

# Concern Directie

## Bespreekstuk

6 november 2019  
V. Roozen

Concerndirectie

**Gegevens steller:**

Matthijs Mulder

E: jm.mulder@rotterdam.nl

T: [REDACTED]

## Agendapunt < nummer\* >. 4<sup>e</sup> Rapportage Functionaris Gegevensbescherming

### 1. Aanleiding tot bespreking

Hierbij bied ik u de vierde rapportage van de Functionaris Gegevensbescherming (FG) aan. In de vorige rapportage, van 26 juni 2019, werd duidelijk dat het register van verwerkingen alle prioriteit moest hebben. Dat is grotendeels gelukt. Waar staan we nu, drie maanden later? Welke punten verdienen de komende tijd de volle aandacht?

### 2. Afgestemd met cluster

- o BCO: - [REDACTED], Privacy Officer (hierna: PO) en Concern Privacy Officer
- o Directie veiligheid: [REDACTED], PO
- o DV: [REDACTED] PO
- o MO: [REDACTED], PO
- o SO: [REDACTED], Strategisch adviseur/PO
- o SB: [REDACTED], PO
- o W&I: [REDACTED], [REDACTED] – [REDACTED] PO
- o Middelen & Control, [REDACTED]

Daarnaast is deze notitie afgestemd met de stuurgroep Privacy en Awareness (hierna: de stuurgroep). Deze stuurgroep wordt voorgezeten door de directeur Concernstaf & Strategie.

### 2. Gevraagde beslissing

Aan de concerndirectie wordt gevraagd om:

- è de conclusies en actiepunten uit deze notitie te onderschrijven en hier binnen de clusters blijvende inzet en aandacht voor te organiseren.

De belangrijkste punten zijn:

- Het op tijd melden van datalekken en deze evalueren;
- Bij nieuwe processen Privacy by Design als verplicht onderdeel toepassen;
- Aandacht voor het volledig maken en houden van het register van verwerkingen;
- Verwerkersovereenkomsten afsluiten met externe verwerkers;

- De behandeltermijn van aanvragen in het kader van 'rechten van betrokkenen' verkorten.

In het bijgevoegde dashboard ziet u de stand van zaken van dit moment.

### 3. Toelichting

#### *Waar staan we nu?*

Het is mooi om te kunnen rapporteren dat er ten opzichte van vorig jaar flinke vooruitgang is geboekt om te kunnen voldoen aan de AVG. Waar het de wettelijk verplichte instrumenten betreft zijn we nu een stuk verder dan een jaar geleden. Het register van verwerkingen is grotendeels op orde, datalekken worden steeds vaker gemeld en er worden DPIA's uitgevoerd. Ook is een plan van aanpak van de CPO waarin de acties om verder compliant te worden concreet zijn uitgewerkt.

Helaas voldoen we nog niet op alle onderdelen aan de AVG en dat geeft reden tot zorg. Zo blijken de bewaartermijnen niet in alle gevallen gehandhaafd te (kunnen) worden, en is autorisatiebeheer niet in alle gevallen op orde. Daardoor kan het zijn dat te veel mensen toegang hebben tot gevoelige gegevens. Ook logging blijkt niet overal adequaat te zijn doorgevoerd.

Een belangrijke adviesrol ligt bij de Privacy Officers, maar deze relatief nieuwe functie heeft nog niet de vanzelfsprekende positie in de organisatie die het zou moeten hebben.

#### *Handhaving AP*

Daarnaast is handhaving door de AP reëel geworden en zijn de eerste boetes uitgedeeld. Dit geeft ook behoorlijke reputatieschade. Ook de gemeente Rotterdam is geconfronteerd met de AP, een voorbeeld is het opvragen van het datalekkenregister, het hierna genoemde onderzoek naar Smart Cities en het systematisch monitoren van gemelde datalekken. Tot slot weten ook steeds meer burgers de AP en de FG te vinden met meldingen over kwesties waarbij wij niet aan de AVG zouden voldoen.

#### *Register van verwerkingen*

Het belangrijkste speerpunt voor de zomer was het register van verwerkingen.

Het is daarom goed om te zien dat het verwerkingenregister voor bijna alle verwerkingen zoals die door de clusters zijn aangeleverd op orde is. Om dat te bereiken is een enorme inhaalslag gemaakt met een mooi resultaat. We hebben nu als gemeente niet alleen een verantwoordingsinstrument dat voldoet aan de AVG, maar ook, nog belangrijker, een sturingstool. Helaas zijn er nog 41 verwerkingen onvolledig. Dit zijn voor een groot deel verwerkingen (met vaak gevoelige gegevens) in regionaal verband en/of gezamenlijke verwerkingen door meerdere clusters, waarover nog geen afstemming is hoe dit moet worden aangepakt. Hier wordt een groot risico gelopen.

