ICTRECHT
adviesbureau

ICTRECHT
IN DE PRAKTIJK

jaargang 7 nummer 4 oktober 2019

Van BBS tot FAMA en AI: vijftien jaar internetrecht in vogelvlucht

5G: evolutie of resolutie?

Een portret van een werknemer in een reclame-uiting, mag dat?

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

Op 15 november is het zo ver: dan bestaat adviesbureau ICTRecht vijftien jaar. We vieren dat met een uniek congres (zie pagina 8) over de toekomst van internetrecht. Maar wat is dat begrip nu, en wat valt er zoal onder? Ik blijf me daarover verbazen, en nodig u graag uit om mee te discussiëren via dit tijdschrift of het congres.

Dat privacy en de AVG onder internetrecht valt, lijkt buiten kijf te staan. Al vijftien jaar, of misschien al 129 jaar relevant? Lees er alles over in het artikel van Dimmen. En ook de techniek staat niet stil, getuige de bijdrage van Matthijs en Derk Jan. Want technologische innovatie is en blijft een van de belangrijkste aspecten van internetrecht, of zo u wilt ICT-recht.

Een nieuw aspect aan internetrecht is het gezondheidsrecht. Sari belicht in haar bijdrage nog de te verwachten wijzigingen aan de WGBO.

Veel leesplezier en wellicht tot vrijdag 15 november!

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
Bram de Vos – Juridisch adviseur – b.devos@ictrecht.nl
Dimmen Smolders – Juridisch adviseur – d.smolders@ictrecht.nl
Matthijs van Bergen – Directeur Legal ICT – m.vanbergen@ictrecht.nl
Derk Jan Pilat – Stagiair
Jay Remmelzwaal – Juridisch adviseur – j.remmelzwaal@ictrecht.nl
Demi Grandiek – Juridisch adviseur – d.grandiek@ictrecht.nl
Iris de Groot – Juridisch adviseur – i.degroot@ictrecht.nl
Sari Jansen – Juridisch adviseur – s.jansen@ictrecht.nl
Beryl Hetharia – Juridisch adviseur – b.hetharia@ictrecht.nl
Tim Wokke – Juridisch adviseur – t.wokke@ictrecht.nl
Linde Mensink – Juridisch adviseur – l.mensink@ictrecht.nl
Raoul van de Laak – Juridisch adviseur – r.vandelaak@ictrecht.nl
Alisa Schurink – Opleidingscoördinator en Marketingmedewerker – a.schurink@ictrecht.nl
Britt Telleman – Office- en Legal Assistant – b.telleman@ictrecht.nl
Nicole Waaijer – Marketing adviseur – n.waaijer@ictrecht.nl
Amanda Butterworth – Vormgever – info@amandabutterworth.com
Leonard Fäustle Stills & Motion – foto's ICTRecht – info@leonardfaustle.nl

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Innovatie | Privacy | Cloud | E-commerce

Van BBS tot FAMA en AI: vijftien jaar internetrecht in vogelvlucht

Waarover ging het eerste vonnis op het gebied van internetrecht? Volgens de onvolprezen jurisprudentiebundel van mr. Tina van der Linden was dat een Bulletin Board System (BBS) dat werd aangesproken op illegaal ter download aangeboden software. BBS'en bestaan niet meer, illegale software nog wel. Maar de kwestie van hoe illegale downloads onder het recht vallen, is welhaast zo alledaags geworden dat een junior medewerker van stichting BREIN zich afvraagt waar de AI blijft die deze kan afhandelen. Nee, de controversiële onderwerpen van vandaag in het internetrecht richten zich op heel andere afkortingen: naast AI de bezigheden van Facebook, Apple, Microsoft en Alphabet en de AVG versus de tracking pixel en andere technologie.

Een verschuivend rechtsgebied

De termijn van vijftien jaar is natuurlijk arbitrair. Internet, althans ICT, en de rechtsvragen die door deze technologie werden opgeroepen zijn al veel ouder dan dat. Maar natuurlijk werd dat niet vanaf het eerste moment als apart rechtsgebied onderkend. Curieuze kwesties en lastige feitencomplexen zijn van alle tijden in het recht. Maar op zeker moment ontstond toch een soort van consensus dat er iets was dat we internetrecht, ICT-recht of technologie-recht zouden kunnen noemen.

Zoals ik in het vorige nummer al schreef, de definitie van wat internetrecht dan is, lijkt vaak neer te komen op het feit dat het zwaartepunt van de rechtsvraag zich bevindt in een internet- of ICT-aspect van de zaak. Oftewel: hoe ingewikkeld is het om de ICT-georiënteerde feiten juridisch te duiden of het best passende wetsartikel te vinden. En cynisch gezegd: pas als het zo ingewikkeld is, dat de gemiddelde jurist deze duiding nog niet kan uitvoeren.

Zo cynisch hoeft het echter niet te zijn. Verfrissender is het gezichtspunt dat de kwalificatie van deze aspecten nieuw is en daarmee diepgaande aandacht vraagt. Bij dat BBS kon serieus nog de vraag worden opgeworpen of men wel van openbaarmaken kan spreken als iemand per telefoon rare piepjes genereert. Enkele jaren later speelde het debat of op een website op "Akkoord" klikken, leidt tot een rechtsgeldige overeenkomst. Of wat denkt u van de jurisdictie-vraag wanneer een Griek in Duitsland via een app bij het in Nederland gevestigde Booking.com een hotelkamer boekt. Dit zijn geen klassieke kwesties in andere rechtsgebieden, en dus krijgt de internetjurist ze op het bord.

Of men het nu cynisch bekijkt of niet, een inherent kenmerk van internetrecht is dat wanneer de

technische aspecten voldoende breed begrepen zijn, een casus minder snel als internetrecht wordt gekwalificeerd. Een aankoop bij een webwinkel is anno 2019 een standaardcasus in het consumentenrecht, bijvoorbeeld. Eind jaren negentig kon men menig juridisch congres vullen met internetrechtelijke vragen over dit onderwerp. Het is volgens mij uniek dat een rechtsgebied door de tijd heen 'opschuift' en rechtsvragen afschuift naar andere gebieden.

Zesentwintig woorden schiepen het internet

Het voorbeeld van het BBS onderstreept dat auteursrecht het eerste rechtsgebied was waar internetrechtelijke kwesties langskwamen, al was het ook toen al zeker zo dat contractuele kwesties rond ICT-projecten actueel waren. Niet zo gek ook: het internet is ontworpen om informatie uit te wisselen, en auteursrecht is ontworpen om de verspreiding van informatie te reguleren. Daarnaast waren (en zijn) auteursrechthebbenden vaak goed geëquipeerd om hun rechten te handhaven. De eerste faxen met sommaties en schadeclaims volgden dan ook al vrij snel.

Een complicatie die daarbij zich vaak voordeed, was dat de partij die aan te wijzen was als verantwoordelijk voor de verspreiding, niet feitelijk de partij was die dit in gang zette. Webhostingbedrijven, internetproviders, forumbeheerders – en die meneer die het BBS beheerde, de *sysop* in de inmiddels vergeten terminologie – kregen met deze claims te maken. Dat was natuurlijk niet helemaal de bedoeling; niet zij maar de klant verrichten de onrechtmatige daad, en hoe kun je als bedrijf klanten informatie laten verspreiden als jij de schadeclaims krijgt? Moet een tussenpersoon zoals een internetprovider niet juridisch beschermd worden?

In Nederland kreeg deze kwestie zich medio jaren negentig grote aandacht toen publiciste Karin Spaink op haar website bij internetprovider XS4ALL publiceerde over de Scientology-beweging, daarbij citerend uitgelekte stukken van de organisatie zelf. Deze greep naar de auteursrechtelijke wapens om hier een eind aan te maken. Het Gerechtshof Den Haag bepaalde in 2003 echter dat de publiciste het gelijk aan haar zijde had – en dat de provider niet zelf aan te spreken was op auteursrechtinbreuk door haar klanten.

Ditzelfde thema kwam in andere landen terug, met name in de Verenigde Staten waar Section 230 van de *Communications Decency Act* in 1996 providers een keiharde wettelijke vrijwaring van aansprakelijkheid gaf voor handelen van hun klanten. Met de nuance van de *Digital Millennium Copyright Act* – dien uw auteursrechtelijke klacht bij de provider in en deze zal onmiddellijk ingrijpen – leidde dit tot een explosie aan online diensten waarbij gebruikers zaken konden plaatsen of versturen, zonder dat de provider continu

zorgen hoefde te hebben over aansprakelijkheid. In bloemrijke taal is *Section 230* daarom wel *"The Twenty-Six Words That Created the Internet"* genoemd.

Europa was met haar e-commercerichtlijn (2000) iets genuanceerder: een provider moest niet alleen op auteursrechtelijke klachten ingrijpen, maar op iedere beweerdelijke onrechtmatige daad wanneer deze 'onmiskenbaar' was. In de praktijk ging dit vrijwel altijd over auteursrechten, zodat de Europese en Amerikaanse praktijk op dit punt gelijk op ging. Naast auteursrechten waren overigens ook de merken en handelsnamen een belangrijk thema, met name rond de domeinnamen en online advertenties.

Van auteursrecht naar privacy

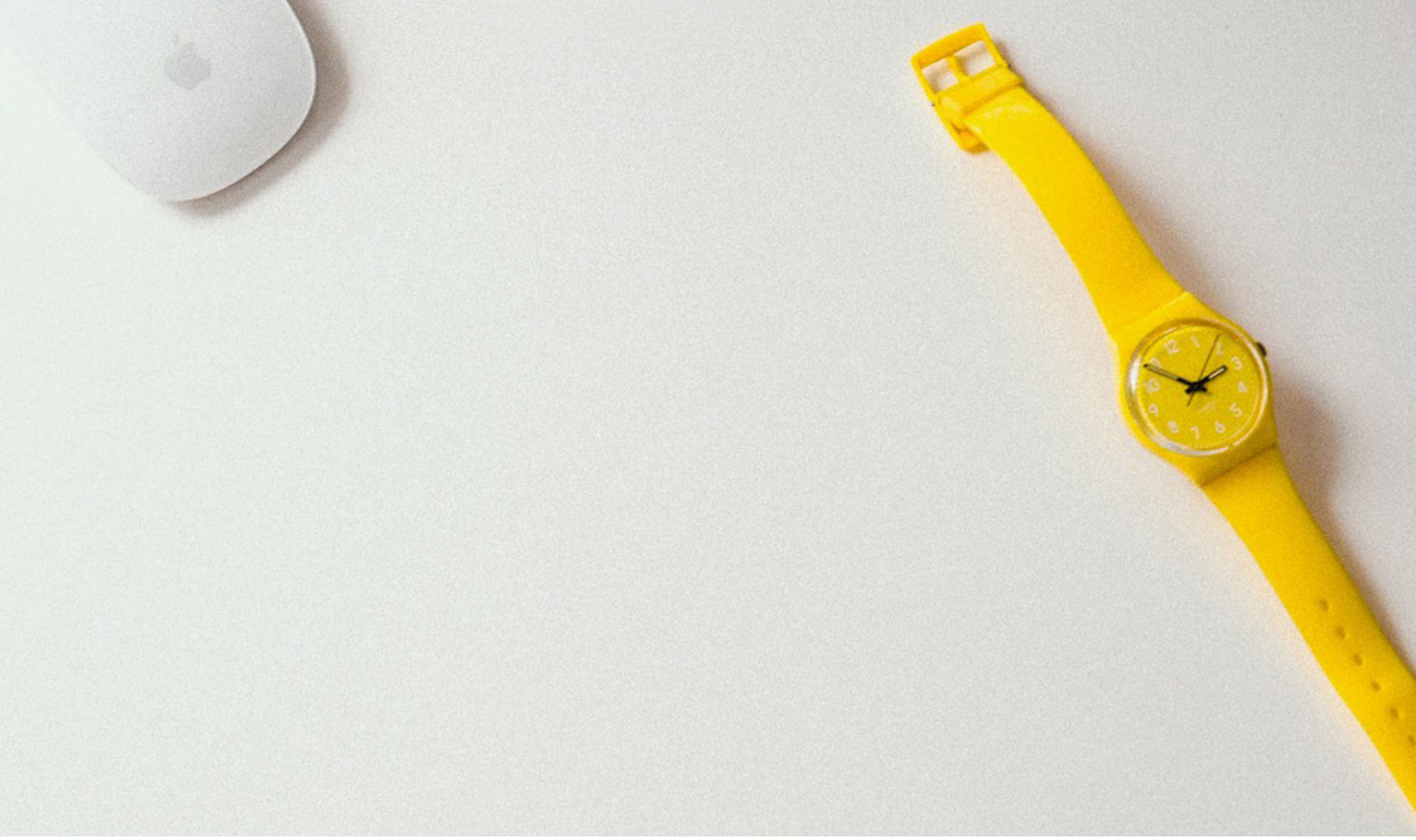
Amerikaanse jurisprudentie en richtsnoeren zijn in het internetrecht sowieso zeer zwaarwegend geweest in de beeldvorming rond dit rechtsgebied. Eind jaren negentig verscheen bijvoorbeeld de Databeschermingsrichtlijn, die strenge regels over omgang met persoonsgegevens stelde. Deze wet werd vrijwel compleet genegeerd in ICT-land. Ja, iedereen had netjes een privacy policy op de site waarin stond hoe men omging met persoonlijke gegevens van de bezoeker, maar dat was ingegeven door een aanbeveling van de Amerikaanse *Federal Trade Commission* dat transparantie en informatie over gegevensverwerking iets is dat een eerlijk ondernemer gewoon doet. Wat de sector oppakte als "zeg in wollige taal wat je doet, en dan mag alles".

De Databeschermingsrichtlijn stond een heel ander regime voor. Wees expliciet en specifiek, vraag toestemming, let op je beveiliging en doe geen dingen die mensen raar, onverwacht of opdringerig vinden. Daar kwam dus weinig van terecht, mede omdat Europese handhaving sterk gefragmenteerd was en zich nauwelijks richtte op de online omgeving. Plus het feit dat er in de meeste landen geen boetebevoegdheid bij toezichthouders was.

De Algemene Verordening Gegevensbescherming (AVG), met strenger geformuleerde regels, veel bozere taal en vooral giga-boetes, zie ik dan ook als niets minder dan een aardverschuiving. Bedrijven moesten nu ineens serieus iets met privacy, en dat was lastig omdat daar nooit echt over was nagedacht. Nieuwsbriefsoftware volgde mensen standaard in hun leesgedrag, online advertenties registreren iedere klik in een interesseprofiel, security software monitort gedrag en ga zo maar door. Kennis over mensen bleek in de tussentijd een zeer waardevol bedrijfsbezit. Maar vanuit de AVG zien we nu langzaam maar zeker een tegenbeweging ontstaan tegen deze datahonger van met name Amerikaanse bedrijven.

De rol van data

Data is juridisch niets, roep ik al geruime tijd. Eigendom op digitale data is niet mogelijk, omdat deze de essentiële eigenschap van uniciteit ontbeert. Dat bepaalde onze Hoge Raad in het Computergegevens-arrest, dat een nuance op het bekende Elektriciteits-arrest vormde.



Met name de opkomst van de cloud en software-as-a-service heeft de randen en risico's van deze rechtspositie blootgelegd. (Het Runescape-arrest dat eigendom op virtuele objecten toepasselijk verklaarde is daar dan weer een specifieke nuance binnen.)

Deze wankele positie verbaast nogal. Data is centraal in de kenniseconomie. *Data is the new oil*, zo luidde het motto op menig *venture capital pitch*. Je zou dus zeggen dat als er iets juridisch beschermd moet zijn, dat het dan data is. Maar dat is dus niet zo. Data is een artefact van het juridische feit dat ict-diensten eigenlijk hetzelfde worden behandeld als andere dienstverlening (de overeenkomst van opdracht). En met artefacten houdt het recht geen rekening.

