Auditdienst Rijk
*Ministerie van Financiën*

# Onderzoeksrapport
# Rijksbreed AVG onderzoek 2022

definitief

# Colofon

| | |
|---|---|
| Titel | Rijksbreed AVG onderzoek 2022 |
| Uitgebracht aan | CIO-Rijk als voorzitter van het CIO-beraad, |
| Datum | 21 maart 2023 |
| Kenmerk | 2023-0000074126 |

*Inlichtingen*
**Auditdienst Rijk**
070-342 7700

# Inhoud

# Interdepartementale lering en samenwerking gewenst voor noodzakelijke verbetering AVG-beheersing binnen de Rijksoverheid

De doelstelling van dit onderzoek is om privacymanagement binnen de Rijkoverheid verder te versterken alsmede departementale best practices aan te dragen voor interdepartementale lering en samenwerking. Deze doelstelling is in de praktijk gebracht door inzicht te verkrijgen in:

- De inrichting van de privacygovernance bij de departementen voor de aantoonbare naleving van de AVG (aantoonplicht).
- De kwaliteit van de afspraken met verwerkers, alsmede de inrichting van de controle en monitoringsactiviteiten die toezien op de naleving van deze afspraken (verwerkersovereenkomsten).
- De gehanteerde privacycriteria in de departementale cloudstrategieën.

### Inrichting privacygovernance voor aantoonbaarheid naleving AVG

Wij hebben geconstateerd dat elk departement beschikt over een privacybeleid maar dat (het proces rondom) het actualiseren van het privacybeleid een belangrijk punt van aandacht is waar actie noodzakelijk is. Dit heeft tevens zijn uitwerking op de beschreven taken, bevoegdheden en verantwoordelijkheden. Bewustwordings-activiteiten vinden veelal (ad hoc) decentraal plaats waarbij ruimte is voor verdere (inter)departementale samenwerking. De PDCA-cyclus inzake privacymanagement voor de aantoonplicht is nog niet bij elk departement ingericht. Met name het Act-gedeelte (opvolging constateringen) is niet altijd beschreven waardoor de PDCA niet sluitend is. Dit geldt tevens voor het beschrijven van het Three Lines Model.

### Kwaliteit van de afspraken met verwerkers en controle hierop

Wij hebben geconstateerd dat bij de departementen veelal een beschreven proces voor het opstellen van verwerkersovereenkomsten niet aanwezig is. Garantie door verwerkers dat zij aan de wettelijke vereisten voor gegevensbescherming voldoen komt hoofdzakelijk terug in ARVODI-2018. Bijna alle verwerkersovereenkomsten zijn afgesloten conform het rijksbrede format. De ADR heeft wel wederom geconstateerd dat het register van verwerkingsactiviteiten nog steeds noodzakelijk verbeterd dient te worden betreft actualiteit en juistheid. Controle en monitoring op afgesloten verwerkersovereenkomsten en de controle en het toezicht op de naleving van de verwerkers op de gemaakte afspraken is ook voor verbetering vatbaar.

### Privacycriteria in departementale cloudstrategieën

Wij hebben geconstateerd dat de clouddiensten binnen het Rijk nog niet overal inzichtelijk zijn. Een cloudbeleid en/of een cloudstrategie is wel aanwezig bij ieder departement maar verdere uitwerking is nodig in afwachting op het rijksbrede cloudbeleid 2022. Wij hebben vastgesteld dat de uitvoering van een risicoanalyse van privacy met name in de uitvoering uitdagend is, zeker bij grote niet-Europese organisaties. Extra punten van aandacht zijn de classificatie van gegevens, het eigenaarschap in het kader van de exit-strategie en de locatie van gegevens. Dit laatste in het bijzonder wanneer data niet wordt opgeslagen binnen de EU.

Tijdens dit onderzoek hebben wij op nagenoeg elk onderwerp een best practice aangetroffen, hetzij centraal, hetzij decentraal binnen een departement. Wij dragen deze best practices aan ter noodzakelijke lering en verbetering en bovendien ter stimulering van interdepartementale samenwerking. Actie is noodzakelijk om tekortkomingen op te heffen om als Rijksoverheid aan de AVG te kunnen voldoen.

