VAST | VERZEKERINGSRECHT AANSPRAKELIJKHEID SCHADE EN TOEZICHT

# Drie jaar AVG-boetes: wat zijn de lessons learned?

VAST 2021 / P-040
26 augustus 2021

Sinds het van kracht worden van de Algemene verordening gegevensbescherming (AVG) op 25 mei 2018 heeft de Autoriteit Persoonsgegevens de eerste AVG-boetes opgelegd. Welke feiten en omstandigheden hebben ertoe geleid dat de AP ingreep en wat waren de gevolgen? In deze bijdrage gaan we daar op in. Daarbij betrekken wij ook relevante rechtspraak met betrekking tot deze boetes. Wat zijn de *lessons learned*?

## 1. Inleiding

Bedrijven en instellingen, waaronder verzekeraars, banken en universiteiten, verwerken (gevoelige) persoonsgegevens van o.a. klanten, relaties en werknemers. Deze bedrijven en instellingen zijn – als 'verwerkingsverantwoordelijken' – verantwoordelijk en aansprakelijk voor de correcte omgang met persoonsgegevens overeenkomstig de AVG.[1] Een van de doelen van de AVG is de bescherming van de privacy van EU-burgers, waarbij een belangrijke rol is weggelegd voor de nationale gegevensbeschermingsautoriteiten (artikel 51 lid 1 AVG). In Nederland is dat de Autoriteit Persoonsgegevens (artikel 6 lid 2 UAVG), veelal afgekort: 'de AP'. De AP houdt toezicht op de naleving van de verplichtingen die verwerkingsverantwoordelijken en verwerkers hebben uit hoofde van de AVG en gerelateerde wetgeving, zoals de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG). Dit toezicht voert zij uit door bijvoorbeeld naar aanleiding van klachten van betrokkenen of gemelde datalekken een onderzoek in te stellen. Wanneer blijkt dat een verwerkingsverantwoordelijke of verwerker zich niet aan de regelgeving houdt, kan de AP een administratieve boete opleggen of andere sanctie toepassen zoals een last onder dwangsom of een verwerkingsverbod (artikel 83 lid 4, 5 en 6 AVG en artikel 14 lid 3 UAVG). De AP maakt in toenemende mate gebruik van haar bevoegdheid om boetes op te leggen.[2]

## 2. De boetes tot nu toe

Tot en met juli 2021 heeft de AP vijftien boetes opgelegd wegens het niet of onvoldoende naleven van verplichtingen onder de AVG. Hiervan is één boete door de rechter vernietigd en één boete gematigd. De regels die niet (voldoende) werden nageleefd zijn grofweg in te delen in vier categorieën, waarop wij in dit artikel nader zullen ingaan:

- het melden van een *datalek* (paragraaf 2.1);
- de *beveiliging* van persoonsgegevens (paragraaf 2.2);
- de *rechtmatigheid* van de verwerking (paragraaf 2.3); en
- de *rechten van betrokkenen en de informatieverplichting* (paragraaf 2.4).

### 2.1 Het schenden van de meldplicht bij een datalek

Volgens artikel 4 (onder 12) AVG, is sprake van een datalek wanneer een 'inbreuk op de beveiliging' van persoonsgegevens plaatsvindt die 'per ongeluk of op onrechtmatige wijze leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of ongeoorloofde toegang tot persoonsgegevens'. In geval van een datalek moet de verwerkingsverantwoordelijke dit in beginsel 'zonder onredelijke vertraging' en binnen 72 uur melden bij de AP (artikel 33 AVG). Een melding hoeft (alleen) niet te worden gedaan wanneer het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen. Soms moet een datalek ook worden gemeld aan betrokkenen (artikel 34 AVG).

