Auditdienst Rijk
Ministerie van Financiën

Deelrapport

Rijksbreed AVG-onderzoek 2024 Ministerie van Landbouw, Natuur en Voedselkwaliteit (kerndepartement en NVWA)

Definitief

Titel:	Rijksbreed AVG-onderzoek 2024 – Deelrapport LNV (kerndepartement en NVWA)
Uitgebracht:	[redacted] CIO LNV
Datum:	30 september 2024
Kenmerk:	2024-0000464566

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. Aangezien 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 privacy-bescherming 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 is bedoeld om 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 Scope

Bij elk te onderzoeken ministerie wordt gekeken naar privacy by design & default en de opvolging van de resultaten uit DPIA’s bij het kerndepartement en één uitvoeringsorganisatie, in dit onderzoek de Nederlandse Voedsel en Warenautoriteit NVWA.

1.4 Opdrachtgever en opdrachtnemer

Deze opdracht wordt door de ADR uitgevoerd in opdracht van [redacted] CIO-Rijk namens de leden van het CIO-beraad. Opdrachtnemer namens de ADR is [redacted] RA, directeur account AZ/JenV. De voorzitter van de CPO-raad en Privacy Adviseur Rijk (PAR), [redacted] 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 Landbouw, Natuur en Voedselkwaliteit (LNV)[1] beschikt over een privacy beleid waarin staat beschreven dat ze zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens willen bewerkstelligen. Dit houdt in dat vanaf de ontwikkeling van beleid tot aan de uitvoering aandacht moet zijn voor privacy. In het beleidskader 'privacy by design EZK en LNV' zijn privacy by design en default uitgewerkt.

De uitvoeringsorganisatie Nederlandse Voedsel- en Warenautoriteit (NVWA) maakt grotendeels gebruik van de documentatie van het kerndepartement. Daar waar de NVWA qua processen afwijkt van het kerndepartement, worden eigen beschrijvingen en werkinstructies gemaakt en geïmplementeerd. Een voorbeeld hiervan is het recent geïmplementeerde programma SPA (Security, privacy & architecture by design).

Voor zowel LNV als de NVWA zijn kaders, inrichting en de technische en organisatorische maatregelen beschreven in het beleidskader voor privacy by design waarin ook privacy by default aan de orde komt. Dit geldt zowel voor zelfontwikkelde systemen als voor systemen die worden ingekocht. Middels een checklist wordt per privacy by design fase nagegaan hoe er wordt omgegaan met de persoonsgegevens op verschillende privacyaspecten.

Middels de jaarlijkse integrale uitvraag over privacy en IB wordt monitoring toegepast. Aan de hand van deze uitvraag worden aanbevelingen gedaan en wordt in de halfjaarlijkse uitvraag opvolging gemonitord van de aanbevelingen. Bij de NVWA verzorgt de afdeling sturing en risicobeheer deze monitoring. Dit gebeurt nu nog handmatig; de NVWA onderzoekt de mogelijkheid tot het implementeren van een digitaal monitoringsysteem.

Aanbeveling

- NVWA: Realiseer het voornemen om te onderzoeken of er GRC tooling (Kennismonitoring) beschikbaar is om hiermee een volgend volwassenheidsniveau te bereiken

2.2 Privacy by design & default bij start nieuwe verwerkingen

Bij het inkopen van ICT is met leveranciers afgesproken hoe een verwerking wordt vormgegeven, DICTU (Dienst ICT Uitvoering) is verantwoordelijk voor de inkoop van de generieke ICT diensten en middelen. Diensten of producten die organisaties zelf inkopen en die persoonsgegevens verwerken worden beoordeeld door privacy officers van de organisatie zelf voordat wordt overgegaan tot aanschaf.

Voor inkoop passen het kerndepartement en de NVWA de rijksbrede ARVI, ARVODI- en ARBIT-processen[2] toe. Ook gebruikt de NVWA de ICO Wizard - bio-overheid om een set van informatiebeveiligingseisen samen te stellen indien relevant bij inkopen en aanbestedingen.

