ICTRECHT adviesbureau

ICTRECHT IN DE PRAKTIJK

jaargang 8 nummer 1 januari 2020

Wetgeving omtrent medische hulpmiddelen komt eraan: wat moet er gebeuren?

Crypto Law - handel in en reizen met encryptie-technologie

Een webshop hebben: makkelijk, toch?

Heeft u uw juridische zaken goed geregeld?

Zeker op het gebied van ICT en privacy is dit geen eenvoudige zaak.
Voorkom juridische ICT- of privacyproblemen en laat ICTRecht u deskundig en praktisch adviseren.
Dat hoeft helemaal niet duur te zijn: naast maatwerk leveren wij standaardproducten en juridische generatoren.

ICTRecht is een flexibel en creatief juridisch adviesbureau. Wij bedienen zowel de grote als de kleine klant. Onze adviezen zijn begrijpelijk, concreet en geven blijk van technische kennis. Onze mensen zijn dan ook juridisch en technisch thuis in onze niche.

Wij kunnen u van dienst zijn met:

Juridische documenten - Juridisch advies - Juridische detachering
Trainingen - Generatoren - Boeken

Meer informatie over hoe wij werken? Bezoek ictrecht.nl

ICTRECHT
adviesbureau

Voorwoord

Terwijl we dit schrijven, moeten de kerstdagen en natuurlijk de eindejaarsdrukte nog tot hun einde komen. U leest dit tijdschrift nu in de hopelijk rustigere maand januari. Daarmee hopen we dat we u een aantal nieuwe belangwekkende zaken mogen voorleggen. Zo komt binnenkort de Verordening voor medische hulpmiddelen uit, die vele appmakers zal raken. En de opkomst van cryptocoins en encryptiediensten botst ook met steeds meer wetgeving. De AVG blijft natuurlijk actueel, helemaal met de vraag of u nu verwerker bent of niet. Hierover leest u in onze hoofdartikelen.

Nieuw dit jaar is ook ons Handboek ICT-contracten, in de geheel herziene editie 2020. Met meer dan 40 modelcontracten en een geheel herzien theoretisch kader. Dit kader is ontwikkeld in onze eenjarige opleiding ICT-jurist, die in maart 2020 weer van start gaat. Zien we u daar?

Directie
Steven Ras en Arnoud Engelfriet

Index

Colofon

Dit is een uitgave van ICTRecht B.V.
020 663 1941, info@ictrecht.nl.

Dit tijdschrift verschijnt vier keer per jaar. Proeftijdschrift is op aanvraag beschikbaar. Abonnementsprijs is € 135,- excl. btw per jaar (papieren editie), inclusief verzendkosten in Nederland. Voor een jaarabonnement (digitale editie) betaalt u € 67,50 excl. btw.

Aan deze uitgave werkten mee:
Arnoud Engelfriet - Algemeen directeur / Opleidingsdirecteur - a.engelfriet@ictrecht.nl
Steven Ras - Algemeen directeur - s.ras@ictrecht.nl
Lisette Meij - Directeur ICTRecht Privacy - l.meij@ictrecht.nl
Peter Kager - Directeur ICTRecht Privacy - p.kager@ictrecht.nl
Alisa Schurink - Opleidingscoördinator en Marketingmedewerker - a.schurink@ictrecht.nl
Beryl Hetharia - Juridisch adviseur - b.hetharia@ictrecht.nl
Bram de Vos - Juridisch adviseur - b.devos@ictrecht.nl
Britt Telleman - Office- en Legal Assistant - b.telleman@ictrecht.nl
Daniëlle van Ginkel - Juridisch adviseur - d.vanginkel@ictrecht.nl
Dimmen Smolders - Juridisch adviseur - d.smolders@ictrecht.nl
Jay Remmelzwaal - Juridisch adviseur - j.remmelzwaal@ictrecht.nl
Jorden Bailey - Juridisch adviseur - j.bailey@ictrecht.nl
Jorien Zwaneveld - Juridisch adviseur - j.zwaneveld@ictrecht.nl
Kim Groot - Juridisch adviseur - k.groot@ictrecht.nl
Laura Monhemius - Juridisch adviseur - l.monhemius@ictrecht.nl
Martijn Michael - Juridisch adviseur - m.michael@ictrecht.nl
Nicole Waaijer - Marketing adviseur - n.waaijer@ictrecht.nl
Tessa van Schijndel - Juridisch adviseur - t.vanschijndel@ictrecht.nl
Eline Pellis - Vormgever - eline@elinepellis.com
Leonard Fäustle Stills & Motion - foto's ICTRecht - info@leonardfaustle.nl

Tessa van Schijndel
Juridisch adviseur

Overheid | Cloud | Privacy

Wetgeving omtrent medische hulpmiddelen komt eraan: wat moet er gebeuren?

Witte rook boven de Europese Commissie! Het lang verwachte richtsnoer voor de kwalificatie en classificatie van software als medische hulpmiddelen werd op 11 oktober 2019 gepubliceerd.[1] Het richtsnoer verduidelijkt wanneer software als medisch hulpmiddel kan worden gekwalificeerd. In de vanaf 26 mei 2020 geldende verordening EU 745/2017 (hierna: "MDR[2]"). Voor medische hulpmiddelen specifiek voor in-vitrodiagnostiek bestaat een aparte verordening, deze wordt in dit artikel buiten beschouwing laten. In dit artikel geven we u een update over het gepubliceerde richtsnoer waarin de Europese Commissie fabrikanten van medische software ondersteunt bij het beantwoorden van de vraag of hun software een medisch hulpmiddel is en in welke risicoklasse het valt.

Hoe zat het ook alweer?
Medische hulpmiddelen zijn instrumenten, toestellen, apparaten en software die voor medische doeleinden worden gebruikt. Software wordt gezien als medisch hulpmiddel wanneer deze wordt gebruikt voor diagnose, preventie, monitoring, voorspelling, prognose of behandeling van een ziekte. Het onderscheid tussen software met een medisch doel of met een algemeen doel, zoals lifestyle- en welzijnsdoeleinden, is niet altijd makkelijk te duiden. Hierdoor is het in veel situaties onduidelijk of software gekwalificeerd moet worden als medisch hulpmiddel. In 2016 heeft de Europese Commissie een eerste richtsnoer gepubliceerd om tekst en uitleg te geven met betrekking tot de oude richtlijn over medische hulpmiddelen. De Europese Commissie heeft nu haar vernieuwde richtsnoer gepubliceerd die uitleg geeft aan de tekst van de MDR.

De MDR brengt enkele wijzigingen ten opzichte van de oude richtlijn in de kwalificatie en classificatie van software als medische hulpmiddelen met zich mee. Voor een overzicht van de regels die van toepassing zijn op software als medisch hulpmiddel verwijzen we u graag naar ons vorige tijdschriftartikel in editie nummer 4, oktober 2019, over dit onderwerp. In het kort komt het erop neer dat het gebruik "medisch hulpmiddel" ruimer wordt gedefinieerd onder de MDR. Onder de medische doeleinden valt nu ook expliciet het voorspellen van een ziekte en het geven van een prognose. Bepaalde technologieën, bijvoorbeeld bij Artificiële Intelligentie (AI), die in staat zijn en bedoeld zijn om het verloop van een ziekte te voorspellen kunnen nu binnen de definitie van een medisch hulpmiddel vallen. Mede aan de hand

1. MDCG 2019-11 Guidance on Qualification and Classification Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR".
2. Verordening (EU) 2017/745 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen.

van de *intended use* (het beoogde doeleinde) van de fabrikant kan worden bepaald of de software een medisch hulpmiddel is en in welke risicoklasse de software valt. Ook de risicoclassificatie is strenger. Dit betekent dat de meeste medische software zal worden geplaatst in risicoklasse IIa. Dit betekent dat er voor deze software uiterlijk op 26 mei 2020 een geldige CE-markering door een notified body afgegeven moet zijn. Onder de oude richtlijn werd de meerderheid van de softwaretoepassingen als medisch hulpmiddel geclassificeerd in risicoklasse I en kon de fabrikant haar software zelf van een CE-markering voorzien.

Het richtsnoer: een verrassing?
Het vernieuwde richtsnoer gebruikt net als het oude richtsnoer beslisbomen en voorbeelden om software te kunnen kwalificeren en classificeren.[3] Het richtsnoer is aangepast aan de veranderingen van de MDR ten opzichte van de oude richtlijn. Er zijn echter geen fundamentele veranderingen te ontdekken. Software wat gekwalificeerd is als software als medisch hulpmiddel onder de oude richtlijn blijft software als een medisch hulpmiddel op grond van de MDR. Er worden daarnaast veel voorbeelden uit het oude richtsnoer hergebruikt.

Wel geeft het richtsnoer duidelijkheid met betrekking tot antwoorden op bepaalde vraagstukken, waar men eigenlijk al over uit was. Zo maakt het niet uit op welke locatie de software draait en door wie de software gebruikt wordt. Dit houdt in dat software als medisch hulpmiddel *on premise* bij een zorginstelling geïnstalleerd kan zijn, in de cloud kan draaien, op een mobiele telefoon kan worden geïnstalleerd of als extra functionaliteit aan een medisch hardware apparaat kan zijn verbonden. Ten aanzien van dit laatste geldt dat de software in dezelfde risicoklasse als de hardware valt als de software wordt gebruikt binnen het kader van het beoogde gebruik van de hardware. Maar als de software meer functies heeft die het beoogde gebruik uitbreiden, dan moet classificatieregel 11, welke speciaal geschreven is om software in een bepaalde risicoklasse te plaatsen, worden ingeroepen om een oordeel te vellen over de risicoklasse van de software.

In afwachting van het vernieuwde richtsnoer is het lang onduidelijk geweest of software die geen acties uitvoert op data nog steeds buiten de toepassing van de MDR valt. Inmiddels kan deze vraag bevestigend worden beantwoord. Software dat gebruikt wordt voor opslag, archivering of het reconstrueren van data wordt niet beschouwd als een medisch hulpmiddel onder de MDR. Ook software wat als communicatiemiddel wordt gebruikt of software wat simpele zoekopdrachten uitvoert valt niet onder de definitie van een medisch hulpmiddel.

Tegenwoordig worden er steeds meer complete softwarepakketten ontwikkeld die voorzien in alle behoeftes van een zorginstelling of een andere afnemende partij. Zo kan de software medische dossiers opslaan, maar ook gebruikt worden om administratieve taken bij te houden.Daarnaast kunnen softwaretoepassingen functionaliteiten bevatten die op basis van de opgeslagen informatie van de patiënt de zorgverlener ondersteuning bieden bij het nemen van medische beslissingen. Het richtsnoer gaat ook in op software dat in de gezondheidszorg wordt gebruikt en functionaliteiten bevatten die zowel uit medische als niet medische hulpmiddelen bestaan. Krachtens het richtsnoer moeten functionaliteiten die als medische hulpmiddelen worden gekwalificeerd aan de eisen uit de MDR voldoen. Voor de niet medische functies geldt dit niet. Het is de verantwoordelijkheid van de fabrikant om de verschillende functionaliteiten van de software te onderscheiden en te kwalificeren.

Een ander onder de richtsnoer onveranderd gebleven vereiste is de eis dat de actie die de software uitvoert op de data in het belang van een individuele patiënt moet worden uitgevoerd. Het richtsnoer geeft aanvullende voorbeelden over software die geen acties in het belang van een individuele patiënt uitvoeren. Denk hierbij aan acties die alleen bedoeld zijn om bevolkingsgegevens samen te voegen, generieke diagnoses stellen of behandelingen voorschrijven. Ook software gericht op medische literatuur, sjablonen, studies of registers vallen niet onder de definitie van een medisch hulpmiddel.

Vaarwel risicoklasse I voor software als medisch hulpmiddel
In de regels 9, 10, 11, 12, 13 en 15 worden voornamelijk de risico's in verband met actieve hulpmiddelen beschreven (waar ook software onder valt) die een diagnostische of therapeutische bijdrage leveren. In overeenstemming met regel 5 van bijlage 8, is de strengste regel van toepassing bij het bepalen van de risicoclassificatie van de software.

Regel 11 uit bijlage 8 van de MDR is van cruciaal belang voor het classificeren van software in een risicoklasse. Software met een therapeutisch of diagnostisch doel wordt geclassificeerd in risicoklasse IIa. Naarmate het belang van de verstrekte informatie en de potentiele impact van een (onjuist) besluit dat is genomen op basis van de software als medische hulpmiddel groter is, valt de software in een hogere risicoklasse. Zo zullen veel oplossingen die worden gebruikt bij ziekten, waarbij het medisch advies kan leiden tot tijdelijke of per-

3. Meddev 2.1/6, juli 2016.

manente verslechtering van de gezondheid van een persoon, worden ingedeeld worden in klasse IIb en III.

Het geven van voorbeelden verduidelijkt iedere situatie. Zo dacht de Europese Commissie er ook over. Zij sluit haar richtsnoer af met een scala aan praktische voorbeelden. Weer geen vernieuwing ten opzichte van het oude richtsnoer, maar wel ontzettend duidelijk. In het kort de belangrijkste voorbeelden:

- Een Elektronisch Patiënten Dossier (hierna: "EPD") is geen medisch hulpmiddel.
- Software welke algemene medische informatie met een algoritme combineert met patiëntspecifieke gegevens is wel een medisch hulpmiddel, zoals planningssystemen om doseringen te berekenen of software wat ECG's (een ECG wordt gebruikt voor het maken van een hartfilmpje) kan interpreteren.
- Een mobiele app die bedoeld is om de hartslag van een gebruiker te analyseren en afwijkingen op te sporen wordt geclassificeerd als klasse IIb, indien de informatie die door de software wordt geleverd is bedoeld om de zorgverlener te begeleiden bij de diagnose.
- Software wat de zorgverlener helpt bij het rangschikken van behandelsuggesties op basis van het medisch dossier van de patiënt en testuitslagen is ook een medisch hulpmiddel.

Overige updates

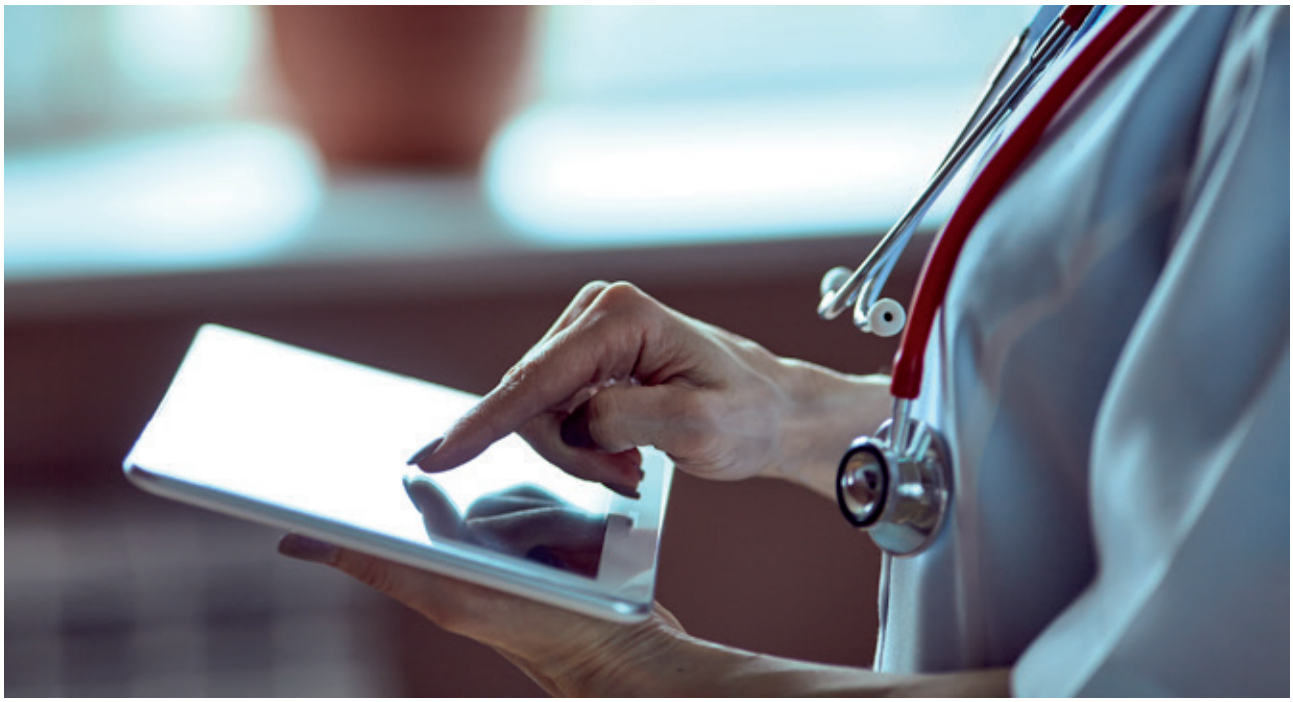
Naast de publicatie over medische software heeft de Europese Commissie ook naar buiten gebracht dat database EUDAMED tot 2022 wordt uitgesteld. De EUDAMED, "European database on Medical Devices" is de centrale Europese database waar alle informatie over medische hulpmiddelen te vinden is. In deze database moet de medische software met een UDI-code (UDI staat voor Unique Device Identifier) worden opgenomen. De UDI-code is een eenduidige vorm van codering van medische hulpmiddelen.

Daarnaast zijn in Nederland inmiddels twee *notified bodies* aangewezen op grond van de MDR. Vanuit het veld is veel zorg geuit over de beschikbaarheid van voldoende *notified bodies*. Ook rijst de vraag of de *notified bodies* over de juiste expertise beschikken om medische software te beoordelen.[4] Vanwege de grote hoeveelheid medische hulpmiddelen die opnieuw getoetst moeten worden aan de MDR, zijn er wettelijke overgangstermijnen opgenomen waarmee een medisch hulpmiddel tot uiterlijk 2025 op de markt kan blijven onder de voorwaarden van de oude richtlijn.

