Deelrapport uitgebracht aan
CIO ministerie van AZ

Datum
20-09-2022

Auditdienst Rijk
Ministerie van Financiën

Rijksbreed AVG 2022
Deelrapport van bevindingen ministerie van AZ
Definitief

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 mei 2022 met als peildatum 01-05-2022 een onderzoek uitgevoerd naar de opzet en waar mogelijk het bestaan van de wijze waarop het ministerie van Algemene Zaken (AZ) 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.

Privacybeleid
Uit onderzoek van de ADR blijkt dat AZ beschikt over een privacybeleid dat op 25-11-2019 is vastgesteld door de SG. Het privacybeleid is aan de medewerkers beschikbaar gesteld via het intranet. Echter is sinds de overgang naar het nieuwe Rijksportaal de pagina van het privacybeleid niet toegankelijk. AZ werkt aan een oplossing om het privacybeleid weer beschikbaar te stellen voor medewerkers. Het privacybeleid van AZ dient iedere drie jaar geëvalueerd te worden en indien nodig herzien. In 2022 is een privacy adviseur aangesteld om het privacybeleid en de -governance te evalueren. AZ verwacht het hernieuwde privacy beleid en de -governance in Q4 van 2022 te hebben afgerond.

Taken, bevoegdheden en verantwoordelijkheden
AZ heeft naast het privacybeleid het document: *privacy governance* opgesteld waarin de taken, bevoegdheden en verantwoordelijkheden van de actoren omtrent privacy concreet en duidelijk zijn uitgewerkt. De privacy governance is ter vervanging van een hoofdstuk uit het privacybeleid waar de taken, bevoegdheden en verantwoordelijkheden in zijn beschreven. In de privacy governance is beschreven dat de CISO en de CIO één taak hebben met betrekking tot privacy. Respectievelijk *Coördineren van de tijdige afhandeling van meldingen over mogelijke datalekken en AZ vertegenwoordigen in de interdepartementale Change Decision Board (CDB) van het AVG-register*. De rol van de CISO en de CPO zijn binnen AZ bij een functionaris belegd.

Bewustwording
In het privacybeleid is opgenomen dat de units en clusters binnen AZ verantwoordelijk zijn voor voldoende bewustwording bij hun medewerkers op het gebied van privacy. Per cluster is een awareness plan privacy opgesteld waarin eenmalige en jaarlijks terugkerende activiteiten zijn gepland. In de praktijk is het awareness plan ten tijde van het onderzoek nog niet ten uitvoer gebracht. AZ is bezig met het ontwikkelen van periodieke nieuwsbrieven omtrent privacy. Deze nieuwsbrieven zullen per mail verstuurd worden met als doel medewerkers te informeren over privacy-gerelateerde zaken.

Inrichting verantwoordingsstructuur
Uit de ontvangen documentatie komt naar voren dat AZ middels aanvullende procedures en instructies voor o.a. datalekken, DPIA en register van verwerkingsactiviteiten in opzet grotendeels invulling geeft aan de verantwoordingstructuur. In de praktijk ontbreken er echter rapportages omtrent de PDCA-cyclus van het privacymanagement en eventuele evaluatierapportages omtrent de PDCA-cyclus en de opvolging hiervan. Privacy Adviseurs rapporteren naar de Privacy Officers, maar deze rapportages zijn incident gedreven en hebben geen vast format. De privacy adviseurs en de privacy officers overleggen wekelijks over AVG-gerelateerde onderwerpen. Daar komen onderwerpen uit die (indien nodig) worden beschreven in een nota.

Three lines of defense (3LOD)
De uitgangspunten en de onderlinge verhouding (eerste lijn, tweede en derde lijn) van de taken/verantwoordelijkheden van het 3LOD zijn niet expliciet in opzet in de privacy governance gedocumenteerd. Wel is mondeling toelichting gegeven op de praktische uitvoering hiervan.

