ICTRECHT
adviesbureau

ICTRECHT
IN DE PRAKTIJK

jaargang 8 nummer 2 april 2020

Brexit is een feit: hoe zit het met mijn leveranciers in het VK?

De toekomst van AI in het recht

Auteursrecht op software

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 - Boeken

Meer informatie over hoe wij werken? Bezoek ictrecht.nl

ICTRECHT
adviesbureau

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 en Opleidingsdirecteur
a.engelfriet@ictrecht.nl
Steven Ras Algemeen directeur
s.ras@ictrecht.nl

Alisa Schurink Opleidingscoördinator en Marketingmedewerker
a.schurink@ictrecht.nl
Anouk van Rijn Juridisch adviseur
a.vanrijn@ictrecht.nl
Bram de Vos Juridisch adviseur
b.devos@ictrecht.nl
Demi Grandiek Juridisch adviseur
d.grandiek@ictrecht.nl
Jay Remmelzwaal Juridisch adviseur
j.remmelzwaal@ictrecht.nl
Jorien Zwaneveld Juridisch adviseur
j.zwaneveld@ictrecht.nl
Laura Monhemius Juridisch adviseur
l.monhemius@ictrecht.nl
Linde Mensink Juridisch adviseur
l.mensink@ictrecht.nl
Maarten van Beek Juridisch adviseur
m.vanbeek@ictrecht.nl
Nicole Waaijer Marketing adviseur
n.waaijer@ictrecht.nl
Sari Jansen Juridisch adviseur
s.jansen@ictrecht.nl
Eline Pellis Grafisch ontwerper
eline@elinepellis.com
Leonard Fäustle Stills & Motion
foto's ICTRecht
info@leonardfaustle.nl

Laura Monhemius
Juridisch adviseur

Privacy

Brexit is een feit: hoe zit het met mijn leveranciers in het Verenigd Koninkrijk?

Het heeft een goede 3,5 jaar geduurd, maar op 17 oktober 2019 bereikten de Britten en de Europese Unie (EU) eindelijk een uittredingsakkoord. Op 31 januari 2020, middernacht was het dan zover: de Britten stapten uit de EU en Brexit was een feit. Het proces kostte het land uitdagende onderhandelingen, twee premiers en vele beslissende dagen. Voor velen leidde dit tot een dag van grote vreugde, terwijl anderen deze historische gebeurtenis eerder zagen als een zwarte bladzijde in de geschiedenis. Wat staat de Britten namelijk te wachten: zelfstandigheid en onafhankelijkheid, of chaos en onduidelijkheid? In dit artikel schetsen we de mogelijke risico's op het gebied van privacy en het (laten) verwerken van persoonsgegevens in het Verenigd Koninkrijk (VK).

'Business as usual'?

De grootste horde lijkt genomen, maar niets is minder waar: een no-deal Brexit is nog steeds mogelijk. Tot en met 31 december 2020 geldt er in ieder geval een overgangsfase. Dat betekent dat tot het eind van dit jaar alle Europese wetten en regels gewoon blijven gelden in het VK. Voor burgers, maar ook voor bedrijven verandert er vrijwel niks in 2020. Dat betekent niet dat men stil hoeft te zitten. Deze periode is bedoeld ter voorbereiding op de nieuwe afspraken tussen het VK en de EU over hun toekomstige relatie. Mochten partijen er niet uitkomen, dan kan de overgangsfase eenmalig verlengd worden met twee jaar tot 31 december 2022. Premier Johnson is echter niet van plan daar gebruik van te maken. Komen de afspraken niet rond? Dan volgt alsnog een no deal-Brexit op 1 januari 2021.

Tot en met 31 december 2020 blijven zowel de Algemene verordening gegevensbescherming (AVG) als de Britse uitvoeringswet daarvan – de *UK Data Protection Act* – dus gewoon gelden in het VK. Voor de huidige verwerkingen van persoonsgegevens dus (nog) geen paniek: hosting in het VK is bijvoorbeeld voor nu geen probleem. De *Information Commissioner's Office* (ICO), de Britse privacytoezichthouder, is hier ook duidelijk over: tot het eind van dit jaar is het *business as usual*. Iedere organisatie die persoonsgegevens verwerkt, binnen en buiten het VK, heeft zich aan de AVG te houden.

Zit ik nu dus veilig met mijn Britse (IT-)leverancier?

De ICO heeft als uitgangspunt dat, deal of no-deal, de AVG na de overgangsperiode zal worden geïmplementeerd als de *'UK GDPR'* (de Engelse term voor de AVG) en dat er hoe dan ook dus praktisch weinig zal veranderen. Als zo'n *UK GDPR* er spoedig komt, gaat men ervan uit dat de Europese Commissie zo snel mogelijk een adequaatheidsbesluit zal nemen over het VK. Ter opfrissing van het geheugen: dat betekent dat de Commissie heeft bepaald dat het land een vergelijkbaar beschermingsniveau heeft op het gebied van persoonsgegevens als de EU. Het land wordt hiermee als 'veilig' bestempeld om persoonsgegevens naar

door te geven. Landen zonder zo'n stempel zijn 'derde landen', waarvoor op een andere manier passende waarborgen dienen te worden getroffen om persoonsgegevens te beschermen. Tot nu toe is dit besluit genomen voor een handjevol landen, waaronder Argentinië, Canada (alleen voor commerciële organisaties), Japan en Nieuw-Zeeland.

Dit klinkt logisch en lijkt meteen de gemakkelijkste en meest praktische oplossing, maar de AVG blijft de strengste privacywetgeving ter wereld. Het is dus zeer aantrekkelijk voor lobbyisten om te proberen hier en daar wat woordjes en komma's toe te laten voegen en toch aan dat beschermingsniveau af te doen. Hoe meer er aan de Britse AVG gesleuteld gaat worden, hoe kleiner de kans dat we na de overgangsperiode veilig zitten in het VK en hoe langer het gaat duren totdat zo'n besluit genomen gaat worden, als het al genomen gaat worden.

Wat te doen na 31 december 2020?
In plaats van te wachten of er wel of niet een adequaatheidsbesluit gaat komen, zoekt een aantal organisaties heil in de *Standard Contractual Clauses* (SCC's of modelclausules) om de doorgifte naar het VK te dekken. De door de Europese Commissie opgestelde modelclausules dekken ofwel de doorgifte van een Europese verantwoordelijke naar een niet-Europese verantwoordelijke, ofwel de doorgifte van een Europese verantwoordelijke naar een niet-Europese verwerker. De SCC's dekken niet alle doorgifte-situaties: wat nou als je als Nederlandse softwareleverancier (lees: verwerker) een Britse hostingpartij (lees: subverwerker) hebt ingeschakeld? Partijen proberen hier nog wel eens contractuele oplossingen voor te zoeken, zoals volmachten vanuit de verantwoordelijke, maar praktisch is het niet. Los daarvan zijn de modelclausules niet alleen oud (respectievelijk uit 2001, 2004 en 2010), ze zijn ook zwaar bekritiseerd door zowel contracterende partijen als toezichthouders. Daar bovenop komt nog dat lang niet alle Britse organisaties bereid zijn om de SCC's te accepteren.

Een ander aandachtspunt is het grote aantal aan reeds gesloten verwerkersovereenkomsten. Het sluiten van zo'n overeenkomst is weliswaar verplicht, maar ze zijn daardoor ook sterk gestandaardiseerd en weinig kritisch uitonderhandeld. Ze bevatten vaak standaardbepalingen als 'doorgifte naar landen buiten de Europese Economische Ruimte is alleen toegestaan met toestemming van Verwerkingsverantwoordelijke', of hetzelfde voor het inschakelen of wijzigen van subverwerkers. Wanneer het VK een derde, juridisch gezien onveilig, land wordt, plaatst dit verwerkers in een lastige situatie: welke verwerkingsverantwoordelijke gaat nog toestemming geven voor subverwerkers in het chaotische en onzekere Brexit-land? En komt die toestemming er

dan niet, is het dan kiezen uit twee kwaden: ofwel het contract beëindigen, ofwel alle data verhuizen naar een Europese leverancier? Het blijft afwachten hoe dit in de praktijk zal gaan uitpakken en hoe organisaties hiermee omgaan.

Wellicht nodeloos om te vermelden, maar een laatste manier om veilig te zitten is om alle betrokkenen toestemming te vragen voor doorgifte naar een derde land. Dit is natuurlijk allerminst efficiënt.

Afsluitend
Zowel Europese als Britse organisaties hoeven zich op dit moment nog geen zorgen te maken over hun Britse (sub)leveranciers vanwege de overgangsperiode. Dat betekent niet dat ze stil moeten zitten. We raden aan om de ontwikkelingen rondom de Brexit nauwlettend in de gaten te houden. De kans op een no-deal Brexit is namelijk nog steeds aanwezig en zelfs bij een deal blijft het goed opletten.

Het inschakelen van een (sub)leverancier in het VK is na de overgangsperiode juridisch gezien waarschijnlijk niet helemaal zuiver. Er kan worden gekozen voor verhuizen naar de EU (duur), voor het sluiten van modelclausules, of men wacht een adequaatheidsbesluit van de Commissie af met het risico dat in de tussentijd gegevens worden verwerkt in een land zonder passende waarborgen (lees: overtreding van de AVG). Wat commercieel gezien de meest wenselijk oplossing is, blijft aan een organisatie zelf.

Bram de Vos
Juridisch adviseur

Wet- en regelgeving

Besluit veiligheid en integriteit telecommunicatie in werking
Op 6 december 2019 is het Besluit veiligheid en integriteit telecommunicatie in werking getreden. Het besluit vloeit voort uit een eerder advies van een interdepartementale *taskforce* onder leiding van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Deze taskforce werd ingesteld na waarschuwingen vanuit de inlichtingen- en veiligheidsdiensten voor spionage door buitenlandse overheden via telecomnetwerken. De taskforce heeft onderzocht of de huidige beveiligingsmaatregelen die aanbieders van dergelijke netwerken nemen afdoende zijn. Geconcludeerd werd dat aanvullende maatregelen nodig zijn, zowel ten aanzien van de genomen beveiligingsmaatregelen als ten aanzien van de door netwerkaanbieders gebruikte producten en diensten. Het besluit biedt een wettelijke basis om invulling te geven aan de aanbevelingen van de taskforce. Zo biedt het besluit een grondslag om beveiligingseisen op te leggen aan netwerkaanbieders, alsmede om hen te verplichten bepaalde producten of diensten via "vertrouwde leveranciers" in te kopen.

https://bit.ly/32vkNl6

Internetconsultatie mkb-vriendelijke Rijksoctrooiwet 1995
Op 18 december 2019 is er een internetconsultatie gestart over een beleidsnota met concrete voorstellen ter modernisering van de Rijksoctrooiwet 1995. De vernieuwingen die in de nota worden voorgesteld, hebben tot doel om het Nederlandse octrooisysteem toegankelijker te maken voor met name het mkb. Met de beleidsnota wordt een vervolg gegeven aan een eerdere evaluatie van het Nederlands intellectueel eigendomsbeleid uit 2018. De voorstellen zijn erop gericht om de octrooiprocedures te vereenvoudigen, de waarde van een Nederlands octrooi te vergroten en de handhavingsmogelijkheden te verbeteren. Voorgesteld wordt onder meer om het mogelijk te maken een "voorlopige aanvraag" in te dienen zodat alvast een indieningsdatum wordt verkregen. Daarnaast wordt geopperd om een aanvraag (op verzoek van de aanvrager) vooraf te laten toetsen op de materiële vereisten. Ook wordt onder meer een laagdrempelige oppositieprocedure voorgesteld. De internetconsultatie staat open tot en met 2 maart 2020.

https://bit.ly/2PrnTks

Invoering UBO-register uitgesteld
De geplande invoering van het UBO-register is uitgesteld. Op grond van de vierde en vijfde anti-witwasrichtlijn (richtlijn (EU) 2015/849 en richtlijn (EU) 2018/843) zou het register eigenlijk per 10 januari 2020 in moeten gaan, maar de daarvoor benodigde implementatiewet is nog niet aangenomen door de Eerste Kamer. De implementatiewet bevat verplichtingen met betrekking tot het registreren van de *Ultimate Benificial Owner* (UBO) van een onderneming. Dit is de natuurlijke persoon die de uiteindelijke zeggenschap heeft over een juridische entiteit zoals een vennootschap, stichting of vereniging. Het is de bedoeling dat deze informatie in de toekomst vastgelegd wordt in het Handelsregister van de Kamer van Koophandel. Streven is nu om het UBO-register in het voorjaar in te laten gaan.

https://bit.ly/2TiqmPA

Verklaring ICO over privacyrechtelijke gevolgen van de Brexit
Op 29 januari 2020 heeft de Information Commissioner's Office (ICO), de Britse privacytoezichthouder, een korte verklaring gepubliceerd over de juridische gevolgen van de Brexit. De toezichthouder benadrukt dat er in ieder geval een transitieperiode geldt tot 31 december 2020. Tot die tijd blijft het dan ook *"business as usual"* en zullen bedrijven de bestaande richtsnoeren van de toezichthouder moeten volgen. Hoe het wetgevingskader er na de transitieperiode uit komt te zien, is vooralsnog onduidelijk. Zie het artikel op pagina 4.

https://bit.ly/3a7jfQx

EARN IT Act heeft potentieel gevolgen voor toepassing sterke versleuteling

Op 30 januari 2020 publiceerde persbureau Bloomberg een conceptvoorstel voor de Amerikaanse Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT Act). Critici wijzen erop dat het voorstel negatieve gevolgen kan hebben voor het gebruik van end-to-end-encryptie door Amerikaanse technologiebedrijven. In het wetsvoorstel wordt een nationale commissie geïntroduceerd die *best practices* moet vaststellen ter voorkoming van de verspreiding van online materiaal over exploitatie van kinderen. Deze best practices kunnen onder andere betrekking hebben op het opsporen van dergelijke materialen en het bewaren en verstrekken van bewijs hieromtrent. Dit is technisch niet mogelijk indien communicatie volledig versleuteld is. Indien een technologiebedrijf de best practices niet naleeft, kan dit resulteren in eigen aansprakelijkheid. Indirect zou het voorstel daarom tot gevolg kunnen hebben dat bedrijven zich genoodzaakt zien zwakheden en/of achterdeuren in te bouwen in hun software. Riana Pfefferkorn van de Stanford Law School schreef een uitgebreide kritiek.

