NEDERLANDS
REGISTER
GERECHTELIJK
DESKUNDIGEN

Jaarverslag Privacy compliancy

Functionaris voor Gegevensbescherming

2022-2023

Inhoud

Managementsamenvatting

Rechtdoen aan de belangen van alle betrokkenen, vraagt continu om zorgvuldige afwegingen en het steeds opnieuw zoeken naar een passende balans.

De in het vorig jaarverslag genoemde trend van meer digitaal werken heeft zich doorgezet, ook bij het NRGD. Zo is de afgelopen jaren ingezet op verdere digitalisering van het werkproces voor registratie en herregistratie. Tijdens de doorontwikkeling is met toepassing van de privacybeginselen van privacy by design en dataminimalisatie geconcludeerd het NRGD in de uitvoering van de werkzaamheden minder persoonsgegevens hoeft vast te leggen.

Het NRGD werkt met deskundigen en toetsers van over de hele wereld. Per betrokken land buiten de Europese Unie moet de privacy officer beoordelen of sprake is van een passend beschermingsniveau van de privacy. Zo konden Amerikaanse toetsers de afgelopen jaren de ene keer wel en een andere keer niet worden ingezet. In juli 2023 heeft de Europese Commissie geoordeeld dat gegevens weer veilig kunnen worden doorgegeven.

Het NRGD heeft aandacht voor privacybewust werken door zowel de eigen bureaumedewerkers als de toetsers en externe medewerkers. In 2023 hebben Bureaumedewerkers de AVG-cursus Zilver gehaald. Voor toetsers en externe medewerkers is gebruik gemaakt van (ondertekening van) de nieuwe integriteitsverklaring om privacybescherming nog eens extra onder de aandacht te brengen.

Ook in de afgelopen periode had het NRGD slechts een enkel verzoek i.v.m. inzage van een betrokkene te behandelen, verder was het aantal incidenten zeer beperkt in aantal en omvang.

In het nu uitgevoerde self-assessment bevindt het NRGD zich op niveau drie, één niveau hoger dan de vorige keer.

Inleiding

Het voorliggende jaarverslag beschrijft de belangrijkste privacy compliancy aandachtsgebieden voor het NRGD uit de periode 2022-2023. Het verslag kan dienen als een in onafhankelijkheid gegeven derdelijns beoordeling in de zin van de AVG.[1]

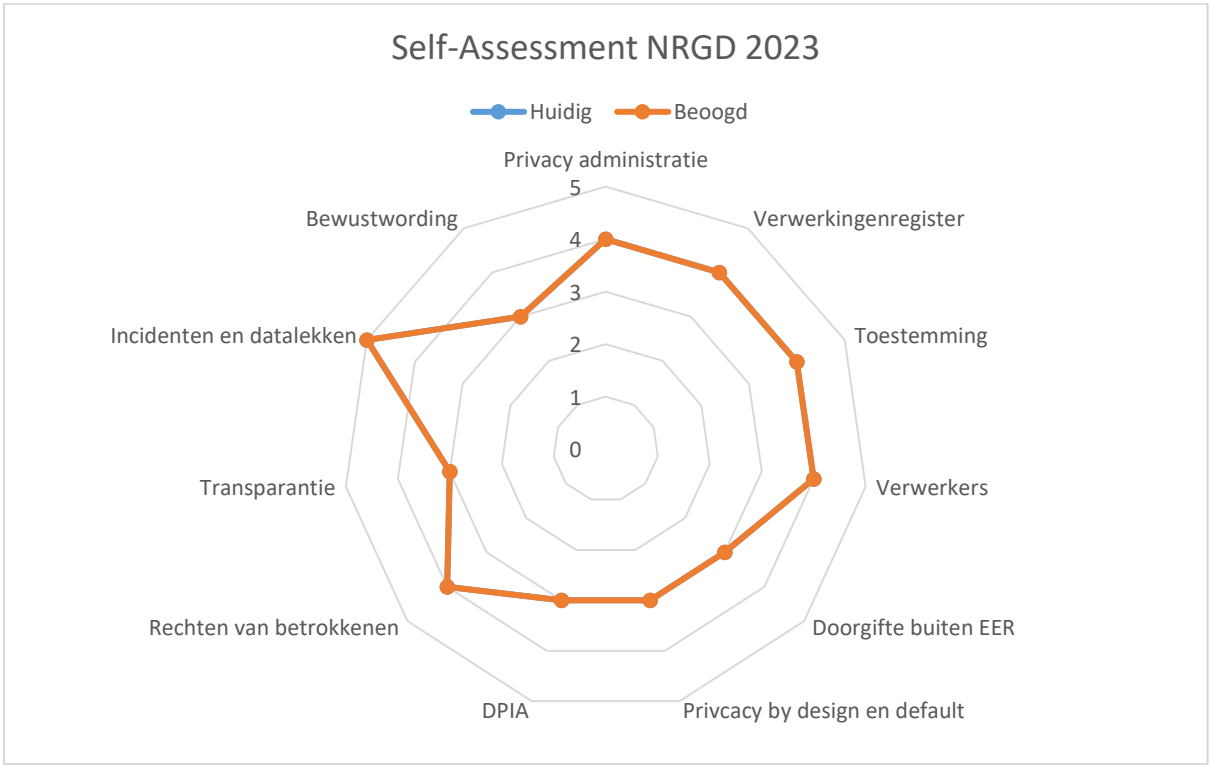
[1] Artt. 37-39 AVG.