Conclusie

Software als medisch hulpmiddel kan vrijwel nooit meer in risicoklasse I worden ingeschaald, maar zal ook zelden in klasse III vallen. Zelfs als software alleen tot klasse IIa behoort, moet klinisch bewijs worden gebruikt om de waarde van de software aan te tonen om het voordeel ervan te rechtvaardigen. Toch is het bewijzen van de waarde van digitale oplossingen niet zo eenvoudig als bij traditionele medische hulpmiddelen. Ook de *notified bodies* moeten over voldoende expertise beschikken, zodat zij in staat zijn om medische software te beoordelen voordat zij een CE-markering afgeven.

4. Kamerbrief 1594336-197064-GMT, 2019/20, 22 november 2019.



Martijn Michael
Juridisch adviseur

Cloud | Software | Innovatie

Crypto Law - handel in en reizen met encryptietechnologie

Encryptie maakt een steeds belangrijker onderdeel uit van ons dagelijks leven. Het nieuws staat geregeld vol artikelen over hoe criminele organisaties of buitenlandse overheden beveiligingslekken in hard- en software uitbuiten om gevoelige data te ontfutselen. Daarbij wordt erop gehamerd om apparaten te updaten en te voorzien van sterke encryptie. Deze ontwikkeling is ook terug te zien op de markt en bij ontwikkelaars. Denk bijvoorbeeld aan Google die vanaf Android Lollipop automatisch full-device encryptie inschakelde terwijl dat in eerdere versies handmatig moest worden gedaan.

Tevens wordt erkend dat encryptietechnologie risico's meebrengt en is handel in en gebruik van encryptietechnologie wereldwijd op verscheidene manieren gereguleerd om misbruik te voorkomen en autoriteiten een kans te bieden tegen crimineel gebruik van encryptie.

Wat als u als bedrijf encryptietechnologie, bijvoorbeeld een cryptofoon, op de globale markt wil brengen? Met welke barrières krijgt u dan te maken? Kunnen uw klanten ongestoord met uw producten op reis, zonder in problemen te komen met buitenlandse autoriteiten? Hoe zit dat met berichtgeving over apparaatdoorzoekingen aan bijvoorbeeld de Amerikaanse grens? En hoe doet Apple dat eigenlijk met zijn versleutelde iPhones?

Dual use technologie
Voldoende geavanceerde encryptietechnologie wordt gekwalificeerd als *'dual use'*. '*Dual use goods and technologies'* zijn producten en technologieën toepasbaar voor zowel commerciële als militaire doeleinden. Omdat deze technologieën in de verkeerde handen grote schade aan kunnen richten, reguleren de meeste landen de verhandeling ervan.

In sommige omstandigheden kunnen *dual use* technologieën vrij worden verhandeld. Bijvoorbeeld wanneer die handel binnen de Europese Unie plaatsvindt. Echter vereisen veel regimes dat importeurs en exporteurs voldoen aan notificatie- of vergunningsprocedures met uiteenlopende gradaties van transparantie, gecompliceerdheid en zekerheid wat betreft uitkomst. In sommige situaties is de wettelijke status van encryptie geheel onduidelijk.

Een reiziger die de grens oversteekt met gereguleerde *dual use* technologie voor persoonlijk gebruik wordt als importeur/exporteur beschouwd. Dezelfde notificatie- of vergunningsprocedures moeten dan worden gevolgd, behalve wanneer het betreffende regime hiervoor een vrijstelling toepast.

Harmonisatie... of toch niet?
Tot nu toe hebben 42 landen de noodzaak tot het reguleren van *dual use* technologieën erkend en getracht een harmonisatieslag te slaan door middel van de Wassenaar Arrangement.

De Wassenaar Arrangement is grotendeels niet bindend voor de betrokken partijen en dient voornamelijk als gids voor invulling van nationale regelgeving. Daardoor is de relevantie van de controlelijsten (de lijsten met goederen en technologieën die onder het akkoord vallen) en *'best practice'* compendia opgenomen in het

akkoord beperkt. Onder het akkoord hebben landen slechts concreet verklaard dat zij:

1. *"have agreed to maintain national export controls on items included in the WA Control Lists. These controls are implemented via national legislation;*
2. *are guided by agreed Best Practices, Guidelines or Elements;*
3. *have agreed to report on transfers and denials of specified controlled items to destinations outside the Arrangement;*
4. *exchange information on sensitive dual-use goods and technologies."*[1]

Hoewel aansluiting van een land bij de Wassenaar Arrangement kan wijzen op de algemene aanpak met betrekking tot de regulering van encryptie, zijn er tussen de aangesloten landen aanzienlijke verschillen in de regulering van handel in dergelijke technologieën en de te volgen procedures voor de vereiste vergunningen.

Op globale schaal en ten aanzien van de Wassenaar Arrangement is het lastig om een beeld te krijgen van de toepasselijke regels. Het wereldwijd in kaart te brengen hiervan is een omvangrijke taak en met betrekking tot sommige regimes ronduit onmogelijk. Regelgeving en beleid omtrent encryptie zijn in gevallen slechts in de originele taal raadpleegbaar of geheel niet transparant of beschikbaar. Daarnaast is regelgeving omtrent dit onderwerp continu in ontwikkeling. Pogingen om een globaal beeld te schetsen van de regels omtrent encryptie, zoals bijvoorbeeld de Crypto Law Survey van hoogleraar Bert-Jaap Koops, zijn daardoor veelal gebaseerd op anekdotes en vanwege ontwikkelingen in en gebrek aan raadpleegbaarheid van (originele) wetgeving lastig om juridisch betrouwbaar en actueel te houden.[2]

Echter, in de Europese Unie wordt de handel in *dual use* technologie geregeld in Verordening 428/2009, die gebaseerd is op de Wassenaar Arrangement. Als gevolg hiervan is export naar landen buiten de EU geharmoniseerd.

Import en export van encryptietechnologie
De Wassenaar Agreement en Verordening 428/2009 reguleren de export van *dual use* technologie om te voorkomen dat deze in de verkeerde handen terechtkomt. Desalniettemin reguleren veel aangesloten partijen, waaronder Nederland, tevens de import ervan, waardoor dat in de meeste gevallen gepaard moet gaan met het indienen van de juiste formulieren bij de juiste autoriteiten. Andere voorbeelden, zoals de Verenigde Staten, beperken de invoer van *dual use* technologie in principe niet. Ten slotte zijn er landen, waaronder China, die de invoer van *dual use* technologie in principe lijken toe te staan, maar waarbij de procedurele details, de vereisten en de resultaten van de stappen die moeten worden doorlopen voor legale invoer en gebruik ondoorzichtig en onzeker zijn.[3]

En de iPhone dan?
Zoals eerder opgemerkt dringt encryptietechnologie steeds verder door in ons dagelijks leven. De beschreven onzekerheden en het gebrek aan harmonisatie roepen misschien de vraag op hoe het dan komt dat er – voor zowel persoonlijk als commercieel gebruik – voortdurend grenzen worden overgestoken met iPhones en andere apparaten zoals laptops, waar geavanceerde encryptietechnologie in is verwerkt.

Reizen met encryptietechnologie: persoonlijk gebruik
Wat betreft reizen met encryptietechnologieën bevatten de Wassenaar Arrangement en de Verordening 428/2009 in Categorie 5 – deel 2, Noot 2 een uitzondering. Namelijk dat wanneer deze voor persoonlijk gebruik over de grens worden gebracht, ze niet onderhavig zijn aan regulering. Hoewel dit voldoende zekerheid biedt tussen lidstaten van de Europese Unie, zijn de overige partijen bij de Wassenaar Arrangement niet gehouden deze uitzondering (of andere onderdelen van de controlelijsten) daadwerkelijk toe te passen. Van de partijen bij de Wassenaar Arrangement passen alleen Rusland en Oekraïne geen uitzondering voor eigen gebruik toe.[4]

iPhones en andere versleutelde apparatuur: algemeen voor het publiek verkrijgbaar
Een andere verklaring voor de stand van zaken waarin een grote hoeveelheid encryptietechnologie probleemloos lijkt te worden verhandeld is een uitzondering opgenomen in Categorie 5 – deel 2 van de controlelijsten bij de Wassenaar Arrangement en de Verordening 428/2009, welke ziet op encryptie. In Noot 3 is een verzameling vereisten opgenomen waaronder encryptietechnologie van handelsregulering is uitgesloten. De vereisten zijn dat (i) de technologie beschikbaar is voor algemeen publiek en uit voorraad wordt verkocht in de detailhandel, (ii) de encryptiefuncties niet gemakkelijk kunnen worden aangepast door de gebruiker, (iii) de goederen zijn ontworpen voor installatie door de gebruiker zonder wezenlijke ondersteuning van de leverancier en (iv) er voldoende gegevens beschikbaar zijn (desnoods op verzoek) aan de hand waarvan de relevante autoriteit in de lidstaat van de exporteur punten (i) – (iii) kan vaststellen. Op basis van de punten drie en vier van de hiernaast genoemde afspraken onder de Wassenaar Arrangement dienen par-

1. https://bit.ly/38AzKVk
2. http://www.cryptolaw.org/
3. https://bit.ly/2YLrvBB
4. https://bit.ly/38ywqtX

tijen informatie uit te wisselen over de exportvergunningen die zij toekennen. Dit zou kunnen voorkomen dat een commercieel product in het ene land onder deze uitzondering wordt geschaard en in het andere land niet. De relevante autoriteit van elk land blijft in staat zelf te beslissen over het toekennen van import- en exportvergunningen. Toepasselijkheid van deze uitzondering, zeker wereldwijd, is voor fabrikanten van encryptietechnologieën dus geen zekerheid.

Reizen met encryptietechnologie: grensdoorzoekingen
Zoals gezegd, stellen partijen bij de Wassenaar Arrangement encryptietechnologieën die voor persoonlijk gebruik over de grens worden vervoerd, vrij van handelsregulering. In sommige regimes kunnengrensautoriteiten echter nog steeds hun ruime onderzoeksbevoegdheden uitoefenen om dergelijke apparatuur in beslag te nemen en te controleren (zoals ze dat ook zouden doen bij het in beslag nemen en doorzoeken van een koffer) aan de grens om welke reden dan ook, zonder bevelschrift.[5]

In één van de meest beruchte voorbeelden van landen met dergelijke doorzoekingsmogelijkheden, de Verenigde Staten, kunnen reizigers verplicht worden om apparaten en de daarin opgenomen informatie in een zodanige vorm te presenteren dat de inhoud ervan kan worden gecontroleerd. Weigering kan tot gevolg hebben dat grensautoriteiten het apparaat in beslag nemen en proberen de versleuteling met technische middelen te kraken, of dat zij andere wettelijke methoden inzetten om de reiziger tot medewerking te dwingen.[6]

Een reiziger kan natuurlijk alsnog weigeren medewerking te verlenen. Moderne en adequate encryptie zal er dan voor zorgen dat de opslagen data veilig blijft.

Grensautoriteiten hebben echter in de meeste gevallen een vrije bevoegdheid om een reiziger tijdelijk vast te houden, het apparaat voor langere tijd in beslag te nemen of de situatie anderszins te escaleren. Zo kunnen niet-ingezeten in de Verenigde Staten, het Verenigd Koninkrijk en Israel het land worden uitgezet als zij weigeren hun wachtwoorden aan de grens bekend te maken.[7] In Nieuw-Zeeland kunnen autoriteiten een boete opleggen bij weigering.[8]
De Verenigde Staten is het meest beruchte voorbeeld van landen die grensdoorzoekingen van apparatuur toepassen. Tegelijkertijd zijn de Amerikaanse regels en praktijk hieromtrent juist het meest transparant en het best gedocumenteerd. Andere voorbeelden zijn Australië, Canada, Nieuw-Zeeland, het Verenigd Koninkrijk, Turkije en Israël. In de meeste gevallen is het onduidelijk in welke mate grensautoriteiten apparaten mogen doorzoeken (is het bijvoorbeeld een vriendelijk verzoek of een bevel?), in welke mate zij van een reiziger kunnen eisen dat hij zijn wachtwoord bekendmaakt en wat er gebeurt als een reiziger dit weigert. Veel verslagen van apparaatdoorzoekingen zijn anekdotisch. Zo werd een Harvard-affiliate in Amsterdam door grensautoriteiten gevraagd om zijn reis met foto's van zijn telefoon te verifiëren voordat hij terug mocht keren naar de VS, terwijl de Nederlandse wet deze bevoegdheid in principe niet toekent aan grensautoriteiten en niet voorziet in een wettelijke manier om een verdachte in een strafrechtelijk onderzoek te dwingen zijn inloggegevens bekend te maken.[9]

Conclusie
Het doorlopen van de juiste procedures kan voor een onderneming die voornemens is encryptietechnologie op de markt te brengen een grote uitdaging vormen, gezien de wereldwijde verschillen in regelgeving. Ondernemingen die dergelijke activiteiten willen ontplooien zullen er niet aan ontkomen om per land de vereiste mate van onderzoek te doen.

Daarnaast bent u er als afnemer van zulke technologie niet altijd zeker van dat u probleemloos grenzen kunt oversteken en in welke problemen u kunt belanden als u weigert grensautoriteiten toegang tot uw apparaat te verlenen. Echter, ondanks de onzekerheden omtrent de wereldwijde regulering van encryptie, lijkt handel in, gebruik van en reizen met encryptietechnologieën in de praktijk toch grotendeels goed te gaan. De tijd zal leren hoe deze vraagstukken zich ontwikkelen naarmate de prominentie van encryptie verder toeneemt.

Dit artikel is geschreven in samenwerking met oud-stagiair Bob van Dijk.

5. Zie bv.: Abidor v. Napolitano, 990 F. Supp.2d 260, 277-282 (E.D.N.Y. 2013).
6. https://bit.ly/34fnwOM p. 6-11.
7. https://bit.ly/2LSO8yJ; https://bit.ly/2EgX6Se
8. https://bit.ly/2RNOcU7
9. https://bit.ly/34ksnho

ICTRECHT
academy

Senior privacy jurist worden?

Privacy (AVG) en bescherming van persoonsgegevens vormen een kernaspect binnen het ICT-recht. De ICTRecht Academy biedt u een praktijkgerichte opleiding tot senior privacy jurist. In één jaar (start maart 2020) doet u gespecialiseerde juridisch én technische kennis op over privacy. U leert onder meer over: datalekken, DPIA, ICT en zorg, legal tech en security.

"Een fijne opleiding die goed afgestemd is op de praktijk. Door veel interactie worden problemen in de praktijk aangekaart en wordt uitgelegd hoe op een pragmatische wijze invulling kan worden gegeven aan de privacywetgeving."

Lubna Bouzariat
Privacy Officer/Juridisch adviseur
bij Gemeente Groningen
– over opleiding senior privacy jurist
2019/2020

Kijk voor meer informatie op
ictrecht.nl/academy-privacy

Gemiddeld beoordeeld met een **8**

Senior privacy jurist

46 PUNTEN PO ADVOCATUUR

NEDERLANDSE ORDE VAN ADVOCATEN

ICT-jurist worden?

De ICTRecht Academy biedt u een praktijkgerichte opleiding tot ICT-jurist op twee niveaus. In één jaar (start maart 2020) doet u gespecialiseerde juridische én technische kennis op over het ICT-vakgebied. U leert onder meer over: privacy en persoonsgegevens, auteursrechten, het recht rond platforms, contracteren, legal tech, blockchain en security.

"De opleiding omschrijf ik als zeer nuttig, leerzaam en interessant. Goede docenten. De afwisseling is ook prettig en de studielast niet te groot. Er is veel ruimte voor eigen inbreng gedurende de trainingen, waardoor vragen beantwoord worden. Ik zou de opleiding zeker aanraden."

