

Jaarverslag 2020



Functionaris Gegevensbescherming



Gemeente
Rotterdam

Jaarverslag Functionaris Gegevensbescherming 2020

Inhoud

1. Inleiding en samenvatting	blz 2
2. Beleid	blz 4
3. Processen	blz 4
4. Samenwerking	blz 5
5. Informatiebeveiliging	blz 6
6. Rechten van betrokkenen	blz 7
7. Verantwoorden	blz 7
8. Diversen	blz 8
9. Bijlage: cijfers 2020	blz.10

Jaarverslag Functionaris Gegevensbescherming 2020

1. Inleiding en samenvatting

Dit is het tweede jaarverslag van de Functionaris Gegevensbescherming (hierna: FG). Het belicht de stand van zaken rond de privacywetgeving binnen de gemeente Rotterdam in 2020.

2020 was een bijzonder jaar. We werden verrast door de corona-epidemie en thuiswerken werd plotseling de norm. Dat had invloed op de stad, op de gemeentelijke organisatie en vooral op de manier waarop we werken. Het thuiswerken zorgde voor nieuwe uitdagingen. De coronacrisis en de bijbehorende maatregelen maakten dat snelheid in sommige gevallen ten koste ging van zorgvuldigheid. Landelijk, maar ook binnen de gemeente Rotterdam.

Maar ondanks negatieve berichten moeten we niet vergeten dat we ondertussen (én tijdens de lockdown) hard aan het voldoen van de AVG gewerkt hebben. En daarbij zijn prestaties geleverd om trots op te zijn! De belangrijkste prestaties zijn:

- Er is een prachtig nieuw register van verwerkingen en datalekkenregister, waardoor nog beter overzicht bestaat en gestuurd kan worden;
- er is een groot aantal DPIA's (Data Protection Impact Assessments) verricht op risicovolle verwerkingen van persoonsgegevens;
- er is een inhaalslag gemaakt bij de verwerkingsovereenkomsten;
- er is een uittreksel van het register van verwerkingen online geplaatst;
- de AVG is een prominent onderwerp aan de directietafels en
- er is ingezet op het vergroten van het privacybewustzijn (e-learning Privacy en Informatieveiligheid)

Maar helaas zijn we er nog niet en blijft voortdurende aandacht nodig om grip te krijgen op de verwerking van persoonsgegevens in de gemeente Rotterdam. Want niet alle risico's zijn in beeld. We hebben een aantal stevige datalekken gehad, waarbij gevoelige gegevens van een groot aantal burgers op straat kwam te liggen. Nog steeds blijkt dat er verwerkingen zijn die niet eerder in beeld waren en waarvan we dus niet weten of die aan de AVG voldoen. In sommige gevallen blijkt zelfs dat de grondslag niet klopt of ontbreekt. Er blijft dus nog wat onder de radar. Dit bemoeilijkt het toezicht en vergroot de risico's.

Daarnaast zien we dat, ondanks alle aandacht die er binnen het concern is voor de AVG er verwerkingen gestart zijn zonder de verplichte DPIA, of gestart zonder dat de DPIA procedure is afgerond. We zien datalekken die te laat zijn gemeld, maatregelen die niet concreet genoeg zijn om nieuwe datalekken te voorkomen en afgesproken beheersmaatregelen die niet nagekomen worden. Dit geldt ook voor de DPIA's die reeds zijn verricht. Hieruit komen een groot aantal beheersmaatregelen om de risico's te mitigeren. Het is zaak dat deze maatregelen voortvarend worden opgepakt.

In dit jaarverslag worden daar ook aanbevelingen voor gedaan. Deze sluiten aan op de bevindingen van de onderzoeken van Concern Auditing, het Plan van Aanpak en de uitkomsten van de onderzoeken van de FG. Door dit uit te voeren kunnen we werken aan een basis die op orde is. Daarna volgt de grote uitdaging om de AVG parallel te laten lopen met de ontwikkelingen in de samenleving (algoritmen, AI) en de ambities van de gemeente Rotterdam.