ICT is dienstverlening. U vraagt, wij draaien. Of het nu gaat om het opslaan van bestanden, het berekenen van aanbevelingen of het doorzoeken van websites. Data is daarbij essentieel maar tegelijk dus onbeschermd. Juridisch gezien is Google een slimme hotelconciërge die het beste tentje voor je weet en onthoudt waar je de vorige keer was. Die conciërge kun je ook niet vragen om een kopie van 'jouw' data.

Ook juridisch ongeregeld: toegang tot de diensten die die data verwerken. Het continuïteitsprobleem, in de literatuur. Diensten stoppen af en toe, en waar sta je dan als afnemer? Dit is wederom volstrekt ongeregeld. Stoppen mag, en wie dan afhankelijk was van die dienst die heeft juridisch gezien gewoon pech gehad. Dat is een probleem: die afhankelijkheid is groot en het probleem bij stoppen dus acuut. Gefragmenteerde rechtspraak tot nu toe laat niet echt een heldere lijn zien waar dit heen moet gaan.

De komende vijftien jaar

Toegang tot online diensten en gebruik van data gaan hét thema worden de komende vijftien jaar. Het kan niet waar zijn dat het recht geen antwoord heeft op een dergelijk fundamenteel probleem al zou men geen toegang kunnen eisen tot diensten waar men sterk afhankelijk van is, als platforms machtiger zijn dan overheden maar zich niet zo opstellen en als data onbruikbaar wordt omdat een opslagprovider dat zo beschikt.

De eerste slagen zullen worden gevochten rond de inzet van data bij wat vroeger *big data* heette en nu *artificial intelligence*: analyses op grote bakken met data om voorspellingen te doen en op basis daarvan beslissingen. De AVG zal daarbij een leidende rol spelen. Maar dit zal slechts een voorhoedegevecht blijken voor de grotere open rechtsvraag: welke positie heeft zo'n supermachtig platform als Facebook of Alphabet nu eigenlijk? Niet alleen aansprakelijkheid, zoals in de jaren negentig, maar ook andere vragen – de positie van de burger, de bevoegdheid tot privaat regels stellen, en ga zo maar door.

We gaan nog heel wat meemaken de komende vijftien jaar.

THE FUTURE IS LEGAL

15 NOVEMBER 2019 • SPOORWEGMUSEUM
BESTEL UW TICKETS OP: THEFUTUREISLEGAL.NL

Op 15 november organiseren wij ter gelegenheid van ons 15-jarig bestaan een uniek congres. In het Spoorwegmuseum te Utrecht zullen 15 sprekers van verschillende disciplines hun visie geven op het thema ‘The Future is Legal’.

15 ★ Jaar ★

Sprekers:

Martijn Arets
INT. PLATFORM EXPERT

Merien ten Houten
AMBER

Michel van Eeten
TU DELFT

Michiel Steltman
STICHTING DINL

En verder o.a.: Melita van der Mersch, Alexander Pleijter, Ronald van den Hoff, Lonneke Driessen, Nynke Brouwer, Natali Helberger, Tim Pastoor, Marten Wilms, Arnoud Engelfriet, Peter Kager en Lisette Meij.


ICTRECHT
The Future is Legal wordt mede mogelijk gemaakt door:
TRUE
ONEL TRADEMARKS
LOUD & CLEAR
evidos
EVIDENCE IN ONLINE SERVICES
juriblox
HISCOX
AI • PLATFORMS • FAKE NEWS • SLIMME AUTO'S • GEZONDHEID • BURGERRECHTEN • REGULERING

Bram de Vos
Juridisch adviseur

Wet- en regelgeving

Experimentenwet nieuwe stembiljetten
Op 9 mei 2019 heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties een wetsvoorstel aangekondigd om vanaf de verkiezingen in 2021 een aantal experimenten met stembiljetten mogelijk te maken. Op dit moment wordt gewerkt met grote biljetten. Dit is voor de kiezers weinig handzaam en bemoeilijkt bovendien het tellen van de uitgebrachte stemmen. Men wil daarom toe naar een aanzienlijk kleiner biljet dat elektronisch geteld kan worden. Dit moet op de eerste plaats het telproces versnellen en moet daarnaast de foutgevoeligheid verkleinen. Mede vanwege beveiligingsrisico's is het tellen van de stemmen op dit moment nog een handmatig proces. Wel wordt al enige tijd gebruik gemaakt van spreadsheetsoftware, al zijn hierbij in het verleden ook veiligheidsrisico's aan het licht gekomen.

https://bit.ly/2KZ7vWV

Wetsvoorstel inzage medische dossiers ingetrokken
Op 13 mei 2019 heeft de Minister voor Medische Zorg en Sport een wetsvoorstel ingetrokken op grond waarvan zorgverzekeraars inzage konden krijgen in medische dossiers bij een vermoeden van fraude. De zorgverzekeraar zou hiervoor geen toestemming nodig hebben van de betreffende patiënt. Hoewel het wetsvoorstel al was aangenomen in de Tweede Kamer, stuitte het in de Eerste Kamer op de nodige kritiek. Ook vanuit patiëntenorganisaties en beroepsverenigingen voor zorgverleners werd kritiek op het voorstel geuit. Critici wijzen onder andere op het medisch beroepsgeheim wat als gevolg van de wet onder druk zou komen te staan. De minister heeft aangekondigd een nieuw, verbeterd wetsvoorstel in procedure te brengen.

https://bit.ly/30DxoRs

Besluit betreffende beperkende maatregelen tegen cyberaanvallen
Op 14 mei 2019 heeft de Raad van de Europese Unie een besluit gepubliceerd op basis waarvan sancties kunnen worden opgelegd bij cyberaanvallen die een bedreiging vormen voor (een lidstaat van) de Europese Unie. De sancties kunnen worden opgelegd indien er sprake is van een externe bedreiging, bijvoorbeeld bij een aanval die wordt uitgevoerd van buiten de Europese Unie of door personen of entiteiten die buiten de Europese Unie gevestigd of actief zijn. Zowel personen die verantwoordelijk zijn voor de cyberaanval (of poging daartoe), die hieraan financiële, technische of materiële steun verlenen, dan wel die hier op een andere wijze bij betrokken zijn of mee geassocieerd worden, kunnen een sanctie opgelegd krijgen. De sancties kunnen onder meer bestaan uit een inreisverbod voor de Europese Unie of een bevriezing van (bank)tegoeden. Alleen met "eenparigheid van stemmen" van de Raad kunnen personen aan de sanctielijst worden toegevoegd.

https://bit.ly/2ZBHAN7

Verordening voor vrij verkeer van niet-persoonsgebonden gegevens
Sinds 28 mei 2019 is de Verordening voor vrij verkeer van niet-persoonsgebonden gegevens van toepassing. Deze verordening moet ervoor zorgen dat niet-persoonsgegevens makkelijker tussen de lidstaten binnen de Europese Unie kunnen worden uitgewisseld. De verordening regelt daarnaast onder meer dat overheden toegang houden tot de gegevens (bijvoorbeeld voor het uitoefenen van toezicht) indien de gegevens zich in een andere lidstaat of in de cloud bevinden. Verder moet de verordening het voor professionele gebruikers gemakkelijker maken om te wisselen tussen verschillende cloudaanbieders (echter volledig op basis van nader vast te stellen zelfregulering). De commissie heeft eveneens richtsnoeren gepubliceerd (zie https://bit.ly/2YVzJWu) waarin wordt ingezoomd op de wisselwerking tussen de Algemene Verordening Gegevensbescherming (welke specifiek betrekking heeft op de verwerking van persoonsgegevens) en deze nieuwe verordening inzake niet-persoonsgebonden gegevens.

https://bit.ly/2ZvFWbn

Wet gebruik passagiersgegevens voor bestrijding terroristische en ernstige misdrijven
Op 4 juni 2019 heeft de Eerste Kamer ingestemd met het voorstel voor de Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven. Onder deze wet wordt het voor luchtvaartmaatschappijen verplicht om passagiersgegevens af te staan aan een nieuw op te richten passagiersinformatie-eenheid ("Pi-NL"). Passagiers die Nederland in- en uitreizen komen in de database van Pi-NL te staan. De gegevens worden 5 jaar bewaard, gedurende welke periode verschillende instanties (waaronder de politie en het openbaar ministerie) reisgegevens kunnen opvragen. Verschillende partijen hebben kritiek geuit op de wet, omdat deze naar hun oordeel ingrijpende gevolgen voor de privacy van passagiers heeft. Privacy First heeft het onderwerp op de agenda van het VN Mensenrechtencomité in Genève laten zetten.

https://bit.ly/2H0h4nt

Wijziging Kadasterbesluit (afscherming persoonsgegevens)
Op 1 juli 2019 is een wijziging van het Kadasterbesluit in werking getreden. Deze wijziging maakt het mogelijk om persoonsgegevens af te schermen van personen die van overheidswege door de politie beveiligd worden. Bestuursorganen, deurwaarders en notarissen kunnen (voor zover nodig voor de uitoefening van hun wettelijke taak) wel toegang krijgen tot de afgeschermde informatie.

https://bit.ly/2KUS3L6

Implementatiewetsvoorstel Richtlijn auteursrechten in de digitale eengemaakte markt
Op 2 juli 2019 is de consultatie voor het implementatievoorstel voor de recent aangenomen (en hevig bekritiseerde) Europese Richtlijn auteursrechten in de digitale eengemaakte markt geopend. In het kader van de implementatie zullen wijzigingen moeten worden doorgevoerd in de Auteurswet, de Wet op de naburige rechten en de Databankenwet. Tot 2 september 2019 konden er reacties op het voorstel worden ingediend.

https://bit.ly/2HrkRst

Wijziging Telecommunicatiewet in verband met een opt-in systeem voor telemarketing
Van 4 juli tot en met 15 augustus 2019 heeft het Ministerie van Economische Zaken en Klimaat een internetconsultatie gehouden inzake een wijziging van de Telecommunicatiewet om ongewenste telemarketing tegen te gaan. Op dit moment geldt voor telemarketing een opt-out systeem. Personen mogen derhalve ongevraagd telefonisch worden benaderd voor marketingdoeleinden, tenzij zij zich hebben ingeschreven in het Bel-me-niet-register. Het uitgangspunt in het nieuwe systeem is dat natuurlijke personen niet telefonisch mogen worden benaderd voor marketingdoeleinden, tenzij zij hiervoor uitdrukkelijk toestemming hebben gegeven (opt-in). De regeling heeft alleen betrekking op natuurlijke personen. Rechtspersonen (zoals vennootschappen, verenigingen en stichtingen) worden niet tegen telemarketing beschermd. Bedrijven zonder rechtspersoonlijkheid (zoals een eenmanszaak) vallen daarentegen wel onder de reikwijdte.

https://bit.ly/2JvAjnV

Ontwerpregeling wet kansspelen op afstand
Op 24 juli 2019 is de internetconsultatie voor de Regeling kansspelen op afstand en de Uitvoeringsregeling kansspelen van start gegaan. Al in februari van dit jaar werd de Wet kansspelen op afstand aangenomen door de Eerste Kamer. Onder deze wet wordt het mogelijk om een vergunning aan te vragen voor het aanbieden van online kansspelen in Nederland. De regelingen geven een nadere invulling aan de nieuwe wet en bevatten bijvoorbeeld concrete regels in het kader van de vergunningsaanvraag, inhoudelijke verplichtingen van de kansspelaanbieder (bijvoorbeeld wat betreft verslavingspreventie) en toezicht en handhaving.

https://bit.ly/2Zk3kxk

Verordening zakelijk gebruik van online handelsplatforms
Op 31 juli 2019 is de Verordening ter bevordering van billijkheid en transparantie voor zakelijke gebruikers van onlinetussenhandelsdiensten in werking getreden. De verordening heeft onder meer betrekking op online marktplaatsen, online winkels voor softwaretoepassingen ('app stores'), zoekmachines en sociale media. De verordening moet er specifiek voor zorgen dat dergelijke platforms transparanter en eerlijker worden ten aanzien van zakelijke gebruikers (oftewel de verkopers cq. aanbieders die het platform gebruiken). Zo wordt het voor de platforms verplicht om duidelijke en begrijpelijke voorwaarden te hanteren. Daarnaast moeten de platforms een systeem inrichten (zowel intern als extern) voor de afhandeling van klachten van de zakelijke gebruikers. Verder moet er onder meer informatie worden verstrekt over de wijze waarop producten en diensten gerangschikt worden.

https://bit.ly/2ZsbzTh

Dimmen Smolders
Juridisch adviseur

Privacy

Vijftien jaar privacy: bescherming van persoonsgegevens toen, nu en straks

Vijftien jaar privacy? 129 jaar privacy zul je bedoelen, als we tenminste het beroemde artikel The Right to Privacy van Warren & Brandeis als oorsprong kiezen. Over de ontwikkeling van de 19e eeuwse privacyrechten tot de vraagstukken waar we mee worstelen in het internettijdperk is genoeg geschreven. In het kader van vijftien jaar ICTRecht beschouwen we hier de ontwikkelingen gedurende deze periode. Waar stonden we toen, hoe heeft ons denken over privacy zich ontwikkeld en zijn we sterker of zwakker komen te staan tegenover mogelijk misbruik van onze gegevens?

Het privacyrecht als "schuilplaats van het kwaad"
Terug naar 2004. Ja, juridisch advieskantoor ICTRecht werd opgericht, maar vreemd genoeg was dat niet het belangrijkste juridische nieuws van dat jaar. We zaten midden in wat de 'strijd tegen terrorisme' heette. In reactie op de aanslagen van 11 september 2001 (en in de jaren daarna die in Madrid en Londen en de moord op Theo van Gogh) trad eerst de Wet terroristische misdrijven in werking, later volgde de Wet ter verruiming mogelijkheden tot opsporing en vervolging van terroristische misdrijven. Een vermoeden dat iemand zich bezighield met terroristische activiteiten was hierdoor voor de politie bijvoorbeeld voldoende grondslag om diegene hinderlijk te volgen, te observeren en telefoons af te tappen. De privacy-discussies betroffen in Nederland veelal de verhouding tussen staat en burger. Privacy van burgers stond pal tegenover veiligheid en er heerste een sterk idee dat die twee onverenigbaar waren. De korpschef van de Amsterdamse politie ging zelfs zover om het privacyrecht de "schuilplaats voor het kwaad" te noemen.[1]

Terugkijkend vanuit het huidige privacylandschap naar vijftien jaar geleden lijkt het alsof commercie nog maar amper een bedreiging voor de privésfeer vormde. In het jaarverslag 2004 van het College bescherming persoonsgegevens, komt de term social(e) media nog niet voor.[2] Zelfs 'Internet' speelt blijkens dat jaarverslag nog slechts een bijrol. In plaats daarvan overheersen onderwerpen als het verplicht bewaren van telecommunicatie- en passagiersgegevens, cameratoezicht, identificatieplicht en landelijke zorgregistraties. De overheid domineerde het nieuws als mogelijke privacy-schender. Hyves beheerde veel persoonlijke gegevens, maar die plaatste je toch allemaal zelf online. Facebook moest zich nog ontpoppen tot de schandalenfabriek die het nu is. Van Cambridge Analytica-achtige applicaties was nog geen sprake, hooguit van knullige beveiliging. In die jaren maakten we nog maar net kennis met gepersonaliseerde advertenties, wat uiteindelijk toch ook voordelen had, zo vonden we. 2004 was wel het geboortejaar van de eerste Nederlandse anti-spamwet; we werden dus al wel (een beetje) beschermd tegen massale ongewenste e-mails.