Sophie Yocarini
Legal Counsel
bij Jobs & Media Group
– over opleiding senior ICT-jurist 2019/2020

Kijk voor meer informatie op
ictrecht.nl/academy

Gemiddeld beoordeeld met een **7,7**

Niveau juridisch adviseur

56 PUNTEN PO ADVOCATUUR — NEDERLANDSE ORDE VAN ADVOCATEN

Niveau senior juridisch adviseur

64 PUNTEN PO ADVOCATUUR — NEDERLANDSE ORDE VAN ADVOCATEN

Bram de Vos
Juridisch adviseur

Wet- en regelgeving

Voorstel tot wijziging Wet kwaliteit, klachten en geschillen zorg
In de periode van 22 juli tot en met 2 september 2019 heeft het Ministerie van Volksgezondheid, Welzijn en Sport een internetconsultatie gehouden met betrekking tot een voorstel tot wijziging van de Wet kwaliteit, klachten en geschillen zorg. Het wetsvoorstel introduceert een wettelijke grondslag voor het verwerken van gepseudonimiseerde persoonsgegevens ten behoeve van twee kwaliteitsregistraties. Het betreft het Landelijk Alcohol Drugs Informatie Systeem (LADIS) en de Landelijke Trauma Registratie (LTR). Deze registers moeten inzicht geven in de kwaliteit van zorg om daarmee ook doelgerichte verbeteringen voor de toekomst te kunnen doorvoeren. De kwaliteitsregisters zijn niet nieuw. Echter werd in het verleden een expliciete grondslag voor de verwerking van de gepseudonimiseerde gegevens niet noodzakelijk geacht. In verband met de invoering van de Algemene verordening gegevensbescherming (AVG) is die noodzaak er nu wel.

https://bit.ly/2OP8Dgp

Nieuwe regels inzake sterke cliëntauthenticatie
Sinds 14 september 2019 zijn nieuwe regels omtrent sterke cliëntauthenticatie van kracht. Deze regels vloeien voort uit de herziene Richtlijn betaaldiensten (ook wel bekend als PSD2) en verplichten betalingsdienstaanbieders om bij bepaalde handelingen van gebruikers sterke cliëntauthenticatie toe te passen. Dit houdt in dat bij de authenticatie gebruik moet worden gemaakt van ten minste twee verschillende factoren zoals kennis (iets wat alleen de gebruiker weet), bezit (iets wat alleen de gebruiker heeft) en inherente eigenschappen (iets wat de gebruiker is). Op die manier moet de veiligheid van het online betaalverkeer worden vergroot en moeten gebruikers beter worden beschermd tegen onder meer fraude. De verplichtingen uit de richtlijn zijn nader ingekleurd in Regulatory Technical Standards (RTS) van de European Banking Autority (EBA). Marktpartijen hadden in principe tot 14 september de tijd om deze RTS te implementeren. Wel is er in bepaalde gevallen ruimte om uitstel krijgen voor de migratie naar sterke cliëntauthenticatie.

https://bit.ly/2QY4E3H

Voorstel tot wijziging Wet toezicht collectieve beheersorganisaties
Op 10 oktober 2019 heeft Minister Dekker (Rechtsbescherming) een voorstel aan de Tweede Kamer toegestuurd dat strekt tot wijziging van de Wet toezicht en geschillenbeslechting beheersorganisaties auteurs- en naburige rechten. Het voorstel verduidelijkt op de eerste plaats de bevoegdheden van het College van Toezicht dat in Nederland collectieve en onafhankelijke beheersorganisaties zoals Buma/Stemra en Sena controleert. Door de wetswijziging moet de slagvaardigheid en doelmatigheid van het toezichtorgaan worden vergroot. Ten tweede wordt via het wijzigingsvoorstel een deel van de toezichtkosten bij de beheersorganisaties neergelegd. Op dit moment worden deze kosten nog volledig uit algemene middelen voldaan.

https://bit.ly/2rtfDYd

Richtsnoer medische hulpmiddelen
Op 11 oktober 2019 heeft de Europese Commissie een richtsnoer gepubliceerd met betrekking tot de kwalificatie en classificatie van software als medisch hulpmiddel. Er was reeds een richtsnoer door de Europese Commissie gepubliceerd in 2016, maar deze ging nog uit van de Richtlijn medische hulpmiddelen (93/42/EEG). Mede in verband met de introductie van de nieuwe Europese verordeningen voor medische hulpmiddelen

(2017/745/EU) heeft de Europese Commissie het richtsnoer nu vernieuwd. Het document bevat onder meer voorbeelden en beslisbomen aan de hand waarvan kan worden beoordeeld of bepaalde software als medisch hulpmiddel kan worden aangemerkt en in welke risicoklasse het hulpmiddel valt. Zie het artikel op pagina 4.

https://bit.ly/34wLA0g

Wijziging van de Rijksoctrooiwet 1995
Op 29 oktober 2019 heeft de Eerste Kamer een voorstel tot wijziging van de Rijksoctrooiwet 1995 aangenomen. De wijziging houdt verband met de introductie van de Europese Verordening tot instelling van eenheidsoctrooibescherming (1257/2012/EU). Op grond daarvan wordt het mogelijk om middels één registratie octrooibescherming te verkrijgen in alle deelnemende Europese lidstaten. Ook voorziet de wetswijziging in een procedure voor Europese geschilbeslechting (voortvloeiend uit de Overeenkomst betreffende een eengemaakt octrooirecht). Geschillen over Europese octrooien kunnen op basis daarvan worden voorgelegd aan het Eengemaakt Octrooigerecht (EOG). Een uitspraak van het EOG heeft werking in alle deelnemende lidstaten, zodat het niet langer nodig is om in elke lidstaat afzonderlijk een inbreukprocedure te beginnen. Ook de geldigheid van een Europees octrooi kan via het EOG in één procedure worden vastgesteld.

https://bit.ly/2Doj8BQ

Focus AP 2020-2023
Op 11 november 2019 heeft de Autoriteit Persoonsgegevens het rapport Focus AP 2020-2023 gepubliceerd waarin de handhavingsprioriteiten van de toezichthouder voor de komende jaren worden toegelicht. Uit het rapport volgt dat de Autoriteit Persoonsgegevens extra aandacht zal besteden aan drie onderwerpen. Een eerste aandachtsgebied is dat van "datahandel". Volgens de Autoriteit Persoonsgegevens vindt er steeds meer ongeoorloofde doorverkoop van persoonsgegevens plaats. Betrokkenen hebben hier slechts zeer beperkt grip op, wat resulteert in een wezenlijke aantasting van hun privacyrechten. Daarnaast zal de toezichthouder zich richten op de digitale overheid. Dit met name omdat de overheid over een grote hoeveelheid - vaak bijzondere of gevoelige - persoonsgegevens beschikt. Een derde en laatste speerpunt is het gebruik Artificiële Intelligentie (AI) en algoritmes. Met het gebruik hiervan gaan belangrijke risico's gepaard. Onverantwoordelijk gebruik kan volgens de toezichthouder onder meer leiden tot foutieve beslissingen, uitsluiting van betrokkenen en discriminatie.

https://bit.ly/2QWsvkk

Leidraad voorkomen misleiding bij doorschakeldiensten
Op 21 november 2019 heeft de Autoriteit Consument en Markt (ACM) een leidraad gepubliceerd waarin zij handvatten biedt voor aanbieders van doorschakeldiensten. Het gaat hierbij om een dienst waarbij de beller via een informatienummer wordt doorgeschakeld naar een ander nummer dat hij wil bereiken. Voor dergelijke doorschakeldiensten wordt meestal een tarief per minuut gerekend. Dit (vaak hoge) tarief wordt betaald gedurende het gehele gesprek, ook nadat de beller is doorgeschakeld. Omdat de ACM vanuit ConsuWijzer signalen ontving dat aanbieders van doorschakeldiensten misleidend adverteren, heeft de toezichthouder nu een leidraad gepubliceerd waarin concrete voorschriften te vinden zijn.

https://bit.ly/2XUMq4t

Beryl Hetharia
Juridisch adviseur

Privacy

Wie ben ik? Verwerkings-verantwoordelijke of verwerker?

De rolverdeling tussen partijen, een lastig onderwerp. Niet alleen organisaties worstelen hiermee, ook onder juristen leidt de rolverdeling vaak tot discussie. Wanneer ben je nou verwerkingsverantwoordelijke en wanneer verwerker? Of zijn organisaties gezamenlijk of misschien wel zelfstandig verwerkingsverantwoordelijken? In dit artikel geven wij handvatten om te bepalen welke rol een organisatie heeft en waar dan op gelet moet worden.

Verwerkingsverantwoordelijke
In de Algemene verordening gegevensbescherming (AVG) is de definitie van verwerkingsverantwoordelijke als volgt omschreven: "Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt".[1]

Doel
Om erachter te komen welke partij het doel vaststelt, kun je verschillende vragen stellen. Waarom vindt verwerking van persoonsgegevens plaats, bij wie ligt het initiatief om persoonsgegevens te verwerken en wie profiteert van de verwerking?[2] Soms is het vrij eenvoudig om een partij aan te merken als verwerkingsverantwoordelijke. Denk aan een webshop die producten te koop aanbiedt. Zodra een bestelling wordt geplaatst, worden er persoonsgegevens verwerkt. Bijvoorbeeld de naam, het leveringsadres en de betalingsgegevens. Deze gegevens zijn nodig ter uitvoering van de overeenkomst tussen de webshop en de consument. Het wordt al wat lastiger wanneer deze webshop op zoek is naar nieuw personeel en hiervoor een derde partij inschakelt. In sommige gevallen is die derde partij een verwerker, maar het is ook goed mogelijk dat de webshop en het wervingsbureau allebei verwerkingsverantwoordelijke zijn. Beide smaken worden in dit artikel uitgewerkt.

Middelen
Naast het hebben van een doel om persoonsgegevens te verwerken, zijn daar ook middelen voor nodig. Het vaststellen van de middelen moet ruim worden opgevat. Het gaat daarbij niet alleen om het technische gedeelte van de gegevenswerking, bijvoorbeeld welke software een bedrijf gaat gebruiken voor de gegevensverwerking. Het omvat ook de manier van verwerking. Denk daarbij aan welke persoonsgegevens verwerkt moeten worden, wie toegang moet hebben tot de gegevens en wanneer de gegevens weer dienen te worden verwijderd.[3]

In de praktijk komt het vaak voor dat juist een verwerker bepaalde software aanbiedt waarmee persoonsgegevens worden verwerkt, maar het is de verwerkingsverantwoordelijke die bepaalt op welke wijze persoonsgegevens verwerkt worden en daarmee stelt de verwerkingsverantwoordelijke de middelen vast.

1. Artikel 4(7) AVG.
2. European Data Protection Supervisor, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 7 november 2019.
3. Artikel 29-werkgroep, Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", .

Verwerker
De definitie van verwerker luidt zo: "Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. In opdracht van de verwerkingsverantwoordelijke verwerkt de verwerker persoonsgegevens.

Zoals hiernaast is aangegeven bepaalt de verwerkingsverantwoordelijke het doel en de middelen. Echter, in de praktijk zien we vaak dat een verwerker de middelen uitkiest. Een makkelijk voorbeeld is het uitbesteden van de administratie. Het administratiekantoor dat de salarisadministratie voor een klant doet, kan gebruik maken van haar eigen boekhoudpakket. Ondanks dat het administratiekantoor de middelen bepaalt, wordt het kantoor als verwerker aangemerkt. De klant schrijft namelijk voor waarom het administratiekantoor persoonsgegevens moet verwerken en door ervoor te kiezen om de administratie uit te besteden aan een specifiek kantoor, worden de middelen daarmee impliciet door de verwerkingsverantwoordelijke bepaald.

Terugkomend op het voorbeeld van de werving en selectie voor de webshop. Wanneer de webshop op zoek is naar nieuw personeel en deze zoektocht wil uitbesteden aan een wervingsbureau, dan gaat het wervingsbureau persoonsgegevens van kandidaten verzamelen. Het gaat dan bijvoorbeeld om een naam en contactgegevens, maar ook een CV is te kwalificeren als persoonsgegeven. Voor deze persoonsgegevens kunnen we het wervingsbureau aanmerken als verwerker. In opdracht van de webshop gaat het wervingsbureau op zoek naar geschikte werknemers en draagt vervolgens de persoonsgegevens van kandidaten over aan de webshop. Het is aan de webshop om de verdere sollicitatieprocedure af te wikkelen. Om de verhouding webshop vs. wervingsbureau aan te duiden als verwerkingsverantwoordelijke-verwerkersrelatie is het belangrijk dat de webshop een welbepaalde opdracht en instructies geeft aan het wervingsbureau. Het wervingsbureau mag hier niet van afwijken. Gebeurt dat toch, en stelt het wervingsbureau dus zelf het doel en de middelen vast, dan wordt het wervingsbureau als verwerkingsverantwoordelijke beschouwd.[4] Dat is bijvoorbeeld het geval wanneer het wervingsbureau een eigen database met kandidaten beheert om eventueel in de toekomst aan een werkgever voor te stellen.

Verwerkersovereenkomst
Schakel je als verwerkingsverantwoordelijke een verwerker in, dan is het wettelijk verplicht om afspraken te maken over de verwerking van persoonsgegevens.[5] Het is gebruikelijk om de afspraken vast te leggen in een verwerkersovereenkomst. Wat regel je in een verwerkersovereenkomst? Enkele onderwerpen zullen we hieronder aanstippen.

Persoonsgegevens
Een open deur: in een verwerkersovereenkomst regel je welke categorieën persoonsgegevens zullen worden verwerkt. Daarnaast leg je vast op welke manier en voor welke doeleinden een verwerker de persoonsgegevens gaat verwerken. Vaak zie je dat een overzicht van persoonsgegevens als bijlage is opgenomen in de verwerkersovereenkomst.

Sub-verwerker
Om de dienst te kunnen leveren, schakelt een verwerker soms een andere partij in, genaamd sub-verwerker. Voordat een verwerker een sub-verwerker betrekt bij de verwerking van persoonsgegevens, is er toestemming nodig van de verwerkingsverantwoordelijke.[6] Daarnaast is het belangrijk dat de sub-verwerker dezelfde verplichtingen opgelegd krijgt als de verwerker opgelegd heeft gekregen van de verwerkingsverantwoordelijke.[7]

Audit
Als verwerkingsverantwoordelijke mag je onder de AVG controleren of de verwerker zijn afspraken uit de verwerkersovereenkomst nakomt. Dit kun je doen door periodiek een audit uit te (laten) voeren. Het is dan belangrijk om afspraken te maken over de kosten van de audit.

Beveiligingsmaatregelen
Zowel een verwerkingsverantwoordelijke als een verwerker is verplicht om passende technische en organisatorische maatregelen te treffen. Een verwerkingsverantwoordelijke wil er immers wel zeker van zijn dat persoonsgegevens goed beveiligd zijn bij de verwerker.

Datalekken
Mocht zich onverhoopt een datalek voordoen, dan zal de verwerker dat moeten melden bij de verwerkingsverantwoordelijke. In een verwerkersovereenkomst leg je de termijn van de meldplicht vast, maar maak je natuurlijk ook afspraken over aansprakelijkheid.

Gezamenlijke verwerkingsverantwoordelijken
De hoofdrolspelers binnen de AVG, de verwerkingsverantwoordelijke en de verwerker, hebben we besproken. Nu gaan we kijken naar de situatie waarbij twee organisaties persoonsgegevens verwerken, maar er geen sprake is van verwerkingsverantwoordelijke-verwerkersrelatie.

4. Artikel 28(10) AVG.
5. Artikel 28(3) AVG.
6. Artikel 28(2) AVG.
7. Artikel 28(3)(d) AVG.

De AVG biedt ruimte voor organisaties die gezamenlijk verantwoordelijk zijn voor de verwerking van persoonsgegevens.[8] Geen eenzijdige instructies van de ene partij naar de andere partij, maar twee (of meer) partijen die samen het doel en de middelen bepalen. Dat is het gemakkelijkst uit te leggen aan de hand van een voorbeeld.

Stel, een bedrijf is zo aan het groeien dat er extra personeel nodig is. Het bedrijf heeft niet veel ervaring met recruitment en schakelt de hulp in van een wervingsbureau. Om de sollicitaties te stroomlijnen, besluiten het bedrijf en het wervingsbureau om samen een online portaal op te starten waar alle sollicitatiebrieven binnenkomen. De organisaties slaan de handen ineen en zijn gezamenlijk verantwoordelijk voor de verwerking van persoonsgegevens.

Nu organisaties gezamenlijk verantwoordelijk zijn, moeten zij bijvoorbeeld onderling afstemmen wie de informatieplicht op zich neemt en wie een verzoek van betrokkene die een van zijn rechten uitoefent, afhandelt.[9] De AVG schrijft niet voor dat er afspraken over de verwerking van persoonsgegevens vastgelegd moeten worden in een overeenkomst, een 'regeling' is voldoende. Met het oog op de verantwoordingsplicht en het voorkomen van onduidelijkheid is het wel verstandig om in bijvoorbeeld de samenwerkingsovereenkomst de verplichtingen van beide partijen op te nemen.[10]

Zelfstandig verwerkingsverantwoordelijken
De laatste variant voor wat betreft de rolverdeling, is die waarbij twee organisaties zelfstandig verwerkingsverantwoordelijk zijn ten aanzien van de verwerking van persoonsgegevens. Ook nu weer gebruiken we het wervingsbureau als voorbeeld.

Een wervingsbureau verzamelt allerlei sollicitatiebrieven en CV's en slaat al deze gegevens op in haar eigen systeem. Mocht een bedrijf haar klantenservice willen uitbreiden, dan kan de HR-afdeling van dat bedrijf het wervingsbureau inschakelen. Het wervingsbureau zorgt bijvoorbeeld voor het werven, selecteren en screenen van kandidaten, maar test de kandidaten ook door ze bepaalde assessments voor te leggen. Vervolgens stelt het wervingsbureau een aantal geselecteerde kandidaten voor, zodat het bedrijf uiteindelijk kan bepalen wie wel of niet wordt aangenomen.

8. Artikel 26 AVG.
9. Hoofdstuk 3 AVG.
10. Artikel 5(2) AVG.

In deze situatie zijn zowel het wervingsbureau als het bedrijf zelfstandig verwerkingsverantwoordelijk voor het verwerken van persoonsgegevens. Het wervingsbureau is verantwoordelijk voor het gehele voorproces, men bepaalt hiervoor immers zelf het doel en de middelen bij het werven van kandidaten. Het wervingsbureau verzamelt alle sollicitatiebrieven en CV's, bewaart deze persoonsgegevens in een grote vergaarbak en plukt er een aantal uit die interessant zijn voor het bedrijf. Vervolgens is het bedrijf óók verwerkingsverantwoordelijke vanaf het moment dat kandidaten zijn voorgedragen en de sollicitatiegesprekken plaatsvinden en uiteindelijk wellicht een arbeidsovereenkomst wordt aangeboden.

Data-uitwisselingsovereenkomst

Ook wanneer partijen zelfstandig verwerkingsverantwoordelijken zijn, is het raadzaam om afspraken te maken over de verwerking van persoonsgegevens. Er worden immers persoonsgegevens uitgewisseld tussen partijen. Denk aan de hele batch van sollicitatiebrieven en CV's die vanuit het wervingsbureau aan de webshop wordt overhandigd. Als het wervingsbureau de persoonsgegevens niet-versleuteld verstuurt en het e-mailbericht wordt niet naar bedrijf A, maar per ongeluk naar bedrijf B verstuurd, dan heb je te maken met een datalek. Daarover wil je wel het een en ander geregeld hebben met de wederpartij.

Maak in een data-uitwisselingsovereenkomst afspraken over:

- welke persoonsgegevens verwerkt worden;
- welke verplichtingen partijen hebben;
- welke beveiligingsmaatregelen getroffen worden;
- wat er moet gebeuren in geval van een datalek;
- wat te doen als een betrokkene een van zijn rechten uitoefent.