1 Self-Assessment

Het NRGD heeft een self-assessment uitgevoerd en gebruikt hiervoor het model dat in samenwerking met o.a. het ministerie van Justitie en Veiligheid tot stand is gekomen.[2] Met behulp van de prestatie-indicatoren maakt een organisatie zichtbaar waar zij zichzelf plot in de omgang met persoonsgegevens, of en zo ja welke groei is gepland en wat dat van de organisatie vraagt. De indicatoren bieden inzicht in de wijze waarop vorm wordt gegeven aan de naleving van de privacy en maakt deze aantoonbaar. Deze sturingsinformatie biedt aanknopingspunten voor overleg, bijvoorbeeld tijdens het bureau-overleg of aan de bestuurstafel.

In het gebruikte model wordt gewerkt met vijf niveaus. Voor de score van het huidige niveau van een KPI, wordt het niveau gekozen waarop de organisatie zich op het moment van invullen bevindt. Een hoger niveau wordt bereikt als *alle* elementen binnen een KPI zich op datzelfde hogere niveau bevinden. In het nu uitgevoerde self-assessment bevindt het NRGD zich op niveau drie, een niveau hoger dan de vorige keer. Binnen de overheid wordt niveau drie gezien als een passend, minimaal volwassenheidsniveau voor privacy-compliancy.

Belangrijker nog is dat het NRGD vanuit de eigen missie en visie bepaalt wat het voor de organisatie passende volwassenheidsniveau is.



In bovenstaande afbeelding is het huidige niveau gelijk aan het beoogde niveau, waardoor de blauwe lijn niet zichtbaar is.

[2] Privacymanagement KPI's JenV, versie november 2021.

2 Ontwikkelingen

Onderstaand enkele relevante, NRGD gerelateerde, ontwikkelingen uit de afgelopen periode.

Aandachtsgebieden Autoriteit Persoonsgegevens (AP)

De AP is de nationale onafhankelijke toezichthouder die de privacybescherming bevordert en bewaakt. De AP werkt risicogestuurd en richt zich op onderwerpen met een groot risico voor betrokkenen. De digitaliserende overheid is een terugkerend focusgebied met daarbinnen wisselende aandachtsgebieden. De afgelopen jaren waren databeveiliging en samenwerkingsverbanden belangrijke aandachtsgebieden. Het NRGD heeft de afgelopen periode ingezet op verdergaande digitalisering en databeveiliging van de primaire werkprocessen: registratie en herregistratie van deskundigen. Naast inperking van risico's op datalekken heeft dit ook geleid tot minder vastleggen van persoonsgegevens, doordat tijdens de doorontwikkeling opnieuw kritisch is gekeken naar de werkprocessen.