Op 27 november 2018 was het voor het eerst raak: de AP legde een boete van € 600.000 op aan taxiplatform Uber. Onbevoegden hadden toegang gekregen tot persoonsgegevens van een groot aantal klanten en chauffeurs en dat was door Uber (feitelijk nog onder de oude wetgeving) niet tijdig gemeld. Op 31 maart 2021 kreeg Booking.com om dezelfde reden een boete opgelegd. Het datalek dat daar plaatsvond was zowel qua omvang als qua gevoeligheid van de gegevens behoorlijk serieus te noemen. Criminelen maakten onder andere creditcardgegevens van 4.000 klanten buit. Hoewel het datalek volgens de AP al op 13 januari 2019 bekend moest worden geacht, werd het datalek pas op 7 februari 2019 gemeld. Booking.com stelde zich op het standpunt dat zij pas veel later op de hoogte was van het datalek. Volgens de AP moet een verwerkingsverantwoordelijke echter op de hoogte worden geacht van een datalek 'wanneer hij een redelijke mate van zekerheid heeft dat zich een veiligheidsincident heeft voorgedaan dat tot de compromittering van persoonsgegevens heeft geleid'. In dit geval was die redelijke mate van zekerheid aanwezig nadat een hotel twee keer in korte tijd melding maakte van phishing met gebruik van persoonsgegevens die afkomstig waren van klanten van Booking.com. De boete bedroeg € 475.000.

De meest recente boete in verband met het te laat melden van een datalek van 'slechts' € 7.500 is op 16 juni 2020 opgelegd aan de PVV Overijssel. De PVV Overijssel had een e-mail uitgestuurd naar 101 mensen, waarbij voor iedereen de e-mailadressen van de ontvangers zichtbaar waren. Een klassiek voorbeeld van een datalek, dat vermoedelijk veel voorkomt. Hierdoor werd aan onbevoegden inzicht gegeven in de politieke voorkeur van de betrokkenen en dat zijn bijzondere, gevoelige persoonsgegevens. De PVV Overijssel had geen melding gemaakt van het datalek, maar een van de geadresseerden wel. Nu het datalek zag op een relatief groot aantal personen en gevoelige persoonsgegevens betrof, moest deze door de PVV Overijssel worden gemeld, en heeft de PVV Overijssel dus haar meldplicht geschonden.

### 2.2 Het onvoldoende beveiligen van persoonsgegevens

Verwerkingsverantwoordelijken (en verwerkers) moeten ervoor zorgen dat de verwerking van persoonsgegevens voldoende is beveiligd. Hiertoe dienen technische en organisatorische maatregelen te worden getroffen die voldoende waarborgen bieden (artikel 32 AVG). Tot nu toe zijn de meeste boetes, vijf stuks, in dit kader opgelegd.

In juli 2019 legde de AP een boete op aan het Haga Ziekenhuis. De aanleiding voor het onderzoek van de AP was dat verschillende medewerkers onbevoegd het patiëntendossier van een bekende Nederlander hadden ingezien. Het Haga Ziekenhuis bleek niet te controleren wie inzage had in patiëntendossiers en paste geen tweefactor-authenticatie (een inlogsysteem waarbij degene die inlogt zich via twee middelen moet identificeren) toe voor de toegang tot patiëntendossiers. Hiermee schoot zij tekort in het treffen van passende beveiligingsmaatregelen, hetgeen het Haga Ziekenhuis een boete van € 460.000 opleverde. De rechter heeft dat bedrag verlaagd naar € 350.000 omdat het boetebedrag onevenredig hoog werd geacht. De rechtbank was van mening dat de basisboete niet verhoogd mocht worden nu het Haga Ziekenhuis intussen behoorlijk veel maatregelen had genomen om te voorkomen

dat een dergelijk datalek nogmaals zou plaatsvinden. Daarnaast nam de rechtbank mee dat ook tijdens de bezwaarprocedure nog verdere maatregelen zijn getroffen. Zo werd tweefactor-authenticatie ingevoerd, de logging geïntensiveerd, werden arbeidsovereenkomsten aangescherpt en een e-learning verplicht.[3]