# 1 Inleiding onderzoek

## 1.1 Aanleiding

Het rijksbreed verkennend 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 negatieve publiciteit over de privacybescherming en het aantal grote datalekken dat een impact heeft gehad op de samenleving onderstrepen het belang van aanhoudend zicht op de beheersing van privacyrisico's binnen de Rijksoverheid. Wanneer de verwerking van persoonsgegevens in overheidsorganisaties niet voldoet aan de AVG, zijn er risico's voor zowel de burger als voor de Rijkoverheid: de betrokkene loopt privacyrisico's met mogelijk nadelige gevolgen voor de persoonlijke levenssfeer. De Rijksoverheid als verwerkingsverantwoordelijke wordt hierdoor geconfronteerd met politiek-bestuurlijke en/of juridische maatregelen, verlies van vertrouwen en beschadiging van imago als gevolg van communicatieve of handhavende maatregelen van betrokkenen, derden en/of de toezichthoudende autoriteiten.

Met name omdat de Rijksoverheid steeds meer een datamacht is en de behoefte aan transparantie toeneemt (zie bijvoorbeeld de uitkomsten van het Parlementaire Ondervragingscommissie Toeslagenaffaire), is het belangrijk dat op het domein van privacy het vertrouwen van de burger in de Rijksoverheid behouden blijft. Het in interdepartementaal verband analyseren van geïnventariseerde goede voorbeelden (best practices) en verbeterpunten in de beheersing, kan bijdragen aan de noodzakelijke versterking van de privacybescherming binnen de Rijksoverheid.

## 1.2 Doelstelling

De doelstelling van dit onderzoek is om privacymanagement binnen de Rijkoverheid verder te helpen versterken, alsmede departementale best practices aan te dragen ten behoeve van interdepartementale lering en samenwerking. Deze doelstelling is in de praktijk gebracht door per departement inzicht te verkrijgen in:

- De inrichting van de privacygovernance bij de departementen voor de aantoonbare naleving van de AVG (aantoonplicht).
- De kwaliteit van de afspraken met verwerkers, alsmede de inrichting van de controle en monitoringsactiviteiten die toezien op de naleving van deze afspraken (verwerkersovereenkomsten).
- De gehanteerde privacycriteria in de departementale cloudstrategieën.

Op basis van de 12 departementale deelrapporten reeds uitgebracht aan de CIO's van de departementen, is dit samenvattend interdepartementale rapport opgesteld.

# 2 Bevindingen onderzoek

## 2.1 Inrichting privacygovernance voor aantoonbaarheid naleving AVG

Met een privacybeleid geven departementen op organisatorisch en strategisch niveau inzicht in de inrichtingskeuzes inzake de AVG en de wijze waarop ze waarborgen dat de verwerking van persoonsgegevens op een rechtmatige wijze plaatsvindt. Onderdeel hiervan is een heldere verdeling van taken, bevoegdheden en verantwoordelijkheden en van middelen en rapportagelijnen zodat geborgd kan worden dat de departementen op de juiste wijze invulling geven aan de eisen van het privacybeleid en de AVG.

Het ontbreken van of het niet beschikken over een actueel privacybeleid leidt ertoe dat departementen geen of geen actueel beeld hebben van wat precies wordt verwacht en wie waar verantwoordelijk voor is. Dit brengt het risico met zich mee dat persoonsgegevens onrechtmatig verwerkt[1] worden.

### *2.1.1 Privacybeleid aanwezig; actualisering in aantal gevallen noodzakelijk*

Nagenoeg alle departementen beschikken over een expliciet beschreven privacybeleid dat is vastgesteld door of namens de secretaris-generaal (SG). Twee departementen hebben voor een andere vorm gekozen. De AVG stelt echter geen harde eisen aan de vorm. Wel adviseert de Autoriteit Persoonsgegevens (AP) om het privacybeleid zo veel als mogelijk in één document vast te leggen om versnippering te voorkomen. De leeswijzer in het privacybeleid van EZK en LNV waardoor het privacybeleid wordt voorzien van context en toelichting draagt de ADR aan als best practice. De manier waarop de departementen in hun privacybeleid invulling geven aan de beginselen inzake de verwerking van persoonsgegevens is niet altijd concreet uitgewerkt naar de praktijk. Actie is noodzakelijk om de beginselen in opzet en bestaan beter te borgen. JenV heeft in het privacybeleid de beginselen geoperationaliseerd en gekoppeld aan de onderliggende processen waardoor het als best practice kan worden beschouwd.

