Auditdienst Rijk
Ministerie van Financiën

Deelrapport uitgebracht aan
Persoonsgegevens Ministerie van Financiën

Datum
28-11-2022

Auditdienst Rijk
Korte Voorhout 7
2511 CW Den Haag

Kenmerk
2022-0000287092

Rijksbreed AVG 2022
Definitief deelrapport van bevindingen Ministerie van Financien

Inleiding

Het rijksbreed AVG-onderzoek 2020 van de Auditdienst Rijk (ADR) heeft het beeld bevestigd dat de verdere inbedding van privacy management 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 Financiën de interne organisatie heeft ingericht ten behoeve van een aantoonbare verantwoordingsverplichting, totstandkoming verwerkersovereenkomsten en -afspraken alsmede de regie en toezicht op de naleving hiervan. Daarnaast is onderzoek gedaan naar de privacycriteria die in de departementale cloudstrategie worden gehanteerd. Deze onderwerpen zijn belangrijke onderdelen van privacy management 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.

In tegenstelling tot andere departementen loopt dit jaar bij Financiën te gelijker tijd met het rijksbrede AVG-onderzoek een ander vraaggestuurd onderzoek naar de verantwoordingsverplichting en verantwoordings-structuur binnen het departement. Om het departement en de organisatieonderdelen niet onnodig extra te belasten, wordt voor de bevindingen betreft de verantwoordingsverplichting en verantwoordings-structuur verwezen naar het *Onderzoeksrapport Implementatie aantoonplicht AVG*. Naar verwachting zal dit rapport eind 2022 uitkomen.

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 privacy risico's ontstaan voor een betrokkene.

Geselecteerde dienstonderdelen en verwerkingen

Vooraf is door de ADR voor dit onderdeel een selectie gemaakt van vijf verwerkingen uit het register van verwerkingsactiviteiten. De eerste 3 verwerkingen vinden plaats bij het organisatieonderdeel *Centraal Administratieve Processen (CAP)* van de *Belastingdienst* en de laatste 2 bij *Domein Roerende Zaken (DRZ)*.

- M880 - Inwinnen van persoonsgegevens voor de taken van de Belastingdienst;
- M882 - Verstrekken van persoonsgegevens;
- M1024 - Invordering: Individuele dwanginvordering – Overheidsvordering;
- M1613 – Het beheren en vervreemden van roerende zaken voor de Rijksoverheid;
- M1770 - Ondersteunende processen DRZ

NB: DRZ heeft verwerkingen in het register opgenomen, waarbij verwezen wordt naar verwerkers die niet verwerkers zijn in de zin van de AVG. Deze organisaties zijn dienstverleners die (voornamelijk) goederen verwerken en niet persoonsgegevens. Hierdoor bleek gedurende het onderzoek dat bij de geselecteerde DRZ-verwerkingen geen verwerkersovereenkomsten aanwezig waren.

Garanties naleving AVG bij verwerkers

In het privacybeleid[1] van het ministerie van Financiën is opgenomen dat de organisatie alleen verwerkers inschakelt die voldoen aan de wettelijke vereisten van de AVG. Dit betekent dat in opzet wordt voldaan aan de norm doordat in het privacybeleid is opgenomen dat voorafgaand aan de samenwerking met externe verwerkers, een risicoanalyse of DPIA uitgevoerd dient te worden.

Belastingdienst/CAP

Door CAP is aangegeven dat voor sommige verwerkingen (nog) geen DPIA is uitgevoerd en dat bij andere verwerkingen een risicoanalyse is gemaakt door de gegevensstroom qua gevoeligheid te toetsen aan al bestaande gegevensstromen.

Procedure opstellen verwerkersovereenkomsten/-afspraken

Het opstellen van verwerkersovereenkomsten/-afspraken komt terug in de handreikingen van de onderzochte organisatieonderdelen (Belastingdienst /CAP en DRZ) waarin een beschrijving op hoofdlijnen is opgenomen over de verdeling van taken en verantwoordelijkheden bij het opstellen van een verwerkersovereenkomst.
Bij Belastingdienst/CAP en DRZ is het proces omtrent de totstandkoming van verwerkersafspraken mondeling toegelicht. Beide organisaties hebben er bewust voor gekozen de procesbeschrijving vooralsnog niet gedetailleerd uit te werken, daardoor ontbreekt momenteel een gedetailleerde procesbeschrijving ten aanzien van het opstellen van verwerkersovereenkomsten waarin de relaties tussen de verantwoordelijke functionarissen inzichtelijk zijn gemaakt.