Privacy in een stroomversnelling
Gaandeweg zijn we heel anders – en vooral méér – over privacy in de online-wereld gaan denken. In het

Privacy-jaarverslag 2003-2004 van internetbedrijf XS4ALL wordt vermeld "dat XS4ALL twee problemen moest oplossen op privacy-gebied; de zichtbaarheid van accountnamen op shellservers en het verwijderen van verouderde administratieve gegevens".[3] Twee problemen op privacygebied, wat een luxe! Anno 2019 worden privacy en security bij grote bedrijven gewaarborgd door 'multidisciplinaire teams' met daarin exotische soorten als *privacy champions*, auditors, ethische hackers en een *Computer Emergency Response Team*. Er hangen vandaag de dag natuurlijk ook boetes van miljoenen euro's boven het hoofd, dus je moet wat.

Deze ontwikkeling heeft in Europa natuurlijk alles te maken met de komst van de AVG. Hoewel het eerste voorstel hiervoor al uit 2012 stamt, bleek de urgentie voor scherpere wetgeving in Europa ineens extra hoog dankzij de onthulling door Edward Snowden van het schandaal rond de Amerikaanse inlichtingendienst NSA in 2013. Uit de 'leaks' van Snowden bleek dat de VS geen veilige plek is voor persoonsgegevens van EU-burgers. De AVG zorgde dat persoonsgegevens – in elk geval wettelijk – overal binnen de Europese Economische Ruimte veilig en netjes verwerkt moeten worden. Op het uitvoeren van persoonsgegevens naar buiten de EER kwam een algemeen verbod, met enkele mechanismen als uitzondering daarop.

Voor zover we weten is het PRISM-programma van de NSA, om zo'n beetje de hele wereld af te luisteren, niet ineens gestaakt. Als gevolg is er nu een strijd gaande om elk mechanisme wat de uitvoer van persoonsgegevens naar de VS in het algemeen mogelijk maakt, onwettig te verklaren. Dankzij deze strijd, met Max Schrems voorop, zijn de Safe Harbour-principes al gesneuveld. Het Europees Hof zal naar verwachting volgend jaar oordelen of het *Privacy Shield* raamwerk een geschikt alternatief is. In de tussentijd bouwen veel grote bedrijven, terecht, hun privacybeleid rondom de nieuwe standaarden die de AVG heeft neergezet.

Big Tech & big hacks

Zo komen we bij het fenomeen *'Big Tech'*: miljardenbedrijven die zich in de afgelopen vijftien jaar in sleutelposities hebben gemanoeuvreerd op internet. Google, Facebook, Amazon, Apple en Microsoft bepalen voor een groot deel het online landschap van consumenten en beheren als gevolg daarvan gigantische hoeveelheden persoonsgegevens. Naast het delen van gegevens met de Amerikaanse overheid hebben dergelijke

bedrijven ook elk hun eigen manieren gevonden om de privacy van gebruikers te verkwanselen. Bij elke fabrikant van smart speakers luisteren bijvoorbeeld medewerkers mee naar de gebruikers, weten we inmiddels na de nodige ophef daarover. Naar Facebook lopen in Ierland alleen al acht onderzoeken onder de AVG en ook in de VS en Canada lopen onderzoeken naar uiteenlopende schendingen van de privacy van gebruikers. Al deze *Big Tech*-bedrijven zullen in de toekomst op zoek moeten naar de balans tussen massale dataverzameling en privacy-bescherming.

Alle goede of kwade intenties van bedrijven daargelaten: grootschalige hacks worden ook steeds meer een factor van betekenis.[4] Treurig genoeg worden er anno 2019 nog steeds wachtwoorden, creditcardgegevens en paspoortgegevens opgeslagen zonder versleuteling. Moeten we in de toekomst er rekening mee houden dat het periodiek wijzigen van je creditcardnummer even gebruikelijk wordt als dat nu is bij je wachtwoorden?

Positieve ontwikkelingen

Tegelijk met de toename van kansen om op grote schaal met gegevens aan de haal te gaan, zijn er gelukkig ook ontwikkelingen die positief gaan stemmen. Zo zijn er met onder meer Japan, Israël, Nieuw-Zeeland, Uruguay, Argentinië en Canada al heel wat zogeheten 'adequate landen' aangewezen waar het veilig wordt geacht om persoonsgegevens vanuit de EU naartoe te exporteren. Zelfs in de VS, waar privacy notoir laag op de politieke agenda staat, neemt de roep om regulering langzaam toe. De recente ervaring in Europa leert dat het privacy-bewustzijn ook bij de bevolking behoorlijk toeneemt in navolging van strengere wetten. Als de explosieve toename van het aantal meldingen bij de AP een indicator is van hoezeer privacy is gaan 'leven', worden burgers daadwerkelijk steeds alerter op misbruik van persoonsgegevens.[5]

Ook op technologisch vlak staat de privacywereld niet stil. Met name blockchain wordt vaak aangehaald als technologie die privacy op grote schaal kan bevorderen. Inherent aan blockchain is bijvoorbeeld de mogelijkheid om de 'betrouwbaarheid' van een wederpartij te toetsen aan een onveranderlijke database waarvan iedereen samen de beheerder is. Overheden zijn met deze vorm van privacy, begrijpelijkerwijs, niet erg blij. Toch kan block-chain-technologie ook op minder duistere manieren waardevol blijken voor privacy-doeleinden. *'Smart'* of zelfs *'secret contracts'* zijn nu nog verre van toepasbaar op grote schaal, maar de achterliggende technologie biedt ongetwijfeld kansen. Verder kan de burger altijd nog zelf zijn best doen om niet 'herkend' te worden, bijvoorbeeld door bonuskaarten uit te wisselen om het opbouwen van profielen te verstoren.[6]

Weet u wel wie ik ben?

We wagen ons maar niet aan voorspellingen voor over vijftien jaar. Hadden we in 2004 ook maar enigszins kunnen voorzien hoe de wereld er in 2019 uitziet, als het op privacy aankomt? We kunnen constateren dat als het privacyrecht vijftien jaar geleden al de schuilplaats van het kwaad was, die schuilplaats nu wettelijk gezien een stuk groter is geworden. Tegelijk is de economische waarde van persoonsgegevens steeds meer duidelijk geworden. Organisaties 'kennen' ons steeds beter, zowel als totale, geaggregeerde groep met al onze gedragingen als op individueel niveau. Of de volgende generaties allemaal privacy-activisten zullen zijn, valt te betwijfelen. Maar ze zullen de beschikking hebben over sterkere wapens in de strijd tegen misbruik van hun gegevens. De vraag is in hoeverre overheden en bedrijven er een wapenwedloop van maken. Maar een andere vraag die, bijvoorbeeld door filosoof Maxim Februari, terecht wordt gesteld is: in hoeverre is de mens in data te vangen?[7] Zodra er een algoritme bestaat wat het ons kan voorspellen hoor ik het graag.

1 https://bit.ly/2lQO5ci
2 https://bit.ly/2mZ5Pmq
3 https://bit.ly/2n1oCxr
4 https://bit.ly/2BT9s2r
5 https://bit.ly/2n1qVR7
6 https://bit.ly/2kIPCBk
7 https://bit.ly/2kIPIca

Iris de Groot
Juridisch adviseur

Privacy | Marketing | Overheid

Een portret van een werknemer in een reclame-uiting, mag dat?

Regelmatig worden er portretten van werknemers voor reclame-uitingen gebruikt. Dit kan echter niet zomaar. Het publiceren van andermans foto verdient enige zorg. Als een geportretteerde namelijk wordt afgebeeld zonder dat hij hiervoor toestemming heeft gegeven kan hij zich tegen de publicatie van de foto verzetten op grond van het Portretrecht (artikel 21 Auteurswet).

Niet bij alle reclame-uitingen wordt toestemming aan de geportretteerde gevraagd. Zo blijkt ook uit een zaak van 22 mei 2019[1], waarbij PostNL (in de zaak aangeduid als Logistics) het niet zo nauw heeft genomen met de toestemmingsvraag. In deze zaak constateert de eiser dat er sinds 2013 foto's van hem worden gebruikt op de website van PostNL. Later, vanaf 2014 zijn deze foto's zelfs gebruikt voor bestickering op busjes en vrachtwagens. Volgens eiser zou dit zonder zijn toestemming zijn gebeurd. PostNL geeft daarentegen aan dat er wel degelijk sprake is van toestemming.

Toestemming

Toestemming voor het publiceren van een foto van de geportretteerde kan zowel expliciet als impliciet. Hierbij is wel van belang dat de gebruiker van de foto er voldoende zeker van is dat de toestemming van geportretteerde ook daadwerkelijk voor die publicatie is gegeven. De gebruiksvorm moet dus te voorzien zijn. De rechtbank geeft bij de PostNL-zaak aan dat de vraag of toestemming geacht wordt te zijn verleend, beoordeeld moet worden aan de hand van het algemene overeenkomstenrecht.[2] Van belang is wat partijen in de gegeven omstandigheden over en weer redelijkerwijs van elkaar mochten verwachten.

Eiser stelt dat de foto's specifiek zijn gemaakt voor intern gebruik ten behoeve van een presentatie aan medewerkers over een nieuwe bedrijfstak van PostNL en niet voor de promotionele of commerciële doeleinden waarvan in het onderhavige geval sprake is. Volgens PostNL was er sprake van een onbeperkte toestemming. Het is echter aan PostNL om deze toestemming te bewijzen.[3] Aangezien de schriftelijke vastlegging van de toestemming ontbreekt, slaagt PostNL niet in deze bewijslevering. Daarbij ontbreekt de reikwijdte van de gegeven toestemming. Of zoals de rechtbank verwoordt:

"Of toestemming geacht moet worden te zijn verleend en zo ja, onder welke voorwaarden dient te worden beoordeeld aan de hand van het algemene overeenkomstenrecht. Daarbij komt het aan op de zin die partijen in de gegeven omstandigheden over en weer redelijkerwijs aan elkaars verklaringen en gedragingen mochten toekennen en op wat zij te dien aanzien redelijkerwijs van elkaar mochten verwachten. Op grond van het bepaalde in artikel 150 Rv, rust bovendien op Logistics de bewijslast van dit bevrijdend verweer. De kantonrechter constateert dat de door [eiser] gegeven toestemming niet schriftelijk is vastgelegd en dat partijen

twisten over de reikwijdte van de gegeven toestemming. De kantonrechter overweegt in dit kader dat toestemming tot het portretteren niet gelijk kan worden gesteld met toestemming tot publiceren. Dat [eiser] zich op een bepaalde manier heeft laten portretteren, betekent dan ook niet dat hij daarmee toestemming voor heeft gegeven voor het (onbeperkte) gebruik van zijn portret door Logistics. Nu op Logistics voorts geen begin van bewijs heeft geleverd dat door [eiser] onbeperkte toestemming is verleend en hiervan overigens ook geen bewijs heeft aangeboden, faalt het verweer van Logistics dat [eiser] toestemming heeft verleend voor het bestreden gebruik van zijn portret."

De rechtbank geeft in deze zaak dus ook aan dat de toestemming voor het maken van een portret niet gelijk staat aan de toestemming tot publicatie. Ook niet als eiser zich op een bepaalde manier heeft laten portretteren. Vooral bij impliciete toestemming moet voor beide partijen dus duidelijk zijn wat het doel van het portret is.

Redelijk belang

Het is vervolgens de vraag of de geportretteerde wel een "redelijk belang" heeft om zich te verzetten tegen de publicatie van zijn portret. Een voorbeeld van een redelijk belang is het recht op privacy, bescherming van eer en goede naam en/of een financieel belang.

Het gaat in dit geval om een reclame-uiting, waarbij eiser samen met een collega centraal staat. Al sinds 1997 geldt dat de geportretteerde in beginsel een redelijk belang heeft zich te verzetten tegen het gebruik van zijn portret ter ondersteuning van een commerciële reclame-uiting.[4] Het gebruik van een portret voor reclame-uitingen wordt namelijk aangemerkt als een inbreuk op de persoonlijke levenssfeer van de geportretteerde.[5] Aangenomen wordt immers dat de geportretteerde door het publiek geassocieerd wordt met het betreffende product of de dienst. Het publiek zal ervan uitgaan dat er toestemming is gegeven voor het portret en de publicatie het opvatten als een blijk van publieke ondersteuning van het product of de dienst door de geportretteerde. Dit maakt dat de geportretteerde zich tegen de openbaarmaking kan verzetten.

Belangenafweging

Het redelijke belang van de geportretteerde moet wel worden afgewogen tegen andere belangen, met name het belang van de informatievrijheid (artikel 10 EVRM)[6]. Het privacy-grondrecht is namelijk niet per definitie verheven boven deze informatievrijheid. Hieronder behoren ook commerciële belangen van bedrijven. Dat bij deze zaak sprake was van een reclame-uiting weegt daarom ook zwaar bij de belangenafweging. PostNL had alleen wel moeten

aangeven waarom het gebruik van het portret de inbreuk op de persoonlijke levenssfeer van de eiser rechtvaardigt. PostNL heeft dat nagelaten. Dit betekent dat het belang om reclame te maken voor de aangeboden diensten van PostNL niet zwaar genoeg weegt bij deze belangenafweging.

Commerciële belangen
Het maakt in dit geval niet uit of de foto's wel of niet schadelijk zijn voor de reputatie en/of dat eiser geen verzilverbare populariteit geniet.[7] Dit is bijvoorbeeld wel van belang als het gaat om portretten van bekende personen. Zij kunnen zich tegen een openbaarmaking van een portret verzetten als dit gebeurt zonder toestemming en zij daar geen vergoeding voor ontvangen. Dit is al in 1979 in het Schaep met de 5 Pooten-arrest bepaald.[8] Hierbij kan het dus een belangrijke rol spelen of de geportretteerde een redelijke vergoeding is aangeboden. Daarbij moet de vergoeding in ieder geval recht doen aan de mate van populariteit en/of bekendheid van de geportretteerde en in overeenstemming zijn met de waarde van zijn exploitatiebelang.[9] De geportretteerde moet namelijk mee kunnen delen in de voordelen van de exploitatie.

Redelijke vergoeding
Uit een zaak uit 2013 blijkt namelijk dat als er een redelijke vergoeding is aangeboden, er bijkomende omstandigheden vereist zijn voor een onrechtmatige publicatie.

"Indien vaststaat of onbetwist is dat een redelijke vergoeding is aangeboden (en bescherming van privacy-belangen niet aan de orde is), zullen in beginsel bijkomende omstandigheden nodig zijn voor het oordeel dat openbaarmaking jegens de geportretteerde onrechtmatig is. Deze omstandigheden zullen door de geportretteerde gemotiveerd gesteld dienen te worden. Gedacht kan bijvoorbeeld worden aan de situatie dat de publicatie afbreuk doet aan of schadelijk is voor de wijze waarop de geportretteerde zijn bekendheid wenst te exploiteren."

Wat precies onder "redelijke vergoeding" moet worden verstaan is afhankelijk van de omstandigheden van het geval. Uit de zaak tussen Mavic en Karakter[10], waarbij foto's van Max Verstappen werden gebruikt voor een autobiografie, lijkt bijvoorbeeld te volgen dat een redelijke vergoeding mede afhankelijk is van de verkoopcijfers, in dit geval van het uitgegeven boek.

Schadevergoeding
Het oordeel in de zaak van PostNL luidt dat het gebruik van de foto van de geportretteerde op de transportmiddelen van PostNL, op het internet en in een reclamefilmpje onrechtmatig is. De publicaties maken inbreuk op het portretrecht van eiser. Eiser had zelf de schade begroot op €10.000. De rechtbank vindt dit echter aan de hoge kant en meent dat het deels ook aan eiser zelf te wijten is dat de foto met zijn portret en de videobeelden van hem inmiddels langdurig gebruikt zijn. Vandaar dat de rechtbank de schade vaststelt op een bedrag van €5.000.

