van BZK beschikken over een overzicht met afgenomen clouddiensten. Sommige passages zijn nog leeg maar het merendeel is ingevuld. Het ontbreekt bijvoorbeeld in sommige gevallen aan het rubriceringsniveau, platform en de al dan niet uitgevoerde risicoanalyse. Het CIO-office van BZK houdt geen centraal overzicht bij. De onderdeel-specifieke uitvraag kan voldoende zijn, mits alle benodigde gegevens worden ingevuld.

Risicoanalyse
In het Beleidskader Privacy- en Informatiebescherming BZK 2021 is in opzet de manier vastgelegd waarop binnen BZK het proces van risicomanagement is vormgeven. Hierin staat tevens de door BZK toegestane speelruimte gespecificeerd. In beginsel kunnen processen met een te beschermen belang van maximaal departementaal vertrouwelijk of processen waarin bijzondere persoonsgegevens worden verwerkt m.b.v. cloudtechnologie worden vormgegeven. Daarnaast beschikt BZK over – de in onderdeel 1 aangehaalde – in opzet beschreven richtlijnen IB en Privacy. Hierin zijn richtlijnen inzake IB en privacy beschreven die verplicht in de risicoanalyse moeten worden opgenomen. De richtlijnen zijn algemeen maar lenen zich ook voor Clouddiensten.

Casus AFAS-online
Door de ADR is vooraf clouddienstverlener AFAS-online geselecteerd om nader de uitgevoerde analyses en gemaakte afspraken te bekijken. SSO-CN

heeft aangegeven een BIV-analyse (Beschikbaarheid, Integriteit en Vertrouwelijk) uitgevoerd te hebben voor AFAS-Online. De ADR heeft echter deze analyse niet ontvangen. Ten aanzien van het opstellen van een verwerkersovereenkomst is door SSO-CN aangegeven dat deze met AFAS-Online niet expliciet aanwezig is. De eisen zijn verwerkt in de voorwaarden van AFAS. De Cloudvisie en -strategie van BZK schrijft voor dat er voor elk proces/ systeem waarin persoonsgegevens worden verwerkt met een hoog risico een DPIA moet worden uitgevoerd. Door SSO-CN is aangeven dat deze niet is uitgevoerd. Echter, is er wel een summiere risicoanalyse die betrekking had op het datatransport uitgevoerd. SSO-CN ontvangt periodiek gegevens vanuit AFAS met betrekking tot de beveiliging en er worden regelmatig pentesten uitgevoerd.

SSO-CN heeft aangegeven een nieuwe structuur te hebben opgezet om gecontroleerd nieuwe projecten uit te voeren via een projectbureau. Daarmee zullen DPIA's en (IB)risicoanalyses voor nieuw afgenomen clouddiensten meer gestructureerd doorlopen en gedocumenteerd worden. Aangegeven is dat voor de hoog risicosystemen bijna allemaal risicoanalyses zijn uitgevoerd, in het bijzonder de recente clouddiensten. Het kan zijn dat bij oudere clouddiensten dit minder het geval is.

Classificatie van data
In de richtlijn IB&P van BZK zijn een aantal classificatieniveau's voor de TBB's in opzet beschreven. Aangegeven is dat er binnen SSO-CN geen data en/ of middelen geclassificeerd of gelabeld worden.

Eigenaarschap
In de cloudstrategie van BZK is in opzet beschreven dat er bij het aanbesteden van een clouddienst een exit-strategie moet worden opgesteld. In de algemene voorwaarden van AFAS-Online is beschreven dat SSO-CN voor beëindiging van het contract alle gegevens kan exporteren. Na 1 jaar worden de gegevens definitief verwijderd bij AFAS. Daarnaast heeft BZK een aantal speerpunten opgesteld waaruit o.a. blijkt dat er voor elk informatiesysteem een eindverantwoordelijke moet worden aangesteld. Door SSO-CN is aangegeven dat zij zelf de eigenaar zijn van de data die op de servers van AFAS-Online staat. Het eigenaarschap van de data is door SSO-CN belegd.

