Auditdienst Rijk
Ministerie van Financiën

Deelrapport uitgebracht aan
CIO ministerie van Defensie

Datum
11-10-2022

Auditdienst Rijk
Korte Voorhout 7
2511 CW Den Haag

Rijksbreed AVG 2022
Definitief deelrapport Ministerie Defensie

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 Defensie 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
Op het gebied van beleidsstukken omtrent privacy geeft Defensie aan zo veel als mogelijk gebruik te maken van de rijksbrede handreiking naleving AVG. Defensie beschikt mede daardoor niet over een eigen expliciet privacybeleid. Wel heeft Defensie de Regeling AVG Defensie opgesteld met daarin geformuleerde uitgangspunten, wordt gebruik gemaakt van het rijksbrede AVG verwerkingenregister en is voor het uitoefenen van rechten betrokkenen een uitgebreide internet/intranetsite. De regeling is vastgesteld door de Staatssecretaris van Defensie op 15 mei 2018 en geeft de SG de bevoegdheid de regeling nader in te vullen. De Regeling is sinds mei 2018 niet herzien of opnieuw vastgesteld. Niet alle onderwerpen die de Autoriteit Persoonsgegevens (AP) adviseert betreft een privacybeleid, komen terug in de Regeling AVG Defensie, waaronder AVG-principes zoals dataminimalisatie, doelbinding en juistheid van gegevens. Momenteel zijn uitgangspunten omtrent privacy aanwezig in verschillende Defensie-specifieke documenten dan wel rijksbrede documenten. De AP adviseert echter één centraal document. Voor de communicatie intern en extern heeft Defensie privacyverklaringen opgesteld en is er op het intranet een privacypagina waarop wordt verwezen naar rijksbrede stukken alsmede de Regeling AVG Defensie.

Taken, bevoegdheden en verantwoordelijkheden
Algemene taken, bevoegdheden en verantwoordelijkheden staan in de rijksbrede handreiking AVG omschreven. Dit is op een abstract niveau en ontbreekt het aan een nadere Defensie-uitwerking. De voornaamste rollen binnen Defensie zijn wel uitgewerkt in de Regeling AVG Defensie.

Bewustwording
De ADR heeft van Defensie meerdere documenten ontvangen waaronder nieuwsbrieven en documentatie over awareness-sessies waaruit blijkt dat Defensie invulling geeft aan bewustwording van nieuw en bestaand personeel op het gebied van privacy en gegevensbescherming. Daarnaast beschikt de privacy-landingspagina binnen het intranet over een tegel voorlichtingsmateriaal en wordt Defensie-breed jaarlijks de week Veiligheid & Privacy gehouden.

Inrichting verantwoordingsstructuur
In de Regeling AVG Defensie is vastgelegd dat de AVG-beheerder jaarlijks vóór 1 januari aan de FG rapporteert over de naleving van de AVG en de wet binnen zijn onderdeel. Het rapport gaat onder andere in op DPIA's, het register van verwerkingsactiviteiten, verwerkersovereenkomsten, rechten van betrokkenen en verbeteracties. Het jaarrapport zou uitgebreid kunnen worden met uitgevoerde bewustwordingsactiviteiten en trainingen. De ADR heeft voorbeelden van jaarrapporten ontvangen betreft Defensie-brede verwerkingen en DOSCO. De manier waarop Defensie dit vormgeeft kan worden beschouwd als best practice.

Naast het jaarlijkse rapport aan de FG, is privacy tevens onderdeel van het proces rondom de reguliere managementrapportage (Aanschrijving Business Control Defensie (ABCDEF)). De commandanten dienen 1/2 pagina's A4 te wijden aan privacy en daarbij een aantal vragen te beantwoorden en de voortgang te beschrijven omtrent een aantal punten.

Three Lines Model
De uitgangspunten en de onderlinge verhouding (1e lijn, 2e en 3e lijn) van de taken/verantwoordelijkheden van het Three Lines Model zijn niet expliciet in opzet gedocumenteerd. Wel is mondeling toelichting gegeven op de praktische uitvoering hiervan.

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

- Overweeg het opstellen van een privacybeleid op basis van de bestaande Regeling AVG Defensie en breid het uit met een explicietere koppeling naar de Defensie-praktijk betreft de taken, bevoegdheden en verantwoordelijkheden, een nadere uitwerking van AVG-principes en het vormgeven van de aantoonplicht. Op deze manier ontstaat er één centraal beleidsstuk zoals AP adviseert.
- Maak als 'nice to have' bewustwording/training onderdeel van het jaarrapport opgesteld door de AVG-coördinatoren om een nog breder en completer beeld te krijgen.
- Documenteer en expliciteer de invulling van het Three Lines Model bijvoorbeeld in de Regeling AVG Defensie of een privacybeleid.