#### *Verwerkingsovereenkomsten.*

Het register geeft inzicht of er bij een verwerking een externe verwerker is betrokken en of een verwerkingsovereenkomst al of niet aanwezig is. In dat geval dient alsnog een verwerkingsovereenkomst te worden afgesloten. Nog steeds ontbreken de

verwerkersovereenkomsten bij veel verwerkingen, dit komt ook omdat hier in het verleden minder aandacht voor was.

In het dashboard staat een cijfermatige weergave, waarbij wordt opgemerkt dat verschillende verwerkingen gebruik maken van dezelfde applicatie en er in dat geval maar één verwerkingsovereenkomst hoeft te worden afgesloten. In het plan van aanpak wordt voorzien in een inventarisatie in november van alle nog af te sluiten verwerkingsovereenkomsten.

#### *Ontwikkelingen in datatechnologie: Privacy by Design*

De technologie neemt een enorme vlucht als het gaat om het slimme gebruik van data, zoals bijvoorbeeld Smart City. Ontwikkelingen die de gemeente in staat stellen de burger nog beter te bedienen en bedrijfsprocessen te verbeteren en zo onder meer de veiligheid op straat of de mobiliteit te verbeteren. Maar dat geeft ook nieuwe risico's, zoals de waarborgen voor persoonsgegevens.

Dat ook de AP hier zorgen over heeft blijkt uit een brief van 8 oktober 2019 waarin de gemeente wordt gevraagd mee te werken aan een onderzoek naar Smart City toepassingen en de waarborgen voor het gebruik van persoonsgegevens. Het is zaak om privacy aan de voorkant mee te nemen in deze ontwikkelingen. Bovendien staan er serieuze boetes op het niet voldoen aan de AVG bij nieuwe ontwikkelingen, zoals het achterwege laten van een verplichte DPIA, voorafgaand aan een risicovolle verwerking.

#### *DPIA's*

Een ander belangrijk speerpunt in het plan van aanpak is om vòòr mei 2021 voor alle bestaande risicovolle verwerkingen een DPIA uit te voeren. In een DPIA wordt beoordeeld of de privacyrisico's voldoende zijn afgedekt.

Belangrijke stappen zijn gezet bij het cluster Werk en Inkomen. Daar zijn nu reeds de 25 meest risicovolle bestaande verwerkingen door middel van een DPIA doorgelicht. Hieruit kwamen meer dan 200 verbeterpunten naar voren die planmatig worden doorgevoerd. Door voortvarend de privacy risico's van een verwerking in beeld te brengen, voorkomen we dat we onbewust blijven van de risico's op het gebied van de AVG.

#### *Datalekken vaak te laat*

Nog steeds neemt het aantal datalekken toe. Enerzijds kan dit komen door een toegenomen bewustzijn, anderzijds laat het ook de kwetsbaarheid zien van de gemeente.

Zorgelijk is dat teveel datalekken te laat worden gemeld bij de AP. Zo zijn er dit jaar 101<sup>1</sup> lekken bij de AP gemeld, waarvan 29 lekken niet binnen de wettelijke termijn van 72 uur. Dat is ernstig, niet alleen omdat snel maatregelen nodig zijn om het lek te dichten en de betrokkenen te waarschuwen, maar ook omdat de AP heeft aangekondigd hier strenger op te gaan handhaven. Daarnaast hebben wij als gemeente ook een belang om op een volwassen manier met datalekken om te gaan. Dit leidt tot daadwerkelijke verbetering van processen en vergroot het vertrouwen van de burger. In het protocol datalekken is opgenomen dat elk datalek moet worden geëvalueerd, daarin kan vastgelegd worden wat we geleerd hebben van het datalek en welke maatregelen we nemen. Dit sluit ook aan bij een aanbeveling van de AP die adviseert om corrigerende

---

<sup>1</sup> Peildatum 28 oktober

maatregelen altijd vast te leggen in het datalekregister. Tevens stelt de AP voor om de maatregelen mee te nemen in de plan-do-check/learn-act cyclus.

Het aantal datalekken verschilt per cluster, dit kan te maken hebben met de hoeveelheid klantcontacten per email en brief. Maar ook met de mate van awareness, waardoor een datalek eerder ontdekt wordt.

De grootste groep datalekken zijn nog steeds e-mails en brieven (met vaak gevoelige gegevens) die bij verkeerde ontvangers terechtkomen. In veel gevallen zijn deze door zorgvuldigheid te vermijden.