En dit is mogelijk. Er is in Rotterdam een enorme drive tot innovatie gecombineerd met durf, expertise en voldoende middelen om de ambities mogelijk te maken. Dit met in acht neming van de spelregels van de AVG. Op dit gebied zijn de afgelopen jaren al successen te melden.

Jaarverslag Functionaris Gegevensbescherming 2020

Voorbeelden zijn de inzet van bodycams om onze boa's te beschermen (landelijk hebben wij daarmee een primeur), slimme technologie om de verkeersstromen in goede banen te leiden, aanpak overlast met geluidssensors en aanpak van naastplaatsingen.

Maar dat gaat vaak niet vanzelf. Door privacy by design, dus een goed ontwerp aan de voorkant van elk nieuw project, kunnen we die bescherming inbouwen en zo met een gerust(er) hart de digitale toekomst tegemoet. Dat bespaart tijd, geld en frustratie wanneer tijdens het proces blijkt die borging er niet inzit waardoor aanpassingen nodig zijn. Zonder die bescherming van de rechten van Rotterdammers komt de haalbaarheid van die ambities onder druk te staan. Dat is de uitdaging waar we nu voor staan.

Matthijs Mulder FG

[Redacted signature]

[Redacted text]

Jaarverslag Functionaris Gegevensbescherming 2020

2. Beleid

De gemeente Rotterdam heeft grote ambities op het gebied van digitalisering. Denk aan de digitale stad, de digitale transformatie van de dienstverlening en ontwikkelingen in de zorg, veiligheid, leefbaarheid en verkeer. Of datagedreven werken dat ons helpt met het verbeteren van beleid, net als het gebruik van algoritmes, diverse vormen van cameratoezicht en samenwerking met partners. Allemaal processen waarbij persoonsgegevens van burgers worden gebruikt en waar de AVG van toepassing is. Deze ontwikkelingen gaan snel. Het jaar 2020 was ook het jaar van de Covid-19 pandemie. De pandemie heeft het verwerken van persoonsgegevens tot een ongekennde schaal gebracht. Bij het testen, bron- en contactonderzoek en vaccineren worden persoonsgegevens van miljoenen burgers verwerkt. Het snel inregelen hiervan met gebruik van data is dan onvermijdelijk, maar werpt ook vragen op over de beveiliging van deze data met, zoals we in januari zagen, een groot landelijk datalek als gevolg. Maar niet alleen beveiliging, maar ook helder zijn waarvoor we de gegevens gebruiken en de burger zeggenschap geven over hun gegevens.

Ook de toeslagenaffaire ontstond voor een groot deel door onzorgvuldige omgang met persoonsgegevens. We zien hier de (onbedoelde) gevolgen van een combinatie van het gebruik van algoritmes, zwarte lijsten, discriminerend datagebruik, bewaartermijnen die niet gehandhaafd zijn en een gebrek aan transparantie.

We zien dus enerzijds een grote vraag naar het gebruik van data, maar anderzijds gebeurtenissen die het vertrouwen van burgers in de overheid kunnen ondermijnen.

Deze risico's dwingen Rotterdam niet alleen tot een grotere zorgvuldigheid en scherper sturen op de veiligheid van persoonsgegevens, maar ook om te zorgen dat je klaar staat om met inachtneming van de AVG de nieuwe ontwikkelingen mogelijk te maken. Al deze ontwikkelingen vragen een heldere visie, uitgewerkt in procedures en richtlijnen, waarbij inzet en betrokkenheid bij de AVG het uitgangspunt is en de wens om hieraan te voldoen vanzelfsprekend. Want de Rotterdamse ambities worden pas mogelijk als rechten van onze burgers en medewerkers goed worden beschermd en het vertrouwen er is dat persoonsgegevens in goede handen zijn bij de overheid. Diverse voorbeelden in onze gemeente hebben laten zien dat dit mogelijk is.

Kortom, dit alles vraagt ook de komende jaren een voortzetting van de ingezette aanpak en sturing vanuit het management. Alleen op die manier kunnen wij als gemeente onze ambities realiseren en de burger erop kan vertrouwen dat zijn of haar gegevens bij de gemeente in veilige handen zijn.

