Auditdienst Rijk
Ministerie van Financiën

Deelrapport uitgebracht aan
CIO ministerie van Infrastructuur en Waterstaat

Datum
24-11-2022

Auditdienst Rijk
Korte Voorhout 7
2511 CW Den Haag

Kenmerk
2022-0000287359

Rijksbreed AVG 2022
Deelrapport van bevindingen ministerie van Infrastructuur en Waterstaat

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 juni 2022 met als peildatum 01-06-2022 een onderzoek uitgevoerd naar de opzet en waar mogelijk het bestaan van de wijze waarop het ministerie van Infrastructuur en Waterstaat 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
Infrastructuur en Waterstaat (hierna IenW) beschikt niet over een formeel gedocumenteerd privacybeleid. IenW geeft impliciet invulling aan een privacybeleid door links, praktische informatie en algemene handleidingen beschikbaar te stellen via een uitgebreide privacypagina op het intranet. Aangegeven is dat hiervoor bewust is gekozen, zodat de medewerkers zelf de benodigde informatie kunnen ophalen

De vormgeving van het privacybeleid in verschillende intranetpagina's vergemakkelijkt het proces rondom het actualiseren. De ADR heeft ook geconstateerd dat sommige pagina's recentelijk nog zijn geactualiseerd. Er is echter nog geen formeel proces ingericht dat de actualisering borgt. Recentelijk zijn er twee privacycoördinatoren IenW aangesteld. Met hen heeft de waarnemend Functionaris Gegevensbescherming (FG) wekelijks overleg waarin actualisering een onderwerp kan zijn.

De verschillende linkjes en documenten op de privacypagina geven gezamenlijk een breed beeld van onderwerpen dat men mag verwachten van een gedocumenteerd privacybeleid. Het ontbreekt echter soms aan de praktische invulling van IenW. Een aspect als dataminimalisatie is terug te vinden in de algemene handleiding AVG waarnaar verwezen wordt. Aangezien dit een algemeen document is, ontbreekt het aan de IenW-specifieke invulling. Een onderwerp als controle en toezicht (op de naleving van het privacybeleid) is niet terug te vinden.

De privacypagina is zeer uitgebreid en biedt behoorlijk wat handvatten voor de medewerker van IenW. De privacypagina als intranetpagina kan als best-practice worden beschouwd. Het ontbreekt echter aan een aantal zaken waardoor het niet als volledige vervanging van een formeel gedocumenteerd privacybeleid kan dienen. IenW is de mogelijkheid voor een concreet fysiek privacybeleid aan het verkennen dat bovenstaande informatie dient te bundelen. Dit zou dan ook een formeel document worden dat mogelijk vastgesteld wordt door of namens de SG.

Taken, bevoegdheden en verantwoordelijkheden
Op de privacypagina is er een specifieke sub-pagina gewijd aan de rollen en verantwoordelijkheden inzake privacy binnen IenW. Dit zijn echter vooral rollen en verantwoordelijkheden uit de AVG zoals een betrokkene en verwerker. Wel is er aandacht besteed aan de rol van privacycoördinator en FG waarnaar via een andere pagina verwezen wordt naar contactinformatie. De rollen en verantwoordelijkheden zijn niet altijd organisatie-specifiek gemaakt. Aangegeven is dat aanvullend op de pagina taken en verantwoordelijkheden zijn omschreven in het integraal beveiligingsbeleid 2018-2021. In een bijlage is inderdaad de aanvulling betreffende taken, bevoegdheden en verantwoordelijkheden weergegeven. Gezien er nog verwezen wordt naar de sinds 2018 niet meer geldende Wbp kan dit overzicht niet als actueel worden beschouwd.

Bewustwording
Aangezien het algemene privacybeleid is vormgegeven via een privacypagina op het intranet met links, praktische informatie en algemene handleidingen, is het voor de medewerkers makkelijk vindbaar. Naast het beschikbaar stellen van deze informatie werkt IenW ook op andere manieren aan privacy-bewust werken en opleiden. De ADR heeft vastgesteld dat er een E-learning beschikbaar is, privacy mee wordt genomen tijdens de onboarding van nieuwe medewerkers, een digitale variant van de dag van de privacy is gehouden en verschillende nieuwsberichten op het intranet worden gedeeld. Deze acties liggen in lijn met het doel van de minister dat iedere medewerker dient te beschikken over een bepaalde basiskennis omtrent de AVG. In opzet zijn de randvoorwaarden hiervoor aanwezig.

