

jaargang 7 nummer 1 januari 2019



Ruim een half jaar AVG:
wat is de stand van zaken?

Rechtskeuze bij
internationale contracten

Blockchain en recht: nieuwe
vraagstukken voor juristen

Heeft u uw juridische zaken goed geregeld?

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

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

Wij kunnen u van dienst zijn met:

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



ICTRECHT
adviesbureau

Meer informatie over hoe wij werken? Bezoek ictrecht.nl

Voorwoord

Een nieuw jaar, een nieuwe blik op juridische zaken. De belangrijkste kwestie om op terug te kijken, is natuurlijk de Algemene Verordening Gegevensbescherming (AVG). De AVG mag met recht een revolutie in de ICT-dienstverlening worden genoemd, maar heeft op veel meer gebieden dan daar impact gehad. De angst voor boetes zit er nog goed in, dus tijd voor een eerste terugblik. Wat is de stand van zaken?

Ook in dit nummer een terugblik op de praktijk rond cryptomunten. Na het vierde kwartaal van 2017 is de manie afgezwakt en is het sentiment teruggekeerd naar een niveau dat ruimte biedt voor reflectie. Hoe ongrijpbaar gaat cryptogeld worden in 2019? En meer algemeen, welke vraagstukken spelen bij blockchain technologie en het recht?

In de contractspraktijk nog steeds goed voor veel discussies: welk recht moet worden gekozen bij internationale overeenkomsten? Natuurlijk wil iedereen het liefst zijn eigen recht, maar in de praktijk levert dat vaak een patstelling op. Hoe daar uit te komen, leest u verderop. En komt u er onverhoopt niet uit, dan wordt het tijd voor conflictoplossing.

In ieder geval wensen wij u een gelukkig 2019!



Directie
Steven Ras en Arnoud Engelfriet

Index

Ruim een half jaar AVG: wat is de stand van zaken?	4
Rechtskeuze bij internationale contracten	7
Wet- en regelgeving	10
Aandachtspunten bij (online) verkoop van vouchers	13
Direct marketingrecht	15
Coinrecht – Jaaroverzicht 2018	17
Recht uit de praktijk: conflictoplossing	20
Blockchain en recht: nieuwe vraagstukken voor juristen	23
ICT en zorg: vragen uit de praktijk	26
Digitaliseren en elektronische handtekening	29
Internetrechtspraak	31
Noot bij Rechtbank Den Haag 30 augustus 2018	37
Van onze blog	39
ICTRecht Academy	42

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 (papiereditie), inclusief verzendkosten in Nederland. Voor een jaarabonnement (digitale editie) betaalt u € 67,50 excl. btw.

Aan deze uitgave werkten mee:

Arnoud Engelfriet - Algemeen directeur / Opleidingsdirecteur - a.engelfriet@ictrecht.nl
Steven Ras - Algemeen directeur - s.ras@ictrecht.nl
Matthijs van Bergen - Directeur Legal ICT - m.vanbergen@legalict.com
Lisette Chew-Meij - Directeur ICTRecht privacy - l.meij@ictrecht.nl
Alisa Schurink - Opleidingscoördinator en Marketing Assistant - a.schurink@ictrecht.nl
Arend Jan Wiersma - Juridisch adviseur - a.wiersma@ictrecht.nl
Bram de Vos - Juridisch adviseur - b.devos@ictrecht.nl
Beryl Hetharia - Juridisch adviseur - b.hetharia@ictrecht.nl
Cas Mevissen - Juridisch adviseur Legal ICT - c.mevissen@legalict.com
Esther Flierman - Juridisch adviseur ICTRecht Groningen - e.flierman@ictrecht.nl
Demi Grandiek - Juridisch adviseur - d.grandiek@ictrecht.nl
Jay Remmelzwaal - Juridisch adviseur - j.remmelzwaal@ictrecht.nl
Jorden Bailey - Juridisch adviseur - j.bailey@ictrecht.nl
Raoul van de Laak - Juridisch adviseur - r.vandelaak@ictrecht.nl
Samantha van de Stouwe - Juridisch adviseur ICTRecht Groningen - s.vandestouwe@ictrecht.nl
Sari Jansen - Juridisch adviseur - s.jansen@ictrecht.nl
Eline Pellis - Vormgever - eline@elinepellis.com
Leonard Fäustle Stills & Motion - foto's ICTRecht - info@leonardfaustle.nl



Fay Kartner
Juridisch adviseur

Privacy

Overheid

Ruim een half jaar AVG: wat is de stand van zaken?