In 2020 is de vervolimplementatie van de AVG, zoals vastgelegd in het Plan van Aanpak, in een stroomversnelling gekomen door een directere sturing van de gemeentesecretaris en de conerndirectie. Om de ambities te realiseren, zullen we hier in 2021 flink op door moeten pakken.

3. Processen

Vertrouwen van de burger in de overheid is essentieel, aangezien burgers voor veel processen wettelijk verplicht zijn hun persoonsgegevens ter beschikking te stellen. Door de toeslagenaffaire is nog eens pijnlijk duidelijk geworden wat er mis kan gaan. De AVG reikt praktische handvatten aan voor verantwoord omgaan met data. De overheid moet open zijn en zich kunnen verantwoorden aan de burger. Uniforme procedures ondersteunen deze verantwoordelijkheid en leiden tot het verder verbeteren van processen.

Jaarverslag Functionaris Gegevensbescherming 2020

Op hoofdlijnen gelden in de gemeentelijke organisatie procesafspraken, maar naleving van de AVG wordt bemoeilijkt als taken, verantwoordelijkheden en processen niet duidelijk zijn. Uitvoering van het privacybeleid moet ertoe leiden dat we medio 2021 kunnen zeggen: de privacyorganisatie is voor wat betreft de basis in 'in control'. Dat wil zeggen dat we de basale wettelijke verplichtingen uit de AVG zoals het register, DPIA's en verwerkersovereenkomsten nakomen waardoor we inzicht hebben en de risico's in beeld zijn. Daarvoor moet wel het in 2019 vastgestelde Plan van Aanpak Privacy versneld worden uitgevoerd.

We zijn dus goed op weg, maar we zijn er nog niet. Dit geldt ook voor de uitvoering van de aanbevelingen uit de Audit Algemene Verordening Gegevensbescherming (AVG) 'Duurzaam en aantoonbaar', die de afdeling Concern Auditing 11 juli 2020 presenteerde. Hierin wordt gesteld dat Rotterdam nog niet duurzaam AVG-proof is.

Zoals in de inleiding al is genoemd, wordt voor alle in het register van verwerkingen opgenomen risicovolle verwerkingen van persoonsgegevens een DPIA (Data Protection Impact Assessment) uitgevoerd. Dit is een risicoanalyse, waarmee wordt getoetst of aan alle organisatorische en beveiligingsmaatregelen van een verwerking wordt voldaan. Ook wordt duidelijk waar maatregelen nodig zijn.

In 2020 had het cluster W&I als eerste deze opgave gereed. Ook de clusters BCO, DV, SO en SB hebben grote voortgang geboekt. Eind 2020 was de gemeente Rotterdam op 60 procent van de opgave. Uit deze DPIA's kwam een groot aantal 'herstelmaatregelen'. Dit zijn vaak serieuze zaken als het op orde brengen van het informeren van de burger, logging, autorisaties, awareness en handhaving van bewaartermijnen waar dat nodig is. De maatregelen worden in 2021 uitgevoerd. Door op deze manier en risicogericht te werken, kunnen we als organisatie voldoen aan de wettelijke normen volgens de AVG.

Daarnaast is het uitvoeren van een DPIA verplicht voordat met een nieuwe risicovolle verwerking wordt begonnen. Waar voorheen erg geworsteld werd met deze verplichting, is in 2020 het besef dat aan deze verplichting moet worden voldaan behoorlijk ingedaald in de organisatie. Bovendien helpt een DPIA met het beter inrichten van de processen.

Met het opstellen van de DPIA's hebben de proceseigenaren, Privacy Officers, Security Officers en Recordsmanagers (Informatiebeheer) intensief samengewerkt. Deze samenwerking heeft tot resultaten geleid waar we als gemeente trots op kunnen zijn, met een flink aantal verwerkingen voor innovatieve toepassingen. Denk daarbij aan DPIA's voor geluidsmetingen, verkeersmonitoring, slimme camera's en de bodycam. Rotterdam loopt hierin vooruit.