Locatie
In opzet is niet gespecificeerd op welke locatie (in welk land) de data mag worden opgeslagen. In de algemene voorwaarden van AFAS-Online is beschreven dat er gebruik wordt gemaakt van twee datacentra in Nederland.

Aanbevelingen
Op basis van deze bevindingen doet de ADR de volgende aanbevelingen:

- Continueer de periodieke uitvraag van clouddiensten en benadruk het belang van het invullen van alle benodigde velden waaronder rubriceringsniveau, risicoanalyse en platform.
- Inventariseer of voor alle (oudere) clouddiensten met een hoog risicoprofiel een gedegen risicoanalyse is uitgevoerd.
- Classificeer informatie en informatiesystemen zodanig dat voor elke gebruiker duidelijk is welk soort informatie wel/niet in het systeem mag worden opgenomen.
- Beschrijf en documenteer het uitgangpunt van BZK ten aanzien van de locatie van gegevens.

Managementreactie CIO van Binnenlandse Zaken en Koninkrijksrelaties

Wij herkennen de bevindingen en de bijbehorende aanbevelingen. Wel maken we de kanttekening dat de impact van enkele bevindingen minimaal is. Bij Logius was de privacy officer gedurende de tijd van het ADR-onderzoek afwezig, echter zijn de taken en verantwoordelijkheden m.b.t. privacy (zoals rechten van betrokkenen) steeds volgens ons beleid en de AVG uitgevoerd.

Het is een juiste constatering dat onze invulling van de beginselen inzake verwerking van persoonsgegevens niet in de beleidsrichtlijn zelf is opgeschreven. Wel verwijzen we in de privacy-managementrichtlijn naar de 'Handreiking AVG'. In deze handreiking worden praktische handvatten gegeven voor de medewerker – op instructieniveau en met voorbeelden. Hoewel de handreiking in 2018 is opgesteld, staan de belangrijkste zaken er in. Deze handreiking is opgenomen in een voor iedere medewerker toegankelijke samenwerkingsruimte. We nemen de aanbeveling over in die mate dat de handreiking beter vindbaar wordt.
Inmiddels zijn wij bezig met de actualisatie van het beleidskader (voorzien eerste helft 2023) en nemen hierin de aanbeveling over om de taken, bevoegdheden en verantwoordelijkheden van een Privacy Officer duidelijker in het beleid op te nemen.

De aanbeveling om de verantwoording over privacy te kwantificeren, vullen we momenteel in met spin-radardiagrammen. Bij de ADR is bekend dat we vanaf de tweede rapportage in 2022 deze diagrammen verplicht hebben gesteld. Wij bevestigen dat in de rapportages tot nog toe IB het hoofdonderdeel is, maar het is nadrukkelijk de bedoeling, ook als onderdeel van een beheerste groei in volwassenheid, dat dit komend jaar evenwichtiger gaat worden.

In de viermaandelijkse IB&P-rapportages die de onderdelen van BZK opstellen, wordt aandacht besteed aan de opvolging van eerdere verbetermaatregelen - hiermee wordt invulling gegeven aan de vijfde aanbeveling. Hierbij plaatsen we de kanttekening dat hier nog meer uniformiteit in moet komen. Doordat de rapportages niet worden opgesteld naar aanleiding van uitvragen maar binnen het onderdeel zelf t.b.v. het management zijn het vaste onderdelen geworden van de PDCA's binnen het onderdeel. Gezamenlijk levert dit het grootste deel van de PDCA van het departement op.

Het klopt dat het three-lines model niet in volledigheid beschreven staat. Het beleidskader beschrijft de inrichting van de eerste en tweede lijn, dat zijn de lijnen waar we binnen BZK zelf verantwoordelijk voor zijn. De derde en vierde lijn zijn respectievelijk ADR en Rekenkamer, maar die maken geen deel uit van ons beleidskader. Omdat wij zien dat dit voor medewerkers toch nuttig kan zijn, zullen wij bij de actualisatie van het beleidskader het model behandelen.

Het BZK Beleidskader Privacy-& Informatiebescherming heeft een retentietermijn van maximaal drie jaar, waarna deze wordt herzien. Hoewel het beleidskader gedurende deze tijd statisch is, kunnen wijzigingen in de richtlijnen tussentijds worden aangebracht. Op deze manier blijven we wendbaar op onvoorziene en voorziene ontwikkelingen. In de periode van het huidige beleidskader is dit twee keer voorgekomen.

De aanbevelingen omtrent verwerkersovereenkomsten en -afspraken zijn duidelijke aanbevelingen die passen bij organisaties met een hoge mate van privacy-volwassenheid. Wij streven deze hoge mate van privacy-volwassenheid na en werken continu aan het versterken van onze privacy-organisatie. De aanbevelingen nemen we mee in de verdere ontwikkeling hiervan. We houden de ADR op de hoogte van onze vorderingen in de periodieke contactmomenten.

Onderzoeksverantwoording

Hieronder is de onderzoeksverantwoording weergegeven van het rijksbrede AVG onderzoek dat in april 2022 heeft plaatsgevonden bij het ministerie van Binnenlandse Zaken en Koninkrijkrelaties.

Opdrachtgever en opdrachtnemer

De politieke leiding van een departement is zelf eindverantwoordelijk voor de naleving van de AVG en dient vanuit het eigen departement hier verantwoording over af te leggen. Uitgaande van deze verantwoordelijkheid heeft de Auditdienst Rijk (ADR) dit rijksbreed onderzoek in opdracht van de leden van het CIO-beraad uitgevoerd. Teneinde dit onderzoek te coördineren en faciliteren heeft de CIO-Rijk als voorzitter van het Beraad de rol van gedelegeerd opdrachtgever vervuld.
De contactpersoon en daarmee aanspreekpunt voor dit onderzoek is P. Severens MBA in zijn rol van Privacy adviseur Rijksdienst (PAR). Hij onderhoudt de contacten met de ADR en draagt zorg voor de afstemming met de gedelegeerde opdrachtgever en de interdepartementale privacy officers.

Opdrachtnemer namens de ADR is, accountdirecteur voor de Ministeries van BZK en JenV. Deze opdracht is op 25 oktober 2021 besproken in het vooroverleg VIO-Beraad en is op 17 november 2021 in het CIO-Beraad behandeld.

Doelstelling en onderzoeksvragen

De doelstelling van dit onderzoek is drieledig:

1. Het verkrijgen van inzicht in de inrichting van de privacygovernance bij de departementen ten behoeve van de aantoonbaarheid van de naleving;
2. Het verkrijgen van inzicht in de kwaliteit van de afspraken met verwerkers alsook de inrichting van de controle en monitoringsactiviteiten die toezien op de naleving van deze afspraken;
3. Het verkrijgen van inzicht in de gehanteerde privacycriteria in de departementale cloudstrategieën.

Alle doelstellingen van dit onderzoek dienen om goede voorbeelden en verbeterpunten te identificeren in de beheersing en inrichting van privacybescherming op departementaal en rijksbreed niveau.

Per departement zijn de volgende onderzoeksvragen beantwoord:

1. Welke maatregelen heeft de organisatie in opzet en bestaan getroffen ten einde te voldoen aan de verantwoordingsverplichting over de naleving van de uitgangspunten van de AVG (art. 5 lid 2 AVG)?
2. Welke maatregelen heeft de organisatie in opzet en bestaan getroffen ten einde te borgen dat de gemaakte afspraken met verwerkers in overeenstemming zijn met de vereisten van de AVG en dat deze door hen worden nageleefd?
3. Welke privacy criteria zijn er in de departementale cloudstrategieën opgenomen?
4. Welke knelpunten worden bij de hierboven genoemde vragen gesignaleerd?

