LOUWERS
IP|TECHNOLOGY ADVOCATEN

Jaaroverzicht: privacy & security

2018 is officieel begonnen. Een mooi moment om terug te blikken op het afgelopen jaar. Privacy en de bescherming van persoonsgegevens waren hot topic in 2017. Bijgaand treft u een kort en bondig jaaroverzicht van de belangrijkste juridische ontwikkelingen op deze gebieden.

WETGEVING

Algemene Verordening Gegevensbescherming

Allereerst moet de Algemene Verordening Gegevensbescherming ('AVG') natuurlijk worden genoemd. Hoewel de AVG al op 24 mei 2016 in werking is getreden, zal deze wet op 25 mei 2018 definitief van kracht worden. Veel organisaties hebben zich het afgelopen jaar dan ook voorbereid op de AVG.

Ook het wetsvoorstel voor de Uitvoeringswet AVG is inmiddels gepubliceerd. In deze wet wordt de keuzeruimte die de AVG biedt nader ingevuld door de Nederlandse wetgever. Uit de tekst van het wetsvoorstel blijkt dat veel bepalingen uit de huidige Wet bescherming persoonsgegevens ('Wbp') inhoudelijk gehandhaafd blijven. De Uitvoeringswet AVG treedt naar verwachting op hetzelfde tijdstip in werking als de AVG. De Wbp zal op dat moment worden ingetrokken.

ePrivacy verordening

Oorspronkelijk zou de ePrivacy verordening ('EPV') gelijktijdig met de AVG in werking treden, maar naar verwachting zal dit nu pas in 2019 zijn. De EPV heeft betrekking op de elektronische communicatiesector en bevat onder meer gewijzigde regels rondom het gebruik van cookies en direct marketing. Voor zogenaamde Over-the-top diensten als WhatsApp en Skype gaan op grond van de EPV dezelfde regels gelden als voor traditionele communicatiediensten.

Payment Services Directive 2

In de zogenaamde Herziene Richtlijn Betaaldiensten, ook wel Payment Services Directive 2 ('PSD2') genoemd, is onder meer geregeld dat banken bankgegevens van klanten moeten delen met andere financiële dienstverleners, mits de klant hiervoor uitdrukkelijk toestemming heeft gegeven. Vanwege privacy issues heeft de Nederlandse implementatie van PSD2 vertraging opgelopen. De Minister heeft op 22 september 2017 aangegeven dat hij het voorjaar van 2018 een realistischere inschatting acht.

TOEZICHTHOUDERS

Artikel 29 Werkgroep

De Europese privacy toezichthouders, verenigd in de Artikel 29 Werkgroep ('WP29'), hebben het afgelopen jaar een aantal opinies gepubliceerd met betrekking tot de AVG. In deze stukken worden een aantal bepalingen en begrippen uit de AVG nader toegelicht.

De eerste opinie (laatst aangepast op 5 april 2017) ziet op het recht op dataportabiliteit. Het recht op dataportabiliteit houdt in dat de betrokkene het recht heeft om zijn persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm te ontvangen en deze aan een andere organisatie over te (laten) dragen. Dit recht wordt voor het eerst geïntroduceerd in de AVG. Lees hier meer over dataportabiliteit.

De tweede opinie (ook laatst aangepast op 5 april 2017) heeft betrekking op de Functionaris voor de Gegevensbescherming ('FG'). Onder de AVG worden verschillende categorieën van organisaties verplicht gesteld om een FG aan te stellen, terwijl aanstelling van een FG onder de Wbp niet verplicht is. Lees hier meer over de FG.

Een volgende opinie (ook laatst aangepast op 5 april 2017) gaat in op het beginsel van de leidende toezichthouder. De AVG beoogt dat organisaties die grensoverschrijdende verwerkingen uitvoeren straks nog maar met één privacy toezichthouder zaken hoeven te doen. Dit wordt ook wel de One Stop Shop-regel genoemd.

De vierde opinie (gepubliceerd op 3 oktober 2017) ziet op de meldplicht datalekken onder de AVG. Deze meldplicht lijkt op de Wet meldplicht datalekken die al vanaf 1 januari 2016 in Nederland van toepassing is. Lees hier meer over dit onderwerp.

Een andere opinie (ook gepubliceerd op 3 oktober 2017) heeft betrekking op geautomatiseerde besluitvorming en profilering. Uitgangspunt in de AVG is dat er geen geautomatiseerde besluitvorming op basis van profilering mag plaatsvinden als daaraan rechtsgevolgen voor de betrokkene zijn verbonden of het besluit hem in aanmerkelijke mate treft. Lees hier meer over dit onderwerp.

Ook zijn er op 3 oktober 2017 richtlijnen verschenen over de toepassing en vaststelling van administratieve boetes onder de AVG. Belangrijk om te weten is dat de maximale boete die de toezichthouder kan opleggen, verhoogd is naar € 20 miljoen of 4% van de jaaromzet. Uit de Memorie van Toelichting bij de Uitvoeringswet AVG blijkt echter dat in de meeste gevallen eerst een last onder bestuursdwang/dwangsom zal worden toegepast voordat de toezichthouder overgaat tot oplegging van boetes. Lees hier meer over administratieve boetes.