Aanbevelingen
Op basis van deze bevindingen doet de ADR de volgende aanbevelingen:
- Implementeer een vast format om periodiek te rapporten over AVG-gerelateerde onderwerpen. Op deze manier kan er concreter en eenduidiger invulling worden gegeven aan de PDCA-cyclus, in het bijzonder het Check en Act gedeelte.
- Documenteer de invulling van het 3LOD in het nieuwe privacybeleid of de nieuwe privacy governance.

Verwerkersovereenkomsten en verwerkersafspraken
Bij de verwerking van persoonsgegevens door derden dienen maatregelen genomen te worden om te borgen dat op de juiste wijze met persoonsgegevens wordt omgegaan en deze worden beschermd. Dit dient vastgelegd te worden 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
Vooraf is door de ADR als steekproef voor dit onderdeel een selectie gemaakt van vier verwerkingen uit het register van verwerkingsactiviteiten. Deze verwerkingen vinden het kerndepartement AZ (AZ-breed) en bij Dienst Publiek en Communicatie (DPC):
1. M492 - Contract- en leveranciersadministratie (AZ-breed)
2. M9962- Abonneeregistratie openbare e-maildiensten PRO (DPC)
3. M7406 - Mediadiensten (DPC)
4. M5837 - Publieksvoorlichting Informatie-Rijksoverheid (DPC).

Procedure opstellen verwerkersovereenkomsten
Vooraf is door de ADR een selectie gemaakt van vier verwerkingen uit het register van verwerkingsactiviteiten. Deze verwerkingen vinden plaats bij het kerndepartement en DPC. Uit de ontvangen documentatie door de ADR komt niet een expliciete procedure naar voren op welke manier AZ invulling geeft aan het proces almede de taken, verantwoordelijkheden en bevoegdheden omtrent de totstandkoming van verwerkersafspraken en/of overeenkomsten. Aangegeven is dat de procedure onderdeel is van het inkoopproces.

In de rijksbrede handreiking AVG staat dat het departement alleen verwerkers inschakelt die voldoende garanties bieden dat zij aan de wettelijke vereisten voor gegevensbescherming voldoen. AZ en DPC voeren een Quickscan uit op een mogelijk verwerker die onderdeel is van het aanbestedingsproces. Een onderdeel van de Quickscan is om de afweging te maken of er een DPIA uitgevoerd moet worden. AZ en DPC vragen bij de verwerkers certificeringen op zoals de ISO 27000 en SOC2. De verwerker wordt gevraagd om een fit-gap analyse in te vullen. In deze fit-gap analyse zijn alle privacy en IB-controls opgenomen. Wanneer een verwerker geen certificering heeft, kan deze ook op voorhand wel aantonen dat zij aan de controls voldoen door middel van de fit-gap analyse. De manier waarop AZ dit vormgeeft kan worden beschouwd als best-practice zijnde.

Risicoanalyse / DPIA
Uit het onderzoek van de ADR komt naar voren dat er in opzet een proces is beschreven voor het uitvoeren van DPIA's. Uit de vier verwerkingen die voor het onderzoek zijn geselecteerd was het niet noodzakelijk om een DPIA uit te voeren.

In het verwerkingsregister van AZ zijn in totaal 99 verwerkingen toegevoegd. Er zijn geen DPIA's in het verwerkingsregister toegevoegd. Of DPIA's noodzakelijk zijn bij een van de 99 verwerkingen is niet onderzocht.

Verwerkersovereenkomsten
De ADR heeft 4 verwerkingen uit het register van verwerkingsactiviteiten geselecteerd en de verwerkersovereenkomsten opgevraagd. Van 3 van de 4 verwerkingen hebben wij verwerkersovereenkomsten ontvangen. De verwerkersovereenkomsten zijn afgesloten conform rijksbreed format. In de verwerkersovereenkomsten zijn ook de afspraken opgenomen zoals vereist is vanuit de AVG. Van 1 overeenkomst hebben wij geen verwerkersovereenkomst ontvangen en daarom is deze verwerking ook niet onderzocht.

