Auditdienst Rijk
Ministerie van Financiën

Deelrapport

Rijksbreed AVG-onderzoek 2024
Ministerie van Algemene Zaken

Definitief

Titel:	Rijksbreed AVG-onderzoek 2024 – Deelrapport AZ
Uitgebracht:	CIO AZ
Datum:	22 augustus 2024
Kenmerk:	2024-0000424010

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 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 op 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 inzicht te geven in de stand van zaken bij elk departement over de inrichting en implementatie van privacy by design & default en de opvolging en monitoring van de resultaten uit DPIA's. Dit doel 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 CIO-Rijk namens de leden van het CIO-beraad. Opdrachtnemer namens de ADR directeur account BZK/JenV. De voorzitter van de CPO-raad en Privacy Adviseur Rijk (PAR),
is namens de voorzitter van het CIO-beraad gedelegeerd opdrachtgever en tevens contactpersoon.

2. Privacy by design & default

2.1 Beleid en uitgangspunten privacy by design & default

Het ministerie van Algemene Zaken (AZ) hanteert een eigen privacybeleid uit 2019 dat dit jaar wordt geactualiseerd met daarbij de focus op de samenvoeging met de privacygovernance. Momenteel heeft AZ nog niet expliciet beschreven op welke manier privacy by design & default tot uiting komt. Ook dit zal nader worden uitgewerkt in het privacybeleid alsmede de koppeling met de Architectuurbeginselen en AVG-beginselen, waarin vereisten van privacy by design en default expliciet zijn opgenomen.

Door AZ is invulling gegeven aan de AVG-beginselen in het privacybeleid. Apart zijn ook de beginselen doelbinding en dataminimalisatie uitgewerkt in de architectuur principes. Met deze principes worden doelbinding en dataminimalisatie voor het departement tastbaar gemaakt en wordt er ook houvast geboden hoe men in de praktijk dient om te gaan met de AVG-beginselen.

AVG-beginselen komen ook indirect terug in het register van verwerkingsactiviteien en bij de totstandkoming van de verwerkingen. Deze komen wel specifiek terug bij de uitvoering van de DPIA's. Controle en monitoring van de AVG-beginselen zijn door het gebruik van Kritieke Prestatie Indicatoren (KPI's) in opzet beschreven.

Aanbeveling

- Realiseer het voornemen om het privacybeleid te actualiseren en neem de manier hierin op hoe privacy by design en default concreet tot uiting komt binnen AZ. Koppel hieraan tevens de Architectuurbeginselen en AVG-beginselen, waarin vereisten van privacy by design en default expliciet zijn opgenomen.
- Maak de (privacy) architectuur principes nog concreter door middel van het aanbieden van handreikingen met suggesties en voorbeelden van hoe de AVG-beginselen er uit zouden kunnen zien in de standaardinstellingen in een van de (grote) IT-systemen.

2.2 Privacy by Design & Default bij start nieuwe verwerkingen

Zoals eerder vermeld onder 2.1 is er geen documentatie aangetroffen waaruit blijkt op welke manier AZ privacy by design & default hanteert waaronder de manier waarop de organisatie borgt dat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor vastgelegde specifieke doel(en)van de verwerking.

Het rijksbrede inkoopbeleid in combinatie met de uitgewerkte architectuurbeginselen van AZ bieden voor nieuwe producten of diensten in de context van privacy houvast totdat er een eigen inkoopbeleid is opgesteld. Het voornemen is om een inkoopbeleid specifiek voor AZ op te stellen. Tijdens de ontwerpfase/inkoop van nieuwe producten of diensten worden de CPO en CISO betrokken. Dit is mogelijk vanwege het kleinschalige karakter van AZ.

Aanbeveling

- Realiseer het voornemen van het opstellen van een toegespitst inkoopbeleid/-procedure voor de eigen organisatie.

3. Data Protection Impact Assessment

3.1 DPIA-proces

AZ beschikt niet over een eigen – op de organisatie toegespitste – DPIA-procedure en volgt de rijksbrede DPIA-procedure en format. De rijksbrede DPIA procedure, bijbehorend DPIA invulformat in combinatie met pre-scan DPIA vanuit Privacy Adviseur Rijk (PAR) vormen de kern van de instructies waarmee de DPIA's binnen AZ worden gerealiseerd. In de (privacy) governance zijn de rollen voor het uitvoeren (medewerkers AZ), toezicht houden op DPIA's (CIO), adviseren/toezien op de uitvoering (FG) ook belegd.