Een ander punt van aandacht is de actualisering van het privacybeleid om het effect van wijzigingen op de privacyvereisten te monitoren, beoordelen en te behandelen. Wij hebben geconstateerd dat het privacybeleid van 6 departementen voor het laatst is vastgesteld in 2018 (25 mei 2018 AVG van kracht) of 2019. Het valt de ADR daarbij op dat sommige departementen het privacybeleid enkel wijzigen bij significante wijzigingen in de bedrijfsvoering of het risicobeeld en andere departementen middels een cyclisch proces uiteenlopend van iedere 2 jaar, 3 jaar, 4 jaar of 5 jaar. De ene manier hoeft echter de andere manier niet uit sluiten en idealiter bestaat het actueel houden van het privacybeleid uit een combinatie van beide. Een privacybeleid dient te allen tijde een actueel beeld te geven over de uitgangspunten van een departement over de verwerking van persoonsgegevens. Voor een aantal departementen is daarom op korte termijn actualisering noodzakelijk. Het privacybeleid van JenV (mei 2022) en EZK/LNV (augustus 2021) kunnen als best practice worden beschouwd omdat die het meest actueel én compleet zijn.

### *2.1.2 Taken, bevoegdheden en verantwoordelijkheden beschreven; actualisering in sommige gevallen punt van aandacht*

De departementen hebben de taken, bevoegdheden en verantwoordelijkheden van de privacyactoren beschreven, waarvan bijna alle departementen in het privacybeleid. Het feit dat bij sommige departementen het privacybeleid niet altijd

[1] Onder 'verwerken' kan worden verstaan; het verzamelen, registreren, bewaren, raadplegen, wijzigen, delen, organiseren, onderling verbinden, vernietigen van persoonsgegevens.

actueel is, werkt ook door in de beschreven taken, bevoegdheden en verantwoordelijkheden. De manier waarop JenV in haar privacybeleid de privacygovernance en taken, bevoegdheden en verantwoordelijkheden ondersteunt door een RASCI-matrix beschrijft, dragen wij aan als best practice.

### *2.1.3 Bewustwordingsactiviteiten vinden veelal (ad hoc) decentraal plaats*

Alle departementen besteden aandacht aan de bewustwording rondom privacy. Een paar departementen hebben een concreet bewustwordingsplan opgesteld, de meeste departementen hebben voor een ad hoc aanpak gekozen. Het valt de ADR op dat er weinig interdepartementale samenwerking is op het gebied van bewustwording. De ADR heeft meerdere (creatieve) voorbeelden aangetroffen waaronder een privacypuzzel van VWS die zich hiervoor zou kunnen lenen, evenals een privacy themaweek bij Defensie.

Wij hebben geconstateerd dat bewustwordingsactiviteiten vooral belegd zijn bij de onderliggende dienstonderdelen binnen de departementen. Hierdoor bestaat de mogelijkheid dat er verschillende bewustwordingsniveaus bestaan binnen een departement. Bij EZK en LNV worden decentrale bewustwordingsacties gedeeld op het AYA-platform zodat andere dienstonderdelen binnen EZK en LNV hier tevens gebruik van kunnen maken. Dit dragen wij aan als best practice.

### *2.1.4 PDCA-cyclus verantwoordingsplicht nog niet overal volledig ingericht; met name Act-gedeelte noodzakelijk voor verbetering*

Met de verantwoordingsplicht moet een departement aan kunnen tonen dat de verwerkingen aan de AVG voldoen. Wij hebben dit aan de hand van de PDCA-cyclus privacymanagement onderzocht en geconstateerd dat dit nog niet overal volledig is ingericht. Ieder departement heeft wel een proces ingericht waarmee jaarlijks verantwoord wordt over de AVG. De onderwerpen dan wel KPI's waarover verantwoord wordt, verschillen echter per departement waardoor een rijksbrede vergelijking lastiger is. Het voornaamste aandachtspunt dat naar voren komt is het Act-gedeelte. Uit de ontvangen evaluaties blijkt niet altijd de manier waarop opvolging is gegeven aan eerdere constateringen waardoor de PDCA-cyclus niet sluitend is. Actie is noodzakelijk om deze tekortkoming op te heffen.

De manier waarop Defensie, EZK/LNV en VWS hun PDCA-cyclus hebben ingericht, kunnen als best practice worden beschouwd. Bij EZK/LNV wordt op basis van de ingevulde self-assessments het Beeld Integrale Beveiliging en Privacy opgesteld dat de Chief Information Officer (CIO) deelt met de (p)SG. Bij Defensie wordt op basis van de ingevulde self-assessments een jaarlijkse toezichtsrapport opgesteld door de functionaris gegevensbescherming (FG) en is privacy tevens onderdeel van het proces rondom de reguliere managementrapportage. Bij VWS rapporteert de Chief Privacy Officer (CPO) op basis van de jaarlijkse self-assessments en 'site visits' minimaal eens per jaar via de CIO aan de bestuurlijk verantwoordelijke over de status van privacy binnen VWS.