Het is alweer meer dan een half jaar geleden sinds de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018 van toepassing werd. Wat heeft deze nieuwe Europese privacywetgeving ons tot nu toe gebracht? Welke onduidelijkheden uit deze wet zijn inmiddels opgehelderd? Wordt er inmiddels druk gehandhaafd? Waar moeten we op blijven letten, ook al hebben we ons keurig voorbereid op de strengere privacy-eisen?

Meer privacybewustzijn, inzage- en verwijderverzoeken

De AVG is bedoeld om minstens 10, 20 of zelfs 30 jaar mee te gaan. Eén van haar hoofddoelen heeft zij inmiddels (in elk geval deels) bereikt: veel meer bewustzijn bij personen over hun privacyrechten. Rond 25 mei kon er geen nieuwsuitzending of krant worden bekeken zonder dat het onderwerp aan de orde kwam, ieders mailbox stroomde vol met geüpdatete privacyverklaringen en verzoeken om (hernieuwde) toestemming voor een nieuwsbrief – en voor bedrijven het sluiten van een verwerkersovereenkomst. Zeker in Nederland blijken mensen bereid om hun stem te laten horen en een klacht, inzage- of vergetverzoek in te dienen.

Veel bedrijven hebben al te maken gehad met dergelijke verzoeken. Het is daarom van belang om te weten hoe hiermee om te gaan, en iemand binnen uw bedrijf hiervoor verantwoordelijk te maken. Beoordeel elk verzoek kritisch: misschien heeft u inderdaad geen reden (meer) om de betreffende gegevens te verwerken, maar in veel gevallen ook wel. Zorg dan dat u dit helder kunt beargumenteren.

Zijn er boetes uitgedeeld?

Misschien wel de vraag waarin bedrijven het meest geïnteresseerd waren, was of er überhaupt boetes uitgedeeld zouden worden, en zo ja aan wie. De maximumbedragen zijn namelijk fors gestegen. Een aantal voorbeelden van partijen die sinds 25 mei beboet zijn voor AVG-schendingen:

- Aan de buitenkant van zijn pand had een Oostenrijkse ondernemer een camera gehangen die een deel van de openbare weg filmde. Hiervoor was geen wettelijke grondslag, en betrokkenen waren niet duidelijk geïnformeerd over het gebruik van de camera. De boete bedraagt 'slechts' € 4.800, doordat rekening gehouden wordt met de financiële draagkracht van de ondernemer.
- Een stuk hoger was een boete die de Portugese toezichthouder CNPD heeft opgelegd: € 400.000 aan het Centro Hospitalar Barreiro Montijo. Dit vanwege het feit dat bijna 1.000 personen toegang hadden tot bepaalde medische gegevens, terwijl er slechts 296 artsen werkzaam waren. Ook waren de systemen niet passend beveiligd.
- Ook is door de Autoriteit Persoonsgegevens (AP) de eerste (hoge) boete opgelegd voor het niet tijdig melden van een datalek, namelijk € 600.000 aan taxibedrijf Uber.

Let wel altijd goed op wanneer u een brief van de autoriteit ontvangt met een boete: er zijn nepbrieven in omloop, verzonden door criminelen. Controleer dus of de AP daadwerkelijk de afzender is wanneer u twijfelt.

Controles door de AP

De AP is daarnaast ook druk aan het controleren op de meer algemene verplichtingen uit de AVG. Zo heeft zij bij een aantal grote organisaties het register van verwerkingen van persoonsgegevens opgevraagd. Hieraan lijkt veel waarde te worden gehecht: de AP ziet het register als een peilstok voor hoe een bedrijf met privacy omgaat. Hoewel het niet alles zegt, is dit wel

een goede manier om een eerste selectie te maken van welke bedrijven serieuze aandacht besteden aan privacy, en welke niet.

Hoewel ook voor kleinere bedrijven of bedrijven die weinig persoonsgegevens verwerken een controle niet uit te sluiten is, lijkt de AP zich tot nu toe vooral te richten op waar de grootste risico's zitten. Bij een aantal overheidsinstanties en ziekenhuizen, banken en verzekeraars is gecontroleerd of deze wel een functionaris voor gegevensbescherming hebben aangesteld.

De AP heeft aan verschillende partijen aangegeven welke maatregelen zij moeten nemen om aan de AVG te voldoen (al dan niet onder dwangsom wanneer niet tijdig voldaan wordt):

- De Belastingdienst verwerkt onrechtmatig het burgerservicenummer (BSN) van mensen met een eenmanszaak. Het btw-nummer van deze bedrijven, bevat het BSN van de ondernemer, hoewel zij verplicht zijn dit te publiceren. De Belastingdienst moet hier een oplossing voor vinden die geen gebruik maakt van het BSN.
- De Nationale Politie moet persoonsgegevens beter beschermen. De politie moet beter controleren of niet te veel personen toegang hebben tot het systeem waarmee inkomende en uitgaande personen in het Schengengebied worden gecontroleerd (de controle vond nog plaats onder de oude wetgeving, maar geeft wel goed aan bij welk soort verwerkingen de prioriteit ligt voor de AP).