Inrichting verantwoordingsstructuur
IenW heeft sinds eind 2021 een tweejaarlijkse uitvraag in gang gezet om in kaart te brengen hoe de verschillende dienstonderdelen vormgeven aan privacyrisicomanagement, het register van verwerkingsactiviteiten en (privacy)risicoanalyses in de vorm van DPIA's. Dit proces is echter nog niet formeel in opzet gedocumenteerd. Bij de eerste uitvraag eind 2021 bleken er veel vragen te zijn waarna de gehanteerde kaders zijn aangepast. In 2022 gaat er een uitvraag plaatsvinden in juli en november. Op basis van de uitkomsten heeft de waarnemend FG inzicht op welke punten zij kan sturen. Aangegeven is dat de 'Act' vanuit de PDCA nog niet heeft plaatsgevonden omdat de eerste uitvraag vooral tot aanvullende vragen heeft geleid.

Ook bij de bestuurskern (BSK) heeft deze uitvraag plaatsgevonden. Aangegeven is dat hierover een zorg bestaat omdat de uitvraag eigenlijk gedaan dient te worden bij de verschillende onderliggende DG's van BSK. Omdat BSK één privacycoördinator heeft zijn alle onderdelen van BSK samengevoegd. Hierdoor bestaat de mogelijkheid dat er een overkoepelend vertroebeld beeld kan ontstaan. Bij de verschillende onderliggende stafdiensten en DG's kunnen verschillende vragen spelen naast het feit dat het primair en secundair proces van elkaar verschillen.

De tweejaarlijkse uitvraag door de waarnemend FG als interne toezichthouder omvat in het kader van de verantwoordingsplicht bijvoorbeeld geen gehouden bewustwordingsacties, datalekken en verzoeken van betrokkenen. Van ILT en RWS ontvangt de waarnemend FG wel elke maand een overzicht van de verzoeken van betrokkenen. Ook een datalekkenoverzicht wordt halfjaarlijks aangeleverd zodat er naar het karakter van de datalekken kan worden gekeken en of gezien het karakter van de datalekken specifieke maatregelen nodig zijn. Aangegeven is dat hiernaast de waarnemend FG, CIO en privacycoördinator van IenW in algemene zin ook op de hoogte worden gebracht van elke (voorlopige) melding door het meldloket IenW.

Three Lines Model
Door de ADR is in opzet geen beschrijving aangetroffen van de manier waarop IenW het Three Lines Model vormgeeft. Aangegeven is dat als verwerkingsverantwoordelijke en gemandateerd verantwoordelijke van de minister de DG de 1e lijn is. Deze wordt hierin onder andere bijgestaan door zijn privacycoördinator en informatiemanager. De 2e lijn wordt vormgegeven door juridische zaken. De 3e lijn wordt vormgegeven door de FG. Aangegeven is dat de waarnemend FG graag een overzicht van het Three Lines Model mee wil nemen in het nieuwe fysieke privacybeleid.

Aanbevelingen
Op basis van deze bevindingen doet de ADR de volgende aanbevelingen:
- Documenteer een IenW-breed privacybeleid met daarin aanvullend op de reeds beschikbare informatie op het intranet; IenW-specifieke invulling van AVG-principes, IenW-specifieke taken, bevoegdheden en verantwoordelijkheden, proces rondom tweejaarlijkse AVG-uitvraag bij de dienstonderdelen (PDCA-cyclus), invulling three lines

model en de manier van controle en toezicht op de naleving van het privacybeleid.
- Laat het fysieke privacybeleid vaststellen door of namens de SG.
- Start en documenteer een proces dat zowel de pagina's op het intranet als het toekomstige fysieke privacybeleid evalueert en actualiseert langs een cyclisch proces om het effect van wijzigingen op de privacyvereisten te monitoren, te beoordelen en te behandelen.
- Continueer de tweejaarlijkse AVG-uitvraag bij de dienstonderdelen en breid het – wanneer daar behoefte aan is naast de reguliere rapportages – uit met onderwerpen zoals bewustwordingsacties, verzoeken rechten van betrokkenen, datalekken, afgesloten verwerkersovereenkomsten en opgepakte verbeteracties voortkomend uit eerdere uitvragen (Act-gedeelte). Maak er door de uitbreiding eventueel een jaarlijkse uitvraag van.
- Splits bij de tweejaarlijkse uitvraag bij de dienstonderdelen BSK op in de onderliggende DG's en de stafdiensten om 'vertroebeling' te voorkomen. Wanneer wel één BSK-rapportage behouden wordt, maak in het BSK-rapport een explicieter onderscheid tussen de onderliggende stafdiensten en DG's.