https://bloom.bg/380cS0e en
https://stanford.io/2wdAZLn

SyRI in strijd met het EVRM

Op 5 februari 2020 oordeelde de Rechtbank Den Haag dat het Systeem Risicoindicatie (beter bekend als SyRI), dat bedoeld is om fraude met sociale voorzieningen op te sporen, in strijd is met artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM). Het systeem werd in 2014 middels een wijziging van de Wet structuur uitvoeringsorganisatie en inkomen (Wet SUWI) ingevoerd. Volgens de eisers zijn de betreffende artikelen uit de Wet SUWI in strijd met hoger recht. De rechtszaak werd aangespannen door een coalitie van verschillende partijen, waaronder het Nederlands Juristen Comité voor de Mensenrechten (NJCM) en Stichting Privacy First. De rechtbank erkent dat het systeem een legitiem doel dient, maar komt tot het oordeel dat de SyRI-wetgeving de toets van noodzakelijkheid, proportionaliteit en subsidiariteit niet doorstaat. Op grond van het transparantiebeginsel, het doelbindingsbeginsel en het beginsel van dataminimalisatie komt de rechtbank tot het oordeel dat de wetgever er niet in is geslaagd om een *'fair balance'* tussen de verschillende belangen te vinden. De rechtbank verklaart dan ook voor recht dat de bestreden wetgeving onverbindend is wegens strijd met artikel 8 EVRM.

https://bit.ly/381AOjJ

Aankondiging wetsvoorstel digitale uitwisseling medische gegevens

Op 11 februari heeft Minister Bruins aangekondigd dat hij ziekenhuizen en klinieken wil verplichten om onderling digitaal gegevens uit te wisselen. De minister geeft aan dat hij daarvoor dit jaar nog met een wetsvoorstel komt. Om te zorgen dat ziekenhuizen en klinieken snel aan de wetgeving kunnen voldoen, wordt er 75 miljoen euro subsidie beschikbaar gesteld.

https://bit.ly/2TnJ1t0

Tweede kamer neemt Wetvoorstel digitale overheid aan

Op 18 februari 2020 heeft de Tweede Kamer het Wetsvoorstel digitale overheid aangenomen. Deze wet regelt verdere digitalisering van de Nederlandse (semi-) overheid. De wet bevat onder meer een grondslag om open standaarden aan te wijzen die overheden moeten hanteren in het elektronisch verkeer met andere overheden, burgers en bedrijven. Daarnaast introduceert het wetsvoorstel een zorgplicht voor de Minister van Binnenlandse Zaken en Koninkrijksrelaties voor de werking, beveiliging en instandhouding van de generieke digitale infrastructuur (GDI). Ook worden eisen gesteld aan het gebruik van elektronische identificatiemiddelen door de (semi-)overheid. De veiligheid van het huidige DigID wordt niet langer toereikend geacht voor bepaalde toepassingen, bijvoorbeeld voor diensten met betekenisvolle rechtsgevolgen. De bedoeling is dan ook dat er een nieuw elektronisch identificatiemiddel komt dat over een hoger betrouwbaarheidsniveau beschikt.

https://bit.ly/3c7iuc5

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Innovatie Cloud

De toekomst van AI in het recht

Het idee is hardnekkig: de robots en/of de AI's komen eraan, en ze gaan onze juridische banen inpikken. Waarbij de illustrator van dienst dan vaste prik een robot in toga tekent die een vlammend betoog ter behoud van de democratische rechtsstaat houdt, of een moeilijk dossier leest met de vinger bij de betreffende regel. Allemaal leuk en aardig maar legal tech en robots gaan helemaal niet het werk van advocaten overnemen of automatiseren. Ze gaan de maatschappij transformeren zodat dat werk irrelevant of een beperkte niche wordt.

Hoe hard zwemt een onderzeeboot

Als vakgebied bestaat AI al vele decennia, maar wat het nu precies is daar is niemand het tot nu toe over eens geworden. Mijn ietwat cynische samenvatting is dat AI haast per definitie een hype is, een belofte voor wat binnenkort mogelijk wordt: zodra het gewoon kán, vinden we het een algoritme oftewel softwaretruc die gewoon wat rekent. Zodra we zien dat het kan, is het niet meer fascinerend.

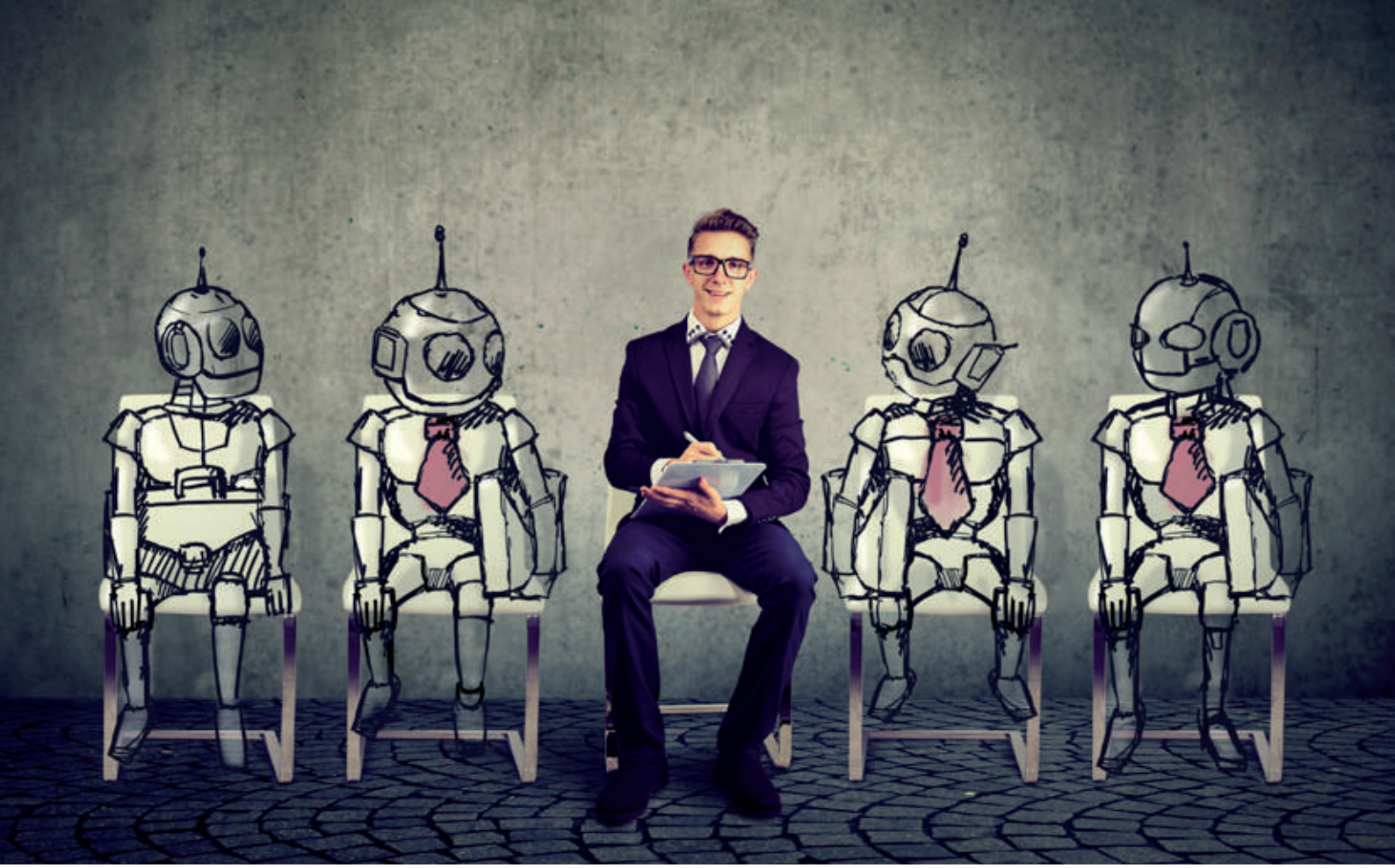
Dat wil niet zeggen dat AI niet innovatief kan zijn. Er zijn de afgelopen jaren vele doorbraken geweest die echt een revolutie in de dataverwerking en -analyse hebben gerealiseerd. Belangrijk daarbij is wel dat u voor ogen houdt dat het eigenlijk niet gaat om een nieuwe intelligentie, maar om een andere manier van conclusies trekken. Zoals de Nederlandse computerwetenschapper en -filosoof Edsger Dijkstra het formuleerde: "The question of whether machines can think, is about as relevant as the question of whether submarines can swim". Computers denken niet, ze opereren volstrekt anders. Maar wat ze daarmee kunnen doen, kan best eens betere resultaten opleveren dan menselijk denken.

De doorbraken in de afgelopen jaren gingen met name over de algoritmes. Hoe kom je van een berg data tot een manier om tot uitspraken over nieuwe input te komen? Hoe ga je snel door die data heen, hoe generaliseer je metingen tot de best passende algemene lijn? Nieuwe algoritmes, en vooral ook nieuwe supersnelle hardware en gigantische geheugenruimte, hebben daarin dingen mogelijk gemaakt die voorheen gewoon écht niet haalbaar waren.

De belangrijkste ontwikkeling op dit gebied was die van *deep learning:* algoritmes die patronen leren herkennen in verschillende fases, waarbij geprobeerd wordt het leerproces (goed of fout herkend) te laten werken zoals menselijke hersencellen ook werken. Dit staat ook wel bekend als neurale netwerken. Maar in de kern komt het eigenlijk altijd neer op statistische analyse waarbij verbanden in grote hoeveelheden data worden gezocht om daarmee algemene regels te formuleren.

Een simpel voorbeeld: ploeg door miljoenen aankopen bij Albert Heijn heen om te zien wat vaak samen gekocht wordt, zie dat een aankoop van diepvriesmaaltijden vaak samen gaat met bier, en dan kun je mensen die een gekoelde stamppot kopen met grote kans op succes aanraden om eens een witbiertje te kopen.

Dit blijkt verbazingwekkend effectief, zelfs als je geen idee hebt waaróm diepvrieseten en bier vaak samen gekocht worden. Wij mensen zijn heel erg goed in het zien van oorzakelijke verbanden, en dat is een risico bij AI: deze analyses trekken conclusies op basis van correlaties, samenloop, en niet op basis van causaliteit, oorzakelijk verband. De computer heeft geen idee maar ziet twee dingen samen gaan dus daar kunnen we wat mee. En dat werkt.



Robots in toga
Dat het werk van advocaten en rechters heel moeilijk te automatiseren is geloof ik graag. Het “heeft een hoge creativiteitsfactor”, zo zegt ABN Amro-bankier en sectorspecialist Han Mesters in de NRC. Slimme argumenten, spitsvondige reacties, aanvoelen wat de rechter eigenlijk wil horen, een schikkingsvoorstel verzinnen dat de emotie van de wederpartij erkent, in een duister uitziende zaak toch een lichtpuntje vinden én met onvermoeibaar pleiten daar de winst uit slepen – nee, daar zie ik vooralsnog geen computerprogramma voor komen.

Software is goed in het automatiseren van het gewone, het alledaagse. Het vinden van afwijkingen, het controleren van patronen, het doen van extrapolaties. Dat is heel iets anders dan het soort maatwerk waar de advocatuur voor staat. Dat zie ik meteen. En om die reden hoef je je inderdaad nul zorgen te maken dat je pleitwerk overgenomen wordt door een robot in een toga.

De rol van AI in het recht
Er zijn verschillende niveaus om een AI in te zetten in juridische analyses. Een eerste, simpele mogelijkheid is een AI in te zetten als een aparte pre-check: mensen kunnen hun aanvraag of verzoek door een AI laten bekijken, die dan zijn bevindingen geeft. Dit verandert niets aan het eigenlijke traject en is vergelijkbaar met even informeel een medewerker bellen met de vraag of je aanvraag in principe akkoord is. Het zal schelen in de kansloze aanvragen en je kunt mensen tips geven om een aanvraag sterker te maken.

Meer winst krijg je als organisatie door de AI als eerste filter in te zetten. De aanvraag of het verzoek wordt dan eerst door de AI bekeken, en de bevindingen worden dan aan de behandelend medewerker verstrekt. Deze kan dan bijvoorbeeld zien of er afwijkingen zijn op bepaalde componenten, of welke onderdelen speciale aandacht nodig hebben. Dat verkleint de doorlooptijd, want een aanvraag waar de AI niets bijzonders aan ziet, kan dan eenvoudiger worden toegewezen. Een risico is natuurlijk dat de AI iets mist en de mens daar niet meer naar kijkt.

Nog sneller gaat het wanneer je die categorie “niets bijzonders” direct goedkeurt. Met zo’n *raketloket* win je nog meer tijd, omdat er nu in het geheel geen mens meer zit tussen de aanvraag en de positieve beoordeling. Uiteraard zit hier kans op fouten (een vals positief) maar je kunt dan steekproefsgewijs een handmatige controle uitvoeren, of de AI een voorlopige beoordeling laten geven en toezeggen dat een mens binnen zeg 14 dagen nog kan piepen. Dat laatste haalt natuurlijk de snelheid er weer uit, want varen op een voorlopige beslissing zal niet iedereen aandurven.

Een afwijzing van het raketloket
Spannender wordt het als de AI ook negatieve beslissingen gaat nemen. Want een AI die met enige zekerheid kan zeggen dat iets mag, kan net zo goed zeggen dat het niet mag. En dan krijg je dus een raketloket waar je ook binnen 5 seconden hoort dat het niet mag, wat je wilt. In ieder geval geldt dan dat de AI in staat moet zijn het besluit te motiveren. En dat is lastig, omdat AI analyses meestal zonder uitleg komen. Deze mail is spam en die niet, je kunt beter linksaf gaan want dat is sneller, of als je in het spel nu schiet dan heb je de meeste kans om te winnen. Zelden tot nooit krijg je erbij te horen waarom dan. Maar omdat het heel vaak klopt, vinden we dat ook niet erg.

Vanuit juridisch perspectief kan dat toch eens best vervelend zijn, zeker als sprake is van een AI die juridisch bindende besluiten neemt. Uw bouwvergunning wordt afgewezen, u komt niet in aanmerking voor verkorte screening, u dient een extra cursus te volgen voordat u mag beginnen met deze studie. Die zorg gaat zo ver dat in de AVG expliciet is opgenomen dat dergelijke besluiten niet genomen mogen worden maar dat er altijd een mens tussen moet zitten, én dat er uitleg over de onderliggende logica van het besluitondersteunende systeem moet komen.