Verder is er een opinie over de Data Protection Impact Assessment ('DPIA') gepubliceerd (laatst aangepast op 4 oktober 2017). Een DPIA is een instrument waarmee organisaties voorafgaand aan een gegevensverwerking de privacyrisico's daarvan in kaart kunnen brengen. Lees hier meer over de DPIA.

Naast voorgenoemde stukken, die allemaal betrekking hebben op de AVG, is nog interessant om te vermelden dat de WP29 zich heeft uitgelaten over gegevensverwerking op het werk en het Privacy Shield.

Het Privacy Shield is de vervanger van het Safe Harbour verdrag dat in 2015 ongeldig is verklaard nadat de Oostenrijker Max Schrems een rechtszaak tegen Facebook had aangespannen vanwege de gebrekkige gegevensbescherming in de VS. De WP29 heeft in een persbericht laten weten nog steeds enkele zorgen te hebben rondom de gegevensuitwisseling met de VS.

Autoriteit Persoonsgegevens

Ook de Autoriteit Persoonsgegevens ('AP') is in 2017 druk bezig geweest met de aankomende AVG. De AP krijgt vanaf komend jaar namelijk diverse nieuwe taken. Het is dan ook niet verwonderlijk dat uit de begroting van het Ministerie van V&J blijkt dat de AP vanaf 2019 jaarlijks structureel € 7 miljoen extra krijgt.

Om organisaties op weg te helpen heeft de AP een 10-stappenplan gepubliceerd, waarin de bewustwording door alle relevante mensen binnen een organisatie de eerste stap betreft. Daarnaast heeft de AP meestgestelde AVG-vragen gepubliceerd en specifieke dossiers geopend voor scholen & de AVG en zorgaanbieders & de AVG.

Los van de AVG, heeft de AP het afgelopen jaar diverse malen handhavend opgetreden. Zo liet de AP op 16 mei 2017 na een onderzoek weten dat Facebook in strijd handelt met de Wbp. Facebook informeerde haar gebruikers onvolledig over het gebruik van hun persoonsgegevens en werden bijzondere persoonsgegevens verwerkt zonder de vereiste uitdrukkelijke toestemming van gebruikers. Ook Microsoft werd door de AP teruggefloten vanwege het onvolledig informeren van gebruikers. Microsoft legde niet uit dat door de standaardinstellingen via de browser Edge voortdurend gegevens werden verzameld over het gebruik van apps en het surfgedrag van gebruikers.

In 2017 richtte de AP haar pijlen eveneens op het onrechtmatige gebruik van burgerservicenummers ('BSN') door organisaties. Omdat het BSN een uniek herleidbaar nummer tot een persoon is, brengt de verwerking daarvan bijzondere risico's met zich mee, waaronder identiteitsfraude. Zo startte de AP een onderzoek naar de wettelijke grondslag voor de verwerking van het BSN in btw-identificatienummers van ZZP'ers door de Belastingdienst, stopte Transportbedrijf Nippon Express de onrechtmatige

verwerking van het BSN van chauffeurs na onderzoek van de AP en staakte Airbnb de verwerking van BSN van klanten op aandringen van de AP.

Ook stelde de AP vast dat het UWV in strijd handelde met de Wbp. Medewerkers verzuimbeheersing verwerkten onbevoegd gezondheidsgegevens van mensen in het kader van een Ziektewetuitkering. Ook was de beveiliging van het online werkgeversportaal volgens de AP onvoldoende, omdat er geen meerfactorauthenticatie werd toegepast bij de toegangsverlening.

Verder is interessant om te melden dat de AP de onderzoeken van de verschillende toezichthouders in Europa naar het datalek van Uber coördineert. Deze Europese taskforce werd opgezet nadat bekend werd dat er in oktober 2016 een datalek bij Uber had plaatsgevonden, waarbij inzage werd verkregen in de gegevens van 57 miljoen klanten.

Over datalekken gesproken: de AP heeft gedurende 2017 elk kwartaal een totaaloverzicht gepubliceerd van de gemelde datalekken. Van januari tot en met september 2017 zijn er in totaal 7222 datalekken gemeld, waarvan de meeste voorkwamen in de sector gezondheid en welzijn. Het meest voorkomende type datalek betreft het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger. Opvallend is dat er tot op heden geen enkele boete is opgelegd in verband met de meldplicht datalekken.