AZ beschikt niet over een eigen – op de organisatie toegespitste – inkoopbeleid/procedure en volgt het rijksbrede inkoopbeleid. Aangegeven is dat er bij het inkopen van nieuwe producten of diensten altijd een pre-DPIA wordt uitgevoerd. Uitkomsten hiervan worden bijgehouden door de CISO in Plato. Indien uit de pre-DPIA naar voren komt dat er een DPIA moet worden uitgevoerd, is dit het signaal voor de CPO om hier opvolging aan te geven.

Privacyrisico's die zich voordoen tijdens het inkoopproces bij nieuwe diensten en/of systemen worden geborgd door het gebruik van het rijksbrede inkoopbeleid samen met de eigen organisatie architectuur principes. Uit gesprekken met CPO werd duidelijk dat gezien de omvang van het departement, restrisico's tijdens het inkoopproces klein zijn. CPO en CISO zijn betrokken bij het inkoopproces.

Door AZ is in het privacybeleid vastgelegd dat DPIA's doorgaans voorafgaand aan de verwerking en door de PO worden uitgevoerd. DPIA's worden tevens uitgevoerd bij bestaande verwerkingen en waar sprake is van gegevensverwerkingen die een hoog privacyrisico opleveren. Het niveau van risico wordt ingeschat met behulp van risicoanalyses, zijnde de pre-DPIA's. Aangegeven is dat binnen de Rijksoverheid door collectief op te treden, privacyrisico's op een efficiënte wijze kunnen worden geborgd. Hier wordt specifiek verwezen naar de grote DPIA's die Rijksbreed spelen.

De 6 DPIA's die de ADR met een steekproef heeft geselecteerd, zijn allen vastgesteld en actueel. Voor het vaststellen van de DPIA's is gebruikt gemaakt van het rijksbrede DPIA model en mitigerende maatregelen met betrekking tot privacyrisico's zijn beschreven in de DPIA's.

3.2 Overzicht en actualisering DPIA's

Het departement komt haar verantwoordingsplicht na door middel van het DPIA-dashboard. Indien noodzakelijk wordt het DPIA-dashboard geactualiseerd.

Het dashboard dat wordt gehanteerd zorgt voor monitoring op privacyrisico's. Inhoudelijk wordt er in het dashboard de naam verwerking, naam DPIA, status DPIA, omschrijving maatregel, status maatregel en opmerkingen bijgehouden. Op basis van het dashboard wordt er door CPO gerapporteerd aan de CIO.

Gezien de schaal en met name de aard van de verwerkingen staat de termijn voor het herzien van een DPIA momenteel op 4 jaar. AZ is voornemens hier 5 jaar van te maken. Er zijn weinig risicovolle verwerkingen die de burgers raken. Voor de verwerkingen waar dit wel het geval is (risk-based approach), heeft het herzien meer prioriteit en wordt wel de 3 jaar termijn gebruikt of eerder indien er een significante wijziging in de verwerking heeft plaatsgevonden.

Aanbeveling

- Realiseer als aanvulling bij het DPIA-dashboard bijbehorende documentatie over de opzet ervan zodat de volledigheid en actualiteit van de tool kan worden geborgd. Neem hierin een periodieke check mee aansluitend op de rapportage aan de CIO.

3.3 Opvolging maatregelen DPIA's

AZ heeft niet beschreven op welke manier er opvolging wordt gegeven aan de maatregelen uit de DPIA's alsmede de manier waarop hier controle op wordt gehouden. Beheer vindt centraal plaats en monitoring continu en ad hoc naar aanleiding van veranderingen of andere feiten. Het DPIA-dashboard speelt daarin een centrale rol.

De rollen en verantwoordelijkheden met betrekking tot de maatregelen die voortkomen uit de DPIA's zijn niet beschreven. Er wordt aantoonbaar opvolging gegeven aan de maatregelen en voortgang wordt in het DPIA-dashboard gemonitord. Het dashboard is echter enkel toegankelijk voor de CPO, waardoor bij zijn/haar afwezigheid de actualiteit van het dashboard niet gewaarborgd is.

Aanbeveling

- Modificeer het DPIA-dashboard zodanig dat de organisatie en relevante stakeholders inzicht kunnen krijgen in de status van de DPIA, rollen en verantwoordelijkheden met betrekking tot maatregelen en de status van de maatregelen.
- Richt een centrale plek in voor het DPIA-dashboard. Bij afwezigheid van de CPO door onvoorziene omstandigheden kan het dashboard doorlopend geraadpleegd 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 betreft 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 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. 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 departementale CIO. Het interdepartementaal onderzoeksrapport wordt uitgebracht aan CIO-Rijk.

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 departementale CIO 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. 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, 22 augustus 2024

Deelprojectleider Auditdienst Rijk