De toekomst van AI in het recht
Wat AI doet, is eigenlijk vooral automatiseren van het juridisch werk. Beter gezegd: het bulkwerk, de standaardzaken. De 80% - al die zaken die zo standaard zijn dat het vonnis niet eens publicatiewaardig is op Rechtspraak.nl. En het is dat bulkwerk wegnemen waar AI goed in is en waar het echt toegevoegde waarde gaat bieden.

Automatiseren is nooit het simpelweg automatisch doen van wat je voorheen handmatig deed. Toen de treinen van stoom naar elektrisch gingen, werden stokers overbodig en moesten machinisten hun vak opnieuw leren. Er kwam geen robot die schepjes diesel in de oven gooide. Datzelfde gaat gebeuren in de juridische sector. De bulk van het proceswerk is standaard, en dáár is software goed in om te verwerken. Daarom gaat 80% van de advocaten minder werk krijgen. Die software zoekt de standaardzaken uit, en er is dan geen advocaat meer nodig die daar nog eens zijn/haar zegje over doet.

Ja, natuurlijk zullen er dan altijd nog rare gevallen zijn waarbij je wél een advocaat zou willen. Een mens die jou uit het bureaucratisch geweld van de machines plukt. Maar dat zullen zeldzame situaties zijn, en ik heb zelfs serieuze twijfels of die nieuwe systemen daar rekening mee gaan houden. Wie procedures ontwerpt, houdt zelden rekening met de rare gevallen. En zonder rare gevallen geen behoefte aan voorvechters om daar uit te komen.

Sari Jansen
Juridisch adviseur

Contracteren | Cloud

Valkuilen bij de algemene inkoop-voorwaarden gezondheidszorg

Bij het aanbieden van uw ICT-diensten is het meestal niet aantrekkelijk om direct de juridische aspecten van een mogelijke samenwerking te bespreken. U wilt graag tot een opdrachtverlening komen, zonder dat daaraan een ellenlange juridische discussie aan voorafgaat. Daardoor lijkt het verleidelijk om de algemene inkoop-voorwaarden van uw (potentiële) klant gewoonweg te accepteren. Hoe makkelijk dit ook lijkt, vaak is oplettendheid wel geboden.

In de zorgbranche krijgt u veelal de Algemene Inkoop-voorwaarden Gezondheidszorg (AIVG 2017) voor-geschoteld. De VGN, ActiZ, GGZ Nederland, NVZ en NEVI-zorg, Intrakoop IAZ en Santeon hebben gezamen-lijk deze inkoopvoorwaarden ontwikkeld. Hierin zijn de regels opgenomen waaraan een leverancier of opdracht-nemer zich dient te houden. Afhankelijk van uw type dienstverlening, zijn er een aantal belangrijke onder-werpen waar u als ICT-leverancier op bedacht moet zijn. In dit artikel brengen wij enkele bepalingen onder de aandacht.

Aansprakelijkheid

Het beperken van aansprakelijkheid is een van de heetste hangijzers in de discussie over de juridische inhoud van de contracten. De aansprakelijkheid is immers het risico dat u als ICT-leverancier op u neemt. Als algemeen uitgangspunt wordt regelmatig gezegd dat de omvang van de aansprakelijkheid in verhouding moet staan tot de waarde van de deal. Spreekt u contractueel niets af over aansprakelijkheid, dan geldt de wet. Dat betekent dat ingeval u aansprakelijk bent, u de daardoor ontsta-ne schade in principe volledig moet vergoeden.

De AIVG 2017 kent een flinke verbeterslag ten opzichte van de eerdere versie van de AIVG uit 2014. Zo zijn de boetes geschrapt en is de aansprakelijkheid van de leverancier beperkt. De laatste versie neemt in artikel 20 als uitgangspunt dat de leverancier aansprakelijk is voor *directe* schade die door de zorginstelling of door derden wordt geleden. Directe schade is geen begrip uit de Nederlandse wet, maar wordt in het aanspra-kelijkheidsartikel wel gedefinieerd. Onder directe schade wordt in feite alle schade verstaan die door de zorg-instelling of derden wordt geleden als gevolg van het niet tijdig of niet volledig nakomen van de verplichtingen uit de overeenkomst door de ICT-leverancier. Er zijn een aantal schadeposten uitgezonderd van de vergoedings-plicht, waaronder bedrijfsschade en winstderving. De schadevergoedingsverplichting bedraagt € 1.250.000,- per gebeurtenis met een maximum van € 2.500.000,- per jaar. U dient zich daarvoor genoeg-zaam te verzekeren.

Afhankelijk van de opdrachtwaarde en de omvang van de mogelijk te lijden schade zijn deze schadeplafonds wel of niet proportioneel. Bij kleine ICT-projecten zullen

de genoemde bedragen veelal niet in verhouding staan tot de opdrachtwaarde. Houd er daarnaast rekening mee dat uw verzekering op de schadebedragen dient aan te sluiten. Het verdient de voorkeur om een maatwerk aansprakelijkheidsartikel te formuleren, die past bij de te leveren ICT-diensten; de schade die daaruit kan ontstaan en in verhouding staat tot de contractswaarde.

Vrijwaringen
Er zijn op verscheidene plekken in de AIVG 2017 vrijwaringen opgenomen. Een vrijwaring houdt kortgezegd in dat u de zorginstelling afschermt tegen een claim die een derde bij de instelling neerlegt. Dat betekent dat u de discussie voert met de betreffende derde en –als het zo ver komt- de procedure moet voeren bij de rechter en de kosten moet dragen. Belangrijk om te vermelden is dat een beperking van aansprakelijkheid niet geldt voor een vrijwaring. Bij een vrijwaring zult u dus alle kosten moeten dragen, zoals de schadevergoeding en de advocaatkosten. Als u bent verzekerd voor aansprakelijkheid, is het maar de vraag of de verzekeraar bij een vrijwaring tot uitkering zal overgaan. Een plicht tot vrijwaring is immers geen verplichting tot het vergoeden van schade. Bij een vrijwaring gaat u verder: u betaalt ook de kosten en dergelijke die niet als schade bij u zouden zijn gekomen. Het is daarom altijd verstandig om uw verzekeringspolis te raadplegen voordat u een dergelijke vrijwaring accepteert. Daarnaast kunt u overwegen om de vrijwaringen uit te sluiten of met meer waarborgen voor u te omkleden.

Intellectuele eigendom
De term “Product” omvat krachtens de definitielijst van de AIVG 2017 ook vermogensrechten. Onder vermogensrechten zoals bedoeld in het Burgerlijk Wetboek vallen ook de (op software rustende) rechten van intellectuele eigendom. Het is niet helemaal duidelijk of het de bedoeling is dat intellectuele eigendomsrechten onder het begrip “Product” vallen. Dit is wel van belang, omdat onder andere artikel 9 van de AIVG 2017 bepaalt dat het eigendom van het Product na volledige betaling overgaat op de zorginstelling. Het uitgangspunt van overdracht van de intellectuele eigendomsrechten zien we ook op andere plekken terug: zo bepaalt artikel 17.3 dat de leverancier die

een specifieke prestatie ontwikkelt, alle intellectuele eigendomsrechten bij voorbaat aan de zorginstelling zal overdragen. De Module Informatie- en Communicatietechnologie (ICT) van de AIVG 2017 maakt overigens wel een onderscheid tussen software met een gebruiksrecht en maatwerksoftware. Bij het laatste dient de leverancier de intellectuele eigendomsrechten over te dragen aan de zorginstelling.

Om daadwerkelijk een overdracht te bewerkstelligen, is een schriftelijk ondertekend stuk (een akte van overdracht) nodig. De overdracht kan dus niet via algemene (inkoop)voorwaarden. De zorginstelling kan de overdracht en de medewerking daaraan op basis van de AIVG 2017 wel van u afdwingen. Het is echter niet altijd wenselijk en/of nodig om intellectuele eigendomsrechten over te dragen, omdat een gebruiksrecht op software vaak ook volstaat voor hetgeen de klant met de software voor ogen heeft. Daarnaast kan de overdracht van de rechten voor u ook zeer onverstandig zijn, voornamelijk wanneer u de software ook voor andere klanten wilt kunnen inzetten. Maak hier dus heldere (afwijkende) afspraken over.

Levering van SaaS
Voor wat betreft de levering van ICT-diensten geldt de Module ICT aanvullend op de algemene module van de AIVG 2017. Wanneer u als ICT-dienstverlener Software-as-a-Service (SaaS) levert, kunnen bepaalde artikelen uit deze module mogelijk problematisch voor u zijn. Op grond van artikel 9 heeft u voorafgaande toestemming van de zorginstelling nodig voor het doorvoeren van een update waarin u een bepaalde functionaliteit beëindigt. Afhankelijk zijn van de voorafgaande toestemming van één specifieke klant is onwerkbaar wanneer u updates en upgrades centraal doorvoert. Ook bent u verplicht om bij het uitkomen van een upgrade en update oudere versies minimaal 24 maanden te ondersteunen. Dit is bij de levering van SaaS niet (altijd) mogelijk. Controleer daarom kritisch wat in de praktijk werkbaar voor u is en formuleer waar nodig uitsluitingen en/of aanpassingen in de overeenkomst.

Prijsafspraken en betaling
Wanneer u uw dienstverlening in abonnementsvorm aanbiedt en/of er sprake is van een duurovereenkomst, kan het commercieel aantrekkelijk zijn om uw prijzen ieder jaar eenzijdig te mogen aanpassen op basis van inflatie. Op basis van artikel 5 van de AIVG 2017 zijn de prijzen echter vast voor de duur van de overeenkomst. Wilt u als leverancier uw prijzen verhogen, dan dient u hierover dus eerst in gesprek te gaan met de zorginstelling. Voorts zijn in de AIVG 2017 vrij vergaande bevoegdheden van de zorginstelling neergelegd om de betaling op te kunnen schorten. Deze bevoegdheid bestaat bijvoorbeeld al op het moment dat er een tekortkoming in de nakoming door de leverancier door de zorginstelling wordt geconstateerd of wanneer de factuur niet alle vereiste gegevens bevat. Dit is strenger dan de wettelijke regeling omtrent opschorting. Een dergelijke opschortingsbevoegdheid kan voor u erg vervelend zijn, omdat er daarmee onzekerheid kan ontstaan met betrekking tot de ontvangst van betalingen.

Conclusie
Ondanks de goede bedoelingen van de initiatiefnemers voor de AIVG 2017, zijn in de voorwaarden voornamelijk de belangen van de zorginstelling ondervangen. In dit artikel zijn een aantal aandachtspunten voor u als ICT-leverancier uiteengezet. Beoordeel kritisch welke risico's acceptabel voor u zijn en ga in gesprek over de dealbreakers. Bestaat er weinig ruimte voor aanpassingen op detailniveau, probeer dan in ieder geval de overeenkomst zo uit te onderhandelen dat de meest ongunstige bepalingen niet van toepassing worden verklaard.

PRIVACY VERIFIED

Verander wetgeving in een strategisch wapen

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

Lisette Meij
Directeur ICTRecht Privacy

Demi Grandiek
Juridisch Adviseur

020 6631941
info@privacyverified.nl

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

Jorien Zwaneveld
Legal assistant
ICTRecht Groningen

Cloud

Auteursrecht op software

Bedrijfsprocessen zijn tegenwoordig steeds meer afhankelijk van IT: producten worden verkocht via internet, financiën worden bijgehouden in speciale administratieprogramma's, communicatie verloopt voornamelijk via e-mail, het telefoonverkeer gaat via het internet en interne documenten worden opgeslagen in de cloud. Digitalisering in het bedrijfsleven is een feit. Achter al deze vormen van digitalisering zit een groep programmeurs die een leeg veld hebben gevuld met code, waaruit deze software is ontstaan. Hoe zijn de inspanningen van de programmeurs beschermd? En hebben de gebruikers het eigendom van de software, of alleen het gebruiksrecht?

Werk

Software kan worden beschermd via het auteursrecht. Om auteursrechtelijke bescherming te krijgen, moet een voortbrengsel worden aangemerkt als 'werk'. In de Auteurswet staat expliciet dat computerprogramma's en het voorbereidend materiaal als werk zouden kunnen worden beschouwd (art. 10 lid 1 onder 12 Auteurswet). De software moet dan wel een "eigen oorspronkelijk karakter" hebben, hetgeen inhoudt dat de software niet ontleend mag zijn aan andere al bestaande software. Daarnaast moet de software het "persoonlijk stempel van de maker" bezitten. Dit is volgens de Hoge Raad het geval wanneer de software het resultaat is van eigen scheppende menselijke arbeid en creatieve keuzes, en dus een voortbrengsel is van de menselijke geest.[1] In hetzelfde arrest heeft de Hoge Raad ook een ondergrens gegeven voor het werk: het voortbrengsel mag niet zo banaal of triviaal zijn dat het aan creatieve arbeid ontbreekt.

Bestaat de software alleen in onderdelen die nodig zijn voor het verkrijgen van een technisch effect, dan is de software geen auteursrechtelijk werk.[2] In het BSA-arrest oordeelde het Hof van Justitie EU dat onderdelen van een grafische gebruiksinterface die slechts worden gekenmerkt door hun technische functie, niet als oorspronkelijk kunnen worden aangemerkt.[3] Dit is anders wanneer de interface blijk geeft van creatieve keuzes zodat er geen sprake is van *enkel* technische effecten.

In de literatuur wordt vaak de vuistregel gehanteerd: is het denkbaar dat twee makers, onafhankelijk van elkaar, precies hetzelfde werk maken? Zo nee, dan is er al snel sprake van een werk. Daaruit kan afgeleid worden dat hoe uitgebreider de software is, hoe groter de kans dat er creatieve keuzes gemaakt zijn, en dus dat er sprake is van een auteursrechtelijk beschermd werk (mits niet louter technisch functioneel). Uit de rechtspraak blijkt dat vaak kleine, taakgerichte software geen persoonlijke stempel van de maker bezitten omdat deze taakgerichte software vooral technisch functioneel bepaald is.

De Softwarerichtlijn, Softwarewet en Auteurswet onderscheiden niet naar het soort of type software. De omvang van de auteursrechtelijke bescherming reikt daarom in principe tot alle soorten software: van device drivers tot games. Zowel de broncode als de objectcode worden door de Auteurswet beschermd.

1. HR 30 mei 2008, ECLI:NL:HR:2008:BC2153 (*Endstra/Uitgeverij Nieuw Amsterdam*).
2. HR 16 juni 2006, ECLI:NL:PHR:2006:AU8940 (*Lancôme/Kecofa*).
3. HvJ EU 22 december 2010, C-393/09, ECLI:EU:C:2010:816 (*Svaz softwarové ochrany/Ministerstvo kultury,Softwarová*).