[1] Ten tijde van het onderzoek was dit de naam van het ministerie dat inmiddels het ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur (LVVN) heet

[2] Algemene Rijksinkoopvoorwaarden c.q. voor diensten en bij IT-overeenkomsten

3. Data Protection Impact Assessment

3.1 DPIA-proces

Het ministerie van LNV beschikt over een procesbeschrijving van het DPIA-proces. De procesbeschrijving dateert uit 2021, echter is aangegeven dat in september 2024 een herziening zal gaan plaatsvinden.
De NVWA heeft een eigen DPIA-procedure met werkinstructie. Er is aangegeven dat de eigen DPIA-procedure met werkinstructie meer handvaten voor de werknemers geeft.

Indien er ICT wordt ingekocht voert het privacy team van het kerndepartement een QuickScan uit. Op basis hiervan wordt advies gegeven om wel of niet door te gaan met het traject van inkoop o.b.v. informatiebeveiligings- en privacyvereisten.
Bij de NVWA is een afdeling die bij inkoop van ICT systemen nauw samenwerkt met de inkooporganisatie en dan bepaalt of er een verwerkers-overeenkomst nodig is. Verder maakt de NVWA ook gebruik van Quick Scans Privacy (QSP) om te bepalen of het uitvoeren van een DPIA noodzakelijk is.

Zowel het kerndepartement als NVWA hanteren het rijksbrede DPIA-model. Bij NVWA wordt voor het invullen van dit model de QSP als hulpmiddel gebruikt, omdat er vrij veel specifieke kennis nodig is om het rijksbrede DPIA-model te vullen. Niet elke proceseigenaar beschikt over deze kennis en de QSP leidt de invuller wat makkelijker en meer concreet door de materie heen.

Aanbeveling

- Concern CIO-office: Realiseer het voornemen om het DPIA-proces te herzien in 2024 zodat niet alleen het kerndepartement zelf, maar ook alle andere gebruikers, zoals uitvoeringsorganisaties, gebruik kunnen maken van een actuele procesbeschrijving.

3.2 Overzicht en actualisering DPIA's

Binnen het ministerie van LNV draagt de privacyregisseur zorg voor het bijhouden van een departementaal register van DPIA's en QuickScans. Het kerndepartement herziet de DPIA's, risicogericht, elke drie jaar.

De NVWA heeft aangegeven dat de DPIA's centraal worden opgeslagen bij de CIO-office. De DPIA's worden niet opgenomen in het AVG-verwerkingenregister, maar er wordt gewerkt met verwijzingen. Dit heeft ermee te maken dat proceseigenaren, die voor actualisatie van hun eigen DPIA's moeten zorgen, geen toegang hebben tot het AVG-register. NVWA kent een kwaliteitssysteem waarbij zaken zoals informatiebeveiliging en privacy zijn opgenomen in een Kennismonitor. De afdeling sturing en risicobeheer coördineert welke proceseigenaar wanneer, welke actie moet uitvoeren.

Aangezien de verwerkingen van de NVWA ten tijde van het actualiseren worden ingetrokken, zijn deze momenteel niet in het AVG-register terug te vinden. De NVWA verwacht deze actualisatie in oktober 2024 afgerond te hebben.

Aanbeveling

- NVWA:
  - continueer de actualisatie van het AVG-register.
  - zoek een oplossing voor het toegankelijk blijven van de DPIA's voor de proceseigenaren.

3.3 Opvolging maatregelen DPIA's

Het ministerie van LNV heeft aangeven bezig te zijn met het implementeren van een risico-register om de doorvoering van de maatregelen te monitoren. Momenteel vinden zij zelf het opvolgen van aanbevelingen c.q. implementeren van maatregelen en de monitoring hiervan door het kerndepartement nog onvoldoende.

De afdeling sturing en risicobeheer bij de NVWA monitort ook de opvolging van maatregelen uit DPIA's en QSP's. Deze maatregelen, n.a.v. onderkende risico's, worden vastgelegd in een risicobehandelplan waarvoor de proceseigenaar heeft getekend.

Aanbeveling

- Kerndepartement:
  - Stel een actiehouder aan en leg een einddatum vast per beheersmaatregel.
  - Monitor de opvolging en implementatie van de maatregelen voortvloeiend uit de DPIA's.
  - Leg dit vast in een centraal register.

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 voor wat 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 3 DPIA's van het kerndepartement en 3 van de uitvoeringsorganisatie 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, 30-09-2024

[redacted]

[redacted]

Projectleider Auditdienst Rijk