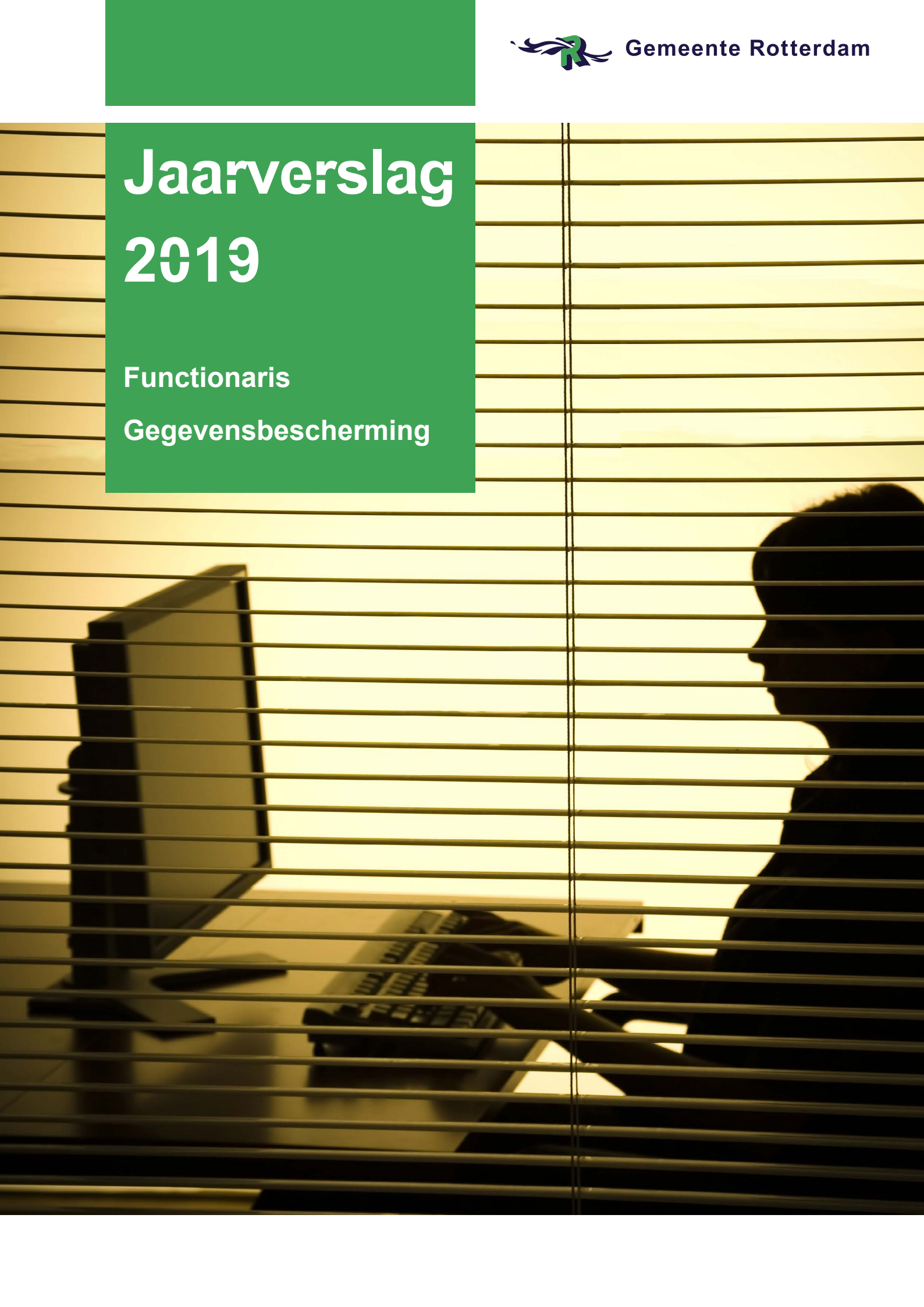




Jaarverslag 2019

Functionaris

Gegevensbescherming



Voorwoord

Dit is het eerste jaarverslag van de Functionaris Gegevensbescherming (hierna: FG) sinds de Algemene Verordening Gegevensbescherming (AVG) in mei 2018 in werking trad. De AVG is de nieuwe Privacy wetgeving die voor de hele Europese unie geldt en zwaardere verplichtingen oplegt aan organisaties bij de omgang met persoonsgegevens dan de voorganger, de Wet bescherming persoonsgegevens (Wbp).

2019 was een bijzonder jaar. De organisatie kreeg voor het eerst in volle omvang te maken met de AVG. Nadat we in mei 2018 het programma Rotterdam Privacy Proof hadden afgerond, bedoeld om de organisatie voor te bereiden op de invoering van de AVG, bleek al snel dat we er daarmee nog lang niet waren.

Het verplichte register van verwerkingen was er in opzet, maar nog lang niet volledig. Het daarvoor aangekochte systeem bleek niet te voldoen aan de behoefte en een duidelijke lijn voor de verantwoording over de AVG moest nog vorm krijgen.