### *2.1.5 Invulling Three Lines Model niet overal beschreven*

De ADR heeft vastgesteld dat de manier waarop een departement invulling geeft aan het Three Lines Model niet overal is beschreven (in het privacybeleid). Samen met de andere eerder besproken punten in deze paragraaf, is dit tevens een onderwerp waar bij een aantal departementen actie noodzakelijk is om de uitgangspunten rondom de AVG en de beheersing daarvan beter te beschrijven en daardoor uitvoering aan te geven. De manier waarop EZK/LNV en JenV het Three Lines Model hebben beschreven, ondersteund door een grafische weergave, kan als best practice worden beschouwd.

## 2.2 Kwaliteit van de afspraken met verwerkers en controle hierop

Bij de verwerking van persoonsgegevens door derden zijn maatregelen noodzakelijk om te borgen dat op de juiste wijze met persoonsgegevens wordt omgegaan en deze worden beschermd. Dit dient vastgelegd te worden in een concrete

verwerkersovereenkomst of een andere rechtshandeling zodat er een verbintenis ontstaat tussen de verwerker en de verwerkingsverantwoordelijke.

Wanneer niet wordt voldaan 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 betrokkenen.

### 2.2.1 *Beschreven procedure opstellen verwerkersovereenkomsten veelal niet aanwezig*

Wij hebben bij driekwart van de departementen geen beschreven procedure aangetroffen over het opstellen van verwerkersovereenkomsten. Dit geldt tevens voor een beschrijving van de taken, bevoegdheden en verantwoordelijkheden rondom dit proces. Veelal geven de departementen aan dat het opstellen van verwerkersovereenkomsten onderdeel is van het reguliere inkoopproces. Het betrekken van privacyexpertise tijdens dit proces is vaak niet in opzet vastgelegd. Wel is aan de ADR door elk departement het rijksbrede format voor een verwerkersovereenkomst aangereikt dat leidend is bij het opstellen van een verwerkersovereenkomst. De dienstonderdelen Dienst Uitvoerend Onderwijs (DUO) van OCW en de Rijksdienst voor Ondernemend Nederland (RVO) van EZK komen met hun procesbeschrijving inclusief taken, bevoegdheden en verantwoordelijkheden als best practice naar voren.

### 2.2.2 *Garanties door verwerkers hoofdzakelijk enkel vastgelegd in ARVODI-2018*

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.

Het in opzet borgen dat enkel verwerkers worden ingeschakeld die voldoende garanties kunnen bieden dat zij aan de wettelijke vereisten voor gegevensbescherming voldoen, komt op andere manieren zelden naar voren bij de departementen. Wel wordt er veelal verwezen naar, en uitvoering gegeven aan, een Data Protection Impact Assessment (DPIA) om de privacyrisico's bij de verwerking van persoonsgegevens in kaart te brengen. Bij VWS wordt door dienstonderdeel Rijksinstituut voor Volksgezondheid en Milieu (RIVM) onder andere relevante certificeringen opgevraagd bij de verwerkers en wordt door dienstonderdeel CIBG tijdens de aanbesteding een programma van eisen geformuleerd dat getoetst wordt bij de potentiële verwerkers. Dit kan als best practice worden beschouwd.

### 2.2.3 *Verwerkersovereenkomsten veelal afgesloten conform rijksbreed format; actualiteit register van verwerkingsactiviteiten vraagt wederom om noodzakelijk actie*

De ADR heeft een steekproef uitgevoerd door in het register van verwerkings-activiteiten van de departementen risicovolle verwerkingen te selecteren. Een expliciet proces over het opstellen van verwerkersovereenkomsten is veelal niet beschreven. Wel maken departementen gebruik van het rijksbrede format. Het rijksbrede format omvat de benodigde gegevens gesteld in de AVG. Ook wanneer bijvoorbeeld Defensie afwijkt van het rijksbrede format en het model van brancheorganisatie 'zorg' als uitgangspunt wordt genomen, worden tevens alle benodigde gegevens opgenomen. CAP, onderdeel van Financiën, maakt gebruik van een Logius-format dat getoetst is aan ARVODI. Toch ontbreken er vereiste passages in de afgesloten verwerkersovereenkomst. Ook heeft de ADR interdepartementaal geconstateerd dat oudere verwerkersovereenkomsten een punt van aandacht zijn. Veelal is hier gebruik gemaakt van een ouder rijksbreed model uit het pre-AVG-tijdperk. Actualisering is noodzakelijk om ook deze overeenkomsten te laten voldoen aan de AVG.

