LOUWERS
IP|TECHNOLOGY ADVOCATEN

Jaaroverzicht Privacy & Security 2019

Nu de Algemene Verordening Gegevensbescherming alweer een jaar van kracht is, zijn privacy en security onderwerpen waar de meeste organisaties niet meer omheen kunnen. De ontwikkelingen binnen dit rechtsgebied gaan bovendien razendsnel. Hieronder is daarom een overzicht opgenomen met de belangrijkste juridische ontwikkelingen binnen dit rechtsgebied in het afgelopen jaar.

WETGEVING

Niet alleen de Algemene Verordening Gegevensbescherming ('AVG') heeft in 2019 haar eerste verjaardag gevierd, maar ook de Uitvoeringswet AVG ('UAVG'). In lijn hiermee heeft Minister Dekker de Tweede Kamer op 31 oktober 2019 geïnformeerd over enkele voorgenomen aanpassingen in de UAVG. Eerder had de Minister de kamer al geïnformeerd over de eerste ervaringen met de UAVG. De Minister streeft ernaar om in het eerste kwartaal van 2020 een wetsvoorstel ter aanpassing van de UAVG in consultatie te brengen.

Oorspronkelijk zou de ePrivacy verordening ('EPV') gelijktijdig met de AVG in werking treden. Duidelijk is dat dit niet is gelukt. Sterker nog, op 22 november 2019 heeft het Comité van Permanente Vertegenwoordigers het laatste tekstvoorstel van de Raad van de EU verworpen. Dit leidt waarschijnlijk tot een vertraging van maanden. De EPV heeft betrekking op de elektronische communicatiesector en bevat onder meer gewijzigde regels rondom het gebruik van cookies en direct marketing.

Op 1 april 2019 is de Wet afwikkeling massaschade in collectieve acties in het staatsblad gepubliceerd. Deze wet maakt het voor benadeelden mogelijk om in een collectieve actie schade te verhalen. Hiermee wordt beoogd te voorkomen dat er meerdere procedures over dezelfde gebeurtenis worden gestart door verschillende belanghebbenden. Dat geldt dus ook voor eventuele betrokkenen die collectief schade willen verhalen op een verwerkingsverantwoordelijke of verwerker wegens schending van de AVG.

TOEZICHTHOUDERS

European Data Protection Board

De European Data Protection Board ('EDPB') heeft het afgelopen jaar weer een aantal interessante documenten gepubliceerd, waaronder de recente richtsnoeren met betrekking tot de territoriale werkingssfeer van de AVG. Hiermee is getracht helderheid te verschaffen over de toepasselijkheid van de AVG in diverse situaties, bijvoorbeeld wanneer een verwerker of verwerkingsverantwoordelijke buiten de EER is gevestigd.

Op 12 februari 2019 heeft de EDPB meer duidelijkheid verstrekt over de vraag wat een eventuele no-deal Brexit zou betekenen voor de doorgifte van persoonsgegevens aan het Verenigd Koninkrijk. Een toelichting op dit document is hier te vinden.

Verder heeft de EDPB de EU-wetgevers in maart 2019 opgeroepen om hun inspanningen voor de vaststelling van de EPV op te voeren. Zoals hiervoor al aan de orde kwam, heeft dit tot op heden nog niet tot het gewenste resultaat geleid.

Op 12 juli 2019 heeft de EDPB proberen te verhelderen in hoeverre de AVG van toepassing is op de verwerking van persoonsgegevens door het gebruik van videoapparatuur. Hoewel de betreffende richtsnoeren niet langer voor consultatie beschikbaar zijn, moet er nog wel een definitieve versie worden vastgesteld.

Op 16 oktober 2019 heeft de EDPB richtsnoeren gepubliceerd over de verwerking van persoonsgegevens op basis van de uitvoering van een overeenkomst. De richtsnoeren gaan specifiek in op de toepassing van deze grondslag bij het verlenen van onlinediensten aan betrokkenen.

In november 2019 zijn er richtsnoeren over privacy by design en privacy by default ter consultatie gelegd door de EPDB. Partijen hebben nog tot 16 januari 2020 de tijd om commentaar te leveren op de inhoud daarvan. In december 2019 zijn er bovendien richtsnoeren over de toepassing van het recht om vergeten te worden door zoekmachines gepubliceerd. Deze liggen nog tot en met 5 februari 2020 ter consultatie.

