Jaarrapportage bescherming persoonsgegevens 2025

OMGEVINGSDIENST REGIO UTRECHT

Colofon

Titel	Jaarrapportage bescherming persoonsgegevens 2025
Versie	1.0
Status	definitief
Datum	9 maart 2026
Aantal pagina's	6
Auteur	Functionaris Gegevensbescherming
Contactpersoon	Functionaris Gegevensbescherming
ODRU	Archimedeslaan 6, 3584 BA Utrecht
Copyright	© Omgevingsdienst regio Utrecht

opgesteld door	Functionaris Gegevensbescherming
beoordeeld door	directeur ODRU
besproken door	dagelijks bestuur 19 maart 2026
ter informatie aan	algemeen bestuur 9 april 2026
kenmerk	ODUTR-1565642653-71656

Inhoud

1. Inleiding

De Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg) leggen de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat zij voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht levert de organisatie een belangrijke bijdrage aan de bescherming van persoonsgegevens. Dit betekent dat de omgevingsdienst moet kunnen aantonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en Wpg: rechtmatigheid, transparantie, doelbinding en juistheid. De formele verantwoordelijkheid hiervoor ligt bij het Dagelijks Bestuur van de omgevingsdienst.

De Functionaris voor Gegevensbescherming (FG) ziet als onafhankelijke interne toezichthouder bij de omgevingsdienst toe op de naleving van de wet- en regelgeving rond de bescherming van persoonsgegevens. De AVG, de Uitvoeringswet AVG (UAVG) en de Wpg vormen de wettelijke basis voor het toezicht door de FG.

De FG rapporteert jaarlijks over zijn bevindingen aan het dagelijks bestuur van de omgevingsdienst. Voor de AVG is dit verankerd in het privacybeleid van de organisatie; voor de Wpg is dit een wettelijke verplichting. Er bestaat geen nadere regelgeving die exact bepaalt wat in een jaarrapportage moet worden opgenomen. Het is daarom van belang om duidelijk af te bakenen op welke bevindingen de rapportage betrekking heeft.

Het jaar 2025 was voor de omgevingsdienst geen regulier jaar. In 2026 staat een fusie gepland, waardoor in 2025 veel aandacht uitging naar organisatorische voorbereidingen, herinrichting van processen en harmonisatie van beleid. Daarnaast is eind 2025 de adviseur informatiebeveiliging en privacy vertrokken, waardoor continuïteit en capaciteit tijdelijk onder druk hebben gestaan. Deze jaarrapportage is daarom opgesteld op basis van de beschikbare informatie en is tot stand gekomen met inhoudelijke input van zowel de CISO als de FG.

2. Samenvatting

De FG stelt een jaarrapportage op voor de AVG en Wpg. Daarin staan de bevindingen voor wat betreft de bescherming van persoonsgegevens, de verantwoording van de wijze waarop het toezicht door de FG invulling heeft gekregen en aanbevelingen voor de verdere bescherming van persoonsgegevens.

3. Het toezicht door de Functionaris Gegevensbescherming

De toezichtwerkzaamheden van de FG richten zich op diverse waarborgen en verplichtingen. Ter uitvoering van de toezichttaak hanteert de FG verschillende instrumenten en methoden voor het waarnemen en verzamelen van informatie, het afwegen en beoordelen van de verwerkingen en het opstellen van bevindingen, conclusies en aanbevelingen.

De wettelijke taken en bevoegdheden van de FG zijn opgenomen in artikel 39 van de AVG en artikel 36 Wpg. Daarin is opgenomen dat de FG erop toeziet dat binnen de organisatie de regels van de AVG en de Wpg worden nageleefd.

4. Bevindingen met betrekking tot de AVG en WPG

Algemene bevindingen en fusie

In 2025 zijn alle relevante informatiebeveiligings- en privacydocumenten van zowel ODRU als RUD Utrecht beoordeeld met het oog op de vorming van Omgevingsdienst Utrecht (ODU). Daarbij is systematisch gekeken welke documenten reeds voldoen aan de benodigde eisen, welke documenten ontbreken en welke opnieuw moeten worden opgesteld om aan te sluiten bij de toekomstige organisatie en het gewenste normenkader.

Op basis hiervan is een overzicht en plan van aanpak opgesteld waarin per document is aangegeven:
– welke documenten van ODRU of RUD Utrecht geschikt zijn voor gebruik binnen ODU,
– welke documenten nog ontbreken,
– welke documenten herziening of volledige herontwikkeling nodig hebben.

