Auditdienst Rijk
Ministerie van Financiën

Deelrapport

Rijksbreed AVG-onderzoek 2024
Ministerie van Financiën

Definitief

Titel:	Rijksbreed AVG-onderzoek 2024 – Deelrapport Financiën
Uitgebracht:	5.1.2e CDIO
Datum:	6 augustus 2024
Kenmerk:	2024-0000398189

1. Inleiding

1.1 Aanleiding

De Rijksoverheid verwerkt persoonsgegevens van alle Nederlandse burgers om haar publieke taken uit te voeren. Het verwerken van deze grote hoeveelheid persoonsgegevens gaat gepaard met een grote verantwoordelijkheid om deze persoonsgegevens op een gepaste manier te behandelen en te beschermen. De Algemene Verordening Gegevensbescherming (AVG) is de Europese verordening die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de Europese Unie standaardiseert.

Sinds de AVG op 25 mei 2018 van toepassing is, is de inbedding ervan voor de Rijksoverheid een uitdaging. De afgelopen jaren is de Rijksoverheid meermaals negatief in de publiciteit gekomen met betrekking tot privacy. Omdat datalekken een grote impact hebben op de Nederlandse burger en samenleving, onderkent het Rijk het belang dat er zicht is en blijft op de beheersing van privacyrisico's. Een tekort aan privacybescherming kan nadelige gevolgen hebben voor de persoonlijke levenssfeer van de Nederlandse burger. Ook wordt daardoor de Rijksoverheid geconfronteerd met politiek-bestuurlijke en/of juridische maatregelen, verlies van vertrouwen en beschadiging van imago.

De Auditdienst Rijk (ADR) heeft in 2019, 2020 en 2022 rijksbrede AVG-onderzoeken uitgevoerd waaruit bleek dat de inbedding van de AVG inderdaad nog een uitdaging is, maar ook dat de Rijksoverheid de laatste jaren stappen heeft gezet naar een hoger volwassenheidsniveau. De Nederlandse toezichthoudende autoriteit op het gebied van privacy, Autoriteit Persoonsgegevens (AP), heeft aangegeven de focus te leggen op onder andere de digitale overheid. Aan de ADR is gevraagd om in 2024 wederom een Rijksbreed AVG-onderzoek uit te voeren met als aandachtspunt de inrichting en implementatie van privacy by design & default en de opvolging en monitoring van de resultaten uit Data Protection Impact Assessment (DPIA's).

1.2 Doel

Het doel van dit onderzoek is om bij elk departement inzicht te geven in de stand van zaken over de inrichting en implementatie van privacy by design (ontwerp) & default (standaardinstellingen) en de opvolging en monitoring van de resultaten uit DPIA's. Dit teneinde de departementen in staat te stellen bij te dragen aan de verdere versterking van de privacybescherming binnen het Rijk. Daarnaast is het doel van dit onderzoek om interdepartementaal inzicht te geven in best-practices op het gebied van de twee eerdergenoemde onderwerpen.

1.3 Opdrachtgever en opdrachtnemer

Deze opdracht wordt door de ADR uitgevoerd in opdracht van 5.1.2e namens de leden van het CIO-beraad. Opdrachtnemer namens de ADR is 5.1.2e 5.1.2e . 5.1.2e 5.1.2e 5.1.2e is namens 5.1.2e gedelegeerd opdrachtgever en tevens contactpersoon.

2. Privacy by design & default

2.1 Beleid privacy by design & default

Het ministerie van Financiën beschikt over een privacybeleid en uitgewerkte Enterprise Architectuur Principes waarin de manier waarop privacy by design & default tot uiting komt concreet is beschreven. Daarnaast wordt er gebruik gemaakt van de algemene Handleiding Privacy by Design opgesteld door JenV. Aangegeven is dat de Belastingdienst gebruik maakt van de documentatie van het kerndepartement. Er is op dit moment nog geen Belastingdienst-specifiek privacybeleid en Belastingdienst-specifiek uitgewerkte privacy by design & default-uitgangspunten.