Door de verwerkersovereenkomsten nader te onderzoeken hebben wij geconstateerd dat het register van verwerkingsactiviteiten veelal (nog steeds) geen actueel en juist beeld geeft van de verwerkingen. Het komt voor dat niet de juiste

verwerkers zijn opgenomen evenals dat niet de juiste en actuele verwerkersovereenkomsten als bijlage zijn opgenomen. De juiste gegevens en bijlages zijn wel aanwezig binnen de departementen maar (nog) niet verwerkt in het register van verwerkingsactiviteiten. Het register van verwerkingsactiviteiten is een belangrijk middel om aantoonbaar rekenschap te kunnen geven over de AVG. Op korte termijn is er actualisering noodzakelijk om een juist beeld te kunnen weergeven over de verwerkingen van persoonsgegevens.

#### *2.2.4 Controle en monitoring verwerkersovereenkomsten veelal niet ingericht*

De departementen beschikken veelal niet over een formeel beschreven proces dat erop toeziet dat bij gewijzigde omstandigheden afgesloten verwerkers-overeenkomsten worden aangepast dan wel dat dit in de bestaande processen voor contractmanagement is verankerd. Het merendeel van de departementen geeft aan dat het controleren en monitoren van afgesloten verwerkersovereenkomsten in de praktijk ad hoc plaatsvindt. Het actualiseren van een DPIA kan hiervoor een aanleiding zijn. Het is noodzakelijk om beter inzicht te krijgen in de afgesloten verwerkersovereenkomsten. Alleen dan is controle en monitoring ook mogelijk.

Als best practice komt 3W van BZ naar voren, dat in opzet en bestaan beschikt over een privacymanagementsysteem waarmee het beoordelen en aanpassen van de verwerkersovereenkomsten is ingeregeld. Daarnaast komt ook Defensie naar voren als best practice. De Defensie-breed afgesloten verwerkersovereenkomsten zijn opgevoerd in SAP, waarin een monitoringsmodule aanwezig is. Deze verwerkers-overeenkomsten worden tevens meegenomen bij de jaarlijkse self-assessments (zie 2.1.4). Ook de Immigratie- en Naturalisatiedienst (IND) van JenV beschikt in opzet en bestaan over een proces voor de controle en monitoring van de afgesloten verwerkersovereenkomsten.

#### *2.2.5 Toezicht en controle op naleving afspraken met verwerkers bijna nergens ingericht*

De ADR heeft bijna nergens een proces in opzet en bestaan aangetroffen dat aangeleverde rapportages van verwerkers over gemaakte afspraken beoordeelt en indien noodzakelijk hiervoor mitigerende maatregelen treffen. Rapportages die periodiek worden aangeleverd zijn veelal geënt op informatiebeveiliging en minder tot niet geënt op privacy dan wel de gemaakte afspraken in de verwerkers-overeenkomst. Meldingen vanuit verwerkers die gedaan worden inzake privacy betreffen hoofzakelijk datalekken. De ADR kan echter geen uitspraak doen over de volledigheid van deze meldingen.

3W van BZ vraagt jaarlijks rapportages op van de verwerkers. AZ heeft in opzet geen proces beschreven maar de Dienst Publiek en Communicatie (DPC) vraagt wel ieder jaar in november aan alle verwerkers een bevestiging of bestaande analyses nog actueel zijn. Gezien het kleine aantal verwerkingen en verwerkers kost deze maatregel niet veel tijd. Het zorgt ervoor dat verwerkers actief worden getriggerd om na te denken of er veranderingen zijn.

### 2.3 Privacycriteria in departementale cloudstrategieën

Waar in het rijksbrede cloudbeleid uit 2021 werd gestreefd naar het gebruik van private clouddiensten zal in het vernieuwde rijksbrede cloudbeleid 2022[2] een visie worden gedeeld op het gebruik van publieke dan wel commerciële clouddiensten. Bij de verwerking van persoonsgegevens in een publieke cloudomgeving spelen niet alleen belangrijke risico's op het gebied van informatiebeveiliging maar ook op het gebied van privacy voor de betrokkenen. Het opnemen van privacycriteria in departementale cloudstrategieën, het uitvoeren van risicoanalyses van de privacy en bijbehorende technische en organisatorische maatregelen zijn noodzakelijk om de privacy van de betrokkenen te beschermen.

[2] Op 29 augustus 2022 is de Tweede Kamer door Staatssecretaris Alexandra van Huffelen (Digitalisering) geïnformeerd over het rijksbreed cloudbeleid 2022. Het veldwerk van dit rijksbrede AVG onderzoek vond plaats in de periode daarvoor. Het rijksbreed cloudbeleid 2022 is daarom niet in de scope van dit onderzoek.