Voornoemde boete vertoont gelijkenis met de boete die op 26 november 2020 werd opgelegd aan het OLVG Ziekenhuis. Ook hier werd onvoldoende bijgehouden wie welk dossier raadpleegde en werd geen tweefactor-authenticatie toegepast. Het OLVG voerde aan dat er wel een slot zat op de ruimtes waarin de computers zich bevonden en dat die computers vervolgens weer met een wachtwoord vergrendeld waren. Dit achtte de AP echter niet voldoende, ook onbevoegden konden nu toegang hebben tot de ruimte waar de computers staan. Twee-factor authenticatie werd vereist omdat het OLVG medische (bijzondere) persoonsgegevens verwerkte van een groot aantal betrokkenen. Verder werd van belang geacht dat het OLVG Ziekenhuis zich zelfstandig had gecommitteerd aan bepaalde (NEN) beveiligingsnormen, terwijl zij hier niet aan voldeed. De hoogte van de boete was € 440.000, eveneens vergelijkbaar met de (initiële) boete voor het Haga Ziekenhuis. De AP heeft bericht dat het OLVG niet meer in bezwaar of beroep is gegaan tegen deze boete.

Schoonmaakbedrijf CP&A kreeg op 24 maart 2021 een boete van € 15.000 opgelegd omdat de verzuimregistratie van zijn werknemers online zonder enige vorm van authenticatie te raadplegen was. Een orthodontiepraktijk kreeg op 4 februari 2021 een boete van € 12.000 opgelegd omdat betrokkenen persoonlijke informatie via een niet-versleutelde – en dus onbeveiligde – verbinding naar de orthodontiepraktijk moesten verzenden. Verder kreeg het UWV op 31 mei 2021 een boete van € 450.000 opgelegd, nadat uit onderzoek (naar aanleiding van negen datalekken) bleek dat de systemen van het UWV voor het versturen van groepsberichten via een persoonlijke omgeving van werkzoekenden onvoldoende waren beveiligd.

### 2.3 Boetes opgelegd in verband met de onrechtmatigheid van de verwerking

Onder de AVG moet je de verwerking van persoonsgegevens kunnen baseren op een legitieme grondslag (artikel 6 AVG). Met betrekking tot dit vereiste heeft de AP vier boetes opgelegd, waarvan er een is vernietigd door de rechter. De boete die is vernietigd, betrof een boete van € 575.000 die op 16 juli 2020 was opgelegd aan VoetbalTV, een platform dat amateurvoetbalwedstrijden filmde en beschikbaar maakte om te streamen. Volgens VoetbalTV kon zij zich beroepen op een commercieel belang, dat een ‘gerechtvaardigd belang’ vormde in de zin van artikel 6 AVG. Dit wees de AP, waarvan al bekend was dat zij op dit punt een strikte interpretatie hanteerde, van de hand. De rechter oordeelde echter dat er geen boete opgelegd had mogen worden, omdat de AP er niet van uit mocht gaan dat een commercieel belang per definitie geen gerechtvaardigd belang kan zijn.[4]

Een paar maanden later legde de AP een boete van € 525.000 op aan de Nederlandse tennisbond (de KNLTB). De KNLTB verkocht persoonsgegevens van haar leden aan sponsoren, die deze gebruikten voor marketingdoeleinden. De gegevens die de KNLTB doorgaf, had zij verzameld in het kader van het lidmaatschap, maar deze werden nu dus voor een ander doeleinde verwerkt. De AP zag ook hier geen ‘gerechtvaardigd belang’ van de KNLTB, omdat haar belang niet dringend en voldoende specifiek was. Wil je op deze grondslag een beroep kunnen doen, dan is het noodzakelijk om aan te tonen dat je een gerechtvaardigd belang hebt. Hiervoor is een legitiem belang vereist, dient te worden aangetoond, dat de verwerking noodzakelijk is voor het behartigen van dat belang en dat de verwerking geen onredelijke inbreuk maakt op de rechten en vrijheden van betrokkenen.[5]