Verder zijn er het afgelopen jaar diverse verslagen verschenen waarin het zogenoemde Privacy Shield wordt geëvalueerd. In het laatste

verslag spreekt de EDPB haar waardering uit voor de inspanningen van de Amerikaanse autoriteiten om het Privacy Shield ten uitvoer te leggen, maar wordt er ook op gewezen dat de naleving van de beginselen van het Pivacy Shield nog steeds een punt van aandacht is.

Autoriteit Persoonsgegevens

Ook de Autoriteit Persoonsgegevens ('AP') heeft in 2019 niet stilgezeten. Dat is ook niet verbazingwekkend, aangezien het aantal privacyklachten dat bij de AP wordt ingediend nog steeds sterk blijft toenemen.

Door de komst van de AVG heeft de toezichthouder er bovendien diverse nieuwe taken bij gekregen, zoals het geven van voorlichting. In het kader van deze taak heeft de AP zes aanbevelingen gedaan aan organisaties om hun privacybeleid in te kunnen richten. Volgens de AP brengen organisaties met een privacybeleid in kaart welke maatregelen er zijn genomen om de persoonsgegevens van bijvoorbeeld klanten, patiënten en cliënten te beschermen. Een privacybeleid verschilt kortom van een privacyverklaring en verwerkingsregister.

Verder heeft de AP een normuitleg gepubliceerd over het gerechtvaardigd belang. In deze uitleg komt duidelijk naar voren dat er aan drie cumulatieve voorwaarden moet zijn voldaan wil er sprake zijn van een rechtmatige gegevensverwerking op basis van deze grondslag: het belang moet gerechtvaardigd zijn, de gegevensverwerking moet noodzakelijk zijn om dat belang te behartigen en de fundamentele rechten en vrijheden van de betrokkene mogen niet prevaleren. Helaas biedt deze normuitleg weinig verheldering en hierop is dan ook veel kritiek.

Verder heeft de AP zich in het kader van haar voorlichtingstaak op het standpunt gesteld dat het gebruik van cookiewalls voor het plaatsen van tracking cookies in strijd is met de AVG. Een cookiewall is een pop-up of banner die in beeld verschijnt met de vraag of een bezoeker akkoord gaat met het plaatsen van cookies. Zo niet, dan krijgt de bezoeker geen toegang tot de website. Meer informatie over deze normuitleg van de AP is hier te vinden.

Het afgelopen jaar richtte de AP zich in het bijzonder op bedrijven die handelen in persoonsgegevens, de overheid en de zorg. En met name in die laatste sector is er in 2019 bijzonder veel gebeurd. Zo bleek de zorgsector opnieuw koploper in het aantal datalekmeldingen bij de AP. De meeste datalekken worden veroorzaakt door het versturen van persoonsgegevens aan de verkeerde ontvanger. De AP heeft vijf tips opgesteld voor zorginstellingen om datalekken te voorkomen.

Een zorginstelling die het afgelopen jaar veel stof deed opwaaien was het HagaZiekenhuis. Toen bleek dat dat tientallen medewerkers onnodig het medisch dossier van een BN'er hadden ingezien, legde de AP het ziekenhuis de eerste boete onder de AVG op. Ook werd een last onder dwangsom opgelegd om te bewerkstelligen dat het ziekenhuis de beveiliging van patiëntendossiers zou verbeteren. Later in het jaar kwam het HagaZiekenhuis opnieuw negatief in het nieuws. Ditmaal omdat er patiëntgegevens in een winkelwagentje van een supermarkt werden aangetroffen.

Ook aan Menzis en VGZ werd een last onder dwangsom opgelegd. Beide zorgverzekeraars verwerkten medische gegevens op onzorgvuldige wijze. Het autorisatiebeleid was niet op orde, er werd niet goed gelogd en marketingmedewerkers hadden ten onrechte toegang tot medische gegevens. Omdat de zorgverzekeraars niet tijdig aan de gehele last hadden voldaan, heeft de AP een dwangsom van € 500.000,- geïnd.