### 2.3.1 *Clouddiensten binnen departementen niet overal inzichtelijk*

De ADR heeft vastgesteld dat de helft van de departementen inzichtelijk heeft welke clouddiensten zijn afgenomen binnen het departement. Bij de departementen waar centraal dan wel decentraal een overzicht aanwezig is, is er wel een verschil in diepte en zijn de overzichten veelal nog niet volledig. Onderwerpen als het rubriceringsniveau of de al dan niet uitgevoerde risicoanalyse op de verwerking van persoonsgegevens is niet altijd opgenomen. Het overzicht van JenV kan als best practice worden beschouwd. Daarin is per clouddienst in kaart gebracht het service model, platform, deployment model, rubriceringsniveau, basisbeveiligingsniveau en risicoafweging. De ADR kan echter geen uitspraak doen over de volledigheid van de overzichten.

### 2.3.2 *Cloudbeleid en cloudstrategie aanwezig bij departementen in afwachting op rijksbreed cloudbeleid 2022*

Bijna alle departementen beschikken over een cloudbeleid dan wel cloudstrategie. De ADR heeft vastgesteld dat (informatie)beveiliging de boventoon voert ten opzichte van privacy. De documentatie is voornamelijk gericht op een toekomstvisie en routekaarten. Veelal is aangegeven dat de verdere uitwerking van het cloudbeleid en de cloudstrategie volgt na inwerkingtreding en op basis van het rijksbreed cloudbeleid 2022. Door een routekaart te combineren met een besluitvormingsraamwerk, kan het afwegingproces cloud uit het cloudbeleid van Defensie en EZK/LNV als best practice worden beschouwd. Departementen BZ en IenW beschikken over een Cloud Competence Community waarin verschillende IV-expertises samenkomen. Ook al zou een extra nadrukkelijke inbreng vanuit privacyperspectief gewenst zijn, beschouwen wij dit initiatief toch als best practice.

### 2.3.3 *Risicoanalyse privacy veelal in opzet opgenomen; noodzakelijke aandacht vereist voor grote niet-Europese bedrijven*

In opzet is beschreven dat om privacyrisico's te inventariseren, te beoordelen en te beperken een DPIA uitgevoerd dient te worden. Met name bij grote, niet-Europese bedrijven, kan de uitvoering van een DPIA en de bijbehorende technische en organisatorische maatregelen uitdagend zijn. Wanneer persoonsgegevens worden verwerkt dan wel opgeslagen in een land buiten de EU, geldt de AVG niet. Het is noodzakelijk dat juist bij deze grootschalige verwerkers extra wordt nagegaan welke risico's aanwezig zijn en of de bescherming van persoonsgegevens op hetzelfde niveau ligt als bij de AVG. Het is Rijksbreed noodzakelijk dat hier op korte termijn nadrukkelijk extra aandacht aan wordt besteed. Het valt ons op dat er weinig tot geen interdepartementale samenwerking is bij het uitvoeren van risicoanalyses omtrent privacy voor grote clouddiensten die ieder departement gebruikt.

### 2.3.4 *Classificatie van persoonsgegevens niet overal in opzet vastgelegd*

De ADR heeft niet bij alle departementen uitgangspunten voor het classificeren van data in opzet aangetroffen. Het classificeren van data is een startpunt om vervolgens privacyrisico's in kaart te brengen en te bepalen welk niveau van bescherming noodzakelijk is. Het dataclassificatiemodel van BZ en de uitwerking van EZK/LNV en JenV geven duidelijke handvatten en kunnen als best practice worden beschouwd.

### 2.3.5 *Eigenaarschap in opzet vastgelegd, vaste exit strategie niet overal beschreven*

Bij de departementen is in opzet beschreven dat zij de eigenaar zijn van de data in de cloud. Een vaste procedure inzake de exit strategie is echter niet overal beschreven terwijl dit wel een belangrijk onderdeel is als het gaat om eigenaarschap. Als best practice identificeren wij dat BZK het opstellen van een exitstrategie opneemt tijdens het aanbestedingsproces.

### 2.3.6 *Locatie van gegevens summier in opzet beschreven, maar niet altijd even strikt*

Bijna alle departementen besteden in hun cloudbeleid dan wel cloudstrategie aandacht aan de locatie van gegevens. Dit gebeurt echter niet uitgebreid en niet

altijd even strikt. Met name de gevolgen van het niet opslaan van data binnen de EU zijn onderbelicht. Het gaat veelal over 'voorkeuren' of 'het in acht nemen van geografische locatie'. Refererend naar paragraaf 2.3.3 inzake de risicoanalyse voor privacy, vraagt het opslaan dan wel verwerken van persoonsgegevens in een land buiten de EU nadrukkelijk om extra aandacht en noodzakelijke maatregelen aangezien daar de AVG niet geldt.