Transparantie

In 2022 zijn Kamervragen[3] gesteld over het bestaan en beschikbaar stellen van DPIA's. Het onderwerp is door de FG's van KleinLef uitgebreid besproken. Vanwege mogelijke risico's die aan openbaarmaking van (delen van) een DPIA kleven is een zorgvuldige afweging van te beschermen belangen noodzakelijk. De FG's hebben dan ook geadviseerd om niet zonder meer over te gaan tot openbaarmaking van een DPIA en dat overwogen zou kunnen worden om een samenvatting te publiceren.

De AP heeft in 2023 openbare registers die persoonsgegevens bevatten onder de loep genomen, omdat afwegingen over openbaarheid die in het verleden zijn gemaakt, door technologische ontwikkelingen nu anders kunnen uitvallen. Bewindspersonen zijn aangeschreven om "per openbaar register dat persoonsgegevens bevat, te laten analyseren of wordt voldaan aan alle eisen die zien op de grondslag voor het bestaan van een openbaar register, geschiktheid van openbaarmaking van persoonsgegevens gezien het doel van dat openbare register en noodzaak tot openbaar zijn van gegevens uit dat openbare register."
Het deskundigenregister van het NRGD is zo'n openbaar register. De FG is achteraf geïnformeerd over de uitvraag en afhandeling door het NRGD. Deze casus is gebruikt om nadere afspraken te maken over het (eerder) betrekken van de FG bij onderzoeken en (informatie)verzoeken van derden. Bijvoorbeeld bij uitvragen via de CPO of Privacy Board van het ministerie van Justitie en Veiligheid en de AP.

Uitbreiding werkterrein en gegevens uitwisseling derde landen

Zowel in 2022 als in 2023 zijn nieuwe (sub)deskundigheidsgebieden opengesteld en is het aantal ingeschreven (internationale) deskundigen en toetsers uitgebreid.

De Algemene Verordening Gegevensbescherming (AVG) beschermt persoonsgegevens binnen de Europese Unie. Worden gegevens elders opgeslagen, dan is dat op grond van de AVG alleen toegestaan als dit derde land een 'passend beschermingsniveau' biedt. Bij toetsers en deskundigen van buiten de Europese Economische Ruimte (EER) moet het NRGD beoordelen of er sprake is van een derde land met een passend

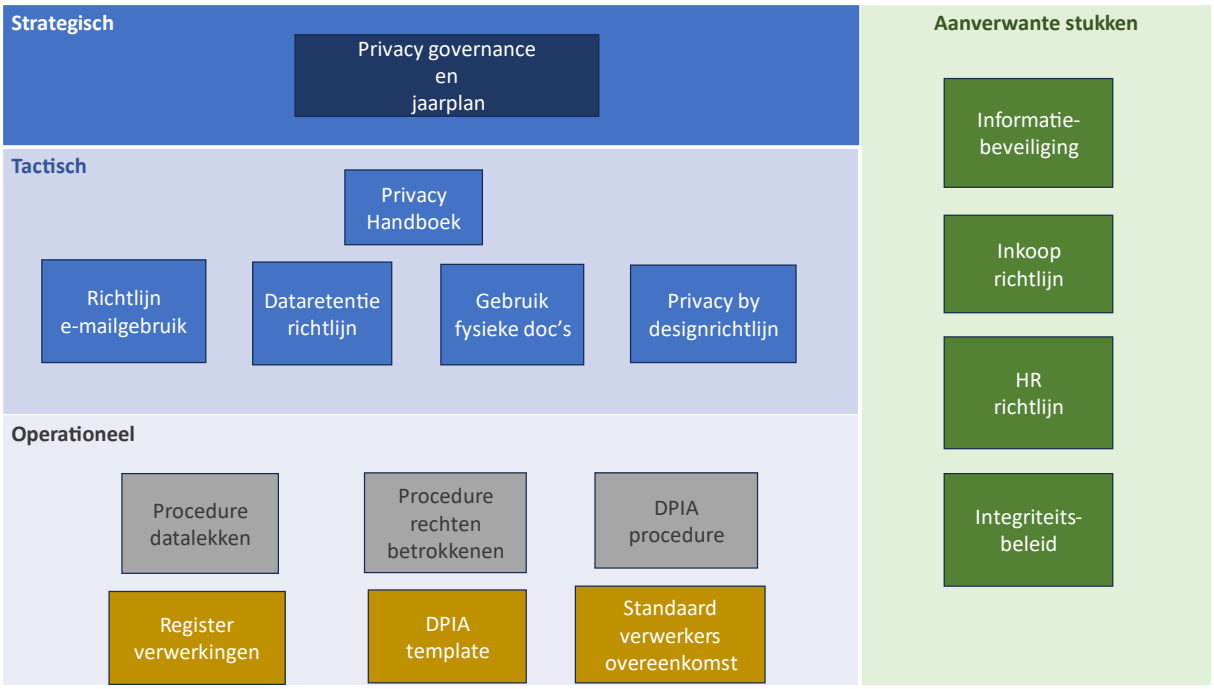
[3] Zijn er op ICT-systemen en het verwerken van data bij u en/of bij uitvoeringsorganisaties Privacy Impact Analyses (PIA) of Gegevensbeschermingeffectbeoordelingen (GEB) uitgevoerd in 2021? Kunt u deze rapportages aan de Kamer sturen?