In december 2019 kreeg een bedrijf dat vingerafdrukken van zijn personeel scande ten behoeve van de aanwezigheids- en tijdsregistratie een boete van € 725.000. Vingerafdrukken zijn ‘biometrische

gegevens' die enkel mogen worden verwerkt op grond van de uitdrukkelijke toestemming van betrokkenen of wanneer het gebruik van die gegevens noodzakelijk is voor authenticatie of beveiligingsdoeleinden (artikel 9 lid 1 AVG en artikel 22 UAVG). Die mogelijkheid is gezien het daarvoor bestaande toetsingskader (als voornoemd) heel beperkt. Nu toestemming van werknemers veelal een heikel punt is, omdat de toestemming vrijelijk moet worden gegeven en die vrijheid beperkt is in een werknemer-werkgeverrelatie, en omdat de aanwezigheids- en tijdsregistratie ook kon plaatsvinden op een manier die minder indringend zou zijn voor de privacy van de werknemers, kon geen rechtvaardiging worden gevonden voor de verwerking van de gegevens.

Met min of meer dezelfde redenering, legde de AP op 11 maart 2021 een boete van € 600.000 op aan de gemeente Enschede voor het volgen van burgers via wifitracking. Wifitracking wordt gezien als iets dat zo ingrijpt in het leven van mensen dat het enkel in uiterste gevallen mag worden ingezet. Het meten van de drukte in de binnenstad is niet een van die gevallen en dit was dus ook niet toegestaan.[6]

### 2.4 Boetes opgelegd in verband met het veronachtzamen van de rechten van betrokkenen en schenden van de informatieverplichting

De AVG geeft naast verplichtingen die verwerkingsverantwoordelijken en verwerkers moeten uitvoeren ook een aantal rechten aan betrokkenen die gerespecteerd dienen te worden. Deze rechten kunnen actief handelen van verwerkingsverantwoordelijken (waar nodig met behulp van verwerkers) vereisen. Zo hebben betrokkenen recht op inzage van de persoonsgegevens die van hen worden verwerkt (artikel 15 AVG), welke inzage kosteloos en op een eenvoudig toegankelijke manier moet worden geboden (tenzij een uitzondering ex artikel 41 UAVG van toepassing is). Er mag wel een redelijke vergoeding worden gevraagd wanneer de betrokkene vraagt om extra kopieën van de gegevens of als het verzoek duidelijk ongegrond of buitensporig is, bijvoorbeeld als een betrokkene heel veel verzoeken bij dezelfde organisatie indient. BKR gaf slechts eenmaal per jaar de mogelijkheid om de verwerkte gegevens gratis in te zien per post. Wanneer betrokkenen de gegevens die het BKR met betrekking tot hen verwerkte digitaal in wilden zien, moest daarvoor een vergoeding worden betaald. Omdat het BKR hiermee niet voldeed aan de vereisten voor het bieden van inzage kreeg zij een boete van € 830.000 opgelegd.

Bedrijven van buiten de Europese Economische Ruimte (EER) die persoonsgegevens verwerken van betrokkenen binnen de EER, maar daar geen vestiging hebben, moeten in beginsel een vertegenwoordiger in de EER aanwijzen (artikel 27 AVG). Dit onder meer om een aanspreekpunt voor betrokkenen en de AP te bieden. De website Locatefamily.com verzamelt persoonsgegevens uit openbare bronnen en verwerkt deze in een register, zodat mensen uit het oog verloren contacten terug konden vinden. Locatefamily.com is niet in de EER gevestigd en heeft ook geen vertegenwoordiger aangewezen. Om die reden legde de AP een boete van € 525.000 op. Hierbij vermelden wij zekerheidshalve ook dat de aanwijzing aan bepaalde vereisten moet voldoen.

De meest recente boete is op 9 april 2021 opgelegd aan social media platform TikTok. Het platform, dat veel jonge gebruikers heeft, bood enkel een Engelstalige privacyverklaring aan. Hiermee werd voor (jonge) gebruikers niet inzichtelijk wat er met hun gegevens gebeurde. De AP vindt dit kwalijk, te meer omdat kinderen onder de AVG extra bescherming verdienen. Duidelijk en eenvoudig taalgebruik naar kinderen wordt daarom extra belangrijk bevonden. TikTok heeft niet voldaan aan haar informatieverplichting en krijgt een boete van € 750.000. Daarnaast staat ook de naleving van de AVG door TikTok op andere punten ter discussie. Dit wordt door andere autoriteiten onderzocht, omdat de (geografische) bevoegdheid van de AP beperkt is.

