Vijf jaar AVG-toezicht in vogelvlucht

Sinds de inwerkingtreding van de Algemene Verordening Gegevensbescherming is privacy een veelbesproken onderwerp geworden. Niet alleen de specifieke invulling van de wettelijke bepalingen houdt ons tot op de dag van vandaag bezig, ook de handhaving door de Nederlandse toezichthouder brengt interessante ontwikkelingen met zich mee. In dit artikel blikken we terug op enkele interessante boetes die de Autoriteit Persoonsgegevens de afgelopen jaren heeft uitgedeeld. Waar moet je als organisatie goed op letten om te voorkomen dat ze op een dag bij jou op de stoep staan?

Laura Huijts LL.M., CIPP/E, CIPM, CIPT
is manager bij KPMG Cyber & Privacy.

Danielle Molenkamp LL.M., CIPP/E
is consultant bij KPMG Cyber & Privacy.

Malik Elbaz LL.M., CIPP/E
is consultant bij KPMG Cyber & Privacy.

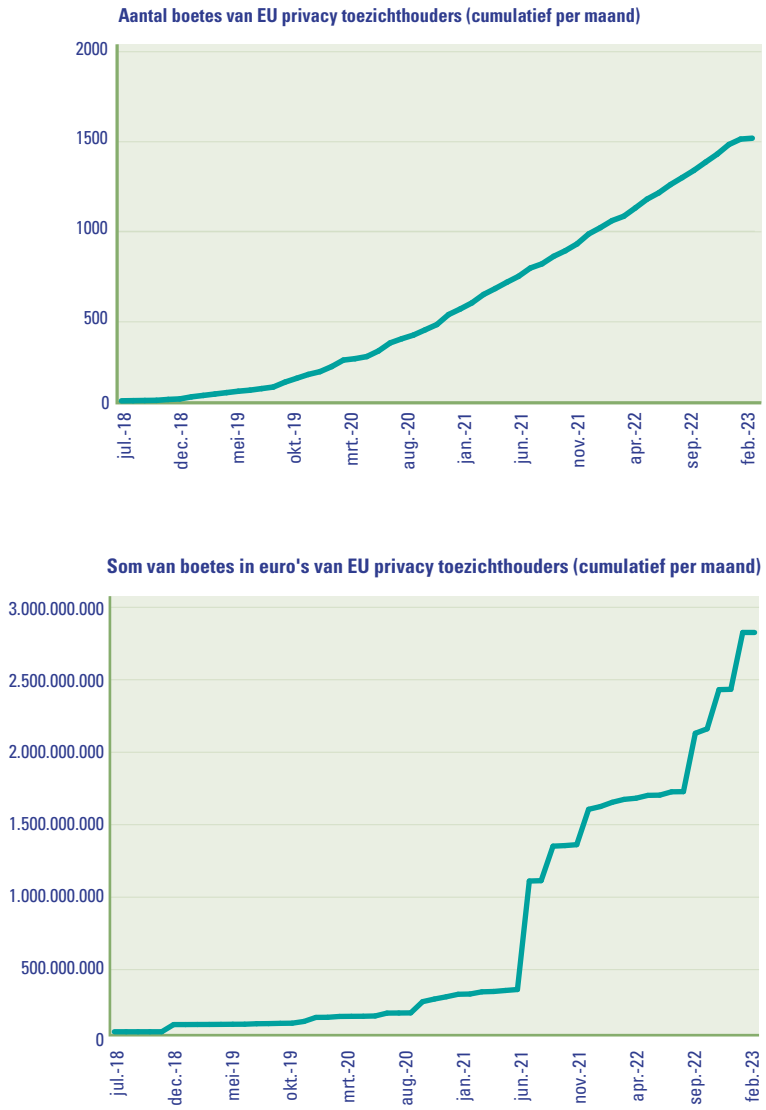
INLEIDING

De Algemene Verordening Gegevensbescherming (hierna: AVG) trad in mei 2016 in werking. Organisaties kregen een transitieperiode van 2 jaar – tot mei 2018 – om hun bedrijfsvoering met de AVG in overeenstemming te brengen. Na die periode mogen privacytoezichthouders handhaven middels het opleggen van een maximale boete van 20 miljoen euro of 4 procent van de jaarlijkse wereldwijde omzet van een organisatie, waarbij de hoogste variant geldt. Echter, de Autoriteit Persoonsgegevens (hierna: AP) is ook na deze transitieperiode terughoudend geweest in het uitdelen van boetes. In de eerste jaren na 2018 zijn er slechts enkele boetes opgelegd. In de jaarverslagen van de toezichthouder is te lezen dat dit komt door de beperkte capaciteit van de organisatie en de keuze om die capaciteit met name in te zetten op grote, impactvolle onderzoeken, zoals de toeslagenaffaire of vraagstukken die verband houden met het coronavirus. Pas in 2021 leek de AP goed op stoom te komen en werden meer organisaties beboet, en voor grotere bedragen. Deze trend gold ook voor de overige Europese toezichthouders – zie hiervoor figuur 1.[1]