Verwerkersovereenkomsten/-afspraken

Belastingdienst/CAP

Bij CAP zijn met de verwerkers van de geselecteerde verwerkingen verwerkersovereenkomsten/-afspraken afgesloten die tweezijdig zijn ondertekend. Door CAP is aangegeven dat gebruik wordt gemaakt van een Logius-format, dat getoetst is aan ARVODI. Door de ADR is geconstateerd dat in de overeenkomsten met ING en Logius geen bepalingen zijn opgenomen m.b.t. privacyrechten en het verwijderen van gegevens. Daarnaast is in de overeenkomst met ING geen bepaling opgenomen met betrekking tot datalekken. In de verwerkersovereenkomsten/-afspraken wordt gesteld dat passende technische en organisatorische maatregelen genomen dienen te worden, maar deze beveiligingsmaatregelen zijn niet nader geconcretiseerd. Daarnaast is in de verwerkersovereenkomst van ING niet vastgelegd dat de verwerker verplicht is risicoanalyses uit te voeren en regelmatig een beveiligingstest te doen.

DRZ

Door de ADR is vastgesteld dat bij beide geselecteerde DRZ-verwerkingen geen verwerkersovereenkomsten aanwezig waren. DRZ heeft aangegeven dat zij een te ruime definitie hanteerde van het begrip 'verwerker' waardoor in het register ten onrechte staat aangegeven dat er sprake is van een verwerker. De ADR heeft geen alternatieve verwerkingen geselecteerd en kan daardoor geen uitspraak doen over de kwaliteit van de verwerkersovereenkomsten bij DRZ.

Controle en monitoring verwerkersovereenkomsten/-afspraken

Belastingdienst/CAP

Het beoordelen en aanpassen van verwerkersovereenkomsten/-afspraken is bij CAP een eerstelijns verantwoordelijkheid, maar hier is geen expliciet proces voor in opzet beschreven en ingericht. Het aanpassen van een verwerkersovereenkomst vindt alleen plaats naar aanleiding van een DPIA, waardoor een risico ontstaat voor verwerkingen waarvoor geen DPIA uitgevoerd wordt. Bij CAP is geen procedure in opzet en bestaan vastgesteld die erop toeziet dat bij gewijzigde omstandigheden verwerkersovereenkomsten worden aangepast. Door CAP is aangegeven dat voor het periodiek beoordelen van risico's gebruik wordt gemaakt door een

[1] Privacybeleid Financiën versie 1.0, d.d. 2 september 2019

zogenoemde 'willen, mogen, kunnen'-toets (WMK-toets) en DPIA's. Het bestaan hiervan heeft de ADR niet kunnen vaststellen omdat hierover geen aanvullend bewijs is aangeleverd.

DRZ
DRZ heeft geen procedure opgesteld inzake het proces met betrekking tot het beoordelen en aanpassen van verwerkingsovereenkomsten.
Door DRZ is aangegeven dat het aanpassen van overeenkomsten nog niet eerder heeft plaatsgevonden. De verantwoordelijkheid voor de controle en monitoring van verwerkersovereenkomsten is belegd bij de Data coördinatoren die de verwerkersovereenkomsten jaarlijks evalueren. Aangezien er geen notulen zijn opgesteld van deze jaarlijkse vergaderingen is de ADR niet in staat om het bestaan vast te stellen van dit proces.

Toezicht en controle op naleving van de afspraken met verwerkers
In het privacybeleid van Financiën is in opzet beschreven dat in verwerkingsovereenkomsten afspraken moeten worden gemaakt over periodieke rapportages specifiek ook met betrekking tot beveiligingsincidenten ofwel grote datalekken. Voor zowel Belastingdienst/CAP als DRZ heeft de ADR geen expliciet beschreven proces kunnen vaststellen dat is ingericht om toe te zien op de verwerkersovereenkomsten en het beoordelen van de periodieke rapportages van de verwerkers.

