Auditdienst Rijk
Ministerie van Financiën

Deelrapport uitgebracht aan
CIO ministerie van Landbouw, Natuur en Voedselkwaliteit

Datum
01-12-2022

Auditdienst Rijk
Korte Voorhout 7
2511 CW Den Haag

Kenmerk
2022-0000289824

Rijksbreed AVG 2022
Deelrapport van bevindingen ministerie van Landbouw, Natuur en Voedselkwaliteit

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 Landbouw, Natuur en Voedselkwaliteit 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
Landbouw, Natuur en Voedselkwaliteit (LNV) beschikt samen met Economische Zaken en Klimaat (EZK) 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/LNV 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 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 zijn 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 vanuit 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 betreffende 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 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 in de implementatie wordt dit gemeld in de rapportage, tezamen met een plan met verbeteracties of geaccepteerde risico's.

Door de ADR is vastgesteld dat EZK/LNV in bestaan aan deze structuur invulling geeft middels de ontvangen rapportages van het kerndepartement en dienstonderdelen NVWA en RVO. Op basis van de ingevulde self-assessments is het Beeld Integrale Beveiliging en Privacy opgesteld dat door de CIO met de (p)SG 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 almede 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 periodieke 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 drie verwerkingen uit het register van verwerkingsactiviteiten van LNV. Deze verwerkingen vinden plaats bij de Nederlandse Voedsel- en Warenautoriteit (NVWA);
1. M12 – Onderzoek naar de hygiënebeleving bij tattooshophouders en consumenten
2. M36 – Bestuurlijke maatregelen
3. M243 – Verificatie inspectie (EU GLB)

Procedure opstellen verwerkersovereenkomsten
NVWA
Door de ADR is vastgesteld dat de NVWA niet over een in opzet beschreven proces beschikt voor wat betreft het opstellen van verwerkersovereenkomsten. Dit geldt tevens voor de taken, bevoegdheden en verantwoordelijkheden van de actoren inzake dit proces.

Aangegeven door de NVWA is dat er in de praktijk wel sprake is van een specifiek proces via de reguliere inkoopprocedure waarbij de eenheid privacy betrokken raakt. Aangegeven is dat afdeling inkoop bijna altijd aangeeft dat een verwerkersovereenkomst nodig is terwijl dit niet altijd het geval is. Door het geringe aantal collega's dat er mee bezig is was het in opzet beschrijven van dit proces voorheen niet opportuun. NVWA heeft het voornemen om het proces te documenteren inclusief een stroomschema.

Garanties door verwerkers / risicoanalyses (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 Algemene Verordening Gegevensbescherming voldoet en de bescherming van de betrokkenen is gewaarborgd.

NVWA
Uit de ontvangen informatie van NVWA komt niet in opzet naar voren op welke manier NVWA vooraf borgt dat er alleen verwerkers ingeschakeld worden die voldoende garanties bieden dat zij aan de wettelijke vereisten voor gegevensbescherming voldoen. NVWA is voornemens om een aanvullende handreiking hiervoor op te stellen alsmede capaciteit vrij te maken om auditors de voorgenomen verwerkers te laten auditen.

De NVWA heeft in opzet beschreven dat een DPIA uitgevoerd moet worden wanneer noodzakelijk. Wanneer het precies noodzakelijk is en wat met de uitkomsten gedaan moet worden valt echter niet op te maken uit de ontvangen documentatie. Bij de geselecteerde verwerkingen staat in het register van verwerkingsactiviteiten aangegeven dat het uitvoeren van een DPIA niet noodzakelijk is. Bij verwerking M36 staat echter aangegeven dat er strafrechtelijke – en daarmee bijzondere – persoonsgegevens verwerkt worden. Een mogelijke indicatie dat een DPIA noodzakelijk is. Onderbouwing waarom er geen DPIA is uitgevoerd ontbreekt.

Register van verwerkingsactiviteiten
NVWA
Aangegeven door de NVWA is dat wanneer een verwerkingsovereenkomst is afgesloten, deze niet wordt toegevoegd aan het register van verwerkingsactiviteiten. Niet iedere relevante collega heeft toegang tot het register van verwerkingsactiviteiten. In plaats hiervan houdt de NVWA zelf een door de ADR in bestaan vastgestelde mappenstructuur bij. NVWA geeft aan hierin alle afgesloten verwerkersovereenkomsten bij te houden die breder toegankelijk is voor andere collega's. Aangegeven is dat de NVWA voornemens is om in de 'database'/mappenstructuur een koppeling te maken naar het register.

Het register van verwerkingsactiviteiten geeft daarmee momenteel geen volledig en juist beeld van de verwerkingen die plaatsvinden binnen de NVWA. Aangegeven is dat er ook meerdere projecten spelen die al dan niet reeds zijn afgelopen. Deze verwerkingen dienen uit het register verwijderd te worden. Aangegeven is dat voor projecten categorieën aangebracht worden waar steeds de projectplannen bijgevoegd zullen worden zodat een verwerking niet steeds moet worden ingetrokken. Dit om de beheerlast te verminderen.

