Auditdienst Rijk
Ministerie van Financiën

Deelrapport uitgebracht aan
CIO ministerie van Economische Zaken en Klimaat

Datum
01-12-2022

Auditdienst Rijk
Korte Voorhout 7
2511 CW Den Haag

Kenmerk
2022-0000288949

Rijksbreed AVG 2022
Deelrapport van bevindingen ministerie van Economische Zaken en Klimaat

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 juli 2022 met als peildatum 01-07-2022 een onderzoek uitgevoerd naar de opzet en waar mogelijk het bestaan van de wijze waarop het ministerie van Economische Zaken en Klimaat 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 Algemene Verordening Gegevensbescerming (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
Economische Zaken en Klimaat (EZK) beschikt samen met Landbouw, Natuur en Voedselkwaliteit (LNV) over een in opzet beschreven privacybeleid vastgesteld door of namens de Secretaris-Generaal (SG). Het privacybeleid bevat een leeswijzer waardoor het een prettig leesbaar en helder document is. Door de ADR is vastgesteld dat het privacybeleid gepubliceerd is op het Rijksportaal en gedeeld is via het privacyplatform waarin informatie m.b.t. privacy met de privacyfunctionarissen van het departement wordt gedeeld. Binnen EZK is er breed draagvlak voor het privacybeleid omdat de privacy officers van de verschillende dienstonderdelen betrokken waren bij het opstellen.

In het privacybeleid is in opzet beschreven dat het CIO-office ten minste eens per drie jaar voor evaluatie en bijstelling zorgdraagt. Indien er eerder aanleiding is om het document op onderdelen te wijzigen kan dit ook door een addendum aan het document toe te voegen. Door de ADR is vastgesteld dat het privacybeleid inderdaad naar aanleiding van de versie in 2018, in 2021 is geactualiseerd.

In het privacybeleid van EZK/LNV is in opzet beschreven op welke manier EZK/LNV invulling geeft aan de beginselen inzake verwerking van persoonsgegevens die vervolgens hun weg vinden in onderliggende beleidsstukken, procedures en richtlijnen, de privacyverklaring op de website, uit te voeren Data Privacy Impact Assessments (DPIA's) en het register van verwerkingsactiviteiten (de vezels van de organisatie).

Taken, bevoegdheden en verantwoordelijkheden
EZK/LNV heeft in opzet overzichtelijk de taken, bevoegdheden en verantwoordelijkheden inzake de privacy-actoren in het privacybeleid beschreven. Hierbij zijn tevens de onderlinge relaties tussen de verschillende verantwoordelijken inzichtelijk gemaakt. Het ontbreekt echter enkel aan de functie van de SG. Ook al heeft de SG in de uitvoering inzake privacy wellicht een minder nadrukkelijke rol, vanuit wetgeving is de SG wel een belangrijk persoon met verantwoordelijkheid.

Bewustwording
EZK/LNV beschikt over een in opzet beschreven bewustwordings- en opleidingsbeleid dat zich richt op integrale veiligheid, integriteit, informatiebeveiliging en privacy om een veilige, betrouwbare en risicobewuste cultuur en voldoende vaardigheden te creëren ofwel te handhaven. Door de ADR zijn meerdere documenten ontvangen waaruit blijkt dat EZK/LNV zowel centraal als decentraal invulling geeft aan bewustwordingsacties en trainingen betreffende privacy en informatiebeveiliging. Decentrale bewustwordingsacties worden gedeeld op het AYA-platform zodat andere dienstonderdelen hier ook gebruik van kunnen maken.

Inrichting verantwoordingsstructuur
EZK/LNV heeft in opzet in het privacybeleid een structuur beschreven waarmee periodiek de stand van zaken van het privacymanagement en daarmee de verantwoordingstructuur gemonitord wordt. Door het kerndepartement en organisatieonderdelen worden tweejaarlijks self-assessments uitgevoerd op de implementatie van wet- en regelgeving en interne beleidskaders. In de uitvraag wordt gebruik gemaakt van privacy kritieke prestatie-indicatoren (KPI's) die zijn gebaseerd op de rijksbrede Handreiking naleving AVG waaronder o.a. DPIA's, datalekken, register van verwerkingsactiviteiten en rechten van betrokkenen. Afgesloten verwerkersovereenkomsten zou een aanvullend onderwerp kunnen zijn (zie onderdeel 2). Als er tekortkomingen zijn bij de implementatie wordt dit gemeld in de rapportage, tezamen met een plan met verbeteracties of geaccepteerde risico's.