# 3 Aanbevelingen en/of vervolgstappen

Op basis van de in hoofdstuk 2 genoemde interdepartementale bevindingen doen wij een aantal aanbevelingen. De meest opportune en noodzakelijke aanbevelingen[3] zijn gemarkeerd met een **(+)** aan het einde. Te beginnen vanuit het doel van dit onderzoek: maak gebruik van elkaars departementale best practices **(+)**.

### Inrichting privacygovernance voor aantoonbaarheid naleving AVG

- Besteed aandacht aan de actualisering van het privacybeleid. Zorg dat er zowel een actualisering plaatsvindt wanneer er sprake is van significante wijzigingen in de bedrijfsvoering of het risicobeeld, als middels een cyclisch proces van iedere 3 jaar of korter **(+)**.
- Besteed aandacht aan het (verder) uitwerken van de beginselen inzake de verwerkingen van persoonsgegevens zowel in opzet als bestaan **(+).**
- Moedig aan om de uitgangspunten omtrent privacy zo veel mogelijk in één document te verzamelen, bij voorkeur in het privacybeleid. Neem de taken, verantwoordelijkheden en bevoegdheden hier ook in mee.
- Deel bewustwordingsactiviteiten zowel breder binnen het departement als interdepartementaal.
- Besteed bij de jaarlijkse verantwoording tevens aandacht aan het Act-gedeelte om de PDCA-cyclus compleet te maken en aantoonbaar rekenschap te kunnen geven over de verantwoordingsplicht **(+)**.
- Beschrijf de manier waarop een departement invulling geeft aan het Three Lines Model **(+)**.

### Kwaliteit van de afspraken met verwerkers en controle hierop

- Beschrijf in opzet de manier waarop een verwerkersovereenkomst opgesteld moet worden, evenals de taken, bevoegdheden en verantwoordelijkheden rondom dit proces. Besteed hierbij behalve aan de afdeling inkoop ook aandacht aan het betrekken van de benodigde privacyexpertise.
- Beschrijf los van de voorwaarde in ARVODI tevens de manier waarop het departement borgt dat er uitsluitend enkel verwerkers worden ingeschakeld die voldoende garanties kunnen bieden dat zij aan de wettelijke vereisten voor gegevensbescherming voldoen.
- Wanneer er wordt afgeweken van het rijksbrede format bij het opstellen van een verwerkersovereenkomst, toets dat alle benodigde gegevens worden opgenomen **(+)**.
- Besteed extra aandacht aan en actualiseer wanneer nodig de afgesloten verwerkersovereenkomsten uit het pre AVG-tijdperk **(+)**.
- Actualiseer het register van verwerkingsactiviteiten zodat het een juist en actueel beeld geeft van de verwerkingen (en bijbehorende verwerkers) die plaatsvinden binnen het departement **(+)**.
- Creëer een algemeen departementaal overzicht van de afgesloten verwerkersovereenkomsten en veranker dit zo nodig in de bestaande processen van contractmanagement, om zo controle en monitoring op de afgesloten verwerkersovereenkomsten mogelijk te maken.
- Vraag actief aan de verwerkers om periodiek te rapporteren over de verwerking van persoonsgegevens die zij namens de verwerkingsverantwoordelijke uitvoeren om zo toezicht en controle mogelijk te maken.

[3] Aanbevelingen die relatief snel opgepakt kunnen worden en noodzakelijk zijn (laaghangend fruit).

### Privacycriteria in departementale cloudstrategieën

- Continueer het inzichtelijk maken van de afgenomen clouddiensten en breng per clouddienst het service model, platform, deployment model, rubriceringsniveau, basisbeveiligingsniveau, risicoafweging en locatie in kaart **(+)**.
- Werk het departementale cloudbeleid naar aanleiding van het rijksbreed cloudbeleid 2022 verder uit met aandacht voor privacycriteria **(+)**.
- Treed als één rijksoverheid op bij het uitvoeren van DPIA's voor risicovolle verwerkingen bij grote niet-Europese bedrijven **(+)**.
- Beschrijf het proces rondom het classificeren van data en continueer het classificeren van data om te kunnen bepalen welk niveau van bescherming noodzakelijk is.
- Werk een vaste exitstrategie voor data in een cloudomgeving verder uit.
- Beschrijf nadrukkelijker de uitgangspunten rondom de locatie van data en de gevolgen dan wel aanvullende maatregelen die noodzakelijk zijn bij het verwerken en opslaan van data in een land buiten de EU.