De beschreven privacyprincipes zijn gekoppeld aan de AVG-beginselen en nader uitgewerkt middels processen en technische en organisatorische maatregelen. Op deze manier heeft het ministerie van Financiën beschreven op welke manier privacy vanaf het ontwerp van wetten en daaraan ondersteunende systemen middels standaardinstellingen is geborgd.

Aangegeven is echter dat de manier waarop privacy by design & default wordt gepraktiseerd kan verschillen per directie omdat de eindverantwoordelijkheid is belegd bij de directie zelf en niet op een hoger niveau. Het kan daardoor vanuit de CPO-rol uitdagend zijn om volgens een uniforme standaard toezicht te houden of advies te geven gezien de eindverantwoordelijkheid lager is belegd. Op de beschreven AVG-beginselen vindt op hoger niveau geen expliciete monitoring en controle plaats. Wel komt privacy in brede zin terug in de P&C-cyclus. De P&C-cyclus bestaat uit kwartaalrapportages (VMR's) waarin aandacht wordt besteed aan verschillende privacyaspecten.

Aanbeveling

- Belastingdienst: maak op basis van de beschikbare privacydocumentatie van het kerndepartement een Belastingdienst-specifieke addendum, zodat het nauw aansluit op de processen binnen de Belastingdienst. Zeker gezien het feit dat de eindverantwoordelijkheid is belegd bij de onderliggende directies.
- Kerndepartement: maak privacy by design en default alsmede de AVG-beginselen expliciet onderdeel van de VMR's uit de P&C-cyclus zodat hier centraal meer inzicht in komt.

2.2 Privacy by design & default bij inkoop

Binnen het ministerie van Financiën is de inkoopbevoegdheid ook decentraal belegd bij de directies. Hierdoor beschikt Financiën niet over een centraal beschreven inkoopprocedure. De manier waarop gegevensbescherming wordt meegenomen in de ontwerpfase/inkoopprocedure is niet centraal beschreven. Het kan hierdoor gebeuren dat dienstonderdelen en onderliggende directies op verschillende manieren privacycriteria al dan wel/niet betrekken bij ontwerp of inkoop. Wel is er een portfolioboard waarin alle ICT-projecten worden besproken waar een Projectstartarchitectuur (PSA) verplichte input is. Wij hebben vastgesteld dat in een PSA privacycriteria zijn opgenomen.

Aanbeveling

- Kerndepartement: beschrijf centrale uitgangspunten over de manier waarop privacy en

gegevensbescherming wordt meegenomen in de ontwerpfase/inkoopprocedure.

- Kerndepartement/Belastingdienst: laat de directies die onder het kerndepartement en de Belastingdienst vallen vervolgens een organisatie-specifieke addendum op de centrale inkoopprocedure maken.

3. Data Protection Impact Assessment

3.1 DPIA-proces

Het ministerie van Financiën beschikt over een Procedure Privacy Impact Assessment waarin de uitgangspunten staan beschreven wat betreft het uitvoeren van een DPIA. De Belastingdienst is momenteel het DPIA-proces uit 2020 aan het actualiseren. De ADR heeft in het concept vastgesteld dat middels een RASCI-model de te nemen stappen zijn beschreven. Echter ook op het gebied van DPIA's kan het voorkomen dat ondanks deze procesbeschrijvingen er verschillen kunnen zijn per directie bij het uitvoeren van een DPIA. Wij hebben ook geen brede uitgangspunten aangetroffen op welke manier DPIA's standaard worden meegenomen tijdens het inkoopproces.

Zowel het kerndepartement als de Belastingdienst hebben beschreven dat wanneer waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen bestaat, voorafgaand aan de verwerking een DPIA moet worden uitgevoerd. Wij hebben een steekproef uitgevoerd op zes DPIA's waaruit is gebleken dat bij alle DPIA's het rijksbrede format is gehanteerd en alle benodigde gegevens bevat. Zo benoemt elke DPIA privacyrisico's bij de verwerking alsmede maatregelen die nodig zijn om deze risico's te mitigeren.