Door de Auditdienst Rijk (ADR) is vastgesteld dat EZK/LNV in bestaan aan deze structuur invulling geeft middels de ontvangen rapportages van het kerndepartement en de dienstonderdelen Nederlandse Voedsel- en Waren Autoriteit (NVWA) en de Rijksdienst voor Ondernemend Nederland (RVO). Op basis van de ingevulde self-assessments is het Beeld Integrale Beveiliging en Privacy opgesteld dat door de Chief Information Officer (CIO)/pSG met de Bestuursraad EZK en LNV wordt gedeeld. De ADR heeft op basis van deze structuur vastgesteld dat EZK/LNV in opzet en bestaan beschikt over een PDCA-cyclus inzake privacymanagement en de inrichting van de verantwoordingsstructuur.

Three Lines Model
EZK/LNV heeft in opzet in het privacybeleid beschreven op welke manier invulling wordt gegeven aan het Three Lines (of Defense) Model, ondersteunt door een grafische vormgeving. Zowel de actoren binnen iedere lijn alsmede de taken, verantwoordelijkheden en bevoegdheden (al dan niet doorverwezen naar een andere paragraaf) zijn beschreven. Hierbij is tevens aandacht voor de positie van de Functionaris Gegevensbescherming (FG).

Aanbevelingen
Op basis van deze bevindingen doet de ADR de volgende aanbevelingen:
- Beschrijf de taken, verantwoordelijkheden en bevoegdheden van de SG in het privacybeleid.
- Maak het afsluiten en periodiek beoordelen van de afgesloten verwerkersovereenkomsten expliciet onderdeel van de self-assessment (zie onderdeel 2).

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 van EZK. Deze verwerkingen vinden plaats bij DG Klimaat & Energie en de RVO;

DG Klimaat & Energie
1. M8957 – Evaluatie AMVB experimenten

2. M9333 – Onderzoek risicoperceptie

RVO
3. M2877 – Registreren Antibioticagebruik Varkens
4. M2654 – Registreren gegevens Preventie Salmonella bij Pluimvee

Procedure opstellen verwerkersovereenkomsten
DG Klimaat & Energie
Door de ADR is vastgesteld dat DG Klimaat & Energie in opzet beschikt over een Quick Reference Card (QRC) waarin o.a. aandacht besteed wordt aan verwerkersovereenkomsten. De QRC bevat een korte beschrijving van het proces, rollen en verantwoordelijkheden en veel gestelde vragen. Het proces inzake het opstellen van verwerkersovereenkomsten is hiermee niet in een formeel document in opzet beschreven, maar de QRC kan in de basis voldoende handvatten bieden omdat tevens wordt verwezen naar het rijksbrede model en verdere contactpersonen. Aangegeven is dat de QRC in de praktijk goed werkt om verwerkersovereenkomsten op te stellen.

RVO
Door de ADR is vastgesteld dat RVO beschikt over meerdere documenten die in opzet het proces rondom het opstellen van verwerkersovereenkomsten beschrijven. De taken, bevoegdheden en verantwoordelijkheden zijn in opzet beschreven en middels aanvullende stukken, waaronder een intakeformulier en invulinstructie voor het rijksbrede model, worden handvatten geboden om invulling te geven aan dit proces.

Risicoanalyse / DPIA
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 en de bescherming van de betrokkenen is gewaarborgd.

DG Klimaat & Energie
Uit de ontvangen informatie van DG Klimaat & Energie (de QRC) komt niet in opzet naar voren op welke manier DG Klimaat & Energie borgt dat er alleen verwerkers ingeschakeld worden die voldoende garanties bieden dat zij aan de wettelijke vereisten van gegevensbescherming voldoen. Aangegeven is dat in de basis altijd een bedrijf wordt aangeschreven waarmee al een mantelovereenkomst afgesloten is. Aangegeven is dat de afdeling Inkoop een check uitvoert of de verwerker of organisatie voldoet aan de eisen die gesteld worden. Indien de verwerking als hoog risico wordt geclassificeerd, voert het team Informatiebeveiliging & Privacy (IB&P) een risicoanalyse uit met betrekking tot privacy en informatiebeveiliging.