- Het UWV heeft het online werkgeversportaal onvoldoende beschermd tegen toegang door onbevoegden. Zo wordt er geen gebruik gemaakt van meerfactorauthenticatie. De AP geeft aan dat dit hier wel passend is, en dus aangepast dient te worden (ook deze controle vond nog plaats onder de oude wetgeving).
- Cameratoezicht: de AP stelt strenge voorwaarden aan cameragebruik, zowel voor het beveiligen van eigendommen, als bijvoorbeeld in billboards.
- Alleen bij hoge uitzondering mag nog wifi-tracking worden toegepast. Daarop is overigens ook de e-Privacyverordening van toepassing die nog in de maak is, dus op de definitieve regeling hiervan moeten we nog even wachten.

De nadruk ligt dus op de overheidsverwerkingen, en gevoelige gegevens zoals gezondheids- en financiële gegevens. Ook direct marketing en doorverkoop van persoonsgegevens krijgen veel aandacht.

Let ook op de 'nieuwe' versie van de AVG, waarin o.a. taalfouten zijn gecorrigeerd. Het is wel apart dat hierin ook enkele (niet onbelangrijke!) inhoudelijke wijzigingen zijn gedaan, maar hierover is al eerder geschreven (lees het artikel hierover van Michelle Wijnant in editie 3, juli 2018 van dit tijdschrift).

DPIA (Data Protection Impact Assessment)

Een verplichting onder de AVG waarmee doorlopend rekening gehouden moet worden, is het uitvoeren van



een DPIA (gegevensbeschermingseffectbeoordeling). Dit is een voorafgaand onderzoek naar een nieuw systeem/project dat waarschijnlijk een hoog risico voor de privacy inhoudt. Denk bijvoorbeeld aan het monitoren van personeel, een elektronisch patiëntendossier, of cameratoezicht. De risico's moeten dan in kaart worden gebracht, en waar mogelijk verminderd worden. Dit is een cyclisch proces. Verandert een verwerking en daarmee het risico, worden er bijvoorbeeld locatiegegevens toegevoegd aan een bepaalde app? Ga dan na of een reeds uitgevoerde DPIA ook een update vereist.

De AP, en alle andere nationale privacytoezichthouders, hebben allemaal een lijst ingediend van verwerkingen waarvoor naar hun mening altijd een DPIA vereist is (zij hebben overigens ook de mogelijkheid om lijsten te maken van activiteiten die nooit een DPIA vereisen, maar dit is nog niet gebeurd). Om te voorkomen dat de werkwijzen van de nationale toezichthouders te veel uiteen gaan lopen, heeft de European Data Protection Board (de vroegere Artikel 29-werkgroep, waarin de toezichthouders verenigd zijn), de lijsten beoordeeld en aanbevelingen gedaan tot wijziging. Voor Nederland houdt dit in dat nog moet worden verduidelijkt wanneer een DPIA vereist is bij de verwerking van biometrische gegevens. Ook moet worden aangegeven dat het verwerken van locatiegegevens op zich, nog geen DPIA vereist, maar wel als dit bijvoorbeeld op grote schaal gebeurt.

Certificeringen

Certificeringen kunnen bijdragen aan het bewijs dat een organisatie aan de AVG voldoet; echter het bezit van een certificering wil nog niet zeggen dat de toezichthouder nooit meer iets aan te merken kan hebben. Ook in de praktijk moet het een en ander goed gaan. De verwachting is echter wel dat bij organisaties die gecertificeerd zijn, het toezicht minder intensief zal zijn. Momenteel is er nog geen certificeringsmechanisme dat door de AP is goedgekeurd, maar in de toekomst is dit zeker te verwachten. De AVG laat er ook ruimte voor dat er in de toekomst een European Data Protection Seal komt dat voor de gehele EU geldt.

Wilt u in de toekomst uw bedrijf laten certificeren voor de AVG? Let erop dat een bepaalde verwerking gecertificeerd wordt (zoals het systeem waarmee u uw marketing uitvoert), en niet het hele bedrijf. De European Data Protection Board heeft richtsnoeren uitgebracht over de eisen waaraan certificeringscriteria moeten voldoen.