Daarnaast kregen we te maken met de eerste onderzoeken van de toezichthoudende Autoriteit Persoonsgegevens, die met de invoering van de AVG veel bevoegdheden kreeg. Er waren verzoeken van burgers die hun dossier wilden inzien. En ook was er een toename van het aantal klachten en datalekken. Dit trok een stevige wissel op de medewerkers die belast waren met de uitvoering van deze taken.

Daarnaast werd duidelijk dat de AVG grote invloed heeft op bijna alle processen van de gemeente en daarmee ook op het werk van de proceseigenaren. Maar met de steun van de concerndirectie zijn grote stappen gemaakt om de gemeente Rotterdam 'in control' te krijgen. Kortom, we hebben een stevige basis gelegd en het is zaak om daar de komende jaren met volle energie op voort te bouwen. Want naarmate we meer weten, wordt ook steeds duidelijker dat er nog een grote opgave ligt.

Dit jaarverslag beschrijft de bevindingen van de FG over het jaar 2019; wat hebben we bereikt en waar staan we nu bij de invoering van de AVG.

Het verslag is tot stand gekomen in samenspraak met de Concern Privacy Officer (CPO), de Concern Information Officer (CISO) en de Privacy Officers van de clusters.

Matthijs Mulder FG



Inhoudsopgave

1.	Samenvatting in cijfers	4
2.	Terugblik	6
3.	Functionaris Gegevensbescherming	8
4.	AVG naar onderdelen	9
4.1	Datalekken	9
4.2	Register van verwerkingen	10
4.3	Rechten van betrokkenen	11
4.4	Beveiliging	11
4.5	Organisatorische inpassing	12
4.6	Samenwerking en uitbesteding	13
4.7	DPIA's	13
4.8	Autoriteit Persoonsgegevens	14
4.9	Klachten en vragen	14
5.	Vooruitblik 2020	15

1 Samenvatting in cijfers

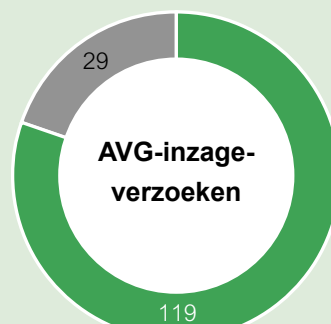


Verwerkingenregister

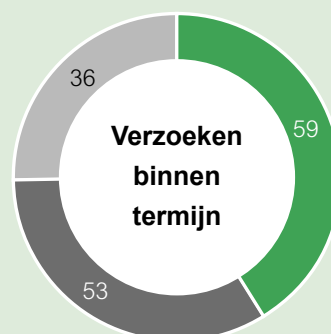


- Complete verwerkingen: **395**
- Totaal verwerkingen in register: **435**

Rechten van betrokkenen



- Verzoeken om inzage: **119**
- Verzoeken om rectificatie, correctie of verwijdering: **29**
- Totaal AVG-inzageverzoeken van burgers in 2019: **148**



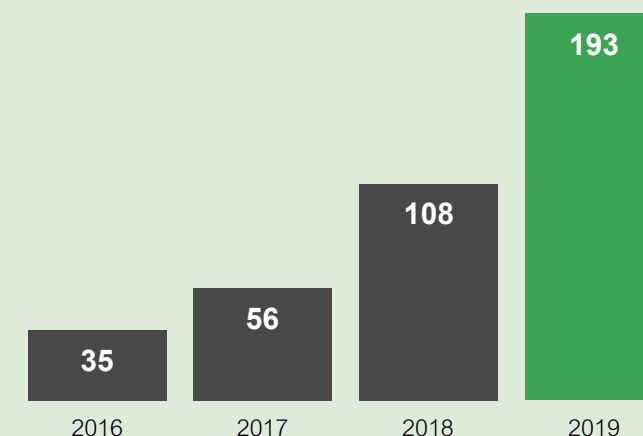
- In 2019 werd 24% van de verzoeken te laat afgehandeld (langer dan drie maanden).
- Binnen de streefdatum (30 dagen): **59**
 - Met verdaging (binnen 3 maanden): **53**
 - Te laat (meer dan drie maanden): **36**
- Het aantal AVG-inzageverzoeken dat op tijd wordt afgehandeld nam in 2019 toe.

Gemelde datalekken

Aantal datalekken dat gemeld is bij de Autoriteit Persoonsgegevens (AP) neemt toe:

- 2019: **193** datalekken, waarvan 131 gemeld aan de AP
- 2018: **108** meldingen
- 2017: **56** meldingen
- 2016: **35** meldingen

Rotterdam volgt hierin de landelijke trend. 25% van de datalekmeldingen wordt **te laat** (+72 uur) gemeld bij de AP.



Verwerkersovereenkomsten

Wanneer een externe partij gegevens verwerkt voor de gemeente moet er een verwerkers-overeenkomst zijn. Bij ruim **100** verwerkingen ontbreekt de overeenkomst nog.