RVO
Uit de ontvangen informatie van RVO komt niet in opzet naar voren op welke manier RVO borgt dat er alleen verwerkers ingeschakeld worden die voldoende garanties bieden dat zij aan de wettelijke vereisten van gegevensbescherming voldoen. Aangegeven is dat het inkoopproces zo is ingericht dat bij de inkoop van diensten of systemen waarbij persoonsgegevens worden verwerkt, standaard een Quickscan Informatiebeveiliging en DPIA wordt overwogen. Gesprekken met Informatiemanagement en het Inkoop en Uitvoeringscentrum (IUC) zijn gaande om informatiebeveiliging en privacy verder in de inkoopprocessen te borgen. Aangegeven is dat deze toets plaatsvindt indien nodig, en dat dit nog niet volgens een gestructureerd proces verloopt. IB&P-collega's worden betrokken bij het proces betreffende het opstellen van een verwerkersovereenkomst. Er worden eisen op hoofdlijnen gesteld aan de leveranciers maar dat is maatwerk. Er kan bijvoorbeeld naar certificeringen worden gevraagd.

Verwerkersovereenkomsten
DG Klimaat & Energie
Door de ADR is er vooraf een steekproef genomen uit het register van verwerkingsactiviteiten. Hierbij zijn voor DG Klimaat & Energie verwerkingen M8957 en M9333 geselecteerd. Uit de steekproef komt naar voren dat bij beide verwerkingen met beide verwerkers een verwerkersovereenkomst is opgesteld conform het rijksbrede format. De verwerkersovereenkomsten bevatten de vereiste gegevens vanuit de AVG.

RVO
Door de ADR is er vooraf een steekproef genomen uit het register van verwerkingsactiviteiten. Hierbij zijn voor RVO verwerkingen M2877 en M2654 geselecteerd. Uit de steekproef komt naar voren dat bij beide verwerkingen met de verwerkers een verwerkersovereenkomst is opgesteld conform een inmiddels verouderd rijksbreed format. De verwerkersovereenkomsten verwijzen naar de Wet bescherming persoonsgegevens (Wbp) waardoor niet alle vereiste onderwerpen vanuit de AVG terugkomen in de overeenkomsten.

RVO erkent deze situatie en geeft aan dat zowel voor M2654 als voor M2877 het voornemen aanwezig is, om deze verwerkingen en afgesloten verwerkersovereenkomsten te actualiseren.

Controle en monitoring verwerkersovereenkomsten/-afspraken
DG Klimaat & Energie
Uit de ontvangen documentatie van DG Klimaat & Energie is niet in opzet een proces beschreven dat bij gewijzigde omstandigheden verwerkersovereenkomsten/-afspraken worden beoordeeld of aangepast dan wel dat dit proces in bestaande processen voor contractmanagement is verankerd.

Aangegeven door DG Klimaat & Energie is dat er wel een proces is ingericht voor het jaarlijks controleren en monitoren van verwerkersovereenkomsten (lang lopende contracten). De controle en monitoring van verwerkersovereenkomsten is niet in bestaan vastgesteld omdat dit vanwege tijd- en capaciteitsgebrek nog niet in de praktijk plaats vindt. Deze controle en monitoring kan zich lenen als onderdeel van de periodieke self-assessment.

RVO
Uit de ontvangen documentatie van RVO komt niet in opzet een proces naar voren dat erop toeziet dat bij gewijzigde omstandigheden verwerkersovereenkomsten/-afspraken worden beoordeeld of aangepast dan wel dat dit proces in de bestaande processen voor contractmanagement is verankerd.

Aangegeven is dat RVO voornemens is om één keer per jaar een kleine controle en één keer per drie jaar een grote controle in te richten. Verwerkersovereenkomsten maken onderdeel uit van de integrale uitvraag. Deze uitvraag beslaat echter enkel de vraag of er een verwerkersovereenkomst is afgesloten. Er vindt geen inhoudelijk controle plaats op de kwaliteit van de verwerkersovereenkomst evenals de actualiteit van de verwerkersovereenkomst. Controle en monitoring op de gemaakte verwerkersovereenkomsten kan zich lenen als onderdeel van de periodieke self-assessment.