Aanbeveling

- Belastingdienst: rond het actualiseren van het DPIA-proces af en draag het Belastingdienst-breed uit onder de verschillende directies.
- Kerndepartement en Belastingdienst: maak het overwegen van een (pre)DPIA standaard onderdeel van een inkoop mits er persoonsgegevens worden verwerkt.

3.2 Overzicht en actualisering DPIA's

Binnen het ministerie van Financiën is de datacoördinator verantwoordelijk voor het opnemen van de DPIA bij de desbetreffende verwerking in het register van verwerkingsactiviteiten. Hier dienen bijvoorbeeld ook verwerkersovereenkomsten te worden opgenomen. Aangegeven is dat er geen centraal overzicht is van DPIA's waarin de status is weergegeven. Gezien de gelimiteerde informatievoorziening rondom DPIA's in het register van verwerkingsactiviteiten, kan het voorkomen dat een DPIA niet tijdig wordt geactualiseerd of herijkt. Aangegeven is dat om mede dit probleem op te lossen gewerkt wordt aan een dashboard (GRC-tool). Dit zou het tijdig actualiseren en herijken van DPIA's moeten vereenvoudigen.

Wij hebben door middel van een steekproef vastgesteld dat alle DPIA's zijn opgenomen in het register van verwerkingsactiviteiten. Eén DPIA is niet herijkt of geactualiseerd ondanks dat dit een DPIA uit 2019 betreft. De andere DPIA's zijn recent van aard waardoor actualiseren op basis van tijd nog niet aan de orde is.

Aanbeveling

- Kerndepartement: maak de DPIA-kalender per directie expliciet onderdeel van de VMR's uit de P&C-cyclus zodat hier centraal meer inzicht in komt.
- Kerndepartement en Belastingdienst: actualiseer ieder kwartaal het overzicht van DPIA's t.b.v. van de VMR's alsmede om zelf inzichtelijk te krijgen of een DPIA geactualiseerd dient te worden.

3.3 Opvolging maatregelen DPIA's

Zowel het kerndepartement van het ministerie van Financiën als de Belastingdienst hebben niet beschreven op welke manier wordt geborgd dat de opvolging van de maatregelen uit de DPIA kan worden aangetoond. Aangegeven is dat de datacoördinator van het onderdeel de opvolging van de maatregelen zou moeten monitoren.

Wij hebben de manier waarop er opvolging is gegeven aan de maatregelen van de zes geselecteerde DPIA's ook niet kunnen vaststellen. In een aantal DPIA's is ook geen duidelijke actiehouder van de maatregel beschreven. Aangegeven is dat de inrichting van en verandering naar het CPO-stelsel tijd kost. Dit heeft tevens zijn uitwerking op de controle & monitoring aangaande privacy i.c.m. de decentraal belegde verantwoordelijkheid.

Aanbeveling

- Kerndepartement en Belastingdienst: beschrijf de manier waarop geborgd wordt dat de maatregelen uit de DPIA's worden uitgevoerd (incl. toekennen actiehouder) alsmede de manier waarop hier controle op wordt gehouden.
- Neem het resultaat hiervan bijvoorbeeld mee in de VMR's zodat er centraal inzicht in is en op gestuurd kan worden.

4. Verantwoording onderzoek

4.1 Object van onderzoek

Het object van onderzoek zijn de beheersingsmaatregelen die een departement in opzet en bestaan heeft getroffen om aan de vereisten uit de AVG te voldoen betreffende privacy by design & default en de opvolging en monitoring van de resultaten uit DPIA's. Hiervoor heeft de ADR onder andere een steekproef uitgevoerd op 6 DPIA's (3 bij het kerndepartement en 3 bij de Belastingdienst) om de opvolging en monitoring van die desbetreffende DPIA's te analyseren. Op basis van de aangetroffen beheersingsmaatregelen hebben wij risico's in kaart gebracht en waar mogelijk voorzien van aanbevelingen.

