

# Concern Directie

## Bespreekstuk

20 februari 2019  
V. Roozen

Concerndirectie

**Gegevens steller:**

Matthijs Mulder

E: jm.mulder@rotterdam.nl

T: [REDACTED]

## Agendapunt 2.A. 2<sup>e</sup> Rapportage Functionaris Gegevensbescherming

### 1. Aanleiding tot bespreking

Hierbij bied ik u de tweede rapportage van de Functionaris Gegevensbescherming (FG) aan. Met daarin een beeld van de stand van zaken van invoering van de Algemene Verordening Gegevensbescherming (AVG) die in mei 2018 in werking is getreden. Op 24 oktober 2018 vroeg de Concern Directie de FG hierover elk kwartaal te rapporteren, met daarin de stand van zaken, de risico's, datalekken, wat er moet gebeuren en met welke prioriteiten en daarmee de mate waarin het concern voldoet aan de wettelijke verplichtingen. De rol van de FG is in de AVG die van onafhankelijk toezichthouder. In Rotterdam rapporteert de FG rechtstreeks aan de gemeentesecretaris.

Vanwege die onafhankelijke rol is een aparte CD notitie bijgevoegd van de Concern Privacy Officer (hierna: CPO), waarin de aanpak en opgave beschreven staat om aan de AVG te voldoen. Echter, in deze fase waarbij de gemeente Rotterdam nog volop in de implementatie zit van de nieuwe wetgeving hebben de CPO en de FG deze notitie en het plan van aanpak met elkaar afgestemd en lopen de rollen deels door elkaar.

### 2. Afgestemd met cluster

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

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

### 2. Gevraagde beslissing

Gevraagd wordt om in te stemmen met de rapportage van de FG, waarin de volgende conclusies zijn:

- Op dit moment voldoen we nog niet aan alle eisen van de AVG, terwijl dit sinds mei 2018 verplicht is.
- de aanvragen van burgers om hun persoonsgegevens in te zien worden niet tijdig afgehandeld;
- het register van verwerkingen is op dit moment kwalitatief onvoldoende;
- dat we flinke stappen hebben gezet, maar er nog niet zijn.

Tevens wordt aan de Concerndirectie gevraagd te zorgen dat aan de belangrijkste eisen van de AVG wordt voldaan door:

- door in te stemmen met het plan van aanpak van de CPO, met die aanvulling dat de aanvragen van burgers vòòr mei 2019 tijdig en juist worden afgehandeld en het register van verwerkingen vòòr 1 juli aan de eisen van de AVG voldoet;
- de verwerkingsverantwoordelijken maandelijks aan de CPO en FG te rapporteren over de voortgang, zodat ik u bij de volgende CD een beeld kan geven van de voortgang/stand van zaken van het register van verwerkingen;
- voldoende middelen beschikbaar te stellen en support te verlenen om aan de hand van een Fit-Gap notitie in control te komen op het gebied van gegevensbescherming en hierover in de volgende CD hierover te rapporteren.

Binnen de clusters is bovenstaande deels al in gang gezet.

### **3. Toelichting**

*Waar staan we nu?*

Zoals eerder opgemerkt is met het opleveren van de verplichte onderdelen van de AVG een grote inspanning geleverd waar wij trots op kunnen zijn. Zo is al een flinke slag gemaakt met het register van verwerkingen, is er een nieuw systeem voor het register verwerkingen en datalekken en zijn er verdere procedures en werkprocessen vastgesteld. Ook zijn de in het privacybeleid genoemde functionarissen inmiddels aangesteld. Maar zo als eerder gemeld, we zijn er nog niet. De eerste opzet heeft verhoudingsgewijs veel tijd gekost. Het tijdsaspect om in control te zijn zal ons noodzaken om er nog een schep bovenop te doen. Het is nu zaak om met zo mogelijk meer energie door te pakken.