Conclusie
Het gebruiken van een portret van een werknemer mag. Werkgevers hebben alleen wel altijd toestemming van de werknemers nodig om portretten te gebruiken. Van belang is dat bij het vragen van toestemming de werkgever ervoor zorgt dat de toestemming is gegeven voor een specifieke publicatie, bijvoorbeeld een reclame-uiting op een bepaald medium. Voor zowel de werkgever als de werknemer moet het gebruik te voorzien zijn. Verstandig is om deze toestemming schriftelijk vast te leggen, zodat er geen verwarring ontstaat.

1 Rechtbank Noord-Holland 22 mei 2019, ECLI:NL:RBNHO:2019:4245.
2 In het bijzonder titel 2 Boek 3 Burgerlijk Wetboek en vgl. HR 13 maart 1981, ECLI:NL:HR:1981:AG4158, NJ 1981/635 (Haviltex).
3 Op grond van artikel 150 Rechtsvordering.
4 HR 2 mei 1997, ECLI:NL:HR:1997:ZC2364, NJ 1997,661, (Discodanser), r.o. 3.3.
5 Dit is in strijd met artikel 8 Europees Verdrag voor de Rechten van de Mens (EVRM).
6 HR 21 januari 1994, ECLI:NL:HR:1994:ZC1240, NJ 1994/473 (Moordenaar G.J. Heijn).
7 Verzilverbare populariteit betekent dat iemand zodanig bekend is dat hij voor het gebruik van zijn portret een vergoeding zou moeten krijgen.
8 HR 19 januari 1979, ECLI:NL:PHR:1979:AC6461, NJ 1979/383 ('t Schaep met de Vijf Pooten).
9 HR 14 juni 2013, ECLI:NL:HR:2013:CA2788 (Cruijff/Tirion).
10 Rb. Amsterdam 6 december 2017, ECLI:NL:RBAMS:2017:8990 (Mavic/Karakter).

Matthijs van Bergen
Directeur Legal ICT

Derk Jan Pilat
Stagiair

Cloud | Innovatie | Overheid

5G: evolutie of revolutie?

In 2020 is het dan eindelijk zover: dan staat de definitieve afronding van de 5G-standaard gepland. Ondertussen zijn de eerste telefoons die 5G ondersteunen al te koop en heeft stadstaat Monaco zelfs al de primeur van een 'landelijk dekkend' 5G-netwerk. Maar wat gaat 5G ons brengen? En wanneer kunnen we het in Nederland verwachten?

Hoe werkt 5G en wat kunnen we ermee?
5G is de benaming voor de vijfde generatie standaarden voor mobiele netwerken sinds het ontstaan van mobiele telefonie kort na de tweede wereldoorlog. Net zoals zijn voorgangers maakt 5G het mogelijk dat mobiele apparaten, op afstand van elkaar, draadloos data kunnen uitwisselen. Hiervoor worden radiosignalen van en naar (5G) zendmasten verzonden die verspreid (zullen) staan over het land. De lidstaten van de Europese Unie hebben afgesproken dat deze radiosignalen over drie frequentiebanden zullen worden verzonden, namelijk 700 MHz, 3,5 GHz en 26 GHz. Het verschil tussen deze banden is dat de hoge frequentie van 26 GHz enorme datasnelheden aankan, maar een beperkt bereik heeft. Dat terwijl de lage frequentie van 700 MHz veel dekking levert, maar minder data door kan geven. De 3,5 GHz band geldt als gulden middenweg en lijkt het meest gebruikt te zullen worden in 5G-netwerken.

De grootste belofte van 5G lijkt het faciliteren van geheel nieuwe mogelijkheden, zoals zelfrijdende auto's en allerlei Internet of Things (IoT) toepassingen. Dergelijke toepassingen kunnen bij uitstek profiteren van de grotere capaciteit en stabiliteit die 5G belooft. Tegelijkertijd vergen dergelijke toepassingen ook een hoger niveau van veiligheid, omdat de impact bij uitval of verstoring nog vele malen groter zal worden dan bij huidige netwerken en toepassingen.

Ook reeds bestaande en veelgebruikte toepassingen, zoals online streaming en videobellen, zullen uiteraard aanzienlijk beter worden met 5G. In dit opzicht is 5G eerder te zien als evolutie dan revolutie, gezien 4G dergelijke toepassingen ook al goed ondersteunt. Ook virtual reality en augmented reality toepassingen zullen goed gebruik kunnen maken van 5G. Een echte doorbraak van dergelijke diensten voor het grote publiek laat nog altijd op zich wachten, dus wellicht dat 5G daar een bijdrage aan kan leveren.

Chinese spionage?
De nieuwe toepassingen zoals zelfrijdende auto's en de grote verbondenheid die van 5G worden verwacht, stellen zoals gezegd hogere eisen aan de beveiliging en stabiliteit van het netwerk. De grootste leverancier van 5G-apparatuur, het Chinese Huawei, ligt echter onder vuur wegens veronderstelde 'achterdeurtjes'. Zo gaf de directeur-generaal van de AIVD dit voorjaar tijdens de presentatie van het jaarverslag aan dat Nederland heel voorzichtig moet zijn bij het aanschaffen van Chinese apparatuur voor de 5G-netwerken.

Naar aanleiding van ongerustheid die was ontstaan binnen de Tweede Kamer door de perikelen rondom Huawei, heeft een speciale taskforce onder leiding van de Nationaal Coördinator Terrorismebestrijding en Veiligheid een risicoanalyse uitgevoerd naar de kwetsbaarheid van de Nederlandse telecommunicatienetwerken voor misbruik via leveranciers van de benodigde technologie. Een van de uitkomsten van deze analyse is dat leveranciers van diensten en producten in kritieke onderdelen van het netwerk moeten voldoen aan extra hoge eisen met betrekking tot de veiligheid en integriteit van de netwerken. Dit najaar zal een algemene maatregel van bestuur worden gepubliceerd, waarin deze aanvullende eisen zijn vastgelegd.

Hoewel het risico van spionage en sabotage bij Huawei-apparatuur vooralsnog niet met concreet bewijs lijkt te zijn aangetoond en de kans bestaat dat het in werkelijkheid meer om economische geopolitieke belangen gaat dan puur security, is het verstandig voor telecomaanbieders om de risico's zoveel mogelijk te beperken en alvast te anticiperen op de extra hoge eisen. Dit kan bijvoorbeeld door (eigen) encryptie toe te passen en niet gebruik te maken van één enkele leverancier. KPN heeft bijvoorbeeld aangegeven alleen Huawei-apparatuur in te zetten voor minder gevoelige onderdelen in zijn nieuw aan te leggen 5G-netwerk. Voor de vernieuwing van de kern van het netwerk willen ze alleen 'westerse leveranciers' gaan gebruiken.

Afluisterpark inlichtingendienst
Ook onze eigen inlichtingendiensten zitten uiteraard niet stil. Zo heeft het Ministerie van Defensie sinds 2005 een grondstation gevestigd nabij het Friese Burum, dat wordt ingezet om satellietcommunicatie te onderscheppen voor de inlichtingendiensten.
Dit afluisterpark heeft boven de denkbeeldige lijn Amsterdam – Zwolle de 3,5 GHz-band volledig in gebruik. Gezamenlijk gebruik van deze band in Noord-Nederland is onmogelijk, zonder invloed op de nationale veiligheid enerzijds of het volledig kunnen benutten van 5G anderzijds. Het kabinet heeft daarom besloten dat het noodzakelijk is om het park naar het buitenland te verplaatsen.

5G in Nederland
Op dit moment is 5G in Nederland alleen nog in kleine 'proeftuinen' beschikbaar. Rondom de Johan Cruijf ArenA is bijvoorbeeld onderzoek gedaan naar verbetering in crowd management met de inzet van het snellere netwerk. Een landelijk 5G-netwerk laat nog even op zich wachten, want eerst moet er nog een verdeling plaatsvinden van de frequentieruimte. Dit zal worden gedaan door middel van twee rondes met veilingen van vergunningen: eind 2019/begin 2020 de 700, 1400 en 2100 MHz banden en eind 2021/begin 2022 de 3,5 GHz band. De 26 GHz band zal voorlopig nog niet worden geveild in Nederland.

De regering heeft bepaald dat er in Nederland minimaal drie partijen 5G moeten gaan aanbieden aan bedrijven en consumenten. De verwachting is dat dit de huidige drie grote telecomproviders zullen zijn: KPN, T-Mobile en VodafoneZiggo. Om de concurrentie op de telecommarkt te waarborgen, kunnen deze marktpartijen over maximaal 40% van het totaal aan beschikbare frequenties beschikken. Daarnaast moeten ze in elke gemeente een dekking van 98% garanderen. Aan de uiterste randen van dit dekkingsgebied gelden snelheden van 8 Mb/s (in 2022) en 10 Mb/s (in 2026) als absoluut minimum.

De start van de uitrol in Nederland wordt in 2020 verwacht, waarbij de steden en verkeersaders het eerst aan de beurt zullen zijn. Het buitengebied zal (aanzienlijk) langer geduld moeten hebben. Van de 5G-snelheden op het platteland mag ook aanzienlijk minder verwacht worden dan in de stad.

Meer antennes
De hogere datasnelheden van 5G zijn alleen mogelijk met significant meer antennes die dichterbij de gebruikers van de diensten staan. Steden hebben nu echter al te maken met schaarste van het aantal opstelpunten. De regering wil deze schaarste deels oplossen met wijzigingen in de Telecommunicatiewet (ter implementatie van de Europese Telecomcode), die het makkelijker moet maken om kleine antennes te plaatsen op publieke infrastructuur, zoals lantaarnpalen, bushokjes en gebouwen. Daarnaast zullen de Rijksoverheid, gemeenten en aanbieders van mobiele telefonie in een nieuw antenneconvenant – de huidige verloopt eind 2019 – afspraken moeten maken over de plaatsing van (vergunningvrije) antennes voor het nieuwe netwerk. Hierbij zullen de nodige afwegingen moeten worden gemaakt tussen ruimtelijke ordening en connectiviteit.

Jay Remmelzwaal
Juridisch adviseur

Demi Grandiek
Juridisch adviseur

Privacy Contracteren

Bent u voorbereid op de Wet Arbeidsmarkt in Balans?

De Wet Arbeidsmarkt in Balans (WAB) zorgt ervoor dat het arbeids- en het socialezekerheidsrecht per 1 januari 2020 op de schop gaat. De huidige vormgeving van de arbeidsmarkt knelt in de visie van het kabinet voor werkgevers én voor werknemers. Door de kosten en risico's die verbonden zijn aan het vaste contract, zijn werkgevers terughoudend om werknemers in vaste dienst te nemen. Het doel van de wet is om het aantrekkelijker te maken om vaste werknemers in dienst te nemen. De veranderingen door de WAB kunnen ook van invloed zijn op uw organisatie. Wees daarom voorbereid. Wat zijn de belangrijkste veranderingen?

Ketenregeling
Momenteel regelt de ketenregeling dat er gedurende 2 jaar, 3 opeenvolgende arbeidsovereenkomsten gesloten mogen worden, zonder dat er een arbeidsovereenkomst voor onbepaalde tijd ontstaat. Per 1 januari 2020 wordt de termijn van 2 jaar veranderd naar 3 jaar. Het aantal opeenvolgende arbeidsovereenkomsten (3) blijft hetzelfde. Door verruiming van de termijn van 2 jaar naar 3 jaar, wordt het mogelijk om werknemers langduriger bij dezelfde werkgever te laten werken met een tijdelijke arbeidsovereenkomst. Hierdoor wordt voorkomen dat flexwerkers onnodig snel hun baan verliezen. De veranderingen gaan per 1 januari 2020 direct in. In de praktijk betekent dit dat een werkgever de komende tijd dient op te letten op welke datum de arbeidsovereenkomst die wordt aangeboden eindigt. Ligt de einddatum van het tijdelijke contract nog in 2019, dan dient een werkgever rekening te houden met de huidige termijn van 2 jaar. Ligt die einddatum in 2020, dan dient een werkgever rekening te houden met de nieuwe termijn van 3 jaar.

Mogelijkheden voor een bepaalde tijd contract Cumulatiegrond
Op dit moment kennen we een gesloten ontslagstelsel. Dat wil zeggen dat werkgevers een werknemer alleen kunnen ontslaan indien er een ontslaggrond aanwezig is. De ontslaggronden zijn limitatief in de wet opgesomd. In de ontslagpraktijk betekent het dat een werkgever een uitgebreid ontslagdossier moet hebben. Per 1 januari 2020 kunnen rechters gebruik maken van de zogeheten cumulatiegrond, zodat er maatwerk geboden kan worden in ontslagprocedures waarbij geen sprake is van een volledige ontslaggrond. Dit betekent dat wanneer de omstandigheden niet voldoende zijn voor één ontslaggrond, maar de kantonrechter tóch van mening is dat van de werkgever niet kan worden gevraagd dat hij de arbeidsovereenkomst voortzet, verschillende ontslaggronden bij elkaar kunnen worden opgeteld. Denk bijvoorbeeld aan een werknemer die niet goed functioneert, maar waarbij het ontslagdossier niet goed is opgebouwd en dit dus niet voldoende kan worden bewezen. Als hier nog eens bij komt dat werkgever en werknemer een verstoorde arbeidsrelatie hebben en niet samen door een deur kunnen, kan dit samen vanaf 1 januari 2020 tóch voldoende zijn voor een rechtsgeldig ontslag door de kantonrechter. Daar staat dan wel tegenover dat de kantonrechter de mogelijkheid heeft om een hogere vergoeding toe te kennen aan de werknemer van maximaal 50% van de transitievergoeding, bovenop de transitievergoeding en billijke vergoeding.

Oproepcontracten
De WAB is daarnaast bedoeld om de positie van oproepkrachten te versterken. Maakt een werkgever gebruik van oproepkrachten? Dan dient deze werkgever per 1 januari 2020 minstens 4 dagen van tevoren de roosters schriftelijk (waaronder ook elektronisch) persoonlijk aan de oproepkrachten mede te delen, anders is de oproepkracht niet verplicht om te komen werken. Wijzigt een werkgever binnen die 4 dagen voorafgaande aan de ingeplande werkzaamheden nog iets in het rooster? Dan hoeft de werknemer met de extra uren niet akkoord te gaan, en bij minder uren dient de werkgever de oorspronkelijke ingeplande uren uit te betalen. Werkgevers dienen er daarnaast vanaf volgend jaar ook rekening mee te houden dat elke medewerker die 12 maanden op basis van een oproepovereenkomst in dienst is geweest een arbeidsovereenkomst met een vaste arbeidsomvang (per week, per maand of per jaar) dient te worden aangeboden.

Een laatste belangrijke verandering voor oproepkrachten is dat zij vanaf 1 januari 2020 de arbeidsovereenkomst met een opzegtermijn van 4 dagen kunnen beëindigen.

Payrolling
Ook voor payrolling gaat de WAB wijzigingen met zich meebrengen. De bedoeling is om de voordelen van payrolling zoveel mogelijk weg te nemen. In de huidige situatie is het zo dat er verschillen kunnen zijn in arbeidsvoorwaarden tussen payrollwerknemers en werknemers die rechtstreeks in dienst zijn bij de opdrachtgever. Dit terwijl de werknemers beiden dezelfde functie en rol hebben. Payrollwerknemers zijn in dienst bij de payrollwerkgever, waardoor bepaalde arbeidsvoorwaarden uit bijvoorbeeld een cao niet hoeven te worden toegepast. Per 1 januari 2020 geldt dat aan payrollwerknemers dezelfde arbeidsvoorwaarden aangeboden dienen te worden als aan de werknemers in soortgelijke functies die rechtstreeks in dienst zijn bij het bedrijf. Om dit te kunnen verzorgen is de inlener verplicht om aan het payrollbedrijf mede te delen welke arbeidsvoorwaarden voor een specifieke werknemer zullen gelden. De inlener heeft er zelf ook een belang bij dat dit gebeurt, omdat hij aansprakelijk kan worden gesteld door de payrollwerknemer. Het is daarom aan te raden de praktische uitwerking van deze laatste eis toe voegen in de opdrachtovereenkomst.