Het feit dat de AP nu regelmatig boetes uitdeelt, is reden om hierop terug te blikken en om te onderzoeken waar organisaties op moeten letten om compliant te zijn met de AVG en een boete te voorkomen. In dit artikel worden per boetecategorie één of meer boetebesluiten besproken.[2] De AP heeft boetes uitgedeeld in onderstaande categorieën, die wij hierna in detail bespreken:

- ontoereikende grondslag voor gegevensverwerking;
- onvoldoende nakoming van informatieverplichtingen;
- onvoldoende uitvoering van de rechten van betrokkenen;
- niet-naleving van de algemene beginselen inzake gegevensverwerking;
- ontoereikende technische en organisatorische maatregelen;
- onvoldoende nakoming van de meldplicht datalekken.

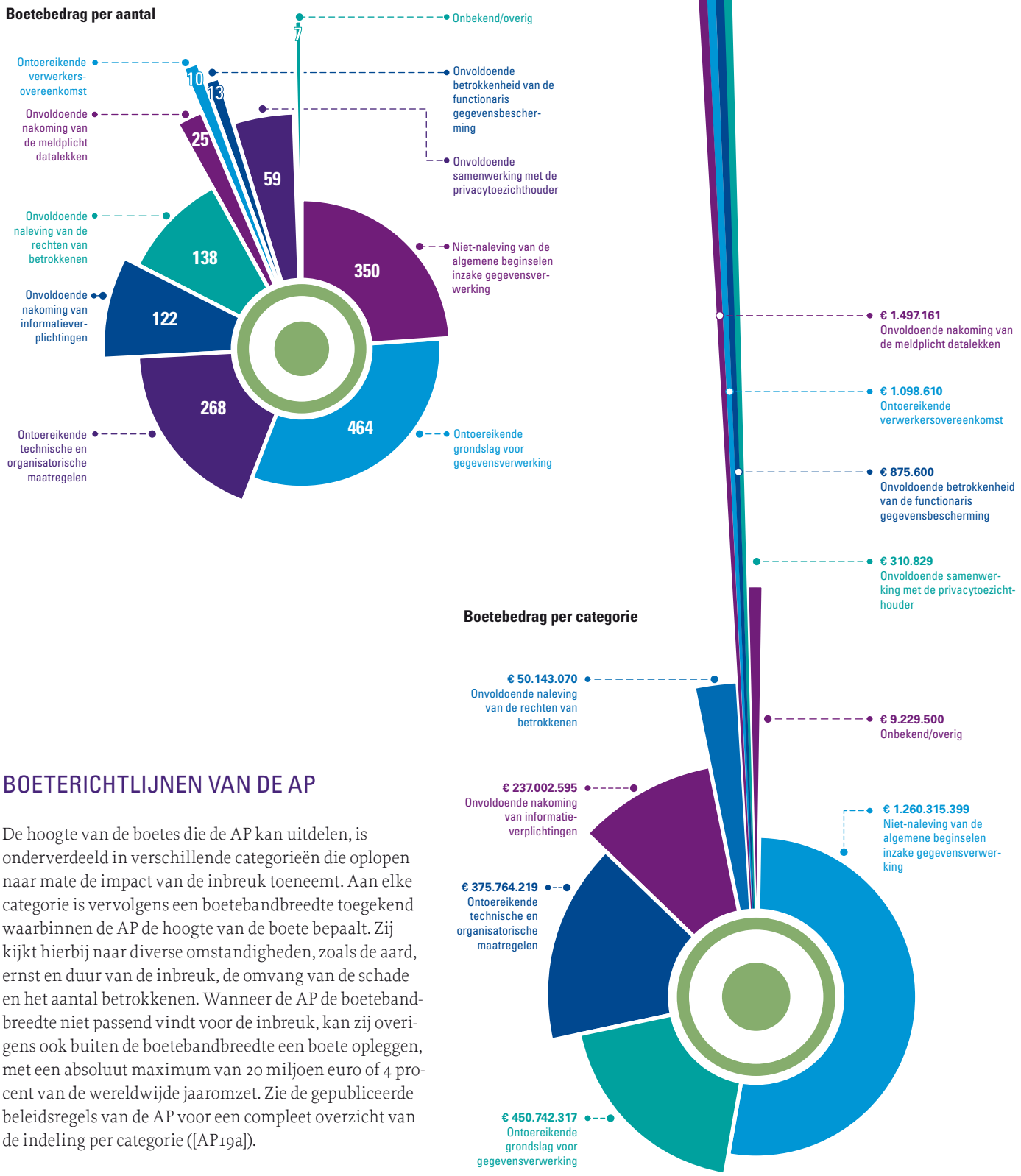
Figuur 1. Overzicht van het aantal en de hoogte van boetes van Europese privacytoezichthouders ([CMS23]).



1 Let wel: deze getallen reflecteren enkel de openbaar gemaakte boetes en geven dus niet het volledige aantal weer. Daarnaast betreffen deze getallen enkel daadwerkelijke boetes en dus niet de gevallen waarbij na een waarschuwing of last onder dwangsom correcte opvolging is gegeven. Zie ook [AP].