4. Samenwerking

Naast het beschermen van de fundamentele rechten van de burger van wie we persoonsgegevens verzamelen, is een tweede doel van de AVG het zogenaamde vrije verkeer van persoonsgegevens. Om dit vrije verkeer te garanderen én tegelijkertijd de rechten van de burger te beschermen gelden hier strenge eisen voor. Wanneer de gemeente een (externe) partij inschakelt om namens haar persoonsgegevens te verwerken, kan zij daarvoor alleen gebruikmaken van verwerkers die afdoende garanties bieden dat die verwerking aan de vereisten van de AVG voldoet.

Die vereisten worden vastgelegd in een overeenkomst met de verwerkende partij. Het is goed te melden dat Rotterdam erin 2020 in is geslaagd voor de meeste verwerkingen waarbij een (externe) verwerker is betrokken een overeenkomst af te sluiten waarin die garanties zijn vastgelegd. Eind 2020 ging het om 170 verwerkingen waarbij een verwerkersovereenkomst nodig is. Er waren 148 overeenkomsten afgesloten. Ook de resterende overeenkomsten

Jaarverslag Functionaris Gegevensbescherming 2020

moeten worden afgesloten, daarnaast is het zaak de 'oude overeenkomsten' te herzien naar de AVG.

Gegevensdeling

Een andere vorm van samenwerking is met de partners op het gebied van veiligheid en zorg, zoals het Riec en het Veiligheidshuis. Het delen van gegevens tussen partijen helpt om meervoudige problematiek te signaleren en op te lossen, maar geeft ook grote privacyrisico's. Over wat hierbij wel en niet mag, bestaat veel onduidelijkheid.

Steeds zal een zorgvuldige afweging moeten worden gemaakt, met oog voor de risico's voor privacy, discriminatie en stigmatisering. Nieuwe wetgeving zoals de Wgs (wet gegevensverwerking door samenwerkingsverbanden) en de WAMS (Wetsvoorstel Aanpak meervoudige problematiek sociaal domein) bieden een juridisch kader, maar vereisen ook die afweging. In het toezichtskader van de Autoriteit Persoonsgegevens, 'Focus AP 2020-2023' is gegevensdeling onderdeel van de speerpunten. De AP wijst erop een goede afweging te maken tussen nut en noodzaak. In 2021 krijgt dit onderwerp ook binnen de gemeentelijke organisatie volop de aandacht.

5. Informatiebeveiliging

De AVG brengt met zich mee dat een organisatie moet aantonen dat zij passende technische en organisatorische maatregelen neemt om persoonsgegevens te beveiligen. De Autoriteit Persoonsgegevens heeft bij organisaties stevige boetes uitgedeeld wanneer dat niet in orde was. Ook is dit een speerpunt van hun toezicht.

In 2020 werd de Baseline Informatiebeveiliging Overheid (BIO) van kracht. Dit is een basisniveau voor informatiebeveiliging voor de gehele overheid. Er ligt een ambitieus programma om ervoor te zorgen dat de beveiliging van (persoons)gegevens gebeurt aan de hand van de BIO-normen. De verdere invoering van de BIO is in 2021 een van de belangrijkste thema's.

Mede door technologische 'tools' te gebruiken, kan de organisatie beter sturen op de effectiviteit van de technische en organisatorische maatregelen. Daarnaast loopt een project om concernbreed een loggingbeleid in te richten zodat dit bij alle systemen doorgevoerd kan worden en we kunnen aantonen dat we ook aan die verplichting voldoen. Logging is het verzamelen en beoordelen van systeemdata en waarschuwingen van bijvoorbeeld applicaties, netwerk infrastructuur, servers en desktop PC's waarmee ongeoorloofde toegang tot dat systeem of tot bepaalde datasets kan worden gesignaleerd.

Daarnaast vindt in het eerste kwartaal van 2021 de verdere uitrol van *Privacy by Design* (hierna PbD) plaats. Er zijn acht processen benoemd waar PbD wordt uitgerold. Denk bijvoorbeeld aan aanschaf en inrichting van applicaties en processen. Nog te vaak zien we dat bijvoorbeeld bewaartermijnen en logging niet aan de AVG voldoen, omdat dit in 'oude' systemen niet is ingericht. Hierbij worden onder andere bij aanschaf en ontwikkeling van nieuwe systemen de privacy en informatiebeveiliging aan de voorkant geregeld. Bijvoorbeeld een 'knop' waarmee persoonsgegevens gewist kunnen worden, naar aanleiding van een AVG-verzoek van een burger. Of een signaleringsfunctie voor bewaartermijnen.