Verwerkersovereenkomsten
NVWA
Door de ADR is vastgesteld dat de NVWA beschikt over een in opzet beschreven rijksbreed format (ARVODI-model) voor het afsluiten van verwerkersovereenkomsten.

Uit de steekproef van de ADR komt naar voren dat verwerking M12 een verouderde verwerking betreft die verwijderd dient te worden uit het register van verwerkingsactivteiten. Aangegeven door de NVWA is dat in het verleden er geen expliciete verwerkingsovereenkomst, maar een raamovereenkomst afgesloten met de verwerker. Verwerkers uit verwerkingen M36 en M243 betreffen overheidsorganisaties. Door de ADR is vastgesteld dat met de overheidsorganisatie uit verwerking M36 geen verwerkersafspraken zijn gemaakt. Met de overheidsorganisatie van verwerking M243 heeft de NVWA wel in opzet en bestaan verwerkersafspraken gemaakt.

Gezien bij de oorspronkelijke steekproef van de ADR het met name overheidsorganisaties betrof, heeft de ADR als aanvullende steekproef 2 extra verwerkersovereenkomsten opgevraagd. Door de ADR is vastgesteld dat beide verwerkersovereenkomsten conform rijksbreed format zijn opgesteld en tweezijdig ondertekend.

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

Aangegeven door de NVWA is dat jaarlijks handmatig wordt gekeken wat er dient te gebeuren met een bepaalde verwerking (welke persoonsgegevens, doel, heeft het te maken met toezicht/opsporing i.h.k.v. Wpg, escalatieladder, looptijd, etc.). De NVWA is voornemens om hier een stoplichtsysteem aan toe te voegen om de doorlooptijd te kunnen monitoren.

Toezicht en controle op naleving van de afspraken met verwerkers
NVWA
Uit de ontvangen documentatie van de NVWA komt niet in opzet een 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.

Gezamenlijke verwerkingsverantwoordelijke
Aangegeven is dat de NVWA nog niet volledig inzichtelijk heeft of er verwerkingen zijn met gezamenlijke verantwoordelijkheid. De NVWA is wel bezig om dit inzichtelijk te krijgen.

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

- NVWA: realiseer het voornemen om het proces betreft het opstellen van verwerkersovereenkomsten in opzet te documenteren inclusief stroomschema. Besteed hierbij tevens aandacht aan de taken, bevoegdheden en verantwoordelijkheden van de actoren inzake dit proces.
- NVWA: realiseer het voornemen om in opzet een handreiking op te stellen om de voorgenomen verwerkers te beoordelen of zij aan de wettelijke vereisten voor gegevensbescherming kunnen voldoen. Besteed hierbij tevens aandacht voor de eigen DPIA-procedure om duidelijk te krijgen welke privacyrisico's er kunnen spelen bij een verwerking.
- NVWA: coordineer en draag zorg dat het register van verwerkingsactiviteiten – als één van de belangrijkere verantwoordingsmiddelen – een actueel, volledig en juiste weergave geeft van de verwerkingen binnen de NVWA. Breid zo nodig de toegang tot het register verder uit om dit te kunnen bewerkstelligen.
- NVWA: maak verwerkersafspraken met de overheidsorganisatie uit verwerking M36.
- NVWA; veranker het (her)beoordelen van de afgesloten verwerkersovereenkomsten naar aanleiding van signalen of malversaties in de bestaande processen van contractmanagement.
- NVWA; beschrijf in opzet en voer in bestaan een proces uit waarmee de NVWA haar verwerkers periodiek toetst op de naleving van de eisen van de AVG en de afspraken uit de verwerkersovereenkomst. Laat de verwerker bijvoorbeeld periodiek rapportages opstellen die vervolgens beoordeeld kunnen worden. Zoek hierbij de samenwerking EZK/LNV-breed.

- NVWA: continueer het voornemen om inzichtelijk te maken of er verwerkingen zijn met een gezamenlijke verantwoordelijkheid.

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 en-strategie
EZK en LNV beschikken over een in opzet beschreven cloudbeleid. Binnen EZK/LNV is er sprake van decentrale verantwoordelijkheid. Dienstonderdelen mogen zelf mag bepalen wat zij doen 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 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 er 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 kritische 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 Landbouw, Natuur en Voedselkwaliteit
De inzichten en aanbevelingen uit dit rapport van bevindingen helpen LNV bij een verdere implementatie van de AVG. De ADR schrijft dat verdere inbedding van privacymanagement voor de onderzochte overheidsinstanties nog een uitdaging is. Voor LNV 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 LNV 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 Landbouw, Natuur en Voedselkwaliteit.

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 [redacted] 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 [redacted], 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 Landbouw, Natuur en Voedselkwaliteit was dit NVWA.

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

Projectleider | Auditdienst Rijk