## 3. De hoogte van de boetes

De hoogte van de besproken boetes varieert van € 7.500 tot € 830.000. Ondanks dat dit soms aanzienlijke bedragen betrof, zijn de boetes van de AP internationaal bezien relatief laag. Ook als we bedenken dat de AVG de mogelijkheid biedt om boetes op te leggen van ten hoogste € 20.000.000 of (zelfs) vier procent van de jaarlijkse wereldwijde omzet van een bedrijf (artikel 83 AVG). In het buitenland hebben de gegevensbeschermingsautoriteiten al meer gebruikgemaakt van die ruimte. Zo heeft de Britse gegevensbeschermingsautoriteit een boete van £18.400.000 opgelegd aan Mariott International, Inc.[7] en zijn in Italië boetes van meer dan € 10.000.000 geen uitzondering.[8]

De AP heeft boetebeleidsregels opgesteld waarbij verschillende overtredingen van de AVG zijn ingedeeld in bandbreedtes die lopen tot € 1 miljoen. De AP heeft wel de mogelijkheid om buiten die bandbreedtes te treden en boetes kunnen cumuleren (bij meerdere overtredingen). Voor de vaststelling van de hoogte van een boete binnen de bandbreedte zijn een aantal factoren van belang: de aard, de ernst en de duur van de inbreuk, de opzettelijke of nalatige aard van de inbreuk (verwijtbaarheid) en de door de verwerkingsverantwoordelijke (of verwerker) genomen maatregelen om door betrokkenen geleden schade te beperken.

Een goed voorbeeld van hoe deze criteria worden toegepast vormt de boete die is opgelegd aan het OLVG. Er werden van een *grote groep betrokkenen* (zo'n 100.000 patiënten) *zeer gevoelige* (bijzondere) persoonsgegevens *voor langere tijd* niet goed *beveiligd*: reden om de basisboete met € 80.000 te verhogen. Daarnaast werd overwogen dat het OLVG bijzonder *nalatig* is geweest, nu het zich niet heeft gehouden aan zijn eigen beleid en de NEN-normen waaraan zij zich had gecommitteerd. De basisboete werd daarom nog eens met € 50.000 verhoogd. Vergelijkbare elementen zijn terug te zien bij de bepaling van de hoogte van de boete die is opgelegd aan het Haga Ziekenhuis.

Aan de andere kant hebben wij ook gezien dat het *treffen van goede maatregelen om de schade voor betrokkenen te beperken* ertoe kan leiden dat de boete wordt verlaagd. Bij Booking.com werd het boetebedrag verlaagd met € 50.000, nu zij na het ontdekken van het datalek betrokkenen snel en adequaat op de hoogte had gebracht. Anderzijds hebben de maatregelen die het OLVG trof tijdens het onderzoek van de AP niet tot verlaging van de boete geleid. In het boetebesluit aan TikTok is te lezen dat het nemen van maatregelen enkel zinvol kan zijn voor zover deze de effecten van de overtreding wegnemen. De put dempen als het kalf verdronken is, heeft dus voor de hoogte van de boete geen zin, maar uiteraard wel om toekomstige boetes (en andere sancties) te voorkomen.

Dat een boete zelfs fors lager kan uitvallen dan de standaard-bandbreedte is gebleken bij de boetes voor PVV Overijssel, CP&A en de orthodontiepraktijk. Deze werden gematigd tot respectievelijk € 7.500, € 15.000 en € 12.000, omdat de organisaties die de boete kregen opgelegd *kleinere organisaties* zijn en *minder financiële draagkracht* hebben. De AP houdt hier rekening mee en kan een boete verlagen indien deze anders in strijd zou zijn met het (bestuursrechtelijke) evenredigheidsbeginsel, dat bepaalt dat de gevolgen van een besluit niet onevenredig zwaar mogen zijn in vergelijking met het belang dat het besluit dient.