Uitvoering van dit programma is essentieel om risico's op dit gebied te voorkomen.

Jaarverslag Functionaris Gegevensbescherming 2020

Bewustwording

In 2020 zijn voortvarend stappen gezet op het gebied van bewustwording, zowel binnen de clusters als met de Awareness campagne 'Blijf alert!' Met de voortzetting van deze campagne kwam eronder meer een e-learning voor alle medewerkers en de 10 gouden geboden. Ondanks vele inspanningen zien we de menselijke factor nog steeds als de grootste oorzaak van datalekken en het te laat onderkennen hiervan. Daarom is het advies om dit programma te versterken met aanvullende technologische instrumenten om het bewustzijn te vergroten en te stimuleren dat mensen er daadwerkelijk naar handelen.

Datalekken

In 2020 waren er 188 datalekken. Dat zijn er ongeveer evenveel als in 2019. Ons protocol datalekken schrijft voor dat alle datalekken worden geëvalueerd, zodat maatregelen kunnen worden genomen die herhaling voorkomen. Het merendeel van de datalekken is geëvalueerd. In de evaluaties worden ook de te nemen maatregelen genoemd. Deze zijn echter niet altijd concreet (bijvoorbeeld 'beter uitkijken voor je iets mailt').

Een herziening van het datalekkenprotocol moet dit proces verbeteren zodat ook de effectiviteit van de maatregelen gemeten kan worden, toegezien wordt op het daadwerkelijk doorvoeren van de maatregelen en gericht gewerkt kan worden aan het voorkomen van datalekken.

6. Recht van betrokkenen

In de AVG staat de betrokkene centraal en heeft die een aantal rechten zoals het recht op informatie, inzage, rectificatie en verwijdering van gegevens. Dit recht is belangrijk en dient tevens om de naleving van de AVG af te dwingen. Immers, je moet een betrokkene kunnen uitleggen waarom je zijn gegevens nodig hebt, wat ermee gebeurt en hoe ze beveiligd zijn. In 2020 is het proces van recht van betrokkenen verbeterd. Er werden 153 verzoeken ingediend. Het overgrote deel betrof het recht op inzage, gevolgd door het recht op wijziging van gegevens. Van deze aanvragen werd 77 procent afgehandeld binnen de termijn van een maand. Dat is een verbetering ten opzichte van voorgaande jaren. In 2019 was dat nog maar 45 procent.

Transparantie

Een belangrijke mijlpaal was daarnaast het plaatsen van een uittreksel van het register van verwerkingen op de website. Hierdoor is de informatie aan burgers verbeterd. Maar ook hier is nog verbetering mogelijk. Nog vaak vragen burgers wat er met hun gegevens gebeurt of met wie deze worden gedeeld en duurt het lange tijd hierop adequaat antwoord te geven. In 2021 worden ook samenvattingen van DPIA's gepubliceerd. Hiermee wordt de informatie aan burgers verder verbeterd en wordt voldaan aan de motie 'Beslagen ten ijs komen'.

7. Verantwoorden

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aan te tonen dat die voldoet aan de privacyregels. In 2020 hebben we de eerste stap gezet om het register van verwerkingen over te zetten in een nieuw systeem waardoor deze beter beheerst kunnen worden. In 2020 is de interne verantwoording over de AVG verbeterd. Vanuit de privacykolom worden dashboards en rapportages opgesteld ter verantwoording naar CD en/of college. Een vervolgstap is dat de verantwoordelijken zelf rapporteren over de gemaakte voortgang waar het gaat om de AVG, waar nodig geadviseerd door de privacy office.