Internationale doorgiften

Onder de AVG gelden extra strenge eisen wanneer

persoonsgegevens worden doorgegeven aan landen buiten de Europese Economische Ruimte (EER). Er moet dan aan extra voorwaarden voldaan worden. Voor bedrijven in de VS kan hierbij worden gekeken of het bedrijf Privacy Shield-gecertificeerd is. Veel grote clouddienstverleners zoals Microsoft, Google en Amazon hebben deze. Wel staat het Privacy Shield ter discussie, maar zolang het nog niet ongeldig is verklaard, kan er gebruik van worden gemaakt. Een andere manier is het sluiten van een EU-modelcontract (een speciaal soort verwerkersovereenkomst) met de betreffende partij buiten de EER. Ook over de houdbaarheid hiervan woedt echter een debat.

Deze extra waarborgen zijn echter niet nodig wanneer de Europese Commissie voor het betreffende land een adequaatheidsbesluit heeft genomen (wat betekent dat de privacywetgeving voldoende dicht bij de AVG-standaarden komt, die de strengste ter wereld zijn). Binnenkort wordt deze lijst uitgebreid: voor Japan is momenteel een procedure gaande hiervoor. Zuid-Korea is eveneens bezig met het aanpassen van zijn wetgeving om hiervoor in aanmerking te komen.

Wat dichterbij huis: vergeet niet dat ook het Verenigd Koninkrijk na de Brexit een 'derde land' zal zijn. De 'Brexit-overeenkomst' moet nog worden goedgekeurd door het Britse parlement, de Raad van de Europese Unie, en het Europees Parlement. Zoals het er nu naar uitziet, zal de AVG daar blijven gelden voor persoonsgegevens van EU-burgers die al voor de Brexit werden verwerkt in het VK. Mogelijk zal er op termijn ook een adequaatheidsbesluit komen voor het VK, maar dit is nog allerm minst zeker.

Geeft u slechts incidenteel persoonsgegevens door aan landen buiten de EER? Dan is het goed om te weten dat de European Data Protection Board recent richtsnoeren heeft aangenomen waarin staat aan welke eisen u moet voldoen om geen extra maatregelen zoals hierboven te hoeven nemen. Ook heeft deze instantie verduidelijkt dat wanneer een bedrijf van buiten de EU een vestiging heeft in de EU, of zich op klanten in de EU richt – de AVG ook geldt voor dat bedrijf.

Ook nadat de AVG van toepassing is geworden, zijn er nog genoeg nieuwe ontwikkelingen. Begrippen uit de AVG die onduidelijk waren, worden steeds verder ingevuld. Voor bedrijven en juristen wordt het daarvoor hopelijk steeds gemakkelijker om met de nieuwe regels te werken. Houd er vooral rekening mee dat het onderwerp 'privacy' het publieke debat voorlopig niet zal verlaten, en dat u dus richting zowel betrokkenen als de toezichthouder altijd moet kunnen uitleggen wat u doet met persoonsgegevens, en waarom.



Matthijs van Bergen
Directeur Legal ICT



Cas Mevissen
Juridisch adviseur
Legal ICT

Contracteren

Rechtskeuze bij internationale contracten

Contractonderhandelingen kunnen lang en ingewikkeld zijn, zeker als het gaat om een overeenkomst tussen internationale partijen. Een belangrijke horde daarbij, die vaak maar beter als eerste genomen kan worden, is de keuze welk recht het contract moet beheersen en waar een procedure gevoerd dient te worden in geval van een geschil. In dit artikel geven wij enkele voorbeelden van praktische gevolgen die aan de rechtskeuze kleven en bieden wij manieren om een impasse in de onderhandeling te voorkomen of te doorbreken.

De patstelling: ieder wil zijn eigen recht

Als partijen onderhandelen over welk recht toepasselijk moet zijn op hun overeenkomst, kan er al snel een patstelling ontstaan. Vaak willen beide partijen hun eigen nationale recht van toepassing laten verklaren en een geschil in eigen land beslechten. Dit is uiteraard niet vreemd, partijen zijn hier immers mee bekend en in een eventueel conflict staat de partij met de meeste kennis van het toepasselijke recht een stuk sterker. Maar hoe is daar nu uit te komen?

De patstelling voorkomen of doorbreken

Voor iedere (potentiële) contractpartij zijn er drie mogelijkheden:

1. Vasthouden aan het eigen recht (koste wat het kost, zelfs al komt daardoor geen deal tot stand);
2. Toegeven aan het recht van de ander;
3. Een 'neutraal' recht overeenkomen.

Om een goede keuze te kunnen maken uit deze drie mogelijkheden, is het van belang inzicht te krijgen in de voor- en nadelen van iedere keuze. We beginnen bij de derde optie, namelijk het kiezen van een ander recht dan dat van één van beide partijen. Welke factoren kunnen doorslaggevend zijn in deze keuze?

Een ('neutraal') rechtsstelsel kiezen, wat is van belang?