Onder leiding van de (CPO) wordt de implementatie planmatig opgepakt. Een stuurgroep met daarin vertegenwoordigers van alle clusters heeft de volgende prioriteiten benoemd:

*Vijf speerpunten*

1. Zorgvuldige verwerking van persoonsgegevens, vastgelegd in het register van verwerkingen;
2. Het goed omgaan met verzoeken van burgers om hun privacyrechten uit te oefenen;
3. Goed geïnformeerde medewerkers en procesverantwoordelijken;

4. Opleiding en positie van de PO;
5. Fit Gap analyse; voldoen we op alle punten aan de wet?

De toepassing van de AVG is voor veel organisaties die er mee te maken hebben een zoektocht en kent nog weinig standaarden. Daarnaast is de AVG omvangrijk en het is complex om wetgeving te vertalen naar werkprocessen. Ook de omslag om privacy te incorporeren in werk en denkwijzen vergt een grote attitude verandering. Vanwege de omvang van de opgave wordt in deze notitie gefocust op de meest urgente onderdelen. Aan de hand van de bovengenoemde vijf speerpunten is deze rapportage opgebouwd.

#### *1. Register van verwerkingsactiviteiten*

Zoals ook eerder in uw Concern Directie besproken is op dit moment de kwaliteit van het register nog onvoldoende. Veel verwerkingen moeten nog op juistheid worden gecontroleerd en een deel van de benodigde informatie ontbreekt. Hierdoor valt niet vast te stellen of een verwerking aan de beginselen inzake de verwerking van persoonsgegevens voldoet. Dat brengt risico's met zich mee. Niet alleen vanwege mogelijke boetes van de AP, maar ook reputatieschade.

Daarnaast leidt een onvolledig register tot het ontbreken op zicht op het aantal af te sluiten verwerkingsovereenkomsten en uit te voeren PIA's. Reden om aan het register prioriteit aan te geven.

Het register is een zware verplichting vanuit de AVG en ook de basis is van het compliant zijn aan de AVG. Door een actueel en volledig register voldoen we niet alleen aan de AVG, maar ook aan het gemeentelijk privacybeleid. Maar ook naar de burger willen wij transparant zijn. De Rotterdammer mag er immers op vertrouwen dat wij zorgvuldig met zijn/haar gegevens omgaan. Een volledig register maakt dat inzichtelijk. Tot slot is een volledig en geaccordeerd register de basis voor controle en borging van de privacywetgeving binnen de organisatie.

Desgevraagd dienen wij het register net als het register van datalekken te verstrekken aan de Autoriteit Persoonsgegevens (AP, de toezichthoudende autoriteit). Een korte blik op de website van de AP laat zien dat deze organisatie systematisch bij verschillende organisaties controles uitvoert naar onderdelen van de AVG.

In opzet is het register aanwezig, maar het op orde krijgen hiervan blijkt een behoorlijke opgave, dat tijd en capaciteit vergt van de clusters. In de stuurgroep van 8 februari 2018 is een planmatige aanpak om het register op orde te krijgen vastgesteld. Het is zaak deze opgave voortvarend ter hand te nemen.

In de bijlage treft u een overzicht aan van het aantal verwerkingen per cluster. Tevens treft u hierin een opgave aan van de nog te verrichten gegevensbeschermingseffectrapportages, ook wel PIA's genoemd en nog af te sluiten verwerkingsovereenkomsten. Hierdoor wordt de opgave inzichtelijk.

## 2. *Verzoeken van burgers*

Het tweede speerpunt richt zich op de 'nieuwe' rechten van burgers, zoals inzageverzoeken. Onverwijld en in ieder geval binnen een maand dienen betrokkenen de gevraagde gegevens te ontvangen. Deze termijn wordt nu niet gehaald. Hiermee loopt de gemeente Rotterdam een risico, ten eerste omdat dit onderdeel zichtbaar is voor de burger (reputatieschade), daarnaast financieel vanwege mogelijke uit te betalen dwangsommen van maximaal € 1260 per zaak en als derde het niet compliant zijn aan de gestelde termijnen. Een herijking van het proces loopt om de behandeling van deze aanvragen goed te beleggen en daarmee ook de beslistermijn te versnellen.