De manier waarop de software beschikbaar is gesteld, dus of het op een drager staat of als download beschikbaar is, maakt voor de bescherming ook niet uit. De enige eisen voor bescherming zijn namelijk de eisen van een werk: het eigen oorspronkelijke karakter en de persoonlijke stempel van de maker.

Hierbij bestaat echter wel de ondergrens dat alleen de concrete uitdrukkingsvorm van de software is beschermd. Ideeën die aan het programma ten grondslag liggen of de probleemoplossingen en functionaliteiten die de software biedt, zijn niet via het auteursrecht beschermd. Dit lijkt op het eerste oog misschien vreemd omdat de waarde van de software vaak juist in de functionaliteiten van de software zit. Het zou echter onwenselijk zijn om de functionaliteiten van de software te beschermen omdat dit tot ongewenste monopolies zou leiden.

Twee programma's met dezelfde functionaliteiten zouden in dat geval niet naast elkaar kunnen bestaan omdat de oorspronkelijkheid van het tweede programma zou ontbreken, ook al zijn de programma's volledig los van elkaar ontwikkeld. Andersom zou het tweede programma door dezelfde functionaliteit altijd inbreuk maken op het eerder ontwikkelde programma. Het gevolg hiervan is dat de softwareontwikkeling sterk beperkt zal worden. Er bestaat hier een duidelijk spanningsveld: de functionaliteiten die waarde geven aan het programma, die je als maker juist beschermd wil zien, zijn niet per se beschermd in het Auteursrecht.

In de praktijk is het lastig om te beoordelen wanneer iets louter technisch functioneel is, of dat er toch creatieve keuzes gemaakt zijn. Ik denk wel dat standaard technisch functionele mogelijkheden voor het vergemakkelijken van het gebruik van de software, zoals een "terug"-knop met een pijltje naar links, of een "menu"-icoon met drie streepjes, niet auteursrechtelijk beschermd worden.

Makerschap

Het is van belang om te bepalen wie de maker van de software is, aangezien de maker auteursrechthebbende is. De maker heeft het alleenrecht tot openbaarmaking en verveelvoudiging van de software. De maker bepaalt dus of de software verspreid wordt, aangeboden wordt voor verkoop of bewerkt mag worden. Ook het gebruik van de software valt onder de verveelvoudiging en openbaarmaking, waardoor de maker in beginsel toestemming moet geven om de software te mogen gebruiken.[4]

4. Is er eenmaal toestemming voor gebruik van de software, dan hoeft er geen verdere toestemming gevraagd te worden voor het normale gebruik hiervan.

Het begrip ‘maker’ is een specifiek begrip, aangezien de *auteursrechtelijke maker* niet de *feitelijke programmeur* hoeft te zijn. Wanneer de software wordt vervaardigd in opdracht van een werkgever, en de werknemer als programmeur de code van de software schrijft, zal het auteursrecht toekomen in principe aan de werkgever.

Ook wanneer het werk naar ontwerp van een ander en onder diens leiding en toezicht is gemaakt, lopen de auteursrechtelijke maker en feitelijke maker uiteen. Degene die leiding geeft en toezicht houdt wordt als maker van het werk aangemerkt. De wetgever gaf hier het voorbeeld van schilders zoals Rubens die zich lieten bijstaan door leerling-helpers. Het auteursrecht komt in principe toe aan Rubens, niet aan de leerling-helpers.

Hoe zit het dan als bedrijf X in opdracht van bedrijf Y software ontwikkelt? Meestal wordt de ontwikkeling van software uitbesteed aan een andere partij, wanneer de kennis en kunde voor de ontwikkeling bij de opdrachtgever ontbreekt. Hier kan vaak niet gesproken worden over leiding en toezicht van de opdrachtgever, omdat de softwareontwikkelaar het ontwerp maakt naar eisen van de functionaliteiten van de software. Het is dan ook de persoonlijke stempel van de softwareontwikkelaar die op het werk staat, niet die van de opdrachtgever.

Het is belangrijk om je in zo’n geval te realiseren dat de softwareontwikkelaar het auteursrecht heeft. De softwareontwikkelaar kan dan bepalen wat er met de software gaat gebeuren, of en onder welke voorwaarden de software gebruikt mag worden. Hier is het contractenrecht van groot belang.

Gebruiksrecht en softwarelicenties
De opdrachtgever kan op twee manieren aanspraak maken op het gebruik van het programma. Allereerst kan het auteursrecht worden overgedragen aan de opdrachtgever. Dit is niet automatisch het geval indien het programma wordt ‘gekocht’ en dit zal dus apart geregeld moeten worden. De opdrachtgever heeft dan de exclusieve bevoegdheden die de maker normaal heeft. De softwareontwikkelaar maakt na de overdracht geen aanspraak meer op deze openbaarmakings- en verveelvoudigingshandelingen: het auteursrecht komt volledig bij de opdrachtgever te liggen.

Omdat veel softwareontwikkelaars niet staan te springen om het auteursrecht over te dragen, wordt het gebruik van de software vaak geregeld in licenties. In de softwarelicentie wordt geregeld welk gebruik wel en niet is toegestaan, hoeveel gebruikers er mogen zijn, hoe lang de software gebruikt mag worden en eventueel de exclusiviteit van de licentie. Dit laatste houdt bijvoorbeeld in dat de softwareontwikkelaar slechts aan één partij een gebruikslicentie geeft waarmee het exclusieve gebruik voor een bepaalde periode wordt gegeven. Anderzijds kan een licentie ook heel ruime gebruiksrechten geven. Vaak gaat het daarbij om zogeheten open source licenties.

Conclusie
Al voordat de software wordt geprogrammeerd en er concrete ontwerpplannen op tafel komen te liggen, is het belangrijk om na te denken over bepaalde aspecten van het auteursrecht. Naast de prijs van het project, is het ook raadzaam om vast te leggen wie auteursrechthebbende is, of dit overgedragen gaat worden en zo ja, onder welke voorwaarden, of dat er enkel gebruik wordt gemaakt van een (exclusieve) licentie, al dan niet in combinatie met escrow.

Maarten van Beek
Juridisch adviseur

Contracteren | Cloud

Intellectuele eigendomsrechten bij overname SaaS leverancier: waar moet u op letten?

Bedrijven nemen steeds meer Software-as-a-Service (SaaS) diensten af die gebruikt worden om bijvoorbeeld de salarisadministratie te automatiseren of voor interne communicatiedoeleinden binnen het bedrijf. Bedrijven die SaaS producten aanbieden (hierna: SaaS leveranciers) zijn al een tijd actief op de markt, maar we zien de laatste paar jaar een sterke toename van vraag en aanbod. Vanwege deze groei zien we ook steeds vaker SaaS diensten van eigenaar veranderen, bijvoorbeeld als gevolg van overdracht van de onderneming. In dit artikel wordt ingegaan op het juridische kader van de intellectuele eigendomsrechten die relevant zijn bij de overname van een SaaS leverancier. Het is voor de overnemende partij namelijk essentieel dat de relevante intellectuele eigendomsrechten wel daadwerkelijk rusten bij de partij die wordt overgenomen.

Wat houdt SaaS ook alweer in waarom relevant?
Bij SaaS wordt er software als dienst aangeboden die niet op de eigen servers van de klant draait. De software wordt gehost bij een externe hostingleverancier, oftewel, de software draait in de "cloud". Het kenmerkende van SaaS is dat de afnemers software als dienst afnemen die op dezelfde wijze wordt aangeboden aan alle klanten (uitzonderingen daargelaten). Doordat de markt voor SaaS zich sterk heeft ontwikkeld, is de interesse om SaaS leveranciers over te nemen ook toegenomen. Bedrijven die software bij een SaaS leverancier afnemen zijn voor de interne of externe bedrijfsvoering namelijk afhankelijk geworden van deze dienst wat weer resulteert in het feit dat de overeenkomsten met SaaS leveranciers niet zo snel worden opgezegd. Daarnaast is het bij een SaaS leveranciers vaak eenvoudig om nieuwe klanten aan te sluiten en is er sprake van een constante maandelijkse of jaarlijkse inkomstenstroom.

Welke intellectuele eigendomsrechtsrechten zijn relevant bij SaaS?
Als we kijken naar de intellectuele eigendomsrechten die bij SaaS het meest relevant zijn, kunnen we een essentieel recht onderscheiden: het auteursrecht dat rust op de software. Merkrechten en domeinnamen zijn natuurlijk ook relevant om te onderzoeken bij de overname van een SaaS leverancier maar in dit artikel wordt de focus gelegd op het auteursrecht dat rust op de software.

Juridisch kader
Auteursrecht ontstaat van rechtswege. Dit komt erop neer dat er voor het ontstaan van het recht geen registratieplicht bestaat. Software wordt ontwikkeld door het schrijven van de broncode. Het auteursrecht rust dan ook op de geschreven broncode van de software. De rechthebbende van het auteursrecht is de persoon of partij die aan te merken is als de "maker" van het onderliggende werk, in dit geval de software.

Waar moet op gelet worden?
Op basis van ervaring uit de praktijk is het belangrijkste aandachtspunt waarop gelet moet worden bij het onderzoek naar het auteursrecht dat rust op software dat dit recht ook daadwerkelijk ligt bij de SaaS leverancier. Op basis van de Auteurswet zijn er een aantal vereisten wanneer auteursrecht rechtsgeldig is overgedragen.[1] Kort samengevat komen deze vereisten erop neer dat er sprake moet zijn van een akte (een overeenkomst waar beide partijen hun handtekening onder hebben gezet), er moet in deze akte expliciet zijn opgenomen dat het auteursrecht wordt overgedragen van de ene naar de ander partij en het moet voldoende bepaald zijn wat er precies wordt overgedragen. Er zijn daarnaast ook situaties denkbaar dat de SaaS leverancier automatisch rechthebbende is geworden (onder bepaalde omstandigheden) van het auteursrecht dat rust op de software zoals bijvoorbeeld bij software die is ontwikkeld door medewerkers van de SaaS leverancier. Deze situatie wordt als eerste besproken. Daarna wordt ingegaan op de overdracht van het auteursrecht bij het inschakelen van zowel binnenlandse als buitenlandse externe ontwikkelaars.

Software ontwikkeld door medewerkers
Op basis van de Auteurswet ligt het auteursrecht dat rust op de software die ontwikkeld is door de medewerkers met een arbeidsovereenkomst bij de SaaS leverancier.[2] Uiteraard zijn hier wel een aantal voorwaarden aan verbonden: er moet sprake zijn van arbeid en er moeten bepaalde werken zijn vervaardigd. Aangezien deze overdracht in de wet is geregeld is er geen aparte rechtshandeling nodig om ervoor te zorgen dat de SaaS leverancier rechthebbende wordt van het auteursrecht dat rust op de software die ontwikkeld is door de medewerkers. Toch wordt er vaak in de arbeidsovereenkomst met een medewerker een bepaling opgenomen die de overdracht van de intellectuele eigendomsrechten regelt. Dit wordt gedaan als extra waarborg dat het auteursrecht dat ontstaan is bij de ontwikkeling van de software bij de SaaS leverancier komt te liggen.

Tijdens het onderzoek naar de intellectuele eigendomsrechten bij de overname van een SaaS leverancier is het aan te raden om te onderzoeken wie die software ontwikkeld heeft en in het geval van medewerkers moet er gekeken of deze ontwikkeling binnen de werkomschrijving. Daarnaast is het aan te raden de arbeidsovereenkomsten te controleren of er een bepaling is opgenomen die de overdracht van het auteursrecht regelt. Dit geeft extra zekerheid dat de SaaS leverancier de rechthebbende is van het auteursrecht dat rust op de software die ontwikkeld is door de medewerkers.

Software ontwikkeld door externe ontwikkelaars
De maker van een werk waar auteursrecht op rust is in principe aan te merken als de rechthebbende. Dit betekent dat externe ontwikkelaars die niet op basis van een arbeidsovereenkomst werken als de rechthebbenden worden gezien. Het is voor de overdracht niet voldoende dat er simpelweg betaald wordt voor de diensten van de externe ontwikkelaars. Voor de overdracht is namelijk een akte vereist die voldoet aan de wettelijke vereisten voor de overdracht van het auteursrecht.

In de praktijk komt het vaak voor dat er met externe ontwikkelaars alleen een offerte is overeengekomen waarop algemene voorwaarden van toepassing zijn. Meestal is in de algemene voorwaarden opgenomen dat de auteursrechten die rusten op de ontwikkelde software bij de afnemer komen te liggen maar doordat externe ontwikkelaars als maker worden beschouwd kan je alleen auteursrecht verkrijgen middels een akte conform artikel 2 Auteurswet. Indien er wel sprake is van een akte, dan komt het vaak voor dat er in deze akte niet is opgenomen dat het auteursrecht daadwerkelijk wordt overgedragen. Daarnaast komt het regelmatig voor dat op basis van de akte onduidelijk is wat er precies wordt overgedragen. Dit wordt ook wel het vereiste van "voldoende bepaaldheid" genoemd.
Dit laatste kan worden opgelost door een bijlage bij de akte op te nemen waarin het ontwikkelde werk omschreven wordt en een verwijzing wordt opgenomen naar een account binnen een zogenaamde online repository (denk aan: Github) waar de broncode is opgenomen. Het auteursrecht bij software rust op de broncode van software en door deze verwijzing op te nemen, wordt er voldaan aan het vereiste van voldoende bepaaldheid voor de overdracht van auteursrecht. Indien het voorgaande niet is opgenomen in een akte, is de SaaS leverancier niet de rechthebbende geworden van het auteursrecht dat rust op de software die ontwikkeld is door externe ontwikkelaars.

1. Artikel 2 lid 2 Auteurswet.
2. Artikel 7 Auteurswet.

Tijdens het onderzoek naar de intellectuele eigendomsrechten bij de overname van een SaaS leverancier wordt geadviseerd om de gesloten overeenkomsten met de externe ontwikkelaars te controleren op de overdracht van auteursrechten. Het komt regelmatig voor dat de overeenkomsten niet voldoen aan de wettelijke vereisten voor de overdracht van auteursrecht. Uiteraard kan de overdracht "hersteld" worden door een alsnog akte van overdracht te tekenen om de overdracht te realiseren. Het voorgaande kan wel vertraging van het overnametraject met zich meebrengen.