Een belangrijke praktische overweging is de **taal** waarin het recht beschikbaar is. Het is sterk af te raden om voor een nationaal recht te kiezen dat niet beschikbaar is in een taal die u, of uw juridisch adviseur, begrijpt.

Gezien de voertaal in het internationaal handelsverkeer vaak Engels is, zal het vaak praktisch zijn een rechtsstelsel te kiezen waarvan de wetteksten in het Engels beschikbaar zijn. Bij Engelse wetteksten denkt u, terecht, misschien al snel aan het Engelse en Amerikaanse recht. Er zijn echter ook andere rechtsstelsels waarvan de wetten in het Engels zijn opgesteld, zoals Singapore, Australië of Hongkong. En bijvoorbeeld Zwitserland en Duitsland voorzien in (niet bindende maar in het algemeen kwalitatief goede) Engelse vertalingen van hun wetteksten. Helaas is het Nederlandse recht op het moment, op een paar uitzonderingen na, alleen in het Nederlands beschikbaar.

Uiteraard is de inhoud van het recht ook van groot belang. Is er veel dwingend recht van toepassing of juist weinig? Bevat het recht op belangrijke punten regelend recht waarmee leemtes in het contract kunnen worden ingevuld? En is die invulling dan logisch, praktisch en voldoende voorspelbaar? Als er een keuze gemaakt moet worden voor een 'neutraal' recht dat voor beide partijen vreemd is (of in ieder geval niet hetgeen waar zij primair mee bekend zijn), kan het aan te bevelen zijn om een rechtsstelsel te kiezen waarin de bewoording van het contract het belangrijkste bewijs van de bedoeling van partijen vormt. Dit voorkomt dat een rechter onverwachts met verplichtingen of rechten komt die partijen oorspronkelijk niet voor ogen hadden.

Het Engels recht staat bijvoorbeeld minder gemakkelijk toe dat partijen ander bewijs (zoals e-mailwisselingen in voorafgaande onderhandeling, wat 'parol evidence'



wordt genoemd) aandragen om te beargumenteren wat de partijen precies voor ogen hadden. In het Nederlands recht daarentegen is het de norm om te ‘Haviltexen’, waarbij alle uitingen en gedragingen van de partijen relevant zijn en wat zij daar over en weer redelijkerwijs uit mochten afleiden. Een belangrijk verschil om van bewust te zijn en tevens een reden waarom contracten onder het Engels recht vaak wat langer zijn en ook wat meer uren en kosten van juristen met zich kunnen meebrengen.

Dat brengt ons op het volgende belangrijke punt, namelijk de toegankelijkheid en kostbaarheid van gespecialiseerd juridisch advies. Terwijl bijvoorbeeld over het Engels recht veel goede informatie publiek beschikbaar is, is het inschakelen van een Engelse advocaat in het algemeen juist vrij kostbaar en omslachtig. Engelse advocaten zijn gebonden aan strenge ‘know your customer’ regels, waardoor er eerst een bult informatie over uw bedrijf en aandeelhouders aan de advocaat moeten worden verstrekt voordat hij of zij voor u aan de slag kan. Ook Amerikaanse advocaten staan in het algemeen niet bekend als de goedkoopste, waarbij ook rekening gehouden dient te worden met een aanzienlijk tijdsverschil.

De taal, inhoud en toegankelijkheid van het recht zijn dus belangrijke factoren om te overwegen bij een

rechtskeuze. Tot op zekere hoogte kan dus worden gesproken van concurrentie tussen rechtsstelsels van verschillende landen, met betrekking tot de vraag welk recht het best geschikt is om toe te passen in internationale contracten. Zowel overheden als advocaten en juristen hebben een belang om de toegankelijkheid en kwaliteit van ‘hun’ rechtsstelsel te benadrukken en te vergroten. Dat kan immers leiden tot meer handel en opdrachten.

Twee populaire opties voor internationale contracten: het Engels of Zwitsers recht

Uiteraard is het volstrekt ondoenlijk om van alle landen ter wereld na te gaan welk recht het beste geschikt is voor iedere internationale overeenkomst die u wilt sluiten. Uit onderzoek blijkt dat in de praktijk veel partijen kiezen voor het Engels of Zwitsers recht. Op basis van bovenstaande factoren zoals taal, inhoud en toegankelijkheid zijn daar diverse redenen voor te bedenken.

Voor het Engelse recht kan bijvoorbeeld de taal worden genoemd en de voorspelbaarheid vanwege het feit dat contracten vrij letterlijk naar de inhoud worden getoetst. Al kan het uiteraard ook als nadeel worden beschouwd dat er minder ruimte is om te kijken naar gewekte verwachtingen en redelijkheid en billijkheid, zeker voor partijen die anders gewend zijn.