Object van onderzoek en scope

Het object van onderzoek betreft de beheersing van privacybescherming conform de AVG op het niveau van de eindverantwoordelijke van de geselecteerde verwerkingen. Dit betreft veelal taken die belegd zijn bij de CIO-office of de (concern) privacy-office van het betreffende departement of de hieronder gesitueerde dienstonderdelen. Uitgaande van de beschikbare capaciteit zal naast het kerndepartement maximaal twee dienstonderdelen per departement betrokken worden bij dit onderzoek. Dit rapport heeft betrekking op het kerndepartement Binnenlandse Zaken en Koninkrijkrelaties (BZK) en de dienstonderdelen Rijksdienst voor Identiteitsgegevens (RvIG) en Logius. Bij het kerndepartement is gekeken naar het privacybeleid en de inrichting van de verantwoordingsstructuur. Bij RvIG en Logius is tevens gekeken naar de verwerkersovereenkomsten en de regie hierop. Bij het kerndepartement is gekeken naar de cloudstrategie.

De scope van dit onderzoek is de door de departementen in opzet en bestaan getroffen maatregelen betreffende de geselecteerde verwerkingen van persoonsgegevens teneinde aantoonbaar rekenschap te kunnen geven. Voortkomend uit AVG art 5.2 is de verwerkingsverantwoordelijke verantwoordelijk voor de naleving van deze beginselen én kan deze aantonen. Hierbij zal op departementsniveau het aanwezige beleid, de positionering van de privacy organisatie en de verantwoordings- en rapportagestructuren binnen dit onderzoek vallen.

Onderzoekskader

Voor dit onderzoek is gebruikgemaakt van een onderzoekskader waarin de relevante maatregelen uit het ADR Privacyframework zijn opgenomen alsook de van toepassing zijnde normen uit het Data Pro Code. 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 zijn bij het ADR Privacyframework de Privacy Control Framework van NOREA en de Privacy Baseline van CIP-Overheid meegenomen. Ook is hierbij gebruik gemaakt van relevante normen uit de door de Autoriteit Persoonsgegevens (AP) geaccordeerde gedragscodes voor leveranciers van IT-diensten, de Data Pro Code. Deze Code kent een aantal maatregelen die bijdragen aan de invulling van de toezichtrol bij de opdrachtgever om te kunnen voldoen aan de verantwoordingsverplichting. Voor de toetsing van de cloudstrategieën zijn normen gebruikt die opgenomen staan in het geïntegreerde NORA/ISOR/BIO-kader.

Rapportage en openbaarmaking

Voor de leden van het CIO-Beraad stellen wij een rijksbrede rapportage op met daarin de overkoepelende bevindingen. De basis voor de overkoepelende rapportage zijn de deelrapportages per departement. In het rijksbrede rapport zullen wij goede voorbeelden en verbetermogelijkheden aangeven.

De departementale bevindingen zijn met de verantwoordelijken, waaronder de (concern)privacy officer op het departement afgestemd, waarna het definitief deelrapport aan de departementale CIO is verstrekt. Het deelrapport is een rapport van bevindingen. Met deze rapportages wordt geen zekerheid verschaft omdat geen assurance-werkzaamheden worden uitgevoerd. De rapporten bevatten daarom geen samenvattende conclusie of eindoordeel.

Het eigenaarschap van de deelrapportages is belegd bij de CIO van het betreffende departement waar deze betrekking op heeft.

In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de ADR een eindrapport heeft geschreven, het rapport binnen vier 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 de website. Op 1 mei 2022 is de Wet open overheid (WOO) in werking getreden. Deel- en interimrapporten moeten vanaf 1 mei 2022 gepubliceerd worden door de kerndepartementen.

Dossiervorming en geheimhouding

Bij de uitvoering van de opdracht is de gedragscode van het Instituut van Internal Auditors Nederland (IIA) van toepassing. Wij benadrukken dat op grond daarvan, verkregen (vertrouwelijke) gegevens uitsluitend voor de vervulling van deze opdracht worden gebruikt. De deelrapportages per departement zijn wel beschikbaar voor de tekenend accountant (ADR) van het betreffende departement voor de uitvoering van de wettelijke controletaak (informatiebeveiliging is onderdeel van het financieel en materieelbeheer) ter beperking van de auditlast op een departement.

De IIA-standaarden 2200 - 2600 zijn van toepassing voor deze opdracht evenals de Audit Charter van de ADR voor de uitgangspunten die voor de ADR van toepassing zijn.

Ondertekening

Den Haag, 6 december 2022

Projectleider | Auditdienst Rijk