Software ontwikkeld door buitenlandse ontwikkelaars

Aan het ontwikkelen van software hangt vaak een prijskaartje. Daarom is het tegenwoordig gangbaar om een partij uit het buitenland in te schakelen om de software te ontwikkelen. In de praktijk wordt er vaak gekozen voor een externe ontwikkelaar die gevestigd is in een land uit Oost-Europa, bijvoorbeeld Noord-Macedonië of Tsjechië. Dit komt door het feit dat de uurtarieven voor ontwikkelaars in deze landen een stuk lager liggen dan bijvoorbeeld in Nederland.

Bij het inschakelen van een buitenlandse externe ontwikkelaars moet er worden gelet op het recht dat van toepassing is op de gesloten overeenkomst. Zo is het bijvoorbeeld onder het nationale recht van Tsjechië niet mogelijk om auteursrechten over te dragen. Het auteursrecht blijft bij de maker, in dit geval de externe ontwikkelaar. Het is onder Tsjechisch recht wel mogelijk om licenties uit te geven aan partijen die gebruik willen maken van de software.

Indien een SaaS leverancier een Tsjechische ontwikkelaar heeft ingeschakeld om software te ontwikkelen en Tsjechisch recht is van toepassing op de overeenkomst, is de SaaS leverancier geen rechthebbende geworden van het auteursrecht dat rust op de software. Dat kan een probleem opleveren indien de SaaS leverancier in de veronderstelling was rechthebbende te zijn en dit ook zo gecommuniceerd heeft naar de overnemende partij. Dat is niet wenselijk indien de SaaS leverancier wordt overgenomen. Dit kan worden opgelost door bij het sluiten van overeenkomsten met buitenlandse externe ontwikkelaars Nederlands recht van toepassing te verklaren en verder te voldoen aan de Nederlandse wettelijke vereisten voor de overdracht van auteursrecht. Als dit niet mogelijk is, is het wenselijk te onderzoeken welke alternatieven er onder dat buitenlandse recht beschikbaar zijn en voldoende waarborgen bieden, zoals een exclusieve onherroepelijke licentie.

Tijdens het onderzoek naar de intellectuele eigendomsrechten bij de overname van een SaaS leverancier wordt geadviseerd om de gesloten overeenkomsten met de buitenlandse externe ontwikkelaars te controleren op de overdracht van het auteursrecht dat rust op de ontwikkelde software. Hierbij is vooral belangrijk de overeenkomst na te gaan op het recht dat van toepassing is verklaard. Dit kan grote gevolgen hebben voor de overdracht van het auteursrecht dat rust op de software met het gevolgd dat de SaaS leverancier geen rechthebbende is geworden.

Conclusie

Bij de overname van een SaaS leverancier is er met name één soort intellectueel eigendomsrecht belangrijk om te onderzoeken: het auteursrecht dat rust op de software. Bij dit onderzoek moeten de overeenkomsten met zowel Nederlandse als buitenlandse ontwikkelaars gecontroleerd worden op de rechtsgeldige overdracht van het auteursrecht. Daarnaast wordt er ook aangeraden om de arbeidsovereenkomsten van medewerkers te controleren op een bepaling die deze overdracht regelt. Bij de overeenkomsten met externe ontwikkelaars moet er gecontroleerd worden of de auteursrechten wel rechtsgeldig zijn overgedragen in de zin van de Auteurswet en bij overeenkomsten met buitenlandse partijen moet er daarnaast ook worden gekeken naar het recht dat van toepassing is verklaard. Uiteraard is het mogelijk om alle gebreken te "repareren" maar dit kan het overnametraject behoorlijk vertragen. Het is voor SaaS leveranciers daarom aan te raden om tijdig aandacht te besteden aan het besproken auteursrecht dat rust op de software. Dit kan bij een overnametraject eventuele vertraging voorkomen en hierdoor kunnen partijen zich meer focussen op de commerciële aspecten van de overname.

Demi Grandiek
Juridisch adviseur

Privacy

Toegang tot de mailbox en mappen van werknemers

In de laptop, mailbox en bestanden van werknemers kan cruciale informatie staan, die direct nodig is om bijvoorbeeld een klant goed te bedienen of een verstuurde offerte terug te halen. De werknemer is op dit moment echter niet beschikbaar. Hoe gaat u hiermee om? En als de werknemer uit dienst is, mag u deze informatie dan zomaar opzoeken?

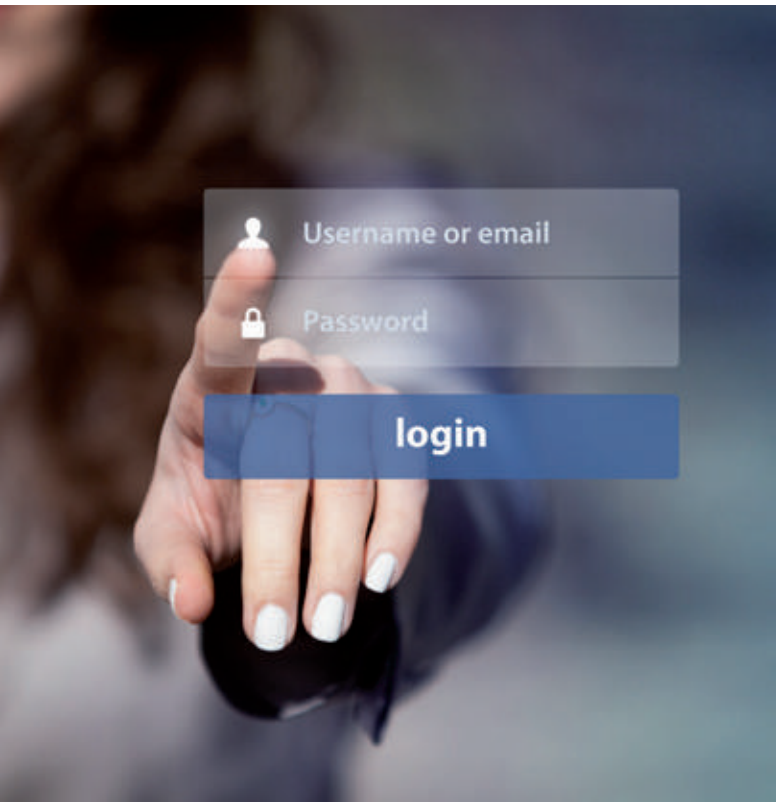
Een kijkje in de eigendommen van de werkgever
Werknemers krijgen voor de uitvoering van de werkzaamheden vaak een laptop en een eigen mailbox. De laptop, mailbox en bestanden zijn in principe het eigendom van werkgever. Vaak is technisch ingeregeld dat werkgevers (op afstand) de macht over de laptop, mailbox en bestanden kan overnemen en de gegevens kan doorzoeken. Volledig begrijpelijk, het is immers eigendom van de werkgever en valt onder diens verantwoordelijkheid. Veel gegevens zijn ook nog eens van groot belang voor de continuïteit van de onderneming.

Er kunnen zich situaties voordoen, waarbij de werkgever toegang nodig heeft tot de inhoud van de laptop, mailbox en bestanden van de werknemer. Te denken valt aan de situatie waarbij de werknemer plotseling uitvalt wegens ziekte of een ongeluk, en de werkzaamheden door collega's overgenomen worden. Ook in de situatie waarbij een werknemer reeds uit dienst is, maar de klanthistorie belangrijk is voor de voortgang van de onderneming kan het nodig zijn om toegang te verkrijgen tot de mailbox en bestanden van de oud-werknemer.

Inbreuk op privacy
Wanneer de werkgever laptop, mailbox en bestanden van (oud)werknemers doorzoekt, maakt hij inbreuk op de privacy. In veel gevallen gebruiken werknemers hun laptop , mailbox en bestanden namelijk ook voor privédoeleinden. Dat dit gebeurt, is overigens niet volledig te voorkomen. Het is niet toegestaan om werknemers volledig te verbieden hun laptop of zakelijke mailbox voor privédoeleinden in te zetten. De werknemer heeft volgens het Europese Hof van de Rechten van de Mens *(Copland, 2007)* ook op de werkvloer recht op privacy. Dit betekent dat de werkgever zorgvuldig om dient te gaan met de persoonlijke gegevens van (oud)werknemers en de regels uit de AVG dient te volgen.

Betekent dit dan dat de werkgever niet meer in de laptop, mailbox en bestanden van de (oud)werknemers mag kijken? Nee, het recht op privacy is niet absoluut. Het is mogelijk dat belangen van werkgevers zwaarder wegen, dan het privacybelang van de betreffende (oud) werknemers. Het betekent echter wél dat een werkgever een rechtmatige grondslag dient te hebben, waaronder die werkgever een inbreuk mag maken op de privacy van betreffende (oud)werknemers. In de werkgever-werknemer relatie betekent dit dat nagegaan dient te worden of de werkgever een voldoende gerechtvaardigd belang heeft, om 'een kijkje te nemen' in de laptop, mailbox en bestanden van de (oud)werknemers.

Rechtmatige grondslag
Het gerechtvaardigd belang dient telkens, bij elke verwerking, te worden afgewogen. De werkgever dient vast te stellen welk belang hij heeft en of dit een gerechtvaardigd belang is. Vervolgens moet de werkgever beoordelen of de zoektocht door de laptop, mailbox en bestanden echt noodzakelijk is. Kan het doel niet op een andere, minder ingrijpende wijze worden bereikt?



Bijvoorbeeld door te zoeken in de bestanden in het CRM-systeem. Of door minder mails en bestanden te bekijken. Is dat niet het geval, dan dient de werkgever als laatste te toetsen of zijn belang zwaarder weegt dan het privacybelang van de (oud)werknemers. De werkgever kan maatregelen nemen om deze belangenafweging in zijn voordeel uit te laten vallen. De redelijke verwachting van de (oud)werknemers is bijvoorbeeld een belangrijke factor. Dit betekent dat de werkgever de (oud)werknemers dient te informeren over de mogelijkheid dat er een kijkje wordt genomen in de laptop, mailbox en bestanden.

De belangenafweging

Het belang van werkgever zit hem veelal in het grondrecht vrijheid op ondernemerschap en het commercieel belang om gesloten overeenkomsten met klanten en leveranciers na te kunnen komen. Wanneer werkgever in de openbare en gedeelde mappen, in het CRM-systeem, of in de eigen mailbox de benodigde documentatie niet heeft terug kunnen vinden, en besloten heeft dat er geen andere mogelijkheid bestaat om de informatie terug te halen, dient de afweging van het gerechtvaardigd belang tegenover het privacybelang van de (oud)werknemer plaats te vinden.

Vragen die een werkgever zich daarbij dient te stellen zijn:

- Worden niet meer gegevens verwerkt dan strikt noodzakelijk? Oftewel, worden persoonlijke bestanden en e-mails die niets te maken hebben met het nastreven van het belang, voor zover mogelijk, buiten beschouwing gelaten?
  Bijvoorbeeld door middel van:
  - Het werken met specifieke zoektermen;
  - Privé aangemerkte berichten of evident persoonlijke informatie links laten liggen (bijvoorbeeld een e-mail met als onderwerp: ‘privéafspraak’);
  - De zoekperiode beperken tot enkel de relevante termijnen.
- Is beleid opgesteld met daarin duidelijke criteria op welke manier (hoe/van wie/welke periode) de toegang gaat plaatsvinden?
- Zijn de (oud)werknemers op voorhand geïnformeerd dat werkgever toegang kan krijgen tot de laptops, mailbox en bestanden en voor welk doel?
- Worden (oud)werknemers op de hoogte gebracht op het moment dat werkgever voornemens is om toegang te verkrijgen en met welk doel?
- Mochten de (oud)werknemers verwachten dat de werkgever toegang zou krijgen tot de laptop, mailbox en bestanden?
- Zijn de (oud)werknemers in de gelegenheid gesteld om persoonlijke informatie te wissen?
- Zijn de (oud)werknemers uitdrukkelijk in de gelegenheid gesteld om bezwaar te maken?

Eisen aan uitvoering

Valt de toets in het voordeel van werkgever uit? Dan mag, voor de eerder bepaalde doeleinden, toegang worden verkregen tot de laptop, mailbox en bestanden van de (oud)werknemer. De werkgever dient zich vervolgens strikt te houden aan het eerder opgestelde beleid over inzage en toegang. In dit beleid zullen regels opgenomen, zoals:

- de gegevens worden niet ingezet voor andere doeleinden. Zo mag een werkgever de gegevens niet gebruiken om werknemers te beoordelen op hun prestaties. Ook niet wanneer tijdens de zoektocht belastende informatie naar voren komt.
- de gegevens moeten op passende wijze worden beschermd, door technische en organisatorische maatregelen te nemen. Zo kan bijvoorbeeld worden geregeld dat er altijd een extra persoon meekijkt bij het doorzoeken van de mails of bestanden, en wordt met beide personen een aanvullende geheimhoudingsverplichting afgesproken.
- er is vastgesteld wie toegang krijgen tot de gegevens van (oud)werknemers (autorisaties). De eis hierbij is dat zo min mogelijk personen toegang hebben.

Ook de vraag of je de mailbox überhaupt nog had mogen bewaren is een punt van aandacht. Als het gaat om een medewerker die al 10 jaar uit dienst is kun je je afvragen waarom een werkgever de mailbox nog heeft.

Jay Remmelzwaal
Juridisch adviseur

Demi Grandiek
Juridisch adviseur

Privacy Overheid

Arbeidsrechtelijke maatregelen voor toegang tot de laptop, mailbox en bestanden van (oud)werknemers

In het voorgaande artikel is beschreven dat de AVG mogelijkheden biedt om onder bepaalde omstandigheden toegang te verkrijgen tot de laptop, mailbox en bestanden van (oud)werknemers. Bij die situatie is niet alleen het privacyrecht interessant, maar ook het arbeidsrecht speelt een rol. Regels over het privégebruik van bedrijfsmiddelen mag een werkgever bijvoorbeeld stellen onder het instructierecht. Daarnaast geeft de jurisprudentie omtrent ontslag werkgevers juist reden om te zoeken in de laptop, mailbox en bestanden van werknemers, ook als dat van de AVG eigenlijk niet mag. Onrechtmatig verkregen bewijs kan namelijk wel bijdragen aan een ontslag.

Instructierecht
Volgens de wet hebben werkgevers een instructierecht. Dit betekent dat de werknemers verplicht zijn om zich te houden aan de voorschriften die de werkgever geeft. Dit kan bijvoorbeeld betrekking hebben op de uitvoering van de werkzaamheden, de omgang met bedrijfsmiddelen of de omgang met collega's. Een voorschrift kan bestaan uit huisregels, over het netjes houden van de werkplek en een representatieve houding richting klanten en collega's. Of een privacybeleid, waarin wordt beschreven hoe werknemers met klantgegevens om dienen te gaan. Ook een IT-reglement, met daarin regels over het gebruik van het internet, de ter beschikking gestelde laptop of telefoon en de zakelijke mailbox behoren tot het instructierecht van de werkgever.