De populariteit van het Zwitsers recht kan bijvoorbeeld worden verklaard door het feit dat veel internationale arbitragehoven in Zwitserland gevestigd zijn. Voor het gemak, of uit onbekendheid met het feit dat rechtskeuze en forumkeuze niet samen *hoeven* te vallen, wordt dan ook vaak voor het Zwitsers recht gekozen. Daarnaast is de algemeen ‘neutrale’ reputatie van Zwitserland als reden aan te wijzen.

Vergeleken met het Engels recht lijkt het Zwitsers recht in diverse opzichten meer op het Nederlands recht. Het Zwitsers en Nederlands recht zijn beide ‘civil law’ (waar het recht van oudsher meer door formele wetten wordt bepaald) terwijl het Engels recht ‘common law’ betreft (waar rechtspraak traditioneel gezien belangrijker is). Verder is onder het Zwitsers recht meer ruimte voor beoordeling van bewijs buiten het contract zelf en de redelijkheid en billijkheid. Ook de goede trouw, die in Engeland een ondergeschikte rol speelt, is in het Zwitserse recht belangrijker. Het Zwitserse recht kent wel een aantal bepalingen die voor ‘buitenstaanders’ vreemd kunnen aanvoelen. Als er bijvoorbeeld goederen geleverd worden die niet de *exacte* goederen zijn volgens het contract is er sprake van ‘niet leveren’, waardoor een koper al sneller meer bevoegdheden heeft dan onder andere wetten.

Wat als er helemaal geen recht wordt gekozen?

Bij onderhandelingen kan een belangrijk aanknopingspunt zijn welk recht van toepassing zou zijn als er geen rechtskeuze zou worden opgenomen. Binnen de EU is dit bijvoorbeeld bepaald in een tweetal verordeningen (‘Rome I en II’ genaamd). Het uitgangspunt is dan vaak dat het recht geldt waar de dienst feitelijk wordt uitgevoerd. Uiteraard kan dit soms moeilijk zijn om vast te stellen, zeker bij moderne online diensten, wat een belangrijke reden is om juist wel een rechtskeuze op te nemen, maar dit kan de onderhandelingspositie van de leverancier wel versterken. Als dienstverlener zou het dus in bepaalde gevallen misschien zelfs goed kunnen zijn om *niets* in het contract op te nemen over de rechtskeuze, omdat dan het eigen nationale recht (in principe) van toepassing kan zijn. Dat is alleen wel wat riskant en niet zo gebruikelijk; de meeste dienstverleners verklaren gewoon expliciet hun eigen recht van toepassing.

Wat doen de grote Amerikaanse providers doorgaans?

Opvallend is bijvoorbeeld dat de grote Amerikaanse partijen die ook vestigingen binnen de EU hebben, zoals Google, Microsoft, Apple en Amazon, voor sommige diensten apart kiezen welke rechtspersoon verantwoordelijk is en welk recht van toepassing is.

Microsoft bepaalt bijvoorbeeld specifiek voor Skype dat je met een Luxemburgse entiteit contracteert, onder het Luxemburgs recht. Voor alle andere diensten van Microsoft geldt dat gratis diensten worden geleverd door Microsoft Corporation in Redmond onder het recht van Washington, terwijl betaalde diensten binnen de EU worden geleverd door Microsoft Ireland Operations en Microsoft daarbij zelf het recht van het land van de klant expliciet van toepassing heeft verklaard. Steeds wordt ook uitdrukkelijk vermeld dat een rechtskeuze geen afbreuk kan doen aan rechten die een consument heeft op basis van dwingend recht van het land waar de consument woont.

Enkele praktische richtlijnen

Voor de meeste partijen blijft het uiteraard te prefereren om onder het eigen recht zaken te doen. Wanneer dat moeilijk of onmogelijk blijkt vanwege de wederpartij, kan worden gekozen voor een populair ‘neutraal’ rechtstelsel, zoals het Zwitsers of Engels recht. Mocht u te maken hebben met een wederpartij die zelf bijvoorbeeld in Zwitserland, Engeland of Duitsland is gevestigd en graag wil dat diens eigen recht van toepassing is, dan kunt u overwegen om de rechtskeuze toe te geven en te proberen dit te gebruiken als ‘wisselgeld’ om een ander belangrijk punt, bijvoorbeeld de aansprakelijkheidsbepaling, meer naar uw hand te zetten. Gezien de taal, inhoud en toegankelijkheid van deze rechtstelsels hoeft deze keuze namelijk niet zo heel bezwaarlijk voor u te zijn, terwijl het doorduwen van het Nederlands recht een onhaalbare opgave kan zijn. Het is dan wel belangrijk dat u een globaal beeld heeft van het recht dat wordt toegepast en u gespecialiseerd advies kunt inwinnen waar nodig.

