Jaarverslag 2024
Functionaris voor de Gegevensbescherming (FG)

Januari 2025

Betsie Panjer

Inhoud

Samenvatting

Met de invoering van de Algemene Verordening Gegevensbescherming (AVG) in 2018 is bij de RUD Utrecht tijdelijk een externe Functionaris voor de Gegevensbescherming benoemd voor de AVG. 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 op de goede weg is om volledig te gaan voldoen aan de AVG en Wpg. Er zijn echter enkele duidelijke aandachtspunten voor de RUD Utrecht om volledig te kunnen 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 niet anonimiseren van stukken die naar buiten gaan.

Voor 2025 adviseert de FG de RUD Utrecht aandacht te besteden aan de boven genoemde punten. De FG zal naast deze punten in 2025 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). 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.

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 2024 en de aandachtspunten voor 2025. 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 2025. 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.

Adviezen

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

- verwerkersovereenkomsten

- interne audits in het kader van de Wpg

- uitvoering en advies op de DPIA voor het zaaksysteem

- advies op de DPIA voor het gebruik van Bodycams

- opstellen generieke dataleveringsovereenkomst

- vragen van medewerkers

- bewustwording en toelichting bij de bijeenkomsten voor nieuwe medewerkers.

Datalekken

Er is in 2024 1 datalek gemeld, dat is wel erg weinig en daar zal dit 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. Het betreft dan met name dat stukken naar buiten gaan die niet geanonimiseerd zijn. Er is in 2024 eindelijk een annonimiseringtool aangeschaft. Hiermee 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 staat voor 2025 weer op de rol.

Begin 2024 heeft nog een herbeoordeling van de in 2022 gehouden externe audit. 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. De interne audit heeft zich dit jaar met name gericht op de nog openstaande aanbeveling uit de in Q1 gehouden herbeoordeling van de externe audit. Tevens hebben zij zich gericht op het kwaliteitshandboek BOA. In het eerste kwartaal van 2025 zal er weer een verplichte externe audit worden uitgevoerd.

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 zijn geen verzoeken voor inzage, rectificatie en of verwijdering bij de RUD Utrecht ingediend.

Verwerkingsovereenkomsten

De RUD Utrecht werkt met een eigen standaard verwerkingsovereenkomst. Er zijn in 2023 zijn daar waar nodig nieuwe verwerkingsovereenkomsten afgesloten. Ook is er in het afgelopen jaar een generieke dataleveringsovereenkomst opgesteld in samenwerking met de privacy officer van de provincie. Dit omdat er steeds meer vragen kwamen om data/gegevens die door de RUD Utrecht worden verzameld te delen met opdrachtgevers. 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 2024 zijn er twee DPIA's uitgevoerd, Een voor de vergunningverlening en toezicht procedures uit het zaaksysteem en één 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 Dit vindt nog nauwelijks aantoonbaar plaats.

Toekomstige ontwikkelingen

Binnen Europa wordt er niet stil gezeten op het gebied van privacy regelingen. 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 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 beperkt zijn met het ook op de ontwikkeling van één nieuwe omgevingsdienst voor de hele provincie Utrecht waar de RUD en de ODRU in opgaan. De verwachting en de hoop is dat in de nieuw organisatie meer capaciteit vrijkomt om de privacy taken beter uit te kunnen voeren.

Aandachtspunten voor 2025

Actie	Wanneer
Organiseren en uitvoeren externe WPG audit	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