Privacy assesment (DPIA)

Er zijn **142** verwerkingen waar naar het huidige inzicht een assessment (DPIA) moet worden uitgevoerd. Dat zijn verwerkingen met een hoog risico omdat er bijvoorbeeld veel privacygevoelige gegevens worden verwerkt. Er zijn er nu enkele tientallen in voorbereiding. In 2019 zijn er **8** vastgesteld.

2 Terugblik

Hoe kijken we terug op het afgelopen jaar, hoe staat de organisatie ervoor?

Register van verwerkingen

Na invoering van de AVG in mei 2018 was het speerpunt het register van verwerkingen. Dit is immers de basis voor alle andere onderdelen van de AVG. Het register biedt inzicht in alle processen waarin persoonsgegevens worden gebruikt, en legt onder meer het soort gegevens vast, het doel ervan, de bewaartermijnen en de beveiliging. Tevens geeft het een indicatie van de risico's van de verwerking. In februari 2019 besloot de conerndirectie dan ook dat het register prioriteit moest krijgen. De privacy officers van de clusters hebben vervolgens met grote inspanning het register, dat tot dan toe bestond uit losse Excelbladen, omgebouwd tot een uitgebreide verantwoordings- en sturingstool. Hoewel hiermee een mooie slag is gemaakt, zijn nog niet alle verwerkingen volledig. Op dit moment zijn bij 91% van de verwerkingen alle gevraagde velden gevuld. Hier ligt dus nog een opgave.

Plan van aanpak

Het register van verwerkingen geeft nu inzicht in de stand van zaken rondom de AVG. Daaruit blijkt dat er nog een grote opgave ligt om volledig aan de AVG te voldoen. Daarom is besloten de meest urgente onderdelen planmatig op te pakken, via een plan van aanpak.

Dit plan dient als monitorings- en sturingsinstrument voor de clusters. Daar ligt immers de ambtelijke verantwoordelijkheid voor het naleven van de AVG. In dit plan wordt inzichtelijk gemaakt waar de gemeente Rotterdam staat bij de invoering van de AVG (en welke risico's dit met zich meebrengt). Tevens is er een planmatige aanpak van de te nemen stappen op cluster- en concernniveau. Inmiddels zijn de eerste resultaten er. Zo is duidelijk hoeveel verwerkersovereenkomsten⁴ nog afgesloten moeten worden en hoeveel DPIA's (Data Protection Impact Assessment). Daarnaast is een slag gemaakt in het wegwerken van achterstanden op het gebied van inzageverzoeken⁵.

Rapportages

Sinds eind 2018 rapporteren zowel de FG als de CPO aan de conerndirectie over de stand van zaken rond de AVG. Tevens zijn de verschillende onderdelen van de AVG, zoals datalekken, rechten van betrokkenen en de voortgang van het register van verwerkingen, onderdeel van de CD-monitor. Dit geeft de conerndirectie de mogelijkheid om te sturen op de uitvoering van de AVG. Voor 2020 staat verdere uitbreiding van de monitor op stapel. Bovendien krijgen dan alle lijnmanagers stuurinformatie voor hun eigen afdeling in de concernbrede rapportages over bedrijfsvoering.

⁴ Organisaties schakelen vaak andere organisaties in om persoonsgegevens voor hen te verwerken. Bijvoorbeeld voor het uitbesteden van de salarisadministratie. In een verwerkersovereenkomst worden afspraken vastgelegd met de verwerker, onder andere dat deze de gegevens niet voor andere doelen mag gebruiken.

⁵ Een Data Protection Impact Assessment is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen (zie hoofdstuk 4.2 en 4.7)



3 Functionaris Gegevensbescherming

De AVG stelt het aanstellen van een FG verplicht voor overheidsinstanties en publieke organisaties. De FG ziet erop toe dat de gemeente Rotterdam voldoet aan de wettelijke verplichtingen bij het verwerken van persoonsgegevens. Hij toetst onder andere de naleving van de wettelijke eisen, gemeentelijke richtlijnen op het gebied van privacy, het privacybeleid en het informatiebeveiligingsbeleid. De FG is zowel adviseur als toezichthouder. Die taken staan in de wet, maar niet de wijze waarop die taken moeten worden uitgevoerd. Er is dan ook flink geïnvesteerd in het zoeken naar de beste invulling van die rol, binnen de context en de schaal van de gemeente Rotterdam. Dit is vastgelegd in twee documenten: het beleidskader FG en het toezichtskader FG, beide te vinden op de concernpagina op RIO.

Bezetting

Sinds 1 januari 2019 heeft het bureau FG 3 fte. Daarnaast krijgt de FG ondersteuning vanuit Juridische diensten en Directie Middelen en Control.