Tips en tricks

Het bepalen van de juiste rolverdeling is makkelijker gezegd dan gedaan. Een eerste stap is om helder te hebben welke partij wat doet met de persoonsgegevens en waarom. Gebeurt het verwerken van persoonsgegevens in opdracht of niet? Hebben twee organisaties samen een lucratief idee bedacht om wat te gaan doen met persoonsgegevens? Zijn zij dan samen verantwoordelijk voor het geheel, of is ieder voor een deel zelfstandig verantwoordelijk? Vervolgens is het belangrijk om duidelijke afspraken op papier te zetten. Welke overeenkomst je dan nodig hebt, is weer afhankelijk van de rolverdeling.

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Contracteren

Preview: het Handboek ICT-contracten editie 2020

In februari 2020 verschijnt de geheel herziene derde editie van het Handboek ICT-contracten. Hieronder leest u een preview van hoofdstuk 2, over kwaliteit en prijsstructuren van contracten in de ICT sector.

De eerste en uiteindelijk belangrijkste aspecten van ieder contract, en dus ook ieder ICT-contract, zijn welke kwaliteit, product of dienstverlening men krijgt en wat dat moet kosten. Deze aspecten worden vaak gezien als een zuiver commerciële discussie, en dat is het natuurlijk ook. Maar wat veel juristen uit het oog verliezen, is dat de overige onderhandelpunten – al is het maar de scope van een bijzin in de overmachtsclausule – allemaal terug te herleiden zijn tot deze keuze. Alles is commercieel.

Resultaat, garanties en inspanningen

De belangrijkste keuze in een contractuele relatie is welke mate van kwaliteit men van de leverancier verwacht. De discussie spitst zich dan vaak toe op een keuze uit drie smaken:

1. Een inspanningsverbintenis, waarbij de leverancier zijn al dan niet gekwalificeerde best doet. De leverancier schiet dan pas te kort als bewezen wordt dat deze inspanning niet geleverd is.
2. Een resultaatsverbintenis, waarbij de leverancier het omschreven resultaat moet leveren en te kort geschoten is wanneer dat er niet is. Hoe hard of zacht daarvoor gelopen is, is niet relevant. Een beroep op overmacht (art. 6:75 BW) is echter wel mogelijk.
3. Een garantie, wat neerkomt op een resultaatsverbintenis waarbij een beroep op overmacht niet mogelijk is. Hiervan is eigenlijk alleen sprake wanneer de verbintenis expliciet het woord "garantie" of vervoeging daarvan bevat.

Een verbintenis kan gekoppeld zijn aan een termijn, bijvoorbeeld een levertijd of deadline. Dergelijke termijnen zijn in beginsel altijd resultaatsverbintenissen – fatale termijnen (art. 6:83 sub a BW). Slechts wanneer de termijn een "andere strekking" heeft dan een concreet levermoment aan te geven, kan dit een inspanningsverbintenis opleveren. Gewoonlijk vereist dit dat explicit termen zoals "gestreefd wordt naar verzending binnen 14 dagen" of "rond 25 mei" bij de termijn zijn opgenomen. Een termijn is echter slechts een garantie als dat er expliciet bij staat.

Voor de hand voor leverancier ligt om altijd inspanningsverbintenissen aan te gaan, en voor klanten om altijd enorme garanties te eisen. Ons inziens is dit te kort door de bocht: wanneer de gewenste verbintenissen meteen aan prijzen worden gekoppeld, ontstaat een veel helderder beeld van de situatie. Is de vraag om een garantie bijvoorbeeld werkelijk ingegeven door een interne dreigingsanalyse, of slechts een reflex om het onderste uit de kan te halen. Of omgekeerd: wil men geen resultaten leveren omdat dat niet haalbaar is voor de prijs, of slechts omdat men bang is voor theoretisch mogelijke claims?

Aan de resultaten gekoppeld is de aansprakelijkheid van de dienstverlener. In feite is immers de keuze voor de hardheid van het resultaat meteen een grens voor diens aansprakelijkheid bij fouten. Het is dus principieel onjuist om de aansprakelijkheid pas uit te onderhandelen nadat de resultaten en de prijs al vastgelegd zijn. Deze drie aspecten moeten tegelijkertijd worden onderhandeld.

Prijsstructuren

Direct gekoppeld aan de toegezegde resultaten is de keuze voor de vergoeding. Deze twee zijn in dusdanige mate verweven dat onderhandelen over de een nooit los mag staan van onderhandelen over de ander. Sterker nog, het onderwerp aansprakelijkheid is even onlosmakelijk verbonden met deze twee. Onderhan-

delen over deze aspecten kan dus alleen als alle drie tegelijk in de onderhandeling op tafel liggen.

Bovenstaande wil niet zeggen dat hoge kwaliteit automatisch moet leiden tot een hoge prijs. Een leverancier die een kwalitatief goede softwaredienst heeft ontwikkeld, kan deze prima voor een lage prijs per maand aanbieden bijvoorbeeld. En een dienstverlener kan een hoge prijs vragen voor een inspanningsplicht zonder aansprakelijkheid, maar met toezegging deze 24/7 beschikbaar te stellen.

Prijsstructuren bij dienstovereenkomsten
Er zijn in de praktijk vijf prijsstructuren die regelmatig worden gebruikt voor dienstovereenkomsten.

1. Uurtarief
2. Uurtarief met prijsplafond
3. Vaste prijs
4. Knipkaart
5. Bonus/malus

Het eenvoudigste model is het uurtarief. Hierbij meldt de leverancier vooraf het tarief dat per uur werk geldt, en wordt op week- of maandbasis een factuur gestuurd op basis van de daadwerkelijk gewerkte tijd. Tijden buiten kantoortijd kunnen met een toeslag (vaak 150% of 200%) worden gefactureerd. Het grootste nadeel van dit model is dat de klant geen voorafgaand zicht heeft op de kosten voor het werk.

Een uurtarief kan een prijsplafond ('cap') hebben. Wanneer het periodiek gefactureerde bedrag hoger zou zijn dan het plafond, wordt in plaats daarvan het plafond in rekening gebracht. Hiermee hoeft de klant nooit meer dan het plafond te verwachten, hetgeen het nadeel van het uurtarief-model tegemoet komt. Voor de leverancier is dit uiteraard minder aantrekkelijk, omdat hij mogelijk meer werk verzet dan hij betaald krijgt.

In plaats van een uurtarief kan een vaste prijs worden gehanteerd. De klant betaalt dan dat bedrag en niet meer – maar ook niet minder. Dit geeft veel zekerheid, ook voor de leverancier die nu kan rekenen op dit bedrag. Natuurlijk moeten beide partijen wel eerlijk kunnen inschatten of het bedrag reëel is voor het te verwachten werk. Daarnaast moet de scope van het werk nu grondig worden afgebakend, om te voorkomen dat achteraf allerlei ander werk gedaan moet worden onder de overeengekomen vaste prijs.

Bij een knipkaart of urenbundel betaalt de klant per uur, maar vooraf en met een korting (vaak 5% of 10%) omdat hij ineens betaalt voor zeg 20 of 40 uur. De leverancier registreert nog steeds alle gewerkte uren en stuurt daarvan een overzicht. De leverancier krijgt zo eerder zijn geld, de klant is goedkoper uit vanwege de korting.

Een bonus/malus structuur is een toevoeging op de andere modellen. Wanneer de eigenlijke prijs dan hoger of lager uitvalt dan gewoonlijk, delen beide partijen in het verschil. Komt de leverancier lager uit dan begroot, dan krijgt hij alsnog de helft van het verschil met de begrote hoeveelheid werk. Komt hij hoger uit, dan mag hij de helft van het verschil factureren. Dit geeft beide partijen een prikkel om een goede schatting te maken, maar zonder al te grote zorgen dat de begroting niet exact wordt gehaald.

Prijsstructuren bij softwarelicenties
Bij softwarelicenties wordt het meest gewerkt met de volgende structuren:

1. Vaste prijs per eenheid
2. Vaste prijs per eenheid per tijd
3. Totale vaste prijs (afkoop)
4. Royalties

Een vaste prijs per eenheid is het eenvoudigste model. Een eenheid is dan bijvoorbeeld een eindgebruiker, een computer, een afdeling of een rechtspersoon. Voor iedere eenheid die de software wil gebruiken, wordt dan de vaste prijs gehanteerd. Dit model geniet het voordeel van de eenvoud – op papier, want in de praktijk kunnen buitengewoon ondoorzichtige definities van 'eenheid' en bijbehorende prijsstructuren zorgen voor stevige discussies over de verschuldigde prijs.

Bij grotere getallen geldt vaak een volumekorting of wordt gewerkt met staffels: een lagere prijs wanneer meer dan 100 stuks worden afgenomen, nog lager boven 500 en de laagste prijs per stuk is bij 1000 stuks of meer ineens.

De vaste prijs is in principe eenmalig. Voor nieuwe versies wordt vaak wel een nieuwe vaste prijs bedongen. Dit maakt het van belang om het onderscheid tussen updates (inbegrepen in de prijs, of althans behorend bij deze versie) en upgrades (niet inbegrepen in de prijs, want effectief nieuwe versies) van groot belang.

In dit model is de kans groot dat de licentie als verkoop wordt gekwalificeerd, gezien de jurisprudentie van de Hoge Raad (Beeldbrigade) en Hof van Justitie (Usedsoft). In een business-to-business situatie betekent dit met name dat afspraken over kwaliteit en duur expliciet moeten worden gemaakt om te voorkomen dat de rechter wettelijke regelingen uit de kooptitel toepast.

Ook vaste prijs per eenheid per tijd komt vaak voor. De prijs is dan bijvoorbeeld per maand of per jaar verschuldigd, en kan daarmee periodiek worden gewijzigd. Wil de afnemer deze niet meer betalen, dan eindigt de licentie. Hiermee kan de licentie niet als koop worden aangemerkt.

Een licentienemer die in bovenstaande geen trek heeft, zal een totale vaste prijs oftewel afkoop bedingen. Hij betaalt dan eenmalig een bedrag en ontvangt een licentie. Meestal is deze voor onbepaalde tijd (en niet-opzegbaar) maar een afkoop voor een gegeven periode is ook mogelijk. Let op dat in dit model de licentienemer géén eigenaar van de auteursrechten wordt, maar nog steeds slechts een licentie geniet. In de praktijk wordt verwarrend genoeg wel gesproken van "afkoop auteursrecht" maar deze term is dus fout.

Een royalty is een licentievergoeding als percentage van de prijs die de afnemer hanteert. Dit model is vooral zinnig bij wederverkoop, omdat daar de prijs het directst vast te stellen is. De prijs kan zowel de bruto als netto prijs (voor of na aftrek van kosten) zijn. Grootste voordeel is dat de royalties meegroeien met de stijgende omzet.

Nadeel is dat de licentiegever een manier moet hebben om te verifiëren dat hij de juiste broncijfers krijgt om zijn royalties te bepalen. Een opgaaf van een (register-) accountant is een veelgebruikt middel om hierin tegemoet te komen.

Voor ongelicentieerd gebruik kan daarbij worden bepaald dat de licentienemer een vergoeding van drie maal de normale licentie verschuldigd zou zijn. Deze praktijk is wijdverbreid in de creatieve wereld van fotografie en tekstschrijvers. Een dergelijke contractuele boete lijkt dan ook in beginsel redelijk. Als toevoeging daarop kan worden bepaald dat een boekenonderzoek om schendingen vast te stellen, moet worden betaald door de licentienemer in geval van schending.

Prijsstructuren bij SaaS

De prijsstructuren bij SaaS lijken veel op die bij klassieke licenties. Het voornaamste verschil is dat vrijwel altijd met periodieke prijzen wordt gewerkt. Veel voorkomend zijn de volgende structuren:

1. Vaste prijs per eenheid per tijd
2. Totale vaste prijs (afkoop)
3. Aanschaf van credits

Over de vaste prijs per eenheid per tijd geldt wat hiernaast al is opgemerkt. De keuze voor de eenheid is veel ruimer: per gebruiker, per megabyte opslag, per minuut rekencapaciteit, per verzonden bericht, per ontvangen bericht, per geüploade afbeelding en ga zo maar door. Ook de tijdseenheid kan sterk variëren: per dag, per week en per maand zijn veel voorkomende keuzes.

De totale vaste prijs komt zelden voor maar is een optie voor grootzakelijk gebruik.

De aanschaf van credits is in feite een vaste prijs per eenheid waarbij vooraf wordt betaald, vaak met een staffelkorting (zie onder 'Prijsstructuren bij dienstovereenkomsten' hierboven). De credits zijn dan op hun beurt inzetbaar voor onderdelen dienstverlening, waarbij verschillende delen verschillende aantallen credits kosten. Dit model is met name populair bij SaaS diensten (en apps) gericht op consumenten, aangezien hiermee het feitelijk uitgeven van geld losgekoppeld wordt van de precieze prijs. Wie weet er halverwege zijn spelletje nog wat drie credits ook alweer kosten?

Geheel herzien:
Handboek ICT-contracten

Het handboek ICT-contracten is uitgebreid! Met een geheel herzien theoretisch deel en meer dan 40 relevante ICT-contracten, waaronder het hostingcontract, de verwerkersovereenkomst, het agile ontwikkelcontract, app licenties en de service level agreement.

€ 86,50

inclusief btw en verzendkosten

Voorintekenen kan vanaf nu!
ictrecht.nl/handboek-editie-2020

ICTRECHT
adviesbureau

Daniëlle van Ginkel
Juridisch adviseur
ICTRecht Groningen

Jorien Zwaneveld
Legal Assistant
ICTRecht Groningen

E-commerce Privacy

Een webshop hebben: makkelijk, toch?

De periode rond de jaarwisseling is vaak het moment om de zaken te evalueren. Waar willen we ons in het nieuwe jaar op richten? Hoe kunnen we de afzet vergroten? Kan het nog uit om deze producten te verkopen, of gaan we wat anders aanbieden? Misschien bent u van plan om een nieuwe webshop op te zetten of wilt u uw huidige webshop uitbreiden? Wij krijgen vaak de vraag welke juridische aspecten komen kijken bij het hebben van een webshop. In dit artikel nemen we u mee in de juridische webshopjungle.

Informatieplichten
Volgens de wet zijn er een aantal zaken waarover u een consument dient te informeren, voordat de consument een aankoop doet. Wij zien vaak in de praktijk dat webshops al deze informatie in hun algemene voorwaarden plaatsen. De algemene voorwaarden gelden echter niet als vindplaats van deze informatieplichten. Algemene voorwaarden worden overigens ook niet als gemakkelijk leesbaar beschouwd. Het is belangrijk dat de informatie op een makkelijk vindbare en logische plaats op de website te raadplegen is. Plaats de informatie bijvoorbeeld onder een duidelijk kopje in de footer, of op een klantenservicepagina. Wij hebben voor u de belangrijkste informatieplichten op een rijtje gezet.

Uw bedrijfsgegevens
Vermeld alle contact-/bedrijfsinformatie, waaronder de bedrijfsnaam en ondernemingsvorm, het KvK- en BTW-nummer, het vestigingsadres en contactgegevens zoals een e-mailadres en telefoonnummer.

Klachten en garantie
Ook over garantie dient geïnformeerd te worden. Dit kunt u doen door te beschrijven dat alle producten moeten voldoen aan de eisen die de consument er redelijkerwijs van mag verwachten. Daarnaast kunt u eigen garanties geven, bijvoorbeeld dat u instaat voor de kwaliteit van de producten voor vijf jaar. U kunt ook vermelden welke fabrieksgaranties op de producten van toepassing zijn. Belangrijk is dat u in ieder geval niet de wettelijke garantie beperkt met uw eigen verleende garantie.

Verder dient er op de website ook een klachtenprocedure vindbaar te zijn. In de klachtenprocedure staan onder andere de vragen: waar kan de klant terecht bij een klacht, en binnen welke termijn wordt deze klacht door u met de consument behandeld?

Herroepingsrecht
Een van de belangrijkste informatieplichten voor consumenten is het herroepingsrecht. Hoe kan een consument een product dat niet bevalt retourneren en binnen welke termijn moet de consument het product aan u terugzenden?

Wanneer de consument online producten bestelt, heeft de consument wettelijk een bedenktijd van minstens 14 dagen na ontvangst van de producten door de consument of een aangewezen derde (het herroepingsrecht). Een aangewezen derde kan bijvoorbeeld de buurman zijn. Kiest de consument in het bestelproces ervoor het pakketje bij de buren te laten bezorgen, dan begint de bedenktijd vanaf het moment dat de buren het pakket in ontvangst nemen. Het staat u uiteraard vrij om een langere bedenktijd aan te bieden dan de wettelijke 14 dagen, aangezien dit in het voordeel van de consument is. Voor diensten en abonnementen die online zijn afgesloten, zoals bijvoorbeeld Spotify, geldt dat de bedenktermijn ingaat op het moment dat de overeenkomst is afgesloten. Het is erg belangrijk dat u de consument goed informeert over de bedenktijd. Wanneer u de consument niet goed informeert, loopt u het risico dat de bedenktijd wordt verlengd tot een jaar.

Hoe zit het met de terugbetaling van geretourneerde producten?
Besluit de consument om de producten terug te sturen, dan dient u binnen 14 dagen nadat u op de hoogte bent gebracht van dit besluit, terug te betalen. Let erop dat wanneer de klant de gehele bestelling retourneert, ook de verzendkosten voor de heenzending en eventuele betaalkosten teruggestort moeten worden. U mag voor het terugstorten wel wachten totdat de producten door u zijn ontvangen of totdat de consument heeft aangetoond dat de producten zijn opgestuurd.

Zakelijke afnemers
Het wettelijke herroepingsrecht geldt echter niet voor zakelijke afnemers. Indien u niet wenst dat zakelijke afnemers gebruik maken van het herroepingsrecht, dan raden wij u aan om dit duidelijk te vermelden op uw website om verwarring te voorkomen.