beschermingsniveau. Heeft de Europese Commissie bijvoorbeeld een adequaatheidsbesluit afgegeven voor dat land? Dan is sprake van een met de AVG vergelijkbaar niveau van gegevensbescherming. Is er geen adquaatheidsbesluit voor een bepaald land, dan moeten er extra acties ondernomen worden om de persoonsgegevens te beschermen, bijvoorbeeld door gebruik te maken van een door de Europese Commissie vastgesteld modelcontract.

Vervolgens moet gemonitord worden of een land blijvend voldoet aan het passende beschermingsniveau. De afgelopen jaren, sinds de uitspraak Schrems II, was veilige uitwisseling met personen en organisaties in Amerika niet mogelijk. In juli 2023 heeft de Europese Commissie een nieuw adequaatheidsbesluit genomen, op grond waarvan gegevens tussen de EU en Amerika veilig kunnen worden doorgegeven. Gevolg hiervan is dat het NRGD nu weer toetsers uit Amerika kan inzetten.

3 Privacy administratie

3.1 Privacybeleid en Governance



Samenhang beleidsdocumenten

Begin 2022 heeft het NRGD een eigen privacy beleidskader vastgesteld, daarvoor werd gewerkt met een beleidskader van het ministerie van Justitie en Veiligheid.

3.2 Verwerkingenregister

Voor het vastleggen van de verwerkingen houdt het NRGD een register bij in een extern, binnen de rijksoverheid, belegde tool. De betrouwbaarheid van de gegevensopslag bleek te wensen over te laten. Zo heeft een externe de naam van de FG kunnen wijzigen. Bij controle van een deel van het register door de FG bleek een afwijkend adres bij de contactpersoon te staan. Het NRGD heeft besloten om te stoppen met het gebruik van deze externe tool.

Gelet op de beperkte omvang van processen waarbinnen persoonsgegevens worden verwerkt is het NRGD voornemens om voortaan met een eigen format te werken.

Toestemming

Binnen het NRGD wordt alleen voor de toezending van de nieuwsbrief gebruik gemaakt van de grondslag toestemming.

3.3 DPIA's en (pre)DPIA-register

Om goed grip op privacy te krijgen moet privacy vanaf de start worden meegenomen, of het nu gaat om een nieuw project, wetgeving of een ICT-inkooptraject. Dat kan op verschillende manieren. Bijvoorbeeld door Privacy by design/default toe te passen, maar ook door voorafgaand aan iedere nieuwe verwerking van persoonsgegevens een risico-analyse uit te voeren, een zogenoemde pre-DPIA (Data Protection Impact Assessment). Volgt daaruit een waarschijnlijk hoog risico voor de rechten en vrijheden van betrokkenen, dan moet er een reguliere DPIA uitgevoerd worden. Uiteraard kan ook, zoals bij het NRGD, eigener beweging gekozen worden voor het uitvoeren van een reguliere DPIA.