4.2 Referentiekader

In samenspraak met de opdrachtgever is het referentiekader gebaseerd op de Handreiking Naleving AVG (januari, 2022) (HNA). In deze handreiking zijn uitgangspunten weergegeven, gekoppeld aan de verschillende onderwerpen uit de AVG. De uitgangspunten van privacy by design & default alsmede de opvolging en monitoring van DPIA's vormen de basis van het referentiekader voor dit onderzoek. Het referentiekader is als bijlage opgenomen met daarbij de verwijzing naar de paragrafen in dit departementale deelrapport.

4.3 Rapportage

Dit rapport betreft een departementaal deelrapport met bevindingen en aanbevelingen. Het eindrapport van deze opdracht is een interdepartementaal onderzoeksrapport dat een geaggregeerd beeld geeft van de belangrijkste bevindingen uit het onderzoek. Input hiervoor zijn de departementale deelrapporten uitgebracht aan de 5.1.2e Het interdepartementaal onderzoeksrapport wordt uitgebracht aan 5.1.2e .

Zowel met het interdepartementale rapport als met de departementale deelrapporten wordt geen zekerheid verschaft, omdat geen assurance-werkzaamheden zijn uitgevoerd. De rapporten bevatten daarom geen samenvattende conclusie of eindoordeel.

De opdrachtgever, het CIO-beraad, is eigenaar van het interdepartementale rapport. De 5.1.2e is eigenaar van het departementale deelrapport.

4.4 Openbaarmaking

De ADR is de interne auditdienst van het Rijk. Het rapport over dit onderzoek 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. Bijlage: referentiekader

#	Norm	Referentie	Paragraaf
	Privacy by design & default		
1.1	De organisatie stelt een privacy by design & default beleid op.	HNA 2.4.3	2.1
1.2	De organisatie stelt passende technische en organisatorische maatregelen op met het doel de beginselen van gegevensbescherming gedurende het gehele verwerkingsproces uit te voeren en bewaakt de implementatie van de maatregelen.	HNA 2.4.1	2.1
1.3	Aan de hand van standaardinstellingen, borgt de organisatie dat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor vastgelegde specifieke doel(en)van de verwerking (privacy by default).	HNA 2.4.2	2.1
1.4	De behoeftesteller dient de organisatie te wijzen op de plicht gegevensbescherming mee te nemen in het ontwerp.	HNA 2.4.4	2.2
	Voorbereiding DPIA		
2.1	Een procesbeschrijving is aanwezig voor het uitvoeren van DPIA's.	HNA 7.3.5	3.1
2.2	Het inkoopproces is zo ingericht dat bij de inkoop van diensten of systemen waarbij persoonsgegevens worden verwerkt, standaard een DPIA wordt overwogen.	HNA 7.3.3	3.1
2.3	Wanneer waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen bestaat, in het bijzonder wanneer gelet op de aard, de omvang, de context en de doeleinden nieuwe technologieën worden gebruik, wordt voorafgaand aan de verwerking een DPIA uitgevoerd.	HNA 7.3.1	3.1
	Monitoring DPIA		
2.4	Elke uitgevoerde DPIA wordt in een register opgenomen.	HNA 7.3.6	3.2
2.5	De DPIA wordt minimaal een keer in de drie jaar geëvalueerd en wordt opnieuw uitgevoerd bij grote wijzigingen in het systeem of proces.	HNA 7.3.2	3.2
	Opvolging maatregelen DPIA		
2.6	Er is een procesbeschrijving voor aantoonbaar opvolging te geven aan de aanbevelingen/verbetervoorstellen uit de DPIA's.	HNA 7.3.5	3.3
2.7	Er is aantoonbaar opvolging gegeven aan de beheersmaatregelen en daarbij is een actiehouder aangewezen.	HNA 7.3.7	3.3

Ondertekening

Den Haag, 6 augustus 2024

5.1.2e

5.1.2e Auditdienst Rijk