8. Diversen

Wet politiegegevens

Naast de AVG heeft de Wet politiegegevens (Wpg) voor onze organisatie de nodige consequenties. Het gaat daarbij meestal om verwerkingen waarbij BOA's zijn betrokken, zoals handhaving en de Leerplichtwet. In 2020 zijn de eerste stappen hiervoor gezet, die in 2021 afgerond moeten worden. Dit gebeurt door onder meer DPIA's te verrichten. Bij SB wordt een nieuw systeem ingericht om de verschillende wetten ook administratief en organisatorisch op elkaar af te stemmen.

Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (hierna: AP) is de toezichthouder op de AVG in Nederland. In 2019 is de AP gestart met een onderzoek naar Smart City-toepassingen bij (grote) gemeenten. Het onderzoek richt zich op gegevensverwerkingen in de openbare ruimte met sensoren en andere technologieën. Het gebruik van data in de openbare ruimte raakt namelijk iedereen die zich daarin begeeft. De digitale overheid is daarom een van de aandachtsgebieden de komende jaren voor de AP. In 2020 heeft de AP haar voorlopige conclusies hierover gepresenteerd. Daarnaast is een gesprek geweest met de wethouder Economie, wijken en kleine kernen. Begin 2021 wordt het definitieve rapport verwacht. Het onderzoek onderstreept het belang om voorafgaand aan een risicovolle verwerking een DPIA te verrichten. Gemeenten moeten duidelijk aangeven welke gegevens er in de praktijk worden verwerkt met bijvoorbeeld sensoren en camera's aldus de AP. Daarnaast loopt een onderzoek naar de inzet van camerawagens tijdens de coronacrisis. Voorts heeft de AP diverse malen contact opgenomen met de FG naar aanleiding van datalekken en klachten van burgers.

FG

Team FG (3 fte) heeft, naast de taken op het gebied van DPIA's en datalekken, dit jaar de volgende onderzoeken gedaan:

- naar de juistheid van het register van verwerkingen;
- naar de opvolging van maatregelen naar aanleiding van datalekken;
- naar het systeem ██████ (publieksreacties);
- naar de three lines of defence bij gemeentelijke systemen.

De rapporten zijn besproken met de proceseigenaren en in de Stuurgroep Privacy en delen van de aanbevelingen worden meegenomen bij de verdere uitrol van het programma.

Daarnaast heeft Team FG (digitale) lezingen georganiseerd over onder meer datalekken, besluiten van de AP en uitleg van de AVG.

Samenwerking

De FG werkt nauw samen met de Concern Privacy Officer en de Chief Information Security Officer. Hun input is in dit jaarverslag verwerkt. Het jaarverslag is besproken in de Stuurgroep Privacy.

Jaarverslag Functionaris Gegevensbescherming 2020

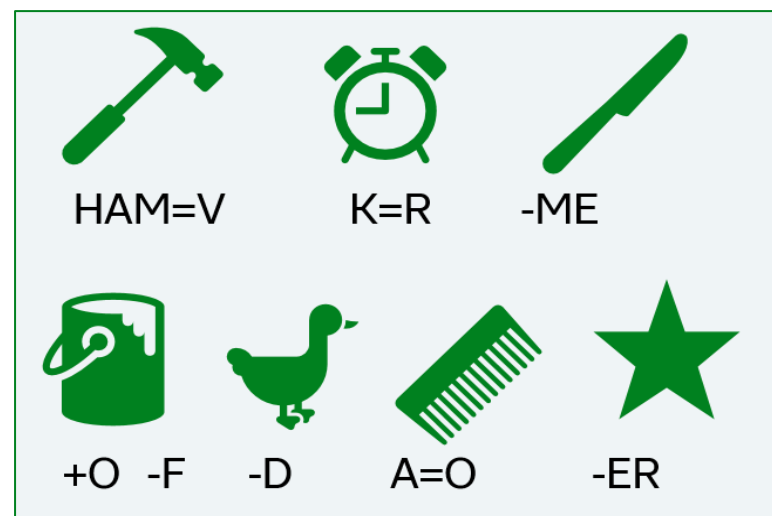
Klachten

Bij de FG zijn diverse klachten, vragen, meldingen datalekken en inzageverzoeken binnengekomen. Reacties hierop zijn in samenspraak met de clusters gegeven, waarbij het in de meeste gevallen lukte om de burgers van antwoord te voorzien. Veel klachten gaan over het recht op inzage, waarbij klagers meer stukken willen zien dan zij gekregen hebben. Ook zijn er veel vragen over de reden van het gebruik van sommige persoonsgegevens voor een bepaald proces.