2 Aan de hand van de boetecategorieën is een selectie gemaakt van de gepubliceerde boetes.

Figuur 2. Overzicht van het aantal en de hoogte van boetes per boetecategorie ([CMS23]).



BOETERICHTLIJNEN VAN DE AP

De hoogte van de boetes die de AP kan uitdelen, is onderverdeeld in verschillende categorieën die oplopen naar mate de impact van de inbreuk toeneemt. Aan elke categorie is vervolgens een boetebandbreedte toegekend waarbinnen de AP de hoogte van de boete bepaalt. Zij kijkt hierbij naar diverse omstandigheden, zoals de aard, ernst en duur van de inbreuk, de omvang van de schade en het aantal betrokkenen. Wanneer de AP de boetebandbreedte niet passend vindt voor de inbreuk, kan zij overigens ook buiten de boetebandbreedte een boete opleggen, met een absoluut maximum van 20 miljoen euro of 4 procent van de wereldwijde jaaromzet. Zie de gepubliceerde beleidsregels van de AP voor een compleet overzicht van de indeling per categorie ([AP19a]).

BOETEBESLUITEN VAN DE AP

Ontoereikende grondslag voor gegevensverwerking

Vingerafdrukken gebruiken voor tijdklokken van werknemers op basis van toestemming
Persoonsgegevens worden onderscheiden in 'gewone' en 'bijzondere persoonsgegevens', waarbij bijzondere persoonsgegevens gevoelig van aard zijn. Bij gewone persoonsgegevens kan gedacht worden aan naam, adres en telefoonnummer, terwijl bijzondere persoonsgegevens bijvoorbeeld informatie bevatten over gezondheid of politieke opvattingen. Vanwege het gevoelige karakter van die bijzondere persoonsgegevens is het verwerken ervan in beginsel verboden.

In april 2020 heeft de AP een bedrijf beboet voor het onrechtmatig verwerken van bijzondere persoonsgegevens ([AP19d]). Het bedrijf maakte gebruik van scanners waarbij vingerafdrukken van werknemers werden gemaakt voor het in- en uitklokken. Vingerafdrukken zijn biometrische gegevens die worden aangemerkt als bijzondere persoonsgegevens. Hiervoor geldt een verwerkingsverbod, maar in artikel 29 UAVG is bepaald dat het verwerken van deze gegevens wel is toegestaan voor beveiligingsdoeleinden. In deze situatie werden de vingerafdrukken echter uitsluitend gebruikt voor aanwezigheids- en tijdsregistratie, waardoor de uitzondering niet van toepassing is. Toestemming van de werknemers zou tevens een uitzondering kunnen vormen, maar dit wordt veelal niet aangenomen. Toestemming dient namelijk vrijelijk te worden gegeven en dat wordt in een afhankelijke relatie zoals die tussen een werknemer en werkgever niet snel toegelaten. Daarnaast is niet alleen het verkrijgen van toestemming belangrijk, het bedrijf moet dit ook kunnen aantonen. Dit was in casu niet het geval, waardoor het bedrijf in strijd handelde met het verwerkingsverbod van artikel 9 AVG. Dit is door de AP bestraft met een boete van 725.000 euro.

Het onderzoek van de AP benadrukt nogmaals welke voorwaarden worden gesteld aan de toestemming van de betrokkene. Een toestemming is rechtsgeldig wanneer deze vrijelijk, duidelijk en voldoende geïnformeerd is gegeven. Hierbij is van belang dat het weigeren van toestemming in geen enkele vorm nadelige gevolgen mag hebben. Ook dient de toestemming aantoonbaar te zijn.

Wifitracking op basis van een algemene wettelijke grondslag
Het verwerken van (gewone) persoonsgegevens dient gebaseerd te zijn op een van de grondslagen die genoemd worden in artikel 6 AVG. De gemeente Enschede was van mening dat zij voor het meten van drukte in de binnenstad persoonsgegevens mocht verwerken op grond van de uitoefening van een publieke taak. Met behulp van elf sensoren werden voortdurend wifisignalen van voorbijlopende burgers opgevangen, die vervolgens (gepseudonimiseerd) werden opgeslagen. De publieke taak op grond waarvan de persoonsgegevens worden verwerkt, dient in een wettelijke bepaling te zijn opgenomen. Die kon volgens de gemeente worden gevonden in artikel 160 Gemeentewet, maar de AP vond deze bepaling te ruim geformuleerd. Burgers konden op basis hiervan namelijk niet afleiden dat hun persoonsgegevens werden verwerkt. De grondslag van een gerechtvaardigd belang ging in deze situatie ook niet op. Een overheidsinstantie kan zich over het algemeen niet beroepen op deze grondslag, omdat de taken van de overheid in een wettelijke bepaling moeten zijn omschreven. Een uitzondering hierop is wanneer een overheidsinstantie handelt als een private partij, maar daar is in deze situatie geen sprake van.

Naast dat er geen specifieke rechtsgrond is voor de wifitracking, wordt niet voldaan aan het noodzakelijkheidsvereiste. Het meten van drukte kan immers op een veel minder inbreukmakende manier. Bovendien werden de gegevens te lang bewaard, waardoor burgers konden worden gevolgd en leefpatronen konden worden herkend. Op die manier was bijvoorbeeld te achterhalen waar iemand werkte. De verwerking door de gemeente Enschede is dus om meerdere redenen als onrechtmatig aan te merken, wat voor de AP aanleiding is geweest om een boete van 600.000 euro op te leggen ([AP21a]).

Het onderzoek van de AP benadrukt dat overheidsorganisaties moeten oppassen met het baseren van verwerkingen op te algemene bepalingen. Daarnaast moet ook een gedegen beoordeling van het noodzakelijkheidsvereiste worden gedaan.

Het gebruiken van gerechtvaardigd belang voor louter commerciële doeleinden
Als laatste mogelijke grondslag voor het verwerken van persoonsgegevens noemt artikel 6 AVG de behartiging van een gerechtvaardigd belang. Het is bekend dat een overheidsinstantie zich hier over het algemeen niet op kan beroepen, maar er is nog onduidelijkheid of een private partij met uitsluitend commerciële belangen zich hier wel op kan beroepen.

De Nederlandse tennisbond KNLTB heeft persoonsgegevens van zijn leden verstrekt aan twee sponsors voor promotionele doeleinden. Een van de sponsors heeft de adressen van leden gebruikt voor het aanbieden van kortingsflyers en de andere sponsor heeft de leden telefonisch benaderd met een aanbieding. De KNLTB beargumenteerde dat de gegevens zijn verstrekt onder het mom van een gerechtvaardigd belang, maar daar kan volgens de AP geen sprake van zijn. Voor een geslaagd beroep op de grondslag van een gerechtvaardigd belang dient de verwerking noodzakelijk te zijn voor de behartiging

van het belang, mag het belang van de betrokkene niet zwaarder wegen én moet het belang een gerechtvaardigd belang zijn. Dit laatste betekent volgens de AP dat het belang in (algemene) wetgeving of elders in het recht moet zijn benoemd als rechtsbelang. Het dient te gaan om een belang dat in rechte wordt beschermd en kan worden afgedwongen. Bovendien dient de (geschreven of ongeschreven) rechtsregel voldoende duidelijk en nauwkeurig te zijn. De rechtsregel waar de KNLTB de verwerking aan hangt, is de vrijheid van ondernemerschap. De AP noemt dit belang onvoldoende concreet om te kunnen kwalificeren als gerechtvaardigd belang en legt de tennisbond dan ook een boete op van 525.000 euro ([AP19e]).

De KNLTB is het niet eens met de boete en is in bezwaar gegaan. De rechtbank heeft na twijfel over de invulling van het begrip 'gerechtvaardigd belang' prejudiciële vragen gesteld aan het Hof van Justitie. Een prejudiciële vraag is een vraag die een nationale rechter kan stellen aan het Hof van Justitie om een Europese wet uit te leggen. De visie van de AP is al eerder weerlegd door de Europese Commissie en door de rechtbank in de zaak tegen VoetbalTV, waar de AP dezelfde visie over gerechtvaardigd belang hanteerde; het is afwachten of het Hof van Justitie wél meegaat in de visie van de AP.

Of een private partij zich op een gerechtvaardigd belang mag beroepen met uitsluitend commerciële belangen, blijkt onvoldoende duidelijk uit het boetebesluit van de AP. Het is aan te raden deze grondslag zo restrictief mogelijk te gebruiken.

Onvoldoende nakoming van informatieverplichtingen

Een privacyverklaring die niet op de doelgroep aansluit

In 2021 kreeg het steeds populairder wordende TikTok een boete van 750.000 euro van de AP ([AP21b]). TikTok handelde namelijk in strijd met de vereisten uit het eerste lid van artikel 12 van de AVG. Dit artikel stelt onder andere dat organisaties informatie over de verwerking van persoonsgegevens in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal beschikbaar moeten stellen voor betrokkenen. Deze informatie wordt in de praktijk vaak gegeven in de vorm van een privacyverklaring. De privacyverklaring van TikTok werd aan Nederlandse gebruikers echter uitsluitend in het Engels aangeboden. Omdat deze gebruikers voornamelijk jongeren van onder de 16 zijn, mocht TikTok er niet van uitgaan dat zij de Engelse taal machtig waren.

Voor organisaties is het dus van belang om van tevoren de doelgroep te bepalen. Aan de hand daarvan kan een begrijpelijke privacyverklaring worden opgesteld met als maatstaf een gemiddeld lid van de beoogde doelgroep. Daarnaast is van belang dat een vertaling van de privacyverklaring beschikbaar is als de doelgroep een andere taal spreekt. Als er sprake is van een doelgroep bestaande uit jongeren, die specifieke bescherming genieten volgens de AVG, zal een privacyverklaring moeten worden opgesteld die ook voor jongeren begrijpelijk is.

Onvoldoende uitvoering van de rechten van betrokkenen

Een inzageverzoek in lijn met artikel 12 AVG

In artikel 12 van de AVG zijn nadere regels voor de uitoefening van de rechten van de betrokkene vastgelegd. Een van die rechten is het verzoek tot inzage. Het verstrekken van de gegevens moet kosteloos gebeuren, tenzij de verzoeken van de betrokkene ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter. Wat repetitief is, moet individueel worden beoordeeld. Zo ondervond ook het Bureau Krediet Registratie (hierna: BKR). Het BKR bood twee mogelijkheden aan voor het indienen van een inzageverzoek: een inzageverzoek kon ofwel op elektronische wijze worden ingediend (waarvoor betaald moest worden), ofwel eenmaal per jaar gratis via de post. Het standaard betalen voor een inzageverzoek op elektronische wijze was volgens de AP niet in lijn met artikel 12 van de AVG en zij bestrafte dit met een boete van 830.000 euro ([AP19c]).

Het feit dat de optie via de post eenmaal per jaar gratis was, deed daar volgens de AP niets aan af. Ook het feit dat inzage via de post maar één keer per jaar gratis was, was in strijd met artikel 12. Meer dan één inzageverzoek per jaar is niet per definitie buitensporig, dat moet individueel worden beoordeeld.

> Meer dan één inzageverzoek per jaar is niet per definitie buitensporig, dat moet individueel worden beoordeeld

Het inzien van persoonsgegevens is een verwerking waar de AVG op van toepassing is

Vanzelfsprekend zal bij een inzageverzoek de identiteit van de betrokkene moeten worden vastgesteld zodat de juiste gegevens met de juiste betrokkene worden gedeeld. DPG Media kreeg echter een boete van de AP omdat zij vroegen om het opsturen van een kopie van een legitimatiebewijs om betrokkenen te identificeren ([AP22a]). De AP vond dit te ingrijpend, met name vanwege het gevoelige karakter van legitimatiebewijzen. De AP stelt dat gebruik moet worden gemaakt van de minst ingrijpende manier om betrokkenen te identificeren, bijvoorbeeld door een combinatie van informatie die de verwerkingsverantwoordelijke al bezit. Hierbij kan gedacht worden aan een klantnummer in combinatie met een adres.

Het is dus belangrijk te zorgen voor een gratis inzageverzoek en dat, als er sprake lijkt te zijn van een buitensporig verzoek, dit individueel wordt beoordeeld. Daarnaast is het belangrijk voor het identificatieproces dat de minst ingrijpende manier van identificeren wordt gekozen. Het opsturen van een kopie van een legitimatiebewijs lijkt in ieder geval te ingrijpend te zijn.

Niet-naleving van de algemene beginselen inzake gegevensverwerking

Een Europese vertegenwoordiger voor organisaties buiten Europa

De AVG geldt zowel voor organisaties die gevestigd zijn in de Europese Unie als voor organisaties die buiten de EU gevestigd zijn als zij zich richten op het verwerken van persoonsgegevens van EU-burgers. Zo ondervond ook LocateFamily.com. De website voldeed niet aan het vereiste van artikel 27 van de AVG om schriftelijk een vertegenwoordiger in de EU aan te wijzen. Zij waren in de veronderstelling dat zij, doordat zij niet gevestigd waren in de EU, niet aan de AVG hoefden te voldoen. Dit bleek echter niet het geval en leverde de website een boete op van 525.000 euro ([AP20d]).

Door het internationale karakter van het internet ben je als organisatie al vrij snel persoonsgegevens van EU-burgers aan het verwerken. Als dit het geval is en je website bijvoorbeeld beschikbaar is in de EU en de euro als valuta voor transacties gebruikt kan worden, zul je waarschijnlijk moeten voldoen aan de verplichtingen van de AVG. Tevens dien je in dat geval een vertegenwoordiger in de EU aan te wijzen.

Ontoereikende technische en organisatorische maatregelen

Onvoldoende beveiliging van de interne systemen

Een van de eerste boetes die de AP heeft uitgedeeld sinds de inwerkingtreding van de AVG, was aan het Haga-Ziekenhuis. Het ziekenhuis kreeg deze boete opgelegd omdat de medische patiëntendossiers onvoldoende beveiligd waren, waardoor tientallen medewerkers in het dossier van een bekende Nederlander (Barbie van het

tv-programma *Oh Oh Cherso*) konden kijken, zonder dat daar een noodzaak voor was. Het ziekenhuis had hier volgens de AP op moeten monitoren. Daarnaast was de beveiliging onvoldoende, omdat er geen gebruik werd gemaakt van meerfactorauthenticatie. Het treffen van onvoldoende beveiligingsmaatregelen heeft het HagaZiekenhuis een boete van 460.000 euro opgeleverd ([AP19b]).