Veel werkgevers zijn nog van mening dat je in zo'n IT-reglement de werknemers kunt verbieden om de laptop, mailbox te gebruiken voor privédoeleinden. En dat het dan, omdat er toch geen privégegevens instaan, toegestaan is om de laptop, mailbox en bestanden door te zoeken op belastende informatie. Zo werkt het echter niet. Privacy geldt, zoals je op de voorgaande pagina's hebt kunnen lezen, ook op het werk en het doorzoeken raakt dan altijd de privacy van werknemers. Wel is het mogelijk om privégebruik als onwenselijk aan te merken en werknemers te instrueren zoveel mogelijk privéinformatie te verwijderen of als privé te markeren, om de werkgever zo gemakkelijker in de gelegenheid te stellen werkinformatie terug te halen waar nodig, zonder de privacy van werknemers te schaden. Deze instructie kan weer meespelen in de belangenafweging of de werkgever een kijkje mag nemen in de laptop, mailbox en privédoeleinden van (oud)werknemers.

Onrechtmatig doorzoeken
Hoewel 'zomaar' doorzoeken van de laptop, mailbox en bestanden van de werknemers onder de AVG niet

mag, gebeurt dit dikwijls nog wel. Als sprake is van een geschil of een werkgever toewerkt naar een ontslag, heeft de werkgever bewijs nodig en wordt het zoeken naar (aanvullend) bewijs in de laptop, mails en bestanden interessant. De werkgever gaat dan op zoek naar bewijsmateriaal om ontslag te onderbouwen of om de overtreding van het geheimhoudings- of relatie- en concurrentiebeding te kunnen staven.

Ondanks dat zo'n zoektocht volgens de AVG vaak niet is toegestaan, kan onrechtmatig verkregen bewijs wel meewegen in de rechtbank. Dit betekent bijvoorbeeld dat bewijs verkregen uit een onrechtmatige zoektocht wel kan bijdragen aan een beëindiging van de arbeidsovereenkomst. In september 2019 nog, werd een werknemer op staande voet ontslagen toen uit zijn mails bleek dat hij geld inzamelde voor zijn privégewin. Het doorzoeken van de mailbox loonde en de mails dienden in deze zaak als bewijs. Het risico voor werkgever zit hem in dat geval enkel in het betalen van een (extra) vergoeding wegens schending van de privacy. En dat risico is weer afhankelijk van de verwachting die de werknemer mocht hebben op een eventuele inbreuk op diens privacy.

ICTRECHT
adviesbureau

Uw informatie goed beveiligd met ICTRecht

Informatie en IT zijn onmisbaar voor de continuïteit van uw bedrijfsvoering. Het is dan ook van groot belang dat informatie en systemen binnen uw organisatie adequaat worden beveiligd.

Maar waar te beginnen?
En wanneer is de bescherming ‘adequaat’?

ICTRecht biedt organisaties op maat gemaakte security-oplossingen. Zo helpen wij uw organisatie veilig te houden. Wij kunnen o.a. de volgende werkzaamheden voor uw organisatie oppakken:

- Uitvoeren van security quickscans of risico-analyses - al dan niet conform ISO 27001/27002, NEN 7510, BIO
- Adviseren over informatiebeveiligingsbeleid en maatregelen
- Maatregelen implementeren om risico’s te beperken
- Audits, pentesten en andere controles initiëren

Wilt u weten hoe volwassen uw organisatie op gebied van security is?
Doe nu onze online security test op ictrecht.nl/security!

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Internetrechtspraak

Rechtbank Den Haag 30 oktober 2019
(Ontbinding telecomdiensten)
Een consument neemt internet af van een telecom-leverancier, maar ondervindt regelmatig problemen. Er moest meermalen een monteur langs komen en haar Mediabox ging bij iedere keer aanzetten scannen waardoor het 5 tot 10 minuten duurde voordat zij televisie kon kijken. Na geruime tijd ontbindt zij de overeenkomst tot levering. De leverancier is het daar niet mee eens; zulke problemen zijn niet ernstig genoeg. De rechtbank ziet dat anders: wanneer het bedrijf er herhaalde malen niet in slaagt de gemelde storing te verhelpen en zij telkens 5 á 10 minuten moet wachten voordat zij televisie kan kijken, is dat wel degelijk een tekortkoming die ontbinding rechtvaardigt.

https://bit.ly/3aukqKj

Hoge Raad 8 november 2019
(Ongevraagde waterlevering)
Een man woont sinds 2012 in een huis in Amsterdam, en krijgt van Waternet water geleverd via leidingbuizen. Waternet stelt dat een contract is gesloten, de man ontkent dat met klem. Hij had betrekkelijk korte tijd nadat Waternet zich in november 2014 tot hem had gewend, zowel telefonisch als schriftelijk aan Waternet kenbaar gemaakt dat hij geen overeenkomst met Waternet had en dat hij, zoals Waternet duidelijk had moeten zijn, een dergelijke overeenkomst ook niet wenste. De rechtbank merkt dit aan als ongevraagde levering in de zin van art. 7:7 lid 2 BW, wat het Hof bevestigt. De Hoge Raad zoekt een balans tussen enerzijds dit artikel (dat vrij expliciet is over ongevraagde waterlevering) en andrzijds de Nederlandse praktijk van het continu leveren van water. Prejudiciële vragen worden gesteld.

https://bit.ly/2VPFN4m

Rechtbank Amsterdam 26 november 2019
(Formulier)
In een verstekzaak eist een bedrijf betaling van een consument. Bij dagvaarding is niet gesteld of, en zo ja, op welke wijze aan de precontractuele en contractuele verplichtingen is voldaan van de onderhavige koop op afstand. Op welke wijze gedaagde partij heeft gekozen voor achteraf betalen, welke informatie daarbij is verstrekt en of door de keuze van gedaagde partij voor achteraf betalen een overeenkomst tussen partijen tot stand is gekomen, is niet toegelicht. De e-mails waar eisende partij naar verwijst zijn niet overgelegd, de overeenkomst, dan wel de bevestiging van de overeenkomst op een duurzame drager evenmin. In de overgelegde factuur staat vermeld dat een zekere webwinkel de eisende partij heeft gemachtigd, conform de algemene voorwaarden, de nota aan gedaagde partij te factureren. Deze algemene voorwaarden zijn ook niet overgelegd. De kantonrechter rekent het niet zijn taak om de door eisende partij geciteerde linken naar de algemene voorwaarden van de webwinkel en eisende partij op internet op te zoeken. Het is aan eisende partij om de stukken die aan de vordering ten grondslag leggen over te leggen.

https://bit.ly/2VIABiY

Rechtbank Rotterdam 5 december 2019
(Tikkie-oplichting)
Vijf verdachten zijn veroordeeld voor 'tikkie-fraude', waarbij marktplaatsverkopers met valse tikkie-links werden bewogen om te klikken op een link naar een phishing website. Deze wekte de indruk de bankwebsite van het slachtoffer te zijn, zodat men inloggegevens en TAN-codes kon verwerven. Met hulp van de verkregen inloggegevens werden veelal dure goederen gekocht. Drie verdachten werden naast computervredebreuk, diefstal en oplichting, ook veroordeeld voor lidmaatschap criminele organisatie.

https://bit.ly/2IfM3dJ

Rechtbank Rotterdam 5 december 2019
(Foto met toestemming)
Het bedrijf Luxury Bedding verkoopt bedden/matrassen van het merk Serta, en huurt een fotograaf in om productfoto's hiervan te maken. Concurrent Sefa vindt twee van deze foto's via internet en publiceert ze op haar eigen Facebookpagina. Na aangesproken te worden op inbreuk auteursrecht verweert ze zich dat er toestemming zou zijn verkregen. Op een beurs maakte men zelf foto's van de producten, en toen zou door een vertegenwoordiger van Luxury Bedding gezegd zijn dat de foto's op internet beter zijn en gebruikt mochten worden. Gezien het karakter van een kort geding is bewijsvoering in deze lastig, maar omdat Sefa toe heeft gezegd de foto's verwijderd te houden, wordt de vordering wegens inbreuk afgewezen.

https://bit.ly/2wowwpB

Rechtbank Noord-Nederland 12 december 2019
(Verwijderverzoek gevangene)
Verzoeker heeft verwijdering verzocht van zoekresultaten die verschijnen bij een zoekopdracht op zijn naam in Google Search en die verwijzen naar het door verzoeker gepleegde strafbare feit. Verzoeker is veroordeeld tot een gevangenisstraf van 11 jaar en zeven maanden met oplegging van tbs. Verzoeker heeft zijn straf uitgezeten en bevindt zich thans in het forensisch kader van de tbs-maatregel. De sinds 2006 verstreken tijd is, gezien het huidige, nog bestaande forensische kader, de ernst van het strafbare feit en de impact die het op de samenleving heeft gehad, relatief gezien nog maar beperkt. Onder dit publieke belang moet ook worden begrepen het eveneens zwaarwegend belang van auteurs van de betreffende informatie, dat hun informatie kan worden gevonden hetgeen meer in het bijzonder geldt voor de pers die verslag heeft gedaan en doet alsmede commentaar heeft gegeven en geeft op de gerechtelijke procedures en de uitkomsten daarvan naar aanleiding van het door [verzoeker] gepleegde ernstige strafbare feit.

https://bit.ly/2Plj06H

Hoge Raad 17 december 2019
(Is e.dentifier een geautomatiseerd werk?)
Grootschalige vorm van skimmen en betaalpasfraude vindt plaats door bankpasgegevens van klanten af te tappen door gemanipuleerde e.dentifiers in bankshops van een bank te plaatsen. Hiermee zijn vervolgens valse betaalpassen vervaardigd, waarna met die valse betaalpassen in totaal meer dan € 1 miljoen contant is opgenomen. Rechtsvraag is of dit aftappen van gegevens via een geautomatiseerd werk (art. 139c Sr) oplevert. Is een e.dentifier een geautomatiseerd werk? Een inrichting kan alleen als 'geautomatiseerd werk' worden aangemerkt indien zij geschikt is om drie functies te vervullen, te weten opslag, verwerking en overdracht van gegevens. Dat begrip 'geautomatiseerd werk' is echter niet beperkt tot apparaten die zelfstandig aan deze drievoudige eis voldoen. De e.dentifiers werken samen met andere apparatuur en het Internet Bankieren-systeem van de banken, en dat geheel is een geautomatiseerd werk.

https://bit.ly/39iusOi

Hof van Justitie van de EU 19 december 2019
(Airbnb een informatiedienst)
De Franse vereniging voor accommodatie en toerisme klaagt Airbnb aan wegens het verrichten van vastgoedactiviteiten zonder beroepskaart, welke onder Franse wetgeving verplicht is. Dit leidt tot prejudiciële vragen, waarbij het HvJ oordeelt dat Airbnb hoofdzakelijk een tool is om vraag en aanbod bij elkaar te brengen. Er wordt vastgesteld dat Airbnb de prijzen van de aangeboden accommodaties niet bepaalt, en evenmin een selectie maakt van verhuurders of accommodaties die worden aangeboden op haar website. Airbnb moet daarom worden gekwalificeerd als "dienst van de informatiemaatschappij" in de zin van richtlijn 2000/31. Vanwege deze kwalificatie kan Frankrijk haar lokale wetgeving (de Wet Hoguet) niet onverkort handhaven jegens Airbnb.

ECLI:EU:C:2019:1112

Rechtbank Noord-Holland 24 december 2019
(Toegang tot iCloud bekende Nederlanders)
Verdachte heeft zich gedurende enkele jaren zonder toestemming van rechthebbenden de toegang tot een grote hoeveelheid iCloud-accounts verschaft en heeft zich daarmee schuldig gemaakt aan computervredebreuk, dan wel pogingen daartoe. De slachtoffers betreffen vrouwen die bekend zijn van televisie, sport, of afkomstig zijn uit de kring van de familie van verdachte of (ex-) collega's. In het geval van één slachtoffer heeft verdachte bovendien onrechtmatig ingelogd op haar Gmail account. Bij dit alles ging verdachte geraffineerd en planmatig te werk door gebruik te maken van speciaal daartoe aangeschafte software. Verder heeft verdachte geprobeerd één van de slachtoffers op te lichten door haar gedurende bijna drie jaar met enige regelmaat emailberichten te verzenden en zich daarbij voor te doen als vrouw met de bedoeling haar onder valse voorwendselen zo ver te krijgen dat zij seksueel getinte foto's van zichzelf naar hem zou sturen. Vrijspraak van smaad en belediging en van poging tot computervredebreuk bij 195 iCloud accounts.

https://bit.ly/2VPLUpk

Rechtbank Rotterdam 24 december 2019
(Boetes consumentenmisleiding)
Telecombedrijf T-Mobile biedt diverse abonnementen op haar website aan, met onder meer de tekst "Onbeperkt GB" en "Internet: Je kunt je GB's gebruiken in NL én EU". Hierdoor werd volgens de ACM de indruk gewekt dat er met de "Onbeperkt GB" bundels geen beperkingen worden gesteld aan het gebruik van data in de EU. In de prijsplannen wordt over het gebruik van de databundel in de EU bij het Unlimited abonnement vermeld: "Na het bereiken van de limiet van jouw databundel, wordt de internetverbinding tijdelijk verbroken. Je krijgt vervolgens de keuze om verder te internetten in de EU door het aanschaffen van een GB-aanvuller of door te kiezen voor betalen per MB (Pay for Use)." Volgens de ACM levert dit een overtreding op van art. 6:193c lid 1 sub b BW, omdat deze informatie in het oog moet springen bij de eerste informatie. Dus niet pas in de brochures of algemene voorwaarden, en ook niet – zoals T-Mobile deed – in een informatievakje dat met een (i) knopje op te roepen was.