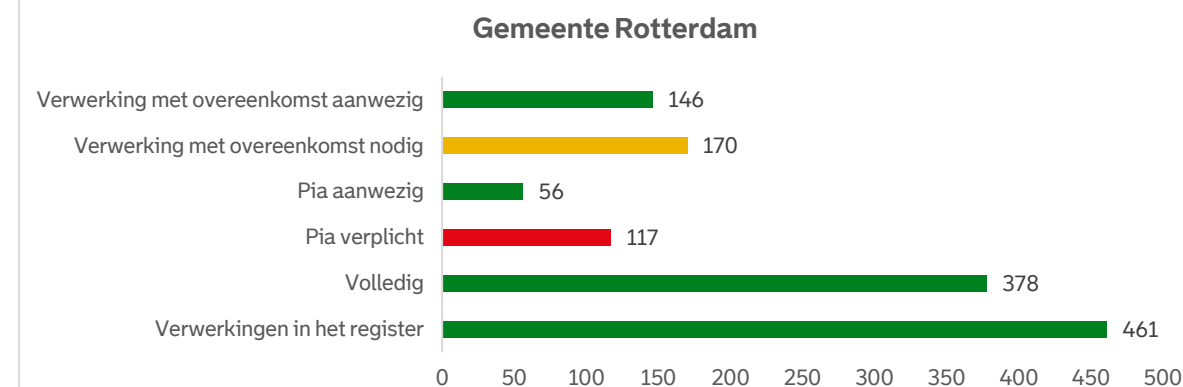
RAPPORTAGE PRIVACY ROTTERDAM December 2020, 2^e editie



Informatie:

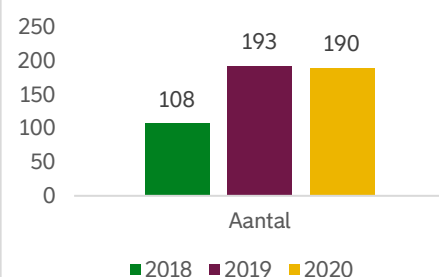


Verwerkingsregister (PRiC)