Alle bestaande documenten die onderdeel uitmaken van het framework, inclusief de documenten afkomstig van RUD Utrecht, zijn opgenomen in de map Overdracht Anouk onder framework. Deze map vormt daarmee de centrale verzamellocatie voor de huidige documentatie en de uitgangspositie voor de verdere ontwikkeling van het ODU-brede informatiebeveiligings- en privacyframework.

Specifieke bevindingen

In deze volgende paragraaf wordt nader ingegaan op een aantal bevindingen in 2025.

Privacy mailbox

In 2025 is de privacy-mailbox actief beheerd. De mailbox werd dagelijks gecontroleerd en binnengekomen vragen zijn waar nodig behandeld. Hoewel de instroom beperkt was, blijft frequente monitoring van belang om tijdig op privacygerelateerde verzoeken en signalen te kunnen reageren. Complexere of inhoudelijk gecompliceerde vragen zijn via Informatiemanagement doorgezet naar de CISO voor verdere behandeling. De privacy-mailbox is volledig up-to-date; alle historische berichten zijn verwerkt en correct opgenomen in de betreffende postvakken.

Bewustwording

Voor het zorgvuldig omgaan van de medewerkers met persoonsgegevens is bewustzijn van groot belang. Dat blijkt ook uit de rest van deze rapportage waaronder bijv. het geringe aantal geregistreerde datalekken.

Rechten van betrokkenen

Informatievoorziening is een belangrijk recht van betrokkenen. In 2025 is één inzageverzoek binnengekomen en deze is succesvol afgehandeld. Daarnaast is er één melding van een medewerker binnengekomen omtrent een mogelijk onterechte verwerking van persoonsgegevens. Na onderzoek van de CISO en FG is dit afgehandeld.

Geregistreerde datalekken

In 2025 zijn meerdere incidenten gemeld door zowel medewerkers als externe partijen. Dit gebeurt soms direct bij de FG, CISO of een andere medewerker van ODRU. Daarnaast vinden meldingen plaats in de privacy mailbox. In 2025 zijn twee incidenten ook daadwerkelijk geclassificeerd als datalek. Dit ging om een verkeerd verzonden mail en een gecompromitteerde LinkedIn account van een medewerker. Beide geval zijn onderzocht en bestempeld als datalek. Op basis van deze incidenten zijn de nodige maatregelen genomen. Een melding aan de Autoriteit Persoonsgegevens was niet nodig.

5. Aanbevelingen

Op basis van de uitgevoerde beoordelingen en de bevindingen in 2025 zijn vijf verbeterpunten en aanvullingen onderkend die van belang zijn voor de verdere professionalisering richting de ODU.

1. Uniformeren en actualiseren van het IB- en privacyframework

Hoewel het documentatieoverzicht van de ODRU en RUD is opgesteld en gebundeld in de map Overdracht Anouk, blijkt dat meerdere documenten nog ontbreken of niet volledig aansluiten op de toekomstige situatie binnen ODU. Het framework dient in 2026 verder te worden geharmoniseerd, geactualiseerd en aangevuld zodat één consistent en organisatiebreed stelsel ontstaat.

2. Structurele borging van de privacy-mailbox

De privacy-mailbox is in 2025 goed beheerd en volledig opgeschoond. Voor 2026 is het belangrijk dit structureel te borgen, zodat monitoring – waaronder het tijdig signaleren van risico's – niet afhankelijk is van specifieke personen. Het proces rondom doorgeleiding van complexe casuïstiek naar de CISO/FG dient vastgelegd te worden.

3. Versterken van bewustwording en opleiding

Hoewel het lage aantal datalekken positief is, laten de meldingen zien dat voortdurende bewustwording essentieel blijft. Het is wenselijk om in 2026 extra aandacht te geven aan gerichte trainingen, onboarding-instructies en periodieke communicatie over veilig en zorgvuldig omgaan met persoonsgegevens.

4. Formalisering van processen rond rechten van betrokkenen

De afhandeling van het inzageverzoek en de melding over een mogelijke onterechte verwerking in 2025 laat zien dat het proces functioneert. Wel is het nodig om dit proces voor ODU te borgen, inclusief duidelijke verantwoordelijkheden, termijnen en documentatie-eisen.

5. Verbeteren van het meldproces incidenten en datalekken

In 2025 zijn twee incidenten als datalek geclassificeerd. Meldingen kwamen via verschillende kanalen binnen (direct bij FG/CISO of via medewerkers). Voor ODU is het wenselijk om het meldproces verder te standaardiseren, inclusief een eenduidig meldpunt, duidelijke instructies voor medewerkers en centrale registratie. Dit versterkt de traceerbaarheid, de kwaliteit van analyses en de consistentie van opvolging.