Levering
Een andere belangrijke informatieplicht gaat over de levering van de producten (uitvoering van de overeenkomst). De wet geeft geen concrete eisen hoe er over levering geïnformeerd moet worden. Het gaat erom dat het voor de consument duidelijk is wat er gebeurt nadat de overeenkomst wordt gesloten. Bijvoorbeeld: wanneer kan de klant het pakketje ontvangen? Via welke vervoerder wordt het pakket verstuurd? Krijgt de klant een track&trace code?

Wat betreft de levertijden geldt dat het niet verplicht is om een levertijd te vermelden. Indien er geen levertijden op de website worden vermeld wordt u geacht om binnen 30 dagen te leveren. Heeft u op de website wel een levertijd staan, bijvoorbeeld '*Op werkdagen voor 13:00 uur besteld, morgen in huis*' dan dient u dit ook waar te maken. Indien de levering vervolgens uitblijft binnen de gestelde termijn, dan mag de consument de aankoop ongedaan maken.

Prijzen
Voor alle producten die u aanbiedt, moet het aanbod duidelijk zijn. Dit betekent onder andere dat de prijs van de producten voor consumenten inclusief btw getoond moet worden. Ook moet er duidelijk worden geïnformeerd over de hoogte van bijvoorbeeld de verzendkosten.

Nieuwsbrieven
Wilt u de consument een digitale nieuwsbrief sturen, dan dient u rekening te houden met regels omtrent de privacywetgeving. Vanwege deze privacywetgeving is het immers niet toegestaan om zomaar naar iedereen een nieuwsbrief te versturen.

Wanneer u in uw nieuwsbrief enige commerciële uitingen wilt doen, is de regel dat voor het versturen van de nieuwsbrief toestemming (opt-in) van de ontvanger is vereist. Deze informatie moet voor de ontvanger in begrijpelijke taal zijn opgesteld. Verder dient de toestemming 'vrij, specifiek, geïnformeerd en ondubbelzinnig' te zijn. U dient dus bij het versturen van een digitale nieuwsbrief in de toestemmingsvraag de volgende informatie te verwerken:
- namens wie wordt de nieuwsbrief verzonden (bijvoorbeeld ICTRecht);
- hoe vaak wordt de nieuwsbrief verstuurd (bijvoorbeeld 1x per week);
- wat is de inhoud van de nieuwsbrief en voor welk doel wordt deze verstuurd (denk bijvoorbeeld aan het sturen van aanbiedingen);
- op welke manier wordt de nieuwsbrief verzonden (per e-mail of per post).

Het moet voor de ontvanger daarnaast duidelijk zijn waar hij terecht kan voor meer informatie. Denk hierbij bijvoorbeeld aan het opnemen van een verwijzing/link naar de privacyverklaring.

Let op dat voor de opt-in een actieve handeling moet plaatsvinden door degene die de opt-in geeft. Vooraf aangevinkte hokjes voldoen dus niet aan het vereiste van toestemming.

Uitzondering voor klanten
U hoeft geen uitdrukkelijke toestemming van de consument te verkrijgen voor het versturen van de digitale nieuwsbrief als u aan de volgende vereisten voldoet:
- de consument heeft eerder een product of dienst bij u gekocht (let op: er moet dus voor betaald zijn);
- de nieuwsbrief ziet alleen op producten en/of diensten die soortgelijk zijn aan wat de klant heeft gekocht;
- de consument is duidelijk op de hoogte gebracht dat hij na aankoop van het product/de dienst een nieuwsbrief gaat ontvangen;
- de consument heeft nog vóór het moment van aankoop de mogelijkheid gehad om zich te verzetten (opt-out) tegen het ontvangen van die nieuwsbrief. Dit kan eenvoudig gedaan worden door tijdens een bestelproces een checkbox voor het ontvangen van de nieuwsbrief al aangevinkt te tonen, waarbij de klant deze wel zelf kan uitvinken.

Wilt u commerciële nieuwsbrieven versturen, let er dan op wie de ontvanger is en of u hiermee een bestaande klantrelatie heeft.

Kim Groot
Juridisch adviseur

Cloud Overheid

Nieuwe uitspraak Hof van Justitie verduidelijkt de verantwoordelijkheid van hostingpartijen voor effectieve aanpak van onrechtmatige informatie

In een recente uitspraak heeft het Hof van Justitie (hierna: “het Hof”) extra duidelijkheid gegeven over de verantwoordelijkheid van hostingpartijen, in casu Facebook, met betrekking tot verwijdering van onrechtmatige informatie. Het Hof geeft hiermee een nadere uitleg over de reikwijdte van de bepalingen over hostingdienstaanbieders in de ‘Richtlijn inzake elektronische handel (2000/31)’ (hierna: “richtlijn”). De richtlijn voorziet onder andere in de mogelijkheid om een hostingpartij -middels een gerechtelijk bevel- de verplichting op te leggen om onrechtmatige informatie, zoals een lasterlijk bericht, te verwijderen. Om dit soort berichten effectief aan te kunnen pakken mag een dergelijk gebod eveneens gelden voor alle inhoudelijk overeenstemmende informatie, aldus het Hof. In dit artikel bespreken we wat er door deze uitspraak precies verandert en wat dit betekent voor de aansprakelijkheid van hostingdienstaanbieders voor de content van hun gebruikers.

De zaak

Op 3 oktober 2019 heeft het Hof prejudiciële vragen beantwoord van een Oostenrijkse rechter, met betrekking tot een geschil tussen het platform Facebook en politica Eva Glawischnig-Piesczek. Aanleiding was een bericht met lasterlijke inhoud op Facebook over mevrouw Glawischnig-Piesczek, waarna zij Facebook heeft aangesproken het bericht te verwijderen. Daarnaast verzocht zij dit ook voor alle voortbouwende lasterlijke berichten, zoals gedeelde versies van het oorspronkelijke bericht en berichten met vergelijkbare inhoud. Omdat Facebook geen (volledig) gehoor gaf aan dit verzoek, kwam de zaak uiteindelijk bij de rechter in Wenen terecht. De prejudiciële vragen zagen op de interpretatie en reikwijdte van artikel 15 van de richtlijn en daarmee ook de potentiele reikwijdte van een het potentieel verbod tot verwijdering.

Aansprakelijkheid hostingdienstaanbieders

De artikelen 12 tot en met 15 van de richtlijn bevatten regels over aansprakelijkheid van tussenpersonen, waaronder hostingdienstaanbieders. Op basis hiervan is het uitgangspunt dat een hostingsdienstaanbieder in beginsel niet aansprakelijk is voor content en informatie welke door gebruikers geplaatst is. Dit is natuurlijk ook niet zo vreemd: wanneer deze dienstaanbieders immers aansprakelijk zouden zijn voor alle content en informatie in de dienst zou dit een groot risico meebrengen voor de dienstaanbieders waardoor deze gedwongen zouden zijn om alle informatie te filteren

op mogelijk onrechtmatige informatie. Dat is onbegonnen werk en leidt tevens tot problemen in het kader van de vrijheid van meningsuiting. Door eventuele filter- en censuurtechnieken zouden gebruikers waarschijnlijk behoorlijk beperkt worden in wat zij op deze diensten kunnen plaatsen. Het is daarom voor zowel gebruikers en hostingdienstaanbieders prettig dat gebruikers zelf verantwoordelijk zijn voor berichten en content die zij op deze diensten plaatsen.

Op het voorgaande geldt echter wel een uitzondering. Artikel 14 lid 1 van de richtlijn bepaalt dat de hostingdienstaanbieder, om voor de aansprakelijkheidsuitsluiting in aanmerking te komen, snel moet handelen zodra hij kennis heeft van onrechtmatige activiteiten, bijvoorbeeld door de informatie te verwijderen of ontoegankelijk te maken. Doet hij dit niet, dan kan de aanbieder geen beroep meer doen op de wettelijke uitsluiting van aansprakelijkheid.

De effectieve aanpak van onrechtmatige informatie
Tot voor kort was de algemene aanname dat een dergelijke *notice-and-take-down* verplichting enkel zag op de specifieke onrechtmatig verklaarde berichten. Voor nieuwe berichten zou dan telkens een nieuwe kennisgeving door het slachtoffer nodig zijn. De Weense rechter die het geschil behandelde had hier zijn twijfels bij en stelde aan het Hof de vraag of artikel 15 van de richtlijn in de weg stond aan een gerechtelijk gebod tot wereldwijde verwijdering van onrechtmatige publicaties jegens een hostingdienstaanbieder. Ook vroeg de rechter zich af of een dergelijk gebod betrekking mag hebben op alle informatie en publicaties die identiek zijn aan, of inhoudelijk overeenstemmen met de oorspronkelijke informatie. Hiermee zou een *notice-and-take-down* per bericht, kunnen verschuiven van een algehele *notice-and-stay-down* van de informatie in het betreffende bericht.

Het Hof gaf aan dat de relevante regels uit de richtlijn uitdrukkelijk tot doel hebben elke inbreuk te doen eindigen of elke verdere aantasting van de betrokken belangen te verhinderen, zodat de reikwijdte van die maatregelen in beginsel niet beperkt is. Door niet slechts het originele onrechtmatige bericht op het Facebook platform te verwijderen, maar tevens alle identieke berichten en de inhoudelijk overeenstemmende berichten, met vergelijkbare informatie en inhoud als het origineel, te verwijderen kan dus een daadwerkelijk effectieve aanpak plaatsvinden. De gevolgen van een gerechtelijk bevel zouden anders gemakkelijk te omzeilen zijn door het plaatsen van berichten die nauwelijks verschillen van berichten die eerder onrechtmatig verklaard zijn.

Identieke en inhoudelijk overeenstemmende informatie?
Volgens het Hof mag een gebod tot verwijdering van onrechtmatige informatie dus ook zien op identieke informatie en inhoudelijk overeenstemmende informatie. Hoe moet dit gezien worden in de context van een platform als Facebook?

Met identieke informatie worden de berichten bedoeld met een identieke inhoud, maar geplaatst door een andere gebruiker, zoals de gedeelde versies van het oorspronkelijke bericht. Met inhoudelijk overeenstemmende informatie worden berichten bedoeld welke dezelfde informatie bevatten als het originele onrechtmatige bericht, maar welke anders geformuleerd kunnen zijn, dan wel toevoegingen en onvolledigheden kunnen bevatten.

Om vast te kunnen stellen of een bericht in voldoende mate inhoudelijk overstemt dient het bericht volgens het Hof: “Specifieke gegevens te bevatten, zoals de naam van de persoon op wie de eerder vastgestelde

inbreuk betrekking had, de omstandigheden waarin deze inbreuk is vastgesteld en een inhoud die overeenstemt met de eerder onrechtmatig verklaarde inhoud." De rechtbank moet dan in het bevel aangeven welke specifieke informatie offline gehouden moet worden.

Geen actieve zoekverplichting

Voor de duidelijkheid benadrukt het Hof in haar arrest nog wel meermaals dat er voor de hostingdienstaanbieders geen actieve zoekverplichting naar onrechtmatige informatie bestaat. Dit zou een excessieve verplichting voor de dienstaanbieder meebrengen. Dit is ook niet meer dan logisch, nu een dergelijke autonome scanplicht precies die situatie zou meebrengen waar niemand op zit te wachten, namelijk de situatie waarin hostingaanbieders content binnen hun dienst actief gaan monitoren. Doordat een bevel echter specifieke gegevens moet bevatten, is er geen algemene toezichtverplichting, maar een specifieke. Hierdoor is dit volgens het Hof niet in strijd met de regels van de richtlijn.

Wereldwijde gevolgen

De reikwijdte van een gebod tot verwijdering mag volgens het Hof dus behoorlijk breed zijn, juist omdat dit in bepaalde gevallen nodig is om een inbreuk ook daadwerkelijk te beëindigen. Opvallend is dat het Hof aangeeft dat uitleg van de richtlijn geen territoriale beperking tot gevolg heeft en er dan ook niet voor in de weg staat dat de middels een bevel genomen maatregelen wereldwijde gevolgen kunnen hebben. Dit betekent dat wanneer een beperkte ontoegankelijkmaking van informatie binnen een bepaald gebied niet voldoende is voor het beëindigen van een inbreuk, een bevel ook een wereldwijde werking mag hebben.

Impact uitspraak

Met deze uitspraak bepaalt het Hof dus dat er geen Europese regels zijn die zich verzetten tegen een bevel om ook de met onrechtmatige informatie overeenstemmende berichten te verwijderen. Voor de hostingdienstaanbieders als Facebook is voortaan dan ook het uitgangspunt dat zij, ondanks dat er geen actieve zoekverplichting is, er een actievere houding en aanpak geëist kunnen worden. Voor slachtoffers neemt dit de noodzaak weg om herhaaldelijk naar de rechtbank te moeten voor nieuwe vergelijkbare berichten, en is daarmee een grondslag voor het zogenaamde *'notice-and-stay-down'.*

De vraag is echter wat de gevolgen van deze uitspraak zullen zijn voor platformgebruikers en de vrijheid van meningsuiting nu de norm van 'inhoudelijk overeenstemmende informatie' vrij open is. Mogelijk kan dit zelfs leiden tot censuurmaatregelen. Voor nu is het dus nog even afwachten hoe dit soort bevelen door partijen als Facebook in de praktijk tot uitvoering gebracht zullen worden.

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Internetrechtspraak

Rechtbank Den Haag 8 mei 2018
(Auteursrechtinbreuk werknemer)
(Gepubliceerd 10 oktober 2019) Een werknemer heeft gebruik gemaakt van data, modellen en tools waarop het auteursrecht van een derde rust zonder dat werkgever dit wist. Werkgever verzoekt daarom ontbinding van de arbeidsovereenkomst (art. 7:686 BW jo. 6:265 BW). Dit wordt afgewezen. Weliswaar was sprake van auteursrechtinbreuk, maar de rechthebbende heeft zich welwillend opgesteld zodat dit met een sisser is afgelopen. Ook heeft de werkgever zich vanaf het begin hard opgesteld, door van alles te sommeren en eisen in plaats van met de werknemer in overleg te gaan.

https://bit.ly/2DMG3Hn

Rechtbank Rotterdam 22 augustus 2019
(Bewijsbeslag in ICT)
Softwarebedrijf JDK verzoekt conservatoir bewijsbeslag te leggen bij de Haven Rotterdam, wegens schending van een licentieovereenkomst tussen de Haven en JDK. De Haven zou in strijd met de licentie gegevens uit een softwareapplicatie delen met haar dochterbedrijf. Aan de stelplicht van degene die verlof vraagt om bewijsbeslag te leggen, moeten hoge eisen worden gesteld (ECLI:NL:HR:2013:BZ9958). De verzoeker dient zijn belang bij de beslaglegging voldoende aannemelijk te maken, alsmede feiten en omstandigheden waaruit volgt dat de beslaglegging met het oog daarop noodzakelijk is. Daarop gaat het mis voor JDK: bewijsbeslag op alle gegevensdragers van de Haven zou een ernstige belemmering van het functioneren van het havenbedrijf kunnen opleveren. Er zijn ook alternatieven, zoals het horen van medewerkers – dit zijn semi-ambtenaren zodat hun verklaring onder ede in beginsel betrouwbaar genoeg zou moeten zijn.

https://bit.ly/33MNCZg

Rechtbank Rotterdam 10 september 2019
(Infecteren met malware)
De 22-jarige verdachte heeft zich maandenlang schuldig gemaakt aan het op grote schaal infecteren van computers van derden met malware, waardoor hij deze computers kon overnemen. Met achterhaalde inloggegevens heeft hij ingelogd op online accounts van die derden. Hij heeft bestellingen geplaatst, simkaartwissels aangevraagd en bedragen overgeboekt.

https://bit.ly/2qjL8nj

Rechtbank Noord-Nederland 10 september 2019
(Foto-inbreuk op internet)
Een adviseur publiceert op zijn site een foto die eigendom is van fotobureau Hollandse Hoogte. Deze spreekt hem aan op auteursrechtinbreuk voor €855, wat de adviseur weigert te betalen. De rechtbank stelt eenvoudig vast dat er sprake is van inbreuk. Voor de schade volgt de rechtbank de Tarievenlijst van Foto Anoniem en komt uit bij €248,25 als licentievergoeding (waar HH 500 euro rekende) en het liquidatietarief vanwege het zeer eenvoudige karakter van de zaak.

https://bit.ly/2MniCsl

Raad van State 11 september 2019
(Stuk in archief niet openbaar)
Een burger vraagt onder de Wet openbaarheid van bestuur informatie op. De gemeente weigert dit, omdat de informatie al openbaar zou zijn: deze kan worden opgevraagd bij het archief, aan de balie of via het internet. De burger accepteert dat niet, omdat hij niet via internet kan werken en verstrekking aan de balie afhankelijk is van de medewerker en bovendien soms wel, soms niet leges vereist worden. Dat is niet 'openbaar' in de zin van de Wob. De RvS is het daarmee eens. Er is geen onbeperkte toegang via internet. Aan de balie worden verzoeken gescreend, men mag niet zelf zoeken in archiefstukken en documenten worden vooraf op AVG-schending getoetst. Ook is in beginsel altijd leges verschuldigd bij een opvraging. Dat is geen openbaarheid van informatie.

https://bit.ly/366vSJT

Gerechtshof Arnhem-Leeuwarden 17 september 2019
(Zorgplicht DDoS-aanval)
Een bedrijf koopt hostingdiensten in voor haar websites en (hosting/reseller)-diensten, en krijgt vervolgens te maken met een DDoS-aanval van derden. De kosten van het daarmee gepaard gaande dataverkeer worden haar in rekening gebracht, wat zij weigert te betalen. De algemene voorwaarden van de hostingleverancier vermelden geen bijzondere zorgplicht tegen DDoS-aanvallen, en de klant is gezien haar eigen dienstverlening kundig genoeg zichzelf te wapenen tegen dergelijke misdrijven. Ook een beroep op overmacht gaat niet op, om diezelfde reden. De klant moet dan ook betalen.