Tot slot vonden wij het opvallend dat het niet meewerken aan het onderzoek van de AP, hoewel dit uiteraard niet in dank wordt afgenomen, niet per definitie lijkt te leiden tot verhoging van een boete.[9]

## 4. Conclusie

Tot en met juli 2021 zijn door de AP reeds diverse boetes opgelegd met betrekking tot de beveiliging, het niet (tijdig) melden van datalekken, het ontbreken van een wettelijke verwerkingsgrondslag en het niet op passende wijze waarborgen van rechten van betrokkenen – inclusief het ontbreken van een vertegenwoordiger in de EU – en het verstrekken van afdoende informatie over de gegevensverwerking.

Deze boetes zijn tot nu toe, gezien de in andere landen opgelegde boetes en de mogelijkheden die de AVG biedt, relatief laag. Ook wordt er rekening gehouden met de draagkracht van partijen. Toch worden ontegenzeggelijk boetes opgelegd voor behoorlijk hoge bedragen. Daarnaast vinden wij dat nog te bezien valt hoe redelijk dit allemaal uitpakt. De boete die de KNLTB (een organisatie met een eigen vermogen van ongeveer € 6.000.000) kreeg opgelegd verschilde niet veel met die van Booking.com (een organisatie met een paar miljard winst per jaar). Het lijkt er wel op dat procederen kan lonen, want de Nederlandse rechter is al tweemaal van oordeel geweest dat de opgelegde boete niet terecht respectievelijk te hoog was.

## Aanbevelingen voor de praktijk

Het niet voldoen aan de vereisten onder de AVG kan stevige (financiële en andere) consequenties hebben. Hieronder geven wij een praktisch overzicht met een aantal *tips & tricks*, geïnspireerd op de tot nu toe opgelegde boetes van de AP. Wij verwachten dat het belang van het in acht nemen van deze tips (en de andere verplichtingen onder de AVG) alleen maar toe zal nemen. De AP heeft een toenemende capaciteit om zaken aan te pakken (en dus boetes op te leggen).

Mocht het toch misgaan, handel dan snel om een en ander zo goed mogelijk te herstellen, bekijk of een beroep op een gebrek aan draagkracht van jouw onderneming zinvol kan zijn en onderzoek of het bij een opgelegde boete zou kunnen lonen om bezwaar te maken of naar de rechter te stappen.

| **Actie** | **Hoe doe je dat?** |
|---|---|
| Beoordeel (vooraf) of je een wettelijke grondslag hebt voor de verwerking van persoonsgegevens | Breng verwerkingen in kaart en bepaal bij elke verwerking de in artikel 6 AVG genoemde grondslag (veelal: toestemming, uitvoering van een overeenkomst met de betrokkene, voldoen aan een wettelijke verplichting of een gerechtvaardigd belang). Wees extra kritisch wanneer de verwerking is gebaseerd op een gerechtvaardigd belang, of wanneer het bijzondere persoonsgegevens (zoals gezondheidsgegevens) betreft. |
| Neem passende beveiligingsmaatregelen | Tref overeenkomstig artikelen 32 AVG e.v. technische en organisatorische maatregelen die, rekening houdend met de |

| | |
|---|---|
| | omstandigheden zoals de kosten daarvan, technische (on)mogelijkheden en risico's die betrokkenen lopen, passende waarborgen bieden aan betrokkenen. Denk aan toegangsbeperkingen, geheimhoudingsbepalingen in arbeidsovereenkomsten en versleuteling van gegevens. Hoe hoger de risico's van de verwerking, hoe hoger het beveiligingsniveau zal moeten zijn. Zo is bij het verwerken van gevoelige persoonsgegevens al snel een tweefactor-authenticatie vereist. Sluit ook passende (verwerkers)overeenkomsten. Dit is verplicht als een andere partij 'verwerker' is (artikel 28 AVG) of als er sprake is van 'gezamenlijk verwerkingsverantwoordelijken' (artikel 26 AVG). Maar ook wanneer dit niet het geval is, is het raadzaam om (met name met betrekking tot de categorieën in dit overzicht) afspraken te maken met betrekking tot de verdeling van taken en verantwoordelijkheden van partijen waar het de verwerking van persoonsgegevens betreft. Denk daarbij ook aan de verdeling van de aansprakelijkheid. |
| Waarborg rechten van betrokkenen en informeer hen zorgvuldig | Geef betrokkenen de mogelijkheid om hun rechten genoemd in artikel 15 AVG e.v. uit te oefenen, zoals het verkrijgen van inzage in persoonsgegevens die van hen worden verwerkt, deze te wijzigen of te laten verwijderen. Verleende toestemming moet eenvoudig kunnen worden ingetrokken. Verstrek voorafgaand aan de verkrijging van de persoonsgegevens de op grond van artikel 12 AVG e.v. te verstrekken informatie (veelal middels een privacyverklaring). In geval van een |

