Jaarverslag 2025
Functionaris voor de Gegevensbescherming (FG)
RUD Utrecht

Januari 2026

Betsie Panjer

Inhoud

Samenvatting

Met de invoering van de Algemene Verordening Gegevensbescherming (AVG) in 2018 is bij de RUD Utrecht per 1 april 2019 is de huidige Interne Functionaris voor de Gegevensbescherming benoemd voor zowel de AVG als de Wet politiegegevens (Wpg) door het Dagelijks Bestuur van de RUD Utrecht.

Met dit jaarverslag wordt er gelijktijdig verantwoording afgelegd en gedocumenteerd welke werkzaamheden de FG het afgelopen jaar heeft uitgevoerd om de organisatie te begeleiden in het voldoen aan de privacywetgeving.

Het algemene beeld van de mate waarin de RUD Utrecht voldoet aan de AVG en WPG is dat de RUD Utrecht voldoet aan de AVG en Wpg. Er zijn echter enkele duidelijke aandachtspunten voor de RUD Utrecht, en volgend jaar de Omgevingsdienst Utrecht, om te blijven voldoen aan de AVG en WPG.

Op een aantal aspecten scoort de RUD Utrecht naar het oordeel van de FG nog een onvoldoende:

- Het altijd melden van datalekken;
- Het herkennen van phishing mails;
- Het niet anonimiseren van stukken die naar buiten gaan.

Voor 2026 adviseert de FG de Omgevingsdienst Utrecht, buiten alle documenten die aangepast moeten worden voor de nieuwe Omgevingsdienst Utrecht (ODU), aandacht te besteden aan de boven genoemde punten. De FG zal naast deze punten in 2026 ook de volgende onderwerpen actief volgen: de relatie met audit/control en nieuwe Europese regelgeving (ePrivacy verordening, NIS2, Wet modernisering elektronisch bestuurlijk verkeer (Awb) 2023, AI Act). Voor deze onderwerpen is het van belang dat hierop tijdig en gestructureerd wordt geacteerd om ook in de toekomst aan vereisten uit wet- en regelgeving te kunnen blijven voldoen.

Inleiding

Met dit jaarverslag wordt er gelijktijdig verantwoording afgelegd en gedocumenteerd welke werkzaamheden de FG het afgelopen jaar heeft uitgevoerd om de organisatie te begeleiden in het voldoen aan de privacywetgeving. Daarbij moet worden opgemerkt dat door de beperkte capaciteit en alle extra werkzaamheden in het kader van de fusie minder tijd is besteed aan de taken van de FG dan wenselijk was.

In het kort omvat de taak van de FG het informeren en adviseren van de werknemers van de RUD Utrecht inzake hun verplichtingen, het uitoefenen van toezicht op naleving van de AVG, advisering met betrekking tot de uitvoering van data protection impact assessment (DPIA) en het onderhouden van contacten met de Autoriteit Persoonsgegevens (AP). De FG voert zijn dagelijkse werkzaamheden uit met beperkte ondersteuning van een jurist van de RUD Utrecht. De verantwoording zoals in dit jaarverslag is verwoord gaat in op het algemene beeld van de compliance ten aanzien van de AVG en Wpg, de uitgevoerde activiteiten en opgeleverde producten, de bevindingen over het jaar 2025 en de aandachtspunten voor 2026. Het jaarverslag van de FG wordt aangeboden aan het Dagelijks Bestuur van de RUD Utrecht omdat zij eindverantwoordelijk is voor de verwerking van de persoonsgegevens. Het Dagelijks Bestuur dient niet alleen kennis te nemen van het jaarverslag maar ook besluiten te nemen over de aandachtspunten voor 2026. Daarnaast kan het Dagelijks Bestuur het jaarverslag ter informatie aanbieden aan het Algemeen Bestuur en indien gewenst het publiceren op de website van de RUD Utrecht.