In de bijlage treft u een overzicht aan van de aantallen inzage verzoeken met daarbij de behandeltermijnen.

## 3. *Goed geïnformeerde medewerkers en procesverantwoordelijken.*

Dagelijks worden we geconfronteerd met klachten van burgers over privacy en datalekken. Naast onduidelijkheid of het ontbreken van juiste instructies om met persoonsgegevens om te gaan blijkt uit een analyse een deel van de problemen terug te leiden naar menselijk handelen. Daarnaast zijn de afdelingen zelf verantwoordelijk voor de uitvoering van de AVG in hun processen. Maar door het ontbreken van (voldoende) kennis bij de afdelingen, alsook producten/instructies waarmee zij aan de slag kunnen is er nog veel onduidelijkheid en/of zijn nog niet alle zaken opgepakt. En dat kan ook niet anders, het gaat hier om nieuwe wetgeving waarbij zoals gezegd standaarden nog in ontwikkeling zijn.

Dit geldt ook voor de PIA's, waarvan het opstellen en analyseren van de risico's op uitvoeringsproblemen stuit.

Onder leiding van de CPO worden stappen gezet om door middel van het vaststellen van procedures, formats en templates de medewerkers te faciliteren om aan de verplichtingen die de AVG met zich meebrengt te voldoen. Het is zaak om hiervoor voldoende middelen voor vrij te maken. Hiermee wordt ook voldaan aan de aanbevelingen van concern auditing uit mei 2018.

## 4. *Opleiding en positie van Privacy Officers.*

Per cluster is een PO benoemd. Deze PO heeft primair een adviserende op het gebied van privacyvraagstukken. In de praktijk komt deze rol in de knel. De oorzaken hiervoor zijn onder andere de opgave aan privacyvraagstukken en de awareness van de afdelingen voor hun verantwoordelijkheid over hun verwerkingen. Dit alles betekent een zware belasting voor de PO-ers. Het is zaak dat zij voldoende worden ondersteund en dat de functie van PO-er verder wordt geprofessionaliseerd en dat voldoende aandacht is voor de competenties en opleidingen.

## 5. *Fit gap analyse; voldoen we op alle punten aan de wet?*

Een van de aanbevelingen van concern auditing is het opzetten van een fit gap analyse om aan de hand hiervan te kijken waar staan we nu staan om zo de implementatie planmatig uit te rollen.

Belangrijke onderdelen, onder andere governance, van de AVG zijn inmiddels geïmplementeerd, maar om daadwerkelijk in control te komen is het zaak om processen, kaders en richtlijnen te ontwikkelen. Door deze analyse wordt niet alleen helder wat de totale opgave is, door het planmatig implementeren hiervan kan aangetoond worden dat aan de AVG wordt voldaan.

Denk hierbij aan een belangrijk uitgangspunt van de AVG, het privacy by design. Hiervoor zijn de afgelopen weken voor de belangrijkste processen uitgangspunten geformuleerd, die in de komende periode in de Rotterdamse processen moet worden ingebouwd.

*Conclusie:*

Er zijn goede stappen gezet om aan de AVG te voldoen en het proces wordt ook voortvarend ter hand genomen. Maar we zijn er nog niet en dit brengt risico's met zich mee. Dit zijn mogelijke boetes, maar ook reputatieschade bij incidenten.

Naast support vanuit uw directie zal ook de inzet voor de implementatie geïntensiveerd moeten worden tot dat wij compliant te zijn aan de privacywetgeving.

#### **4. Financiële consequenties**

Voor de financiële consequenties die te maken hebben met de implementatie van de AVG worden besproken in de notitie van de CPO.

In deze notitie worden de mogelijk boetes genoemd aan het niet voldoen aan de privacywetgeving.

#### **5. Communicatie/impact**

**Geen.**

#### **6. Procedure**

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

#### **7. Bijlagen**

AVG in cijfers