Werkzaamheden

Aanvankelijk was de voornaamste taak van de FG het melden van en adviseren over datalekken. In 2019 kwam het accent meer te liggen op het blijvend voldoen aan de AVG, met nadruk op het genoemde register van verwerkingen. Na de zomer lag het accent steeds meer bij de advisering op de Data Protection Impact Assessment's (DPIA), het starten van onderzoeken en het toezien op de juistheid en volledigheid van het register van verwerkingen. Daarnaast rapporteert de FG periodiek aan de concerndirectie en Stuurgroep Privacy over de invoering van de AVG. In 2019 voerde de FG drie onderzoeken uit; over datalekken, rechten van betrokkenen (verzoeken om inzage van burgers) en de aanwezigheid van verwerkingsovereenkomsten⁶ (met externe verwerkers) in het register van verwerkingen.

Kennisborging

Om de kennis op peil te houden, hebben de medewerkers van het team van de FG de CIPP/E cursus afgerond en is geïnvesteerd in workshops over toezicht, audits, DPIA's en informatiebeveiliging. Daarnaast onderhouden ze een uitgebreid netwerk met de FG's van de vijf grote gemeenten en een flink aantal regiogemeenten, het Havenbedrijf en de Erasmusuniversiteit.

Een andere taak van de FG ligt bij de kennisborging in de organisatie. Het team FG organiseerde lezingen door experts over samenwerkingsverbanden en Privacy by Design. Daarnaast gaf men zelf lezingen over de AVG in Rotterdam, DPIA's en datalekken. Zo gaf de FG driemaal een masterclass aan medewerkers over het melden van datalekken.

Tot slot is de FG belast met het bijhouden van het register van verwerkingen en het register van datalekken en het rapporteren daarover.

⁶ Zie voor uitleg paragraaf 4.6

4 AVG naar onderdelen

4.1 Datalekken

Bij een datalek gaat het om het vrijkomen, wijzigen of vernietigen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is. Een ernstig datalek moet dan ook gemeld worden bij Autoriteit Persoonsgegevens (AP) en in veel gevallen ook aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Datalekken zijn een risico voor de organisatie (en voor de burgers die het betreft) en moeten daarom goed en snel worden afgehandeld. Daarnaast is het een wettelijke verplichting om datalekken tijdig en volledig te melden, dat wil zeggen binnen 72 uur na de ontdekking van het lek. Ook moeten betrokkenen zo snel mogelijk geïnformeerd worden en er moeten maatregelen worden genomen om het lek te dichten en de schade te beperken. De tabel op pagina 4 en 5 geeft de ontwikkeling van het aantal datalekken weer vanaf 2016, toen verplicht werd deze te melden bij de Autoriteit Persoonsgegevens.

Datalekken moeten worden gemeld aan de Autoriteit Persoonsgegevens tenzij het risico voor betrokkenen gering is. In dat geval is een interne registratie voldoende. Om te voorkomen dat een datalek zich herhaalt, heeft de gemeente in het datalekkenprotocol de verplichting opgenomen dat elk datalek wordt geëvalueerd en dat er maatregelen worden genomen.

Terugblik 2019

Dit jaar waren er 193 datalekken, dus een toename ten opzichte van vorige jaren. Mogelijk is dit mede toe te schrijven aan toegenomen bewustzijn. Van de **193 meldingen** zijn er **131 gemeld** bij de Autoriteit Persoonsgegevens (AP). Evaluatie van een datalek is een belangrijk middel om herhaling te voorkomen en is daarom vastgelegd in het privacybeleid. Op 1 januari 2020 waren **147 datalekken** van een evaluatie voorzien. Ook moeten betrokkenen van wie gegevens zijn gelekt, snel geïnformeerd worden over het datalek. In **117 gevallen** gebeurde dat. Wanneer voor de betrokkenen het risico gering is, kan die stap achterwege blijven.

Onderzoek datalekken

In 2019 deed de FG onderzoek naar de datalekken. De belangrijkste bevindingen waren onder meer dat niet alle datalekken direct als zodanig worden herkend en daardoor pas veel later gemeld worden bij de FG. Verder bleek een derde deel van de datalekken na de ontdekking niet binnen de wettelijke termijn van 72 uur gemeld bij de AP. Ook bleek dat niet alle datalekken zijn geëvalueerd. Waar dat wel gebeurde, zijn genoemde maatregelen over het algemeen concreet en uitvoerbaar en sommige zijn al direct verwerkt in het proces. De aanbevelingen uit het onderzoek worden verwerkt in de herziening van het datalekkenprotocol. Later in het jaar 2020 doet de FG een toets op de opvolging van datalekken.

Oorzaken van datalekken

De meeste datalekken vallen in de categorie 'persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger'. Het betreft meestal een verkeerde adressering van e-mail of post, stukken van een andere persoon die in een verkeerde envelop belanden, en e-mails aan grotere groepen burgers in de cc in plaats van de bcc, waardoor alle e-mailadressen zichtbaar zijn. Dat kan vervelende gevolgen hebben, zeker voor groepen kwetsbare personen. De meeste datalekken komen voor bij de clusters waar ook de meeste klantcontacten zijn. Zij versturen ook de meeste post en e-mail. Dat zijn grote aantallen, waardoor er weleens wat fout gaat. Zo verstuurt Belastingen 2.500.000 poststukken per jaar en zijn er 368.000 baliebezoeken voor Dienstverlening.