JURISPRUDENTIE

Op Europees niveau

In 2017 is er weer interessante hogere rechtspraak verschenen. Zo stond in het Salvatore Manni arrest van 9 maart 2017 de vraag centraal of een voormalig bestuurder van een failliet verklaarde vennootschap zijn persoonsgegevens kan laten verwijderen uit de vennootschapsregisters, zodat hij niet meer in verband kan worden gebracht met dat faillissement. Het Hof van Justitie van de Europese Unie ('HvJ EU') gaf aan groot belang te hechten aan de openbaarheid van het vennootschapsregister en oordeelde dat de belangen van derden ten aanzien van deze openbaarheid in beginsel prevaleren boven het recht op privacy van een individu.

Daarnaast was het HvJ EU op 4 mei 2017 van oordeel dat het belang van een derde om persoonsgegevens te verkrijgen van iemand die schade heeft aangebracht aan diens eigendom om de schade op deze persoon in rechte te verhalen, kan worden aangemerkt als een gerechtvaardigd belang in de zin van de Privacyrichtlijn.

In het Satamedia/Finland arrest van 27 juni 2017 hadden twee Finse bedrijven de belastinggegevens van 1,2 miljoen mensen in de krant gepubliceerd. De Finse autoriteiten waren van oordeel dat de publicatie in haar huidige vorm onrechtmatig was en legden een publicatieverbod op. De Finse bedrijven beriepen zich daarop op hun vrijheid van meningsuiting, maar het Europese Hof voor de Rechten van de Mens ging daar niet in mee.

Op 27 september 2017 oordeelde het HvJ EU in de zaak Peter Puskar/Slowakije dat persoonsgegevens zonder instemming van een betrokkene op een zwarte lijst geplaatst mogen worden ten behoeve van de bestrijding van belastingfraude, mits voldoende aanwijzingen bestaan om te vermoeden dat de betrokkene terecht op die lijst staat.

Op 3 oktober 2017 deed het Ierse gerechtshof uitspraak in de zaak die ook wel Schrems 2.0 wordt genoemd. Deze rechtszaak heeft wederom betrekking op de uitwisseling van persoonsgegevens van Europese burgers met de VS, maar dit keer op grond van de zogenaamde EU Standard Contractual Clauses. Op aandringen van de betrokken partijen heeft het Ierse gerechtshof besloten om prejudiciële vragen aan het HvJ EU te stellen over de rechtmatigheid van deze modelcontracten.

Op Nederlands niveau

De Hoge Raad ('HR') liet zich op 24 februari 2017 voor het eerst uit over het zogenaamde 'recht om vergeten te worden'

afkomstig uit het Google/Costeja arrest. De HR oordeelde dat een zoekmachine exploitant in beginsel gehouden is om een verwijderingsverzoek te honoreren. Het privacybelang van een natuurlijke persoon prevaleert in de regel boven het belang bij informatie van internetgebruikers en boven het economisch belang van de exploitant. Dit kan anders zijn in bijzondere gevallen, wanneer sprake is van bijzondere redenen die de inmenging in het recht op privacy rechtvaardigen.

Eveneens op 24 februari 2017 was de HR in drie afzonderlijke zaken van oordeel dat de Belastingdienst geen gebruik mag maken van foto's die zijn vastgelegd door Automatic Numberplate Recognition-camera's voor de controle van rittenregistraties in het kader van privégebruik van een auto van de zaak. Hiervoor bestaat namelijk geen toereikende wettelijke grondslag.

Op 23 augustus 2017 is de inspectie voor de gezondheidszorg ('IGZ') op de vingers getikt door de Raad van State. Een vrouw had in het kader van een klachtenprocedure tegen haar voormalige fysiotherapeut medische gegevens gedeeld met de IGZ. De vrouw verzocht de IGZ vervolgens om haar gegevens te verwijderen, maar de IGZ weigerde dat met een beroep op de Archiefwet. De Raad van State oordeelde kortgezegd dat de verwerking van medische gegevens door de IGZ niet was gebaseerd op een geldige wettelijke grondslag en dat de IGZ het verzoek van de vrouw dan ook niet had mogen afwijzen.

Op 1 december 2017 heeft de HR geoordeeld dat elektronische uitwisseling van patiëntengegevens in de zorg (de zorginfrastructuur) gebaseerd op toestemming van de patiënt op dit moment aanvaardbaar is. Daarbij is van belang dat het hof heeft onderkend dat de zorginfrastructuur in de toekomst – met de komst van de AVG – zo zal moeten worden ingericht dat meer onderscheid kan worden gemaakt tussen (soorten) gegevens en (categorieën) zorgaanbieders.

Meer weten?

Neem dan contact op met onze specialisten:

Direct: +31 70 2400 836
Mobiel: +31 6 1099 2888
E-mail: dejong@louwersadvocaten.nl

Direct: +31 40 2393 209
Mobiel: +31 6 4639 3938
E-mail: dewit@louwersadvocaten.nl

Direct: +31 70 2400 836
Mobiel: +31 6 2156 4116
E-mail: molenaars@louwersadvocaten.nl

Direct: +31 40 2393 200
Mobiel: +31 6 8344 1117
E-mail: vangroezen@louwersadvocaten.nl