En de forumkeuze dan?

Belangrijk om tot slot te vermelden is dat de rechtskeuze en forumkeuze niet noodzakelijkerwijs hetzelfde hoeven te zijn. Het is dus bijvoorbeeld mogelijk om te bepalen dat het Nederlands recht van toepassing zal zijn, maar dat geschillen worden voorgelegd aan de rechter in Zwitserland. Of dat ook praktisch is, is een andere vraag die het beste in een nader artikel over forumkeuze kan worden behandeld. Daarin kan dan ook worden ingegaan op de voor- en nadelen van een keuze voor alternatieve vormen van geschilbeslechting, zoals arbitrage en mediation.

Dit artikel is geschreven door medewerkers van Legal ICT, de internationale tak van ICTRecht, welke is gevestigd in Brussel.



Bram de Vos
Juridisch adviseur

Wet- en regelgeving

Wetsvoorstel patiëntgerichte zorg en inzage recht in medisch dossier van overleden patiënten

Op 12 juli 2018 is er een wetsvoorstel ingediend bij de Tweede Kamer met betrekking tot de verbetering van patiëntgerichte zorg en het opnemen van een wettelijke regeling voor inzage in het medisch dossier van een overleden patiënt. Op dit moment geldt als uitgangspunt dat een hulpverlener alleen een behandeling mag uitvoeren met “geïnformeerde toestemming” van zijn patiënt. Het advies van de hulpverlener is daarbij leidend en specifieke wensen en behoeften van de individuele patiënt spelen een ondergeschikte rol. In het wetsvoorstel wordt meer de nadruk gelegd op patiëntgerichte zorg, waarbij overleg tussen de hulpverlener en patiënt centraal staat. Daarnaast voorziet het voorstel in een uitgebreidere regeling voor inzage in het medisch dossier van overleden patiënten door nabestaanden en voormalig vertegenwoordigers. Ook wordt in het wetsvoorstel de bewaartermijn voor het medisch dossier verlengd van 15 naar 20 jaar. Door medische ontwikkelingen en de toenemende levensverwachting vindt het kabinet het wenselijk dat medische gegevens langer worden bewaard. Dit is onder andere van belang om correlaties tussen ziekten en behandelingen beter te kunnen vaststellen.

<https://bit.ly/2R1kdF5>

Wetsvoorstel register onderwijsdeelnemers

Op 25 september 2018 heeft de Tweede Kamer ingestemd met het Wetsvoorstel register onderwijsdeelnemers. In het voorstel worden verschillende (reeds bestaande) onderwijsregisters, waaronder het basisregister onderwijs, het meldingsregister relatief verzuim, het diploma-register en het register vrijstellingen en vervangende leerplicht, samengebracht in één nieuw register en in één centrale wettelijke regeling. Door het onderwijsregister centraal te regelen, moet er een completer beeld komen van de (persoons)gegevens die het Ministerie van Onderwijs, Cultuur en Wetenschap van onderwijsdeelnemers verzamelt en van het gebruik van die gegevens. Daarnaast moet de wet de informatie-uitwisseling tussen verschillende onderwijssectoren

verbeteren en het hergebruik van onderwijsgegevens vereenvoudigen.

<https://bit.ly/2GeZkp5>

Wetsvoorstel verwerking gepseudonimiseerde persoonsgegevens in de zorg

Op 25 september 2018 is er een wetsvoorstel ingediend bij de Tweede Kamer met betrekking tot de verwerking van gepseudonimiseerde persoonsgegevens in de zorg. Het voorstel ziet onder andere op het controleren van de verzekeringsplicht door zorgverzekeraars. Zorgverzekeraars mogen op grond van de Zorgverzekeringswet (Zvw) alleen een zorgverzekering verstrekken aan personen die verzekeringsplichtig zijn. Bij de vaststelling van de verzekeringsplicht zijn de verzekeraars echter grotendeels afhankelijk van informatie die de verzekeringsnemer zelf verstrekt. Het wetsvoorstel maakt een periodieke controle mogelijk van het gezamenlijk bestand van zorgverzekeraars en het bestand van de SVB, waardoor personen die onterecht verzekerd zijn eerder kunnen worden geïdentificeerd. Het wetsvoorstel voorziet eveneens in een grondslag voor een aantal andere verwerkingen van gepseudonimiseerde persoonsgegevens door de Minister voor Medische Zorg, het Zorginstituut Nederland en het RIVM. Deze gegevensverwerkingen hebben onder andere betrekking op de vaststelling en toekenning van de vereffeningsbijdrage voor zorgverzekeraars en het verwerken van persoonsgegevens ten behoeve van infectieziektebestrijding.