Belastingdienst/CAP
Naar wij hebben vernomen worden door de onderzochte verwerkers van CAP periodiek rapportages opgesteld, maar CAP heeft aangegeven dat er geen controleactiviteiten worden uitgevoerd op de overeenkomst met de ING (verwerking 1024). Voor de overeenkomsten met Logius (verwerking M882) en RINIS (verwerking M880) heeft CAP aangegeven dat de controleactiviteiten hierop zeer beperkt zijn omdat de verwerkers overheidsorganisaties zijn. Daarom acht CAP in dat laatste geval een in control statement als voldoende en willen zij niet zelf nog controleactiviteiten uitvoeren. Dit is volgens CAP in lijn met de afgesproken governance binnen de Digitale Overheid.

DRZ
DRZ als onderdeel van de beleidskern heeft ten tijde van het onderzoek aangegeven dat het plan is om een risicoregister op te stellen door gebruik te maken van de KCD-tool[2]. Hierin zal dan een volledig overzicht worden gegenereerd van de risico's die voortvloeien uit de DPIA's en de bijbehorende opgestelde maatregelen. DRZ heeft aangegeven dat het de bedoeling is om vast te leggen in hoeverre deze maatregelen de risico's afdekken zoals opgenomen in verwerkersovereenkomsten.

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

- Belastingdienst/CAP en DRZ; beschrijf in opzet het proces rondom het opstellen van verwerkersovereenkomsten/-afspraken neem hierbij de onderlinge relaties tussen de betrokken actoren in mee.
- Belastingdienst/CAP en DRZ: beschrijf in opzet en richt in bestaan een proces in dat periodiek de juistheid en actualiteit van de reeds afgesloten verwerkersovereenkomsten/-afspraken monitort. Veranker dit bijvoorbeeld in de bestaande processen van contractmanagement en service level management met de interne overheidsdienstverleners.
- DRZ; Realiseer het voornemen om het verwerkingsregister bij te werken en draag hierbij zorg voor een actueel overzicht van de verwerkers en de verwerkersovereenkomsten/-afspraken.
- DRZ; Prioriteer het voornemen inzake de realisatie van een risicoregister (KCD-tool) waarmee een overzicht opgesteld kan worden van de risico's uit de DPIA's en de daarbij behorende opgestelde maatregelen.
- Belastingdienst/CAP en DRZ; richt een gestandaardiseerd proces in waarbij de periodieke rapportages[3] van verwerkers over de afgesproken privacy normen worden beoordeeld door de verwerkersverantwoordelijken.

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 cloud strategieën. Naar aanleiding hiervan heeft de ADR een inventarisatie gehouden van de privacy criteria in deze departementale strategieën.

Cloudstrategie departement Financiën
Het ministerie van Financiën is bezig met de formalisering van een kader voor het gebruik van Cloud toepassingen als volwaardig alternatief op de traditionele on premise[4] IV. Financiën conformeert zich aan het Rijksbrede Cloudbeleid. Er is een departementale werkgroep die zorgt dat het Afwegingskader Cloud Financiën (2021) in lijn wordt gebracht met dit cloudbeleid. In de uitgangspunten van het kader zijn de volgende aandachtspunten opgenomen: sourcing[5], architectuur, informatiebeveiliging, privacy en data. Bij privacy kijkt men onder meer naar de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie die wordt opgeslagen op de cloudtoepassing evenals het transport en de verwerking van gegevens.

Clouddiensten binnen Financiën
Financiën en de onderliggende dienstonderdelen beschikken in opzet en bestaan over een overzicht met de afgenomen clouddiensten. Het overzicht is risicogericht opgezet. Van niet alle applicaties is het overzicht compleet. Het deploymentmodel (bijv. Private Cloud) is wel overal opgenomen in de lijst. Van ongeveer een kwart van de clouddiensten van het beleidsdepartement ontbreekt het servicemodel (bijv. Saas[6], on premise) in de lijst. Bij ongeveer 1/3 deel ontbreekt het Basis Beveiligingsniveau (BBN) niveau.

TopDesk
De ADR heeft onderzoek gedaan naar TopDesk[7] als cloudtoepassing binnen de beleidskern, hierbij is in opzet gekeken naar beveiligingsaspecten, toegang en privacy, classificatie, (data) eigenaarschap en geografische locatie van die dienstverlener. Ten tijde van het onderzoek is aangegeven dat de contracten met TopDesk worden bezien om de verschillende TopDesk-applicaties (zowel SaaS als on premise) terug te brengen naar één contract. In hoeverre de onderlinge afspraken tussen cloud consumer en cloud provider zullen worden herzien dan wel geconcretiseerd, zal op een later moment moeten worden bezien.