https://bit.ly/34Q4Ztt

Rechtbank Limburg 17 september 2019
(Doorzoeken mailboxen werknemers)
Sinds medio 2011 overlegt Maastricht met de gemeenten Heerlen en Sittard-Geleen over een op te zetten *shared service centre*. De OR maakt bezwaar tegen overheveling van ambtenaren naar dit SSC en stelt zich daarbij hard op, wat wethouders als extreem ervaren. In de daarop volgende escalatie blijkt het SSC in conceptnotulen brisante stappen tegen OR medewerkers te hebben voorgesteld – wat in de finale notulen weggelaten is. Deze concepttekst komt bij OR-medewerkers terecht, waarop de gemeente een integriteitsonderzoek start om te achterhalen wie er zijn of haar ambtsgeheim heeft geschonden. Daarbij worden mailboxen van alle OR-leden doorzocht. De rechtbank oordeelt dat de gemeente gezien deze situatie een zwaarwegend belang had voor de doorzoeking. Echter, de gemeente wachtte zes weken na interne ontdekking, en dat is te lang. Zeker met de motivatie dat men alsnog ging onderzoeken "omdat het maar niet ophield" met het extreme gedrag, en vervolgens zo ongeveer alle OR leden werden onderzocht, terwijl er geen directe reden was te vermoeden dat de OR-leden dit document direct per mail toegespeeld had gekregen. Dit wekt de indruk dat het onderzoek ingesteld is als represaille en niet om een daadwerkelijke wetsovertreding of plichtsverzuim aan te pakken.

https://bit.ly/2PdIdpW

Hof van Justitie van de EU 24 september 2019
(Vergeetrecht Google is Europees)
Wanneer Google zoekresultaten voor een persoon verbergt ("het vergeetrecht") beperkt zij dit effect tot zoekopdrachten vanuit Europa. Eerst door naar de extensie van de zoekdienst te kijken (dus wel bij .nl maar niet bij .com) en later door het IP-adres van de bezoeker te controleren. De Franse toezichthouder oordeelt dat dit in strijd is met de AVG, omdat het vergeeteffect te beperkt is. Het Hof oordeelt anders: bij invoering van de AVG heeft de Europese wetgever het niet aangedurfd om een wereldwijd vergeetrecht in te voeren. Daarom bestaat een dergelijk recht op dit moment niet. Google moet wel effectieve maatregelen (blijven) nemen om te zorgen dat Europese zoekers de 'vergeten' zoekresultaten niet te zien krijgen.

https://curia.europa.eu, zaaknr. C-507/17

Hoge Raad 24 september 2019
(Op YouTube, althans op internet)
Een rapper plaatst een video op YouTube waarin hij een clip verwerkt waarin twee agenten hem aanspreken. De teksten die daar overheen worden gezegd, leiden tot vervolging wegens belediging. In de tenlastelegging wordt de rapper de belediging verweten door de handeling van het plaatsen. De Hoge Raad oordeelt dat dit onjuist is, een plaatsingshandeling is op zichzelf niet genoeg om van belediging te spreken. Terugverwijzing.

https://bit.ly/2Lnb8FM

Hof van Justitie van de EU 1 oktober 2019
(Vooraf aanvinken is geen toestemming)
Het Duitse bedrijf Planet49 organiseert een loterij waarbij deelnemers zich moeten aanmelden en dan toestemming moeten geven voor een mailing en voor analytics door een zelfstandig opererende derde. Het vinkje voor de laatste stond reeds aan. Het Hof concludeert dat een dergelijke vorm van toestemming vragen in strijd is met de Privacyrichtlijn. En de AVG, nu deze minstens zo streng is over toestemming en bovendien letterlijk vermeld dat "stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit" niet als toestemming mogen gelden. Dit geldt ook bij cookies en dergelijke zaken die onder de E-Privacyrichtlijn worden geplaatst op randapparatuur terwijl daar geen

verwerking van persoonsgegevens plaatsvindt. Zie de noot op pagina 36.

https://bit.ly/2LRzec6

Hof van Justitie van de EU 3 oktober 2019
(Geen bezwaar tegen wereldwijde takedown)
Een Oostenrijkse politicus constateert dat tegen haar smadelijke uitspraken op Facebook worden gedaan. Zij eist verwijdering en verwijderd houden (*notice and stay down*) van deze uitspraken, nadat de rechter had vastgesteld dat de eerste uitspraak smadelijk is. Facebook maakt bezwaar, onder meer omdat ook "overeenstemmende uitingen" moeten worden verwijderd en zo'n verwijdering wereldwijd effect zou hebben in plaats van uitsluitend in Oostenrijk. Het Hof oordeelt in prejudiciële vragen dat Europese regels (zoals de E-commercerichtlijn) niet in de weg staat aan een dergelijke eis. Nationaal recht bepaalt of en in hoeverre een wereldwijd effect opgelegd kan worden. Zie het artikel op pagina 24.

https://bit.ly/2Qj5l0i

Gerechtshof Arnhem-Leeuwarden 8 oktober 2019
(NEN normen ter inzage)
De gemeente Almere maakt de Legesverordening 2016 bekend, en verwijst daarin naar NEN norm 2580 als vereiste om te bepalen hoe oppervlakte en inhoud van te bouwen objecten moeten worden bepaald. In zo'n geval moet die NEN norm gepubliceerd worden conform artikel 139 Gemeentewet, wat inhoudt het gemeenteblad, het Staatsblad of de website van de gemeente. Dat is hier niet gebeurd; dat de norm ter inzage lag en verkregen had kunnen worden, doet daaraan niet af.

https://bit.ly/34QHa4u

Rechtbank Gelderland 9 oktober 2019
(Foto-auteursrecht)
Een bedrijf publiceert op haar website een foto waar het ANP auteursrecht op heeft. Geëist wordt de licentievergoeding conform de tarievenlijst van Foto Anoniem, waar de rechter in meegaat. De eveneens geëiste opslag van 50% wordt afgewezen, omdat dit een punitief element zou toevoegen dat het Nederlands schadevergoedingsrecht niet kent. Wel worden ruim €800 aan proceskosten toegewezen.

https://bit.ly/2PcaX15

Rechtbank Rotterdam 11 oktober 2019
(Voorbereiden terrorisme)
De Hoge Raad heeft geoordeeld (ECLI:NL:HR:2017:416 en ECLI:NL:HR:2019:906) dat het voldoende is om tot een bewezenverklaring van voorbereiding of bevordering van terroristische misdrijven te komen, indien het oogmerk van de verdachte op het begaan van die misdrijven is gericht. Een concretisering van het voor te bereiden of te bevorderen misdrijf naar tijdstip, plaats en wijze van uitvoering is niet vereist. Hier is van belang dat artikel 134a Sr, kort gezegd, strafbaar stelt aan het deelnemen en meewerken aan training voor terrorisme. Onder de reikwijdte van artikel 134a Sr valt ook de eenling die zich via internet op de hoogte stelt van kennis en informatie over het vervaardigen van een explosief die hij vervolgens wil inzetten voor het plegen van een terroristisch misdrijf of het vergemakkelijken ervan.

https://bit.ly/387CrxC

Gerechtshof Arnhem-Leeuwarden 15 oktober 2019
(Annulering zakelijke overeenkomst)
Na verstrijken van de overeengekomen bedenktermijn van drie dagen beëindigt een kleine ondernemer alsnog de kort voordien aangegane advertentieovereenkomst. Advertentiebedrijf maakt daarop aanspraak op annuleringsvergoeding ter grootte van 40% van de nog resterende termijnen. Geen reflexwerking van de voor consumenten beschermende bepalingen waardoor niet de in artikel 6:230o BW bedoelde bedenktermijn van 14 dagen van toepassing is. De contractuele bepalingen over de duur van de bedenktermijn en de annuleringsvergoeding zijn evenmin onredelijk bezwarend. Aangezien het advertentiebedrijf nog niets voor de ondernemer had gedaan, is het maatstaven van redelijkheid en billijkheid wel onaanvaardbaar dat het bedrijf aanspraak maakt op de volledige annuleringsvergoeding. Deze vergoeding wordt beperkt tot € 500,- welk bedrag al door de ondernemer ter compensatie is betaald.

https://bit.ly/383uk53

Rechtbank Amsterdam 16 oktober 2019
(Exoneratie in ICT contract)
Succesvol beroep op overeengekomen aansprakelijkheidsbeperking. Leaseweb verwijst naar de 'Nederland ICT Voorwaarden' en voert aan dat het in de dienstverlenende ICT-branche algemeen aanvaard is dat een ICT-leverancier zijn aansprakelijkheid voor directe schade beperkt door een aansprakelijkheidslimiet en zijn aansprakelijkheid voor indirecte schade uitsluit. Het exoneratiebeding moet, volgens Leaseweb, in overeenstemming met deze norm worden uitgelegd en was ook de bedoeling van partijen. Deze uitleg wordt gevolgd. Er wordt als volgt overwogen: i) Ctac heeft onvoldoende gemotiveerd betwist dat een dergelijke wijze van exonereren gebruikelijk is in de dienstverlenende ICT-branche. ii) de totstandkoming van het exoneratiebeding wijst op de juistheid van zo'n uitleg. iii) Het volgen van de uitleg van Ctac zou de beperking in lid 2 van het exoneratiebeding nagenoeg betekenisloos maken. iv) Ctac heeft haar stelling, dat een volledige uitsluiting van vermogensschade is ingeprijsd gelet op haar zeer scherpe prijs, onvoldoende toegelicht en onderbouwd.

https://bit.ly/34NfuO0

Rechtbank Midden-Nederland 25 oktober 2019
(Zwarte lijst artsen)
SIN-NL is een stichting die zich inzet om de positie van slachtoffers van medische fouten of hun nabestaanden en de patiëntveiligheid en kwaliteit van de gezondheidszorg te verbeteren. Op haar website worden zwarte lijsten met artsen en anderen gepubliceerd die dergelijke fouten zouden maken of verdoezelen. Daar verschijnt nu ook een artikel over een officier van justitie, die tekort zou zijn geschoten in een medische strafzaak. De rechtbank constateert dat de uitingen over de officier allen feitelijk onjuist zijn en daarmee geen daadwerkelijke misstand betreffen. De uitingen zijn onrechtmatig. Tevens wordt de zwarte lijst in strijd met de AVG geacht, helaas zonder argumentatie, en is de foto van de officier in strijd met het portretrecht gepubliceerd.

https://bit.ly/33MQhSK

Rechtbank Amsterdam 4 november 2019
(Bankrekening cannabiswinkel)
ABN Amro bank moet een bankrekening verschaffen aan een cannabisteler die wil meedoen aan het Experiment gesloten cannabisketen. De bank had dit eerder geweigerd omdat de cannabisteler onderdeel uitmaakt van een integriteitsgevoelige sector en er daarom een risico bestaat op witwassen, en zich daarbij beroepen op haar contractsvrijheid. Echter, omdat de ABN een nutsbank is, is deze niet onbeperkt. Wanneer de argumenten over integriteit uitsluitend algemeenheden betreffen, is dat niet genoeg om de aanvraag te mogen weigeren gezien het feit de teler uitsluitend van plan is legale activiteiten te ontplooien onder de te verwachten nieuwe wetgeving in 2020. Genoemd wegens relevantie voor blockchain- en bitcoinondernemingen, die met exact dezelfde redenering worden afgewezen bij banken.

https://bit.ly/2ONqV2x

Centrale Raad van Beroep 5 november 2019
(Persoonsgegevens Marktplaats)
De sociale recherche stelt een onderzoek in naar de bijstandsuitkering van een persoon na een tip over handel in gestolen goederen. Daarbij worden ook gegevens van Marktplaats BV opgevraagd. Nadat de sociale recherche de namen, de adressen, de geboortedata en de telefoonnummers van appellanten en hun kinderen had verstuurd, heeft Marktplaats de informatie over de advertenties verstrekt. Appellanten vinden dat de op deze manier ingewonnen informatie onrechtmatig is verkregen en niet als bewijs kan worden toegelaten. De rechtbank ziet dit anders. Het opvragen van die gegevens om vast te stellen of appellanten recht hadden op bijstand kan worden gezien als het behartigen van het belang van het economisch welzijn van Nederland, waaronder het tegengaan van misbruik en fraude van sociale uitkeringen. Dit doel is gerechtvaardigd. De anonieme meldingen, de onregelmatigheden op de ingeleverde bankafschriften en de afschrijving naar Marktplaats waren een toereikende aanleiding om de gevraagde gegevens bij Marktplaats op te vragen. Het opvragen van de gegevens voldoet ook aan de vereisten van proportionaliteit en subsidiariteit.

Het staat in redelijke verhouding tot de daarmee gemaakte inbreuk op de privacy van appellant en in de gegeven omstandigheden was er niet een voor appellanten minder ingrijpende manier om een goed inzicht te krijgen in de activiteiten van appellant op Marktplaats.

https://bit.ly/2PpJtW3

Rechtbank Rotterdam 6 november 2019
(Meebieden door verkoper)
Bij een internetveiling blijkt de verkoper mee te bieden en uiteindelijk het hoogste bod te hebben geboden. De veilingorganisatie wijst het verkochte nu toe aan de enahoogste bieder, die dit weigert omdat hij het ziet als manipulatie van de veiling, hoewel de algemene voorwaarden het toestaan. De rechtbank verklaart deze voorwaarde niet toepasbaar in deze situatie, omdat het tot een uitkomst in strijd met de redelijkheid en billijkheid zou leiden.

https://bit.ly/2qgtP6y

Rechtbank Amsterdam 11 november 2019
(Nep-Facebookadvertenties John de Mol)
Met regelmaat duiken op Facebook advertenties op waarin BN-ers als John de Mol zogenaamd zouden stoppen met hun werk omdat zij rijk zijn geworden door bitcoinspeculatie. De Mol eist bij de rechter dat Facebook deze advertenties tegenhoudt, wat Facebook zegt niet te kunnen behalve in individuele gevallen en op klacht. (In de aanloop naar de rechtszaak blijken de advertenties met De Mol erin niet meer op te duiken.) Facebook stelt met name een neutrale tussenpersoon te zijn, die niet aansprakelijk is voor gepubliceerde advertenties en daar ook geen actieve monitoring rol in hoeft te nemen. De rechtbank verwerpt dit verweer. Facebook is zozeer betrokken bij het verwerken en doorgeven van advertenties dat zij geen tussenpersoon te noemen is. Daarom moet zij maatregelen nemen, zeker bij deze evident onrechtmatige advertenties. Welke maatregelen dat zijn, is het probleem van Facebook, maar de maatregelen moeten in beginsel al deze nepadvertenties (met De Mol erin) tegenhouden.

https://bit.ly/2DKUWtJ

Jorden Bailey
Juridisch adviseur

Jay Remmelzwaal
Juridisch adviseur

Privacy

Privacy Verified: verander wetgeving in een strategisch wapen

Het voldoen aan de AVG een te grote horde? Niet als het aan ICTRecht ligt! Middels de dienst Privacy Verified helpen wij organisaties om privacy in te zetten als een belangrijke commerciële toegevoegde waarde. Met Privacy Verified bieden wij aan organisaties de kans om privacy op een structurele basis op te pakken en kopzorgen op dit vlak weg te nemen. Hoe wij dit doen? Wij praten u graag bij!

De AVG is zo verkeerd nog niet!
Ook met het aanbreken van een nieuw jaar is een groot aandeel van de organisaties in Europa nog druk bezig met het implementeren van de regels uit deze Europese verordening. En dat terwijl de kerstman in de tussentijd al tweemaal is langs geweest. Hoe komt dit toch, zien wij u denken?

Gedeeltelijk valt dit toe te schrijven aan de consensus die heerst ten aanzien van dit stukje wetgeving uit Europa. Er bestaat namelijk een beeld van de AVG als 'een blok aan het been,' 'wetgeving dat van alles en nog wat verbiedt, en innovatieve ideeën in de weg staat.' Daarbij is de kreet: "Dat zal wel niet mogen van de AVG" een veelgehoorde uitspraak. Wat ons betreft klopt deze uitspraak niet. Sterker nog: de AVG laat stiekem best veel toe. De sleutel naar deze kansen ligt voor een groot gedeelte in het goed kunnen verantwoorden wat u met persoonsgegevens doet en waarom u dit doet.

De AVG in een notendop
Concreet bestaat de bovenstaande verantwoordingsplicht uit twee belangrijke onderdelen. Allereerst dient u voor uzelf op een rijtje te zetten wat u als organisatie met de gegevens van bijvoorbeeld uw klanten, medewerkers en leveranciers wil en welk doel u met de gegevens hebt. Stap twee is het vertalen van deze informatie in een duidelijk verhaal richting deze groep betrokkenen. Voor hen dient duidelijk te zijn waarom hun persoonsgegevens verwerkt worden en welk doel deze verwerking(en) dient. Wees verder eerlijk en open in wat u doet met de persoonsgegevens. Leg dat netjes uit in een privacyverklaring en documenteer dat in een verwerkingsregister.

Om vervolgens ook echt wat met persoonsgegevens te mogen doen dient u wel aan een aantal voorwaarden te voldoen. Allereerst zult u een grond moeten hebben uit de wet om van start te kunnen gaan met de verwerking van persoonsgegevens; een passende grondslag zoals dat zo mooi heet. Bij zo'n grondslag kunt u denken aan het welbekende uitvragen van toestemming, of het baseren van de verwerking op een gerechtvaardigd belang dat u als organisatie hebt. Als dat helder is, bepaalt u welke persoonsgegevens u nodig hebt om dat doel te bereiken.