Bewustwording

Het is en blijft belangrijk om medewerkers regelmatig te stimuleren en scherp te houden ten aanzien van privacygevoelige zaken.

Op Viadesk (intranet) en via de mail is er regelmatig aandacht geweest voor privacygevoelige zaken. Het ging hierbij voornamelijk wijzen op bijv. Phishingmails en de procedure voor het melden van Datalekken. Bij de introductie van nieuwe medewerkers wordt hier ook aandacht aan besteed door middel van een kleine pubquiz.

Met het invoeren van teamdagen, na de corona periode, probeert de FG op wisselende dagen aanwezig te zijn op de werkvloer. Aanwezigheid op de werkvloer triggert medewerkers toch eerder om vragen te stellen of juist bij een datalek dit (alsnog) te melden. Gelukkig weten medewerkers de FG via mail of telefoon goed te vinden.

Continu aandacht voor kwetsbaarheden

We moeten continu aandacht hebben voor kwetsbaarheden in onze IT-omgeving. Gelukkig kunnen we daarbij steunen op de expertise die via de samenwerking met ICT Houten voor ons beschikbaar is. Het samenwerkingsverband met ICT Houten maakt namelijk gebruik van een zogenaamde SOC (Security Operations Center) van ASAPCloud. Zij monitoren onze omgeving continu op 'gebeurtenissen' die risicovol zouden kunnen zijn. Indien nodig wordt er ingegrepen. Bijvoorbeeld door inlog-account (tijdelijk) te blokkeren. Daarnaast is er aandacht voor het 'patchen' van componenten in onze IT-omgeving. Patchen betekent dat kwetsbaarheden middels een nieuwe release van software of firmware (op hardware) worden opgelost.

De mens is de zwakste schakel

Feit is dat de medewerker het grootste risico vormt voor de veiligheid van onze informatie. Dat heeft alles te maken met hoe medewerkers omgaan met hun toegang tot onze IT-omgeving. Klikken op een 'hyperlink' in een phishingmail is natuurlijk al een gevaar. Uit de bovenstaande onderzoeken blijkt dat er toch nog regelmatig door een medewerker op een link wordt geklikt. Om de bewustwording te vergroten hebben we afgelopen jaar weer een "nep"phishing mail gestuurd naar, ihkv de fusie, zowel medewerkers van de RUD als de Odru. Uit de uitkomsten blijkt dat dit ook komend jaar de nodige aandacht verdiend.

Aantallen	**RUD**	**ODRU**	**Totaal**
Mails	249	301	550
Geklikt op link	67 (27%)	42 (14%)	109 (20%)
Gegevens ingevoerd	28 (11%)	20 (7%)	48 (9%)

Adviezen

Door de FG heeft een aantal adviezen uitgebracht ten aanzien van de volgende onderwerpen:

- verwerkersovereenkomsten

- interne audits in het kader van de Wpg

- externe Wpg audit

- advies op de DPIA voor het gebruik van Bodycams

- advies opstellen dataleverings- en uitwisselingsovereenkomsten

- vragen van medewerkers

- bewustwording en toelichting bij de bijeenkomsten voor nieuwe medewerkers.

Datalekken

Er zijn in 2025 7 datalekken gemeld waarvan 2 naar aanleiding van de "nep"phishing mail, dat is wel erg weinig en daar zal ook komend jaar meer aandacht voor moeten zijn. Medewerkers zullen meer bewust gemaakt moeten worden van wat een datalek is en dat ze deze moeten melden. Hiervoor zijn in het verleden meerdere acties ondernomen om medewerkers hierop te attenderen Met de aangeschafte annonimiseringtool kan het niet geanonimiseerd sturen van documenten voor een groot deel worden ondervangen.