Het uitvoeren van een DPIA kan bewerkelijk zijn. Soms kent het opstellen van een DPIA een langere doorlooptijd vanwege capaciteitsbeperkingen. De (tijdige) totstandkoming van een DPIA, de DPIA als werkproces, behoeft aandacht zo blijkt uit het overgelegde DPIA-register. Met name het afhechten van de DPIA en het vastleggen van het aansluitend monitoren van risico's en maatregelen is nog een aandachtspunt.

4 Incidenten en datalekken

Bij een datalek gaat het om een inbreuk op persoonsgegevens. Afhankelijk van de omstandigheden van het geval moet een datalek, binnen 72 uur, gemeld worden bij de AP en eventueel ook aan betrokkenen. Als verwerkingsverantwoordelijke is het NRGD verplicht een incidentenregister bij te houden.

In de periode 2022 - 2023 zijn twee meldingen opgenomen in het incidentenregister, waarvan één is beoordeeld als beveiligingsincident en één als niet meldingsplichtig datalek. Het is de bedoeling om in de vergadertool te werken met geanonimiseerde zaaksrapporten. De gelakte persoonsgegevens bleken na uploaden toch zichtbaar gemaakt te kunnen worden. Door de betreffende documenten voorafgaand aan het uploaden op een andere manier op te slaan is dit probleem verholpen.

In het register is niet vermeld op welke datum en tijdstip een melding is afgehandeld. Daardoor is niet duidelijk of de 72-uurs termijn gehaald zou zijn mocht een incident toch meldingsplichtig blijken. Een volledige registratie levert waardevolle informatie voor de evaluatie van incidenten en de (periodieke) evaluatie van het ingerichte werkproces.

Het is belangrijk om in de bewustwordingssessies blijvend aandacht te besteden aan: wanneer spreek van je van een datalek en hoe te handelen. Dit geldt ook voor de door het NRGD ingezette toetsers en 'medewerkers' die niet in loondienst zijn van het NRGD.

5 Transparantie

De AVG verlangt van het NRGD dat het betrokkenen informeert over de verwerking van persoonsgegevens. In sommige gevallen moet dit nog vóór de betrokkene zijn

persoonsgegevens doorgeeft. Het aanmelden voor de NRGD-nieuwsbrief is AVG-compliant ingericht.

De privacyverklaring is een middel om aan betrokkenen uit te leggen hoe het NRGD met persoonsgegevens omgaat en hoe zij gebruik kunnen maken van hun rechten. Het NRGD heeft een externe privacyverklaring, gepubliceerd op de eigen website.

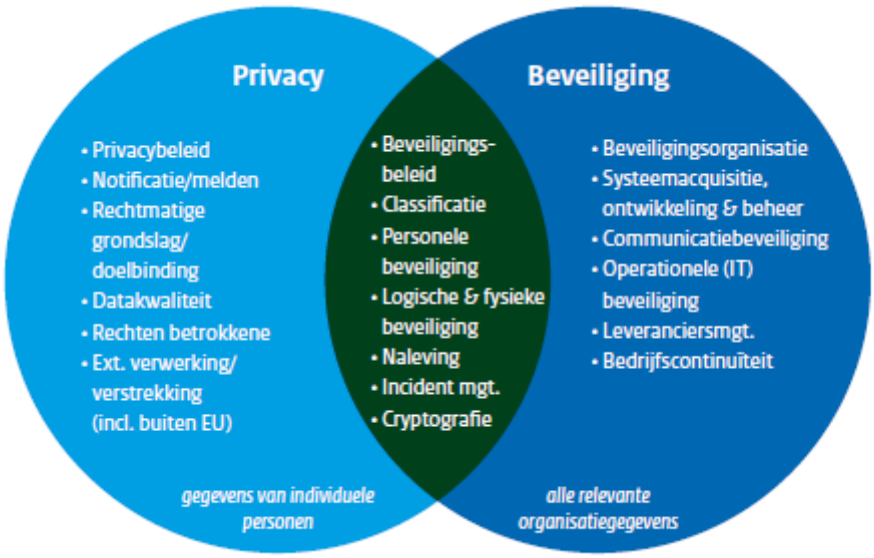
De interne privacyverklaring ontbreekt nog steeds. Het gegeven dat het merendeel van de verwerkingen van interne betrokkenen via P-direkt loopt doet niet af aan het feit dat het NRGD onder eigen verwerkersverantwoordelijkheid gegevens van interne betrokkenen verwerkt en dat betrokkenen hierover op transparante wijze (lees via interne privacyverklaring) geïnformeerd moeten worden.