| | |
|---|---|
| | vestiging buiten de EER, is het van belang een vertegenwoordiger in een van de lidstaten aan te wijzen. |
| Meld datalekken, indien nodig, tijdig | Meld datalekken conform artikel 33 en 34 AVG:<br><br>- Documenteer bij binnenkomst van signalen van een mogelijk datalek het moment van ontdekking en start het onderzoek naar het datalek.<br><br>- Beoordeel o.a. het risico voor rechten en vrijheden van betrokkenen en of het datalek gemeld moet worden bij de AP/betrokkenen (en doe dat tijdig)en onderzoek welke maatregelen kunnen worden getroffen om herhaling te voorkomen en de gevolgen te beperken.<br><br>- Wijs hiervoor een verantwoordelijke aan binnen de organisatie. |
| Privacybeleid naleven | Stel een privacybeleid op en leef dit na. Denk ook aan het bijhouden van een verwerkingsregister. |

*Dit artikel is op eigen titel geschreven door mw. mr. N. Witt en mr. L.R.J.M. Boer, beiden werkzaam als advocaat bij Ploum, Rotterdam Law Firm. De boetes tot en met juli 2021 zijn in dit artikel meegenomen.*

**Noten**

[1] De AVG zal veelal van toepassing zijn op de verwerking van persoonsgegevens door de lezer van dit artikel. Voor het materiële respectievelijk territoriale toepassingsgebied van de AVG verwijzen wij naar de artikelen 2 en 3 AVG.

[2] Alle boetes die de Autoriteit Persoonsgegevens heeft opgelegd zijn te raadplegen via de website van de Autoriteit Persoonsgegevens: Autoriteit Persoonsgegevens, *Boetes en andere sancties*, te vinden op www.autoriteitpersoonsgegevens.nl (laatst geraadpleegd op: 23 augustus 2021).

[3] Rechtbank Den Haag 31 maart 2021, ECLI:NL:RBDHA:2021:3090.

[4] Rechtbank Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111.

[5] Zie hierbij ook: Rechtbank Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111.

[6] Zie over dit onderwerp ook: M. Poulus: *Computerrecht* 2018/112, 'Wifi-tracking: de cookie is op'.

[7] Deze boete is opgelegd voor de Brexit, en dus onder de AVG. Na de Brexit is de AVG niet meer van toepassing in het Verenigd Koninkrijk.

[8] Information Commissioner's Office (ICO), ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure, te vinden op www.ico.org.uk (laatst geraadpleegd op: 9 augustus 2021); Bobby Hellard, *Italy tops GDPR penalty list with €46m worth of fines this year*, te vinden op www.itpro.co.uk (laatst geraadpleegd op: 9 augustus 2021).

[9] Zie: Autoriteit Persoonsgegevens, *Boetebesluit Locatefamily.com*, te vinden op www.autoriteitpersoonsgegevens.nl (laatst geraadpleegd op: 12 augustus 2021).

## Keywords

Administratieve boete
Algemene Verordening Gegevensbescherming (AGV)
Autoriteit persoonsgegevens (AP)
Privacyrecht
Verwerking

## Auteur(s)

**Nina Witt**

Advocaat bij Ploum, Rotterdam Law Firm

LinkedIn

**Lars Boer**

Advocaat bij Ploum, Rotterdam Law Firm

LinkedIn