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 Defensie. Deze verwerkingen vinden plaats bij Defensie-brede verwerkingen en DOSCO:

- M1129 Onderzoek naar het welzijn en eventuele (na)zorgbehoeften ISAF-veteranen (defensie-brede verwerking)
- M2283 Militaire geestelijke gezondheid (Defensie-brede verwerking)
- M2309 Geïntegreerde eerstelijnsgezondheidszorg (DOSCO)
- M2341 Bewaking en beveiliging inclusief toegangscontrole en bezoekersregistratie (DOSCO)

Procedure opstellen verwerkersovereenkomsten
Het opstellen van een verwerkersovereenkomst komt terug in de Regeling AVG Defensie en is onderdeel van het reguliere inkoopproces. De taken, verantwoordelijkheden en bevoegdheden rondom het opstellen van de verwerkersovereenkomsten zijn daarmee ook specifiek belegd bij verwerving en inkoop. Wanneer een dienst wordt afgenomen waarbij sprake is van een verwerking van persoonsgegevens wordt verwacht dat de inkopers een verwerkersovereenkomst afsluiten. Aangegeven is dat dit omschreven staat in de functionele aanwijzingen voor inkoop. Tevens staat hierin aangegeven dat bij het afsluiten van een verwerkersovereenkomst in beginsel de rijksbrede formats gehanteerd dienen worden tenzij het niet anders kan.

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. In het programma van eisen behorend bij een aanbesteding of bij het 'inkoopcontract privacy' dient met deze verantwoordelijkheid rekening te worden gehouden. De garantie van de verwerker komt onder andere tot uiting in artikel 14.1 van de Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten (ARVODI-2018). Wanneer er bijzondere informatie wordt verwerkt, wordt de Algemene Beveiligingseisen Defensieopdrachten (ABDO) bedongen. Wanneer ABDO wordt bedongen, voert de MIVD een onderzoek uit of de dienstverlener aan de normen van de ABDO kan voldoen.

Risicoanalyse / DPIA
Uit het onderzoek van de ADR komt naar voren dat wanneer er een DPIA uitgevoerd dient te worden dit ook conform rijksbreed format gedaan is. Uit de DPIA's komen de privacyrisco's naar voren alsmede maatregelen op technisch en organisatorisch gebied. Ook is advies ingewonnen bij de Functionaris van Gegevensbescherming. Daarnaast is geconstateerd dat de ABDO is bedongen wanneer noodzakelijk.

Verwerkersovereenkomsten
Vooraf is door de ADR een selectie gemaakt van vier verwerkingen uit het register van verwerkingsactiviteiten. Deze verwerkingen vinden plaats bij Defensie-brede verwerkingen en DOSCO. Met alle verwerkers uit de geselecteerde verwerkingen is een verwerkersovereenkomst afgesloten die tweezijdig is ondertekend. Geconstateerd is dat niet altijd het rijksbrede format is gehanteerd. Het komt voor dat het model van brancheorganisaties zorg als uitgangspunt is genomen bij het opstellen van de overeenkomst. Desondanks omvatten de verwerkersovereenkomsten wel alle benodigde gegevens zoals de AVG dat stelt.

Controle en monitoring verwerkersovereenkomsten/-afspraken
De monitoring op de verwerkersovereenkomsten is ingebed in de reguliere inkoopprocedure. Alle verwerkersovereenkomsten dienen door de verwerver/inkoper te worden opgevoerd in SAP waarin een monitoringsmodule zit. Hierin kan worden gezien welke overeenkomsten binnenkort verlopen. Voor de controle en monitoring van verwerkersovereenkomsten is dus geen apart expliciet proces ingericht, maar zit geborgd in het reguliere inkoopproces. De ADR heeft dit echter enkel aangetroffen voor de Defensie-brede verwerkingen. Uit de jaarrapporten blijkt dat nog niet voor alle onderdelen binnen Defensie een goed overzicht aanwezig is van verwerkersovereenkomsten die nog afgesloten of geactualiseerd dienen te worden.

Toezicht en controle op naleving van de afspraken met verwerkers
Geconstateerd is dat er nog geen expliciet systeem is ingericht dat erop toeziet dat de ontvangen rapportages van de verwerkers worden beoordeeld en indien noodzakelijk mitigerende maatregelen getroffen worden die de naleving van de AVG borgen. Wel wordt Defensie op de hoogte gebracht van datalekken bij een verwerker wanneer deze hebben plaatsgevonden en verplicht het ABDO de verwerker indien er iets wijzigt in de beveiliging dit te melden aan Defensie.