Payrolling wordt in de wet opgenomen als definitie, waardoor geen gebruik meer kan worden gemaakt van de voordelen die gelden voor de uitzendovereenkomst. Denk daarbij aan afwijking van de ketenregeling, uitsluiting van de loondoorbetalingsplicht tijdens de eerste 6 maanden, en het automatisch eindigen van de arbeidsovereenkomst als de inlener de opdracht beëindigt. Om de impact hiervan iets te verzachten, gaat een deel van deze regels pas gelden voor een na 31 december 2019 gesloten arbeidsovereenkomst met een payrollwerknemer.

Transitievergoeding
Momenteel hebben werknemers pas na 2 jaar dienstverband recht op transitievergoeding. Per 1 januari 2020 ontstaat dit recht al vanaf de eerste dag. Besluit een werkgever een werknemer na een week te ontslaan in zijn proeftijd? Ook dan heeft de werknemer dus recht op een transitievergoeding. Hier staat tegenover dat de hogere opbouw van de vergoeding bij een dienstverband van langer dan 10 jaar komt te vervallen. Voor elke ontslagprocedure die op of na 1 januari 2020 is gestart, dient deze nieuwe rekenmethode te worden gehanteerd. Het kan dus financieel voordeliger zijn voor werkgevers om een ontslagprocedure uiterlijk 31 december 2019 te starten. Voor beëindiging van rechtswege, bijvoorbeeld in geval van een tijdelijke arbeidsovereenkomst, geldt de nieuwe regeling onmiddellijk. Wilt u gebruik maken van de huidige regeling? Zorg er dan voor dat uw verzoekschrift bij de rechtbank of aanvraag bij het UWV uiterlijk op 31 december 2019 is ontvangen.

Voor de transitievergoeding doen een aantal compensatieregelingen haar intrede. Naar verwachting gaat de compensatieregeling bij langdurige arbeidsongeschiktheid van de werknemer in op 1 april 2020 en heeft deze terugwerkende kracht tot 1 juli 2015. Op basis daarvan ontvangt de werkgever een vergoeding van het UWV voor de betaalde transitievergoeding na langdurige arbeidsongeschiktheid van de werknemer. Kleine ondernemers kunnen aanspraak maken op compensatie van de transitievergoeding, als het eindigen van een arbeidsovereenkomst verband houdt met de beëindiging van de werkzaamheden van de onderneming wegens pensionering of ziekte. Dit wordt nog nader uitgewerkt in een regeling.

WW-premie
Op dit moment is de hoogte van de WW-premie afhankelijk van de sector waarin het bedrijf werkzaam is. Om het aantrekkelijker te maken vaste werknemers in dienst te nemen, wordt de WW-premie voortaan bepaald aan de hand van het soort arbeidsovereenkomst. Bij arbeidsovereenkomsten voor bepaalde tijd dient er een hoge WW-premie te worden betaald, en bij arbeidsovereenkomsten voor onbepaalde tijd een lage. Heeft u een oproepkracht in dienst met een arbeidsovereenkomst voor onbepaalde tijd? Ook dan geldt het hoge tarief. Het verschil tussen het hoge en het lage tarief wordt ongeveer 5%.

Nb. Zoals met veel arbeidsrechtelijke regels het geval is, kan van een groot deel van bovenstaande regels bij cao worden afgeweken.

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Internetrechtspraak

Rechtbank Amsterdam 15 februari 2019
(Inbreuk software-auteursrecht)
(Gepubliceerd 4 juli 2019) Het bedrijf Wedel heeft software ontwikkeld waarmee radiostations op eenvoudige wijze radiocommercials kunnen inplannen en uitzenden. Een radiostation-exploitant heeft een licentie op deze software genomen maar zou daarbij 26 stations meer hebben aangesloten dan toegestaan was. Verweer is onder meer dat is gevraagd of deze stations toegevoegd mochten en dat stilzwijgend toestemming is gegeven vanwege uitblijven reactie. Dit verweer faalt, een professionele partij kan niet zomaar op stilzwijgen afgaan. Het dreigement van Wedel om bij niet-betaling van schadevergoeding voor de extra stations tot algehele afsluiting over te gaan is echter onrechtmatig: daardoor dreigt onevenredig grote schade voor de wederpartij, die stelt een advertentievolume van afgerond €200.000 per dag te genereren, en dat het op korte termijn voor haar onmogelijk is van de diensten van een andere dienstverlener gebruik te maken.

https://bit.ly/2n5ZBBs

Hoge Raad 9 april 2019
(Computervredebreuk bij portscannen)
Een persoon voert een portscan uit op kwetsbaarheden op de site van de aangever. Deze wist een aantal van dergelijke pogingen tot binnendringen te onderscheppen, maar kan niet uitsluiten dat andere zijn geslaagd. De scanner wordt vervolgd voor computervredebreuk, maar in de bewijsmiddelen wordt slechts gesproken van aanvallen d.m.v. “cross site scripting” en “directory traversal”, waarvan de werking niet nader is toegelicht. Dit maakt dat in het midden blijft of verdachte toegang heeft verworven door een technische ingreep of dat het bij een poging daartoe is gebleven. Volgt vernietiging en terugwijzing.

https://bit.ly/2I048ER

Gerechtshof Den Haag 16 april 2019
(Verwijdering Google onder AVG)
Een persoon wordt in een aflevering van onderzoeksprogramma Argos gefigureerd, waarbij onrechtmatige uitingen worden gedaan, zo komt vast te staan bij de rechter. Daarna eist deze persoon verwijdering van zekere zoekresultaten daarover, op grond van het vergeetrecht uit de AVG. Dit leidt tot een vonnis in eerste instantie, waartegen hoger beroep aangetekend wordt. Hoewel het vonnis ten tijde van de Wbp is gedaan, past het Hof de AVG toe vanwege diens directe werking en het verzoek van partijen daarom. Het kader blijft hetzelfde: de Costéja-uitspraak van het Hof van Justitie. Binnen dat kader wint in beginsel de privacy van de informatievrijheid, tenzij er bijzondere omstandigheden aan te wijzen zijn. Dat is in dit geval het feit dat de persoon zich nog bezig houdt in het publieke leven, met charitatieve instellingen waarbij transparantie voorop staat. Er blijkt weinig informatie beschikbaar over deze persoon, en de behoefte aan informatie in deze specifieke situatie levert dan ook zo’n bijzondere omstandigheid op. Dat er ook onrechtmatige uitingen zijn geweest, doet daar niet aan af.

https://bit.ly/2In4pC1

Rechtbank Amsterdam 8 mei 2019
(Youtube-beleid als gewijzigde omstandigheden)
Naar aanleiding van aangescherpt beleid van YouTube zijn Music Nations en Zoom.in met elkaar in conflict geraakt. Zowel Zoom.in als Music Nations stellen dat de tussen hen geldende overeenkomst is ontbonden respectievelijk dient te worden ontbonden en dat de ander gehouden is schade te vergoeden. De door Zoom.in gevorderde ontbinding wordt toegewezen: het aangescherpte YouTube beleid levert een gewijzigde omstandigheid op waarmee partijen bij het sluiten van de overeenkomst geen rekening hadden gehouden. Music Nations moet aan Zoom.in de schade vergoeden die zij heeft geleden wegens wanprestatie van Music Nations: Music Nations is tekort geschoten in de nakoming van de overeenkomst door niet op te treden tegen een te hoog aantal malafide kanalen, waardoor Zoom.in haar roll up tool is verloren, en door

niet mee te werken aan het gewijzigd beleid van YouTube inzake subnetworks. Zoom.in moet aan Music Nations de schade vergoeden die zij heeft geleden door onrechtmatig handelen van Zoom.in.

https://bit.ly/2l05z6d

Autoriteit Persoonsgegevens 18 juni 2019
(Haga-ziekenhuis)
De Autoriteit Persoonsgegevens (AP) heeft besloten aan Stichting HagaZiekenhuis een bestuurlijke boete van €460.000 op te leggen, omdat het HagaZiekenhuis in de periode van januari 2018 tot heden niet heeft voldaan en niet voldoet aan het vereiste van tweefactor authenticatie en het regelmatig beoordelen van logbestanden. Daarmee heeft zij onvoldoende passende maatregelen genomen als bedoeld in artikel 32, eerste lid, van de Algemene Verordening Gegevensbescherming (AVG). De schending van de AVG kwam aan het licht toen bleek dat diverse personeelsleden onbevoegd toegang konden krijgen tot dossiers van een bekende Nederlandse die was opgenomen in het ziekenhuis.

https://bit.ly/2l05z6d

Rechtbank Amsterdam 15 juli 2019
(Schokkende blog journalist)
Een columnist doet op zijn blog zeer grove uitspraken over een persoon. Hij stelt dat hij in deze column het 'trollen' van deze en andere personen aan de orde heeft willen stellen. Deze zouden er volgens hem alles aan doen om hem te treiteren en hem in diskrediet te brengen. Verdachte geeft als voorbeelden in de column dat hij de islamitische partner van verdachte altijd 'muzelvrouwtje' noemt en dat hij heeft voorspeld dat zij de relatie met verdachte zou beëindigen rond 17 maart, welke datum niet toevallig gelijk viel met het einde van de islamitisch voorgeschreven periode van rouw om de overleden moeder van de partner van verdachte. De uitlatingen kunnen echter niet los worden gezien van de context waarin ze zijn gebruikt, te weten een column over 'trollen', oftewel het provoceren, schelden, etc. op internet teneinde iemand in diskrediet te brengen. Anders dan de officier van justitie is de politierechter van oordeel dat verdachte hiermee wel een onderwerp aan de orde heeft willen stellen waarmee een publiek belang is gemoeid. Dat hij daarbij ingaat op zijn eigen ervaringen doet hieraan niet af. Volgt vrijspraak.

https://bit.ly/2l05z6d

Gerechtshof Den Haag 23 juli 2019
(Auteursrechtinbreuk lesmateriaal)
Vereniging GEU faciliteert exploitatie van leermateriaal voor onderwijs. Het bedrijf Snappet biedt een dienst aan basisscholen waarbij de leerlingen een tabletcomputer in bruikleen krijgen. Op de tablets is door Snappet ontwikkelde software geïnstalleerd waarmee de leerlingen oefenopgaven kunnen maken. GEU ziet de meegeleverde opgaven en materiaal als inbreukmakend. Gerechtshof wijst dit af: de punten van overeenstemming hebben betrekking op niet beschermde elementen (thema's en themawoorden, lessenstructuur (moment waarop de opgaven worden aangeboden), lesdoelen en aard van de opgaven). Wat overblijft is de overeenstemming op het niveau van de concrete opgaven. Op dat punt is de overeenstemming echter gering; er bestaan blijken het voorgaande in het oog springende verschillen. Door deze prominente verschillen is de totaalindruk van de lesmaterialen van Snappet anders dan die van de Leerroutes. Van inbreuk is geen sprake.

https://bit.ly/2n4M6Sp

Rechtbank Amsterdam 26 juli 2019
(Gebruik van formuliersysteem)
Eiser heeft op 26 juli 2018 een uitkering gevraagd op grond van de Participatiewet, en gebruik gemaakt van het aangewezen systeem Edison van de gemeente Amsterdam. De aanvraag werd incompleet ingevuld, en Edison biedt na twee dagen dan een hersteloptie die na 5 dagen verloopt. Eiser heeft deze optie niet gebruikt. Het systeem heeft hem meldingen per SMS gestuurd maar de gemeente kan niet aangeven welke

teksten daarin stonden. Daarom oordeelt de rechtbank dat geen sprake is van een fatale termijn, zodat niet voldaan is aan de zorgvuldigheidseis uit artikel 3:2 Awb voor het bestuursorgaan. Verder heeft verweerder de rechtbank niet kunnen inlichten over de betrouwbaarheid van Edison. Volgens verweerder gaat het om een nieuw geprogrammeerd systeem, maar verweerder kan niet aangeven of het systeem is gecertificeerd volgens een bepaalde norm. Evenmin kan verweerder aangeven of het systeem grondig is getest en welke bevindingen en foutmeldingen daaruit naar voren zijn gekomen. Ook is niet bekend of uitgesloten kan worden dat zich een storing in het systeem heeft voorgedaan bij de aanvraag van eiser. De rechtbank acht al deze informatie wel van belang, omdat eiser stelt dat hij na het ontvangen van het sms-bericht wel heeft ingelogd, maar dat de tweede opdracht niet klaar stond. Dit blijkt echter niet uit de log-gegevens uit het systeem. Ook heeft eiser gesteld dat hij bij het doen van de aangifte de hulp heeft gehad van een sociaal juridisch werker. Die heeft aangegeven zeer regelmatig deze aanvragen te doen en dat het hem zeer zou verbazen als hij in dit geval de standaardvragen inzake het inkomen zou hebben overgeslagen. Nu de rechtbank zich geen enkel beeld kan vormen van de betrouwbaarheid van Edison, klemt het te meer dat niet kan worden geverifieerd of aan eiser een fatale termijn werd gesteld.

https://bit.ly/2IzIB7a

HvJ EU 29 juli 2019
(Like-knop maakt medeverantwoordelijk)
Een Duitse modewebwinkel plaatst op haar site de Like-knop van Facebook. Deze knop verzamelt "onder water" allerlei persoonsgegevens van bezoekers, waarvoor Facebook als verwerkingsverantwoordelijke heeft te gelden. De bezoekers komen dit niet te weten, omdat de modewebwinkel noch Facebook hier duidelijkheid over verschaft. Het Hof van Justitie bepaalt dat een website-exploitant die een social plug-in invoegt die ervoor zorgt dat de browser van een bezoeker van die site content van de aanbieder van die plug-in opvraagt en daartoe persoonsgegevens van de bezoeker aan deze aanbieder doorzendt, als mede-verwerkingsverantwoordelijke daarbij wordt aangemerkt.

http:://curia.europa.eu, zaaknr. ECLI:EU:C:2019:629

Rechtbank Midden-Nederland 31 juli 2019
(Overname teksten webshop)
Twee webwinkels verkopen beiden spirituele sieraden en andere spirituele producten. Eiser weet 26 productenteksten aan te wijzen die gedaagde zou hebben overgenomen. Gedaagde verweert zich met onder meer de stelling dat dergelijke teksten gebaseerd zijn op informatie van de fabrikant, met feitelijke informatie over het product, zoals bijvoorbeeld materiaal, kleur, maten, oorsprong en wetenswaardigheden (zie ECLI:NL:RBARN:2009:BI0225). De rechter ziet deze teksten toch als creatief gezien er meer dan feitelijk/zakelijke teksten in staat. Vergelijkbare teksten staan op vele plaatsen, maar eiser kan de oudste datum laten zien.

https://bit.ly/2Izxnyx

Rechtbank Noord-Holland 7 augustus 2019
(Tetherverbod in strijd met AV)
Een klant van Tele2 heeft een abonnement van 2 jaar voor mobiel 4G internet en bellen. Tele2 stelt na enige tijd dat wanprestatie gepleegd is door in strijd met artikel 8.2 van de algemene voorwaarden, de simkaart te gebruiken in een ander apparaat dan een mobiele 4G telefoon, te weten in een router of dongel ("tethering"). Zij ontbindt de overeenkomst op die grond. De kantonrechter leest de AV nog eens goed. De zinsnede "Gebruik van een ander toestel dat 4G van Tele2 ondersteunt, is eveneens toegestaan in combinatie met het Tele2 Mobiel 4G abonnement." verbiedt niet tetheren an sich, de term 'toestel' kan niet zo beperkt worden gelezen dat het alleen over telefoontoestellen (en dus niet dongels) zou gaan. De ontbinding van Tele2 was dan ook onterecht.