De gemeente minimaliseert de risico's door organisatorische en technische maatregelen te nemen. Zo is de bewustwordingscampagne een belangrijk middel om bij medewerkers het bewustzijn te verhogen rond de risico's op datalekken. Ook wordt onderzocht in hoeverre de techniek kan helpen om bijvoorbeeld verkeerde verzending te voorkomen en worden trainingen gegeven.

4.2 Register van verwerkingen

De AVG geeft niet alleen aan hoe organisaties met persoonsgegevens om moeten gaan, ook moet de organisatie kunnen aantonen dat zij handelt in overeenstemming met de regelgeving. Dat betekent dat de organisatie een register van verwerkingsactiviteiten (hierna: het register) moet bijhouden met daarin alle verwerkingen waarbij persoonsgegevens worden gebruikt. Door een actueel en helder register voldoen we niet alleen aan de AVG, maar ook aan het gemeentelijk privacybeleid. Het register geeft inzicht in alle processen en vormt daarom de basis van waaruit we andere thema's kunnen oppakken.

Op 1 januari 2020 had de gemeente Rotterdam **436 verwerkingen** in het register. Daarvan zijn **396 compleet**. Dat wil zeggen dat alle velden zijn gevuld. Zo'n 9% is dus nog niet volledig.

Zo hebben we nu inzicht in het aantal onvolledige verwerkingen, de DPIA's die nog verricht moeten worden en tot slot het aantal verwerkingen waarvoor nog een overeenkomst moet worden afgesloten.

Transparantie en informatieverplichting

Op het portal voor de burger, rotterdam.nl, is een privacyverklaring gepubliceerd. Op diezelfde pagina wordt verwezen naar de rechten van burgers, met name het recht op inzage- en correctieverzoeken. Via de website kan de burger om inzage verzoeken in zijn/haar persoonsgegevens. Het streven is om in 2020 het 'register van verwerkingen' op de website te plaatsen zodat voor Rotterdammers inzichtelijk is welke categorieën gegevens worden gebruikt voor welk proces.

Voorbeelden van datalekken:

- In bepaalde brieven werd onterecht een BSN-nummer gebruikt (een BSN-nummer wordt beschouwd als 'gevoelig persoonsgegeven'). De werkwijze is aangepast.
- Bij het versturen van een nieuwsbrief zijn de mailadressen van betrokkenen in de CC rubriek gezet in plaats van in de BCC-rubriek waardoor deze zichtbaar zijn voor de andere ontvangers.
- Uitspraak van de Rechtbank is per ongeluk met de verkeerde advocaat gedeeld. Advocaat heeft echter geheimhoudingsplicht en de advocaat is verzocht om vernietiging van de gegevens.

Maatregelen:

- Extra alert zijn op anonimiseren van voorbeeldgegevens in de nieuwsbrief
- Het gebruik van Move It bij verzending van persoonsgegevens buiten de organisatie wordt nog eens onder de aandacht gebracht.
- Het betreft een datalek ontstaan door een menselijke fout. Geheel voorkomen is daarom onmogelijk. De Privacy Officer schuift aan in een teamvergadering om te praten over datalekken (ook het proces) en hoe hier mee om te gaan.
- Gesprekken zijn gevoerd met de groep om na te gaan waardoor er foutief gemuteerd is. De werkinstructie is verbeterd.



Blijf Alert!-campagne tijdens de Dag van de Privacy



4.3 Rechten van betrokkenen

Onder de AVG zijn de zogenoemde rechten van betrokkenen versterkt. Dit recht houdt onder meer in dat burgers inzage kunnen krijgen in de eigen persoonsgegevens. De AVG schrijft voor dat dit per ommekeer moet gebeuren, doch uiterlijk binnen één maand. Het verzoek kan in complexe gevallen met twee maanden worden verdaagd. In 2019 werden **148 aanvragen** ingediend in het kader van 'rechten van betrokkenen'.

Termijnen

De termijnen waarbinnen de aanvragen werden afgehandeld:

- Binnen de streefdatum (30 dagen): 59
- Met verdaging (tussen een maand en drie maanden): 48
- Te laat (meer dan drie maanden): 36

In de tweede helft van het jaar is het beter gelukt de verzoeken tijdig af te handelen.

Clusters

Het aantal verzoeken verschilt per cluster. Het cluster W&I heeft de meeste verzoeken ontvangen (43) gevolgd door MO en BCO (17 en 15).

Onderzoek rechten van betrokkenen

De FG heeft in 2019 gedaan naar het proces van de rechten van betrokkenen. Dit onderzoek laat zien dat er belangrijke winst te behalen is in de tijdigheid van de afhandeling door het proces op een aantal punten te verbeteren. De verbeterpunten zijn voorgelegd aan de stuurgroep Privacy.