Om aan te kunnen tonen dat u de bovenstaande regels volgt en daarnaast voldoet aan eventuele andere toepasselijke voorwaarden uit de AVG heeft ICTRecht, Privacy Verified ontwikkeld. Een transparante en onafhankelijke toetsing, waarbij wij verifiëren of uw dienst, product, applicatie, of voltallige organisatie in lijn met de AVG handelt. Met ons certificeringsprogramma wordt privacy in drie heldere stappen een onderscheidende propositie van uw organisatie, of simpelweg een praktische wijze van voldoen aan de privacywetgeving. Kortom: met Privacy Verified verandert u uw privacywetgeving in een strategisch wapen!

Kies de certificering die past bij uw organisatie
Organisaties zijn er in verschillende soorten en maten. Privacy Verified biedt met drie certificeringsprogramma's voor elke organisatie een passende oplossing. Zo kunt u zelf beslissen, welke vorm van certificering het beste bij uw organisatie past.

Privacy Verified kent het "Basic traject", "Extended traject" en "Enterprise traject". Het Basic traject is de lichtste variant. Met Privacy Verified Basic genereert u de wettelijk verplichte documentatie die door ons is aanbevolen aan de hand van een door u zelf door te lopen vragenlijst. Zijn onze aanbevelingen passend uitgevoerd, dan ontvangt uw organisatie van ons de certificering. Privacy Verified Basic leent zich hiermee perfect om uw website te controleren op naleving van de toepasselijke privacywetgeving. Hiermee kunt u uw websitebezoekers in één oogopslag laten zien dat het wel goed zit met hun privacy.

Privacy Verified Extended gaat een stap verder en is interessant wanneer u naast een controle van de wettelijk verplichte documentatie ook een specifieke dienst of product wil laten toetsen. Denk bijvoorbeeld aan het toetsen van een nieuw ontwikkelde applicatie. Testen of de applicatie voldoet aan de eisen van *privacy by design*? Dan is de Extended variant van Privacy Verified de juiste keuze. Privacy Verified Extended is daarmee bij uitstek ook interessant voor organisaties die middels een audit aan dienen te tonen dat hun dienst of proces in lijn met de AVG is ingericht en persoonsgegevens volgens de regels worden verwerkt. Een inventarisatie wordt opgevolgd door een praktische 'to-do-list' met concrete verbeterpunten. Zijn deze naar behoren opgepakt, dan kunt u met een gerust hart het Privacy Verified certificaat overhandigen aan de auditor, of bijvoorbeeld tonen op uw website.

Het Enterprise traject is de denkbeeldige 'Rolls Royce' binnen Privacy Verified. Middels Privacy Verified Enterprise toetst ICTRecht of uw gehele organisatie in lijn handelt met de AVG. Dit is overigens geen kleine operatie, middels dit traject wordt namelijk zowel de 'voor-' als 'achterkant' van een organisatie getoetst op naleving. Dit houdt in dat niet enkel de processen met betrekking tot het verwerken van gegevens van bijvoorbeeld klanten getoetst worden, maar ook de interne processen ten aanzien van de omgang met gegevens van medewerkers. Een intensieve inventarisatie levert uiteindelijk een *to-do-list* op met praktische, concrete aanbevelingen. Voert u deze goed uit, dan ontvangt u na een controle op deze punten het Privacy Verified certificaat.

Krijg toegang tot het Privacy Verified portaal
Om organisaties op een zo goed mogelijke manier bij te kunnen staan gedurende het Privacy Verified traject, wordt bij afname van elke variant toegang verschaft tot het Privacy Verified portaal. Leuker kunnen we de privacywetgeving niet maken (al doen we ons best); makkelijker maken we het op deze manier wel. Dit is namelijk precies waar het Privacy Verified portaal voor bedoeld is. Niet alleen zetten we in dit portaal de *to-do-list* om in taken, zodat direct inzichtelijk is wat er dient te gebeuren op het gebied van privacy. Ook kunt u hierbinnen in een handomdraai aan de hand van vragenlijsten de benodigde privacy documenten genereren.

Daarnaast kunt u in het portaal de verwerkingsactiviteiten bijhouden en zo nodig datalekken registeren. Dit zorgt er niet alleen voor dat alle werkzaamheden worden bijgehouden en u op een praktische manier kan voldoen aan de AVG, maar ook dat alles wat te maken heeft met de AVG op één plek is opgeslagen. Wel zo handig. Natuurlijk begrijpen wij als geen ander dat u soms wel eens tegen vragen aanloopt. De AVG is immers niet uw *core business*. Wij zorgen er daarom voor dat u er nooit alleen voor staat. Wij kunnen altijd over uw schouder meekijken in het Privacy Verified portaal. Mocht dat nodig zijn dan neemt u met één druk op de knop contact met ons op, zodat we een helpende hand kunnen bieden.

Tot slot is het belangrijk om te onthouden dat voldoen aan de AVG een doorlopend proces is, waarbij mensen een belangrijke rol spelen. Natuurlijk kan een foutje gebeuren, dat is menselijk. Bewustwording op het gebied van privacy kan echter een hoop fouten voorkomen. Ook daar voorziet het Privacy Verified portaal in. U heeft via het portaal toegang tot webinars om de bewustwording binnen de organisatie op peil te krijgen en te houden.

Privacy Verified stap 1: inventarisatie
Het Privacy Verified-traject start met een inventarisatie. Hiermee leggen we een fundament voor het gehele traject. We nemen een kijkje in de keuken van uw organisatie. Het doel van de inventarisatie is het verzamelen van informatie, zodat dat we een goed beeld hebben van uw organisatie. Afhankelijk van het gekozen traject doen wij dit door de privacy documenten te bekijken die reeds bij u in huis zijn, uw product en/of dienst onder de loep te nemen en *key-users* binnen de organisatie te interviewen. Daarbij is met name van belang welke persoonsgegevens er worden gebruikt, hoe daarmee wordt omgegaan en of de privacy documenten voldoen aan de wettelijke vereisten.

Privacy Verified stap 2: uitkomst inventarisatie
Aan de hand van de inventarisatie zal beoordeeld en uiteengezet worden waar de juridische risico's zitten en wat de mogelijke oplossingen hiervoor zijn. We stellen vervolgens een praktische *to-do-list* op met werkzaamheden op het gebied van privacy. Denk aan het opstellen van privacy documenten zoals een privacy- en cookieverklaring en het sluiten van de benodigde verwerkersovereenkomsten met derde partijen. Voor het oppakken van de werkzaamheden bieden we twee smaken: u kunt de werkzaamheden zelf oppakken, maar we kunnen u daarin ook ontzorgen. Een combinatie van beide is ook mogelijk. Wij kijken graag met u mee wat daarin de wensen zijn en het beste bij u past.

Privacy Verified stap 3: verificatie
Zodra de benodigde werkzaamheden die voortkomen uit de inventarisatie zijn doorgevoerd doen wij een controle. Als alle werkzaamheden naar behoren zijn uitgevoerd ontvangt u van ons het Privacy Verified-certificaat. Dit certificaat en het logo mogen op de website worden geplaatst, maar uiteraard ook worden gedeeld met belanghebbenden.

Privacy Verified als visitekaartje
Privacy Verified is hét middel om op een eenvoudige manier naar buiten toe te laten zien dat u en uw leveranciers aan de AVG voldoen op de punten die zijn getoetst. U kunt aantonen dat er niet over één nacht ijs is gegaan bij het voldoen aan de AVG, dat er voortdurend aandacht wordt besteed aan het voldoen aan de AVG en u dat ook verlangt van alle partijen waarmee samen wordt gewerkt. Naast dat Privacy Verified een middel is om simpelweg aan wetgeving te voldoen, kunt u met Privacy Verified privacy dus inzetten als belangrijke commerciële toegevoegde waarde.

PRIVACY VERIFIED

Verander wetgeving in een strategisch wapen

Het vastleggen en managen van uw privacy (AVG/GDPR), is een verplichting die steeds belangrijker is voor uw klanten en partners. Met ons certificeringsprogramma wordt privacy in 3 heldere stappen, een onderscheidende propositie van uw organisatie.

Lisette Meij
Directeur ICTRecht Privacy

Peter Kager
Directeur ICTRecht Privacy

020 6631941
info@privacyverified.nl

Wilt u meer weten over Privacy Verified?
Bezoek onze geheel vernieuwde website:
privacyverified.nl

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Noot bij Planet 49: het einde van de vooraf aangevinkte cookie pop-ups?

Op 1 oktober 2019 heeft het Hof van Justitie van de Europese Unie uitspraak gedaan over het vragen van toestemming bij het plaatsen van cookies. De uitspraak kwam niet als donderslag bij heldere hemel, maar is eigenlijk een bevestiging van wat wij al wisten: voor het plaatsen van cookies is namelijk de actieve toestemming vereist van een internetgebruiker. Dit staat zelfs letterlijk zo in de AVG: "stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit" mogen niet als toestemming gelden.

Het Duitse Planet 49 organiseerde via haar website een winactie. Bij het deelnameformulier hoorden twee aanvinkvakjes. Het eerste vakje moest verplicht worden aangevinkt, en stelde toestemming te geven voor contact door partners van Planet49 met een aanbieding. Het tweede vakje vroeg toestemming voor advertentiecookies. Beide vakjes waren vooraf aangevinkt, maar het tweede vakje kon worden leeggemaakt waarna deelname mogelijk bleef.

Duitse consumentenorganisaties waren het niet eens met deze handelswijze en stapten naar de rechter, die de vraag voorlegde aan het Hof van Justitie. De gestelde vragen waren:

1. Is er sprake van daadwerkelijke toestemming wanneer […] wordt toegestaan door middel van een vooraf aangevinkt selectievakje dat door de gebruiker moet worden uitgevinkt in geval hij weigert zijn toestemming te verlenen?
2. Maakt het […] enig verschil of de opgeslagen of opgevraagde gegevens persoonsgegevens zijn?
3. Is […] sprake van daadwerkelijke toestemming in de zin van artikel 6, lid 1, onder a), van [verordening 2016/679] (de AVG)?
4. Welke informatie dienen door de aanbieder van diensten aan de gebruiker te worden verstrekt in het kader van de […] te verstrekken duidelijke en volledige informatie? Valt daaronder ook de informatie hoelang de cookies actief blijven en of derden toegang tot de cookies hebben?

De vragen verbazen een beetje – dit wéét iedereen toch al? Dat je voor cookies (behalve de strikt noodzakelijke) toestemming nodig hebt, staat al jaren in de cookiewet. Maar omdat toestemming vragen nogal een gedoetje is, wordt daar massaal de hand mee gelicht. Het idee was overigens dat door zulke strenge regels aan toestemming te stellen, partijen minder cookies zouden inzetten. Moehaha, inderdaad. En dan krijg je dus – naast de cookiemuur – allerhande constructies die dat recht moeten praten; ik heb alle termen wel gehoord, van *soft optin* tot *silent consent* en *browsewrap*-toestemming. Nee, dat werkt dus niet.

Het Hof is erg duidelijk in haar oordeel bij de eerste vraag. Er is géén sprake van toestemming wanneer men een vinkje weg moet halen uit een vakje. Toestemming is immers gedefinieerd als "elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden verwerkt". Alleen al die term 'wilsuiting' impliceert al dat iets actiefs moet worden gedaan.

En bovendien staat dit letterlijk zo in de AVG: “stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit” mogen niet als toestemming gelden.

Het is daarbij praktisch ook onmogelijk om objectief vast te stellen of de gebruiker van een website door een standaard aangevinkt vakje niet uit te vinken, inderdaad toestemming heeft gegeven om zijn persoonsgegevens te verwerken en in ieder geval of deze toestemming op basis van informatie is verleend. Het kan immers niet worden uitgesloten dat deze gebruiker de informatie bij het standaard aangevinkte vakje niet heeft gelezen of dat hij dit vakje niet eens heeft opgemerkt voor hij zijn activiteiten op de bezochte website voortzette.

Als laatste laat het Hof meewegen dat in de ‘oude’ cookieregels met opt-out werd gewerkt, terwijl de huidige regels opt-in eisen. Een situatie waarbij men actief nee moet zeggen, kan dan eigenlijk op geen enkele manier legaal zijn, want de nieuwe regels moeten toch strenger zijn dan de oude.

Ook het feit dat men uiteindelijk de deelnameknop (insturen van formulier) heeft gebruikt, kan niet als wilsuiting worden gezien. Die uiting gaat niet specifiek over het toestemming geven voor cookies maar over deelname aan de winactie. Het is niet toegestaan om toestemming voor cookies te combineren met een andere wilsuiting.

De tweede vraag ging over het punt dat hier toestemming werd gevraagd voor cookies die op zich geen persoonsgegevens betroffen of zouden doen verwerken. De AVG (en voorheen de Richtlijn, waar de Wbp op gebaseerd was) regelt immers toestemming en andere zaken rondom persoonsgegevens. Het Hof is ook hier duidelijk: het doet er daarbij niet toe of de cookies iets met persoonsgegevens te maken hebben. Hoewel de regels over toestemming uit de AVG komen, is de cookiewet breder. Ieder opslaan of uitlezen van informatie op iemands computer vereist AVG-compliant toestemming. Ook bij bijvoorbeeld een update van je software of het opvragen van een bestandje zonder persoonlijke informatie. Blijf van mijn laptop tenzij ik zeg dat je erin mag. En dat mag dus niet met vooraf aangevinkte vinkjes.

Deze uitlegging wordt bevestigd door overweging 24 van richtlijn 2002/58 waarin staat te lezen dat alle informatie die wordt bewaard in de eindapparatuur van gebruikers van netwerken voor elektronische communicatie, deel uitmaakt van de op grond van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden te beschermen persoonlijke levenssfeer van de gebruikers. Deze bescherming is van toepassing op alle informatie die is opgeslagen op deze eindapparatuur, ongeacht of het gaat om persoonsgegevens, en beoogt met name, zoals uit dezelfde overweging blijkt, de gebruikers te beschermen tegen het risico dat verborgen identificatoren en andere soortgelijke programmatuur zonder hun medeweten binnenkomen in hun eindapparatuur.

De derde vraag borduurt hierop voort. Welke informatie moet je verstrekken over cookies, voordat aan de informatieplichten uit de cookiewet is voldaan? Hierbij gaat het niet alleen om de identiteit van de voor de verwerking verantwoordelijke en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, maar ook om verdere informatie zoals met name de ontvangers of de categorieën ontvangers van de gegevens voor zover die, met inachtneming van de specifieke omstandigheden waaronder deze verdere informatie verkregen wordt, nodig is om tegenover de betrokkene een eerlijke verwerking te waarborgen. Onder de Richtlijn was het niet letterlijk verplicht ook te vermelden hoe lang de cookies bleven staan. De AVG eist van wel, en het Hof oordeelt dan ook dat deze informatie gewoon essentieel is.

Als laatste moet ook bij de informatie vermeld worden aan welke derden de informatie achter de cookies wordt verstrekt. Helaas gaat men niet in op het detail hoe dat precies moet; Planet49 werkte met de bekende praktijk van een lange lijst van derden in een hyperlink achter de toestemmingsvraag. Deze praktijk lijkt daarmee legaal.

De grote vraag: hoe moet toestemming vragen dan wel? Een cookiebanner ligt het meest voor de hand. Hierin vermeldt men dan welke partijen cookies plaatsen, wat voor cookies worden geplaatst (bijvoorbeeld social media cookies), wat die cookies doen (denk aan gepersonaliseerde advertenties laten zien) en waar meer informatie gevonden kan worden (in de privacy- en cookieverklaring).

Een websitebezoeker moet een actieve handeling verrichten om toestemming te verlenen. Dat wil zeggen dat een websitebezoeker zelf moet aanvinken welke cookies geplaatst mogen worden. Het is dus niet de bedoeling dat een website de categorieën cookies aanvinkt. Alle vinkjes moeten uit staan.

Wat is nog meer niet goed? Wij zien weleens cookiebanners voorbijkomen met daarop een tekst als “Indien u verder klikt op onze website, gaat u akkoord met het gebruik van cookies”. Natuurlijk is het verder surfen op de website een actieve handeling, maar op deze manier wordt impliciete toestemming gegeven. Dat is niet toegestaan. Een websitebezoeker moet akkoord gaan met het plaatsen van cookies, maar moet ook de mogelijkheid hebben om te weigeren dat cookies worden geplaatst. Dan vinkt diegene niet aan dat advertentie-, social media of andere tracking cookies geplaatst mogen worden.

Van onze blog

Privacy | Contracteren | E-commerce

1 november 2019

Kleine lettertjes: de kunst van een goede privacyverklaring

Kunst en recht worden niet vaak aan elkaar verbonden. Een jurist met beroepsdeformatie kan weliswaar kunst zien in een schitterend, complex stuk wetgeving of een onvoorstelbaar creatieve overeenkomst. Het feit dat veel grote kunstenaars, zoals Matisse, Tsjaikovski en Kafka, ook juridisch geschoold waren is bovendien kennis die bij een pubquiz goed van pas kan komen. Maar kunst is meestal (gelukkig) niet juridisch ingestoken en de wereld van het recht is vaak weinig artistiek. Des te opvallender was het vorige week dat de Volkskrant berichtte over een kunstwerk, bestaande uit 835 sets privacyvoorwaarden[1].

Kunstenares Julia Jansen bezocht de website van The Daily Mail, waardoor via cookies haar surfgegevens bij al die 835 bedrijven belandden. Zij verzamelde alle privacy-voorwaarden die daardoor op haar van toepassing waren en liet deze achter elkaar voorlezen. Kunst met een duistere ondertoon dus. Al die kleine lettertjes, die we zelden lezen maar die wel juridische gevolgen hebben, dat is welhaast om moedeloos van te worden. Hoe zijn we in deze werkelijkheid beland, waar de eerdergenoemde Kafka een puntje aan had kunnen zuigen? En hoe maken we leesbare privacyverklaringen waar je niet tureluurs van wordt?