Beveiligingsaspecten
De ADR heeft onderzocht in hoeverre er beschikbaarheids- integriteits- en vertrouwelijkheidsmaatregelen zijn getroffen voor de opslag, de verwerking en het transport van data binnen TopDesk. TopDesk was ten tijde van het onderzoek nog niet opgenomen in het risicoregister van de beleidskern, aangegeven is dat hierdoor de documentatie m.b.t. de te treffen maatregelen niet kan worden aangeleverd. De ADR heeft wel een Quickscan Informatiebeveiliging en een Pre-scan DPIA ontvangen. Vooraf besteed Financiën dus wel aandacht aan de privacy criteria. De documentatie van de te treffen maatregelen ontbreekt echter nog.

Toegang en privacy
De ADR heeft onderzocht of er ter bescherming van data en privacy, beveiligingsmaatregelen zijn getroffen in de vorm van data-analyse, DPIA, sterke toegangsbeveiliging en encryptie. Voor TopDesk is er een DPIA uitgevoerd en een Quickscan Informatiebeveiliging. Wat betreft data-analyse en encryptie specifiek zijn er op voorhand geen te treffen maatregelen opgenomen in het proces. Zoals hiervoor aangegeven ontbreekt de documentatie van de te treffen maatregelen, maar zullen deze op termijn wel worden opgenomen in het beoogde risicoregister.

Classificatie
De ADR heeft onderzocht of er door de verwerkingsverantwoordelijke aan data en middelen waarin/waarop zich data bevindt een classificatie wordt toegekend gebaseerd op datatype, waarde, gevoeligheid en kritische gehalte voor de organisatie. Voor TopDesk heeft de ADR een Quickscan

[2] KCD-tool staat voor Key Control Dashboard
[3] Dit kunnen ook In Control Statements zijn
[4] On premise is een model waarbij de software draait op de eigen locatie
[5] Onder sourcen wordt verstaan: het bepalen wat de organisatie zelf doet en wat uitbesteedt wordt aan leveranciers.
[6] Software-as-a-Service (SaaS) is een model waarbij softwaretoepassingen via internet worden aangeleverd
[7] Topdesk is software dat service managementprocessen ondersteund, zoals bijvoorbeeld wijzigingenbeheer.

Informatiebeveiliging ontvangen, hierin wordt de data geclassificeerd en gelabeld o.b.v. een BBN (Basis Beveiligings Niveau) -niveau.

Eigenaarschap & Locatie
In het afwegingskader staat omschreven dat Financiën integraal verantwoordelijk blijft voor de keuze van een cloudtoepassing. Een uitwerking van wat moet worden verstaan onder integrale verantwoordelijkheid is niet nader omschreven. Weliswaar wordt het belang van een exit-strategie benoemd in het geval dat een overeenkomst dient te worden beëindigd, maar een verdere verdeling van eigenaarschap tussen cloudconsumer en cloudprovider is bewust niet opgenomen in het kader. Aangegeven wordt dat dergelijke afwegingen dienen te worden gemaakt op basis van de beschikbare expertise die men meeneemt in het procurement proces, elke aanbesteding is en wordt daarmee maatwerk. Financiën neemt bij het afnemen van een cloud toepassing in acht dat het specificeren van de geografische locatie van de clouddienst van groot belang is.

Controle en monitoring op cloudtoepassingen
Een concreet proces rondom de controle en monitoring achteraf op gemaakte afspraken betreft cloud toepassingen is (nog) niet in opzet en bestaan ingericht. Het geplande risicoregister zal hier gedeeltelelijk invulling aan kunnen geven, maar is nog niet gerealiseerd en heeft alleen aandacht voor risico's en bevat niet de monitoring van alle afspraken met de cloudprovider.

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

- Actualiseer het Afwegingskader Cloud (2021) en concretiseer indien nodig de privacy criteria;
- Zorg bij het in kaart brengen van de verschillende afgenomen clouddiensten met name dat alle benodigde gegevens volledig ingevuld worden in het overzicht en houd dit overzicht actueel.
- Formaliseer het proces om privacy expertise te betrekken bij de aankoop zoveel mogelijk om te borgen dat privacycriteria standaard worden meegenomen in de afspraken met de leveranciers en niet kunnen worden vergeten;
- Richt een proces in dat achteraf toeziet op de gemaakte afspraken met Clouddiensten (denk hierbij ook aan het recht-op-audit/right-to-audit).