Wet Politiegegevens (Wpg)

De WPG en Besluit politiegegevens buitengewoon opsporingsambtenaren (Bpg boa) is voor de RUD van toepassing omdat zij BOA's in dienst heeft en de werkzaamheden van de BOA's vallen onder werking van de WPG en meer specifiek de Bpg boa. Voor de BOA's bij de RUD geldt dat zij onder twee regimes vallen, nl. voor het "gewone" toezicht vallen zij onder de AVG maar voor hun werkzaamheden als opsporingsambtenaar vallen ze onder de Wpg.

In de Wpg is vanaf 2021 de verplichting opgenomen om jaarlijks een interne audit en 1 x in de vier jaar een externe audit uit te voeren. De externe audit is afgelopen jaar eer uitgevoerd. Deze is met goed gevolg afgesloten. De RUD Utrecht heeft 3 medewerkers die interne audits uitvoeren. Zij hebben een audit plan opgesteld en de interne audit uitgevoerd. Zij hebben zich met name gericht op de naleving van de protocollen uit het kwaliteitshandboek BOA.

Toezicht

Afgelopen jaar is er, door gebrek aan tijd, geen prioriteit gegeven aan de procedures uit het toezichtplan. Komend jaar zullen een aantal processen beoordeeld worden door mee te draaien met de interne audits.

Verzoeken om inzage

Er is één verzoek gedaan om inzage in beelden die gemaakt zijn met de bodycam verder zijn er geen verzoeken voor inzage, rectificatie en of verwijdering bij de RUD Utrecht ingediend.

Verwerkingsovereenkomsten

Er zijn in 2025 daar waar nodig nieuwe verwerkingsovereenkomsten afgesloten. Dit heeft ook voornamelijk te maken met de fusie waar nieuwe contracten zijn of moeten worden afgesloten. De FG heeft hierbij geadviseerd.

Data Protection Impact Assessments (DPIA's)

DPIA's zijn een goed hulpmiddel bij het beoordelen of er sprake is van risico's en voor het bepalen van daartoe adequate maatregelen. Een DPIA is verplicht wanneer er 'waarschijnlijk sprake is van een hoog risico voor de rechten en vrijheden van natuurlijke personen' (AVG art 35). Ook is er door de Autoriteit persoonsgegevens een lijst uitgegeven wanneer een DPIA verplicht is. Om te kunnen bepalen of er een DPIA moet worden uitgevoerd is er door het onafhankelijke Europese adviesorgaan WP29 een richtsnoer uitgegeven. Deze stelt dat 'In gevallen waarin het niet duidelijk is of een DPIA vereist is, deze toch uit te voeren omdat het de verwerkingsverantwoordelijke helpt om aan de wetgeving te voldoen.

In 2025 is er één DPIA uitgevoerd voor het gebruik van Bodycams voor onze BOA's.

Privacy-by-design en privacy-by-default

Waar DPIA's inzicht geven in nodige maatregelen rond verwerkingen zijn deze twee aspecten vooral bedoeld om bij het procesontwerp privacyaspecten als dataminimalisatie en opslagbeperkingen (beginselen AVG art 5)

standaard mee te nemen. Ook dienen standaardinstellingen van een programma, app, website, dienst of apparaat zodanig zijn dat maximale privacy wordt betracht. Hier wordt bij de uitvoering voldoende aandacht aan besteed.

Toekomstige ontwikkelingen

Binnen Europa wordt er niet stil gezeten op het gebied van privacyregelingen. De ontwikkelingen op dit gebied zullen nauwgezet worden gevolgd zodat wij als organisatie op de hoogte blijven van eventuele nieuwe regelgeving waar wij aan moeten voldoen zoals bijv. NIS2, AI Act en Wet modernisering elektronisch bestuurlijk verkeer (Awb) 2023.