Aangegeven is dat Defensie voornemens is om een proces in te richten waarbij de verwerkers dienen te rapporteren over een aantal normen uit de ISO/NEN waaraan privacy performance indicatoren zijn gekoppeld. Dit geldt vooral voor de grote/kritische verwerkingen. Hierover dient vervolgens periodiek te worden overlegd.

Aanbevelingen
Op basis van deze bevindingen doet de ADR de volgende aanbevelingen:
- Draag zorg voor een concreet en expliciet overzicht van afgesloten verwerkersovereenkomsten (in de jaarrapporten aan de FG) om inzichtelijk te maken welke verwerkersovereenkomsten nog afgesloten en geactualiseerd dienen te worden.
- Realiseer het voornemen om een proces in te richten waarbij de verwerkers dienen te rapporteren over een aantal normen uit de ISO/NEN waaraan privacy performance indicatoren zijn gekoppeld én dat deze rapportages worden beoordeeld.

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.

Cloudstrategie Defensie
Gezien steeds meer bedrijven richting de cloud gaan, heeft Defensie een stapsgewijze en grafisch vormgegeven routekaart opgesteld waarin uitgebreid wordt ingegaan op hoe Defensie hiermee om wil gaan. De routekaart alsmede het bijgevoegde besluitvormingsraamwerk kan als best practice worden beschouwd. In de routekaart is er naast het Defensie Beveiligingsbeleid (DBB) tevens een koppeling gemaakt met vereisten voorkomend uit de AVG, waaronder het opstellen van een DPIA indien nodig. Het startpunt van de routekaart is het rubriceringsniveau. Indien er persoonsgegevens worden verwerkt, wordt er gekeken of er ge(pseudo-)anonimiseerd kan worden. Voor ABDO gecertificeerde bedrijven zijn er eisen toegevoegd aan het ABDO-beoordelingskader over het gebruik van de Cloud.

Binnen Defensie leunt de beveiliging van persoonsgegevens in relatie tot de cloud op het DBB. De beveiliging hiervan komt tot uiting in de verwerkersovereenkomsten en het programma van eisen. Hiermee worden de elementen uit de AVG die betrekking hebben op de beveiliging afgedekt.

In de afgelopen periode heeft een case by case benadering Defensie ervaring opgeleverd. Deze ervaring wordt binnenkort geplot in een cloud-instructie aanvullend op de routekaart. De instructie wordt vervolgens weer onderdeel van het DBB en de ABDO. In de aanvullende cloud-instructie zal privacy niet expliciet worden meegenomen. Rijksbreed wordt er ook gewerkt aan een cloudstrategie, maar Defensie is hiervan uitgesloten.

Clouddiensten binnen Defensie
Defensie beschikt nog niet over een expliciet centraal overzicht van alle clouddiensten die binnen het departement zijn afgenomen. Wel zijn er mondeling een aantal clouddiensten toegelicht en welke samen voor deze diensten zijn doorlopen.

Defensie EersteLijns Informatievoorziening GezondHeidszorg Toekomstbestendig (DELIGHT)
Het project DELIGHT maakt onderdeel uit van het vernieuwingsprogramma Smart Band-Aid waarin Defensie de informatievoorziening van zowel de reguliere als de operationele gezondheidszorg verbetert en voorbereidt op de toekomst. In de specificaties van de eisen is nadrukkelijk aandacht besteed aan beveiliging en privacy. Aangegeven is dat er gekeken is hoe er omgegaan dient te worden met (gevoelige) persoonsgegevens waarna is besloten om pseudonimisering toe te passen. Tevens is middels het besluitvormingsraamwerk besloten de gegevens in een private cloud te verwerken. Hierbij geldt dat de ABDO-eisen dwingend zijn. Dit betekent dat er geen contract wordt afgesloten wanneer niet aan deze eisen voldaan kan worden. De ABDO-eisen worden momenteel nader uitgewerkt in een apart kader voor cloudtoepassingen.

Eigenaarschap
Om juridische redenen kan Defensie geen eigenaar zijn van de data. Defensie spreekt meer van verantwoordelijkheid voor de data. In die zin zijn er een aantal afspraken. Defensie wil niet dat anderen toegang hebben tot de data van Defensie (via een private-cloud omgeving). Voor wat betreft de data zelf zijn daar prima afspraken over te maken. Aangegeven is dat het lastiger wordt met meta-data bij de grote partijen als Microsoft en Google.

