Jaarverslag 2022
Functionaris voor de Gegevensbescherming (FG)

Maart 2023

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 uitvoeren van interne audits voor de Wpg;
- Het altijd melden van datalekken;
- privacy-by-design en privacy-by-default standaard als uitgangspunt hanteren;
- De aandachtspunten uit de externe Wpg audit.

Voor 2023 adviseert de FG de RUD Utrecht aandacht te besteden aan de boven genoemde punten. De FG zal naast deze punten in 2023 ook de volgende onderwerpen actief volgen: de relatie met audit/control en nieuwe Europese regelgeving (ePrivacy verordening). 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 2022 en de aandachtspunten voor 2023. 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 2023. 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 maar ook de hoe ga je om met privacy op de thuiswerkplek.

Door de coronacrisis is de signaalfunctie en toegankelijkheid op de werkvloer zeer beperkt geweest. Met het invoeren van teamdagen 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.

Adviezen

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

- verwerkersovereenkomsten

- zoeken interne auditor in het kader van de Wpg

- opstellen intern auditplan

- uitvoering van DPIA voor de wildcamera's, dashcams en drone

- aanschaf anonimiseringstool

- vragen van medewerkers

Datalekken

Er zijn in 2022 2 datalekken 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.

Een van de datalekken betrof het meezenden van een niet geanonimiseerd document met een WOB verzoek. Hiervan is melding gemaakt bij de Autoriteit Persoonsgegevens (AP) en aan betrokkene.

Het andere datalek is gemeld door een medewerker die per ongeluk een CV had meegestuurd. Dit is in overleg met de ontvanger opgelost en niet gemeld bij de AP.

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.

Omdat de RUD nog geen gekwalificeerde interne auditors heeft is er in 2021 gestart met een externe pre-audit en definitieve audit. Daarvoor is Duijnborgh Audit b.v. ingehuurd.

De eerste externe audit is in maart 2022 afgerond en ingediend bij de AP. De tekortkomingen zijn het niet uitvoeren van interne audits, geen jaarverslagen van de FG en het niet beschikbaar hebben van een geformaliseerd toezicht plan (FG). De rest van het jaar is gebruikt om deze tekortkomingen op te lossen.

Toezicht

Afgelopen jaar is een toezichtplan opgesteld. (zie bijlage) Naar aanleiding hiervan is een inventarisatie gedaan welke processen er zijn en hoe we deze in een cyclus van 5 jaar kunnen vastleggen. Welke processen dan als eerste onder de loep worden genomen zijn de processen met het hoogste risico op privacy inbreuken.

Verzoeken om inzage

Er zijn geen verzoeken voor inzage, rectificatie en of verwijdering bij de RUD Utrecht ingediend. Wel is er een procedure beschrijving gemaakt hoe om te gaan als dergelijke verzoeken worden ingediend.

Verwerkingsovereenkomsten

De RUD Utrecht werkt met een eigen standaard verwerkingsovereenkomst. Er zijn in 2022 geen nieuwe verwerkingsovereenkomsten afgesloten.

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 PIA vereist is', deze toch uit te voeren omdat het de verwerkingsverantwoordelijke helpt om aan de wetgeving te voldoen.

Mede naar aanleiding van de Wpg audit is eind 2022 gestart met een DPIA voor het gebruik van dashcams en wildcamera's. Deze zullen begin 2023 worden afgerond.

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 gewerkt aan een voorstel voor de ePrivacy-verordening dit is na de invoering van de AVG het sluitstuk van de inspanningen van de Europese Commissie om het kader voor gegevensbescherming in Europa te voltooien. De verordening bevat regels om de privacy bij online communicatie beter te waarborgen. Het uitgangspunt daarbij is dat de inhoud van deze berichten alleen toegankelijk is voor de partijen die direct bij de communicatie betrokken zijn. Op dit moment is er nog geen datum waarop deze verordening van kracht wordt.

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. Het verdient dan ook aanbeveling om de mogelijkheid te onderzoeken of er formatie is voor het aanstellen van een Privacy Officer, eventueel samen met de Odru. Hierbij moet wel worden aangemerkt dat de markt voor Privacy Officers op dit moment erg moeilijk is gezien de grote vraag.

Aandachtspunten voor 2023

Actie	Wanneer
De aandachtpunten en verbeterpunten die voortvloeien uit de externe en interne BOA audit	doorlopend
Het afronden van DPIA's: Dashcams en wildcamera's,	Q2
Uitvoeren DPIA's zaaksysteem en gebruik drones.	Q2 en Q3
Het uitvoeren van privacy-by-design en privacy-by-default voor de ontwikkeling van app's	Q3
Opzetten en uitvoeren van een intern audit	Q2
Aanpassen toezicht plan van FG	Q2
Blijvende aandacht voor bewustwording van medewerkers	continue