Auteur: Nico Mookhoek is privacy jurist en oprichter van DePrivacyGuru. DePrivacyGuru helpt organisaties op een pragmatische manier met hun privacyvraagstukken. Van FG as a service tot standaarddocumenten en hoogwaardig advies. Nico is daarnaast jurylid van de Nederlandse Privacy Awards. Nico is bereikbaar via: mookhoek@nmla.nl.

Algemene Verordening Gegevensbescherming

Wat heeft drie jaar AVG ons gebracht?

Afgelopen mei was de Algemene Verordening Gegevensbescherming (AVG) drie jaar van kracht. De nieuwe wet, een implementatie van een Europese Richtlijn, werd samen met de Uitvoeringswet, de UAVG, op 25 mei 2018 van toepassing. Wat heeft de nieuwe wet de eerste drie jaar van haar bestaan opgeleverd?

Bij de invoering werd vooral de nadruk gelegd op de hogere boetes die de toezichthouder, de Autoriteit Persoonsgegevens (AP), op kan leggen. De maximale boete die onder de AVG opgelegd kan worden is 20.000.000 euro of 4% van de wereldwijde jaaromzet, mocht dat bedrag hoger uitkomen. Hoewel dit aspect veel aandacht kreeg, is de kans op een boete voor een gemiddeld bedrijf, klein.

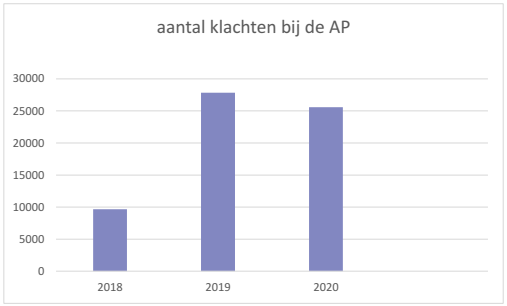
Werden er dan helemaal geen boetes uitgedeeld? Jazeker wel, en vrij forse ook. Bureau Krediet Registratie (BKR) is koploper met een boete van 830.000 euro voor het berekenen van kosten voor een inzageverzoek. Een bedrijf dat vingerafdrukken van haar personeel liet vastleggen voor toegangscontrole kon 725.000 euro boete aftikken. Hekkensluiter van de top 3 is Uber dat al kort na de invoering van de AVG in november 2018 een boete opgelegd kreeg van 600.000 euro voor het niet melden van een datalek. Voor hetzelfde feit kreeg Booking.com afgelopen maart een boete van 475.000 euro.

Het HagaZiekenhuis kreeg in juli 2019 een boete van 460.000 euro opgelegd voor het onvoldoende beveiligen van persoonsgegevens (door de Rechtbank later gematigd tot 350.000 euro). Ook het OLVG kreeg een boete voor slecht beveiligde patentendossiers opgelegd: 440.00 euro. Maar ook kleinere organisaties ontsnappen niet aan het toezicht van de AP. Een orthodontiepraktijk moest 12.000 euro overmaken aan de AP vanwege een onbeveiligde patiëntenwebsite.

Op de site van AP zijn al deze boetes, en ook de andere opgelegde sancties terug te lezen. Het boetebeleid is daarbij gebaseerd op de beleidsregels zoals die in 2019 zijn vastgesteld. Een onderbouwing van de boete gebaseerd op deze beleidsregels is te vinden in het Besluit over de betreffende boete.

Privacy bewustzijn neemt toe

Tweede opvallende ontwikkeling in de drie jaar dat de AVG van kracht is, is het toegenomen privacy bewustzijn bij burgers. Uit een onderzoek van de AP begin 2020 blijkt dat 94% zich zorgen maakt over de bescherming van haar/zijn persoonsgegevens, 32% daarvan maakt zich zelfs ernstige zorgen. De door de AP opgelegde boetes zullen daar zeker aan bijgedragen hebben. Maar ook de zichtbaarheid van de AP als de privacy in het geding is heeft hierbij geholpen, zoals bij de CoronaMelder App. Dat toegenomen privacy bewustzijn bij burgers vertaalt zich ook in het aantal klachten dat de AP



Figuur 1 - Aantal klachten bij AP.