4.4 Beveiliging

Informatiebeveiliging

De Algemene Verordening Gegevensbescherming vraagt organisaties om in deze snel digitaliserende wereld zorgvuldig om te gaan met persoonsgegevens. Organisaties moeten persoonsgegevens passend beveiligen. Informatiebeveiligingsmaatregelen dragen bij aan privacy. Het gaat daarbij om technische en organisatorische maatregelen en maatregelen op het aspect van de 'mens'.

Organisatie en techniek

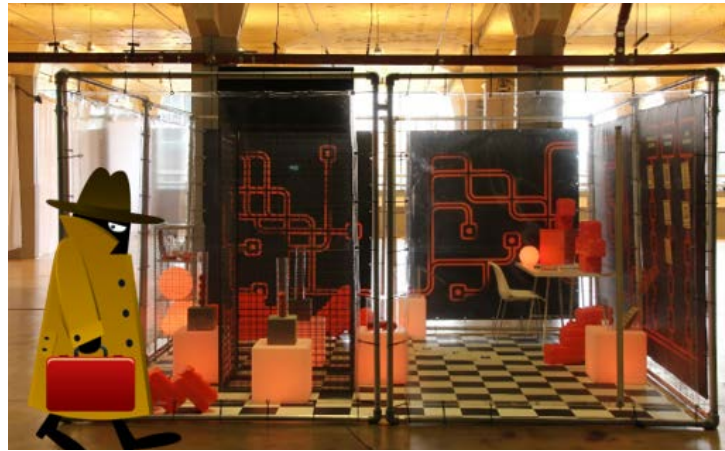
Ook informatiebeveiligingsmaatregelen op het gebied van organisatie of techniek dragen bij aan privacy. In 2019 is onder meer de toegangsbeveiliging verbeterd en zijn voorbereiding getroffen voor het invoeren van de draagplicht van de concernpas. Daarnaast is de beveiliging van de ICT-infrastructuur verbeterd en is er zgn. *continuous security monitoring* ingericht waarmee gemeente Rotterdam continu en direct kan reageren op signaleren van geavanceerde dreigingen, kwetsbaarheden en cyberaanvallen op de infrastructuur.

Mens / bewustzijn

Bewustzijn vormt de randvoorwaarde voor zowel een goede invoering als een goede naleving van de AVG. Niet voor niets heeft de Autoriteit Persoonsgegevens bewustzijn bovenaan in het tienstappenplan voor de invoering van de AVG gezet. Kennis, houding en gedrag zijn dé sleutel om data in veilige handen te houden. Gemeente Rotterdam is in 2018 een bewustwordingscampagne gestart gericht op informatieveiligheid en privacy. Deze campagne liep door in 2019. Hieronder staat een korte weergave van de acties en resultaten tot nu toe.

- Diverse communicatie uitingen (bijv. flyers, posters, banners, RIO etc.)
- Hackdemo's en data escaperoom (ervaringen)
- Informatieveiligheid en privacy challenge

Ook in 2020 wordt nadrukkelijk blijvend aandacht gevraagd voor datalekken en het versterken van het basis-kennisiniveau (o.a. middels het volgen van een verplichte e-learning). Daarnaast ligt de focus op het concretiseren van rollen en taken van directie en lijnmanagement (proceseigenaren en procesbetrokkenen).



Data Escaperoom

4.5 Organisatorische inpassing

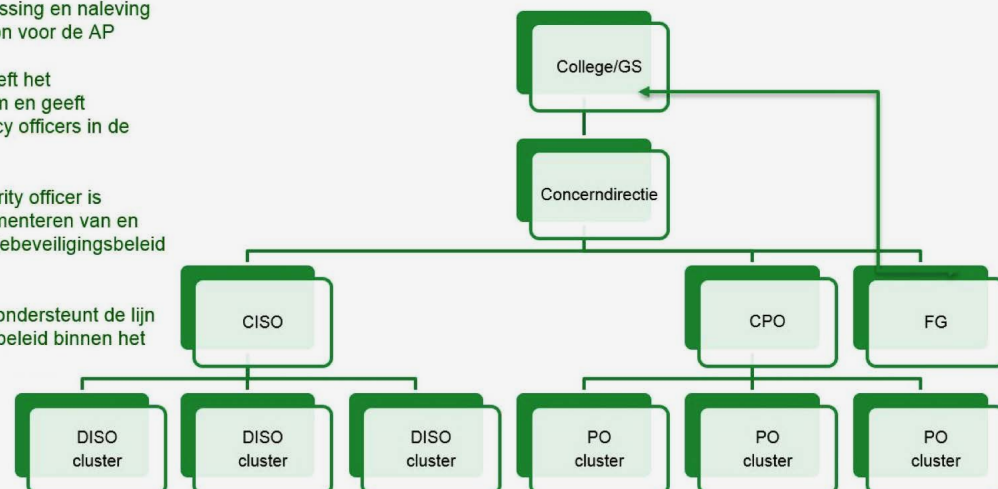
Privacy organisatie

FG Functionaris gegevensbescherming is een verplichte functie. Deze houdt binnen de organisatie toezicht op de toepassing en naleving van de AVG en is contactpersoon voor de AP

CPO Concern privacy officer geeft het privacybeleid en de aanpak vorm en geeft functioneel leiding aan de Privacy officers in de clusters.

CISO Concern information security officer is verantwoordelijk voor het implementeren van en toezicht houden op het informatiebeveiligingsbeleid en stuurt de DISO's aan.

PO Privacy officer adviseert en ondersteunt de lijn bij de uitvoering van het privacybeleid binnen het cluster



4.6 Samenwerking en uitbesteding

Wanneer een externe partij wordt ingeschakeld om de verwerking van gegevens uit te voeren (of een deel daarvan) verplicht de AVG tot een overeenkomst tussen de verantwoordelijke organisatie en de verwerker (denk bijvoorbeeld aan de salarisadministratie die is uitbesteed). In deze overeenkomst moet onder meer worden vastgelegd hoe de verwerker met de gegevens om moet gaan, hoe de beveiliging is geregeld en wat er moet gebeuren met de gegevens na afloop van de samenwerking.

Onderzoek verwerkersovereenkomsten

In 2019 deed de FG onderzoek naar de aanwezigheid van overeenkomsten in het register. Hieruit bleek dat een deel van de overeenkomsten niet in het register is opgenomen, niet aanwezig was of niet was ondertekend. Dit is vervolgens aangepast in het register.

Bij **208 verwerkingen** die in het register staan is een verwerkersovereenkomst nodig. Bij **122 verwerkingen** is een overeenkomst aanwezig. Er ontbreken dus nog flink wat overeenkomsten. Hoewel het kan zijn dat er voor meerdere verwerkingen met een overeenkomst kan worden volstaan, ligt hier dus nog een opgave om te voldoen aan de AVG. Deze opgave is ook in het plan van aanpak opgenomen voor 2020.

4.7 DPIA's

Zoals gesteld kent de AVG de verplichting om een DPIA (Data Protection Impact Assessment) of, de Nederlandse term, een gegevensbeschermingseffectbeoordeling uit te voeren voor verwerkingen met een hoog risico. Met deze analyses worden de risico's voor de betrokkenen bij een verwerking in kaart gebracht, evenals de maatregelen om deze risico's te ondervangen. Wanneer die risico's niet kunnen worden ondervangen is er sprake van een hoog restrisico. In dat geval moet de verwerking voor de start van het proces of activiteit worden voorgelegd aan de Autoriteit Persoonsgegevens.



Planning DPIA's

Het streven is om voor alle risicovolle verwerkingen voor mei 2021 – drie jaar na invoering van de AVG – een DPIA verricht te hebben. Daarmee worden de risico's inzichtelijk en kunnen gericht maatregelen worden genomen. Uit een recente inventarisatie blijkt dat voor **142 verwerkingen** een DPIA nodig is. Daarnaast moet voor alle nieuwe verwerkingen met een risico een DPIA worden opgesteld, nog voordat begonnen wordt met het project of proces. Hier ligt een grote opgave, want het opstellen van een DPIA vraagt een flinke inzet vanuit meerdere disciplines. In 2019 zijn daarom medewerkers getraind op het uitvoeren van DPIA's. Daarnaast zijn handleidingen geschreven om het proces makkelijker te maken. Als de Privacy officer en daarna de FG over de DPIA heeft geadviseerd en de proceseigenaar instemt met het advies, kan de DPIA worden vastgesteld.

De volgende DPIA's zijn vastgesteld in 2019:

- Bodycam pilot (SB)
- Bodycam (SB)
- Fysieke beveiliging gemeentelijke gebouwen (BCO)
- Handhaving milieuzones met ANPR camera's (SO)
- Citydeal vastgoedfraude (Directie veiligheid)

Daarnaast zijn er ook DPIA's van voor de AVG in het register opgenomen:

- Landelijke aanpak adreskwaliteit (DV)
- PIA Parkeerhandhaving (scanauto).
- GFT Hoogbouw (SB, betreft een landelijk uitgevoerde PIA)
- Verlenen diensten aan werkgevers (Hallo Werk) (W&I)

Naast de vastgestelde DPIA's zijn er enkele tientallen in voorbereiding.

4.8 Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) is de toezichthouder op het gebied van de AVG. De bevoegdheden van de AP zijn ruim en maken het onder meer mogelijk om onderzoek te doen binnen een organisatie en boetes op te leggen tot een maximum van 20 miljoen euro.

Direct na de invoering van de AVG in 2018 begon de AP een aantal verkennende onderzoeken. Bij een van deze onderzoeken werd ons datalekkenregister opgevraagd. Het meest recente onderzoek van de AP betreft het onderzoek naar Smart City-toepassingen bij meerdere gemeentes waaronder Rotterdam.

Daarnaast deed de AP onderzoeken en/of interventies naar aanleiding van specifieke meldingen of klachten. Een daarvan betrof een melding over een kwetsbaarheid in ██████. Na maatregelen van onze organisatie heeft de AP dit onderzoek afgesloten.

Ook waren er onderzoeken naar aanleiding van klachten over een verzoek om inzage. Dit betrof de manier waarop wij de identiteit vaststellen van betrokkenen. De AP concludeerde daarop dat de werkwijze van Rotterdam niet in strijd is met de wet.

De AP neemt af en toe ook direct contact op met de FG. Dat gebeurde bijvoorbeeld over het gebruik van het BSN-nummer bij het milieupark⁷. Maar ook over datalek-meldingen heeft de AP diverse malen contact opgenomen. Bijvoorbeeld wanneer een voorlopige melding te lang open bleef staan of wanneer de AP van mening was dat de betrokkenen op de hoogte gesteld moesten worden van een datalek.

Ook in 2019 gaf de AP weer richtlijnen en uitleg en organiseerde voor het eerst de dag van de FG. Tot slot heeft een kennismakingsgesprek plaatsgevonden tussen de FG en medewerkers van de afdeling systeemtoezicht van de AP.

4.9 Klachten en vragen

De AVG verplicht de organisatie om naam en contactgegevens van de FG te publiceren zodat de Rotterdamse burger contact kan opnemen. Het afgelopen jaar hebben rond de zestig personen van deze mogelijkheid gebruik gemaakt, met vragen en/of klachten over de AVG. Niet altijd zijn dat burgers, en vaak betreft het een vraag.

De meeste van die vragen en klachten gaan over

- de toepassing van de AVG, (bijvoorbeeld: 'mag de gemeente mijn gegevens gebruiken voor onderzoek';
- rechten van betrokkenen: dat de behandeling te lang duurt, of dat men ontevreden is met wat opgeleverd wordt;
- overige kwesties die op een andere afdeling thuishoren (bijvoorbeeld een adreswijziging die niet goed is doorgevoerd of een klacht die over iets anders blijkt te gaan) en
- vragen van collega's over toepassing van de AVG en vragen van FG's van andere organisaties of gemeenten om kennis te delen over de toepassing van de AVG op bepaalde gebieden.

De aard van de vragen van burgers laat zien dat mensen zich steeds meer bewust worden van hun privacyrechten en zich vaker afvragen wat de gemeente doet met hun persoonsgegevens. Zo zijn er bijvoorbeeld drie vragen binnen gekomen over een wijkonderzoek waarbij persoonsgegevens uit BRP zijn verstrekt voor wetenschappelijke doelen.

5 Vooruitblik 2020

Nieuwe technologie

De technologie neemt een enorme vlucht als het gaat om slim gebruik van data, zoals bijvoorbeeld Smart City. Een slimme stad is een stad waarbij informatietechnologie en het internet der dingen gebruikt worden om de stad te beheren en te besturen. 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, omdat soms persoonsgegevens van burgers worden verwerkt. De bescherming daarvan moet gewaarborgd worden.

Dat ook de Autoriteit persoonsgegevens 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 van het begin af aan 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.

Hier ligt een grote uitdaging; het verder invoeren en borgen van het principe van Privacy by Design, waardoor bij nieuwe ontwikkelingen privacy al in de ontwerpfase wordt meegenomen. Privacy moet daarbij niet beschouwd worden als een remmer of belemmering, maar als een belangrijke voorwaarde en kans voor innovatie. Het is zaak dit voortvarend op te pakken en dit principe toe te passen.

Overig

Hoewel in 2019 de nodige acties in gang zijn gezet om te voldoen aan de AVG en het Plan van Aanpak Privacy daar zeker een bijdrage aan heeft geleverd, liggen er nog flinke uitdagingen voor de komende jaren. Het is zaak daar met onverminderde aandacht op door te pakken.

Daarnaast wordt geadviseerd om verder in te zetten op het uitvoeren van DPIA's en de daaruit voortkomende maatregelen uit te voeren.

Tot slot blijven ook datalekken een punt van aandacht. Het belang van het evalueren van elk datalek blijft onverminderd groot zodat er gerichte maatregelen kunnen worden genomen om verdere datalekken te voorkomen. Het behandelen van datalekken kost een hoop werk en ze schaden het vertrouwen van de burger in de door hun aan ons toevertrouwde gegevens.

Het komend jaar zal de FG deze ontwikkelingen dan ook nauwgezet volgen en hierover rapporteren.

“

Privacy has historically been viewed as an impediment to innovation and progress, but that's so yesterday and so ineffective as a business model. Without user trust, technologies can't move forward.

Ann Cavoukian, PhD, voormalig information and privacy commissioner uit Ontario, die organisaties sinds de jaren '90 al aanmoedigt om het concept van privacy by design toe te passen.

”

⁷ Bij het aanbieden van grof vuil moeten burgers zich bij twijfel identificeren omdat deze faciliteit er alleen is voor inwoners en bedrijven in Rotterdam.

Colofon

Tekst, beeld en redactie
Gemeente Rotterdam

Vormgeving
Awareness+zootz

Jaar van uitgave
2020

Rotterdam.nl