Verder gaf de AP de Alliantie kwaliteit in de geestelijke gezondheidszorg (Akwa GGZ) een berisping voor het verwerken van gezondheidsgegevens. Akwa GGZ had een onvoldoende geanonimiseerde set gezondheidsgegevens overgenomen, terwijl die verwerking niet op een wettelijke uitzonderingsgrond kon worden gebaseerd. De verwerking was kortom in strijd met het verwerkingsverbod dat voor bijzonder persoonsgegevens geldt.

Maar niet alleen binnen de zorgsector werd handhavend opgetreden. Zo liet de AP weten dat zij onderzoek doet naar de verwerking van nationaliteit door de Belastingdienst. Dit heeft te maken met de wijze waarop de Belastingdienst fraude met kinderopvangtoeslag opspoort. Het onderzoek loopt nog. De Belastingdienst werd in 2017 ook

al door de AP onderzocht. Toen werden er diverse beveiligingsrisico's ontdekt. In oktober 2019 constateerde de AP dat de Belastingdienst voldoende verbetermaatregelen had getroffen om de informatie te beveiligen.

Ook de ING bereikte het afgelopen jaar het nieuws wegens privacy perikelen. De ING zou namelijk de bij- en afschrijvingen van klanten gaan lezen om hen persoonlijke aanbiedingen te kunnen sturen. De AP heeft naar aanleiding van deze berichtgeving een waarschuwingsbrief naar de Nederlandse Vereniging van Banken gestuurd.

In het kader van de handhaving is nog van belang dat de boetebeleidsregels van de AP het afgelopen jaar zijn aangepast. Hiermee wordt inzicht gegeven in de factoren die de hoogte van een boete bepalen, zoals de ernst, omvang, duur, opzet en recidive. Deze beleidsregels worden toegepast totdat er Europese richtsnoeren zijn voor de berekening van de hoogte van boetes.

Verder is er door de AP een definitieve lijst vastgesteld van verwerkingen van persoonsgegevens waarvoor een data protection impact assessment (DPIA) nodig is. Hierop staan onder andere zwarte lijsten, fraudebestrijding en cameratoezicht. Een DPIA is een instrument om vooraf de risico's van een gegevensverwerking in kaart te brengen.

NLdigital (hiervoor: Nederland ICT) heeft in 2019 de zogenoemde Data Pro Code voor verwerkers in de ICT- branche opgesteld. Wanneer verwerkers deze gedragscode volgen, voldoen zij aantoonbaar aan de verplichtingen uit de AVG. De code ligt momenteel nog ter goedkeuring bij de AP.

Op de valreep in 2019 heeft de AP samen met de Raad voor Accreditatie (RvA) het AVG-certificaat geïntroduceerd. Momenteel is de RvA bezig met het accreditatieproces voor instellingen die deze AVG-certificaten zullen gaan uitgeven. Vervolgens zullen de certificatieschema's door de AP worden beoordeeld. Een AVG-certificaat geeft aan dat op een bepaald onderdeel of proces voldaan wordt aan de AVG.

Tot slot is het nog interessant om te vermelden dat AuditConnect het verwerkingsregister van de AP heeft opgevraagd en ontvangen. Hieraan kan door organisaties inspiratie worden ontleend bij de inrichting van hun eigen verwerkingsregister. Let wel: de AP heeft een aantal velden in haar verwerkingsregister opgenomen, die daar op grond van de AVG niet verplicht in opgenomen hoeven te worden. Lees hier meer over de documentatieplicht.

JURISPRUDENTIE

In 2019 is er weer interessante jurisprudentie verschenen. Hieronder volgt een korte uiteenzetting van enkele van deze uitspraken.

Op Europees niveau

Op 14 februari 2019 oordeelde het HvJ EU dat het publiceren van video-opnames van een politieverhoor op Youtube door een niet-professionele journalist onder de reikwijdte van de Privacyrichtlijn 95/46/EG valt. Het HvJ EU benadrukte verder dat het begrip journalistiek ruim moet worden uitgelegd en oordeelde dat de journalistieke exceptie van toepassing is indien het doel van de publicatie uitsluitend erin bestaat om informatie, meningen of ideeën aan het publiek kenbaar te maken.