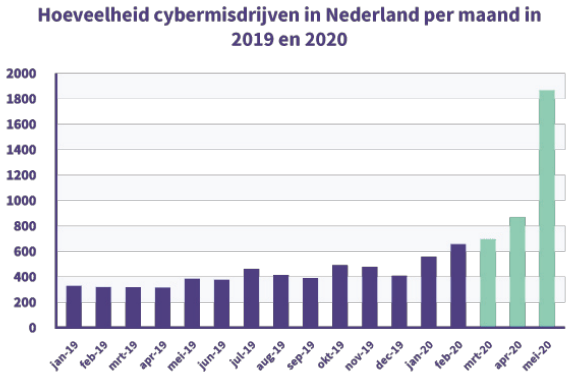
ontving. Sinds de invoering van de AVG hebben burgers het recht een klacht in te dienen bij de toezichthouder als zij niet tevreden zijn over de wijze waarop een organisatie met hun persoonsgegevens omgaat. In 2019 groeide dit explosief naar 27.850 klachten. In 2020 bleef het met 25.590 klachten vrijwel op hetzelfde hoge niveau.

De toename betekende een forse vertraging van de afhandeling van klachten door de AP. In maart 2021 luidde de voorzitter van de AP hierover de noodklok. Gemiddeld duurt het volgens hem zes maanden eer de AP kan beginnen met de behandeling van een klacht. Die signalen van de voorzitter klinken al langer. In een interview met Trouw in november 2020 geeft hij al aan dat er achterstanden zijn en dat uitbreiding van de capaciteit met 182 FTE noodzakelijk is.

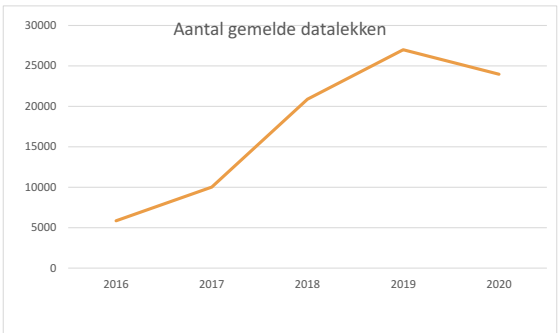
Naar aanleiding van deze signalen liet de minister van Rechtsbescherming, Sander Dekker, door KPMG een onderzoek doen. Uit het onderzoek dat in november 2020 verscheen, blijkt dat de kosten van de AP ten opzichte van andere toezichthouders (ACM, AFM, AT en NVWA) over het algemeen lager zijn. Europees gezien mag de AP volgens het KPMG-rapport niet klagen. Vergeleken met de 31 European Data Protection Board-leden heeft de AP een relatief hoog budget en kent ze een relatief sterke groei in budget en personeel. Tegelijkertijd heeft de AP te maken met relatief meer klachten en meer meldingen van datalekken.

Het rapport signaleert ook dat er nog werk aan de winkel is op het gebied van automatisering en organisatieontwikkeling. 'AP is een organisatie in opbouw. Een aantal functies is nog niet ingevuld, de automatiseringsgraad is laag en bedrijfsvoering staat nog in de kinderschoenen.'

Nadat minister Dekker probeerde de beslissing naar een



Figuur 2 - Aantal Cybermisdrijven in Nederland.



Figuur 3 - Aantal datalekken gemeld bij Autoriteit Persoonsgegevens.

volgend kabinet te tillen, stemde de Tweede Kamer toch in met een motie om de AP uit te breiden. Vanaf 2022 gaat de AP van 184 medewerkers naar 470 voltijdsmedewerkers.

Toename cybercriminaliteit = toename aantal datalekken

Sinds de uitbraak van COVID-19 in 2020 is de cybercriminaliteit fors toegenomen. In mei 2020 is voor het eerst een historische mijlpaal bereikt: er werden meer incidenten op het gebied van cybercriminaliteit bij de politie gemeld dan woninginbraken.

Uit de grafiek blijkt dat maart 2020 een stijging van 119% kende t.o.v. maart 2019. In de maand april werd dat nog overtroffen. Het aantal meldingen van cybercriminaliteit nam in die maand met 174% toe ten opzichte van april 2019.
De cijfers over toenemende cybercriminaliteit zijn ook terug te zien in de rapportage van de AP over datalekken. Een hack, phishing of malware incident leidt altijd tot een datalekmelding. Van een datalek is immers ook sprake als persoonsgegevens gecompromitteerd zijn geraakt, zoals wanneer door een hack het systeem platligt en persoonsgegevens niet meer bereikt kunnen worden. Niet elk beveiligingsincident hoeft dus een datalek te zijn, maar als er persoonsgegevens in het geding zijn, is sprake van een datalek en zal er een melding gedaan moeten worden bij de AP.
De AP geeft jaarlijks een overzicht en analyse van de bij haar gemelde datalekken. De gegevens zijn beschikbaar vanaf 2016.