Toezicht en controle op naleving van de afspraken met verwerkers
DG Klimaat & Energie
Uit de ontvangen documentatie van DG Klimaat & Energie komt niet in opzet een beschreven proces naar voren dat periodiek toeziet op de naleving van de gemaakte afspraken met verwerkers. Aangegeven is dat er momenteel binnen EZK/LNV zowel centraal als decentraal nog geen proces is ingericht om de verwerkers periodiek te laten rapporteren over de verplichtingen voortkomend uit de verwerkersovereenkomsten én het beoordelen van deze rapportages. Dit onderdeel is wel onderwerp van de periodieke self-assessment. Aangegeven is dat het voorkomt dat verwerkers bijvoorbeeld een melding doen van een datalek.

RVO
Uit de ontvangen documentatie van RVO komt niet in opzet een beschreven proces naar voren dat periodiek toeziet op de naleving van de gemaakte afspraken met verwerkers. Aangegeven is dat er momenteel binnen EZK/LNV zowel centraal als decentraal nog geen proces is ingericht om de verwerkers periodiek te laten rapporteren over de verplichtingen voortkomend uit de verwerkersovereenkomsten én het beoordelen van deze rapportages. Dit onderdeel is wel onderwerp van de periodieke self-assessment. Aangegeven is dat het voorkomt dat verwerkers bijvoorbeeld een melding doen van een datalek.

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

- DG Klimaat & Energie en RVO; voer een check uit op de verwerkers of zij aan de wettelijke vereisten voor gegevensbescherming kunnen voldoen als onderdeel van het proces betreffende het opstellen van verwerkersovereenkomsten.
- RVO; actualiseer de verwerkersovereenkomsten uit het Wbp-tijdperk om zo de onderwerpen uit de AVG in de overeenkomsten te dekken.
- DG Klimaat & Energie en RVO; veranker het (her)beoordelen van de afgesloten verwerkersovereenkomsten naar aanleiding van signalen of malversaties in de bestaande processen van contractmanagement.
- DG Klimaat & Energie en RVO; beschrijf in opzet en voer in bestaan een proces uit waarmee de (risicovolle) verwerkers periodiek getoetst worden op de naleving van de eisen van de AVG en de afspraken uit de verwerkersovereenkomst. Laat de verwerker (van risicovolle verwerkingen) bijvoorbeeld periodiek rapportages opstellen die vervolgens beoordeeld kunnen worden.

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
EZK en LNV beschikken over een in opzet beschreven cloudbeleid. Binnen EZK/LNV is er sprake van decentrale verantwoordelijkheid. Dienstonderdelen mogen zelf bepalen wat zij doen wat betreft cloud zolang het binnen het departementale kader valt. Middels het cloudbeleid worden de dienstonderdelen begeleid op de weg naar het meer inzetten van public cloud door middel van kaders op het gebied van privacy en informatiebeveiliging en een in opzet beschreven gedetailleerd besluitvormingsproces (inclusief instructies) omtrent public cloud.

Clouddiensten binnen EZK/LNV
Door de ADR is vastgesteld is dat er nog geen register in opzet en bestaan aanwezig is met alle clouddiensten die in gebruik zijn bij EZK/LNV. Aangegeven is dat een algemeen register wel gewenst is. Het nieuwe rijksbrede cloudkader zou als trigger kunnen dienen om een register te bewerkstelligen. Wel heeft er een inventarisatie plaatsgevonden van web-based SaaS-oplossingen, heeft de Chief Information Security Officer (CISO) periodiek overleg met Dienst ICT Uitvoering (DICTU) over de lopende cloud projecten en wordt de CISO in algemene zin op de hoogte gehouden over concernbrede cloud trajecten met een hoog risico. Binnen EZK/LNV ligt de voornaamste uitdaging bij de kleine systemen/shadow IT waar minder zicht op is.