#### *Rechten van betrokkenen*

De behandelingstermijn van AVG aanvragen van burgers (*rechten van betrokkenen*) loopt wat in ten opzichte van het eerste half jaar. Er is dus verbetering, maar nog steeds loopt 30% van de aanvragen over de fatale termijn van drie maanden. Opgemerkt wordt dat de behandeltermijnen verschillen per cluster. In het plan van aanpak is een verbetering van het totale proces voorzien.

#### *Plan van aanpak*

Er is nu een plan van aanpak van de CPO, waarin een aantal opgaven die in deze notitie genoemd worden geadresseerd. Het implementeren van de AVG bleek weerbarstig, maar met dit plan is een urgente en noodzakelijke stap gezet. De implementatie van dit plan is een essentiële voorwaarde om de AVG succesvol te implementeren. Om die reden wordt de concerndirectie gevraagd om de volle steun te bieden om het plan van aanpak te laten slagen.

#### *Reactie van de Concern Privacy Officer*

Met de invoering van de Algemene Verordening Gegevensbescherming (AVG) in 2018 heeft de gemeente Rotterdam een verplichting ten aanzien van het privacybeschermingsniveau van zowel burgers, ondernemers als medewerkers. Betrokkenen moeten te allen tijde op kunnen vertrouwen dat de persoonsgegevens die de gemeente Rotterdam van hen verwerkt in veilige handen is. Daarnaast heeft de gemeente Rotterdam onder de AVG een verantwoordingsplicht. Dit houdt in dat de gemeente aan moet kunnen tonen dat zij aan de AVG voldoet. Hier kan gevolg aan worden gegeven door:

- Inzicht geven in de processen waarbij persoonsgegevens worden verwerkt (het register van verwerkingen);
- Aantoonbaar stimuleren van de privacy bewustzijn binnen de organisatie (Privacy Awareness);
- Bijhouden van een register van datalekken;
- Burgers in staat stellen hun privacyrechten uit te oefenen (Rechten van betrokkene)
- Het uitvoeren van een Data Protection Impact Assessment (DPIA) (vooraf in kaart brengen van privacy risico's)

Om te kunnen voldoen aan de AVG is de gemeente Rotterdam al enige tijd bezig met de implementatie van de AVG. Om sneller in control te raken is in juli 2019 het Plan van Aanpak Privacy opgesteld. Dit Plan van Aanpak dient als monitorings- en sturingsinstrument richting de

clusters, aangezien de ambtelijke verantwoordelijkheid voor het naleven van de AVG bij de clusterdirecteuren ligt. Met dit plan van aanpak wordt inzichtelijk gemaakt waar de gemeente Rotterdam staat ten opzichte van de AVG-implementatie (en welke risico's dit met zich meebrengt); Tevens is een planmatige aanpak gecreëerd van de te nemen stappen op cluster-, en concernniveau zodat duidelijk is wie wat wanneer oplevert.

De CPO deelt de mening van de FG dat de afgelopen periode stappen zijn gezet in de implementatie van de AVG binnen de organisatie, maar dat er nog wel een kwaliteitsslag nodig is. Processen als Privacy by Design en het uitvoeren van DPIA's (een risico evaluatie van een verwerkingsproces), zijn complexe processen die de komende jaren steeds meer van de organisatie zullen eisen. Het onder de knie krijgen van deze processen is echter van essentieel belang om zorgvuldige omgang met de persoonsgegevens van burgers, ondernemers en werknemers te kunnen blijven waarborgen.

Gesteld kan worden dat formeel de zaken op orde zijn, maar dat materieel nog het één en ander geregeld moet worden.

Om materieel op orde raken, wordt daarom naast aandacht, tijd en monitoring, ook de benodigde (financiële) investering gevraagd. In 2019 zijn éénmalig extra middelen toegekend voor extra expertise. Dit is echter niet voldoende om verder in control te raken. Ook voor 2020 is extra geld en inzet nodig. Voor de Voorjaarsretraite 2020 zal om deze reden een extra capaciteitsclaim worden ingediend.

#### *Conclusie:*

Waar het de wettelijk verplichte instrumenten betreft zijn we nu een stuk verder dan een jaar geleden. Er is een Plan van Aanpak waarin de onderwerpen concreet zijn benoemd, met een planning in de tijd. De uitvoering staat of valt met de bereidheid vanuit de organisatie om hieraan uitvoering te geven.

#### 4. Financiële consequenties

Niet van toepassing. Voor het plan van aanpak is dekking.

#### 5. Communicatie/impact

Geen.

#### 6. Procedure

Na besluitvorming in de conerndirectie over de beslispunten volgt bespreking met wethouder Financiën, Organisatie, Haven, Binnenstad en Sport.

#### 7. Bijlagen

AVG in cijfers