https://bit.ly/2TlOzFN

Gerechtshof Den Haag 24 december 2019
(Verwijderverzoek bijzondere persoonsgegevens)
Een persoon is strafrechtelijk veroordeeld voor poging tot dwang (bij twee van zijn huurders) en bestuurlijk beboet voor onveilige bouwwerken. Hij probeert publicaties over een en ander uit Google verwijderd te krijgen, en wijst er onder meer op dat hier bijzondere persoonsgegevens in worden verwerkt. Omdat Google geen journalistiek medium is, heeft zij daar in beginsel geen grondslag voor. Op grond van het arrest GC/CNIL (HvJ EU 24 september 2019) mag echter via de route van de reden van zwaarwegend algemeen belang het verwerkingsverbod van deze gegevens worden gepasseerd als de informatie strikt noodzakelijk is voor de vrijheid van informatie. Dat is hier het geval. De informatie is juist en actueel en staat niet ter discussie. Dergelijke, voor het maatschappelijke en publieke debat relevante informatie valt bij uitstek onder de vrijheid van informatie van het publiek en is daarom van zwaarwegend belang voor de internetgebruiker.

https://bit.ly/38nYtuW

Gerechtshof Den Haag 24 december 2019
(Downloaden geheime werkgeversdata)
Een bedrijf klaagt een ex-werknemer aan wegens overtreding van diens geheimhoudingsbeding. De werknemer had ontslag genomen omdat hij vond dat de werkgever de Code of Conduct van een klant had geschonden, waar hij niet mee kon leven. De dag voor dat ontslag had hij maar liefst 1901 documenten van het onderhavige project met die klant gedownload, welke documenten bij die klant terecht waren gekomen. Daarmee kon de klant het project afronden zonder betrokkenheid van de werkgever. De rechtbank wijst de contractuele boete voor schending geheimhouding toe.

https://bit.ly/3cnCKGy

Rechtbank Overijssel 24 december 2019
(Bitcoin-gijzeling bedrijf)
Een man breekt in bij de gegevens van een verhuurmakelaar uit Apeldoorn en verkrijgt zo persoonsgegevens van 18.500 klanten. Hij eist 10.000 euro aan bitcoins van de makelaar onder dreiging de gegevens anders openbaar te maken. Hem wordt computervredebreuk en digitale afdreiging (art. 317 lid 2 Sr) ten laste gelegd. Het laatste wordt echter afgewezen, nu de man heeft gedreigd deze gegevens openbaar te maken en niet om ze te wissen of onbruikbaar te maken. Dat is niet strafbaar.

https://bit.ly/2IfgxNd

Rechtbank Midden-Nederland 9 januari 2020
(Stem als persoonsgegeven)
Het slachtoffer van een overval werkt mee aan een uitzending van "Opsporing Verzocht", en zegt in een voice over dat de dader een "Ali B accent" heeft. Zij claimt dat dit moest van de redactie. Dit gaf de nodige ophef, en leidt onder meer tot aandacht op televisie bij College Tour (NTR) en een theatershow bij RTL 4. Omdat de vrouw veel last heeft van de uitspraak die overal opduikt, doet zij een vergeetverzoek bij de producenten. De rechtbank wijst dit af. De uitspraak is een persoonsgegeven, omdat de stem te herleiden is tot de persoon met een eenvoudige zoekopdracht. Echter, de uiting in de theatershow is een artistieke verwerking (art. 85 AVG jo. 45 Uitvoeringswet AVG) en daarom is een vergeetverzoek niet mogelijk.

https://bit.ly/3cxmB1c

Rechtbank Midden-Nederland 22 januari 2020
(Vertrouwen in contractspartij)
Een webwinkel verkoopt en levert drie iPhones aan een consument. Deze betaalt alleen de eerste iPhone en verweert zich tegen de incasso voor de andere twee door te zeggen dat hij onder bedreiging van een derde de aanschaf heeft gedaan, en niet wist dat het om meer dan één telefoon zou zijn gegaan. Rechtbank wijst dit af. Alle gegevens zijn die van gedaagde, inclusief bankrekening. Telefoon is ook daar geleverd en aangenomen. Dat sprake is van bedreiging, is onwaarschijnlijk gezien overlegde WhatsApp-chat met de derde.

https://bit.ly/39nGWEs

Rechtbank Amsterdam 27 januairi 2020
(Oneerlijke cursusbeschrijving)
Een man schrijft zich via internet in voor een opleiding tot Professional Music Production van 24 lessen. Hij betaalt deze niet volledig. Volgens hem zijn de in de omschrijving aangekondigde onderdelen Arrangement, Compositie en Mastering niet behandeld, hebben hij en zijn medecursisten vooral veel moeten wachten in de studio, is de docent aan het einde van de opleiding vanwege ruzie met de leiding plots vervangen, is het eindcertificaat niet aan hem toegestuurd en is er na afloop tegen de belofte in niet gecoacht. De rechtbank speelt langs de lijn van de oneerlijke handelspraktijk. Online werd nameleijk aangekondigd dat je "168 uur actief in de studio" bent, dat "de focus op het opnemen en produceren van muziek" ligt en dat je "de ins and outs van het vak in een professionele studio" leert en "werkt met hoogwaardige apparatuur!". In de praktijk konden slechts twee studenten tegelijk mixen en moest de rest wachten in de hal. Prijs wordt teruggebracht om te compenseren voor het deel van de cursus dat wel conform verwachting is gegeven.

https://bit.ly/2VHceC3

Gerechtshof Arnhem-Leeuwarden 18 februari 2020
(Prijsdifferentiatie)
Digital Revolution en Media Concept bieden online inkt- en tonercartridges voor printers aan: Media-Concept maakt reclame voor haar printercartridges via Google Shopping, waarbij zij met een lagere prijs adverteert dan te zien is als haar website rechtstreeks – dus niet via Google Shopping – wordt benaderd. Eenmaal aangekomen op prindo.nl via Google Shopping, kan de klant echter maar één product voor die lagere prijs kopen. Dat staat dan wel duidelijk bij het prijsaanbod vermeld. Digital Revolution meent dat er sprake zou zijn van misleiding, oneerlijke handelspraktijken en ongeoorloofde vergelijkende reclame. Het hof is met Media Concept van oordeel dat het beroep van Digital Revolution op artikel 6:194a BW alleen al moet worden afgewezen omdat de vergelijking niet door Media Concept maar door Google Shopping wordt uitgevoerd. Meer algemeen acht het Hof legaal om bezoekers die via Google Shopping binnenkomen andere prijzen aan te bieden.

https://bit.ly/3cqC3wp

Rechtbank Den Haag 5 februari 2020
(Inzet SyRI in strijd met hoger recht)
Het Systeem Risicoindicatie (hierna: SyRI) is een wettelijk instrument dat de overheid gebruikt ter voorkoming en bestrijding van fraude op het terrein van de sociale zekerheid en inkomensafhankelijke regelingen, de belasting- en premieheffing en de arbeidswetten. Grofweg worden diverse bronnen met elkaar verbonden, waarna het systeem op onnavolgbare wijze (pardon: via artificial intelligence) mensen signaleert als mogelijke fraudeur. De rechtbank komt tot het oordeel dat de SyRI-wetgeving in haar huidige vorm de toets van artikel 8 lid 2 EVRM niet doorstaat. De rechtbank heeft de doelen van de SyRI-wetgeving, namelijk het voorkomen en bestrijden van fraude in het belang van het economisch welzijn, afgezet tegen de inbreuk op het privéleven die de wetgeving maakt. Volgens de rechtbank voldoet de wetgeving niet aan de 'fair balance' die het EVRM vereist om te kunnen spreken over een voldoende gerechtvaardigde inbreuk op het privéleven. De wetgeving is wat betreft de inzet van SyRI onvoldoende inzichtelijk en controleerbaar. Zie de noot op pagina 32.

https://bit.ly/32UJV4L

juriblox

VERGROOT DE EFFICIËNTIE VAN CONTRACTEREN

Herkent u dit?

Heeft u al veel energie gestoken in onderhandelingen met een leverancier of klant, moet u óók nog veel tijd steken in de juridische documenten om het af te maken. Waar stond ook alweer de laatste versie van het document? En welke wijzigingen heeft de wederpartij aangebracht?

NAUWKEURIGE JURIDISCHE DOCUMENTEN ZIJN ONMISBAAR. MAAR:

- door toenemende werkdruk is er grote kans dat zaken vergeten worden of documenten inconsistent zijn
- het contracteren kost veel tijd, zeker de laatste onderhandelingen
- vaak is het niet duidelijk wie de meest recente versie heeft

Dat kan anders!

De innovatieve documentengenerator van JuriBlox zet de norm voor slimme documenten. Iedereen in uw organisatie – met of zonder juridische kennis – kan een juridisch document opstellen. Vervolgens kunt u gemakkelijk samen met de wederpartij onderhandelen, zonder versies kwijt te raken. Als u er samen uit bent gekomen, ondertekent u het document digitaal en slaat u deze overzichtelijk op!

Benieuwd naar de mogelijkheden? Neem contact op met **Mark Hoogewerf**!

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

juriblox.nl →

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Noot bij Rechtbank Den Haag 5 februari 2020 (ECLI:NL:RBDHA:2020:865)

Het computersysteem dat de overheid gebruikt om fraude te ontdekken, schendt de privacy. Dat blijkt uit de langverwachte SyRI uitspraak van de rechtbank Den Haag. Die wijst de inzet van SyRI door het UWV af omdat er geen onderbouwde noodzaak is. Logische uitspraak, zou je zeggen. Maar het is wel een héle dikke lap vonnis die men neerlegt: ik heb nog nooit 118 overwegingen gezien om een eis toe te wijzen.

Het Systeem Risicoindicatie (hierna: SyRI) is een wettelijk instrument dat de overheid gebruikt ter voorkoming en bestrijding van fraude op het terrein van de sociale zekerheid en inkomensafhankelijke regelingen, de belasting- en premieheffing en de arbeidswetten. Het gaat volgens de wetgever om technische infrastructuur en de bijbehorende procedures waarmee in een beveiligde omgeving anoniem data kunnen worden gekoppeld en geanalyseerd, zodat risicomeldingen kunnen worden gegenereerd. In de praktijk werkt dit door gegevens van burgers uit allerlei overheidsdatabases te koppelen. Via een algoritme komen vervolgens risicoprofielen en personen met een verhoogd risico op fraude naar voren.

Grof gezegd: als in het weekend je waterverbruik hoger is dan normaal en je staat als alleenstaand bekend, dan ben je een mogelijke fraudeur, pardon een risico want kennelijk woont je partner in het weekend bij jou. Dus dan krijg je een onderzoek en moet je aantonen dat je in het weekend gewoon graag in bad gaat. (Let op dat jij de bewijslast hebt want jij moet alle relevante feiten melden, dus ook bewijzen dat je alles hebt gemeld.)

Dat dit systeem velen de kriebels gaf, hoeft niet te verbazen. Een principiële rechtszaak was dan ook het gevolg, aangespannen door een aantal maatschappelijke organisaties, waaronder het Nederlands Juristen Comité voor de Mensenrechten, stichting Privacy First en twee burgers. Zij stellen dat dit systeem fundamenteel in strijd is met de wet, meer specifiek artikel 8 EVRM omdat de burger zo niet langer onbevreesd zichzelf kan zijn.

Om als overheid de privacy van de burger te mogen inperken, zet de wet (artikel 8 EVRM) een aantal grenzen. De eerste lijkt de makkelijkste: er moet een wet zijn die bepaalt wanneer dit mag, waarom en tot hoe ver dan. Die wet maken kostte onze overheid nog even tijd, maar hij kwam er dan toch in 2014 als een wijziging in de Wet SUWI. Deze bepaalt dat “risicomeldingen” kunnen worden gedaan binnen een samenwerkingsverband, op basis van data die een aantal samenwerkende instanties tot hun beschikking hebben.

Daarbij is, getuige het stroomschema hiernaast, behoorlijk nagedacht over de procedurele kant.

Maar met een wet ben je er niet. Die wet moet ook een legitiem doel dienen. Daar is de rechtbank vrij snel klaar mee: fraudebestrijding is legitiem want dat kost ons allen veel geld. Zo’n 150 miljoen euro, en daar achteraan willen is legitiem. (Als de rechtbank had gezegd dat dat slechts 0,2 procent van het totaal aan uitkeringen is, dan had dat zo raar geklonken. En ik laat u tussen deze haakjes achter met de constatering “Het gemiddelde fraudebedrag per uitkering is 17 euro.”)

Oké, kennelijk legitiem dus. Maar dan komt de laatste en grootste horde: noodzakelijkheid, proportionaliteit en subsidiariteit in het licht van de doelen die de wet dient. Dit is een hele mond vol, maar concreet moet er

sprake zijn van een ‘fair balance’ tussen de doelen van de SyRI-wetgeving en de inbreuk op het privéleven die de wetgeving oplevert.

De grote pijn bij SyRI zit hem hier. Met name wreekt zich dat je niet kunt zien wanneer je een verhoogd risico bent, of waarom dan precies. De wet vermeldt dat niet maar laat dat aan de implementatie over (“specificatie: het doet wat het doet”). Verder dan “je krijgt punten voor iedere risicofactor en er zijn modellen die factoren herleiden tot een signalering” lijkt men niet te zijn gekomen qua uitleg. En dat is bepaald vervelend, zeker als je bedenkt dat je met een systeem als dit juist mensen treft die toch al in een zwakke positie zitten én met wetgeving te maken hebben waarvan het niet frauderen bepaald geen sinecure is. (Had ik al gezegd dat 'vergeten door te geven dat je moeder 3 weken komt logeren' een vorm van fraude is?) Daarmee ontbreken dus de benodigde waarborgen om fouten te voorkomen of de gevolgen daarvan in te kunnen perken.

Vorig jaar waarschuwde ook een speciaal rapporteur van de VN dat SyRI voor 'digitale stigmatisering van arme burgers' zou zorgen. De rechtbank zegt dat bewezen is dat vooral arme mensen werden doorgelicht door het systeem. “Dat op zichzelf hoeft niet te impliceren dat die inzet in alle gevallen disproportioneel is, maar gegeven de grote hoeveelheden gegevens die in aanmerking komen voor verwerking in SyRI, en de omstandigheid dat gebruik wordt gemaakt van risicoprofielen, bestaat wel het risico dat met de inzet van SyRI onbedoeld verbanden worden gelegd op basis van bias, zoals een lagere sociaal economische status of een immigratieachtergrond”, aldus de rechtbank.

Het belangrijkste verweer lijkt te zijn geweest dat SyRI ‘slechts’ een indicatie geeft en nog lang geen vonnis. Dat mag zo zijn, maar in de praktijk krijg je natuurlijk gewoon een onderzoek op je dak, en mede vanwege die omgekeerde bewijslast én de weinig juridisch onderlegde mensen die je dan treft, pakt dat dus erg vervelend uit. Zeker als je bedenkt dat meer dan de helft van de signaleringen vals positief was, zo blijkt uit Kamervragen begin januari 2019.

Ook werd aangevoerd dat diverse deelnemers toetsen of hun inzet wel rechtmatig is. Maar de optelsom van de toetsen kan niet zonder meer als een integrale toets vooraf worden beschouwd. De SyRI-wetgeving geeft geen inzicht in de werking en validatie van de risicoindicatoren en het risicomodel. Het risicomodel en de risico-indicatoren zijn immers mede van betekenis voor de beoordeling of en in hoeverre de gegevensverstrekking noodzakelijk is en daarmee ook voor het algehele effect op het privéleven van de vergelijking van de verschillende datasets die in SyRI plaatsvindt. Ook tegen deze achtergrond heeft een betrokkene naar het oordeel van de rechtbank onvoldoende zekerheid dat zijn privacy bij de inzet van SyRI is gewaarborgd.

Gelet op de grote hoeveelheid gegevens die in aanmerking kunnen komen voor de verwerking in SyRI en de omstandigheid dat in een concreet SyRI-project de noodzakelijkheidstoets door de afzonderlijke deelnemers aan het project wordt verricht, derhalve zonder integrale en bovendien geen onafhankelijke toets voorafgaand aan de goedkeuring door de Minister, bevat de SyRI-wetgeving dan ook onvoldoende waarborgen voor de conclusie dat, gelet op de beginselen van doelbinding en dataminimalisatie, voldaan is aan artikel 8 lid 2 EVRM. Inzet van het systeem werd dan ook vrij snel na de uitspraak gestaakt.

Van onze blog

Overheid Privacy

19 februari 2020

De journalistieke exceptie: waar ligt de grens?

Wanneer sprake is van journalistieke publicaties op het internet, is de Algemene verordening gegevensbescherming (AVG) slechts gedeeltelijk van toepassing. Dit wordt ook wel de journalistieke uitzondering genoemd, en is er om balans te creëren tussen de vrijheid van meningsuiting en de bescherming van privacy. Wanneer is sprake van een publicatie met een journalistiek doel, en waar komt deze journalistieke exceptie vandaan?

Wat is journalistiek?
Het College Bescherming Persoonsgegevens (CBP) besloot in 2007 in Nederland tot het vaststellen van 'richtsnoeren'[1] om te kunnen analyseren of een artikel onder de journalistieke exceptie valt. De richtsnoeren hebben het karakter van een beleidsregel. Er vindt een globale beoordeling plaats door naar de uiting in context te kijken en daarna tot een afweging van belangen te komen. Daarbij worden vier criteria gehanteerd:

1. Is de activiteit gericht op (objectieve) informatieverzameling en verstrekking?
2. Gaat het om een regelmatige bezigheid?
3. Gaat het erom iets van maatschappelijke strekking aan de orde te stellen?
4. Kent de publicatie een recht van repliek of rectificatie achteraf?

Als een publicatie aan alle vier criteria voldoet, is de journalistieke exceptie in ieder geval van toepassing. Maar: ook wanneer een publicatie niet aan alle criteria voldoet, kan de vrijstelling gelden.

Nederland versus Europa
De ruime interpretatie van journalistiek die gevormd is in de rechtspraak van het Hof van Justitie wijkt af van de beperktere invulling van de Autoriteit Persoonsgegevens. Het HvJ oordeelde in het Satamedia[2] arrest dat journalistieke activiteiten zo aangeduid kunnen worden als zij bekendmaking van informatie, meningen of ideeën aan het publiek tot doel hebben. Deze activiteiten zijn niet voorbehouden aan mediaondernemingen, aldus bepaald in het *Satamedia* arrest. In het arrest van Gasteren/Hemelrijk[3] werd aangekaart dat ook online media journalistiek kunnen verwerken.

Het is voor de journalistieke exceptie van de AVG van belang voor welke doeleinden verwerking van persoonsgegevens plaatsvindt. De AP geeft aan[4] dat om onder de journalistieke uitzondering te vallen, een publicatie uitsluitend een journalistiek doel dient te hebben. Dit wordt bepaald aan de hand van de vier criteria die eerder zijn opgesteld door het CBP. Deze interpretatie wijkt af van de visie van het HvJ.

Of sprake is van journalistieke doeleinden, hangt volgens vaste rechtspraak van het HvJ namelijk af van onder meer de bijdrage aan een debat van openbaar belang, de bekendheid van de betrokken persoon, het onderwerp van het bericht, het eerdere gedrag van de betrokken persoon, de inhoud, de vorm en de gevolgen van de publicatie, de wijze waarop en de omstandigheden waarin de informatie is verkregen en de waarachtigheid ervan. Het concept 'uitingsvrijheid' moet ruim worden uitgelegd en de journalistieke uitzondering ziet dus niet enkel op krantenberichten.

1. https://bit.ly/3cua4vF
2. https://bit.ly/2TkAtEA
3. https://bit.ly/2xaFrez
4. https://bit.ly/2uVUurO

Kamervragen
Over dit verschil in interpretatie zijn Kamervragen[5] gesteld. Volgens minister Dekker wordt in Europese wet- en regelgeving het begrip journalistiek heel breed opgevat, *"omdat er heel veel verschillende journalistiek onder valt"*. Het is jammer dat de minister er niet voor kiest wat dieper in te gaan op het onderscheid in interpretatie. Wel geeft de minister aan dat de uitzondering, zoals opgenomen in artikel 43 UAVG, meebrengt dat enkel een aantal algemene beginselen en basale verplichtingen voor de verwerkingsverantwoordelijke van toepassing zijn op gegevensverwerkingen in het kader van de journalistieke doeleinden. De minister noemt hierbij als voorbeeld beginselen van proportionaliteit en de verplichting om gegevens op passende wijze te beveiligen. Uit deze bewoording zou de conclusie getrokken kunnen worden dat er van de ruime interpretatie van het HvJ uit wordt gegaan, nu de vier richtsnoeren niet worden genoemd maar enkel algemene beginselen.

Uitzonderingen
Het is duidelijk dat we de journalistieke uitzondering ruim kunnen interpreteren en hier vaak meer onder valt dan de naam doet vermoeden. In Nederland is in de UAVG besloten tot het uitzonderen van bepaalde zaken wanneer de verwerking van persoonsgegevens plaatsvindt voor journalistieke doeleinden. Een voorbeeld hiervan is de uitzondering op het recht om je toestemming in te trekken, maar ook het bijhouden van een verwerkingsregister van deze verwerkingen.

5. https://bit.ly/2lgd1BZ

Het zou ook niet haalbaar zijn om alle verzoeken van betrokkenen in te moeten willigen wanneer er sprake is van een journalistieke publicatie. Stel je voor dat alle blogposts, interviews en andersoortige artikelen moeten worden aangepast, omdat een betrokkene er achteraf toch niet zo blij mee was. Dit zou een zeer negatief effect hebben op de vrijheid van meningsuiting. Afsluitend geldt voor de verwerking van bijzondere persoonsgegevens dat deze alleen verwerkt mogen worden als dat strikt noodzakelijk is voor het journalistieke doel. Voor deze gegevens geldt dus een (extra) noodzakelijkheidstoets.

Auteur
Linde Mensink
Juridisch adviseur

Deze blog is in samenwerking geschreven met Anouk van Rijn, juridisch adviseur bij ICTRecht.

31 januari 2020

Internetscreenen van sollicitanten: iedereen doet 't, maar mag het?

Met één druk op de knop kun je vandaag de dag al een hoop te weten komen over een sollicitant: even googelen of een kijkje nemen op iemands Instagram en Facebook. Het is openbare informatie dus dat mag toch gewoon? Zo simpel ligt het niet. Het gaat om persoonsgegevens en dus is de AVG van toepassing. Dit betekent dat je eerst een aantal zaken op orde moet hebben voordat je de wondere wereld van het internet mag gaan afstruinen, op zoek naar informatie over een sollicitant.

De AVG in de sollicitatieprocedure

In de sollicitatieprocedure staat het verzamelen van informatie centraal. De AVG speelt daarin een belangrijke rol, zoals we eerder al schreven[1]. Er worden immers veel persoonsgegevens verwerkt. Dit is ook het geval bij een internetscreening. Wanneer je bijvoorbeeld naar beneden scrolt op iemands tijdlijn op Facebook kun je vaak veel informatie over iemand verzamelen. Denk aan berichten, foto's en gedeelde media. Niet zelden is dit materiaal waarvan de sollicitant liever niet wil dat een potentiële werkgever dit onder ogen krijgt. Als werkgever kun je een negatief beeld krijgen van een sollicitant, als bepaalde berichten, foto's en gedeelde media niet in de smaak vallen. Dit kan weer van invloed zijn op of een sollicitant wel of niet wordt aangenomen. Een internetscreening kan dan ook ingrijpend zijn voor de privacy van de sollicitant en impact hebben op de sollicitatieprocedure. De wetgever vindt daarom ook dat je niet zomaar mag gaan screenen. Wanneer dan wel?

1. https://bit.ly/2IloIHU
2. https://bit.ly/2PMw2QP
3. https://bit.ly/2Ijp9T6

Gerechtvaardigd belang als grondslag voor internetscreening

Internetscreening van sollicitanten kan niet gebaseerd zijn op toestemming. De AVG eist namelijk dat toestemming in vrijheid moet zijn gegeven om rechtsgeldig te zijn. Gezien de afhankelijkheidsrelatie is vrije toestemming in dit geval niet mogelijk. De werkgever zal dan ook uit een ander vaatje moeten tappen en een gerechtvaardigd belang[2] moeten hebben om te mogen screenen. Daarbij dient de werkgever een schriftelijke belangenafweging te maken tussen de belangen van de werkgever en de werknemer.

Als werkgever moet je kunnen uitleggen waarom het belangrijk is dat er een screening wordt gedaan, oftewel je moet een zakelijk belang hebben. Vaak zie je dat er wordt aangevoerd dat een werkgever erop moet kunnen vertrouwen dat zijn toekomstige werknemer integer en betrouwbaar is. Voor de ene organisatie en/of functie geldt dat wat meer dan voor de ander. Bij een medewerker op een kinderopvang ligt dat bijvoorbeeld net wat anders dan iemand die pizza's bezorgt. Voer als werkgever alleen een internetscreening van je sollicitant uit als je hiervoor een goede reden hebt. Bijvoorbeeld als het online verzamelen van informatie over kandidaten echt noodzakelijk en relevant is voor de organisatie en uitvoering van de functie.

De internetscreening moet worden toegespitst op de eventuele risico's van de organisatie en de betreffende functie en de werkgever mag alleen de hiervoor relevante informatie opnemen in het dossier. Sta ook stil of er minder ingrijpende middelen beschikbaar zijn, bijvoorbeeld of bepaalde informatie kan worden achterhaald door er gewoon in het sollicitatieproces naar te vragen. Uiteindelijk is het van belang dat jij als organisatie in de belangenafweging tot uitdrukking weet te brengen *waarom* een internetscreening écht nodig is, en niet alleen handig.

Informeren
Het informeren van sollicitanten is verplicht volgens de AVG, zodat de sollicitant weet waar hij of zij aan toe is. Je moet transparant zijn over dat je (mogelijk) gaat screenen op het moment dat iemand solliciteert. Doe dit door in de vacaturetekst aan te geven dat er (mogelijk) een internetscreening wordt uitgevoerd. Denk er ook aan om een privacyverklaring[3] op je website op te nemen, waar de sollicitant nadere informatie kan vinden. Je dient in de vacaturetekst naar de privacyverklaring te verwijzen. In deze verklaring geef je aan waarom je persoonsgegevens verzamelt, wat de grondslag is en wat je met de resultaten doet. Ook achteraf dien je de sollicitant te informeren over de uitkomsten van de internet-screening. Maak dit dus bespreekbaar of verstuur dit per e-mail.

Verlies de AVG niet uit het oog
Mocht je een belangenafweging hebben gemaakt en op juiste wijze hebben geïnformeerd, dan ben je er nog niet. Verlies ook niet de overige vereisten van de AVG uit het oog als je gaat screenen. Dit betekent onder andere dat de gegevens die worden verzameld niet voor een ander doel mogen worden gebruikt dan waarvoor je ze hebt verzameld. Zorg daarnaast voor passende beveiligingsmaatregelen en bewaar de gegevens niet langer dan nodig. En schakel je een derde partij in die in opdracht van jou de internet-screening gaat uitvoeren? Sluit dan een verwerkers-overeenkomst waarin je afspraken maakt over de omgang met persoonsgegevens.

Auteur
Jay Remmelzwaal
Juridisch adviseur

Deze blog is in samenwerking geschreven met Anouk van Rijn, juridisch adviseur bij ICTRecht.

4 PUNTEN PO ADVOCATUUR
NEDERLANDSE ORDE VAN ADVOCATEN

6 PUNTEN PO ADVOCATUUR
NEDERLANDSE ORDE VAN ADVOCATEN

iapp CPE credits approved

Trainingsoverzicht april – juli 2020

Donderdag 16 april

ICT en gezondheidsrecht (6 PO)

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

https://bit.ly/37KVuO0

Donderdag 23 april

Privacy en persoonsgegevens: de basis (6 PO)

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

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

https://bit.ly/2L1JM86

Dinsdag 12 mei

Contracteren: de basis (6 PO)

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

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

https://bit.ly/2sqpyhJ

Dinsdag 26 mei

Update Algemene verordening gegevensbescherming (AVG) (4 PO)

Wij praten u in een middag bij over de belangrijkste recente ontwikkelingen op het gebied van de Algemene verordening gegevensbescherming (AVG). Er worden praktijkvoorbeelden behandeld, onder meer over datalekken en boetes.
De insteek van de training is interactief en praktijkgericht.

https://bit.ly/2OpHt0q

Dinsdag 16 juni

Privacy en persoonsgegevens: de verdieping (6 PO)

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

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

https://bit.ly/35LBVU1

Donderdag 2 juli

Contracteren: de verdieping (6 PO)

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

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

https://bit.ly/2pXlg0j

Nog niet voldoende juridische kennis in huis? Dan is een inhouse training van ICTRecht iets voor u.

Wij ontwikkelen een inhouse training volledig voor u op maat waarbij voorbeelden uit uw eigen praktijk in het lesprogramma worden verwerkt. Mogelijke onderwerpen zijn onder meer: privacywetgeving en de AVG, ICT-contracten en digitaliseren binnen de overheid.

Meer weten of een offerte aanvragen? Kijk op:
https://bit.ly/33nmSy8

Heeft u vragen of wilt u meer weten?

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

Alisa Schurink
Opleidingscoördinator
en Marketingmedewerker


ICTRECHT
adviesbureau