Twee jaar later deed een soortgelijke situatie zich voor bij een ander ziekenhuis, namelijk het Amsterdamse OLVG. Onvoldoende controle op de geraadpleegde dossiers en een ontoereikende beveiliging werden door de AP bestraft met een boete van 440.000 euro ([AP20c]). Het onvoldoende beveiligen van de interne systemen zien we bij meerdere organisaties terugkomen. Zo kreeg onderhoudsbedrijf CP&A een boete van 15.000 euro voor het ontoereikend beveiligen van de verzuimregistratie ([AP20a]), het ministerie van Buitenlandse Zaken werd beboet voor 565.000 euro voor de te beperkte beveiliging van het Nationaal Visum Informatie Systeem (NVIS) ([AP22b]) en had het UWV onvoldoende technische maatregelen genomen om het proces voor het verzenden van groepsberichten te beveiligen, wat een boete opleverde van 450.000 euro ([AP21c]).

Net als ziekenhuizen werken ook zorgverzekeraars met medische gegevens van betrokkenen. Om die reden dient de autorisatie zo te zijn ingericht dat uitsluitend medewerkers voor wie het noodzakelijk is om hun werk te verrichten, bij bepaalde persoonsgegevens kunnen. Uit onderzoek van de AP bleek echter dat marketingmedewerkers van zorgverzekeraar Menzis ook bij de gevoelige persoonsgegevens konden. Belangrijk om te weten is dat ook het inzien van persoonsgegevens een verwerking is waar de AVG op van toepassing is. Naast het onvoldoende inrichten van toegangsrechten, hield Menzis geen logbestanden bij. Ondanks dat er geen aanwijzingen waren dat de marketingmedewerkers ook daadwerkelijk deze persoonsgegevens hadden ingezien, was het feit dat de mogelijkheid er was voor de AP genoeg om een last onder dwangsom op te leggen aan Menzis ([AP18]).

Ook het inzien van persoonsgegevens valt onder een verwerking waar de AVG op van toepassing is. Het is aan te raden alleen medewerkers voor wie het noodzakelijk is dat zij deze toegang hebben, toegang te geven tot deze gegevens. Daarnaast is het belangrijk om ervoor te zorgen dat de systemen kunnen bijhouden wie de persoonsgegevens kan inzien, zodat ongeoorloofde inzage kan worden gemonitord.

Onvoldoende vereisten aan een wachtwoord

Naast het belang van meerfactorauthenticatie, blijkt dat het stellen van vereisten aan een wachtwoord tevens essentieel is om een inbreuk te voorkomen. In september 2019 zijn de systemen van Transavia gehackt middels twee accounts van de IT-afdeling van het bedrijf. De hackers konden deze accounts gemakkelijk binnendringen omdat daar geen meerfactorauthenticatie voor nodig was, maar ook omdat de wachtwoorden eenvoudig te kraken waren. Hierbij kan gedacht worden aan wachtwoorden zoals '12345' of 'Welkom'. Bovendien hadden de hackers aan deze accounts voldoende om toegang te krijgen tot de grote systemen – hier waren verder geen drempels voor ingericht. Hoewel Transavia het datalek tijdig heeft gemeld, besloot de AP vanwege de ernst een boete op te leggen van 400.000 euro ([AP21d]).

Het in artikel 32 AVG genoemde beveiligingsniveau waarnaar gestreefd dient te worden, is afhankelijk van het risico dat met de verwerking gepaard gaat. Een adequaat beveiligingsniveau wordt bepaald aan de hand van verschillende factoren, zoals de aard en omvang van de persoonsgegevens die worden verwerkt.

Onvoldoende nakoming van de meldplicht datalekken

Het niet (tijdig) melden van datalekken

De laatste boetecategorie die wordt besproken, heeft betrekking op een onderwerp dat helaas vaak voorkomt: datalekken. In elke organisatie kan het voorkomen dat onbevoegden toegang krijgen tot persoonsgegevens, of dat deze persoonsgegevens onbedoeld vrijkomen of worden vernietigd. In dat geval spreken we van een datalek, dat – bij een mogelijk risico voor de betrokkene(n) – binnen 72 uur bij de AP dient te worden gemeld. Zo heeft PVV Overijssel te maken gehad met een datalek, omdat een e-mail is verstuurd naar 101 geadresseerden waarbij alle e-mailadressen voor iedereen zichtbaar waren. Omdat de meldingsplicht niet werd nageleefd, heeft PVV Overijssel een boete opgelegd gekregen van 7.500 euro ([AP20b]). Ook Booking.com heeft een boete opgelegd gekregen vanwege een datalek waarbij een onbekende derde toegang heeft gekregen tot de persoonsgegevens van betrokkenen. Omdat Booking.com het datalek niet binnen 72 uur na ontdekking bij de AP heeft gemeld, heeft dit uiteindelijk geleid tot een boete van 475.000 euro ([AP20e]).