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 plaats bij Uitvoering en Decentraal Advies en Control (UDAC) en DG Milieu en Internationaal (DGMI);

1. M5912 - Landelijk Asbestvolgsysteem (LAVS) [DGMI]
2. M5845 – AMICE [DGMI]
3. M5456 - Activiteitenbesluit Internet Module (AIM) [DGMI]
4. M6065 - Leer Management Systeem en Elektronische leeromgeving [UDAC]

Procedure opstellen verwerkersovereenkomsten
Door de ADR is geconstateerd dat UDAC en DGMI niet over een expliciet beschreven procedure beschikken voor het opstellen van een verwerkersovereenkomst evenals de daarbij behorende taken, verantwoordelijkheden en bevoegdheden. Wel maakt het opstellen van verwerkersovereenkomsten onderdeel uit van de algemene inkoopprocedure en is er een beslisboom betreffende het wel/niet opstellen verwerkersovereenkomst beschikbaar gesteld op de privacypagina op het intranet waar tevens algemene informatie betreffende verwerkersovereenkomsten uiteen is gezet.

Aangegeven is dat met de privacycoördinator contact wordt opgenomen wanneer afdeling inkoop een verwerkersovereenkomst ontvangt van de andere partij. Bij het opstellen van een verwerkersovereenkomst dient er gebruik gemaakt te worden van de rijksbrede ARBIT/ARVODI-modellen zoals omschreven is op de privacypagina op het intranet.

Risicoanalyse / DPIA
Uit de ontvangen documentatie valt geen expliciet proces op te maken op welke manier IenW en haar onderliggende dienstonderdelen borgen dat enkel verwerkers ingeschakeld worden die voldoende garanties bieden dat zij aan de wettelijke vereisten voor gegevensbescherming voldoen. Alleen in het privacybeleid van RWS wordt er expliciet aandacht aan besteed. In het programma van eisen behorend bij een inkoop/aanbesteding dient met deze verantwoordelijkheid rekening te worden gehouden (privacy by design). Op welke manier hier praktische uitvoering aan wordt gegeven is niet expliciet beschreven.

Aangegeven is dat als onderdeel van een inkoop een verwerker alleen persoonsgegevens mag verwerken conform de afspraken gemaakt in een verwerkersovereenkomst. In de Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten (ARVODI-2018) is in opzet in art. 14.1 vastgelegd dat de opdrachtnemer (verwerker) de toepassing van passende technische en organisatorische maatregelen garandeert, opdat de verwerking aan de vereisten van de AVG voldoet.

Voor de BSK, waar UDAC en DGMI onder vallen, is er een uitgebreide procesbeschrijving privacy opgesteld waarin o.a. het proces rondom het opstellen van een DPIA staat omschreven. In de procesflow van de DPIA zijn garanties door verwerkers echter niet opgenomen.

Betreffende de geselecteerde verwerkingen is door de ADR geconstateerd dat voor verwerking M5912 Landelijk Asbestvolgsysteem (LAVS) in het register is aangegeven dat er geen DPIA uitgevoerd hoeft te worden maar dit wel heeft plaatsgevonden vanuit safety-first-principe. De vraag is of de uitgevoerde (achteraf gezien onnodige) DPIA nog bijgevoegd dient te worden in het register. Deze situatie geldt ook voor verwerking M6065 LMS. Aangegeven is dat er regelmatig vragen binnenkomen over DPIA's bij de privacycoördinator. Er bestaat onduidelijk of een DPIA uitgevoerd dient te worden en interpretatie hierover verschilt binnen verschillende afdelingen.

Verwerkersovereenkomsten
Uit de steekproef van de ADR komt naar voren dat het register niet altijd een actueel beeld geeft van de verwerkers en afgesloten verwerkersovereenkomsten. Voor verwerkingen M5912 LAVS en M5845 AMICE geldt dat er een verouderde verwerkersovereenkomst met CGI is bijgevoegd en vervangen dient te worden met de verwerkersovereenkomst met IBM. Deze verwerkersovereenkomst met IBM is conform rijksbreed ARBIT-model, omvat de benodigde gegevens maar is echter niet tweezijdig ondertekend. Aangegeven is dat de oorzaak hiervan besloten ligt in het feit dat de overeenkomst RAD -d.d. 2 november 2015- is afgesloten onder ARBIT 2014. Deze kent, in tegenstelling tot overeenkomsten afgesloten onder ARBIT 2018, geen afdwingbaar artikel om te komen tot een separate tweezijdig getekende verwerkersovereenkomst.

Voor verwerking M6065 LMS en M5456 AIM geldt dat er met de desbetreffende verwerker een verwerkersovereenkomst is opgesteld conform rijksbreed ARBIT-model, de verwerkersovereenkomst de benodigde gegevens omvat en tweezijdig ondertekend is.

Controle en monitoring verwerkersovereenkomsten/-afspraken
Aangegeven is dat er binnen de BSK, waar UDAC en DGMI onder vallen, nog geen formeel proces is ingericht dan wel in de bestaande processen voor contractmanagement is verankerd dat erop toeziet dat bij gewijzigde omstandigheden de verwerkersovereenkomsten worden aangepast. Een verwerkersovereenkomst maakt onderdeel uit van het contractendossier. Een algemeen overzicht van de afgesloten verwerkersovereenkomsten zou handig zijn en kan ook controle en monitoring hierop bewerkstelligen. De vraag is of dit vanuit een centraal IenW perspectief bijgehouden dient te worden of vanuit de verschillende onderdelen. Om dit vorm te geven zal door verwerkingsverantwoordelijke extra capaciteit beschikbaar gesteld te dienen te worden.

Toezicht en controle op naleving van de afspraken met verwerkers
In het Rijkswaterstaat Applicatie Diensten (RAD) Dossier Afspraken en Procedures is een specifiek paragraaf toegewijd aan sturende processen. Hierin wordt aangegeven dat IBM maandelijks rapportages aanlevert. In de maandelijkse rapportages wordt echter geen lijn gelegd met de verwerking van persoonsgegevens. Hiermee is er geen proces ingericht betreffende de toezicht en controle op de naleving van de afspraken met verwerkers inzake de verwerking van persoonsgegevens. Om dit vorm te geven zal extra capaciteit benodigd zijn. Aangegeven wordt dat vertrouwen een grote rol speelt door de langdurige goede relatie. Dit komt onder andere doordat ook kleine datalekken worden gemeld en bericht wordt ontvangen dat er een audit is uitgevoerd op ISO27001 waarna hierover ook wordt gesproken.

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

- Breid de privacypagina op het intranet uit met de taken, verantwoordelijkheden en bevoegdheden rondom het proces van het opstellen van verwerkersovereenkomsten alsmede een korte verwijzing naar het proces an sich.

- Neem in opzet in de reeds bestaande DPIA-handreiking op dat er alleen verwerkers ingeschakeld worden die voldoende garanties bieden dat zij aan de wettelijke vereisten voor gegevensbescherming voldoen. Voer in bestaan ook de daadwerkelijke check uit.
- Actualiseer het register van verwerkingsactiviteiten door de juiste DPIA's, verwerkers en bijbehorende verwerkersovereenkomsten toe te voegen. Laat de verwerkingsverantwoordelijke zo nodig capaciteit uitbreiden om dit te kunnen bewerkstelligen.
- Draag zorg voor een generieke aanpak van DPIA's om te voorkomen dat er niet-noodzakelijke DPIA's worden uitgevoerd om zo de schaars beschikbare capaciteit zo efficiënt mogelijk te benutten.
- Creëer overzicht van de afgesloten verwerkersovereenkomsten om inzichtelijk te maken welke verwerkersovereenkomsten nog afgesloten en geactualiseerd dienen te worden in het kader van controle en monitoring. Betrek daarom verwerkersovereenkomsten in de tweejaarlijkse uitvraag (zie eerdere aanbeveling).
- Breid de periodieke rapportages van de verwerkers uit met privacycriteria om de nakoming van de verplichtingen voortvloeiend uit de verwerkersovereenkomst/-afspraak over de naleving van de afspraken omtrent de bescherming van persoonsgegevens te borgen

Privacycriteria in departementale cloudstrategie

Aangezien 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 Cloud Competence Community
IenW beschikt over een Cloud Competence Community (CCC) dat in 2016 is ontstaan uit het verzoek van de CIO-raad om een stuk op te stellen waarin staat hoe IenW omgaat met cloudtoepassingen. Dit heeft geleid tot een uitgebreid cloudbeleid 1.0 en later 2.0 (maart'22). In de community worden Cloud-gerelateerde ervaringen eens per 2 maanden uitgewisseld. Het initiatief van een CCC kan als best-practice worden beschouwd.

Aangegeven is dat op dit moment binnen de CCC voornamelijk samenwerkingen zijn met architecten en Informatiebeveiligingsexperts vanuit alle organisatieonderdelen. Privacy krijgt met name aandacht bij andere processen. Dit neemt niet weg dat een nadrukkelijke input vanuit privacy-perspectief binnen de CCC noodzaak is en iets is wat IenW momenteel aan het verkennen is met de recent aangestelde privacycoördinatoren IenW. Voornamelijk met betrekking tot Cloudproviders uit de VS is enige extra privacykennis nodig. Internationale uitwisseling van persoonsgegevens is gebonden aan de AVG.

Clouddiensten binnen Infrastructuur en Waterstaat
IenW beschikt niet over een lijst met alle lopende clouddiensten binnen het departement. Wel wordt bij de CCC het initiatief genomen om dit in kaart te brengen. CCC is begonnen met het uitvragen en na te denken over op welke manier de cloudtoepassingen het meest handig geregistreerd kunnen worden, dit in relatie tot andere initiatieven op het gebied van portfoliomanagement die al bij IenW lopen.

Risicoanalyse Cloudtoepassingen
In het cloudbeleid staat aangegeven dat bij dataopslag bij een externe partij altijd een DPIA vooraf uitgevoerd dient te worden. Daarin wordt de rubricering bepaald en vastgesteld dat deze aantoonbaar wordt toegepast. Een cloudtoepassing brengt specifieke andere uitdagingen met zich mee dan een reguliere inkoop. Aangegeven is dat de intentie is om met een aanvullende handreiking bij een inkoop verder te gaan dan een vinkje bij een Quickscan Informatiebeveiliging die inclusief een pre-DPIA scan al verplicht wordt uitgevoerd binnen IenW voor alle IV/ICT projecten. De handreiking wordt hiermee een verlengde van het stappenplan in het cloudbeleid.

Classificatie
Naast de algemene classificatie/rubricering van data binnen de rijksoverheid (DepV, Stg., etc.) heeft RWS een aanvullende methode. Aangegeven is dat het bij de bestuurskern is het algemeen zo is dat de hele werkplekomgeving DepV is. Individuele data wordt niet bij alle bedrijfsonderdelen geclassificeerd. Bij RWS gebeurt dit wel. Aangegeven wordt dat wat betreft Cloud vanuit de Quickscan Informatiebeveiliging in algemene zin wordt geclassificeerd, zo specifiek en gedetailleerd als nodig wordt geacht.

Eigenaarschap
Conform de gehanteerde ARBIT-voorwaarden is IenW eigenaar van de data. Eigenaarschap van de voorziening komt men hoe dan ook tegen bij het inkoopproces en de projectuitvoering. Wanneer er nagedacht wordt over de restrisico's voor wat betreft de voorziening beschrijft het cloudbeleid de algemene verantwoordelijkheden. Voor data komt de verantwoordelijk in het Cloudbeleid niet expliciet naar voren. CCC is voornemens om dataeigenaarschap explicieter op te nemen in het cloudbeleid.

Locatie
In het Cloudbeleid is in opzet beschreven dat als uitbreiding op de risico's de karakteristieken van de clouddienst alsmede de geografische regio van verwerking en opslag van gegevens worden meegenomen. Of de Cloud Service Provider (CSP) deze verslaglegging doet of de cloud broker is niet duidelijk.

Controle en monitoring op cloudtoepassingen
Een concreet proces rondom de controle en monitoring achteraf op gemaakte afspraken betreffende cloudtoepassingen is niet nog ingericht. In de algemene architectuur zijn wel een aantal mechanisme ingebouwd zoals een DPIA om vooraf te zorgen dat er over de juiste onderwerpen wordt nagedacht. Er is een overleg met alle privacycoördinatoren voorgezeten door de FG, als interne toezichthouder IenW. De FG maakt hiervoor een agenda aan met input van de privacycoördinatoren. Aangegeven is dat wanneer relevant Cloud hier ook een onderdeel van is.