Sinds de invoering van de AVG is het aantal datalekmeldingen spectaculair gestegen. In 2017 bedroeg het aantal meldingen 10.009, wat al bijna een verdubbeling was ten opzichte van de 5.849 meldingen in 2016. In 2018, het eerste jaar van de AVG werden 20.881 meldingen gedaan, een toename van meer dan 100%. De stijgende lijn zette zich voort in 2019. Het jaar 2020 liet een trendbreuk zien, het aantal meldingen daalde dat jaar rond de 10%. Volgens de toelichting van de AP bij deze cijfers is de oorzaak van deze daling een verminderd aantal meldingen van incassobureaus die een andere werkwijze hebben geïmplementeerd.

Let wel: bovenstaande cijfers betreft het aantal gemelde datalekken. Uit de boetes die aan Uber en Booking.com zijn opgelegd, blijkt dat niet elk datalek ook gemeld wordt bij de AP.

In de rapportage over 2020 licht de AP het aantal datalekken dat verband houdt met cybercriminaliteit extra toe. In 2020 steeg het aantal meldingen over hacking, malware of phishing met 30% ten opzichte van 2019 naar 1.173 meldingen. Opmerkelijk is dat bij 41,5% van de meldingen meer dan 500 personen waren betrokken. Datalekmeldingen met deze oorzaak komen het meest voor in de sector gezondheid en welzijn (13%) gevolgd door onderwijs (11%), ICT-dienstverlening (9%) en handel en autobranche (8%). Op basis hiervan komt de AP tot de conclusie dat vooral grotere organisaties die persoonsgegevens van veel mensen verwerken het doelwit zijn van hacking, malware of phishing.

Het is nu aan de privacy professionals, de Autoriteit Persoonsgegevens maar zeker ook aan de FG's en PO's in het veld om de volgende fase in te gaan.

Toekomst

De eerste drie jaar heeft de AVG in Nederland definitief een plek verworven. Steeds meer organisaties realiseren zich dat privacy een blijvertje is en geen hype. Om de privacy functie te versterken nemen steeds meer organisaties naast een vaak verplichte functionaris gegevensbescherming (FG) ook een privacy officer (PO) aan. Die laatste is meer eerste aanspreekpunt voor de medewerkers bij privacy vragen en issues.

De Autoriteit Persoonsgegevens gaat uitbreiden, wat ruimte geeft om de taken voortvarender uit te voeren. En voor wie dacht dat het allemaal wel weer over zou waaien: de opgelegde boetes zijn niet mals. Ook de burger wordt sinds de invoering van de AVG steeds privacy bewuster en doet meer beroep op zijn rechten uit de AVG.

Kortom, de eerste stappen zijn gezet en het privacy vak groeit naar volwassenheid. Het is nu aan de privacy professionals, de Autoriteit Persoonsgegevens maar zeker ook aan de FG's en PO's in het veld om de volgende fase in te gaan.

Twee zaken zijn daarbij wat mij betreft essentieel. Ten eerste meer betrokkenheid van directie en management bij het onderwerp privacy, daar schort het nu nogal eens aan. De FG is bij uitstek de figuur om dit onderwerp bij hen op de agenda te krijgen zodat het net als Legal en Finance een vaste plek krijgt bij het Bestuur.

Een tweede stap die in het verlengde daarvan ligt is de focus te verbreden van AVG naar privacy. Nu de AVG geïmplementeerd is en wordt onderhouden, wordt het tijd te kijken naar privacy in de brede zin van het woord. Daarbij komen meer beleidsmatige onderwerpen aan de orde. Onderwerpen als: 'Gaan we meer doen met het onderwerp privacy nu we voldoen aan de AVG?' 'Hoe kunnen we een privacy gerichte organisatie worden?', 'Willen we privacy gecertificeerd worden?', 'Hoe kunnen we met privacy waarde creëren?, 'Willen we wat met een onderwerp als data-ethiek?'

Kortom, na drie jaar AVG zijn de eerste stappen gezet, nu ligt de bal bij de privacy professionals om het vak tot volwassenheid te brengen.

Bronnen

https://www.autoriteitpersoonsgegevens.nl/nl/publicaties/boetes-en-sancties

Onderzoek taken en financiële middelen bij de AP, KPMG, 2 november 2020.

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken