ICTRECHT adviesbureau

ICTRECHT IN DE PRAKTIJK

jaargang 7 nummer 2 april 2019

Wordt 2019 het jaar van de ePrivacy Verordening?

Online gokken, binnenkort toegestaan in Nederland

Digitale gegevensuitwisseling straks wettelijk verplicht in de zorg

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

Dat 2019 het jaar van de privaycwetgeving wordt, staat wel vast. Al sinds de vankrachtwording van de Algemene Verordening Gegevensbescherming (AVG) vorig jaar zien we een juridische aardverschuiving: vrijwel alle nieuwe conflicten op het gebied van ICT hebben een privacy-component. Dit jaar komt daar waarschijnlijk nog een schepje bovenop, want de ePrivacy Verordening – met nieuwe, strengere regels over persoonsgegevens bij telecom- en internetdiensten – zal dan van kracht worden. Wat dat zal betekenen, en wat de AVG nu al opgeleverd heeft, leest u in dit nummer.

Maar er is meer. Natuurlijk zijn auteursrechtkwesties niet ineens weg, integendeel. De nieuwe Richtlijn Auteursrechten introduceert vérgaande verplichtingen voor platforms en tussenpersonen op internet. Dit heeft tot veel kritiek geleid, omdat het tot filters en sluiting van diensten zou leiden. Daarnaast wordt het aantal meldplichten voor security- en datalekken uitgebreid met nieuwe wetgeving, en kan zelfs online gokken legaal worden dit jaar. Er staat ons dus een hoop te wachten!

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
Matthijs van Bergen - Directeur Legal ICT - m.vanbergen@legalict.com
Niels Winters - Directeur JuriBlox B.V. - n.winters@ictrecht.nl
Alisa Schurink - Opleidingscoördinator en Marketingmedewerker - a.schurink@ictrecht.nl
Beryl Hetharia - Juridisch adviseur - b.hetharia@ictrecht.nl
Britt Telleman - Office Assistant - b.telleman@ictrecht.nl
Cas Mevissen - Juridisch adviseur Legal ICT - c.mevissen@legalict.com
Dries Lawrence - Juridisch adviseur - d.lawrence@ictrecht.nl
Esther Flierman - Juridisch adviseur ICTRecht Groningen - e.flierman@ictrecht.nl
Jessica Hof - Oud-medewerker ICTRecht Groningen
Kim Groot - Juridisch adviseur - k.groot@ictrecht.nl
Laura Monhemius - Juridisch adviseur - l.monhemius@ictrecht.nl
Lili Ujvári - Marketingmedewerker - l.ujvari@ictrecht.nl
Nicole Waaijer - Marketing adviseur - n.waaijer@ictrecht.nl
Tessa van Schijndel - Juridisch adviseur - t.vanschijndel@ictrecht.nl
Eline Pellis - Vormgever - eline@elinepellis.com
Leonard Fäustle Stills & Motion - foto's ICTRecht - info@leonardfaustle.nl

Laura Monhemius
Juridisch adviseur

Privacy

Wordt 2019 het jaar van de ePrivacy Verordening?

Voor de Digital Single Market-strategie heeft de Europese Commissie de laatste jaren bergen geprobeerd te verzetten om het wetgevingslandschap te moderniseren. De onderhandelingen over de Auteursrechtrichtlijn zijn inmiddels afgerond (hoewel een aantal lidstaten daar allesbehalve blij mee is), de Wet beveiliging netwerk- en informatiesystemen is aangenomen en – last but not least – is de Algemene Verordening Gegevensbescherming (AVG) natuurlijk in werking getreden. Een vraag die wij steeds vaker krijgen is of dit jaar dan eindelijk het jaar van de ePrivacy Verordening (ePV) gaat worden.

Wat is nieuw onder de ePV?
De ePrivacy Verordening zal de ePrivacy Richtlijn vervangen. In Nederland kennen we deze als de Telecommunicatiewet (Tw) – bij velen ook wel bekend als de Cookiewet. De Tw regelt echter meer dan alleen cookies. De wet kent ook strenge regels voor spam, radio, televisie en netneutraliteit. Maar juist omdat dit een richtlijn was, zijn er grote verschillen tussen de Europese Lidstaten. Nederland heeft er in 2009 bijvoorbeeld voor gekozen om het spamverbod ook op B2B-marketingberichten van toepassing te laten zijn, terwijl in het Verenigd Koninkrijk B2B-marketing via alle digitale kanalen is toegestaan.

De ePV beoogt om deze regels te harmoniseren, vereenvoudigen en bovendien te moderniseren. Inmiddels alledaagse diensten (lees: Facebook Messenger, Gmail en WhatsApp) vallen nu bijvoorbeeld buiten het toepassingsbereik van de Tw. Dit zijn zogenaamde *over-the-top*-aanbieders, die content via het internet aanbieden, waarbij traditionele telecomproviders worden omzeild. Naar verwachting zal de ePV ook voor hen gaan gelden, in ieder geval voor zover het gaat om het aanbieden van elektronische communicatie. De ePV wordt ook verwacht het een en ander te regelen voor het *Internet of Things* en *Voice over IP* (VoIP).

Daarnaast wil de Commissie de eindgebruiker meer controle geven over zijn gegevens. Toestemming zal waarschijnlijk vaker vereist worden, waarbij 'passieve' toestemming niet langer genoeg is. Het toestemmingsbegrip blijft gekoppeld aan de AVG en zal dus met een actieve handeling gegeven moeten worden. Wat toestemming ook onaantrekkelijk maakt, is dat de gebruiker deze altijd weer moet kunnen intrekken, net zo makkelijk als dat die gegeven is.

Sinds de inwerkingtreding van de AVG hebben we de eisen voor toestemming natuurlijk al zien veranderen voor het gebruik van cookies en het versturen van nieuwsbrieven. De Commissie heeft voorgesteld om – behoudens enkele uitzonderingen – ook toestemming te vereisen voor *device fingerprinting,* bepaalde verwerkingen van metadata en het toepassen van WiFi-tracking.

Ontwikkeling van de ePV
In 2016 is de Europese Commissie begonnen met de eerste consultaties voor de ePV. Al jaren klonken er geluiden dat de oude richtlijn verouderd was en dat het tijd was voor nieuwe regelgeving. In januari 2017 – inmiddels alweer ruim twee jaar geleden – heeft de Commissie het eerste voorstel voor de verordening ingediend. Het oorspronkelijke plan was om de ePV tegelijk met de AVG op 25 mei 2018 in werking te laten treden, maar dat is niet gelukt.

Gezien het nieuwe toepassingsbereik zal de ePV een grote impact hebben op de marketing- en advertisingindustrie. Er wordt dan ook sterk gelobbyd tegen het

voorstel, iets dat we bij de AVG ook hebben gezien. Zodoende is het voorstel van alle kanten bekritiseerd, waarbij voorgestelde wijzigingen elkaar in rap tempo hebben opgevolgd. Of de Commissie de beoogde vereenvoudiging nog kan opleveren, valt inmiddels te betwijfelen.

Verhouding tot de AVG

De ePV sluit niet alleen op het gebied van toestemming aan op de AVG. De nieuwe wet is bedoeld als *lex specialis* ten opzichte van de AVG en ziet dus op elektronische communicatie, ongeacht of er sprake is van een verwerking van persoonsgegevens. Naar verwachting zal de ePV hetzelfde territoriaal toepassingsbereik hebben als de AVG. Dat betekent onder meer dat ook niet-Europese bedrijven zich aan de wet zullen moeten houden, als zij hun diensten in Europa aanbieden. Ook zal er waarschijnlijk nog maar één toezichthouder bevoegd zijn op het gebied van elektronische communicatie, namelijk de Autoriteit Persoonsgegevens (AP). Op dit moment is het toezicht verdeeld tussen de Autoriteit Persoonsgegevens en de Autoriteit Consument en Markt. De AP wordt trouwens bevoegd om boetes in dezelfde twee categorieën op te leggen als onder de AVG: €20.000.000 of 4% van de wereldwijde omzet, of €10.000.000 of 2% van de wereldwijde omzet – welke hoger is.

Belangenstrijd

De belangrijkste discussiepunten lijken te liggen bij welke verwerkingen zijn toegestaan. Met name de nieuwe regels voor het gebruik van metadata, cookies en cookiewalls, en de hervormingen op het gebied van (B2B-)marketing komen er moeilijk doorheen. Vanuit de Europese burger klinken positieve geluiden: 92% van consumenten vindt online privacy steeds belangrijker. Ook voor het bedrijfsleven wordt de impact verwacht mee te vallen, juist vanwege de overlap met de AVG. Beide (privacy)wetten vullen elkaar aan en zorgen voor duidelijkheid over wat mag, wie de bevoegde toezichthouder is en wat de gevolgen van non-compliance zijn. Voldoen aan de AVG zal voor een groot deel ook voldoen aan de ePV betekenen.

Minder enthousiaste geluiden klinken vanuit de partijen die ook tegen de AVG waren. De nieuwe regels voor bijvoorbeeld metadata zouden innovatie juist tegengaan. Ook wordt een grote (negatieve) impact op marketing en advertising verwacht, mede omdat toestemming een steeds grotere rol lijkt te gaan spelen. Daarnaast is het voorstel volgens sommigen alweer verouderd en is het volgens hen wellicht beter om gewoon een aantal artikelen aan de AVG toe te voegen.

Verkiezingen

Eind mei vinden de Europese Parlementsverkiezingen plaats. Omdat het Europese Parlement medewetgever is, betekent dit dat de kaarten voor lopende wetgevingsprocessen opnieuw geschud worden. Ligt er vóór de verkiezingen geen definitief voorstel voor de ePV, dan zullen de onderhandelingen erna weer opnieuw geopend worden. Nu de Europese wetgever geen haast lijkt te hebben met de afronding – de eerstvolgende bespreking van de verordening staat officieel gepland op 7 juni 2019 – is een definitieve ePV nog niet in zicht. Geen enkele parlementariër wil natuurlijk het verwijt krijgen afbreuk te hebben gedaan aan het fundamentele recht op privacy door zaken te overhaasten.

Bram de Vos
Juridisch adviseur

Wet- en regelgeving

Governanceregels EU-internetdomeinnamen
Op 5 december 2018 bereikte het Europees Parlement en de Raad een voorlopig akkoord over de hervorming van de governanceregels voor het .eu topleveldomein (zoals vastgelegd in Verordening (EG) 733/2002 en Verordening (EG) 874/2004). Op dit moment kunnen alleen personen, organisaties en bedrijven in de Europese Unie een .eu domeinnaam registreren. Onder de nieuwe governanceregels wordt dit ook mogelijk voor Europese burgers die buiten de unie woonachtig zijn. Ook wordt er een multi-stakeholdergroep ingesteld die de Europese Commissie zal adviseren over misbruik van het topleveldomein. De overeengekomen tekst moet nog worden bijgewerkt, voordat deze formeel kan worden aangenomen.

https://bit.ly/2Hf4lga

Richtlijn grensoverschrijdende toegang tot online media-aanbod
Op 13 december 2018 hebben het Europees Parlement en de Raad een voorlopig akkoord bereikt over een richtlijn die de beschikbaarheid van online tv- en radioprogramma's binnen de Europese Unie moet verbeteren. Steeds meer omroeporganisaties bieden hun media-aanbod niet alleen via de traditionele kanalen, maar ook via het internet aan. De nieuwe richtlijn moet de beschikbaarheid van dit media-aanbod in andere lidstaten verbeteren. Op dit moment is het ingewikkeld om de rechten te vereffenen indien het media-aanbod in verschillende lidstaten wordt aangeboden. De richtlijn voorziet in een vereenvoudigd regime, zodat de vereffening volledig kan plaatsvinden in de lidstaat waar de omroeporganisatie haar hoofdvestiging heeft. De richtlijn vergemakkelijkt ook de vereffening indien een radio- of tv-uitzending rechtstreeks wordt doorgegeven naar een andere lidstaat (bijvoorbeeld via kabel, satelliet of ether). Het Europees Parlement en de Raad moeten het voorlopig akkoord nog bekrachtigen voordat het formeel kan worden aangenomen.

https://bit.ly/2TghegV

Wet implementatie artikel 1 richtlijn elektronische handel
Op 18 december 2018 heeft de Eerste Kamer de Wet implementatie artikel 1 richtlijn elektronische handel aangenomen, waarmee een aantal wijzigingen in de Wet op de omzetbelasting worden doorgevoerd. Deze wijzigingen moeten de btw-verplichtingen vereenvoudigen voor ondernemingen die grensoverschrijdend digitale diensten aanbieden. Ondernemingen die incidenteel (met een maximale omzet van €10.000 per jaar) digitale diensten aan consumenten in een andere lidstaat aanbieden, dragen voortaan btw af in hun eigen lidstaat. Daarmee worden de administratieve lasten voor deze ondernemingen beperkt. Ook worden via de implementatiewet de bewijseisen versoepeld omtrent de vaststelling van de plaats waar de consument woonachtig is. Verder worden de factuureisen versoepeld. Het wetsvoorstel maakt onderdeel uit van het pakket Belastingplan 2019 en is op 1 januari 2019 in werking getreden.

https://bit.ly/2Hgmgmu

Wet vastleggen en bewaren van kentekengegevens door de politie
Op 1 januari 2019 is de Wet vastleggen en bewaren van kentekengegevens door de politie in werking getreden. Onder deze wet kan de politie kentekeninformatie die wordt verkregen via camera's met *automatic number-plate recognition* (ANPR) vastleggen in een centraal register. ANPR-camera's worden door de politie al een aantal jaren gebruikt om kentekens van passerende voertuigen af te zetten tegen een referentiebestand. Op die manier kan bijvoorbeeld worden gecontroleerd of een passerend voertuig op naam staat van een voortvluchtige verdachte. De nieuwe wet maakt het mogelijk om de kentekeninformatie niet alleen af te zetten tegen een referentiebestand, maar vervolgens ook op te slaan in een centraal register. Op die manier kan op een later tijdstip informatie over passerende

voertuigen worden teruggezocht, bijvoorbeeld in het kader van een opsporingsonderzoek. De informatie die in het kentekenregister wordt opgeslagen, mag voor een periode van vier weken worden bewaard.

https://bit.ly/2iPeqnZ

Nota van wijziging bij Wetsvoorstel gebruik van passagiersgegevens

Op 30 januari 2019 werd er een nota van wijziging uitgebracht voor het voorstel voor de Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven. Het wetsvoorstel strekt tot implementatie van de Europese richtlijn over het gebruik van persoonsgegevens van passagiers (Richtlijn 2016/681/EU). Onder de wet wordt het voor luchtvaartmaatschappijen verplicht om passagiersgegevens af te staan aan een nieuw op te richten passagiersinformatie-eenheid ("Pi-NL"). Verschillende instanties (waaronder de politie en het openbaar ministerie) kunnen vervolgens reisgegevens bij Pi-NL opvragen. Om de privacy te waarborgen is de bewaartermijn van de gegevens beperkt tot vijf jaar. Ook worden de gegevens na zes maanden "gedepersonaliseerd" en mogen er geen bijzondere persoonsgegevens worden verwerkt. De bij Pi-NL aanwezige gegevens kunnen onder bepaalde voorwaarden (op eigen initiatief van Pi-NL, dan wel op verzoek) ook aan buitenlandse autoriteiten worden verstrekt.

https://bit.ly/2C6TukK

Wet kansspelen op afstand

Op 19 februari 2019 heeft de Eerste Kamer de Wet ter modernisering van de Wet op de kansspelen aangenomen. Door de modernisering wordt het mogelijk om, onder strikte voorwaarden, online kansspelen aan te bieden. Met de wet wil de regering waarborgen dat de speler toegang heeft tot een aantrekkelijk aanbod van kansspelen, maar tegelijkertijd beschermd wordt tegen kansspelverslaving en criminaliteit. Alleen ondernemingen met een vergunning van de Kansspelautoriteit mogen een online kansspel aanbieden. De wet voorziet in verschillende maatregelen om spelers te beschermen tegen een kansspelverslaving. Zo moet de kansspelaanbieder voldoen aan verschillende informatieverplichtingen. Daarnaast mogen er alleen online kansspelen worden aangeboden nadat de speler een profiel heeft ingevuld, waarin hij grenzen voor zijn speelgedrag heeft ingesteld. Ook wordt er een centraal register ingesteld waarin spelers worden ingeschreven die (vrijwillig of onvrijwillig) niet mogen deelnemen aan bepaalde online kansspelen. De wet bevat tevens aanvullende toezicht- en handhavingsbevoegdheden voor de Kansspelautoriteit.

https://bit.ly/2zSxFXQ

Wet Computercriminaliteit III

Op 1 maart 2019 is de Wet Computercriminaliteit III in werking getreden. De wet voorziet in aanpassingen van het Wetboek van Strafrecht en het Wetboek van Strafvordering en geeft de opsporingsautoriteiten meer bevoegdheden in het digitale domein. Onder de Wet Computercriminaliteit III kunnen autoriteiten heimelijk en op afstand computers, smartphones of servers van verdachten binnendringen bij de opsporing van ernstige delicten. Ook kunnen er verschillende andere bevoegdheden worden ingezet. Zo voorziet de wet in mogelijkheden om computergegevens te kopiëren of om deze ontoegankelijk te maken. Ook biedt de wet de mogelijkheid om communicatie van de verdachte af te tappen. Verder kunnen er op grond van de Wet Computercriminaliteit III opsporingsambtenaren als "lokpubers" worden ingezet om digitaal kinderlokken ("grooming") tegen te gaan. Tot slot worden er via de Wet Computercriminaliteit III een aantal nieuwe delictsomschrijvingen aan het Wetboek van Strafrecht toegevoegd.

https://bit.ly/2ECKghT

Matthijs van Bergen
Directeur Legal ICT

Cas Mevissen
Juridisch adviseur
Legal ICT

Overheid | Innovatie

De Richtlijn die auteursrechten in het digitale tijdperk beter moet beschermen

Afgelopen maanden is er veel te doen geweest over de nieuwe Europese Richtlijn betreffende auteursrechten. Tijdens de onderhandelingen is er veel kritiek geuit op verschillende belangrijke punten van deze Richtlijn. U heeft in het nieuws vast wel een paar keer de term 'uploadfilter' voorbij horen komen. Inmiddels is de Richtlijn net definitief geworden, waardoor wij in dit artikel kunnen terugblikken op de achtbaanrit van deze controversiële EU-wetgeving.

Een terugblik op de totstandkoming van de Richtlijn
De Richtlijn is onderdeel van de 'digitale interne markt-strategie' van de Europese Unie, die de digitale groei binnen Europa probeert te stimuleren. Het hoofddoel van de Richtlijn is het updaten en harmoniseren van de huidige Europese auteursrechtwetgeving (Richtlijn 2001/29/EC). De nieuwe Richtlijn probeert met name het grote verschil in inkomsten tussen auteursrecht-hebbenden en online platforms/diensten die aan auteursrechtelijk beschermde werken verdienen, te verkleinen.

Toen de inhoud van de Richtlijn bekend werd, kon deze op flinke kritiek rekenen. Mensenrechten-organisaties (onder andere Bits of Freedom), gerenom-meerde hoogleraren en internetlegendes hadden geen goed woord over voor het voorstel van de Europese Commissie. Vooral artikel 11 (een 'belasting' voor hyperlinks) en artikel 13 (een 'uploadfilter') kregen er flink van langs. Naar aanleiding van deze kritiek heeft het Europese Parlement enkele wijzigingen in onder andere deze artikelen aangebracht. Europarlementariër Julia Reda, fel tegenstander van de Richtlijn, noemde deze aanpassingen vervolgens 'slechts cosmetisch.'

Ondanks de aanhoudende kritiek werd er overgegaan op de volgende stap van het wetgevingsproces: het overleg tussen de Raad van de Europese Unie, het Parlement en de Commissie ('de trialoog'). Er ontstond een sprankje hoop bij de tegenstanders van de Richt-lijn toen bekend werd dat Duitsland en Frankrijk er niet uitkwamen in de onderhandelingen. Die hoop doofde echter snel nadat bekend werd dat de twee landen tot een compromis waren gekomen dat, in de ogen van critici, nog nadeliger was dan de oorspronke-lijke Richtlijn.

Hoewel er hevig is geprotesteerd in Europa, met zelfs duizenden betogers in de straten van Berlijn, is de Richtlijn uiteindelijk toch door het Europese Parlement aangenomen, op 26 maart 2019. Vanaf die datum heb-ben de lidstaten nu nog twee jaar de tijd om de regels in hun nationale wetgeving te implementeren. Dit duurt nog even, maar gezien de impact van deze nieuwe wetgeving kan het geen kwaad om eens goed naar de inhoud te kijken.

Is artikel 11 echt een 'belasting voor hyperlinks'?
Niet helemaal. Artikel 11 verplicht 'verleners van diensten van de informatiemaatschappij' (oftewel: verleners van

online diensten – breed begrip) ertoe om uitgevers van nieuws te vergoeden wanneer er ‘meer dan een hyperlink vergezeld met afzonderlijke woorden’ van een persbericht wordt gebruikt. De verduidelijking ‘een hyperlink met afzonderlijke woorden’ is toegevoegd door het Europese Parlement nadat de oorspronkelijke bepaling veel kritiek ontving. Onder de eerste versie van artikel 11 vielen namelijk alle vormen van hyperlinken, waardoor dit artikel al snel uitgemaakt werd voor ‘een linkbelasting’.

De toevoeging van het Parlement neemt de kritiek gedeeltelijk weg, maar zorgt wel voor nieuwe verwarring: nu is het onduidelijk wat precies bedoeld wordt met ‘afzonderlijke woorden’. Gaat een enkele zin al over deze grens heen of is het beperkt tot losstaande woorden zonder samenhang? Hoe zit het met een (thumbnail-)afbeelding? Uit de Richtlijn en haar overwegingen valt niet op te maken wat de antwoorden op deze vragen zijn. Aangezien de bepaling gericht lijkt te zijn op diensten zoals Google News lijkt het waarschijnlijk dat een combinatie van een zin en een (thumbnail-)afbeelding buiten de uitzondering van ‘afzonderlijke woorden’ valt.

De Richtlijn maakt wel duidelijk dat privégebruik door individuen niet onder artikel 11 valt. Dit betekent dat u zelf nog steeds hyperlinks (inclusief begeleidende teksten) kan delen met anderen, zonder dat u hiervoor hoeft te betalen.

Waarom is artikel 13 zo controversieel?
Kort samengevat verplicht artikel 13 online diensten die als voornaamste doel hebben om toegang te geven tot een grote hoeveelheid door gebruikers gedeelde content (YouTube, Facebook et cetera) tot samenwerking met auteursrechthebbenden, om te voorkomen dat auteursrechtelijk beschermd materiaal beschikbaar wordt gesteld op hun websites. Deze verplichting geldt niet voor *alle* online diensten waarmee gebruikers content delen. Non-profit organisaties (zoals Wikipedia), internetaanbieders en clouddiensten waar gebruikers of bedrijven voor eigen gebruik informatie uploaden, zijn van deze verplichtingen uitgesloten.

De diensten die wél onder artikel 13 vallen, moeten hun uiterste best doen om te voorkomen dat beschermde werken, waar zij geen licentieovereenkomst voor gesloten hebben, beschikbaar zijn op hun platforms. Mochten de beschermde werken desondanks alsnog op hun platforms verschijnen, zijn zij hiervoor aansprakelijk. Alleen als ze hun uiterste best hebben gedaan om toestemming van de rechthebbende te krijgen en, na een klacht, hun best doen om het werk te verwijderen en in de toekomst te blokkeren van het platform, zijn zij van deze aansprakelijkheid uitgesloten. Hoewel de Richtlijn niet specifiek ingaat op welke maatregelen moeten worden getroffen om te voorkomen dat beschermde werken beschikbaar worden gesteld, impliceert het de toepassing van 'uploadfilters'.

De verplichting tot het gebruik van dergelijke uploadfilters viel niet alleen slecht bij verschillende online platforms, ook vele internetgebruikers waren niet over het voorstel te spreken. De meest opvallende kritiek bestond uit een brief die gericht was aan de president

van het Europese Parlement. Deze brief was geschreven door 70 experts op het gebied van technologie en recht, waaronder Vincent Cerf (internetpionier), Tim Berners-Lee (bedenker van het *World Wide Web*) en Jimmy Wales (medeoprichter van Wikipedia). Hun bedenkingen lagen vooral bij de zware lasten voor kleine dienstverleners[1], de onzekerheid over welke diensten onder de Richtlijn zouden vallen en de verandering van het aansprakelijkheidsmodel van de Richtlijn elektronische handel[2]. Zij voorspelden zelfs desastreuze gevolgen voor het open en vrije internet.

Wat is er mis met uploadfilters?
Het klinkt in eerste instantie misschien nog helemaal niet zo gek: het filteren van door gebruikers geüploade informatie, zodat rechthebbenden mee kunnen delen in de winst van de gigantische online platforms die op dit moment (flink) verdienen aan beschermde werken. Deze uploadfilters brengen echter verschillende problemen met zich mee. Het is technisch gezien heel lastig om informatie op de juiste manier te filteren. Daardoor wordt er óf te veel óf te weinig gefilterd; precies genoeg is eigenlijk niet haalbaar.

Wat artikel 13 in de praktijk van online dienstverleners vraagt, is om **(1)** alle werken van alle rechthebbenden in de wereld op te slaan in een database, in combinatie met alle licenties ter wereld die gegeven zijn, **(2)** automatisch alle content te monitoren die wordt geüpload door gebruikers en te controleren of deze content ook aanwezig is in de auteursrecht-database (hierbij rekening houdende met de uitzonderingen op het auteursrecht, zoals parodieën) en om **(3)** automatisch alle content te blokkeren waar geen licentie of uitzondering voor is.

Dit is een gigantische klus die waarschijnlijk alleen door de allergrootste online platforms geklaard zou kunnen worden. En zelfs dat is nog maar de vraag, aangezien YouTube bijvoorbeeld al langer uploadfilters hanteert die regelmatig de plank misslaan. Zo werd een video van een spinnende kat geblokkeerd, omdat het filter dacht dat deze auteursrechtelijke beschermd werk van EMI Music bevatte. Als uploadfilters op dit moment nog dergelijke fouten maken, is het bijna niet voor te stellen hoe ze in de toekomst complexe situaties, zoals parodieën en gebruik voor onderwijsdoeleinden, moeten gaan herkennen.

Naast de technische tekortkomingen van filters, zullen veel platforms waarschijnlijk risicomijdend gedrag gaan vertonen. Om claims van rechthebbenden te voorkomen, kunnen ze beter een paar keer te veel blokkeren dan een paar keer te weinig. Hoewel online dienstverleners volgens de Richtlijn verplicht zijn om een beroepsmogelijkheid te bieden, inclusief menselijke tussenkomst, is de content op dat moment al geblokkeerd. Daarnaast is het nog maar de vraag hoe klantvriendelijk deze mogelijkheid in de praktijk zal zijn.

Kleine bedrijven worden gespaard, of toch niet?
Een andere belangrijke wijziging die het Europese Parlement heeft aangebracht, is de vrijstelling voor kleine bedrijven. Zij hoeven daardoor niet te voldoen aan de verplichtingen uit de Richtlijn. Het gaat hierbij om ondernemingen met minder dan 50 werknemers en minder dan 10 miljoen omzet per jaar. In de trialoog vond Frankrijk deze vrijstelling te breed en Duitsland te smal. In het uiteindelijke compromis tussen deze twee landen is de vrijstelling iets smaller geworden.

Door deze meest recente wijziging in de trialoog mogen 'kleine bedrijven' hun diensten niet langer dan 3 jaar in de EU hebben aangeboden om vrijgesteld te zijn. Daarnaast mogen ze niet meer dan 5 miljoen bezoekers per jaar ontvangen; anders moeten ze 'hun best doen' om, na een klacht van een rechthebbende, te voorkomen dat de betreffende werken na de klacht nog geüpload worden op hun platform. De rechthebbende moet het kleine bedrijf hier wel bij helpen.

Middelgrote bedrijven zullen overigens nog steeds 'passende' maatregelen moeten treffen, waarbij het de vraag blijft hoe ver zij moeten gaan in hun maatregelen. Als zij tot de conclusie komen dat een goed uploadfilter voor hen niet haalbaar is, door beperkte middelen bijvoorbeeld, mogen zij deze dan achterwege laten? De Richtlijn geeft hier helaas geen duidelijkheid over.

En nu?
Ondanks de wijzigingen die doorgevoerd zijn in de twee Parlementaire stemmingen en de trialoog, blijft de Richtlijn controversieel. Het is daarom nog even afwachten op welke manier de regels van de Richtlijn door de lidstaten in nationale wetgeving omgezet gaan worden. Als u niet tot de volgende uitgave van ons tijdschrift wilt wachten, kunt u de laatste ontwikkelingen ook volgen via de website van ons internationale label: www.legalict.com.

1. In de laatste versie van de Richtlijn zijn bepaalde kleine bedrijven uitgesloten van haar verplichtingen, zie 'Kleine bedrijven worden gespaard'.
2. In de Richtlijn elektronische handel worden diensten die slechts informatie doorgeven *('mere conduit')* onder bepaalde voorwaarden uitgesloten van aansprakelijkheid voor de inhoud van die informatie. Deze uitsluiting van aansprakelijkheid ging uit van de *passieve* rol van online platforms. De nieuwe Richtlijn legt platforms echter een *actieve* verplichting op.

Kim Groot
Juridisch adviseur

Privacy | Overheid

Wet Beveiliging Netwerk- en Informatiesystemen: nieuwe meldplicht voor digitale dienstverleners

Een paar maanden geleden is de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) in werking getreden. Na de Algemene Verordening Gegevensbescherming (AVG) brengt ook deze nieuwe wet een meldplicht met zich mee. De wet is onder meer relevant voor sommige digitale dienstverleners, en bevat een meldplicht voor incidenten en een zorgplicht met betrekking tot het treffen van geschikte beveiligingsmaatregelen. In dit artikel bespreek ik daarom de belangrijkste aandachtspunten van deze nieuwe wet: voor welke digitale dienstverleners is deze wet relevant, welke incidenten moeten er gemeld worden, wat is de meldingsprocedure en wat zijn de handhavingsbevoegdheden van de toezichthouder?

De Wet Beveiliging Netwerk- en Informatiesystemen
Cybersecurity en het beschermen van kritieke infrastructuur staan in de Europese Unie al een tijd op de agenda. Uit dit beleid is in 2016 de Europese Netwerk- en Informatiebeveiligingsrichtlijn voortgekomen. De lidstaten van de Unie hebben de verplichting richtlijnen om te zetten in nationale wetgeving, wat in Nederland heeft geleid tot de inwerkingtreding van de Wbni op 9 november 2018. Middels de Wbni en de daarin opgenomen verplichtingen voor digitale dienstverleners wil de overheid Nederland digitaal veiliger maken en de digitale weerbaarheid vergroten. Zij heeft Agentschap Telecom aangewezen als toezichthouder op deze wet. Het Agentschap ziet toe op de beschikbaarheid en betrouwbaarheid van IT- en communicatienetwerken, zodat Nederlanders veilig gebruik kunnen maken van deze netwerken. In de wet is naast een zorgplicht tot het treffen van goede beveiligingsmaatregelen daarom ook een meldplicht opgenomen voor beveiligingsincidenten. Hierin is opgenomen dat bepaalde incidenten gemeld moeten worden aan Agentschap Telecom en het CSIRT (Computer Security Incident Response Team), een overheidsinstantie met de taak om schade te beperken door het verspreiden van actuele dreigingsinformatie.

Valt een geleverde dienst onder de Wbni?
De hamvraag is natuurlijk wanneer digitale dienstverlening onder de Wbni valt. Immers vallen niet alle aanbieders van digitale diensten onder de Wbni. Er wordt gekeken naar de type digitale dienst en de omvang van de onderneming. Om te bepalen of een onderneming een dienst aanbiedt die mogelijk onder de werking van de Wbni valt, stelt u uzelf onderstaande vraag:

Biedt de onderneming een:
- digitale marktplaats;
- digitale zoekmachine; of
- digitale clouddienst?

Indien u bovenstaande vraag bevestigend kan beantwoorden, is de Wbni mogelijk van toepassing. Als dit niet het geval is, kunt u ervan uitgaan dat de

Wbni niet van toepassing is. Socialmedia-bedrijven en webshops bieden bijvoorbeeld ook een digitale dienst maar hoeven niet aan de Wbni te voldoen.

Omvang van de onderneming en vestigingsplaats
Aanbieders van online marktplaatsen, zoekmachines en clouddiensten dienen een bepaalde minimale omvang te hebben voordat de Wbni van toepassing is. De wet geldt namelijk alleen voor (middel)grote ondernemingen. Als een aanbieder van deze dienst(en) aan één van de onderstaande criteria voldoet is hier sprake van:

De onderneming heeft:
- minimaal 50 medewerkers en een Europese hoofdvestiging in Nederland; of
- minder dan 50 medewerkers, een balanstotaal of jaaromzet van minimaal 10 miljoen euro en een Europese hoofdvestiging in Nederland.

Geen Europese hoofdvestiging in Nederland?
Als de onderneming geen Europese hoofdvestiging in Nederland heeft, maar wel minimaal 50 medewerkers of minimaal 10 miljoen balanstotaal of jaaromzet, moet er ook rekening mee worden gehouden dat de Wbni of andere vergelijkbare Europese wetgeving van toepassing zal zijn. Is er namelijk een hoofdvestiging in een ander Europees land? Dan valt de onderneming onder de wetgeving van dat land. Is er geen Europese hoofdvestiging? Dan dient er een vertegenwoordiger in een Europese lidstaat aangewezen te worden. Als er een vertegenwoordiger in Nederland aanwezen wordt, is de Wbni van toepassing.

AVG-achtige meldplicht en boetes?
Als u na mijn bovenstaande uitleg tot de conclusie bent gekomen dat de Wbni en haar verplichtingen ook voor u of uw cliënt gelden, doet u er wellicht goed aan eens na te denken over de gehanteerde beveiligingsmaatregelen en -procedure voor de omgang met incidenten. Mogelijk zijn er in mei 2018, toen de AVG in werking trad, al bepaalde maatregelen getroffen die ook voor de Wbni relevant zijn. De overeenkomst met de AVG en de bijbehorende meldplicht voor incidenten met betrekking tot persoonsgegevens laat wellicht alarmbellen rinkelen. Mogelijk vraagt u zich af of er, net zoals bij de AVG, een risico is op een hoge boete wanneer een incident niet (tijdig) gemeld wordt bij de toezichthouder. Ik kan u in dat geval alvast geruststellen dat het Agentschap Telecom voor nu geen 'AVG-achtige' hoge boetes gaat uitdelen. Dit betekent echter niet dat de Wbni genegeerd mag worden. Ondernemingen zijn alsnog verplicht aan de wet te voldoen en kunnen een bestuurlijke boete opgelegd krijgen wanneer zij niet voldoen.

Zorgplicht en meldplicht
Ondernemingen die onder de werking van de Wbni vallen hebben een zorgplicht en een meldplicht. De zorgplicht houdt in dat een onderneming 'passende

en evenredige organisatorische en technische maatregelen' moet nemen om risico's voor de beveiliging van ICT-systemen te voorkomen en beheersen. Deze norm is vergelijkbaar met de norm voor beveiliging die we terugzien in de AVG. Tevens moeten maatregelen genomen worden om de gevolgen van eventuele incidenten, mogen deze onverhoopt toch ontstaan, te minimaliseren. De meldplicht is relevant voor de situaties waarin een incident is ontstaan en schrijft voor dat incidenten onverwijld gemeld moeten worden bij het Agentschap Telecom en het CSIRT.

Wanneer is er sprake van een incident?
De vraag is echter wanneer er precies sprake is van een incident. De Wbni verstaat onder een incident *"elke gebeurtenis met een schadelijk effect op de beveiliging van netwerk- en informatiesystemen".* Hiervoor worden de BIVA-punten gehanteerd. Er kan sprake zijn van een incident wanneer een gebeurtenis een schadelijk effect heeft op één of meer van de BIVA-punten:

- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid
- Authenticiteit

Niet elk incident hoeft echter gemeld te worden. Er moet namelijk vastgesteld worden of het incident 'aanzienlijke gevolgen' heeft voor de dienstverlening van de onderneming. De gevolgen kunnen aanzienlijk genoemd worden indien er een minimaal aantal gebruikers getroffen wordt door het incident of wanneer de gevolgen van het incident dusdanig groot zijn voor economische en maatschappelijke activiteiten. Om duidelijk te kunnen toetsen of een incident 'aanzienlijke gevolgen' heeft, zijn er drempelwaarden opgesteld om incidenten te kunnen beoordelen. Deze zijn als volgt:

- de dienst was in de EU voor meer dan 5.000.000 gebruikersuren niet beschikbaar *(aantal gebruikers in de EU X aantal uren dat de dienst niet beschikbaar is); of*
- het incident heeft negatieve gevolgen met betrekking tot integriteit, authenticiteit of vertrouwelijkheid voor meer dan 100.000 gebruikers in de EU; of
- minimaal één gebruiker in de EU heeft meer dan €1.000.000 schade opgelopen; of
- er was en/of is een risico voor de openbare veiligheid en/of beveiliging; of
- er was en/of is een risico op een verlies van mensenlevens.

Indien er bij het incident aan één of meer van de bovenstaande drempelwaarden voldaan wordt, heeft het incident aanzienlijke gevolgen en dient het gemeld te worden.

Hoe en waar meldt u een incident?
Bij kennisneming van een incident met aanzienlijke gevolgen is de dienstverlener verplicht het incident onverwijld te melden bij Agentschap Telecom en bij het CSIRT voor digitale dienstverleners. Met onverwijld melden wordt bedoeld dat het incident onmiddellijk, of in de woorden van het Agentschap: "zo snel mogelijk en zonder onnodige vertraging", gemeld moet worden. De melding dient in eerste instantie het incident zelf te omschrijven, de zichtbare gevolgen van het incident en de huidige status van het incident. Deze gegevens kunnen op een later tijdstip worden aangevuld met nadere informatie over de geraakte onderdelen binnen de organisatie, de oorzaak van het incident, de wijze waarop het incident ontdekt is, de vermoedelijke manier van aanvallen (bijvoorbeeld DDOS of malware), nadere gegevens over de impact en meer informatie over de geraakte gegevens.

Een melding kan via e-mail of telefoon gemeld worden bij het Agentschap Telecom. Op de website van het Agentschap vindt u tevens een invulformulier zodat u alle benodigde informatie verstrekt. Daarnaast dient er ook op de website van het CSRIT een formulier ingevuld te worden. Ik adviseer daarnaast om er rekening mee te houden dat een incident aanvullend ook een 'datalek' of beveiligingsincident in de zin van de Algemene Verordening Gegevensbescherming kan zijn. In dat geval kan er ook sprake zijn van een verplichting tot het doen van een melding bij de Autoriteit Persoonsgegevens.

Bevoegdheid en handhaving toezichthouder
Nadat een incident gemeld is kan de toezichthouder aankloppen, informatie opvragen en onderzoek doen naar de oorzaak van het incident. Daarnaast heeft de toezichthouder, ook wanneer er geen melding gedaan is, bij een vermoeden van overtreding van de Wbni de bevoegdheid om informatie op te vragen bij een organisatie om te kunnen beoordelen of de beveiliging van netwerk- en informatiesystemen op orde is. Ondernemingen dienen dus ook over de documentatie te beschikken zodat de toezichthouder kan nagaan of de onderneming zich daadwerkelijk aan beveiligingseisen houdt.

Wanneer het Agentschap concludeert dat een dienstverlener zich niet aan zijn wettelijke verplichtingen houdt, kan zij de Wbni op verschillende wijzen handhaven. Zij kan een bindende aanwijzing geven waarin de aanbieder van de dienst verplicht wordt om binnen een redelijke termijn bepaalde maatregelen te treffen. Daarnaast heeft zij de bevoegdheid om een last onder bestuursdwang of een bestuurlijke boete op te leggen.

ICTRECHT
privacy

Een deskundige Functionaris Gegevensbescherming (FG) nodig?

Het aanstellen van een FG is onder de AVG voor verschillende organisaties verplicht. De privacy juristen van ICTRecht kunnen de rol van FG - op afstand - voor uw organisatie invullen. Onze FG's hebben ruime ervaring opgedaan binnen diverse organisaties en zijn direct inzetbaar. Wij ontzorgen u op het gebied van de AVG en garanderen u hierbij een flexibele samenwerking die maandelijks opzegbaar is. Daarnaast zorgen wij ervoor dat de FG wordt ingeschreven bij de Autoriteit Persoonsgegevens.

1 FG op afstand - BASISPAKKET | € 950 excl. btw per maand

- Proactief adviseren over compliance met de AVG
- Adviseren omtrent het uitvoeren van DPIA's
- Informeren en adviseren over nieuwe wet- en regelgeving omtrent gegevensbescherming
- Beoordelen en melden van datalekken
- Toegang tot noodnummer (24/7 bereikbaar)
- Altijd binnen drie uur een reactie
- Vast contactpersoon
- Circa vijf uur per maand tijdsbesteding
- Eventuele aanvullende werkzaamheden kunnen op oproepbasis door de FG worden opgepakt, middels het afnemen van een aanvullende knipkaart tegen verlaagd tarief

2 FG op afstand - ONTZORGINGSPAKKET | € 1.850 excl. btw per maand

- Proactief adviseren over compliance met de AVG
- Adviseren omtrent het uitvoeren van DPIA's, het sluiten van verwerkersovereenkomsten en het bijhouden van het verwerkingsregister
- Informeren en adviseren over nieuwe wet- en regelgeving omtrent gegevensbescherming
- Beoordelen en melden van datalekken
- Ondersteunen bij verzoeken van betrokkenen
- Ondersteunen bij onderhandelen over verwerkersovereenkomsten Fungeren als vast aanspreekpunt voor interne vragen
- Reviewen en aanpassen van privacydocumenten, zoals de privacyverklaring
- Toegang tot noodnummer (24/7 bereikbaar)
- Altijd binnen twee uur een reactie
- Vast contactpersoon
- Onbeperkte tijdsbesteding, op basis van fair use

3 FG op afstand - ONTZORGINGSPAKKET EXTRA | € 2.500 excl. btw per maand

Bestaat uit het 'FG op afstand - ontzorgingspakket', plus:

- Jaarlijkse organisatiebrede AVG-check
- Zorgen voor interne bewustwording (in overleg)
- Altijd binnen één uur een reactie
- Maandelijkse compliance test, bestaande uit:

1. Inzage- en verwijderverzoeken (rechten van betrokkenen) testen
2. Opt-in/opt-out testen
3. Juridische websitescan
4. Cookiescan

ictrecht.nl/fg
privacy@ictrecht.nl
020 663 1941

ICTRECHT
privacy

Heeft uw Functionaris Gegevensbescherming (FG) ondersteuning nodig?

Heeft de FG binnen uw organisatie behoefte aan extra ondersteuning, bijvoorbeeld door tijdgebrek? Wij merken dat het AVG-vraagstuk vaak meer tijd kost dan voor handen is. De privacy juristen van ICTRecht kunnen uw FG hulp bieden bij uiteenlopende privacyvraagstukken. Zo fungeert ICTRecht als sparringpartner voor uw FG en pakken wij de werkzaamheden op waar geen tijd voor is. Wij garanderen u hierbij een flexibele samenwerking die maandelijks opzegbaar is.

1 FG ondersteuning - BASISPAKKET | € 950 excl. btw per maand

- Proactief adviseren over compliance met de AVG
- Adviseren omtrent het uitvoeren van DPIA's
- Informeren en adviseren van de FG over nieuwe wet- en regelgeving omtrent gegevensbescherming
- Ondersteunen bij het beoordelen en melden van datalekken
- Ondersteunen bij het bepalen van de FG-rol
- Toegang tot noodnummer (24/7 bereikbaar)
- Altijd binnen drie uur een reactie
- Vast contactpersoon
- Circa vijf uur per maand tijdsbesteding
- Eventuele aanvullende werkzaamheden kunnen op oproepbasis door de privacy juristen van ICTRecht worden opgepakt, middels het afnemen van een aanvullende knipkaart tegen verlaagd tarief

2 FG ondersteuning - ONTZORGINGSPAKKET | € 1.850 excl. btw per maand

- Proactief adviseren over compliance met de AVG
- Adviseren omtrent het uitvoeren van DPIA's, het sluiten van verwerkersovereenkomsten en het bijhouden van het verwerkingsregister
- Informeren en adviseren van de FG over nieuwe wet- en regelgeving omtrent gegevensbescherming
- Ondersteunen bij het beoordelen en melden van datalekken
- Ondersteunen bij verzoeken van betrokkenen
- Ondersteunen bij onderhandelen over verwerkers-overeenkomsten
- Ondersteunen bij het bepalen van de FG-rol
- Ondersteunen bij coördineren en uitzetten van taken
- Ondersteunen bij beantwoording van interne vragen
- Reviewen en aanpassen van privacydocumenten, zoals de privacyverklaring
- Vervangende rol van de FG in geval van ziekte/vakantie
- Toegang tot de trainingen van ICTRecht Academy voor de FG
- Toegang tot noodnummer (24/7 bereikbaar)
- Altijd binnen twee uur een reactie
- Vast contactpersoon
- Onbeperkte tijdsbesteding, op basis van fair use

3 FG ondersteuning - ONTZORGINGSPAKKET EXTRA | € 2.500 excl. btw per maand

Bestaat uit het 'FG ondersteuning - ontzorgingspakket', plus:

- Ondersteunen bij jaarlijkse organisatiebrede AVG-check
- Ondersteunen bij interne bewustwording (in overleg)
- Altijd binnen één uur een reactie
- Maandelijkse compliance test, bestaande uit:

1. Inzage- en verwijderverzoeken (rechten van betrokkenen) testen
2. Opt-in/opt-out testen
3. Juridische websitescan
4. Cookiescan

ictrecht.nl/fg
privacy@ictrecht.nl
020 663 1941

Esther Flierman
Juridisch adviseur
ICTRecht Groningen

Jessica Hof
Oud-medewerker
ICTRecht Groningen

Contracten

Recht uit de praktijk: conflictoplossing inzake schending zorgplichten

Regelmatig krijgen wij de vraag van cliënten hen bij te staan in een conflict over een mislukt automatiseringsproject. Dergelijke conflicten zijn vrijwel altijd complex. Met name omdat in ICT-contracten veelal een inspanningsverplichting is opgenomen in plaats van een resultaatsverplichting. Hierdoor is het vaak onduidelijk wat er van de ICT-leverancier mag én kan worden verwacht. Doordat het niet eenvoudig is om voor een automatiseringsproject harde afspraken vast te leggen, kan een dergelijk project sneller uitlopen op een dure teleurstelling. In dit artikel bespreken wij de zorgplichten van een ICT-leverancier en in welke gevallen er sprake is van een schending van deze plichten.

Gemengde overeenkomst

Hoofdregel in het Nederlandse overeenkomstenrecht is contractsvrijheid.[1] Dit betekent dat partijen een grote vrijheid hebben bij het contracteren, zolang de afspraken niet in strijd zijn met de wet, de openbare orde en de goede zeden.[2] Op elke hoofdregel geldt ook een uitzondering. Dit is het geval bij "benoemde overeenkomsten": overeenkomsten die de wetgever zo belangrijk vond dat hij deze nader in de wet heeft omschreven. Te denken valt aan de koopovereenkomst, huurovereenkomst, arbeidsovereenkomst en de overeenkomst van opdracht.

ICT-contracten hebben een zeer bijzondere positie in het recht. Hiervoor geldt noch volledige contractsvrijheid, noch zijn ze te kwalificeren als een specifiek benoemde overeenkomst. ICT-contracten zijn daarom "gemengde overeenkomsten". Afhankelijk van de geleverde diensten door de ICT-leverancier, bevatten zij kenmerken van bijvoorbeeld de overeenkomst van opdracht en de huurovereenkomst. De overeenkomst van opdracht omdat de ICT-leverancier voor de afnemer een softwaresysteem op maat ontwikkelt en een huurovereenkomst omdat het systeem draait op de server van de leverancier via hosting.

Inspanningsverplichting

Verder staan ICT-contracten erom bekend dat hierin een inspanningsverplichting wordt opgenomen voor de ICT-leverancier in plaats van een resultaatsverplichting. Dit betekent dat er niet zozeer een concreet resultaat wordt overeengekomen, maar dat de ICT-leverancier een bepaalde mate van inspanning dient te verrichten bij zijn dienstverlening. In beginsel is dit niet heel vreemd. De meeste automatiseringsprojecten vinden namelijk plaats op basis van de Agile-methodiek.

Indien een softwaresysteem wordt ontwikkeld op basis van agile, dan staat de inhoud van alle functionaliteiten van het systeem nog niet op voorhand vast.[3] De ontwikkeling vindt plaats op basis van "sprints", waarbij gedurende iedere sprint een nieuwe functionaliteit voor het systeem wordt bedacht, ontwikkeld en opgeleverd.

1. Den Tonkelaar, in: *GS Verbintenissenrecht,* artikel 213 Boek 6 BW, aant. 60.
2. Artikel 3:40 Burgerlijk Wetboek.
3. C. Jeloschek & J.J. Linneman, "Contracteren over agile softwareontwikkeling", *Computerrecht* 2013/82.

Doordat de volledige functionaliteiten van het softwaresysteem nog niet van tevoren volledig zijn uitgedacht en het systeem gaandeweg wordt opgebouwd, is het lastig om hieraan een resultaatsverplichting te koppelen zoals bij de bouw van een huis. De bouw van een huis vindt immers plaats aan de hand van een vooraf volledig uitgewerkte bouwtekening, waardoor het zo goed als onmogelijk is om hier tijdens de bouw sterk van af te wijken.

Zorgplicht
Hoe kan dan door de afnemer juridisch worden opgetreden tegen een ICT-leverancier wanneer het automatiseringsproject volgens hem is uitgelopen tot een fiasco en er geen concreet resultaat is afgesproken? De afnemer kan in dit geval een juridische procedure starten op basis van de door ICT-leverancier geschonden zorgplicht.

In zijn algemeenheid hebben contractspartijen een algemene zorgplicht ten opzichte van elkaar. Dit vloeit voort uit de wet. Er bestaat volgens de wet zowel een algehele zorgplicht tussen schuldeiser en schuldenaar[4] als een specifieke zorgplicht tussen een opdrachtgever en opdrachtnemer.[5] Ook vloeit een dergelijke plicht voort uit de redelijkheid en billijkheid.[6]

Voorgaande brengt met zich mee dat de afnemer een bepaald niveau van bekwaamheid en inzet mag verwachten. De ICT-leverancier moet daarbij handelen als een "redelijk bekwaam en redelijk handelend beroepsbeoefenaar". Van een ICT-leverancier mag dus worden aangenomen dat hij beschikt over de desgevraagde deskundigheid, ook als hij deze mate van deskundigheid niet blijkt te bezitten. Van hem mag dan ook worden verwacht dat hij extra voorzorgsmaatregelen neemt en zich onder andere op de hoogte houdt van de meest recente ontwikkelingen binnen zijn vakgebied.[7]

Bijzondere zorgplicht
Uit de rechtspraak volgt dat binnen de ICT-dienstverlening een verzwaarde zorgplicht geldt. Deze verzwaarde zorgplicht omvat een informatie- en waarschuwingsplicht. De achterliggende gedachte van deze zorgplicht is dat wordt verondersteld dat de ICT-leverancier een deskundige is op zijn vakgebied. Deze kennis en kunde ontbreekt veelal bij de afnemer. Aan de ICT-leverancier wordt daarom eveneens een adviesrol toegekend, evenals dit in de financiële sector het geval is.

4. Artikel 6:27 Burgerlijk Wetboek.
5. Artikel 7:401 Burgerlijk Wetboek.
6. Artikel 6:248 lid 1 Burgerlijk Wetboek.
7. Asser/Tjong Tjin Tai 7-IV 2018/93.

Wat de reikwijdte is van de betreffende zorgplicht is onder andere afhankelijk van de inhoud van de opdracht. Verder worden de kans op schade en de potentiële omvang van de schade hierin meegenomen. Ook het kennisniveau van de afnemer en zijn ervaringen rondom automatisering zijn relevant. Tot slot spelen de doelstellingen van de afnemer en de waarde van de opdracht een rol.

Dossiers
Hieronder worden twee dossiers uit onze praktijk besproken. In het eerste dossier stonden wij de afnemer bij, in het tweede dossier stonden wij de ICT-leverancier bij.

Wel schending zorgplicht
Een webdesigner had in een opdracht van onze cliënt een webplatform ontwikkeld. Onze cliënt leverde via het platform onlinediensten aan haar klanten. De eindgebruikers konden via hun account inloggen op de online omgeving. Al snel na oplevering bleek dat de eindgebruikers veel problemen hadden met inloggen. De webdesigner probeerde de problemen op te lossen onder de noemer support. Onze cliënt kreeg derhalve

van doen met meerwerkfacturen. Helaas leverde de support geen oplossing.

Onze cliënt schakelde een derde in om het platform eens onder de loep te nemen. Er was veel mis met het opgeleverde werk. In de ontwikkeling van het webplatform waren niet de gebruikelijke webstandaarden, PHP standaarden en de betreffende CMS standaarden in acht genomen evenmin was acht geslagen op de *best practice* inzake het betreffende CMS. Hierop is de webdesigner aangeschreven met de mogelijkheid de problematiek binnen een redelijke termijn op te lossen. Er werd aldus een beroep gedaan op schending van de zorgplichten door de webdesigner. Van een redelijk bekwaam vakgenoot mag immers verwacht worden dat hij werkt conform de standaarden in de branche en hij zich dus conformeert aan de webstandaarden, PHP standaarden en de betreffende CMS standaarden.

De webdesigner was evenwel van mening dat het niet aan hem lag. Een en ander werkte, dus het voldeed aan de overeenkomst. De afnemer had te hoge verwachtingen van het geleverde webplatform, de afnemer verwachtte functionaliteiten die niet waren overeengekomen. Het verbeteren van het platform betrof dus meerwerk, aldus de webdesigner. Tegen een redelijke vergoeding was hij bereid een en ander te verbeteren.

Naar onze mening was duidelijk aangetoond dat de performance van het webplatform onvoldoende was en dat dit werd veroorzaakt doordat slecht (programmeer)werk was geleverd. De overeenkomst werd dan ook buitengerechtelijk ontbonden middels een schriftelijke verklaring.

Geen schending zorgplicht
Onze cliënt, de ICT-leverancier, had een overeenkomst gesloten met een grote organisatie voor een nieuw factureringssysteem in een cloudoplossing. De overeenkomst werd aangegaan met een contractduur van 3 jaren en vertegenwoordigde een aanmerkelijke contractwaarde.

Gedurende het migratie- en implementatietraject ontstaan problemen. De streefdatum voor oplevering van de cloudoplossing wordt niet gehaald. Ook in de communicatie ontstaan problemen. Het voornaamste probleem betrof het feit dat de koppeling tussen de nieuwe cloudoplossing en de administratie-omgeving niet lukte. De grote organisatie verweet de ICT-leverancier gebrek aan expertise om de koppeling tot stand te brengen en ging over tot buitengerechtelijke ontbinding van de gehele overeenkomst.

In beide zaken is met behulp van onze dienstverlening een minnelijke regeling bereikt naar grote tevredenheid van cliënten waarbij zij schadeloos zijn gesteld.

Beryl Hetharia
Juridisch adviseur

E-commerce Overheid

Online gokken: binnenkort toegestaan in Nederland

In Nederland zijn online kansspelen momenteel verboden. Op grond van de huidige Wet op de kansspelen (Wok) is het namelijk niet mogelijk om een vergunning te verlenen dan wel te krijgen voor het aanbieden van online kansspelen. Maar daar komt verandering in. Binnenkort, waarschijnlijk vanaf 2020, is online gokken toegestaan en mogen aanbieders van online kansspelen hun diensten aanbieden op de Nederlandse markt. In dit artikel bespreken we onder meer waarom online gokken wordt gereguleerd, wat de voorwaarden zijn voor het aanvragen van een vergunning om online kansspelen aan te bieden, hoe het zit met de kansspelbelasting en aan welke regels online aanbieders zich moeten houden. Ook wordt stilgestaan bij het toezicht op en de handhaving tegenover vergunninghouders.

Waarom willen we in Nederland regels om online te kunnen gokken?
Op grond van de Wok is het in Nederland verboden om kansspelen aan te bieden wanneer daarvoor geen vergunning is verleend. De Wok voorziet niet in een vergunningsmogelijkheid voor het organiseren van kansspelen op afstand. Daarom waren Nederlandse spelers 'genoodzaakt' om mee te doen aan online kansspelen die werden aangeboden door buitenlandse aanbieders. Uit onderzoek is gebleken dat bijna 2 miljoen Nederlanders deelneemt aan illegale online kansspelen.[1] Van online pokeren tot online sportweddenschappen. De bedrijven die online kansspelen aanbieden zijn voornamelijk in Zuid-Europese landen en op overzeese eilanden gevestigd. Nederland had daarom geen grip op het illegale aanbod van gokwebsites.

Wat is een online kansspel?
Onder een online kansspel, in de Wok 'kansspel op afstand' genoemd, verstaan we het deelnemen aan een kansspel dat op afstand via elektronische communicatiemiddelen wordt aangeboden en waarbij er geen fysiek contact is tussen de speler en (het personeel van) de organisator van het kansspel. In de volksmond spreken we ook wel van online gokken. Denk aan het spel roulette, waarbij je als deelnemer geen invloed hebt op de uitkomst van het spel.

Aanvragen van een vergunning
Bedrijven mogen in Nederland een online kansspel aanbieden als zij daarvoor een vergunning hebben. Een vergunning kan worden aangevraagd bij de Kansspelautoriteit. De geldigheidsduur van een vergunning is in principe 5 jaar. Om een vergunning te verkrijgen, moet een online kansspelaanbieder aan enkele voorwaarden voldoen:

- een aanvrager moet gevestigd zijn in de Europese Unie of de Europese Economische Ruimte. Als dat niet het geval is, dan moet de aanvrager een vestiging openen in de EU of de EER;
- de aanbieder moet een vertegenwoordiger hebben die deskundig is op het gebied van kansspelverslaving

1. J. Senster & E. van de Ven, 'Nederlanders gokken massaal op internet', *Motivaction.nl*, 29 januari 2019.

en verslavingspreventie;
- aanvragers zullen worden getoetst op betrouwbaarheid. In de praktijk komt het erop neer dat aanvragers informatie over de bedrijfs- en financieringsstructuur moeten voorleggen aan de Kansspelautoriteit. Daarnaast onderzoekt de Kansspelautoriteit welke (rechts)personen betrokken zijn bij de aanvrager. En ook wordt gekeken naar eventuele strafrechtelijke en bestuursrechtelijke antecedenten;
- een bedrijf zal naar verwachting € 40.000 moeten betalen voor een vergunningsaanvraag.

Bovenstaande vergunningsvoorwaarden kunnen nog worden aangepast. Reden hiervoor is dat de minister voor Rechtsbescherming (verantwoordelijk voor het kansspelbeleid), een algemene maatregel van bestuur en een ministeriële regeling gaat opstellen, en daarin kunnen aanvullende vergunningsvoorwaarden worden opgenomen.

Kansspelbelasting afdragen
Bij het winnen van geldprijzen komt de Belastingdienst om de hoek kijken. In de Wet op de kansspelbelasting is vastgelegd of de deelnemer, dan wel de kansspelaanbieder belasting moet afdragen. Voor online kansspelen geldt straks dat de aanbieders een percentage over het gewonnen brutobedrag moeten afdragen aan de Belastingdienst. Momenteel is het percentage 29%, maar dit kan veranderen.

Welke regels gelden voor online kansspelaanbieders?
De online kansspelregelgeving heeft diverse doelen. Dit betreft onder andere het voorkomen van kansspelverslaving en het beschermen van de consument. Deze doelen hebben tot gevolg dat aanbieders van online kansspelen zich moeten houden aan verschillende regels.

Voorkomen van kansspelverslaving
Op aanbieders van online kansspelen rust een uitgebreide zorgplicht om kansspelverslaving zoveel mogelijk te voorkomen. Op meerdere manieren dienen online aanbieders ervoor te zorgen dat spelers niet gokverslaafd worden:
- *Informatieplicht*
  De aanbieder moet spelers informeren over de risico's van deelname aan kansspelen op afstand, de wijze van verantwoord spelen en eventuele zorg.

Deze informatie moet duidelijk zijn omschreven en op een gemakkelijk vindbare plek op de website staan.

- *Speelgedrag*
  Voordat een speler kan deelnemen aan een online kansspel, moet een speler een spelersprofiel invullen. Aanbieders moeten een formulier ontwerpen waarin de speler kan aangeven hoe vaak en hoe lang hij wil gokken, en wat de maximale storting en het tegoed op de spelersrekening mag zijn. Heeft een speler geen spelersprofiel ingevuld, dan mag een aanbieder die speler geen toegang geven tot het online kansspel.
- *Centraal Register Uitsluiting Kansspelen*
  Online kansspelaanbieders moeten zijn aangesloten bij het Centraal Register Uitsluiting Kansspelen. Hierin worden spelers geregistreerd die tijdelijk (minstens zes maanden) niet mogen deelnemen aan een online kansspel.
- *Verslavingsfonds*
  Aanbieders zijn verplicht om jaarlijks een financiële bijdrage te leveren aan het verslavingsfonds. Vanuit dit fonds worden spelers geholpen die gokverslaafd dreigen te worden of zelfs al gokverslaafd zijn. Het percentage, dat over het bruto spelresultaat moet worden afgedragen, wordt jaarlijks vastgesteld door de overheid.

Consumentenbescherming
Een ander uitgangspunt van de nieuwe regels is dat aanbieders consumenten moeten beschermen tegen hun eigen speelgedrag. Aanbieders moeten op de volgende zaken letten:

- *Voorkomen deelname minderjarigen*
  Minderjarigen mogen niet online gokken. Om te voorkomen dat minderjarigen zich voordoen als meerderjarigen worden eisen gesteld aan de identificatie van de speler. Denk aan het overleggen van een kopie van het identiteitsbewijs en een verificatiebetaling vanaf de betaalrekening van de speler. Of deze verificatiewijze waterdicht is valt te betwijfelen.
- *Spelerstegoed*
  De consument moet erop kunnen vertrouwen dat hij altijd bij zijn geld kan dat op de speelrekening staat. Daarom moeten aanbieders alle spelerstegoeden afscheiden van het eigen vermogen. Hiervoor kan een stichting derdengelden worden opgericht.
- *Reclame- en wervingsactiviteiten*
  Reclameactiviteiten mogen niet aanzetten tot deelname aan een online kansspel. Wanneer een speler net geld heeft verloren, mag bijvoorbeeld niet in een reclame-uiting naar voren komen dat een speler een bonus ontvangt wanneer er verder wordt gespeeld.

Toezicht en handhaving
In de gewijzigde Wok zijn enkele bevoegdheden voor de toezichthouder, Kansspelautoriteit, opgenomen. Zo mag de Kansspelautoriteit anoniem deelnemen aan een online kansspel, met als doel de identiteit van illegale kansspelaanbieders te achterhalen. Daarnaast mag de Kansspelautoriteit partijen die online gokken bevorderen, aanspreken om daarmee te stoppen. En een ander punt is dat in de gewijzigde Wok een wettelijke basis is voor internationale samenwerking tussen de Nederlandse toezichthouder en buitenlandse toezichthouders.

Vanaf volgend jaar massaal gokken, of toch niet?
Veel aanbieders hebben uitgekeken naar het moment om legaal online kansspelen aan te bieden. Naar verwachting zullen bedrijven massaal een vergunning aanvragen. Er is veel aandacht besteed aan het voorkomen van kansspelverslaving. Het is nu afwachten of wij in Nederland op een verantwoorde manier online kunnen gokken. In ieder geval zal de overheid hier ook flink aan verdienen. Of zal over een paar jaar het online gokken worden ontmoedigd, net zoals dat is gebeurd met het roken? Wordt er dan een rechtszaak gestart tegen de gokindustrie? De tijd zal het leren.

Tessa van Schijndel
Juridisch adviseur

Overheid | Cloud | Privacy

Digitale gegevens-uitwisseling straks wettelijk verplicht in de zorg

Digitale patiëntengegevensuitwisseling wordt straks wettelijk verplicht voor zorgaanbieders. Hoewel digitalisering van de zorg tot op heden aan zorgaanbieders is overgelaten, wil de minister nu alsnog de regie in handen nemen. Dat zegt minister Bruins van Medische Zorg en Sport in een debat van de Tweede Kamer over gegevensuitwisseling in de zorg: *"Mijn ambitie is dat de gegevensuitwisseling in de zorg in Nederland in rap tempo volledig digitaliseert, waardoor ook patiënten al hun eigen gegevens digitaal kunnen inzien en beheren".*[1] De maatregelen om de zorg te digitaliseren, komen als geroepen. De deadline nadert en vanaf 1 juli 2020 moeten alle ICT-systemen in de zorg zijn ingericht om gegevens elektronisch beschikbaar te maken. De deadline die nadert. In dit artikel bespreek ik de huidige ontwikkeling met betrekking tot de gegevensuitwisseling in de zorg.

Vormen van gegevensuitwisseling in de zorg

De uitwisseling van patiëntengegevens tussen zorgverleners onderling en de uitwisseling van het medisch dossier met patiënten gaan hand in hand. Op grond van de wet is iedere zorgaanbieder verplicht om een medisch dossier aan te leggen met betrekking tot de behandeling van een patiënt. Hiervoor gebruiken veel zorgaanbieders een eigen elektronisch patiëntendossier (epd). Voor gegevensuitwisseling tussen zorgaanbieders onderling wordt, onder andere, gebruik gemaakt van het Landelijk Schakel Punt (LSP). Via het LSP kunnen zorgaanbieders gegevens opvragen bij andere zorgaanbieders, mits de patiënt hier toestemming voor heeft gegeven. Het LSP is ook voor zorgaanbieders vrijwillig en het gebruik ervan is beperkt tot regio's. Als een patiënt uit Amsterdam in Maastricht wordt behandeld, kunnen gegevens niet worden uitgewisseld. Op dit moment hebben patiënten nog niet voldoende digitaal inzicht in hun medische gegevens en is de gegevensuitwisseling tussen zorgaanbieders onderling minimaal. Enerzijds ligt de oorzaak hiervan in het feit dat de epd-systemen van iedere ICT-leverancier meestal niet compatibel zijn met elkaar. Dit komt omdat er nog geen standaarden geïmplementeerd zijn voor welke patiëntgegevens hoe verzameld moeten worden. Daardoor is de dataportabiliteit nu nog niet optimaal. Anderzijds kunnen gegevens niet gemakkelijk uitgewisseld worden met verschillende zorgaanbieders, omdat iedere zorgaanbieder op een eigen manier patiëntgegevens registreert. Bij de behandeling van één patiënt kunnen namelijk veel zorgaanbieders betrokken zijn. Registratie van patiëntgegevens gebeurt door alle betrokken beroepsgroepen op een andere manier.

1. Kamerbrief van Minister Bruins over elektronische gegevensuitwisseling in de zorg (20-12-2018)

Wettelijke verplichtingen voor gegevensuitwisseling
Voor elektronische gegevensuitwisseling in de zorg bestaan specifieke wettelijke verplichtingen. Dit zijn de Wet cliëntenrechten bij elektronische verwerking van gegevens in de zorg en het Besluit elektronische gegevensverwerking door zorgaanbieders.

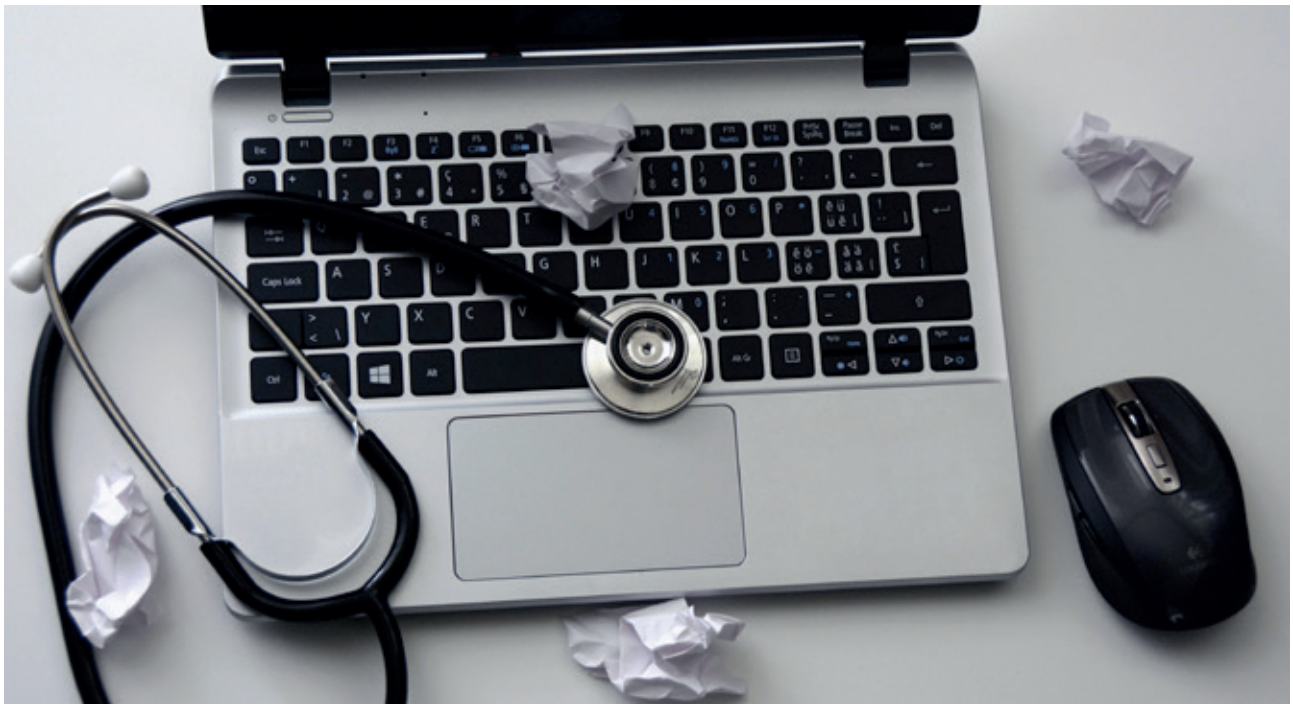
De Wet cliëntenrechten bij elektronische verwerking van gegevens spreekt van elektronische gegevensuitwisseling als *"twee of meer zorgaanbieders een systeem gebruiken om op elektronische wijze patiëntgegevens raadpleegbaar te kunnen maken."* Het gaat om elektronische uitwisselingssystemen waarmee de zorgaanbieders medische dossiers of gegevens uit dossiers inzichtelijk kunnen maken voor andere zorgaanbieders. Dit heet pull-verkeer. Push-verkeer is het gericht sturen van een bericht tussen twee zorgverleners in het kader van de behandeling. Voor push-verkeer, bijvoorbeeld bij een doorverwijzing, wordt volgens de Wet op de geneeskundige behandelovereenkomst (WGBO) uitgegaan van veronderstelde toestemming van de patiënt. De Wet cliëntenrechten bij elektronische verwerking van gegevens is ook niet van toepassing op interne communicatie van zorgaanbieders, zoals op het epd van een ziekenhuis.

In het Besluit elektronische gegevensverwerking door zorgaanbieders wordt ingegaan op welke eisen er zijn voor de beveiliging van zo'n elektronisch uitwisselingssysteem (en van een zorginformatiesysteem).

Het jaar van de gegevensuitwisseling in de zorg
Het jaar 2020 wordt het jaar van de gegevensuitwisseling in de zorg. Niet alleen heeft de minister van Medische Zorg en Sport als doelstelling dat alle zorgaanbieders de patiëntgegevens digitaal, gestandaardiseerd, beveiligd en met toestemming van de patiënt overdragen aan andere zorgaanbieders. Ook treedt op 1 juli 2020 het tweede deel van de Wet cliëntenrechten bij elektronische verwerking van gegevens in werking. Waarbij de patiënt extra rechten krijgt met betrekking tot elektronische gegevensuitwisseling tussen zorgaanbieders.

Vanaf 1 juli 2020 geldt het volgende:

- **Gespecificeerde en geregistreerde toestemming:** aan de patiënt moet de mogelijkheid geboden worden om aan te geven welke gegevens wel of niet door welke categorieën van zorgaanbieders mogen worden ingezien. Deze toestemming moet vervolgens geregistreerd worden. De inwerkingtreding van het recht op gespecificeerde toestemming is uitgesteld tot 1 juli 2020, omdat in de praktijk de wijze van registreren niet voldoende duidelijk was. Indien iedere individuele patiënt kan aangeven welke gegevens met welke categorie van zorgaanbieders wordt gedeeld, levert dit ontelbaar veel keuzemogelijkheden op. De patiënt moet zich over iedere keuze uitspreken en kan op ieder moment zijn keuze veranderen.
- **Elektronische inzage en afschrift van het medisch dossier en logging:** ook krijgt de patiënt het recht om zijn dossier elektronisch in te zien en een elektronisch afschrift van het dossier en de logging daarvan te krijgen. Zorgaanbieders konden op 1 juli 2017 nog geen garantie afgeven dat de elektronische inzage en afschrift veilig genoeg was. Daarom is de inwerkingtreding van deze bepaling uitgesteld.



Op basis van de Wet cliëntenrechten bij elektronische verwerking van gegevens zijn zorgaanbieders wettelijk verplicht om gegevens elektronisch beschikbaar te maken. Of en op welke manier de zorgaanbieder dat doet, is zijn eigen keus. Indien er gebruik wordt gemaakt van gegevensuitwisseling via een elektronisch uitwisselingssysteem dan dienen zorgaanbieders dat veilig en verantwoordelijk te doen aan de hand van opgelegde normen. Ook de ICT-leverancier is gebonden aan de normen die het Besluit voorschrijft. Hij moet de systemen van de zorgaanbieders zo inrichten dat deze aan de normen voldoen.

Dit zegt echter nog niks over wat er precies wordt uitgewisseld en dat er ook daadwerkelijk wordt uitgewisseld als dat nodig is. Als gevolg hiervan hebben veel zorgaanbieders voor een eigen gegevensuitwisselingssysteem gekozen. De betreffende ICT-leveranciers hebben ieder op eigen wijze hun systemen vormgegeven. Niet alleen moet de interopabiliteit (datauitwisseling tussen ICT-systemen) tussen gegevensuitwisselingssystemen worden verbeterd. Ook moeten de patiëntgegevens op dezelfde manier worden geregistreerd in de systemen. En dan moeten ook nog de leveranciers van de software worden verplicht de uitwisseling mogelijk te maken. Zorgaanbieders zullen de maatregelen die nodig zijn om aan de wet te kunnen voldoen, geïmplementeerd willen zien in de dienst die zij afnemen.

Welke initiatieven zijn er al genomen?
De minister gaat stapsgewijs maatregelen nemen om zorginstellingen te verplichten om op een eenduidige manier digitale patiëntgegevens met elkaar uit te wisselen. Dat er veel maatregelen genomen moeten worden, blijkt wel uit het feit dat de minister drie maanden uittrekt om met een plan van aanpak te komen. Maar welke maatregelen gaan er genomen worden om te zorgen dat zorgaanbieders in 2020 in staat zijn om patiëntgegevens uit te wisselen? Komt er een nieuw landelijk LSP of krijgen nieuwe initiatieven een springplank zoals MedMij en PGO's?

Op dit moment stelt MedMij spelregels op over gegevensuitwisseling tussen zorgaanbieder en patiënten, via een persoonlijke gezondheidsomgeving (PGO), waarop je inlogt met je DigiD. Patiënten hebben er inzage in al hun medische gegevens van zorgaanbieders. Men bepaalt zelf welke gegevens in het PGO komen en met welke zorgaanbieders zij welke informatie delen.

Het initiatief om gegevensuitwisseling tussen zorgaanbieders onderling te verbeteren is het implementeren van een landelijke standaard die gebruikt wordt voor een goede overdracht van patiëntgegevens. Dit is de Basisgegevensset Zorg (BgZ). Deze standaard is ontwikkeld door het Nationaal ICT Instituut in de Zorg. De BgZ bestaat uit gegevens die bijna altijd nodig zijn voor het registreren van patiëntgegevens. Dit zijn zogenaamde zorginformatiebouwstenen. Zorginformatiebouwstenen (zibs) zijn een middel om op een eenduidige wijze patiëntgegevens te registreren. Er bestaan verschillende zibs, zoals algemene patiëntkenmerken (NAW-gegevens), metingen ter ondersteuning van de zorg (bloeddruk, een bepaalde pijnscore of gewicht) en de zorgsituatie. De zibs zijn opgesteld vanuit de gedachte dat dezelfde informatie voor alle zorgaanbieders die betrokken zijn bij de behandeling van een patiënt, relevant zijn.

Al deze initiatieven zijn nog gebaseerd op vrijwilligheid. Volgens de minister moet er per zorgproces toegewerkt worden naar een wettelijke basis voor gegevensuitwisseling. Hoe deze wettelijke basis eruit gaat zien, is nog onduidelijk. Indien zorgaanbieders worden verplicht om gegevens elektronisch uit te wisselen, maar de patiënt zelf geen gespecificeerde toestemming heeft gegeven, houdt in mijn ogen de uitwisseling van gegevens van die desbetreffende patiënt op. Althans, op elektronische wijze wanneer de ene zorgaanbieder patiëntgegevens voor de andere zorgaanbieder inzichtelijk maakt (het zogenaamde pull-verkeer). Wanneer het gaat om push-verkeer zou er een tweede - met dezelfde veiligheidswaarborgen omkleed - systeem in het leven geroepen moeten worden. Hier wordt toestemming namelijk veronderstelt aanwezig te zijn. Een andere maatregel die de minister gaat vormgeven is het gebruik van dezelfde bouwstenen door verschillende zorgaanbieders. Met bouwstenen bedoelt de minister het op dezelfde manier vastleggen van medische gegevens, waardoor patiëntgegevens eenduidig worden geregistreerd.

Op basis van de brief die de minister naar de Tweede Kamer stuurde, lijkt het dat de minister niet alleen een verbetering verplicht wil stellen, maar ook de digitalisering zelf. Deze wettelijke verplichting zal bindend zijn voor zorgprofessionals, zorginstellingen en ICT-leveranciers. Het gebruik van standaardmodellen moet verplicht worden. Deze worden ingebed in de ICT van de zorgaanbieder, zodat systemen met elkaar kunnen communiceren. In ieder geval heeft het kabinet €400 miljoen beschikbaar gesteld om het doel van de minister te behalen. Op 1 januari 2020 zou een veilig, landelijk werkend systeem voor inzage en uitwisseling van medische gegevens klaar moeten zijn. Of het gaat om een verplichte landelijke infrastructuur, standaarden, wetgeving - of een combinatie daarvan - zal op 1 april 2019 duidelijk worden. Dan presenteert minister Bruins van Medische Zorg en Sport zijn plan van aanpak aan de Tweede Kamer.

Wilt u de juridische kennis binnen uw organisatie verhogen?

Dan is een inhouse training van ICTRecht iets voor u.

ICTRecht verzorgt al jaren met succes juridische trainingen, zowel voor juridische professionals (PO-gecertificeerd) als voor algemeen publiek. Een inhouse training kan volledig voor u op maat ontwikkeld worden waarbij voorbeelden uit uw eigen praktijk in het lesprogramma worden verwerkt.

Inhouse trainingen zijn ontwikkeld om de praktische kennis omtrent juridische zaken te verhogen. We oefenen aan de hand van vele voorbeelden en praktijkcases en uiteraard is er veel ruimte voor eigen inbreng. Op verzoek kunnen trainingen als PO-training voor advocaten worden gegeven.

Mogelijke onderwerpen voor een juridische inhouse training zijn:

- ICT-contracten opstellen en redigeren (gehele dag)
- De nieuwe privacywet (gehele dag)
- Open source (middag)
- Octrooieren van software (gehele dag of middag)
- E-mailmarketing en de wet (middag)
- Continuïteit en/of privacy en/of security in de cloud (gehele dag of middag)
- ICT en de curator (middag)
- Digitalisering binnen de overheid (middag)

Alisa Schurink
Opleidingscoördinator
en Marketingmedewerker
020 663 1941

Meer weten?

Bezoek ictrecht.nl/inhouse of mail met onze opleidingscoördinator via academy@ictrecht.nl

ICTRECHT
academy

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Internetrechtspraak

Rechtbank Gelderland 22 oktober 2018
(Zakelijk vergeetrecht)
(Gepubliceerd 1 januari 2019) Eisers vorderen dat Google de link, die verwijst naar een artikel van de Quote waarin wordt verwezen naar een persbericht van de FIOD over een groot onderzoek naar witwaspraktijken in relatie tot eisers, zal verwijderen uit de zoekresultaten bij een zoekopdracht op de naam van eisers. Hoofdregel is (sinds HR X/Google) dat vergeetverzoeken moeten worden toegewezen. Dat kan in bijzondere gevallen anders zijn, afhankelijk van de aard van de betrokken informatie en de gevoeligheid ervan voor het privéleven van de betrokkene en van het belang dat het publiek erbij heeft om over deze informatie te beschikken, wat met name wordt bepaald door de rol die deze persoon in het openbare leven speelt. Hier is sprake van zo'n geval: de publicatie heeft betrekking op de professionele integriteit en fiscale moraal van eiser, en het gaat om relatief recente ernstige criminaliteit.

https://bit.ly/2SO6K3p

Gerechtshof Arnhem-Leeuwarden 4 december 2018
(Geen internet)
Een man wordt door de Belastingdienst in 2015 uitgenodigd digitaal aangifte inkomstenbelasting te doen, en reageert door de brief terug te sturen met daarop handgeschreven "Ondergetekende heeft geen internet". Diverse vervolgbrieven hebben geen effect, waarop de Belastingdienst een ambtshalve aanslag oplegt. De man gaat in beroep, en formeel met succes. Voor 2014 gold de regel nog dat men op papier aangifte mocht doen op verzoek en de man is daarop niet gewezen. De ambtshalve aangifte wordt echter overgenomen, omdat geen feiten zijn bewezen dat zijn inkomstenbelasting anders had moeten worden berekend.

https://bit.ly/2Wpdk2t

Rechtbank Overijssel 5 december 2018
(Deliverables)
Eiser Vita Motion heeft een zorgrobot ontwikkeld. Het bedrijf Sintecs heeft een deel van de software van de door Vita ontwikkelde zorgrobot in opdracht van Vita verder ontwikkeld. Vervolgens is tussen partijen een discussie ontstaan over al dan niet uitgevoerde werkzaamheden en facturen, over de reikwijdte van de gegeven opdracht en over al dan niet verricht meerwerk. Na het treffen van een regeling is tussen partijen weer discussie ontstaan over al dan niet uitgevoerde werkzaamheden en verschuldigdheid van facturen, alsmede over al dan niet verricht meerwerk en hebben daarover weer veelvuldig met elkaar gecommuniceerd. Uiteindelijk vordert Vita afgifte van deliverables zoals broncodes en softwaremodules op straffe van een dwangsom. Volgens haar is de discussie over meerwerk niet relevant: betaling van meerwerk werd niet als voorwaarde gesteld in de schikking, zodat Sintecs momenteel gehouden is tot afgifte van de verlangde deliverables. Echter, de rechtbank leest de tekst anders: zij ziet staan dat de deliverables, waarvan Vita afgifte vordert, eerst door Sintecs moeten worden afgegeven wanneer overeenstemming bestaat over de gewerkte en gefactureerde uren. Immers, de tekst vermeldt "Ten aanzien van de gevorderde afgifte van de "intellectuele eigendomsrechten" (de Deliverables) wordt overeengekomen dat (1) uw cliënte bereid is om deze deliverables over te dragen, nadat overeenstemming is bereikt over punt 5 dan wel daarover in rechte is beslist".

https://bit.ly/2Fw0pVR

Gerechtshof Amsterdam 11 december 2018
(ACAB anno 2017)
Verdachte zong tijdens een voetbalwedstrijd de tekst "ACAB, ACAB" en keek daarbij naar politieagenten. Deze arresteerden hem voor belediging van een ambtenaar in functie. De verdachte verklaarde niet te weten wat deze term betekende, maar het Gerechtshof acht dat onwaarschijnlijk: uit een Google-zoekopdracht (met periode beperkt tot 2017) blijkt dat over de

afkorting (en de beledigende betekenis daarvan) zeer veel nieuwsberichten zijn gepubliceerd, zowel door regionale als landelijke media. Deze berichten kwamen mede naar aanleiding van ECLI:NL:HR:2011:BP0291 waarin juist werd gezegd dat Googelen niet mag om de bekendheid van een term vast te stellen. Het Hof concludeert nu dat gezien de landelijke bekendheid van de uitspraak en de term, deze nu wel algemeen bekend geacht wordt te zijn.

https://bit.ly/2OvqWq6

Gerechtshof Den Haag 13 december 2018
(Porno-foto's als smaad)
De verdachte heeft pornografische afbeeldingen van aangeefster met vergezellende teksten naar familieleden en collega's van aangeefster gestuurd per e-mail. Deze afbeeldingen gingen gepaard met teksten als (letterlijk): "Dit is wat ik doe bij mijn klienten (ook bij collegas) om hun te voldoen en tevreden te houden. Ik ben ook bi. Binnenkort ga ik alles op internet zetten zodat jullie weten hoe het is om een klient tevreden houden". Het hof oordeelt onder meer dat het hier gaat om duidelijk te onderkennen concrete gedragingen, en dat de afbeeldingen ook heden ten dage strijdig zijn met de positieve (seksuele) moraal. Als strafverzwarend weegt het hof daarbij mee dat de verdachte de foto's verzond met het (door hem voor aangeefster ontoegankelijk gemaakte) mailadres van aangeefster en het aldus voor deed komen of zíj degene was die de foto's verzond.

https://bit.ly/2NUlqNP

Gerechtshof Den Haag 19 december 2018
(Ziggo-Phishing)
Door middel van phishingmails in de opmaak van Ziggo heeft de verdachte slachtoffers bewogen in te loggen op een nagemaakte Ziggo website. Daarna kopieerde hij hun inloggegevens en plaatste hij bestellingen op hun naam. Nadien is verdachte overgestapt op een andere werkwijze waarbij gebruik werd gemaakt van een nep-Ziggo factuur, die melding maakte van een betalingsachterstand. Ook hierbij werden slachtoffers bewogen diverse inloggegevens te verstrekken. Dankzij de aldus verkregen inloggegevens kon de verdachte daarna via hun PayPal accounts betalingen verrichten. Het Hof heeft de verdachte veroordeeld wegens (poging tot) oplichting, diefstal, computervredebreuk, het voorhanden hebben van kwaadaardige software en het verwerven en voorhanden hebben van computerwachtwoorden om daarmee computervredebreuk te plegen. Een door de verdediging gevoerd zogenaamd "hack-verweer", erop neerkomend dat "iemand anders" dan de verdachte zich de toegang had verschaft tot een laptop van de verdachte en diens IP-adressen, heeft het Hof verworpen.

https://bit.ly/2SPaEsR

Rechtbank Den Haag 20 december 2018
(Foto's in identiteitsfraude)
Een man wordt vervolgd voor identiteitsfraude vanwege het gebruik van de foto van een ander op socialmedia-accounts. Complicatie is dat het betreffende artikel (231b Strafrecht) spreekt van "identificerende persoonsgegevens, niet zijnde biometrische gegevens" en foto's onder de definitie van biometrische (persoons)gegevens kunnen vallen. De Rechtbank ziet een uitweg: deze definitie geldt alleen wanneer deze foto's worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken (overweging 51 AVG). Daarvan is geen sprake met publicatie van een foto op social media.

https://bit.ly/2VNxymt

Rechtbank Zeeland-West-Brabant 30 januari 2019
(YouTube-hardrijder)
Een man wordt vervolgd onder artikel 5 Wegenverkeerswet voor het met meer dan 250 kilometer per uur over de snelweg rijden. Verdachte is door verbalisanten en door een getuige herkend als degene die achter het stuur van de auto te zien is. In het door verdachte op zijn YouTube-kanaal geplaatste filmpje en strafrechtelijk onderzoek wijst uit dat de geconstateerde snelheidsovertredingen op 2 juni 2016 zijn begaan. Daarnaast staat de auto op zijn kenteken. Het Hof ziet daarin genoeg om hem als dader aan te merken.

https://bit.ly/2H2LZjf

Rechtbank Amsterdam 31 januari 2019
(Vergeetverzoek bij perspublicatie)
In een verzoekschriftprocedure eist de verzoeker dat

een publicatie op internet over hem wordt verwijderd, met een beroep op artikel 17 AVG (vergeetrecht). Kern van de publicatie is dat hij producten verkoopt aan gedetineerden waarbij hij de gedetineerden oplicht. De rechtbank constateert dat het hier gaat om een journalistieke uiting, waardoor artikel 17 AVG niet geldt (artikel 43 lid 2 Uitvoeringswet AVG) zodat het verzoek moet worden afgewezen. Of het dan goede of slechte (onrechtmatige) journalistiek is, kan dan niet worden bepaald. De verzoeker zal zich tot de gewone rechter moeten wenden met een dagvaardingsprocedure gebaseerd op onrechtmatige perspublicatie.

https://bit.ly/2VHVPds

College van Beroep voor het bedrijfsleven
5 februari 2019 (ACM boete webwinkels)
ACM heeft bij besluit van 9 juni 2016 voor drie overtredingen van de Wet handhaving consumentenbescherming (Whc) bestuurlijke boetes aan een webwinkel opgelegd van in totaal € 500.000. Het betrof misleidende handelspraktijken, het onjuist terugbetalen van geld na ontbinding van koop op afstand en het werken met een 'piepsysteem' bij onvolledige retouraanmeldingen. Het Cbb is het eens met ACM dat de webwinkel consumenten onjuist voorlichtte: in principe kreeg men een waardebon in plaats van geld terug. Tevens werd geen geld terugbetaald wanneer de consument geen IBAN opgaf, maar werd de consument niet geïnformeerd over dit gebrek. De consument moest er dan zelf achteraan. Het Cbb vindt de drie feiten echter zodanig met elkaar verweven dat de boetes gematigd moeten worden.

https://bit.ly/2VElz9q

Rechtbank Midden-Nederland 8 februari 2019
(DutchFilmworks NAW-gegevens)
Filmproducent DutchFilmWorks wil individuele downloaders aanpakken en spreekt daartoe internetprovider Ziggo aan. Deze beschikt over NAW-gegevens behorende bij IP-adressen gebruikt bij het via BitTorrent downloaden van de film "The Hitman's Bodyguard" waar DFW distributierechten voor heeft. De rechtbank toetst aan Lycos/Pessers maar komt bij de afweging van belangen (vierde stap) negatief uit voor DFW: zij maakt onvoldoende duidelijk hoe zij de IP-adreshouders zal benaderen. In de pers zijn diverse bedragen genoemd die men als schadevergoeding wil eisen, echter zonder zelfs maar een begin van onderbouwing. Ook is onduidelijk hoe objectief en eerlijk DFW de vermeende inbreukmakers zal aanspreken. DFW heeft reeds hoger beroep aangekondigd. Zie de noot op pagina 32.

https://bit.ly/2ESA1WN

Rechtbank Gelderland 11 februari 2019
(Handlichting YouTuber)
Een vijftienjarige ontvangt handlichting om zelfstandig een bedrijf te gaan uitoefenen als YouTuber/influencer. Meer in het bijzonder wenst verzoeker over de navolgende bevoegdheden te beschikken: het verrichten van alle rechtshandelingen die nodig zijn om dit bedrijf uit te kunnen oefenen, waaronder het aangaan van overeenkomsten tot een bedrag van € 5.000,- en het verrichten van betalingen tot € 500,-. De beide ouders hebben ten blijke van instemming van het verzoek het verzoekschrift medeondertekend. Rechtbank wijst dit toe.

https://bit.ly/2UoS6RZ

Rechtbank Noord-Holland 20 februari 2019
(Geen koopovereenkomst via internet)
Het bedrijf Wincoop biedt cursussen aan via internet. Zij stelt een overeenkomst te hebben met eisende partij, die echter meent niet meer dan oriënterend op de site van Wincoop te hebben gekeken. Volgens eiser blijkt uit het bestelformulier niet wat de prijs voor de cursus zou zijn. Ook blijkt niet dat hij enige bestelling voor akkoord heeft aangevinkt. Hij heeft geen schriftelijke bevestiging gekregen. Zonder al te veel woorden geeft de rechtbank hem gelijk: de gegevens van eiser kunnen door iedereen zijn ingevuld, er is geen bewijs dat de overeenkomst is bevestigd (art. 6:227c lid 2 BW) en - dan ook nog eens - zonder prijs kan niet van een overeenkomst gesproken.

https://bit.ly/2tVSKuu

Niels Winters
Directeur JuriBlox B.V.

Contracten Software

10 punten waarop te letten bij het sluiten van een escrow-overeenkomst

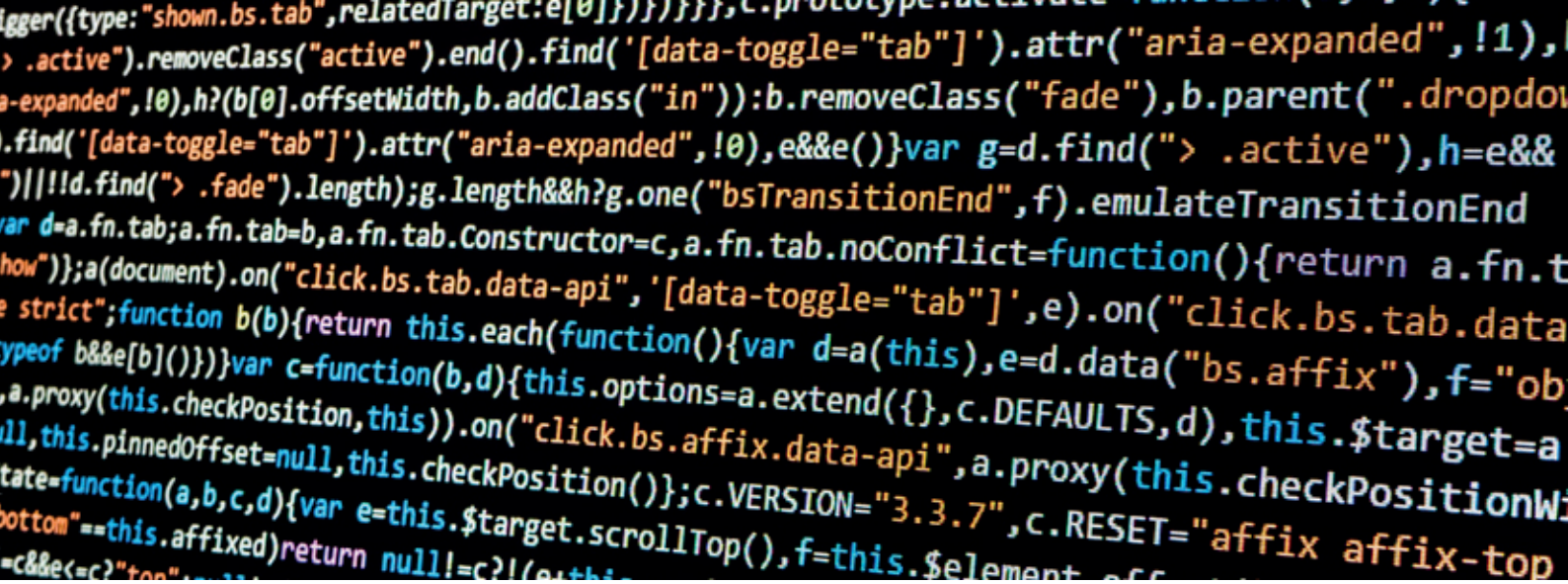
Bij klassieke escrow geeft de leverancier van software de broncode in bewaring bij een escrow-agent of een bewaarnemer. Deze partij bewaart een kopie van de broncode in een kluis tot het moment dat de leverancier niet meer in staat is de software te onderhouden (bijvoorbeeld in geval van een faillissement). Middels een escrow-overeenkomst verkrijgt de klant op dat moment de kopie van de broncode inclusief het recht op deze voor continuïteitsdoeleinden te gebruiken. De praktijk leert dat escrow-overeenkomsten er heel verschillend uit kunnen zien. Hieronder 10 punten waar op te letten bij het sluiten van een escrow-overeenkomst.

1. Past de regeling bij de praktijk?
In sommige gevallen wordt nog steeds de klassieke escrow aangeboden, terwijl er sprake is van een clouddienst. Alleen afgifte van de broncode van de software is dan niet voldoende om continuïteit te bieden voor de afnemers van de clouddienst. Er moeten aanvullende maatregelen worden getroffen ten aanzien van de beschikbaarheid van de data en het in de lucht houden van de dienst. Niet alle standaard escrow-overeenkomsten zijn dus een daadwerkelijke praktische oplossing voor continuïteit.

2. Breng alle relevante partijen en assets goed in kaart
Bij escrow is het van belang om te inventariseren welke partijen en assets relevant zijn in geval zich een calamiteit voordoet bij de softwareleverancier. Het kan hier bijvoorbeeld gaan om een hostingleverancier of een colocatieleverancier die niet meer doorbetaald wordt door de softwareleverancier als deze failliet gaat. Tevens is het van belang om te beoordelen welke assets onderdeel zijn van de dienstverlening, zoals het eigendom van de hardware. Valt deze hardware bijvoorbeeld in de boedel? Als dit niet van tevoren goed in kaart is gebracht, is het mogelijk dat de escrow-overeenkomst niet goed uitgevoerd kan worden.

3. Bij wie liggen de intellectuele eigendomsrechten?
In een inventarisatie is het van belang om vooraf duidelijkheid te hebben wie rechthebbende is ten aanzien van de software. Als je niet van tevoren goed controleert hoe het zit met de intellectuele eigendomsrechten loop je namelijk de kans dat de escrow-overeenkomst met de verkeerde partij wordt gesloten. Bijvoorbeeld de werkmaatschappij, terwijl die niet de auteursrechten heeft. Tevens kan tijdens de inventarisatie blijken dat de rechten überhaupt niet liggen bij de partij, die er zelf vanuit gaat dat hij rechthebbende is, omdat de rechten bijvoorbeeld nog bij een externe ontwikkelaar liggen. Ook kunnen verpandingen of open source componenten conflicteren met de afspraken in een escrow-overeenkomst.

4. Hoe zit het met de back-to-back afspraken?
Zoals hierboven ook aangegeven, is het van belang om de keten te kennen, die achter de softwareleverancier zit. In geval de software bijvoorbeeld een cloudapplicatie



betreft, kunnen de afspraken die de softwareleverancier met zijn toeleveranciers maakt effect hebben op de tenuitvoerlegging van de escrow-overeenkomst. De toeleveranciers moeten hun medewerking hebben toegezegd aan dergelijke constructies.

5. Regel een exit voor de escrow
Het moet mogelijk zijn om de escrow-overeenkomst op te zeggen, zowel voor de softwareleverancier als de afnemer. Wel moet dit op een manier gebeuren dat de softwareleverancier niet om 'twee voor twaalf' de escrow-overeenkomst kan opzeggen, zodat de afnemers alsnog vlak voor een calamiteit met lege handen komen te staan.

6. Meer dan alleen broncode depot
Bij cloudapplicaties is escrow meer dan broncode depot alleen, dat hebben we hierboven al gezien. Los van de continuïteit ten aanzien van de data en de hosting, kunnen ook medewerkers relevant zijn voor de continuïteit. Dit kunnen bijvoorbeeld de belangrijkste ontwikkelaars zijn of bepaalde helpdeskmedewerkers. Toegang tot deze medewerkers in geval van calamiteit moet dus onderdeel zijn van de escrow-overeenkomst.

7. Technisch en praktisch uitvoerbaar?
Bij klassieke escrow komt het nog steeds wel eens voor dat er broncodes in escrow worden genomen, die niet gecontroleerd zijn door een onafhankelijke derde. In dat geval loop je het risico dat je een escrow-object hebt dat niet geschikt is voor het doel: *het voorkomen van continuïteitsproblemen met de afnemer*. Van belang is het om met betrekking tot datgene wat in escrow wordt gebracht te controleren op of het goed gedocumenteerd, bruikbaar en overdraagbaar is. Tevens is het essentieel om periodiek het escrowproces te herhalen, zodat je zeker weet dat er een actueel escrowobject aanwezig is en dat er niets veranderd is in de auteursrechtelijke situatie.

8. Voldoet de escrow-overeenkomst aan de voorwaarden van de AVG?
Indien er persoonsgegevens worden verwerkt in het escrow-proces is het van belang om te controleren of deze conform de AVG worden verwerkt. Het is uiteraard niet de bedoeling dat de escrow-overeenkomst niet kan worden uitgevoerd, omdat dit bijvoorbeeld strijdig zou zijn met de rechten van betrokkenen. Zorg bij verwerking van persoonsgegevens voor een duidelijke wettelijke grondslag, zodat je niet voor verrassingen komt te staan bij een calamiteit.

9. Conflict over de regeling?
Check bij een escrow-overeenkomst goed wat er is afgesproken in geval er een conflict ontstaat over de tenuitvoerlegging van de overeenkomst. Wat zijn de afgiftegronden en wat gebeurt er als er een conflict is over deze gronden op het moment van calamiteit? Wat gebeurt er als er onenigheid is over het wel of niet aanwezig zijn van wanprestatie? Het is voor een afnemer van belang dat er - in geval van een calamiteit - op een zo kort mogelijke termijn continuïteit wordt geleverd. Zorg dus voor heldere afgiftegronden en goede afspraken over conflictoplossing.

10. Geen conflicterende afspraken
Zorg ervoor dat er in de escrow-overeenkomst geen afspraken staan, die conflicteren met de andere afspraken. De afspraken in de licentieovereenkomst of in de SLA moeten er niet voor zorgen dat de tenuitvoerlegging van de escrow-overeenkomst in gevaar komt. Zo kan er in de licentieovereenkomst staan dat de overeenkomst eindigt bij faillissement van de softwareleverancier. Een geldige licentie is echter wel nodig om een beroep te kunnen doen op de escrow-overeenkomst. Zorg er dus voor dat deze afspraken op elkaar aansluiten.

juriblox

The future of legal automation

JuriBlox **bespaart u tijd**. De interactieve tool helpt u **razendsnel** aan **juridische documenten** of **adviezen** die 100% relevant zijn. Met slimme automatisering **voorkomt** u tijdrovend handmatig maatwerk en onnodige fouten.

Begin vandaag met juridische innovatie!

Geïnteresseerd in de mogelijkheden van JuriBlox of wilt u de tooling en kennis uitproberen?

juriblox.nl

Neem contact op met **Mark Hoogewerf** voor informatie over de mogelijkheden

020 229 33 45 **of**
m.hoogewerf@juriblox.nl

JuriBlox B.V.
Jollemanhof 8a
1019 GW Amsterdam

020 229 33 45
info@juriblox.nl
juriblox.nl

JuriBlox

Documenten op maat

JuriBlox helpt u bij het opstellen van documenten op maat, waaronder privacyverklaringen, (sub-)verwerkersovereenkomsten en arbeidsovereenkomsten. De documenten stelt u samen aan de hand van een interactieve vragenlijst. Deze maakt elk document volledig toegesneden op uw situatie en doelstellingen. Bovendien zorgt JuriBlox ervoor dat alle teksten up-to-date blijven met nieuwe regelgeving.

JuriBlox

Toegang tot kennisbank

Beschik direct over de benodigde juridische kennisbank en stel de documenten op maat samen met de documentgenerator. Met onze kennispartners bieden wij een breed scala aan gebruiksklare templates. Word automatisch voorzien updates aan templates en stel uw documenten op aan de hand van de juiste en laatste versie. De gerenommeerde kennispartners zijn specialisten in hun vakgebied.

JuriBlox

Portaal voor uw klanten

Biedt uw klanten de mogelijkheid om zelfstandig documenten te genereren middels een gepersonaliseerd klantenportaal. Uw klanten kunnen de door u ter beschikking gestelde documenten gemakkelijk op maat maken door gebruik te maken van de interactieve vragenlijst, geheel zonder uw tussenkomst!

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Noot bij Rechtbank Midden-Nederland 8 februari 2019

(DutchFilmworks NAW-gegevens)

Al enige jaren houdt DutchFilmWorks (DFW) de gemoederen in Nederlands downloadland bezig. Men wil illegale downloaders van hun filmrepertoire actief aanspreken op dit onrechtmatig handelen, en daarbij ook 'boetes' – pardon, schadevergoeding – van ze vorderen. Deze keuze wijkt af van de handelwijze die stichting BREIN al ruim een decennium voert, waarbij wordt gefocust op grote uploaders en platforms, en bovendien ingezet wordt op staken en pas bij herhaling (contractuele) boetes worden gevorderd. Maar in theorie is de werkwijze van DFW natuurlijk natuurlijk legaal, alleen moesten er nog wat hobbels worden genomen.

In theorie is het vrij simpel om achter illegale downloaders aan te gaan. Wie op Bittorrent up- of downloadt, zal daarbij immers zijn IP-adres onthullen aan de andere 'peers' in het netwerk (de zwerm, in computertaal). Een rechthebbende, of het ingeschakelde opsporingsbedrijf, kan zich simpelweg aansluiten op dat netwerk en doen alsof hij het bestand ook wil hebben. De IP-adressen van aanbieders komen dan vanzelf binnen. Daarmee kun je dan naar de betreffende internetproviders om NAW-gegevens te eisen, waarna je de betreffende persoon sommeert en aanklaagt.

Juridisch gezien ligt dit iets complexer. Allereerst is sprake van grootschalige verwerking van persoonsgegevens met als doel het aanpakken van onrechtmatig handelen, dan wel strafbare feiten. Daarvoor is onder art. 31 Wbp (toenmalig recht) toestemming van de Autoriteit Persoonsgegevens (AP) nodig. Dat duurde even, mede vanwege diverse bezwaren die door derden (waaronder 'auteur dezes') naar voren waren gebracht over de betrouwbaarheid van het proces dat DFW had geschetst. Uiteindelijk oordeelde de AP dat de bezwaren allen terzijde gezet moesten worden en dat het aangepaste protocol (gepubliceerd 6 december 2017 in de Staatscourant) rechtmatig was.

DFW toog daarop aan de slag en inventariseerde diverse Ziggo-klanten die zonder toestemming de film 'The Hitman's Bodyguard' downloadden via BitTorrent. Vervolgens stapte men naar de rechter met als eis de afgifte van NAW-gegevens, zodat deze personen konden worden aangesproken. Dat zou in principe een formaliteit moeten zijn geweest; het Lycos/Pessers arrest uit 2006 biedt immers een toetsingskader dat bij auteursrechtinbreuk eigenlijk vrij evident in het voordeel van de rechthebbende uitpakt.

In de tussentijd was echter de AVG aangenomen en dat gaf de advocaten van Ziggo nieuw vuur om de legaliteit van dit arrest ter discussie te stellen. Een inbreuk op privacy en verwerking van persoonsgegevens vereist een specifieke wettelijke basis (het zijn immers grondrechten) en art. 6:162 BW is natuurlijk weinig specifiek te noemen. De rechtbank passeert dit fundamentele bezwaar vrij makkelijk:

het begrip ‘wet’ is in het EVRM namelijk niet beperkt tot de wet in formele zin, maar strekt zich uit over het gehele nationale recht (dus ook het ongeschreven recht), mits het nationale recht voldoende toegankelijk is en de gevolgen daarvan voorzienbaar zijn. Daaraan is voldaan met een arrest van de Hoge Raad. Ik verwijs naar de al wat oudere analyse van Sil Kingma, “de botsing tussen IE- en privacyrechten” (Privacy & Informatie Afl. 2012-4, p. 171-176 of https://www.ie-forum.nl/artikelen/de-botsing-tussen-ie-en-privacyrechten-1) voor een uitgebreidere kritiek.

Een tweede nieuw bezwaar tegen de Lycos/Pessers aanpak betrof de invulling van de belangenafweging, het vierde element van de toets uit dit arrest. De klassieke invulling daarvan betrof eigenlijk altijd simpele botsingen tussen rechten, zoals bij een klokkenluider die via de omweg van inbreuk op IE-rechten wordt achtervolgd. Hier ziet de rechtbank een ander, maar ook stevig belang: hoe gaat DFW vervolgens deze juridisch niet onderlegde consumenten aanspreken, en hoezo lezen wij daarbij termen als ‘boete’ en uit de lucht gegrepen getallen als €150 in de pers?

De hoogte van een schadeclaim bij een online inbreuk is natuurlijk vaak een zeer heikel issue, vergelijk de vele zaken waarin fotografen met allerlei tarieflijsten of zelfverzonnen bedragen duizenden euro’s onderbouwen voor één foto. En zeker bij dit soort consumenten-downloadzaken is het zeer de vraag wat die schade zou moeten zijn.

Hoofdregel van de HR (hoewel alweer uit de jaren vijftig) is dat de gemiste licentie-inkomsten de beste benadering is voor de schade. Dat werkt bij professionele relaties, maar hoe vertaalt dit zich naar de consumentensituatie? Is dat dan de aanschafprijs van de film en moeten we dan kijken naar de kosten van de DVD, de luxe Blu-Ray Special Edition of de eenmalig kijken-prijs bij online aanbieder Videoland? Of nemen we dan 1/30e uit het duurste abonnement van all-you-can-eat streaming-koning Netflix?

DFW heeft in haar persbericht van 21 december 2017 kenbaar gemaakt dat zij de houder van het IP-adres direct een schikkingsvoorstel van €150 zal doen (hoewel zij in de Volkskrant nog meldt aan “honderden euro’s’ per geval” te denken). Dat voelt in alle gevallen wat hoog en vooral nogal arbitrair. Dat sancties bij de handhaving van het auteursrecht doeltreffend en evenredig moeten zijn en de sancties ook een bijzondere preventieve werking moeten hebben, betekent echter niet dat er ruimte is voor punitieve elementen bij een schadevergoeding, aldus de rechtbank. Populair gezegd: u wilt boetes opleggen, en daar is het schadevergoedingsrecht niet voor.

Aanverwant is het punt dat Ziggo zich afvraagt of haar klanten wel bestand zijn tegen het ‘geweld’ van DFW en haar juridisch adviseurs. Er zijn bijvoorbeeld geen standaardbrieven overlegd, zodat niet kan worden ingeschat of DFW op zakelijke wijze zal uitnodigen tot een gesprek over een vermeende onrechtmatige daad, of in typische 'blafbrieftaal' zal spreken van een inbreuk op intellectuele eigendomsrechten (hierna te noemen: de Strafbare Inbreuk), waarbij men opdracht heeft rechtsmaatregelen te treffen inclusief een volledige proceskostenvergoeding dewelke kan oplopen tot €8.000 conform het door de Rechtspraak goedgekeurde tarievenmodel, maar indien u nu een bedrag van €150 betaalt (hierna te noemen: de Boete) zal hiervan worden afgezien. De laatste werkwijze zou niet geheel conform Nederlands recht zijn.

Zoals de rechtbank het formuleert: “De opmerking van DFW ter zitting dat er een brief zal worden gestuurd en dat er dan rustig zal worden afgewacht wat de reactie zal zijn, is erg mager, zeker in de omstandigheid dat de inhoud van de brief niet (voldoende) bekend is.” Alles bij elkaar concludeert men dan ook dat de belangenafweging door DFW niet duidelijk genoeg onderbouwd is. De vordering wordt dan ook afgewezen.

Nadrukkelijk blijft de deur openstaan om met een beter onderbouwde vordering terug te komen, bijvoorbeeld door redelijk klinkende sommatiebrieven te overleggen en aan te geven hoe om te gaan met klachten dat sprake is van persoonsverwisseling, een downloadende huisgenoot et cetera en een onderbouwing van de €150. DFW heeft aangegeven in hoger beroep te gaan.

Van onze blog

Privacy Innovatie

21 februari 2019

Een analyse op basis van je DNA; veilig voor je privacy?

In een artikel van RTL Nieuws[1] konden we gisteren (20 februari) lezen dat je het DNA van je baby kunt laten testen. Hieruit komt bijvoorbeeld naar voren of je kind later meer een denker of een doener wordt en of hij of zij kans maakt marathons te rennen of niet. "Veel persoonlijker dan je DNA wordt het niet", zo staat vermeld op de website van het bedrijf. En dat klopt. Met een DNA-test worden genetische gegevens verzameld die unieke informatie verschaffen over een (pasgeboren) persoon. Hoe zit het met het verwerken van deze gegevens op basis van de huidige privacywetgeving?

Bijzondere persoonsgegevens
De AVG is van toepassing wanneer er persoonsgegevens worden verwerkt. Een persoonsgegeven is alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Met een DNA-test worden genetische gegevens verzameld. Volgens de AVG vallen deze gegevens onder de categorie "bijzondere persoonsgegevens". Bijzondere persoonsgegevens zijn vanwege de gevoeligheid hiervan door de wetgever extra beschermd. Voor deze categorie geldt dan ook: verwerking is verboden, tenzij de AVG een uitzondering maakt.

Data delen met derde partijen
De persoonsgegevens die worden verzameld met de DNA-test, die ook beschikbaar is voor volwassenen, kunnen interessant zijn voor derde partijen. Bijvoorbeeld voor wetenschappelijk onderzoek. Het delen van deze persoonsgegevens met derden is verboden, tenzij er een uitzondering uit de AVG geldt. Eén van de uitzonderingen is uitdrukkelijke toestemming. Het bedrijf deelt de DNA-data ook alleen met derde partijen als er expliciete toestemming wordt gegeven. Tot zover gaat het dus goed. Overigens geldt wel dat een eenmaal gegeven toestemming altijd weer kan worden ingetrokken. Dit is niet in de privacyverklaring opgenomen, terwijl dit op basis van de AVG wel verplicht is. Daarnaast zijn er ook een paar andere zaken die onduidelijk of onvolledig op de website staan vermeld.

Data ontdoen van NAW-gegevens
Als je toestemming hebt gegeven om je data te delen voor bijvoorbeeld wetenschappelijk onderzoek, dan wordt de data ontdaan van alle NAW-gegevens. Volgens het bedrijf is de data op deze manier niet meer te herleiden tot jou als persoon en worden daarom nooit persoonsgegevens gedeeld met andere partijen. Genetische gegevens verschaffen echter unieke informatie over een natuurlijke persoon en zijn dus altijd herleidbaar. Er is dus nog steeds sprake van persoonsgegevens wanneer enkel de NAW-gegevens worden gewist.

Verwerkersovereenkomst sluiten
Omdat er bij het delen van de DNA-data persoonsgegevens worden verwerkt, moeten er afspraken worden gemaakt tussen het bedrijf en de derde partij. In de privacyverklaring van het bedrijf staat dat er een verwerkersovereenkomst wordt gesloten als data wordt doorgestuurd. Een verwerkersovereenkomst moet worden gesloten tussen een verwerker en een verwerkingsverantwoordelijke. In het geval van wetenschappelijk onderzoek is de derde partij die de data ontvangt echter geen verwerker. Deze derde partij zal namelijk niet in dienst van het bedrijf werken en zal zelf het doel en de middelen voor de verwerking bepalen. Een verwerkersovereenkomst is daarom niet de juiste overeenkomst. Overigens wordt met het sluiten van verwerkersovereenkomsten

1. https://bit.ly/2DXJnis

erkend dat de gegevens nog herleidbaar zijn. Voor het overdragen van anonieme gegevens is namelijk helemaal geen verwerkersovereenkomst nodig.

Bewaartermijnen

Als laatste nog een opmerking over de bewaartermijnen. Op de website van het bedrijf is te vinden dat DNA-samples drie maanden na de analyse worden vernietigd. Maar welke bewaartermijn geldt er voor de andere persoonsgegevens, zoals de analyse zelf? Volgens de privacyverklaring worden persoonsgegevens niet langer bewaard dan nodig om de dienst te leveren. Onduidelijk blijft echter hoe lang dit precies is. Wanneer er geen toestemming wordt verleend voor het delen van deze gegevens, zouden de afgeleide samplegegevens ook na drie maanden verwijderd moeten worden. Het doel van de gegevensverwerking, het informeren over de DNA-analyse, is dan namelijk bereikt.

Houd grip op je gegevens

Met een DNA-test worden bijzondere persoonsgegevens verzameld, waar zorgvuldig mee moet worden omgegaan. Hoewel zo'n test voor je baby of voor jezelf grappig en interessant kan zijn, moet er wel duidelijk worden geïnformeerd over wat er met deze persoonsgegevens gebeurt. Op dat vlak is er nog werk aan de winkel.

Deze blog is geschreven in samenwerking met werkstudent Demi Rietveld.

Auteur
Dries Lawrence
Juridisch adviseur

Privacy | Contracten | Overheid

11 maart 2019

Patiënt, let op uw dossier!

De complete inboedel van het MC Slotervaart ziekenhuis staat sinds vorige week via een online veiling te koop. Dit is het gevolg van het faillissement van het ziekenhuis op 25 oktober 2018.[1] Een MRI-scan, hartritme-apparaat of ziekenhuisbed nodig? Vanaf 10.000 euro kan er meegeboden worden op een MRI-scan. Maar wat gebeurt er met de achtergebleven patiëntendossiers?

Vele medische dossiers blijven achter

Voor de verkoop zijn alle patiëntengegevens gewist. Wat achter is gebleven in de kelders van het ziekenhuis zijn honderdduizenden medische dossiers met privacygevoelige informatie van patiënten. Opeisen van medische dossiers door patiënten als eigendom van de patiënt is niet mogelijk. Noch een arts van het ziekenhuis, noch een patiënt heeft het juridisch eigendom van een medisch dossier. Het ziekenhuis is wel eigenaar van de gegevensdrager (de computer of het papieren dossier). Doordat de patiënt geen eigenaar is van het medisch dossier, kan hij het dossier ook niet opeisen. De patiënt heeft wel bepaalde rechten met betrekking tot de inhoud van het medisch dossier. Zo heeft de patiënt het recht om de gegevens in te zien, zo nodig aan te vullen, te corrigeren, te vernietigen of daarvan een afschrift te krijgen.

Oplossing voor de medische dossiers

Voor medische dossiers van patiënten die nog onder behandeling van een arts staan, geldt een eenvoudige oplossing. In het kader van de Wet op de geneeskundige behandelovereenkomst worden deze overgedragen aan de nieuw behandelend artsen met toestemming van de patiënt.

1. https://bit.ly/2Juvqeh

Voor medische dossiers van patiënten die niet meer onder behandeling van een arts staan, is de oplossing wat ingewikkelder. Voor medische dossiers geldt een bewaarplicht van 15 jaar na de laatste behandeling (ook indien patiënt inmiddels overleden is). Wat er met oude dossiers moet gebeuren, is nog onduidelijk. Op dit moment wordt het archief met de medische dossiers onderhouden door medische professionals die worden ingehuurd door de curator. Dit is echter een tijdelijke oplossing.

Wie is verantwoordelijk?
De verantwoordelijkheid voor het beheer van het medisch dossier ligt bij het ziekenhuis. Het feit dat het Slotervaart ziekenhuis failliet is verklaard, dan eindigt daarmee nog niet de bewaarplicht. De wettelijke verplichting is niet gekoppeld aan het behoud van de status van de hulpverlener. Dit zou de plicht in deze situaties inhoudsloos maken. De bewaarplicht van een zorginstelling om medische dossier te bewaren, impliceert dat de zorginstelling tijdig geschikte maatregelen dient te treffen om te zorgen dat de dossiers correct bewaard blijven. Het treffen van deze maatregelen wordt gezien als onderdeel van de uitvoering van de bewaarplicht. De vraag is of het treffen van deze maatregelen onder de werkzaamheden van de curator vallen, indien het Slotervaart deze maatregelen niet heeft getroffen. Een curator verricht zijn werk ten behoeve van de gezamenlijke schuldeisers en niet in het belang van het failliete ziekenhuis.

Stichting als de oplossing?
Voor de continuïteit van de zorg is het van belang dat de verantwoordelijke voor de medische dossiers ervoor zorgt dat de dossiers beschikbaar zijn en beschikbaar blijven. Deze verantwoordelijkheid kan niet zomaar worden overgedragen aan een andere instelling. Een zorgverzekeraar, die in het kader van de continuïteit van de zorg, de verantwoordelijkheid kreeg over de patiëntenzorg, heeft onder geen beding toegang tot het medische dossier. Het onderbrengen van de medische dossiers in een stichting lijkt een goede oplossing.

Dit was een oplossing bij een vergelijkbare zaak in de VS. De rechter oordeelde daar dat de rechten van de ex-patiënten zwaarder wogen dan de claims van de andere schuldeisers. Ten koste van de schuldeisers werd er geïnvesteerd in een stichting waar de patiëntdossiers ondergebracht werden. Uiteindelijk moet er op basis van goed hulpverlenerschap gehandeld worden en moet een oplossing gevonden worden waarbij patiëntdossiers van levende patiënten – waarbij de bewaarplicht van 15 jaar nog niet verstreken is en die al dan niet nog onder behandeling van een arts staan – niet op straat komen te liggen.

Wij zien benieuwd wie de verantwoordelijkheid krijgt voor het beheer van de medische dossiers van het Slotervaart ziekenhuis. Wij houden u op de hoogte!

Auteur
Tessa van Schijndel
Juridisch adviseur

Trainingsoverzicht april 2019 – september 2019

Voor juridische professionals

Dinsdag 16 april 2019 en donderdag 26 september 2019

Contracteren: de basis (6PO)

Contracteren ligt aan de wortel van een groot deel van het ICT-recht. ICT-contracten kennen verschillende types, van softwarelicentie tot resellerovereenkomst en van algemene voorwaarden tot mantelcontract. Elk contract vereist algemene aandachtspunten en daarnaast specifieke aspecten.

https://bit.ly/2rjRy19

Dinsdag 14 mei 2019 en dinsdag 24 september 2019

Privacy en persoonsgegevens: de basis (6PO)

In deze dagtraining wordt de AVG op hoofdlijnen uitgewerkt om zo het kader voor een zorgvuldige omgang met persoonsgegevens te kunnen realiseren.

https://bit.ly/2s4yA12

Donderdag 16 mei 2019

Legal tech: modulair contracteren II (4PO)

Middels de JuriBlox-tooling worden juridische documenten opgesteld. Een senior adviseur is daarbij in staat nieuwe sjablonen op te stellen en standaardbepalingen te redigeren voor gebruik in dergelijke sjablonen. Zo kan hij effectief zijn kennis uitdragen aan collega's.

https://bit.ly/2QDgn81

Dinsdag 21 mei 2019

Ondernemen: verdienmodellen en financiering (4PO)

Geld verdienen kan op vele manieren, zeker binnen de ICT waar innovatieve modellen snel getest en gerealiseerd kunnen worden. Denk aan abonnementen, betalingen middels credits of advertentiegebaseerde modellen. Een belangrijke rol hierbij speelt de investeerder zoals de venture capitalist: de financiering van ICT-diensten is niet altijd eenvoudig.

https://bit.ly/2BSrEJG

Dinsdag 18 juni 2019

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

Donderdag 27 juni 2019

Legal tech: slimme contracten en blockchain (4PO)

Legal technology of legal tech zal de sector transformeren. Documenten worden met slimme hulpmiddelen samengesteld, bestaand werk verandert wezenlijk van aard en de klassieke taken van de jurist worden steeds vaker door geautomatiseerde diensten vervangen of aangevuld. Blockchaintechnologie en smart contracts zijn te beschouwen als een nieuwe juridische innovatie. Gebruikers kunnen in slimme contracten afspraken maken en die vastleggen in programmeertaal. Zodra het slimme contract in de blockchain is geplaatst, kunnen gebruikers met dit slimme contract interacties aangaan. De gevolgen die deze interacties hebben zijn afhankelijk van wat in het slimme contract is geprogrammeerd.

https://bit.ly/2m3TyK8

Dinsdag 2 juli 2019

Privacy en persoonsgegevens: de verdieping (6PO)

Privacywetgeving kent open normen en grijze gebieden. Als jurist moet u deze kunnen identificeren en op een deskundige en begrijpelijke wijze naar de praktijk kunnen vertalen. Tijdens de training leert u onder meer over binding corporate rules, de verwerkersovereenkomst, registers en de Functionaris Gegevensbescherming.

https://bit.ly/2rk8VPi

Donderdag 4 juli 2019

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

Donderdag 5 september 2019

Technologie: werking internet II (4PO)

Technische kennis stelt de ICT-jurist in staat om de vertaalslag te maken van het juridische naar het technische en vice versa. In de huidige tijd waarbij ICT grotendeels online wordt geleverd, is kennis van de werking van het internet daarbij cruciaal.

https://bit.ly/2EiXXCJ

Dinsdag 10 september 2019

Cloud en software: beschikbaarheid van clouddiensten (4PO)

Outsourcing naar de cloud brengt enorme afhankelijkheid mee. Gebruikers van clouddiensten moeten daarom altijd afspraken maken over beschikbaarheid. Verlies van data of dienst kan immers leiden tot bedrijfsdiscontinuïteit. Daarbij wordt onderscheid gemaakt tussen tijdelijke onbeschikbaarheid en definitieve onbeschikbaarheid. De eerste situatie kan met een goede service level agreement (SLA) worden opgevangen, de tweede vereist exit- of continuïteitsafspraken.

https://bit.ly/2TUcB8M

Dinsdag 17 september 2019

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 19 september 2019

Cloud en software: softwarerecht (4PO)

Om te kunnen adviseren over cloud en software moet de ICT-jurist software kunnen kwalificeren en bekend zijn met de relevante wetten en de contractspraktijk. De ICT-jurist moet creatief zijn en wetten en regels vertalen, zodat ze zoveel mogelijk toepasbaar blijven op voortschrijdende technologie.

https://bit.ly/2ASguRb

Voor algemeen publiek

Donderdag 12 september 2019

Update Algemene Verordening Gegevensbescherming (AVG)

Wij praten u in een middag bij over de belangrijkste veranderingen die de Europese vervanger van de Wbp, de Algemene Verordening Gegevensbescherming (AVG), met zich mee heeft gebracht. Over hoe u onder de AVG moet omgaan met persoonsgegevens, beveiliging en datalekken, en wanneer een Functionaris Gegevensbescherming verplicht is. De insteek van de training is praktijkgericht.

https://bit.ly/2UfAf06

ICT en Gezondheidsrecht

Dinsdag 23 april 2019

Medische gegevens: medisch dossier gerelateerd
https://bit.ly/2TV4SHA

Medische gegevens: buiten het medisch dossier
https://bit.ly/2Gx8LPM

Binnen de zorg wordt op grote schaal geïnnoveerd en gedigitaliseerd. Het is daarbij van groot belang om de juridische aspecten van de omgang met medische gegevens te constateren en daarmee aan de slag te gaan. In deze training maakt u kennis met de relevante wet- en regelgeving in de zorg en ICT én de praktische uitwerking daarvan. Daarnaast leert u te werken met (standaard) IT-contracten in de zorg.

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