Managementreactie [redacted] van Financiën

Wij danken de ADR voor het uitgevoerde onderzoek.
Het beleidsdepartement en de Belastingdienst herkennen zich in de bevindingen en de aanbevelingen worden overgenomen. De aanbevelingen liggen in het verlengde van de, dit jaar, door de werkgroep Privacy op Orde, ingezette verbeteringen om de inrichting, beheersing en verantwoording van privacybescherming van het ministerie van Financiën te verbeteren. Daarbij valt te denken aan het actualiseren van het privacybeleid, het voorbereiden van de werving van een departementale Chief Privacy Officer, het uitvoeren van een nulmeting door Douane, het aanstellen van projectleiders AVG bij Douane en Toeslagen
Tevens valt op te merken dat de aanbevelingen uit het RBO AVG 2021 op 1 na zijn opgelost. De nog openstaande aanbeveling is het opnemen van de PDCA-cyclus in het Privacybeleid.

Hieronder wordt, samenvattend, ingegaan op de aanbevelingen die de ADR heeft meegegeven.

Verwerkersovereenkomsten en verwerkersafspraken
Er worden vijf aanbevelingen gedaan door de ADR gericht op CAP en DRZ de aanbevelingen richten zich met name op het beschrijven en verbeteren van het proces van verwerkersovereenkomsten. Concreet worden daar door Financien de volgende maatregelen aan gekoppeld:

- Herzien en aanvullen van de gehanteerde werkinstructies in 2023 waardoor bijvoorbeeld de juistheid en actualiteit van de afgesloten verwerkersovereenkomsten/-afspraken wordt gemonitord. Om deze monitoring te ondersteunen wordt gebruik gemaakt van een risicoregister (KCD-tool). De verkregen inzichten uit KCD worden door de eerste lijn gebruikt om de privacy governance te versterken.
- Om de maatregelen ten aanzien van risico's die voortvloeien uit een DPIA te monitoren en te prioriteren, zijn deze opgenomen in het risicoregister van het risicoregister.
- Vanuit de Belastingdienst worden de verwerkingen met de daaronder hangende verwerkersovereenkomsten opgevoerd in het verwerkingsregister. Gelijktijdig worden ook de procedures herzien. Om dit te borgen wordt ook de verbinding gelegd met al lopende verbeterprogramma's als Herstellen, Verbeteren en Borgen.

Privacycriteria in departementale cloudstrategie
De genoemde aanbevelingen worden opgepakt. Op dit moment wordt het Cloudbeleid herzien op basis van het Rijksbrede cloudbeleid en de implementatierichtlijn cloud zoals toegezegd aan de Tweede kamer. Onderdeel van het inrichten van de implementatierichtlijn is het opstellen en bijhouden van een overzicht van bij Financien in gebruik zijnde clouddiensten zoals bedoeld in het Rijksbrede Cloudbeleid.
Voor wat betreft de inkoop wordt er overleg met de CDI gepland om privacycriteria standaard op te laten nemen in contracten.

Onderzoeksverantwoording

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

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 Persoonsgegevens van het Beraad de rol van gedelegeerd opdrachtgever vervuld.

De contactpersoon en daarmee aanspreekpunt voor dit onderzoek is Persoonsgegevens Persoonsgegevens in rol van Persoonsgegevens Financiën (beleidsdepartement). De Opdrachtnemer namens de ADR is Persoonsgegevens voor de Ministeries van BZK en JenV. Deze opdracht is op 25 oktober 2021 besproken in het vooroverleg CIO-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 (interne) verwerkings-

verantwoordelijke van de geselecteerde verwerkingen. Dit betreft veelal taken die belegd zijn bij de CIO-office of de (concern) privacyoffice van het betreffende departement of de hieronder gesitueerde dienstonderdelen. Bij het ministerie van Financiën waren dit het agentschap Domein Roerende Zaken (DRZ) en de Belastingdienst met dienstonderdeel *Centrale Administratieve Processen* (CAP).

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 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 Cloud strategieën 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 afgestemd, waarna het definitief deelrapport aan de departementale [illegible] 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 [illegible] van het desbetreffende 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, 28 november 2022

Persoonsgegevens

Persoonsgegevens Auditdienst Rijk