# 4 Verantwoording onderzoek

## 4.1 Werkzaamheden en afbakening

De werkzaamheden en afbakening zijn een gevolg van de drieledige doelstelling van dit onderzoek. De afbakening van dit onderzoek was de door de departementen in opzet en bestaan getroffen maatregelen betreffende geselecteerde verwerkingen van persoonsgegevens teneinde aantoonbaar rekenschap te kunnen geven over de naleving van de beginselen:

- Rechtmatigheid, behoorlijkheid en transparantie (AVG art 5.1a);
- Doelbinding (AVG art 5.1b);
- Minimale gegevensverwerking (AVG art 5.1c);
- Juistheid gegevens (AVG art 5.1d).

Voortkomend uit AVG art 5.2 is de verwerkingsverantwoordelijke verantwoordelijk voor de naleving van deze beginselen én kan deze aantonen (aantoonplicht). Hierbij hebben wij per departement het aanwezige privacybeleid, de positionering van de privacyorganisatie en de verantwoordings- en rapportagestructuren binnen dit onderzoek onderzocht.

Per departement hebben wij vervolgens aan de hand van drie tot vijf verwerkingen uit het register van verwerkingsactiviteiten inzicht verschaft in de kwaliteit van de afspraken met de verwerkers en de controle- en monitoringsactiviteiten omtrent de naleving van deze afspraken. Hierbij ging het om de procedures omtrent het aangaan/de totstandkoming van een verwerkersovereenkomst alsmede de borging van de juistheid en de volledigheid van de inhoudelijke afspraken. Daarnaast is inzicht verschaft in de inrichting van de regiefunctie die toeziet op de naleving van de gemaakte afspraken. Hierbij is uitgegaan van de vereisten zoals opgenomen in artikel 28 “Verwerker” van de AVG. Contracten met subverwerkers vielen buiten scope van dit onderzoek.

Als derde hebben wij per departement het vastgestelde cloudbeleid/cloudstrategie onderzocht op privacycriteria en privacyrisico’s bij de gemaakte keuzes. Vanuit het rijksbreed informatiebeveiligingsonderzoek 2021 is in het najaar 2021 een inventariserend deelonderzoek naar de cloud uitgevoerd zoals beschreven in het plan van aanpak dat op 15 september 2021 in het CIO-Beraad is besproken. Hiervan hebben wij mede gebruik gemaakt om de auditlast te minimaliseren.

Op basis van de 12 departementale deelrapporten reeds uitgebracht aan de CIO’s van de departementen, is dit samenvattend interdepartementaal rapport opgesteld om departementale best practices aan te dragen ten behoeve van interdepartementale lering en samenwerking.

## 4.2 Referentiekader

Voor dit onderzoek is gebruikgemaakt van een referentiekader waarin maatregelen uit het ADR Privacyframework zijn opgenomen alsmede de van toepassing zijnde normen uit de Data Pro Code. Het uitgangspunt van het ADR Privacyframework is de AVG en de UAVG, rekening houdend met de adviezen die de 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 maken wij gebruik 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 hebben wij normen gebruikt die opgenomen zijn in het geïntegreerde NORA/ISOR/BIO-kader.

### 4.3 Gehanteerde Standaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zouden we wellicht andere zaken hebben geconstateerd en gerapporteerd.

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

### 4.4 Verspreiding rapport

De opdrachtgever, de leden van het CIO-beraad, zijn eigenaar van dit rapport. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Hoewel het rapport de context van het onderzoek zo goed mogelijk probeert te beschrijven, is het mogelijk dat iemand die de context niet (volledig) kent, de uitkomsten anders interpreteert dan bedoeld.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Voor openbaarmaking door het opdrachtgevende ministerie van door de ADR aan dit ministerie uitgebrachte rapporten gelden de voorschriften uit de Wet Open Overheid (WOO). De minister van Financiën stuurt elk halfjaar een overzicht van door de ADR uitgebrachte rapporten naar de Tweede Kamer.

# 5 Ondertekening

Den Haag, 21 maart 2023

Projectleider | Auditdienst Rijk

# Managementreactie

Indien u nog een managementreactie wenst te geven op het rapport, dan ontvangen wij deze graag, wij zullen uw reactie toevoegen bij het rapport.

**Auditdienst Rijk**
Postbus 20201
2500 EE  Den Haag
(070) 342 77 00