Locatie
Defensie geeft de voorkeur aan, zoals beschreven in het ABDO, het opslaan van gegevens op Nederlands grondgebied. Als hiervan afgeweken wordt, wordt er gekeken naar de EER-landen, Zwitserland en het VK.

Regie op cloudtoepassingen
Defensie geeft aan dat in relatie tot de regie op cloudtoepassing teamwork van groot belang is. Dit komt ook terug in het besluitvormingsraamwerk waarin verschillende kennis en kunde bij elkaar zijn gebracht en onderdeel uitmaken van het raamwerk. Er zijn een aantal partijen die telkens terugkomen (verwerker inkopen, beleidsfunctionaris etc.). Aangegeven is dat het kan voorkomen dat bij kleine, minder gevoelige projecten het zicht op de radar iets minder is. Defensie geeft aan dat binnen de organisatie bekend is dat wanneer men iets wil in de cloud met grote hoeveelheden gegevens, de beheerders weten dat je het niet zomaar kan doorgeven en

verstrekken. Aangegeven is dat dit zowel in de techniek als in de mensen zit verankerd.

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

- Stel een centraal overzicht op met de afgenomen clouddiensten waarbij ook aandacht is voor de kleine, minder gevoelige projecten.
- Continueer het voornemen om de ABDO-eisen nader uit te werken in een apart kader voor cloudtoepassingen.

Managementreactie CIO van Defensie

De beschrijving van de status van de verantwoordingsplicht specifiek bij de inzet van verwerkers is herkenbaar. Defensie constateert instemmend dat de ADR de wijze waarop Defensie rapporteert over de naleving van de AVG als een best practice heeft beoordeeld.

De ADR heeft drie aanbevelingen geformuleerd over de verantwoordingsverplichting en -structuur, twee aanbevelingen richten zich op verwerkersovereenkomsten en – afspraken. Deze aanbevelingen neemt Defensie over met de volgende aantekeningen:

- Privacybeleid: artikel 24 AVG definieert geen specifieke vorm en inhoud voor het gegevensbeschermingsbeleid. De AP hanteert in haar rapportage verkennend onderzoek gegevensbeschermingsbeleid (z2018-27134) drie verplichte onderdelen van het gegevensbeschermingsbeleid: een omschrijving van de (categorieën van) persoonsgegevens, een beschrijving van de doeleinden van de gegevensverwerking en de rechten van betrokkenen. Het is de vraag of de aanbeveling om ‘’alle informatie’’ in één document te vervatten bij Defensie voldoende effectief en efficiënt is. Dat komt door zowel het hoge aantal verwerkingen als door de grote verscheidenheid van processen die plaatsvinden bij Defensie en de gedetailleerde registratie-eisen die de AVG stelt. De omschrijving van de (categorieën van) persoonsgegevens en de doelstelling van de verwerking worden expliciet wel als onderdeel benoemd in het verwerkingenregister van de Rijksoverheid dat Defensie gebruikt. Voor de behandeling van rechten betrokkenen is een uitgebreide intra- en internetsite beschikbaar. Het uitwerken van het privacybeleid door DGB/DBE in aanvulling op het rijksbeleid wordt opgepakt op het moment dat de aanvullende (beleids-) capaciteit beschikbaar is en zal in een jaarplanning worden gecommuniceerd.
- Bewustwording, voorlichting en training maakt standaard onderdeel uit van de jaarlijkse rapportage die de Defensieonderdelen doen aan de FG.
- Verwervers/inkopers nemen verwerkersovereenkomsten en –afspraken op in het contractenregister Defensie (opzet). Tijdige en betrouwbare (volledige en juiste) registratie is hierbij een bekend aandachtspunt en key-control van de inkooporganisatie.

Daarnaast constateert Defensie met genoegen het oordeel best practice voor de Routekaart Cloud en het bijgevoegde besluitvormingsraamwerk. De ADR heeft over Cloud twee aanbevelingen geformuleerd. Deze aanbevelingen worden beide overgenomen met de volgende aantekening:

- Centraal overzicht afgenomen clouddiensten: het opstellen en bijhouden van een centraal overzicht geeft extra werklast. Door zorg van CIO wordt bezien of registratie mogelijk is in het configuratiemanagementsysteem van JIVC (JIVC Direct) en het uitwerken van het high level ontwerp van werkstromen.

Onderzoeksverantwoording

Hieronder is de onderzoeksverantwoording weergegeven van het rijksbrede AVG onderzoek dat in mei 2022 heeft plaatsgevonden bij het ministerie van Defensie.

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 xxxxxxxxxx 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 xxxxxxxxx, 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 Defensie waren dit Defensie-brede verwerkingen en DOSCO.

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.