Overige waarnemingen

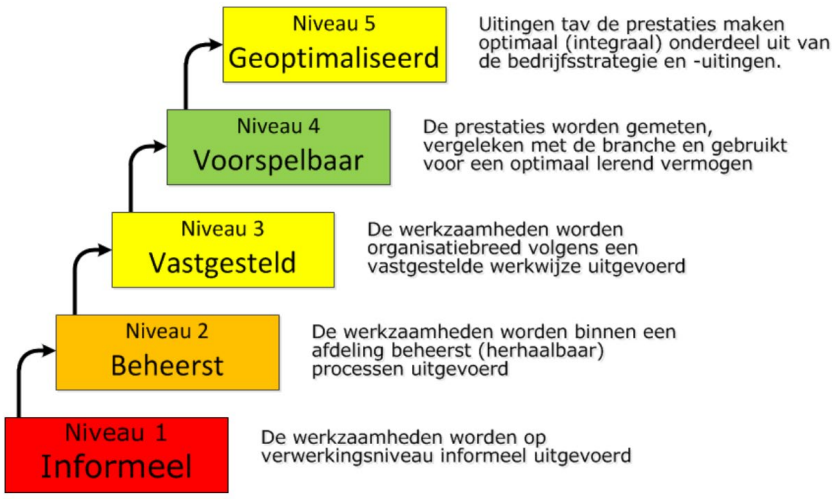
De RUD Utrecht is een kleine organisatie met beperkte capaciteit voor de uitvoering van de werkzaamheden van de FG. De FG wordt beperkt ondersteunt door een jurist die zich op privacy gebied heeft ingewerkt. Door de beperkte capaciteit is het niet altijd mogelijk voor de FG om haar taak volledig en zorgvuldig uit te voeren. Ook het komende jaar zal de capaciteit nog beperkt zijn met het oog op de ontwikkeling van de nieuwe Omgevingsdienst Utrecht. De verwachting is dat in de nieuw organisatie meer capaciteit vrijkomt om de privacy taken beter uit te kunnen voeren.

Aanbevelingen voor ODU

Voor de nieuwe organisatie beveelt de FG een tweetal zaken aan:

1. Eind 2026 een self assessment CIP uit te voeren om te kijken wat het volwassenheidsniveau van de ODU is.

Het CIP heeft een systeem beschreven van verschillende volwassenheidsniveaus met de bijbehorende maatregelen om de volwassenheid van een organisatie op het gebied van privacy te beschrijven. Dit systeem helpt organisaties te groeien naar het volwassenheidsniveau dat past bij de visie en de missie van de organisatie ten aanzien van de privacybescherming. Er worden 5 volwassenheidsniveaus onderscheiden, grofweg van geen of versnipperde aandacht voor privacy, tot perfecte organisatie brede beheersing en benutting van de privacybescherming. Een niveau geeft daarbij de mate aan, waarin de 'organisatie van privacy' is gesystematiseerd en geïnternaliseerd in de organisatie.



Het CIP geeft aan dat op voorhand niveau 3 een redelijk volwassenheidsniveau is voor organisaties die persoonsgegevens verwerken. Het is doorgaans voldoende om de compliance-toets te doorstaan en het is ook een niveau dat voor grotere en kleinere organisaties alleszins haalbaar is.

Voor de ODU is het doel om in de komende jaren door te groeien naar volwassenheidsniveau 3. Binnen de ODU worden veel persoonsgegevens verwerkt van burgers, bedrijven en personeel. Waarbij ook gevoelige of bijzondere persoonsgegevens zijn, zoals personeelsgegevens, camerabeelden en strafrechtelijke gegevens. Te werken naar volwassenheidsniveau 3 is daarmee voor nu proportioneel.

Aandachtspunten voor 2026

Actie	Wanneer
Aanpassen beleidstukken en protocollen etc. voor de ODU-organisatie	Q1
De aandachtpunten en verbeterpunten die voortvloeien uit de externe en interne BOA audit	doorlopend
Uitvoeren van een interne audits	Q2 en Q3
Blijvende aandacht voor bewustwording van medewerkers	continue
Self assessment CIP uitvoeren	Eind 2026
Medewerkers opleiden in AI-geletterdheid	2026