Controle en monitoring verwerkersovereenkomsten/-afspraken
Aangegeven is dat AZ geen expliciete procedure heeft opgesteld voor de controle en monitoring op verwerkersovereenkomsten. Wel is er eens in de drie jaar een controle of de verwerkersovereenkomsten nog aan de eisen voldoen. De hoeveelheid overeenkomsten die gecontroleerd moeten worden zijn beperkt, vanwege de verwerkingen die vaak eenmalig zijn. Er worden dan ook beveiligingsscans gedaan. Er is contractueel vastgelegd dat verwerkers veranderingen moeten doorgeven. Ook als dat niet het geval is, vraagt DPC ieder jaar in november aan alle partijen een bevestiging te overleggen dat de bestaande analyses nog actueel zijn. Deze maatregel kost AZ niet veel tijd. Het zorgt ervoor dat verwerkers wel nadenken over of er veranderingen zijn die wellicht geen grote impact hebben, maar die wel doorgegeven moeten worden. De manier waarop AZ dit vormgeeft kan worden beschouwd als best-practice zijnde.

Het is nog niet eerder voorgekomen dat een verwerkersovereenkomst tussentijds is aangepast. Aangegeven is dat indien een verwerkersovereenkomst tussentijds aangepast dient te worden AZ opnieuw het proces doorloopt van het opstellen van een verwerkersovereenkomst, met dezelfde procedure als bij een nieuwe overeenkomst.

Toezicht en controle op naleving van de afspraken met verwerkers
Aangegeven is dat AZ geen expliciete procedure of systeem heeft ingericht om rapportages van verwerkers te ontvangen en te beoordelen. In de praktijk ontvangt AZ ook geen rapportages. Wel wordt er, net zoals hierboven genoemd, ieder jaar in november aan alle partijen gevraagd een bevestiging te overleggen dat de bestaande analyses nog actueel zijn. Daarnaast voert DPC ieder jaar een aantal pentesten en steekproeven uit bij de verwerkers. Tijdens de steekproeven kijkt DPC mee in de systemen van de verwerkers. Op deze wijze kan DPC vaststellen welke persoonsgegevens worden verwerkt en of dat conform afspraak is. DPC kan vaak de statistische gegevens inzien van verwerkers en op basis van die gegevens kan DPC nadere rapportages opvragen. Dit gebeurt alleen als DPC een indicatie heeft dat er iets niet in orde is.

Aanbevelingen
Op basis van deze bevindingen doet de ADR de volgende aanbevelingen:
- Stel een procedure op voor het afsluiten van verwerkersovereenkomsten waarin ook een proces is opgenomen inzake dat er periodiek op wordt toegezien dat bij gewijzigde omstandigheden de verwerkersovereenkomst/-afspraken worden aangepast en beoordeeld worden of deze nog voldoen aan de eisen.
- Zorg voor een actueel verwerkingsregister waarin alle relevante documentatie inzake de verwerkingen is opgenomen. Denk hierbij aan DPIA's en verwerkersovereenkomsten indien van toepassing.

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.

Clouddiensten binnen AZ
Aangegeven is dat AZ cloud als tweeledig ziet. Enerzijds zijn er de kleine cloudzaken zoals apps op de werktelefoons van medewerkers. Anderzijds zijn er de grote cloud providers zoals Google, Amazon en Microsoft. Van de grote cloud providers maakt AZ enkel gebruik van Microsoft. De afspraken met Microsoft zijn rijksbreed gemaakt, waar AZ aanvullend een DPIA op heeft uitgevoerd.

Cloudstrategie AZ
AZ beschikt over een actueel cloudbeleid dat in juli 2021 is vastgesteld. Het doel van het beleid is duidelijk te maken onder welke voorwaarden gebruik kan worden gemaakt van public cloud dienstverlening door en voor medewerkers van AZ. Aangegeven is dat het beleid conform de Rijkskaders is. Voor de opslag, de verwerking en het transport van data zijn beschikbaarheids-, integriteits- en vertrouwelijkheidsmaatregelen. In het cloudbeleid is opgenomen dat cloudleveranciers dienen te voldoen aan: IB- en privacybeleid AZ, verschillende ISO-certificeringen, BIO en SOC 2 type II normen. Daarnaast worden Beveiligings Uitgangspunten Quickscan (BUQS) een fit-gap analyse en indien nodig een DPIA opgesteld. AZ beschikt over modelovereenkomsten die gebruikt worden om clouddiensten af te sluiten.

Classificatie
AZ classificeert en houdt opslaglocaties bij van de clouddiensten. Hiervan is een overzicht aangeleverd. AZ stelt voor elk informatiesysteem een BUQS op en dit betekent dat ze een processchema voor classificatie doorlopen. Dit zorgt er ook voor dat meteen duidelijk wordt of een DPIA nodig is of niet.

Eigenaarschap
Aangegeven is dat AZ eigenaar blijft van de data in de cloud. Het initiatief voor een cloudapplicatie wordt genomen door de data-eigenaar. Het initiatief wordt voorgelegd aan het CISO office en het volledige proces tot en met de inkoop van de cloudapplicatie dient te worden goedgekeurd door de CISO. AZ beschikt over een overzicht van alle systeemverantwoordelijken en het CISO-office houdt dit overzicht bij. AZ geeft aan geen vaste procedure te hebben voor een exit strategie. Echter zijn er wel beheersmaatregelen inzake de exit strategie beschreven in het cloudbeleid zoals: *AZ houdt zeggenschap over de eigen gegevens, zorg voor volledige overdracht van gegevens na beëindiging van de dienstverlening en ontwikkel fall-back scenario's.*

Aanbevelingen
Op basis van deze bevindingen doet de ADR de volgende aanbevelingen:
- Zorg dat er een formeel proces komt voor het opstellen van een exitstrategie, dat een directe relatie heeft met het cloudbeleid.

Managementreactie ministerie van AZ

AZ herkent zich in het in dit rapport beschreven beeld en zal de adviezen van de ADR opvolgen. Met betrekking tot de rapportage volgt AZ het ADR advies op door te rapporteren over de AVG in het Informatiebeveiligingsbeeld. In de periode 2022/2023 zal het privacy beleid worden herzien waarin wij de aanbevelingen van de ADR (3LOD) meenemen. Naar aanleiding van de het nieuwe Rijksbrede cloudbeleid zal AZ haar eigen cloudbeleid herzien en aanpassen. Hierbij zal er een standaard proces met betrekking tot Cloud Exit Strategie gerelateerd aan de eisen in het Cloudbeleid worden opgesteld.

Onderzoeksverantwoording

Hieronder is de onderzoeksverantwoording weergegeven van het rijksbrede AVG onderzoek dat in mei 2022 heeft plaatsgevonden bij het ministerie van Algemene Zaken (AZ).

Opdrachtgever en opdrachtnemer

De politieke leiding van een departement is zelf eindverantwoordelijk voor de naleving van de AVG en heeft vanuit het eigen departement hier verantwoording over afleggen. 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 drs. J.W. van Wingerde RA, 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 zijn naast het kerndepartement maximaal twee dienstonderdelen per departement betrokken worden bij dit onderzoek. Bij het ministerie van Algemene Zaken waren dit het kerndepartement (AZ-breed) en Dienst Publiek en Communicatie (DPC).

De scope van dit onderzoek was 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 zijn op departementsniveau het aanwezige beleid, de positionering van de privacy organisatie en de verantwoordings- en rapportagestructuren binnen scope van dit onderzoek gevallen.

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.