1. https://bit.ly/2tfwyhS
2. https://app.nos.nl/op3/cookies/
3. https://nyti.ms/2RVeF2h

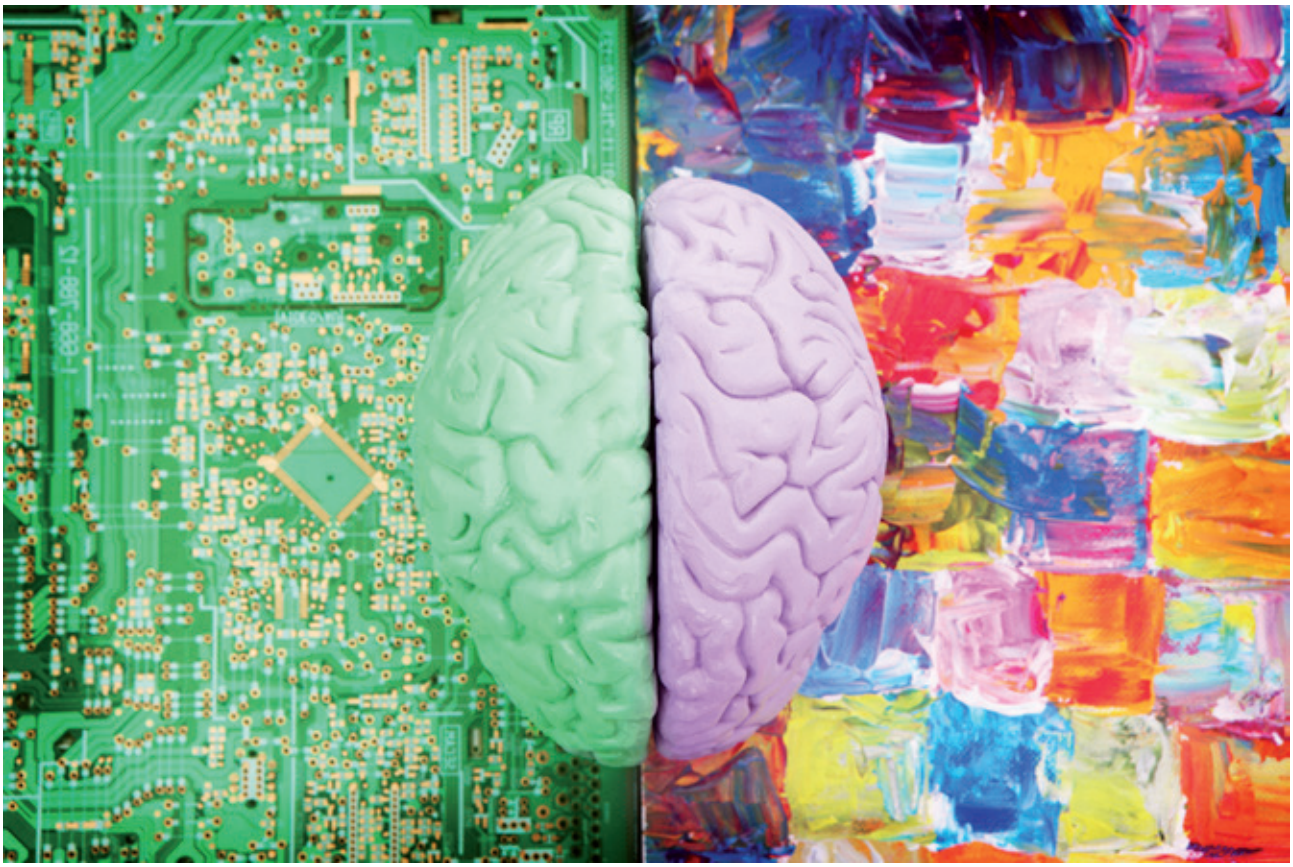
Real-time bidding

Het proces van *real-time bidding*, ook wel *programmatic advertising* genoemd, zorgt er allereerst voor dat surfgegevens soms naar honderden partijen worden gestuurd. De NOS bracht onlangs mooi in beeld[2] hoe het er achter de schermen aan toegaat, wanneer tracking cookies worden geplaatst om advertenties te tonen. De websitebezoeker, die zelf alleen een banner of pop-up als eindresultaat te zien krijgt, wordt in een fractie van een seconde 'verkocht' op een enorme virtuele marktplaats. Het opgebouwde profiel van de bezoeker bepaalt voor welke adverteerder hij of zij het meeste waard is. De hoogste bieder wint en betaalt de website-eigenaar – via allerlei tussenpersonen – om aan de bezoeker zijn reclame te tonen. Alle deelnemers binnen die marktplaats verwerken zijn of haar persoonsgegevens.

Hou het beknopt, transparant, begrijpelijk, gemakkelijk, duidelijk en eenvoudig

De AVG verplicht dat je uitlegt wat je doet met persoonsgegevens. Ook als dat heel ingewikkeld is om uit te leggen. Hier staat een overzicht van wat er allemaal in de privacyverklaring thuishoort. Hoewel deze verklaring volgens de wet in een 'beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal' moet worden aangeboden, valt dat in de praktijk nog vaak tegen.[3] Airbnb wint de prijs van langste en meest onbegrijpelijke privacyverklaring; die tekst is even moeilijk te lezen als Kritiek van de Zuivere Rede van Immanuel Kant.

De kleine lettertjes zijn de consument al lange tijd een doorn in het oog. Hoe moet het dan wel, een beknopte en duidelijke privacyverklaring? Allereerst: ken je publiek. Aangezien de meeste bedrijven zich niet uitsluitend richten op juristen is het raadzaam om de privacyverklaring ook niet als een juridisch stuk in



te steken. Als typisch voorbeeld, wie gelooft nou de belofte van deze openingszin: “Wij respecteren de privacy van onze klanten en bezoekers” als de lezer even later de volgende tussenkop moet ontcijferen: “Doorgifte aan dienstverleners die als verwerkingsverantwoordelijke jouw gegevens verwerken bij de uitvoering van je bestelling bij de betaling van goederen aan de bij de bestelling opgegeven aanbieder van betaaldiensten of een financierende bank”?

Wilt u de korte of de lange versie?
Naast de toon is ook de lengte van de verklaring een factor om rekening mee te houden. Een gelaagde structuur kan daarbij een nuttig middel zijn om elke lezer effectief van informatie te voorzien. Op de eerste laag geef je algemene informatie over de omgang met persoonsgegevens en een samenvatting van elk specifiek onderwerp in de verdiepende laag. Voor de meeste lezers is dit misschien al voldoende informatie. Via uitklapvelden of kruisverwijzingen is de verdiepende laag toegankelijk. Daar leg je, bijvoorbeeld, in detail uit wat er gebeurt bij elke afzonderlijke verwerking van persoonsgegevens, hoe men zijn of haar rechten kan uitoefenen en welke technische beveiligingsmaatregelen er zijn. Zo worden de meer kritische of technisch geïnteresseerde lezers voorzien van het volledige verhaal.

Creativiteit mag, maar duidelijkheid moet
Voor de meeste organisaties zal de meest standaard vorm van de privacyverklaring – een stuk tekst wat te bereiken is via een link onderaan de website – prima voldoen. Sommige partijen laten meer creativiteit los op de informatieplicht (en hebben nog een marketingpotje over). EasyJet biedt bijvoorbeeld via een video op YouTube[4] op toegankelijke wijze informatie over privacy.

Proactief nieuwe manieren bedenken om privacy bij je gebruikers of klanten onder de aandacht te brengen, dat is alleen maar positief. Vergeet daarbij niet om eerst de basis op orde te brengen: beschrijf in begrijpelijke taal wat je met persoonsgegevens doet en behandel daarbij in ieder geval de eisen van de AVG.

4. https://bit.ly/34eqXVX

Auteur
Dimmen Smolders
Juridisch adviseur

Privacy Contracten Overheid

20 november 2019

Overnames: mogen persoonsgegevens zomaar mee?

Bij het kopen of verkopen van organisaties worden ook persoonsgegevens overgenomen. Dat kunnen gegevens van medewerkers zijn, maar ook gegevens van zakelijke contacten, leveranciers, en natuurlijk klantenbestanden. Op de overname en dus de verwerking van deze persoonsgegevens is de Algemene verordening gegevensbescherming (AVG) van toepassing. Mag je deze persoonsgegevens zomaar toevoegen aan je eigen database na overname?

Due diligence

Wanneer een organisatie in de verkoop staat, is het *due diligence* onderzoek een vast onderdeel van het aankoopproces. Hiermee hoopt een koper te voorkomen dat hij spreekwoordelijke lijken in de kast aantreft na de overname. Naast het gebruikelijke boekenonderzoek wordt ook onderzoek gedaan naar de commerciële en juridische stand van zaken bij de organisatie. Onder dat laatste valt inmiddels ook de plicht om te voldoen aan de AVG. Vrijwel alle organisaties verwerken immers persoonsgegevens. Eén van de basisbeginselen van de AVG is de verantwoordingsplicht: iedere organisatie die persoonsgegevens verwerkt dient te kunnen aantonen dat deze aan de verschillende verplichtingen uit de privacywet voldoet. Heeft de verkopende partij de zaken op orde? Dan dient deze eenvoudig onder andere de volgende stukken te kunnen aanleveren:

- Het verwerkingsregister (zowel in de rol van verwerkingsverantwoordelijke als verwerker): het overzicht van de verwerkingen, grondslagen, ontvangers, etc;
- Privacybeleid: hoe medewerkers reeds omgaan met persoonsgegevens;
- Beveiligingsbeleid: welke passende beveiligingsmaatregelen de verkoper heeft genomen om persoonsgegevens te beschermen tegen o.a. datalekken;
- Verwerkersovereenkomsten: een overzicht van de overeenkomsten over de omgang met persoonsgegevens die zijn gesloten met derde partijen.

Mochten er zaken niet op orde zijn, dan zal de kopende partij investeringen moeten doen. Dat kan worden meegenomen in de koopovereenkomst.

Grondslag voor overname

Los van de voorwaarden en vereisten van een koopovereenkomst, dient voor de verwerking van persoonsgegevens een wettelijke grondslag aanwezig te zijn. Zoals we eerder al hebben schreven, wordt snel aan toestemming gedacht. Dat is echter niet de enige grondslag die gebruikt kan worden. In het geval van een overname zal de koper vaak een beroep kunnen doen op het 'gerechtvaardigd belang', zeker met betrekking tot het klantenbestand. Het commerciële belang van de kopende organisatie dient hierbij zwaarder te wegen dan het privacybelang van diegene van wie de persoonsgegevens zijn (betrokkene). Zolang de koper de gegevens alleen gebruikt om de overeenkomst uit te voeren en daarmee de wens van de klant na te komen, zal de privacyinbreuk gering zijn. Aanvullend dient aan de andere eisen van de AVG te worden voldaan, zoals het informeren over de overname en het naleven van bewaartermijnen.

En hoe zit het met medewerkersgegevens?

Een belangrijk deel van een overname is natuurlijk het personeel. Tijdens het *due diligence* onderzoek wil een potentiële koper ook graag inzage verkrijgen in de stand van zaken en mogelijke risico's met betrekking tot de medewerkers. Welke arbeidsvoorwaarden gelden er en welke specifieke afspraken zijn er met individuele medewerkers gemaakt? Daar heeft hij dan ook een gerechtvaardigd belang bij. Partijen dienen echter niet de andere AVG-verplichtingen uit het oog te verliezen. Denk bijvoorbeeld aan het principe van dataminimalisatie: alleen de gegevens die voor de koper noodzakelijk zijn voor het onderzoek dienen verstrekt te worden. Tot individuele medewerkers herleidbare gegevens zullen niet snel noodzakelijk zijn. Waar mogelijk dienen documenten en gegevens daarom geanonimiseerd te worden. Denk daarbij aan personeelsoverzichten en arbeidsovereenkomsten, maar ook ziekteverzuim

en informatie over arbeidsconflicten. Zorg er tot slot voor dat alle gegevens binnen één beveiligde omgeving worden uitgewisseld, om het risico op incidenten en datalekken te beperken.

Mag je commerciële mails blijven sturen?
Daarnaast is de nieuwsbriefdatabase van commerciële waarde bij een overname. De koper wil namelijk een zo groot mogelijk publiek informeren over zijn producten en diensten. De ontvangers hebben alleen toestemming gegeven voor mails van X, niet van Y. Mag deze database dus zomaar mee met de overname? Wanneer de verkoper doorgaat onder de naam van de koper mag dat. Maar: informeer goed over de overname en dat er niks verandert aan de dienstverlening en de lopende zaken. De nieuwsbrief zal voortaan alleen onder een andere naam worden verstuurd. Uiteraard heeft de ontvanger altijd de mogelijkheid om zich weer af te melden.

Auteur
Laura Monhemius
Juridisch adviseur

Trainingsoverzicht januari – juli 2020

Donderdag 23 januari

Privacy en persoonsgegevens: privacy by design/ default (4 PO)

Privacy in de ICT brengt nieuwe aandachtspunten met zich mee. Twee belangrijke zijn de begrippen privacy by design en privacy by default. Deze begrippen zullen centraal staan bij ontwikkeling en gebruik van ICT-systemen. Hoe kan privacy worden meegenomen in een ontwikkeltraject, hoe borgt men adequate privacy-instellingen in het gebruik en hoe wordt een en ander praktisch vastgelegd?

https://bit.ly/2DsnvM8

Donderdag 16 april

ICT en gezondheidsrecht (6 PO)

Werkt u bij een zorginstelling of bent u een ICT-dienstverlener in de zorg? Vraagt u zich af wat de regels zijn voor het uitwisselen van medische gegevens online en hoe men moet werken in de cloud? U leert het tijdens deze eendaagse training over ICT, beveiliging & privacy in de zorg.

https://bit.ly/37KVuO0

Donderdag 23 april

Privacy en persoonsgegevens: de basis (6 PO)

Wanneer is de AVG van toepassing, wat is een persoonsgegeven en waar moet u rekening mee houden op privacygebied? In deze dagtraining wordt de AVG op hoofdlijnen uitgewerkt om zo het kader voor een zorgvuldige omgang met persoonsgegevens te kunnen realiseren.

De insteek van de training is interactief en praktijkgericht. We spreken vanuit cases waarin wij dagelijks adviseren. Ook wordt de meest recente en relevante jurisprudentie behandeld. Door het interactieve karakter van de training is er ruimte voor al uw vragen en twijfels.

https://bit.ly/2L1JM86

Dinsdag 12 mei

Contracteren: de basis

Contracteren ligt aan de wortel van een groot deel van het ICT-recht. ICT-contracten kennen verschillende types, van softwarelicentie tot resellerovereenkomst en van algemene voorwaarden tot mantelcontract. Elk contract vereist algemene aandachtspunten (onder meer kwaliteit, aansprakelijkheid, intellectueel eigendom, datatoegang, continuïteit en persoonsgegevens) en daarnaast specifieke aspecten.

De insteek van de training is interactief en praktijkgericht. We spreken vanuit cases waarin wij dagelijks adviseren. Ook wordt de meest recente en relevante jurisprudentie behandeld. Door het interactieve karakter van de training is er ruimte voor al uw vragen en twijfels.

https://bit.ly/2sqpyhJ

Dinsdag 26 mei

Update Algemene verordening gegevensbescherming (AVG)

Wij praten u in een middag bij over de belangrijkste recente ontwikkelingen op het gebied van de Algemene verordening gegevensbescherming (AVG). Er worden praktijkvoorbeelden behandeld, onder meer over datalekken en boetes.
De insteek van de training is interactief en praktijkgericht. We spreken vanuit cases waarin wij dagelijks adviseren. Ook wordt de meest recente en relevante jurisprudentie behandeld. Door het interactieve karakter van de training is er ruimte voor al uw vragen en twijfels.

https://bit.ly/2OpHt0q

Dinsdag 16 juni

Privacy en persoonsgegevens: de verdieping

Privacywetgeving kent open normen en grijze gebieden. Als jurist moet u deze kunnen identificeren en op een deskundige en begrijpelijke wijze naar de praktijk kunnen vertalen. Hierbij is diepgravende kennis over de relevante technologie van groot belang. Tijdens de training leert u onder meer over binding corporate rules, de verwerkersovereenkomst, registers en de Functionaris Gegevensbescherming (FG).

De insteek van de training is interactief en praktijkgericht. We spreken vanuit cases waarin wij dagelijks adviseren. Ook wordt de meest recente en relevante jurisprudentie behandeld. Door het interactieve karakter van de training is er ruimte voor al uw vragen en twijfels.

https://bit.ly/35LBVU1

Donderdag 2 juli

Contracteren: de verdieping

Contracteren in de ICT vereist bijzondere aandacht, met name waar het gaat om software. Van ontwikkeling tot licentie en distributie en omgang met open source: software ligt immers aan de basis van vrijwel alle ICT-dienstverlening. Voortbouwend op de basistraining worden de algemene aandachtspunten uitgewerkt en nieuwe aspecten, zoals Agile ontwikkeling van software, geïntroduceerd. U gaat niet weg tot u al onze praktijktrucs kent!

De insteek van de training is interactief en praktijkgericht. We spreken vanuit cases waarin wij dagelijks adviseren. Ook wordt de meest recente en relevante jurisprudentie behandeld. Door het interactieve karakter van de training is er ruimte voor al uw vragen en twijfels.

https://bit.ly/2pXlg0j

Wilt u de juridische kennis binnen uw organisatie verhogen? Dan is een inhouse training van ICTRecht iets voor u.

Een inhouse training kan volledig voor u op maat ontwikkeld worden waarbij voorbeelden uit uw eigen praktijk in het lesprogramma worden verwerkt.

Kijk voor meer informatie over onze inhouse trainingen op: **https://bit.ly/33nmSy8**

Heeft u vragen of wilt u meer weten?

Neem contact op met onze opleidingscoördinator Alisa Schurink via e-mail: academy@ictrecht.nl of telefoonnummer: 020 663 19 41.

Alisa Schurink
Opleidingscoördinator
en Marketingmedewerker


ICTRECHT
adviesbureau