Risicoanalyse cloudtoepassingen | MS Teams
Als onderdeel van het afwegingsproces is in opzet beschreven dat vooraf een risicoanalyse gemaakt dient te worden. Hierbij worden de minimale beveiligingseisen, de te onderzoeken risico's, het opnemen van de verwerking in het AVG-register en het uitvoeren van een DPIA - wanneer noodzakelijk - meegenomen. Deze stappen worden ondersteund en nader toegelicht in de bijlages van het cloudbeleid. Als wet- en regelgeving zijn ook expliciet genoemd Baseline Informatiebeveiliging Overheid (BIO), ISO27001, AVG, cloud- en freedom act. De CISO wordt op de hoogte gesteld van nieuwe cloudtoepassingen met een hoog risico. De uitdaging blijft zoals eerder vermeld bij de kleine systemen/shadow IT.

Als casus is door de ADR vooraf MS Teams geselecteerd. De risicoanalyses en besluiten rondom MS Teams hebben plaatsgevonden voor de start van de Waiver Advisory Board (WAB). Door de ADR is geconstateerd dat voor MS Teams de risico's besproken en afgewogen zijn door de CISO, pSG, FG en directeur bedrijfsvoering.

Beveiligingsaspecten en stadia
EZK/LNV heeft in opzet voor opslag, de verwerking en het transport van data beschikbaarheids-, integriteits- en vertrouwelijkheidsmaatregelen beschreven door 27 maatregelen te implementeren die de BIV-aspecten raken. Deze maatregelen komen middels een risicoanalyse tot stand. Er is een (WAB) dat adviseert over de manier waarop deze maatregelen geïmplementeerd kunnen worden. De ADR heeft documentatie ontvangen van de besluitvorming rondom de casus MS Teams waaruit blijkt hoe de maatregelen in de praktijk gestalte hebben gekregen.

Classificatie
EZK/LNV heeft in opzet beschreven hoe zij classificatie toekennen aan data en middelen waarin/waarop zich data bevindt, gebaseerd op datatype, waarde, gevoeligheid en kritisch gehalte voor de organisatie.

Eigenaarschap
Het eigenaarschap van de middelen die deel uitmaken van de clouddiensten is in opzet beschreven in het cloudbeleid. Bij het beëindigen van een contract wordt er uitgegaan van de exit-strategie. Directie bedrijfsvoering is hierbij als eigenaar van de data in de lead. Voor MS Teams wordt momenteel verder verkend welke aanvullende scenario's mogelijk zijn en hoe een eventuele exit vorm zou moeten krijgen. In de basis is er in opzet een exitstrategie beschreven.

Locatie
In het cloudbeleid is in opzet beschreven welke uitgangspunten EZK/LNV hanteert ten aanzien van de locatie van de opslag van data. Door de ADR is vastgesteld dat de Cloud Service Provider tevens specificeert en documenteert in welk land de data is opgeslagen.

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

- Realiseer het voornemen om de cloudtoepassingen binnen EZK/LNV verder in kaart te brengen en expliciet vast te leggen in een centraal register.

Managementreactie ministerie van Economische Zaken en Klimaat

De inzichten en aanbevelingen uit dit rapport van bevindingen helpen EZK bij een verdere implementatie van de AVG. De ADR schrijft dat verdere inbedding van privacymanagement voor de onderzochte overheidsinstanties nog een uitdaging is. Voor EZK is het voldoen aan privacywetgeving geen statisch gegeven, maar een continu proces. Privacybescherming is onderhevig aan nieuwe jurisprudentie, uitspraken van toezichthouders en technologische ontwikkelingen. Aan EZK de taak om hier voortdurend op te sturen zodat persoonsgegevens van burgers en medewerkers worden beschermd en rechtmatig verwerkt. De aanbevelingen van de ADR worden meegenomen in de jaarplannen van de betreffende organisatieonderdelen waarin afhankelijk van risico's en capaciteit een prioritering wordt aangebracht. Een aantal aanbevelingen wordt concernbreed opgepakt, zoals de aanbeveling rondom verwerkers die valt binnen het bredere thema leveranciersmanagement.

Onderzoeksverantwoording

Hieronder is de onderzoeksverantwoording weergegeven van het rijksbrede AVG onderzoek dat in juli 2022 met als peildatum 01-07-2022 heeft plaatsgevonden bij het ministerie van Economische Zaken en Klimaat.

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 xxx 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 xxx, 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 Economische Zaken en Klimaat waren dit DG Klimaat & Energie en RVO.

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, 01 december 2022