6 Rechten van betrokkenen

Het NRGD heeft in de periode 2022-2023 één verzoek om inzage in persoonsgegevens ontvangen en één verzoek tot verwijderen van persoonsgegevens. Beide verzoeken zijn tijdig afgehandeld.

7 Informatiebeveiliging en AVG

Het NRGD is verantwoordelijk voor het nemen van passende technische en organisatorische maatregelen om te kunnen waarborgen en aan te tonen dat de verwerkingen van persoonsgegevens in overeenstemming zijn met de AVG. Steeds verdergaande digitalisering maakt dat op dit punt van de overheid veel wordt verwacht, niet in de laatste plaats door de AP.



Bovenstaande afbeelding maakt inzichtelijk wat onder (informatie)beveiliging en privacy valt en waar ze elkaar raken.

8 Privacybewust werken en opleiden

Het NRGD is aangesloten op het programma Weerbaar JenV, dit programma maakt het mogelijk om aan te tonen dat medewerkers daadwerkelijk worden getraind. Ook vinden er periodiek phishing-acties plaats om de alertheid t.a.v. veilig en privacybewust werken te testen en te bevorderen.

In de periode 2022-2023 hebben medewerkers nauwelijks gebruik kunnen maken van het e-learning programma door technische problemen. Ondanks herhaalde verzoeken heeft het bijna twee jaar geduurd voordat het probleem is verholpen. De privacy officer heeft aangegeven dat eind 2023 alle medewerkers de AVG-cursus Zilver hebben gehaald.

De privacy en de security officer worden maandelijks van actualiteiten op het gebied van privacy en security voorzien door de FG.

Via het samenwerkingsverband KleinLef nemen medewerkers van het NRGD deel aan de AVG-werkgroep en de CIO/CISO-werkgroep. Het NRGD maakt gebruik van een FG uit de pool van KleinLef. De FG neemt daarnaast deel aan FG-overleggen van onder meer de Manifestgroep. KleinLef, Manifestgroep en de Rijksbrede Benchmark Groep zijn op hun beurt weer aangesloten op het Netwerk van Publieke Dienstverleners (NPD). De groepen delen in toenemende mate kennis en informatie met elkaar. Voor kleinere organisaties als het NRGD zijn dergelijke vormen van samenwerking onontbeerlijk.

In 2023 heeft het NRGD een nieuwe integriteitsverklaring voor toetsers en externe medewerkers vastgesteld. In het kader van het bevorderen van privacy bewustzijn is de nieuwe verklaring ook door huidige toetsers en externe medewerkers ondertekend.

9 Tot slot

Tot slot de belangrijkste aandachtspunten en aanbevelingen op een rij.

Maak werk van een privacyverklaring voor interne betrokkenen, leg uit welke gegevens het NRGD van hen verwerkt en waarom etc.

Door organisatie en Privacy Office dient blijvend gewerkt te worden aan het verder op orde brengen van de (werk)processen en het consequent toepassen ervan. Hecht processen af, leg e.e.a. goed vast en zorg voor ‘onderhoud en beheer’. Dit geldt bijvoorbeeld voor de DPIA’s en het monitoren van de daaruit voortvloeiende risico’s en maatregelen.

Betrek de FG eerder bij onderzoeken en informatieverzoeken van derden met raakvlakken met privacybescherming.

Ella Schepel
Functionaris voor Gegevensbescherming NRGD