Het HvJ EU oordeelde op 29 juli 2019 in het Fashion ID arrest dat de beheerder van een website die een social plug-in heeft ingevoegd, die ervoor zorgt dat de browser van een bezoeker van die site content van de aanbieder van die plug-in opvraagt en daartoe persoonsgegevens van de bezoeker aan deze aanbieder doorzendt, moet worden aangemerkt als verantwoordelijke in de zin van de Privacyrichtlijn 95/46/EG. Deze verantwoordelijkheid is wel beperkt tot de bewerkingen waarvoor de beheerder daadwerkelijk het doel en de middelen vaststelt, te weten het verzamelen en door middel van doorzending verstrekken van de gegevens in kwestie.

In het Google/CNIL arrest werd op 24 september 2019 door het HvJ EU geoordeeld dat een exploitant van een zoekmachine, die een verzoek tot verwijdering van links inwilligt, niet verplicht is om deze links voor alle versies van zijn zoekmachine – en daarmee wereldwijd – te verwijderen. De links moeten wel binnen de EU-lidstaatspecifieke versies van de zoekmachine worden verwijderd. Daarnaast moeten er maatregelen worden getroffen om op zijn minst ernstig te ontmoedigen dat betreffende links alsnog te vinden zijn als

internetgebruikers via een van lidstaten een zoekopdracht uitvoeren op de betrokkene die het vergeetverzoek indiende.

Op 1 oktober 2019 oordeelde het HvJ EU in het Planet49 arrest dat toestemming voor het plaatsen van tracking cookies niet rechtsgeldig is verkregen wanneer er sprake is een vooraf aangevinkt selectievakje dat door de websitebezoeker moet worden uitgevinkt. Er is dan immers geen sprake van een specifieke en dubbelzinnige wilsuiting. Hier kunt u daar meer over lezen.

De langverwachte opinie van A-G Saugmandsgaard øe in de zaak Data Protection Commissioner/Facebook (Schrems II) werd op 19 december 2019 gepubliceerd. De A-G is van mening dat de bij besluit (2010/87) van de Europese Commissie vastgestelde *Standard Contractual Clauses* ('SCC') voor verwerkers buiten de EU geldig zijn. Volgens hem zijn de SCC geldig zolang deze de verwerkingsverantwoordelijke en de toezichthoudende autoriteiten verplichten om de doorgifte te schorsen of te verbieden wanneer de verplichtingen uit de SCC op zodanige wijze in strijd komen met het recht van het betreffende derde land dat de verplichtingen die daaruit voortvloeien niet meer kunnen worden nagekomen. Het is nu afwachten of het HvJ EU het eens is met deze conclusie van de A-G.

Op Nederlands niveau

Het Hof Den Haag oordeelde op 20 augustus 2019 dat degene die met toestemming van de patiënt na diens overlijden verzoekt om afschrift of inzage in het medisch dossier, daar geen zwaarwegend belang voor nodig heeft. De toets van een zwaarwegend belang is kortom niet aan de orde als toestemming bij de patiënt is verkregen voor inzage.

Op 17 september 2019 was het Hof Den Haag van oordeel dat ook interne kerkelijke stukken onder het recht van inzage vallen. Het recht op inzage kan op voorhand niet zonder meer worden geblokkeerd omdat in de desbetreffende documenten sprake zou (kunnen) zijn van vertrouwelijke (interne) correspondentie, stukken waarin persoonlijke gedachten en/of adviezen zijn verwoord die zijn opgesteld met het oog op intern overleg en beraad, dan wel interne besluitvorming.

Op 12 augustus 2019 oordeelde de Rechtbank Amsterdam dat schoenenwinkel Manfield haar werknemers niet mocht verplichten om een autorisatiesysteem te gebruiken voor het kassasysteem dat op basis van een vingerscan werkte. Als hoofdregel geldt namelijk dat verwerking van biometrische gegevens, behoudens gegeven toestemming, verboden is, tenzij wordt voldaan aan de uitzondering van artikel 29 UAVG. Daar is volgens de rechtbank echter niet aan voldaan.

Meer weten?

Neem dan contact op met een van onze specialisten:

T: 070 2400 836
M: 06 1099 2888
dejong@louwersadvocaten.nl

T: 040 2393 209
M: 06 4639 3938
dewit@louwersadvocaten.nl

T: 070 2400 836
M: 06 2156 4116
molenaars@louwersadvocaten.nl

T: 040 2393 202
M: 06 1313 664
peerboom@louwersadvocaten.nl

T: 070 2400 836
M: 06 8344 0502
fonville@louwersadvocaten.nl