https://bit.ly/2mZuaZk

Rechtbank Amsterdam 12 augustus 2019
(Vingerafdruk in strijd met AVG)
Schoenenwinkel Manfield voert een vingerafdruksysteem in voor de kassa's, zodat werknemers met hun vinger kunnen inloggen. Een werknemer maakt bezwaar wegens strijd met de AVG: voor gebruik van deze biometrische en dus bijzondere persoonsgegevens is geen noodzaak (artikel 9 AVG en 29 UAVG) in het kader van beveiliging of authenticatie. De rechtbank wijst dit bezwaar toe, met name omdat Manfield geen analyse of onderzoek heeft gedaan naar de mogelijke alternatieven. Gezien de situatie ligt het voor de hand dat alternatieven zoals een toegangspas, werknemerskaart of (cijfer)codes, al dan niet in combinatie met elkaar, best mogelijk zouden kunnen zijn. Grijpen naar een zwaar middel als vingerafdrukken kan dan alleen als gemotiveerd is vastgesteld dat deze alternatieven in de specifieke situatie van Manfield niet opgaan.

https://bit.ly/2P05w8D

Rechtbank Amsterdam 21 augustus 2019
(Valse creditcard)
In 2017 wordt via internet een American Express card aangevraagd op naam van gedaagde. In de periode van 1 juli 2017 tot en met 3 augustus 2017 is de charge card gebruikt voor het doen van verschillende betalingen en geldopnames, voornamelijk in het buitenland. Gedaagde heeft in Italië verbleven van 19 juli tot en met 27 juli 2017. Voor en na die periode was hij in Nederland. Wanneer hij uiteindelijk tot betaling wordt gesommeerd, stelt hij nooit de kaart te hebben afgenomen. Dat moet een ander hebben gedaan. De rechtbank acht dit niet onaannemelijk, omdat AmEx in het online aanvraagproces niet de mogelijkheid heeft ondervangen dat een ander zich heeft voorgedaan als gedaagde op het aanvraagformulier en de gegevens daarop heeft ingevuld. Ook andere factoren zoals het uitgavenpatroon in Italië ten tijde van gedaagde's vakantie daar mogen het creditcardbedrijf niet baten.

https://bit.ly/2P05w8D

Sari Jansen
Juridisch adviseur

Overheid | Cloud | Privacy

Bewaren van het medisch dossier: toen en nu

Een zorgvuldig bijgehouden dossier is van wezenlijk belang voor de kwaliteit en continuïteit van zorg aan de patiënt. Logischerwijs is het medisch dossier regelmatig onderwerp van gesprek. Met name met betrekking tot de bewaartermijn (en het aanvangsmoment daarvan) is in de afgelopen vijftien jaar het nodige onderzocht en aangepast. In dit artikel lichten we de belangrijkste wijzigingen toe en werpen we een blik op de (nabije) toekomst.

Het dossier in de wet

De Wet op de geneeskundige behandelingsovereenkomst (WGBO) regelt de algemene rechten van patiënten en de plichten van hulpverleners, wanneer er tussen partijen sprake is van een geneeskundige behandelingsovereenkomst. De inhoud van de WGBO sluit in belangrijke mate aan bij gangbare inzichten in de literatuur en jurisprudentie, zoals het uitgangspunt van onderling vertrouwen tussen patiënt en hulpverlener.[1] De regels uit de WGBO gelden vaak ook voor jeugdhulp, namelijk in het geval dat de hulp een geneeskundige behandeling is. Voor vormen van jeugdhulp die niet een geneeskundige behandeling betreffen, gelden de bepalingen uit de Jeugdwet die grotendeels gelijk zijn getrokken met de WGBO.

Eén van de belangrijkste wettelijke plichten onder de WGBO en Jeugdwet, is de verplichting van de jeugdhulpverlener om een (medisch) (cliënt)dossier in te richten.[2] Hierin worden de relevante gegevens opgenomen over de verlening van de geneeskundige behandeling en de gezondheid van de betrokkene.

Zowel in de Jeugdwet als in de WGBO is een bewaartermijn van 15 jaar voor het (medische) (cliënt)dossier opgenomen.[3] Afgelopen april is het wetsvoorstel voor wijziging van de WGBO, de Jeugdwet en enkele andere wetten ter verbetering van patiëntgerichte zorg aangenomen (hierna aangeduid als: "de Wijzigingswet").[4] In deze wet is een langere bewaartermijn opgenomen en is het aanvangsmoment van de bewaartermijn voor het dossier gewijzigd.[5] De veranderingen waren al geruime tijd aangekondigd en lagen al langer in de lijn der verwachting. De bewaartermijn van het dossier is namelijk al sinds (in ieder geval) het jaar 2000 onderwerp van gesprek.[6]

Het dossier vijftien jaar geleden

In 2004 bepaalde de WGBO dat patiëntgegevens tenminste 10 jaar bewaard moesten blijven of zoveel langer als uit de zorg van een goed hulpverlener voortvloeit. In de regel betekende dat dat hulpverleners het dossier na 10 jaar vernietigden. Dat leidde in de praktijk vaak tot problemen, bijvoorbeeld in het geval een behandeling op de langere termijn nog gevolgen bleek te hebben. Hulpverleners en patiëntenorganisaties lieten weten bezorgd te zijn dat gegevens verloren gaan die later van belang kunnen blijken voor de zorg aan de patiënt of diens verwanten.[7] De Gezondheidsraad bepleitte daarom in 2004 een wijziging van de wet en een verlenging van de bewaartermijn.[8] De raad gaf hierbij aan dat de vraag wat een goede bewaartermijn is, niet eenvoudig is te beantwoorden. Ze kon zich voorstellen dat aansluiting zou worden gezocht bij de termijn van 30 jaar die wordt genoemd in nieuwe Europese en Nederlandse regelgeving inzake kwaliteits- en veiligheidsnormen voor lichaamsmateriaal.

De door de Gezondheidsraad ondernomen inventarisatie liet zien dat 10 jaar in veel gevallen een te korte bewaartijd is. Dat hing volgens haar samen met belangrijke ontwikkelingen in de geneeskunde die sinds de periode van de wetsvoorbereiding steeds nadrukkelijker op de voorgrond waren getreden. Denk hierbij aan ziektes waaraan mensen vroeger overleden, maar die nu behandelbaar

zijn. Vaak moet men dan wel levenslang rekening houden met een verhoogd risico opnieuw ziek te worden. Ook het kunnen doen van onderzoek en het verlenen van verdere zorg bij correlaties tussen eerdere ziekten of behandelingen, waren volgens de Gezondheidsraad zwaarwegende argumenten voor het handhaven van een langere bewaartermijn.

In 2005 is gevolg gegeven aan het advies van de Gezondheidsraad en is de bewaartermijn van het medisch dossier van 10 naar 15 jaar verlengd.[9] Het ging hierbij om een voorlopige maatregel, zodat de dossiergegevens in afwachting van een definitieve regeling nog niet zouden worden vernietigd.[10] In het wetsvoorstel voor de Wet cliëntenrechten zorg is vervolgens voorgesteld de wettelijke bewaartermijn te verlengen naar 20 jaar.[11] De Wijzigingswet die dit jaar is aangenomen, is daar een direct uitvloeisel van.

Toekomst: de Wijzigingswet
De huidige WGBO en Jeugdwet bepalen dat de gegevens die in het dossier zijn opgenomen voor een periode van 15 jaar bewaard moeten worden. Deze periode begint volgens de wet te lopen op het moment dat de gegevens zijn vervaardigd. Dit kan met name praktische problemen opleveren bij dossiers van patiënten, die gedurende een langere periode behandeld worden, bijvoorbeeld bij chronisch zieken. Daarom is in de Wijzigingswet bepaald dat het aanvangsmoment van de bewaartermijn wordt gewijzigd naar het moment dat de laatste wijziging in het dossier is aangebracht. Daarnaast wordt de bewaartermijn van 15 naar 20 jaar verlengd. Deze wijzigingen zijn ingegeven vanuit het belang van een goede zorgverlening aan de patiënt, waarbij het kabinet gebruik heeft gemaakt van het eerdergenoemde advies van de Gezondheidsraad. De relevante onderdelen van de Jeugdwet worden ook in lijn gebracht met de wijzigingen.

De bewaartermijn is overigens niet absoluut. De bewaartermijn kan doorbroken worden door een verzoek tot vernietiging van de patiënt van het dossier. Daarnaast kan de hulpverlener op grond van goed hulpverlenerschap besluiten het dossier langer te bewaren dan 20 jaar, bijvoorbeeld in het geval van langlopende en terugkerende aandoeningen.[12] Het is aan de hulpverlener om geschikte maatregelen te treffen om ervoor te zorgen dat de dossiers correct bewaard blijven.

Wijzigingen naast de bewaartermijn
Naast de wijzigingen die specifiek zien op het medisch dossier, behelst de Wijzigingswet nog meer veranderingen. Er wordt verduidelijkt dat er overleg tussen de hulpverlener en de patiënt plaats moet vinden.[13] De informatieplicht van de hulpverlener wordt daarom in de Wijzigingswet aangevuld, waarbij als uitgangspunt "samen beslissen" wordt genomen. Voorts wordt een regeling opgenomen voor het inzagerecht voor nabestaanden en voormalig vertegenwoordigers in het medisch dossier van een overleden patiënt.

Inwerkingtreding
De Wijzigingswet en/of onderdelen daarvan treden in werking op een bij koninklijk besluit te bepalen tijdstip. Op dit moment is nog niet bepaald wanneer de wet in werking zal treden. Hulpverleners (en ICT-dienstverleners die een dossier in de cloud faciliteren) kunnen wel alvast anticiperen op de nieuwe bewaartermijn en hun diensten hierop inrichten. In de Memorie van Toelichting bij de Wijzigingswet is bepaald dat er sprake is van onmiddellijke werking. Dat betekent dat voor bestaande dossiers ook geldt dat deze door de wijziging langer bewaard moeten blijven.[14] Voorlopig dus maar voorzichtig omspringen met het verwijderen van dossiers.

1 Prof. Dr. H.J.J. Leenen e.a., Handboek gezondheidsrecht, Den Haag: Boom juridisch 2017, p. 101.
2 Artikel 7:454 lid 1 WGBO en artikel 7.3.8 lid 1 Jeugdwet.
3 Artikel 7:454 lid 3 WGBO en artikel 7.3.8 lid 3 Jeugdwet.
4 https://bit.ly/2n8i2Wh
5 Wet van 5 juni 2019 tot wijziging van Boek 7 van het Burgerlijk Wetboek, de Jeugdwet en enkele andere wetten ter verbetering van patiëntgerichte zorg en het opnemen van een wettelijke regeling voor het inzagerecht in het medisch dossier van een overleden patiënt.
6 In 2000 deed de Gezondheidsraad namelijk al een aanbieding aan de Minister van Volksgezondheid, Welzijn en Sport voor een signalerend advies over de bewaartermijn voor medische gegevens, zie: Gezondheidsraad. De bewaartermijn voor medische gegevens. Den Haag: Gezondheidsraad 2000, publicatienummer 2000/15.
7 W.J. Dondorp, J. Legemaate en C.J. van de Klippe, Bewaartermijn voor patiëntengegevens; Gezondheidsraad bepleit wetswijziging, Nederlands tijdschrift voor geneeskunde 14 april 2004.
8 Gezondheidsraad, Bewaartermijnen patiëntengegevens. Pleidooi voor wetswijziging, publicatienummer 2004/08. Den Haag: Gezondheidsraad 1 april 2004.
9 Wet van 22 december 2005 tot wijziging van enige bepalingen van het Burgerlijk Wetboek omtrent de overeenkomst inzake geneeskundige behandeling en van artikel IV van de wet van 17 november 1994, Stb. 837.
10 Kamerstukken II 2018-2019, 34994, nr. 6, p. 3.
11 Kamerstukken II 2009-2010, 32402, nr. 2.
12 Artikel 7:454 lid 3 WGBO.
13 Kamerstukken II 2017-2018, 34994, nr. 3 (MvT), p. 3.
14 Kamerstukken II 2017-2018, 34994, nr. 3 (MvT), p. 8.

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 juridische én technische kennis op over privacy. U leert onder meer over: datalekken, DPIA, ICT en zorg, legal tech en security.

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

"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

Gemiddeld beoordeeld met een **8**

Niveau 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.

Kijk voor meer informatie op
ictrecht.nl/academy

"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

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

Onze mensen aan het woord

Dit jaar vieren wij ons 15-jarig jubileum. Al vijftien jaar lang zetten de medewerkers van ICTRecht zich dagelijks in voor ICTRecht en hebben zij ervoor gezorgd dat ICTRecht is gegroeid tot het bedrijf dat het nu is. We geven drie medewerkers van ICTRecht het woord om onder meer te weten te komen hoe zij de groei van ICTRecht tijdens hun werkperiode hebben ervaren en hoe zij denken dat het ICT-vakgebied er over vijftien jaar uitziet.

Beryl Hetharia
Juridisch adviseur
1 jaar werkzaam bij ICTRecht

Wat ik het leukste vind aan mijn werk bij ICTRecht, vind ik lastig om te bepalen. Er zijn namelijk meerdere dingen. Zelf ben ik begonnen in het e-commerce team, waar ik me voornamelijk bezighield met webshops en online platformen. Door mijn werk bij ICTRecht heb ik meer interesse gekregen in de wet- en regelgeving op het gebied van privacy. ICTRecht ving dit op en heeft mij de kans gegeven mij daar verder in te ontwikkelen en mij aan te sluiten bij het privacy team.

De werkzaamheden die ik doe zijn heel divers zijn: van het maken van contracten tot het controleren van cookies op een website. Bedrijven komen bij ons met een bepaald idee en geven dan aan dat ze juridisch alles geregeld willen hebben. Dan moet je inventariseren wat er allemaal nodig is. We horen ook vaak dat bedrijven “AVG-compliant” willen zijn, maar niet weten hoe of wat ze moeten doen. Dan leggen wij als juridisch adviseurs uit wat er nodig is en voeren wij de werkzaamheden voor hen uit.

Als ik kijk naar mijn eigen werkzaamheden, zie ik dat we bij ICTRecht steeds meer de IT-kant op gaan door bijvoorbeeld te automatiseren. Een goed voorbeeld daarvan is het nieuw ontwikkelde Privacy Verified waarbij klanten via een online portaal hun organisatie kunnen laten controleren of ze voldoen aan de privacyregels. Het systeem geeft vervolgens aan of alles in orde is of dat er nog werk aan de winkel is.

Over 15 jaar is het ICT-vakgebied nog geavanceerder. Er wordt meer gebruik gemaakt van robots en op sommige plekken zijn er minder of zelfs helemaal geen medewerkers meer nodig. Denk aan grote fabrieken en magazijnen waar nu al robots worden ingezet, dat zal alleen maar toenemen.

Tim Wokke
Juridisch adviseur
3 jaar werkzaam bij ICTRecht

De groei van ICTRecht heeft ertoe geleid dat het bedrijf eind 2016 is verhuisd naar een prachtige locatie aan ‘t IJ. Het mooie was dat mijn eerste werkdag samenviel met het einde van deze verhuizing en ik dus begon in een spiksplinternieuw kantoor. Het eerste jaar had ik het idee dat ik maar namen van nieuwe collega’s bleef bijleren; de groei (en dus de vraag) was enorm. Al snel behoorde ik tot de 50% van de medewerkers die het langst werkzaam zijn bij ICTRecht. Ondanks dat dit toch wat vreemd aanvoelde, zag je toch dat de nieuwe collega’s (net als ik in het begin) snel hun draai vonden binnen de organisatie. Wat uiteraard een goed teken is.

Hoofdzakelijk hebben de vragen en verzoeken die ik behandel betrekking op contractwerk met een e-commerce component. Als ik terugkijk op de afgelopen drie jaar dan is de variatie in opdrachten en opdrachtgevers een van meest interessante aspecten van mijn werk. Als je dit dan in combinatie ziet met hoe ICTRecht intern te werk gaat en de opleidingsmogelijkheden die worden aangeboden, heeft dat

tot een razendsnelle ontwikkeling geleid. Het mooie aan ICTRecht als bedrijf is dat collega's en teams dicht op elkaar blijven staan - zelfs met de groei van afgelopen jaren.

De grootste ontwikkeling in het ICT-vakgebied die mij tijdens mijn werkperiode bij ICTRecht is bijgebleven, is dan toch de inwerkingtreding van de nieuwe privacyregelgeving (AVG). Dit heeft zo'n enorme impact veroorzaakt dat iedere juridisch adviseur binnen ICTRecht, ook degenen die geen onderdeel uitmaken van ons privacy team, het onderwerp niet meer kon ontlopen. Vanuit de e-commerce sector heb ik hierdoor steeds meer vraagstukken op het gebied van direct marketing, prijspersonalisatie en profilering kunnen oppakken met onze privacy specialisten.

Op juridisch vlak zal de nodige automatisering over 15 jaar hopelijk een groot deel van het repetitieve werk hebben weggenomen. Het zou namelijk toch mooi zijn als we onze tijd voornamelijk kunnen besteden aan de echt lastige onderwerpen. Qua ontwikkeling van de rechtsgebieden verwacht ik weinig verandering, op wat striktere regulering van AI en de steeds machtiger wordende platformen na. Eén ding is wat mij betreft wel zeker; over 15 jaar zullen we nog steeds zeggen dat het recht de technologische ontwikkelingen niet kan bijbenen.

Matthijs van Bergen
Directeur Legal ICT
10 jaar werkzaam bij
ICTRecht / Legal ICT

Toen ik begon met werken bij ICTRecht waren er nog geen collega's, behalve Steven en Arnoud. Ik was hun eerste werknemer. We hadden toen zelfs nog geen fysiek kantoor. Inmiddels hebben we vestigingen in Groningen, Amsterdam en Brussel. In totaal heb ik nu zo'n 60 collega's. Dat is niet in een dag gebeurd. Top aan ICTRecht vind ik nog altijd dat er veel ruimte is voor ontwikkeling en eigen initiatief. Zo heb ik de eerste internationale uitbreiding van ICTRecht in Brussel mogen verzorgen onder ons internationale label Legal ICT. Nu de vestiging is opgericht, heb ik de ruimte gekregen om een poos te gaan reizen en aan mijn proefschrift te werken. Uiteraard ben ik ook erg blij met de collega's en de sfeer onderling.

Het werk is en blijft gelukkig erg gevarieerd. De ene dag zit ik in opdracht van een Nederlands Ministerie bij één van de grootste cloudproviders ter wereld, de andere dag begeleid ik een startup met het opzetten van een e-commerce-platform voor duurzame kleding. Weer een andere dag zit ik gedetacheerd als FG bij de Sociaal-Economische Raad in Den Haag, of geef ik een training in Amsterdam aan externe deelnemers over ICT-contracten, privacy of onderhandelen. Ook help ik nog steeds een regio van samenwerkende gemeenten om een glasvezelnetwerk te realiseren.

Een hele poos terug heb ik Bits of Freedom geholpen om ervoor te zorgen dat het principe van netneutraliteit in de wet beschermd zou worden. Dankzij netneutraliteit zijn internetgebruikers vrij om zelf te bepalen welke diensten of toepassingen op internet zij willen gebruiken, of zelf aan willen bieden. Zonder wetgeving bleken internetproviders het verkeer van bepaalde online diensten of toepassingen steeds vaker anders – dus niet neutraal – te behandelen. Innovatieve diensten zoals Skype en Netflix werden vertraagd of zelfs geblokkeerd om op een oneerlijke manier hun ouderwetsere telefonie- en televisiediensten aantrekkelijker te maken.

Ik vind het nog steeds fantastisch dat het is gelukt om daar een stokje voor te steken. Nederland werd namelijk het eerste land in de EU en het tweede land ter wereld waar netneutraliteit wettelijke bescherming kreeg. Het was ontzettend gaaf om te zien hoe onze adviezen zijn overgenomen in de wet. Vervolgens heb ik als co-auteur een rapport geschreven voor de Raad van Europa (dat is de internationale organisatie waaronder het Europees Verdrag voor de Rechten van de Mens is gesloten) over hoe fundamentele rechten zoals privacy en vrijheid van meningsuiting in de praktijk beter beschermd kunnen worden door wettelijke bescherming van netneutraliteit. Ook de EU heeft uiteindelijk een zeer solide en goed opgeschreven verordening aangenomen om netneutraliteit te beschermen.

Vijftien jaar in de toekomst kijken wordt steeds moeilijker, omdat ontwikkelingen en vooruitgang in de ICT exponentieel lijken te gaan. De veranderingen volgen elkaar dus steeds sneller op en worden steeds ingrijpender. Toch zou je op een abstract niveau misschien wel kunnen zeggen dat alle ICT-ontwikkelingen in grote lijnen één kant op zijn gegaan en zullen blijven gaan.

Over 15 jaar zal de symbiose tussen mens en computer nóg inniger zijn. Dat is tegelijkertijd hoopgevend én beangstigend. Het is daarnaast te hopen dat we er de komende 15 jaar met zijn allen beter in zullen slagen om die enorme hoeveelheid gecombineerde organische en synthetische informatieopslag en -verwerkingscapaciteit in te zetten om onze planeet te redden.

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Noot bij HvJ EU 29 juli 2019 (Like-knop maakt medeverantwoordelijk)

Het is een bekend verschijnsel op niet alleen modewebwinkels, maar vrijwel iedere commerciële site: de Like-knop van Facebook. Vaak gezellig samen met Twitter, Instagram en andere social media en bedoeld voor mensen om hun (positieve) mening over het bedrijf te delen met hun volgers en vrienden. Daar lijkt weinig mis mee – drukken op die knop en een tekst samenstellen is een actieve handeling waar je echt voor moet kiezen. Echter, die knop is meer dan een knop: onder water wordt al bij het tonen van de pagina behoorlijk wat informatie verzameld en doorgestuurd naar de social media bedrijven. En dáár doet het Hof van Justitie nu een baanbrekende uitspraak over.

Like-knoppen zijn ooit begonnen als zuiver een aanklikbaar element, maar zijn uitgegroeid tot complexe stukjes software. De meeste sites bouwen zelf namelijk niet dergelijke knoppen maar gebruiken zogeheten invoegtoepassingen (plugins) die door derden zijn gemaakt om eenvoudig die knoppen toe te voegen. De site-eigenaar kan dan eenvoudig standaardteksten voorstellen, niet-gewenste diensten weglaten en via een mooi dashboard zien hoe veel en waar er wordt geklikt. Ook is hij zo verzekerd van altijd werkende knoppen, want de maker van de plugin is daarvoor verantwoordelijk.

Onder water is zo'n plugin voorzien van software (vaak Javascript-code) die automatisch wordt uitgevoerd wanneer de knop wordt getoond op de website. Deze software kan dan direct alles registreren van de bezoeker, van de pagina waar hij is tot informatie over diens computer, en natuurlijk de eventuele accountgegevens van de betreffende social media dienst. Een dienst als Facebook kan op die manier te weten komen dat gebruiker X op deze pagina is, ongeacht of X op de vind-ik-leuk-knop klikt. Dat is op zich al interessante informatie natuurlijk.

Een Duitse modewebwinkel hanteerde dergelijke knoppen, en kreeg tot haar verrassing een klacht van de Verbraucherzentrale NRW over het onrechtmatig verwerken van persoonsgegevens tegen zich. Dit leidde tot prejudiciële vragen, onder meer over de vraag wie nu verwerkingsverantwoordelijke is voor deze verwerking. Het lijkt voor de hand te liggen dat dat Facebook is, die verzamelt immers de gegevens en past die voor haar eigen doeleinden toe. De modewebwinkel kan weinig meer doen dan lijdelijk toekijken hoe dat in zijn werk gaat.

Het Hof van Justitie kijkt echter nog eens goed naar de situatie en concludeert dat we hier toch moeten spreken van gezamenlijk verwerkingsverantwoordelijkeschap (artikel 26 AVG - twee of meer verwerkingsverantwoordelijken die gezamenlijk de doeleinden en middelen van de verwerking bepalen). Dit op grond van eerdere arresten (EU:C:2018:388 en EU:C:2018:551). Het doet er daarbij niet toe, aldus het Hof, of beide partijen werkelijk gelijkwaardig samenwerken. Het is zelfs niet vereist dat beide partijen toegang hebben tot de uiteindelijk verkregen persoonsgegevens.

In dit geval deed de webwinkel niet meer dan een knop met software plaatsen waarmee Facebook toegang

kreeg tot persoonsgegevens. Maar dat is genoeg: het verzamelen en door middel van doorzending verstrekken van persoonsgegevens van de bezoekers van de modewebsite zijn twee vormen van verwerking, waar de modewebwinkel actief toe besloot door de invoegtoepassing met de knop op te nemen. Dat de website vervolgens alleen generieke informatie krijgt over haar website (93 mensen vonden dit leuk deze week), is niet relevant om dit anders te laten worden.

De verwerkingen daarna intern in de krochten van Facebook zijn echter uitsluitend de verantwoordelijkheid van Facebook zelf. Daarbij is de website geen medeverantwoordelijke.

Het Hof concludeert vervolgens dat de website-eigenaar de meest geëigende partij is om de betrokkenen te informeren (artikel 13 en 14 AVG) en de benodigde toestemming (artikel 6 sub a AVG) te verkrijgen voor de verzameling en verstrekking van de persoonsgegevens. Hij hoeft vervolgens dus niet uit te leggen wat Facebook daarmee doet, aangezien dat buiten zijn verantwoordelijkheid valt.

Wat betekent dit nu voor de praktijk? In feite is dit probleem niet nieuw, al vele jaren weten privacypuristen dat deze knoppen meer informatie doorgeven dan gewenst is. Duitse nieuwssite Heise ontwikkelde al in 2011 een privacyvriendelijk alternatief, dat nu onvermijdelijk lijkt voor iedere internetdienstverlener.

In de kern komt het erop neer dat er standaard alleen een plaatje wordt getoond van de betreffende knoppen, waarbij een en ander ook nog eens in grijstinten wordt getoond. Dit geeft aan dat de knoppen niet werken. Wie zijn muis over dit plaatje stuurt, krijgt een pop-up met uitleg dat er social media widgets ingeladen zullen worden, waarbij persoonsgegevens naar Facebook en consorten zullen worden overgebracht. Pas daarna kan men klikken, en die klik zorgt ervoor dat het plaatje wordt vervangen door de daadwerkelijke widget. Technisch is dit niet heel moeilijk te implementeren.

De oplossing van Heise (zie plaatje hierboven) gaat nog een stapje verder. Hierin kan men per button aangeven of die actief moet worden. Het schuifje links naast de knop is wat men gebruikt om de knop te activeren.

Enige nadeel van deze oplossing is dat men tweemaal moet klikken alvorens men kan aangeven iets leuk te vinden. Maar die hinder zou beperkt moeten zijn. Bijkomend voordeel is dan weer wel dat deze oplossing ook goed werkt op tablets en andere apparaten zonder muis, waarbij het immers niet mogelijk is om een tekst te tonen wanneer de cursor over de afbeelding geplaatst wordt.

Een alternatief is om dergelijke plugins in het geheel niet te gebruiken. In plaats daarvan maakt men zelf knoppen, die de gebruiker doorsturen naar de betreffende social media dienst waar het bericht dan vooringevuld klaar staat. Eigenlijk is dat precies hoe dergelijke knoppen in het begin gebouwd werden. Nadeel hiervan is natuurlijk dat er minder zicht is op het gebruik.

Hoe dan ook, er is werk aan de winkel als uw website zo'n knop heeft.

Van onze blog

Privacy

14 augustus 2019

FG, DPO, CISO, PO: wie is wie?

Het zijn veelgehoorde afkortingen: de FG/DPO, de CISO en de PO, maar drie verschillende functies. Allen privacy professionals, maar met verschillende taken en verantwoordelijkheden. Wie doet wat? En hoe verhouden de functies zich tot elkaar? Zie jij ook door de bomen het bos niet meer? In deze blog lees je meer over de verschillende functies.

FG/DPO

De Functionaris voor de Gegevensbescherming (FG) en haar Engelstalige variant Data Protection Officer (DPO) is de persoon binnen een organisatie die toezicht houdt op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG). De FG heeft een breed takenpakket, waaronder het creëren van privacy-bewustzijn in de organisatie en het actief betrokken zijn bij de wijze waarop de organisatie omgaat met gegevens. De FG/DPO fungeert als eerste aanspreekpunt voor de AP. Kenmerkend voor de FG is dat deze een onafhankelijke rol dient te behouden binnen de organisatie, maar tegelijk rechtstreekse lijnen heeft met het bestuur. De FG heeft kennis van privacywetten en -regelgeving, maar ook voldoende inzicht in en kennis van security én de processen binnen de organisatie. De FG kan een personeelslid van de verwerkingsverantwoordelijke of de verwerker zijn, of kan de taken op grond van een dienstverleningsovereenkomst verrichten.

In bepaalde situaties[1] zijn organisaties verplicht om een FG aan te stellen. Dit geldt voor publieke organisaties en overheidsinstanties, organisaties die doen aan profilering, hun personeel 'tracken' of anderszins vanuit hun kernactiviteiten op grote schaal individuen volgen of diens activiteiten in kaart brengen. Maar ook organisaties die vanuit hun kerntaak op grote schaal bijzondere persoonsgegevens verwerken, zoals gegevens over iemands gezondheid of religie zijn verplicht tot het aanstellen van een FG. Voor deze laatste categorie heeft de AP duiding gegeven over de richtlijn voor grootschaligheid[2], waaruit blijkt wanneer een zorginstelling verplicht is om een FG aan te stellen. Deze verplichting tot aanstelling geldt ook wanneer een organisatie strafrechtelijke persoonsgegevens verwerkt. Daarnaast kunnen EU-lidstaten andere situaties benoemen waarin een FG verplicht is. Meer duiding is nog niet gegeven over de verplichting tot aanstelling van een FG/DPO en het komt dan ook vaak voor dat een organisatie hierover twijfelt. Belangrijk daarbij is dat er een goede onderbouwing is waarom er wél of juist niet voor is gekozen.

CISO

Het vakgebied van de Chief Information Security Officer is nog niet vastomlijnd en verschilt per branche of organisatie. Veel organisaties hebben moeite met het vinden van een Chief Information Security Officer, ofwel CISO. Dit komt mede door het feit dat de CISO verantwoordelijk is voor het implementeren van een informatiebeveiligingsbeleid én het toezicht daarop. Net als de FG/DPO dient de persoon die deze functie bekleedt kennis en ervaring te hebben op het gebied van informatiebeveiliging, risicoanalyse, specialistische beveiligingstechnieken, én kennis van de relevante wet- en regelgeving. De CISO krijgt te maken met het bestuur, maar ook veel met de interne organisatie.

PO

De Privacy Officer (PO), ook wel: de juridisch adviseur op privacygebied die geen FG is. De PO is verantwoordelijk voor het ontwikkelen en bewaken van het privacybeleid. Tevens biedt de PO ondersteuning bij de uitvoering van dit beleid. De PO speelt een grote rol binnen de organisatie, door te fungeren als aanspreekpunt voor privacyvraagstukken die spelen in de organisatie.

1. http://bit.ly/2lxe1tG
2. http://bit.ly/2jZxFxY

De Privacy Officer zorgt ervoor dat de voor de AVG benodigde taken worden uitgevoerd en dat maatregelen worden ingebed in de organisatie. Dit doet hij in nauwe samenwerking met de FG en de CISO, indien aanwezig.

Zijn de functies wel zo verschillend?
Uit bovenstaande blijkt dat de functies op veel gebieden op elkaar lijken: privacy en security staan centraal. Waar bij de FG en de PO het houden van toezicht (FG) en de daadwerkelijke implementatie (PO) wat meer gescheiden is, geldt voor de CISO dat deze functies beide bij hem/haar liggen. Elke organisatie zal om uiteenlopende redenen kiezen voor een FG, PO en/of CISO. Dit geldt ook voor de precieze invulling en inkadering van deze functies. Uiteraard dient men zich daarbij aan de wet te houden, maar er zal in de praktijk regelmatig een FG zijn die taken van een PO op zich neemt. Idealiter blijven deze functies echter ook gescheiden. De Privacy Officer heeft een belangrijke uitvoerende rol in de organisatie en zal wellicht druk ervaren binnen de organisatie. Door dit te combineren met een onafhankelijke functie als FG, zal de invulling van de dagelijkse taken niet altijd ten goede komen. Er wordt veel gevraagd van een FG en, met name binnen de grotere organisaties, is het zeer gewenst om daarnaast één of meer PO's aan te stellen die kunnen helpen bij de uitvoerende werkzaamheden.

Ondanks de samenhang in de takenpakketten van de functies van deze privacy professionals, kunnen de functies niet zomaar voor elke organisatie worden samengevoegd. De FG dient te allen tijde de onafhankelijke positie te bewaren en de combinatie van een FG- en CISO-functie zal de onafhankelijkheid onder druk doen staan. De CISO dient in overleg met de FG tot passende beveiligingsmaatregelen te komen, waarop de FG vervolgens toezicht dient te houden. Daarom kan één persoon niet het eigen beveiligingsbeleid opstellen om deze vervolgens ook zelf te keuren: het cliché 'de slager keurt zijn eigen vlees' gaat hier dan ook op.

Verantwoordelijk
Duidelijk is en blijft dat de FG/PO/CISO niet persoonlijk verantwoordelijk zijn wanneer de AVG niet nageleefd wordt. De AVG maakt duidelijk dat het de verantwoordelijke of de verwerker is die erop toe dient te zien en moet kunnen aantonen dat de verwerking aan de voorwaarden voldoet. Naleving van regels op het gebied van gegevensbescherming is de verantwoordelijkheid van de verantwoordelijke of de verwerker en is bovendien een continue proces.

Auteur
Linde Mensink
Juridisch adviseur

15 augustus 2019

BTW en dropshipping

Dropshipping is een driehoeksverhouding tussen een webshop, consument en (dropshipping)leverancier. De webshop biedt op zijn website producten aan die hij niet zelf op voorraad heeft. Wanneer een consument een dergelijk product bestelt, dan zet de webshop deze bestelling door naar de leverancier. De leverancier verzendt vervolgens het product rechtstreeks naar de consument. Eerder schreven wij een blog over de meest voorkomende valkuilen bij dropshipping.[1] Deze bijdrage gaat in op de implicaties van btw voor Nederlandse webshops die gebruikmaken van dropshipping om Nederlandse consumenten te bedienen. Hierbij wordt gekeken naar drie verschillende levering situaties: vanuit Nederland, een EU-lidstaat en een niet-EU-lidstaat.

Btw-aangifte
Btw is een omzetbelasting die de overheid heft op de verkoop van producten en diensten. Elke ondernemer moet btw in rekening brengen over zijn verkopen, tenzij hij daarvoor is vrijgesteld. Deze vrijstelling geldt voor beroepen in bepaalde branches of specifieke werkzaamheden, zoals bijvoorbeeld medisch specialisten, erkende kinderopvang en uitvaartondernemers. Eens per maand, kwartaal of jaar doet de ondernemer aangifte van de door hem geïnde btw bij de belastingdienst. De btw die de onderneming zelf heeft moeten afdragen aan bijvoorbeeld leveranciers mag hij hiervan aftrekken.

Lees hier meer over de btw-verplichtingen voor webshops.[2]

Situatie 1: levering vanuit Nederland
Zoals in de inleiding al is aangegeven, gaat deze blog uit van een Nederlandse webshop met Nederlandse klanten. Wanneer de webshop een leverancier gebruikt die producten levert vanuit Nederland, dan is er sprake van twee betalingen mét btw-heffing. Ten eerste door de consument aan de webshop en ten tweede door de webshop aan de leverancier. Om hun webshop rendabel te houden bouwen webshops het bedrag dat de consument moet betalen (vaak) op uit allerlei posten, waaronder de inkoopkosten (bij de leverancier) en een winstmarge. De btw die de webshop zelf moet betalen aan zijn leverancier berekent een webshop hierin niet door, omdat hij deze dus kan aftrekken bij zijn periodieke btw-aangifte.

Dus stel dat een webshop een televisie koopt bij de leverancier voor €300 (incl. 21% btw á €63) en deze verkoopt aan een consument voor €400 (incl. 21% btw á €84), dan hoeft hij vanwege de aftrekmogelijkheid maar €21 (= €84 minus €63) aan de belastingdienst af te staan bij zijn periodieke btw-aangifte.

Situatie 2: levering vanuit EU-lidstaat
Wanneer de webshop een leverancier inschakelt die levert vanuit een andere EU-lidstaat, dan wordt deze levering intracommunautaire verwerving[3] genoemd. De lidstaten hebben bepaald dat dergelijke verwervingen in de andere lidstaat met 0% wordt belast. Hier staat tegenover dat dit in Nederland alsnog moet worden gedaan. Hiervoor moet de webshop de btw zelf uitrekenen en aangeven in zijn periodieke btw-aangifte. In dezelfde aangifte kan de webshop deze btw ook weer aftrekken, zodat hij per saldo niks hoeft te betalen. Net zoals in de eerste situatie zorgt de aftrekmogelijkheid ervoor dat de webshop de door hem te betalen btw niet zal doorberekenen aan de consument.

Dus stel dat een webshop een laptop koopt bij zijn Duitse leverancier voor €250 (incl. 0% btw in Duitsland) en deze in Nederland verkoopt aan een consument voor €375 (incl. 21% btw á €78,75), dan moet hij bij de btw-aangifte €52,50 (= 21% btw over €250) aangeven, welk bedrag hij ook meteen mag aftrekken. De €78,75 die door de consument is betaald moet de webshop wel afstaan aan de belastingdienst.

Situatie 3: levering vanuit niet-EU-lidstaat
Gebruik je als webshop een leverancier die levert vanuit een niet-EU-land (zoals China), dan is er geen sprake van intracommunautaire verwerving, maar van import. Bij import moet het product worden aange-

1. https://bit.ly/2mlX59V
2. https://bit.ly/2TYM4Hm
3. https://bit.ly/2lmorwc
4. https://bit.ly/2p21QCl
5. https://bit.ly/2pOeyUn

geven bij de douane en is het mogelijk dat je als webshop belasting moet betalen in het niet-EU-land. Voor deze belasting heb je geen aftrekmogelijkheid in Nederland, maar zal je moeten aankloppen bij de buitenlandse belastingdienst.[4]

Wanneer het geïmporteerde product (excl. verzend- en verzekeringskosten) meer waard is dan €22, dan moet invoer-btw worden betaald aan de douane. Indien het product wordt ingevoerd op de naam van de webshop, dan kan hij de invoer-btw aftrekken bij zijn periodieke btw-aangifte en kom je tot eenzelfde conclusie als bij de eerste twee situaties: de btw hoeft niet doorberekend te worden aan de consument. Bij dropshipping vindt de invoer echter niet plaats op de naam van de webshop, want er wordt immers direct van de leverancier aan de consument geleverd. Meestal vindt hierbij de invoer plaats op naam van de leverancier, om zo niet de consument te hoeven belasten met allerlei formaliteiten en onverwachte kosten. Als feitelijke importeur zou de leverancier dan de invoer-btw kunnen terugvragen of aftrekken per btw-aangifte aan de Nederlandse fiscus. Omdat leveranciers uit niet-EU-landen dergelijke kosten vaak al hebben verrekend in een all-in verkoopprijs aan de webshop, is dit niet interessant voor hun en blijft dit meestal achterwege. Bij deze gang van zaken wordt de invoer-btw doorberekend naar de consument óf de prijsverhoging gaat ten koste van de webshop zijn winstmarge.

Dus stel dat een webshop een tablet koopt bij zijn Chinese leverancier voor €200 (incl. Chinese btw en Nederlandse invoer-btw) en deze verkoopt aan een consument voor €350 (incl. 21% btw á €73,50), dan moet de webshop bij de btw-aangifte €73,50 afstaan aan de belastingdienst. De webshop kan de invoer-btw van €42 (21% van €200) niet aftrekken van zijn aangifte, omdat hij deze niet betaald heeft. De consument betaalt btw over een prijs waar ook al invoer-btw in verborgen zit. Daarnaast kan de webshop de Chinese btw ook niet aftrekken bij deze aangifte.

Mogelijke oplossing voor verborgen invoer-btw

Aansluitend op de invoer verricht de leverancier in de hiervoor geschetste situatie ook een levering in Nederland, namelijk aan de webshop. Het maakt hiervoor niet uit dat het product niet fysiek bij de webshop komt. Wettelijk gezien moet de leverancier hier aangifte van doen. De meeste leveranciers van buiten Europa gaan ervan uit dat zij door de invoer-btw te betalen aan al hun verplichtingen hebben voldaan. Doet de leverancier wel aangifte, dan zou hij de invoer-btw terug kunnen vorderen en aan kunnen geven dat de verschuldigde btw naar de webshop wordt verlegd.[5] Als je als webshop je leverancier zover krijgt om toch deze aangifte te gaan doen, dan is dit een mogelijke oplossing voor de verborgen btw-invoerkosten die anders op het bordje van de consument of de webshop komt.

Deze blog is geschreven door Raoul van de Laak, in samenwerking met stagiair Derk Jan Pilat.

Auteur
Raoul van de Laak
Juridisch adviseur

Trainingsoverzicht oktober – december 2019

Voor juridische professionals

Dinsdag 5 november

E-commerce: consumentenrecht en algemene voorwaarden (4PO)

Bij het (online) zakendoen wordt er veel gebruik gemaakt van algemene voorwaarden. Voor het van toepassing verklaren en wijzigen hiervan gelden specifieke regels. Bij het online zakendoen wordt er (ook) geleverd aan consumenten. Dit is in vérgaande mate dwingend gereguleerd met zeer specifieke voorschriften en heeft grote impact op bedrijfsvoering en communicatie (zoals bij de inrichting van een webshop).

https://bit.ly/2z2KRWA

Dinsdag 12 november

Privacy en persoonsgegevens: verwerkersovereenkomst (4PO)

De verwerkersovereenkomst is de juridische borging in de relatie tussen een verantwoordelijke en een verwerker in de omgang met persoonsgegevens. Vaak wordt hierbij een standaarddocument gebruikt, de uitdaging is dit te laten aansluiten bij de werkelijke situatie en de daarnaast bestaande documenten zoals SLA of licentieovereenkomst.

https://bit.ly/2EeNfy3

Donderdag 14 november

Cloud en software: elektronisch identificeren en contracteren (4PO)

Contact met overheden en het sluiten van contracten tussen commerciële partijen onderling of met consumenten vindt steeds vaker plaats op het internet. Een aandachtspunt daarbij blijft het identificeren en valideren van handtekeningen. Om het vertrouwen in, en de daadwerkelijke betrouwbaarheid van het online contracteren en ander online contact verder te vergroten, is op Europees niveau nieuwe wetgeving uitgegeven.

https://bit.ly/2yYwL8R

Donderdag 21 november

Ondernemen: verschillende klanten, verschillende aanpak (4PO)

Om ICT-ondernemers goed te kunnen adviseren, is het van belang om bekend te zijn met juridische risico's en belangen van verschillende afnemers. Wat hebben deze afnemers nodig en wat zijn de gevolgen hiervan voor de bedrijfsvoering van de leverancier? Belangrijk daarbij is de (bedrijfs-)cultuur van deze verschillende afnemers en het te verwachten technisch niveau ('ontzorgen') bij de afnemer.

https://bit.ly/31Mw7HT

Dinsdag 26 november

Contracteren: de verdieping (6PO)

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!

https://bit.ly/2rjPeqH

Dinsdag 10 december

Contracteren: onderhandelen ICT-dienstovereenkomst (4PO)

Bij ICT-dienstverlening is het contract cruciaal, nu er vrijwel geen wettelijke regelingen zijn om op terug te vallen. Minstens zo belangrijk is de wijze van onderhandelen over de dienst: wat moet worden geborgd, wat is essentieel voor welke partij, en welke terugvalposities zijn er zoal?

https://bit.ly/2PmnuwP

Voor algemeen publiek

Donderdag 24 oktober

Privacy & de overheid

Overheidsinstellingen verwerken zeer regelmatig persoonsgegevens in het kader van hun publieke taak. Hierdoor spelen privacy en de AVG een grote rol binnen de overheid. In deze dagtraining behandelen wij de algemene en specifieke privacyregels en voorwaarden die gelden voor de verwerking van persoonsgegevens door overheidsinstanties, waaronder de Baseline Informatiebeveiliging Overheid.

https://bit.ly/2YPOkaz

Donderdag 7 november

Privacy & de AVG voor administratief ondersteuners

Administratief personeel, office managers en het secretariaat hebben gedurende de dagelijkse werkzaamheden veel te maken met privacygevoelige gegevens. In de training worden de belangrijkste basisregels besproken voor administratief ondersteuners over hoe het beste kan worden omgegaan met de persoonlijke gegevens van collega's, klanten en leveranciers.

https://bit.ly/2KzARea

Dinsdag 3 december

Privacy & online marketing

Online marketing en privacy staan in de praktijk vaak op gespannen voet met elkaar. Ondanks dat, is het verwerken van gegevens voor direct marketingdoeleinden gewoon toegestaan en hoeft er niet overal toestemming voor te worden gevraagd. In deze dagtraining behandelen wij de privacyregels die volgen uit de AVG en komende privacywetgeving, en zoomen we in op concrete marketingonderwerpen.

https://bit.ly/2yYOHjw

ICT en Gezondheidsrecht

Dinsdag 29 oktober

ICT & zorg: medische gegevens (dossier gerelateerd en buiten dossier)

Binnen de zorg wordt op grote schaal geïnnoveerd en gedigitaliseerd. Wij nemen u in deze twee bloktrainingen mee door de juridische aspecten bij toepassing van ICT in de gezondheidspraktijk. In de eerste training gaan we in op de zorginformatiesystemen, PGO's en uitwisselingssystemen. In de tweede training bespreken we waar rekening mee moet worden gehouden bij het doen van wetenschappelijk onderzoek in de zorg, het gebruik van e-mail in de zorg en het gebruik van patiëntportalen.

https://bit.ly/2TV4SHA

Dinsdag 5 november

ICT en gezondheidsrecht: de basis

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/2AyMidW

4 PUNTEN PO ADVOCATUUR — NEDERLANDSE ORDE VAN ADVOCATEN

6 PUNTEN PO ADVOCATUUR — NEDERLANDSE ORDE VAN ADVOCATEN

FG / DPO training

Binnen onze FG-opleiding onderscheiden wij diverse trainingsdagen (de zogeheten themadagen). Op een themadag wordt één specifiek thema behandeld en zijn ook los afneembaar.

- Donderdag 31 oktober – Inventariseren en registreren
- Donderdag 7 november – Rechten van betrokkenen
- Donderdag 14 november – Datalekken
- Donderdag 28 november – Online marketing & cookies
- Donderdag 19 december – FG in de zorg

ictrecht.nl/opleiding-fg-dpo

Heeft u vragen of wilt u meer weten?

Neem dan 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