Het liefst voorkom je natuurlijk een datalek, bijvoorbeeld door passende technische en organisatorische maatregelen te treffen, maar honderd procent waterdicht zal het hiermee niet worden. In het geval er toch sprake is van een datalek, is het essentieel het datalek (tijdig) te melden om de schade voor de betrokkenen én uw organisatie zo goed mogelijk te beperken. Er dient snel actie ondernomen te worden om het datalek te dichten en met het opschroeven van de beveiliging kan een datalek in de toekomst worden voorkomen.

CONCLUSIE

De AP heeft in de afgelopen jaren 'slechts' 22 boetes uitgedeeld die openbaar zijn gemaakt. Toch is dit geen reden voor organisaties om op hun lauweren te rusten. Zo bestaat er bijvoorbeeld nog steeds het misverstand dat alleen grote organisaties zich druk hoeven te maken om onderzoeken en boetes van de AP. Het feit dat de AP zich in de eerste jaren heeft gefocust op grote onderzoeken, betekent niet dat het mkb buiten schot is, zoals we zagen in de boete voor PVV Overijssel.

De AP heeft veel discretionaire bevoegdheid voor wat betreft de sancties die kunnen worden opgelegd. Het overzicht laat zien dat de AP op verschillende manieren kan handhaven, variërend van een boete tot een last onder dwangsom of een combinatie van beide. Daarnaast kan de AP kiezen voor een berisping of een formele waarschuwing. Van deze optie lijkt de AP echter steeds minder gebruik te maken. De laatste formele waarschuwing die de AP heeft gegeven, dateert uit 2020 ([AP20f]).

Het streven voor organisaties is uiteraard om sancties te voorkomen. Uit het overzicht kunnen diverse lessen worden getrokken. Zo is bijvoorbeeld het hebben van een toereikende grondslag erg belangrijk. Een bedrijf werd beboet voor het onrechtmatig verwerken van bijzondere persoonsgegevens in de vorm van vingerafdrukken, alsook een gemeente die locatiegegevens van burgers verzamelde terwijl dit niet in verhouding stond tot het doel van de verwerking, en de betekenis van het begrip 'gerechtvaardigd belang' is nauw uitgelegd in het boetebesluit aan de Nederlandse tennisbond (hoewel hierover nog niet het laatste woord gesproken is). Ook is het belangrijk de informatieverplichtingen voldoende na te komen en hierbij goed te letten op de doelgroep.

Het is een misverstand dat alleen grote organisaties zich druk hoeven te maken om onderzoeken en boetes van de AP

Voorts is het belangrijk dat de uitvoering van de rechten van betrokkenen goed is ingericht en dienen organisaties adequate technische en organisatorische maatregelen te nemen, zoals toegangsbeperking, logging en monitoring, meerfactorauthenticatie en wachtwoordvereisten. Tot slot is het van belang in geval van datalekken aan de meldplicht richting de AP te voldoen.

EN VERDER?

Historisch hebben wij gezien dat (gepubliceerde) boetes vaak klachtgeïnitieerd waren. Wij verwachten dat deze trend van het 'piepsysteem' zich grotendeels zal voortzetten. Het is dus belangrijk als organisatie een goede privacyklachtenprocedure in te richten, om klachten zoveel mogelijk zelf te kunnen verhelpen.

De prejudiciële vragen die worden gesteld vanwege het boetebesluit aan de Nederlandse tennisbond, kunnen grote implicaties hebben. Momenteel heeft de AP een afwijkende mening ten opzichte van andere toezichthouders, in die zin dat volgens de AP een louter winstoogmerk geen gerechtvaardigd belang kan inhouden. Als dit bevestigd wordt door het Hof, heeft dit grote gevolgen voor alle organisaties die deze grondslag veelvuldig toepassen.

Als we een blik op de toekomst werpen, verwachten wij daarnaast dat de AP in de komende jaren veel aandacht zal blijven besteden aan nieuwe ontwikkelingen op het gebied van artificial intelligence (AI), algoritmes, datahandel en profilering. Deze onderwerpen kwamen weliswaar niet zo duidelijk terug in de gepubliceerde boetes, maar waren wel focuspunten van de AP in de afgelopen jaren. Door hun groeiende rol in de moderne samenleving en de snelle ontwikkelingen op deze gebieden, is onze verwachting dat dit focuspunten zullen blijven voor de AP. Zo is er bijvoorbeeld sinds januari 2023 een nieuw organisatieonderdeel binnen de AP, de directie Coördinatie Algoritmes, die specifiek toezicht zal gaan houden op het gebruik van algoritmes.

Hoewel voor de AP in de ontwerpbegroting van het ministerie van Justitie en Veiligheid een verhoging van het budget is opgenomen, onder andere voor de inrichting en werkzaamheden van een algoritmetoezichthouder, noemt de AP dat haar budget onvoldoende toereikend is om alle toezichtstaken naar behoren op te pakken ([AP22c]). Zij moeten het doen met slechts een kwart van het budget dat andere Nederlandse toezichthouders (zoals de AFM of ACM, met ongeveer 100 miljoen euro) hebben. Wij verwachten een blijvende doch gestage groei richting voldoende budget in het komende decennium.

Literatuur

[AP] Autoriteit Persoonsgegevens (z.d.). *Boetes en andere sancties.* Geraadpleegd van: https://www.autoriteitpersoonsgegevens.nl/nl/publicaties/boetes-en-sancties

[AP18] Autoriteit Persoonsgegevens (2018, 15 februari). *Last onder dwangsom en definitieve bevindingen.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_last_onder_dwangsom_menzis.pdf

[AP19a] Autoriteit Persoonsgegevens (2019, 19 februari). Boetebeleidsregels Autoriteit Persoonsgegevens 2019. Geraadpleegd van: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-14586_0.pdf

[AP19b] Autoriteit Persoonsgegevens (2019, 18 juni). *Besluit tot het opleggen van een bestuurlijke boete en een last onder dwangsom.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_haga_-_ter_openbaarmaking.pdf

[AP19c] Autoriteit Persoonsgegevens (2019, 30 juli). *Besluit tot het opleggen van een bestuurlijke boete.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_bkr_30_juli_2019.pdf

[AP19d] Autoriteit Persoonsgegevens (2019, 4 december). *Besluit tot het opleggen van een bestuurlijke boete.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_vingerafdrukken_personeel.pdf

[AP19e] Autoriteit Persoonsgegevens (2019, 20 december). *Besluit tot het opleggen van een bestuurlijke boete.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_knltb.pdf

[AP20a] Autoriteit Persoonsgegevens (2020, 24 maart). *Besluit tot het opleggen van een bestuurlijke boete.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_cpa_verzuimregistratie.pdf

[AP20b] Autoriteit Persoonsgegevens (2020, 16 juni). *Besluit tot het opleggen van een bestuurlijke boete.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_pvv_overijssel.pdf

[AP20c] Autoriteit Persoonsgegevens (2020, 26 november). *Besluit tot het opleggen van een bestuurlijke boete.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_olvg.pdf

[AP20d] Autoriteit Persoonsgegevens (2020, 10 december). *Besluit tot het opleggen van een bestuurlijke boete en een last onder dwangsom.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20210512_boetebesluit_ap_locatefamily.pdf

[AP20e] Autoriteit Persoonsgegevens (2020, 10 december). *Besluit tot het opleggen van een bestuurlijke boete.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_boete_booking.pdf

[AP20f] Autoriteit Persoonsgegevens (2020, 15 december). *Formele waarschuwing AP aan supermarkt om gezichtsherkenning.* Geraadpleegd van: https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/formele-waarschuwing-ap-aan-supermarkt-om-gezichtsherkenning

[AP21a] Autoriteit Persoonsgegevens (2021, 11 maart). *Besluit tot het opleggen van een bestuurlijke boete.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_ap_gemeente_enschede.pdf

[AP21b] Autoriteit Persoonsgegevens (2021, 9 april). *Besluit tot het opleggen van een bestuurlijke boete.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_tiktok.pdf

[AP21c] Autoriteit Persoonsgegevens (2021, 31 mei). *Besluit tot het opleggen van een boete.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_uwv_beveiliging_groepsberichten.pdf

[AP21d] Autoriteit Persoonsgegevens (2021, 23 september). *Besluit tot het opleggen van een boete.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_transavia.pdf

[AP22a] Autoriteit Persoonsgegevens (2022, 14 januari). *Besluit tot het opleggen van een boete.* Geraadpleegd van: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_dpg.pdf

[AP22b] Autoriteit Persoonsgegevens (2022, 24 februari). *Besluit tot het opleggen van een boete en een last onder dwangsom.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_bz_24_februari_2022_openbare_versie_definitief.pdf

[AP22c] Autoriteit Persoonsgegevens (2022, 24 oktober). *Informatievoorziening voor de beantwoording van feitelijke vragen door de minister voor Rechtsbescherming inzake de vaststelling van de begrotingsstaten van het Ministerie van Justitie en Veiligheid voor het jaar 2023* [Ambtsbericht]. Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beantwoording_feitelijke_vragen_door_de_minister_voor_rechtsbescherming_inzake_vaststelling_van_de_begrotingsstaten_van_het_ministerie_van_justitie_en_veiligheid_voor_2023_-_2.pdf

[CMS23] CMS.Law (2023). *GDPR Enforcement Tracker – list of GDPR fines.* Geraadpleegd op 17 februari 2023, van: https://www.enforcementtracker.com/?insights

Over de auteurs

Laura Huijts LL.M., CIPP/E, CIPM, CIPT is manager bij KPMG Cyber & Privacy. Ze werkt sinds de invoering van de AVG in 2018 bij KPMG. Laura heeft een juridische achtergrond.

Danielle Molenkamp LL.M., CIPP/E is consultant bij KPMG Cyber & Privacy. Zij heeft een juridische achtergrond en is afgestudeerd aan de Vrije Universiteit van Amsterdam met de master Internet, IE & ICT.

Malik Elbaz LL.M., CIPP/E is consultant bij KPMG Cyber & Privacy. Hij heeft recent de master Informatierecht aan de Universiteit van Amsterdam afgerond.