Cloudbroker
Aangegeven is dat de onderdelen de behoefte erkennen aan een cloudbroker. De voorkeur vanuit architectuur gaat uit naar een rijkscloud-oplossing zodat het ook in Nederland kan draaien zodat men automatisch gebonden is aan de BIO en AVG. Een concernbreed overzicht is er momenteel nog niet, maar zou wel gewenst zijn. Ook dat wordt meegenomen in het hiervoor genoemde portfoliomanagement-initiatief m.b.t. cloudtoepassingen.

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

- Betrek privacyexpertise in de CCC om te borgen dat privacycriteria worden meegenomen bij cloud-gerelateerde vraagstukken.
- Realiseer het voornemen om de Cloudtoepassingen binnen IenW in kaart te brengen.
- Richt een proces in dat achteraf toeziet op de gemaakte afspraken met Clouddiensten (zie in het verlengde de eerdere aanbeveling omtrent toezien afspraken met verwerkers).
- Realiseer de aanwezige behoefte voor een cloudbroker, bij voorkeur een rijkscloud-oplossing in samenwerking met de andere departementen.
- Realiseer het voornemen om een handreiking Cloud op te stellen om zo cloud-specifieke uitdaging mee te kunnen nemen in het reguliere inkoopproces in het kader van een risicoanalyse.
- Neem eigenaarschap van data expliciet op in het cloudbeleid.

Managementreactie ministerie van Infrastructuur en Waterstaat

Het Ministerie van IenW kan zich vinden in de conclusies van de auditor. We kijken positief naar de toekomst, waarin we verder zullen gaan op de ingeslagen weg en de bevindingen opgenomen in het Deelrapport IenW waar mogelijk zullen overnemen. Ook onderkennen wij dat wij zeker nog stappen kunnen zetten. De belangrijkste stappen die wij nemen zijn de volgende:

Privacybeleid
Het privacybeleid wordt nu in schrift opgesteld. Dit beleid geeft een IenW specifieke invulling van de AVG-principes, IenW-specifieke taken, bevoegdheden en verantwoordelijkheden. Beoogd wordt dat deze in 2023 door de SG wordt vastgesteld tezamen met het geactualiseerde Integrale beveiligingsbeleid IenW.

DPIA-handreiking

Aansluitend actualiseren wij de bestaande DPIA-handreiking zodat deze (meer) handvatten biedt voor een generiekere aanpak van DPIA's om te voorkomen dat niet-noodzakelijke DPIA's binnen IenW worden uitgevoerd. Deze generiekere aanpak houdt ook in dat wij alleen verwerkers inschakelen die voldoende garanties bieden ten aanzien van het voldoen aan de wettelijke vereisten voor gegevensbescherming. Het creëren van effectiever inzicht in de gesloten verwerkersovereenkomsten zal nader de aandacht verkrijgen.

Privacypagina
Tevens zullen wij onze privacypagina actualiseren overeenkomstig het privacybeleid waarbij we de gebruikersvriendelijkheid van de pagina voor onze medewerkers behouden. Hierbij besteden wij in het bijzonder aandacht aan de taken, verantwoordelijkheden en bevoegdheden rondom het proces van het opstellen van verwerkersovereenkomsten.

AVG-uitvraag
Wij continueren de halfjaarlijkse AVG-uitvraag voor het jaar 2023 en nemen deze als zodanig op in het privacybeleid. Daarbij onderzoeken wij de mogelijkheid tot het splitsen van de uitvraag naar dienstonderdelen BSK op onderliggende DG's en de stafdiensten nader evenals het betrekken van verwerkersovereenkomsten.

Cloudbeleid
Tenslotte maakt het cloudbeleid geen specifiek onderdeel uit van het privacybeleid. Wel zorgen we voor privacyexpertise in de Cloud Competence Community voor borging van privacycriteria uit ons privacybeleid bij cloudvraagstukken.

Onderzoeksverantwoording

Hieronder is de onderzoeksverantwoording weergegeven van het rijksbrede AVG onderzoek dat in juni 2022 heeft plaatsgevonden bij het ministerie van Infrastructuur en Waterstaat.

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 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 Infrastructuur en Waterstaat waren dit UDAC en DGMI.

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.

Ondertekening

Den Haag, 24 november 2022