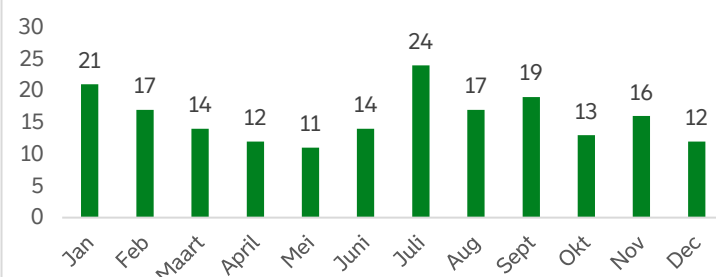


Datalekmeldingen

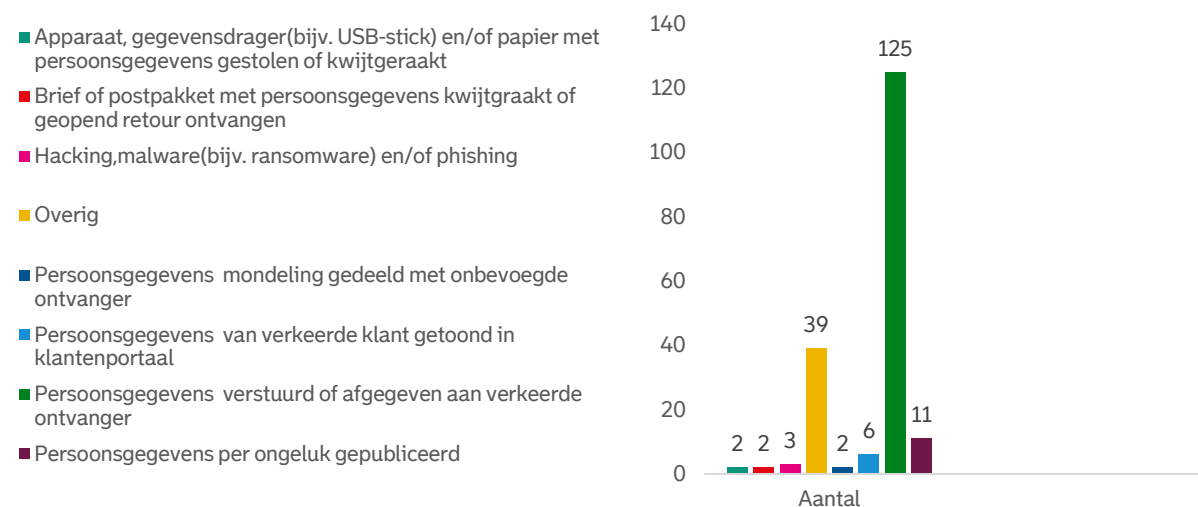
Datalekmeldingen per jaar



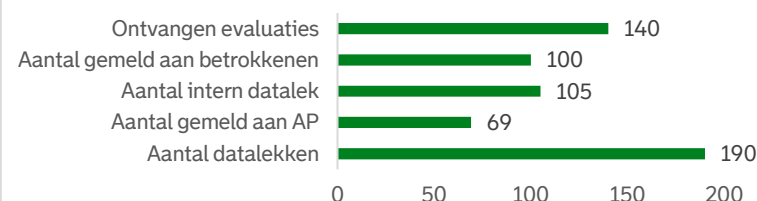
Aantal datalek meldingen per maand 2020



Totalen per categorie 2020



Totalen 2020

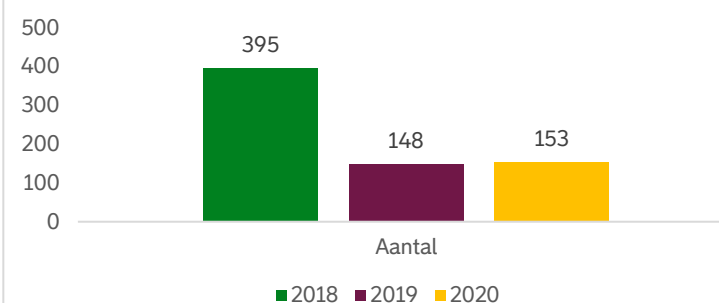


Persoonsgegevens gelekt

Bijzondere persoonsgegevens	29
Financiële gegevens	49
Burgerservicenummer (BSN)	62

Rechten van Betrokkenen

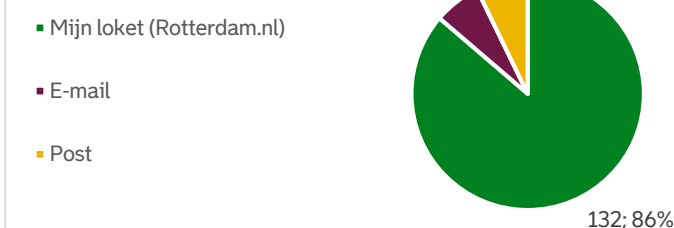
AVG verzoeken per jaar



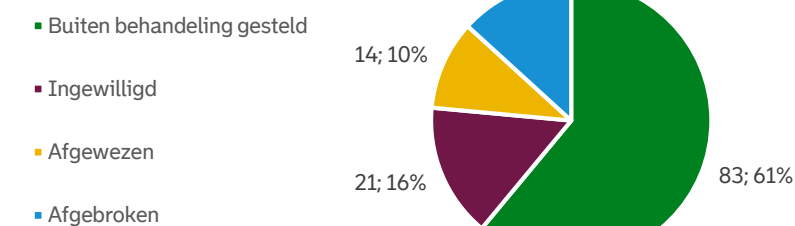
Hoelang duurt het afhandelen van een AVG verzoek?



Hoe komt een AVG verzoek binnen?



Wat is de uitslag van een AVG verzoek?



Van welke AVG rechten wordt gebruik gemaakt?