<https://bit.ly/2zozqZX>

Wetsvoorstel wijziging Paspoortwet in verband met elektronische identificatie

Op 1 oktober 2018 werd een voorstel tot wijziging van de Paspoortwet ingediend bij de Tweede Kamer. Het wetsvoorstel maakt het mogelijk om functionaliteiten aan reisdocumenten toe te voegen met betrekking tot elektronische identificatie (via de chips die in de reisdocumenten zijn aangebracht). Daardoor kan de

burger zich online identificeren bij overheidsdiensten met een hoger niveau van betrouwbaarheid dan met het huidige DigiD. Het wetsvoorstel voorziet ook in een uitbreiding van het basisregister reisdocumenten. Op dit moment worden enkel gegevens over vermiste of vervallen reisdocumenten geregistreerd. Om elektronische identificatie mogelijk te maken, zullen echter ook gegevens over de aanvraag, activatie en intrekking van reisdocumenten in het register moeten worden opgenomen. Door de uitbreiding van het basisregister kan ook effectiever worden opgetreden tegen identiteitsfraude of misbruik van reisdocumenten.

<https://bit.ly/2BSPHRQ>

Besluit onderzoek in een geautomatiseerd werk

Op 9 oktober 2018 is het Besluit onderzoek in een geautomatiseerd werk gepubliceerd. Het besluit geeft verdere invulling aan de Wet computercriminaliteit III die reeds in juni 2018 in werking is getreden. Met deze wet werd onder andere de bevoegdheid aan de opsporingsinstanties toegekend om op afstand in te breken in smartphones, computers en andere systemen. In het besluit wordt verder uitgewerkt op welke wijze deze bevoegdheid mag worden ingezet. Zo voorziet het besluit in een plicht tot het bijhouden van logbestanden en worden er technische eisen gesteld aan de ingezette (hack)software. Ook moet de (hack)software worden gekeurd voordat deze door opsporingsinstanties wordt ingezet.

<https://bit.ly/2NFhCOp>

Besluit verlengbaarheid PAMR-vergunning

Op 13 november 2018 is het besluit verlengbaarheid PAMR-vergunning gepubliceerd. Al in 2005 heeft het Ministerie van Economische Zaken de 450 tot 470 MHz-band ter beschikking gesteld voor de exploitatie van een Public Access Mobile Radio (PAMR) netwerk. Dit netwerk is bedoeld voor mobiele communicatie tussen professionele gebruikers in besloten gebruikersgroepen en wordt onder andere gebruikt door taxi-centrales, beveiligingsdiensten en nutsbedrijven. Omdat de PAMR-vergunning in november 2020 afloopt, heeft het Ministerie van Economische Zaken een markt-onderzoek laten verrichten en is er een consultatie gehouden. Op basis hiervan is besloten tot verlengbaarheid van de PAMR-vergunning tot en met november

2024. Waarschijnlijk zal in 2022 de frequentieruimte opnieuw worden verdeeld voor gebruik na de verlengingsperiode (dus na november 2024).

<https://bit.ly/2roM8mZ>

Implementatiewet herziene richtlijn betaaldiensten

Op 4 december is de Implementatiewet herziene richtlijn betaaldiensten aangenomen door de Eerste Kamer. De wet leidt tot een aantal belangrijke wijzigingen in de Wet op het financieel toezicht (Wft). Zo wordt het toepassingsbereik van de Wft ruimer en worden er strengere voorwaarden gesteld aan de vergunning voor betaaldienstverleners. Daarnaast worden er twee nieuwe vormen van betaaldienstverlening geïntroduceerd (de zogeheten betaalinitiatie- en rekeninginformatiediensten) om innovatie in de betaalketen te stimuleren. In het verlengde daarvan regelt de wet de toegang tot bankrekeningen en betalingssystemen. Betaaldienstverleners moeten onder de nieuwe wet (met toestemming van de gebruiker) toegang kunnen krijgen tot betalingssystemen en bankrekeningen. Eventuele hiervoor geldende voorwaarden moeten objectief, evenredig en niet-discriminerend zijn. Het wetgevings-traject heeft flinke vertraging opgelopen, onder meer vanwege onenigheid over de rolverdeling tussen de betrokken toezichthouders. Eigenlijk had de herziene betaaldienstenrichtlijn al in januari 2018 in de Nederlandse wet geïmplementeerd moeten zijn.

<https://bit.ly/2zIXjMw>

Verordening verwerking persoonsgegevens door Europese instellingen, organen en instanties

Op 11 december 2018 wordt de Verordening verwerking persoonsgegevens door Europese instellingen, organen en instanties van kracht (2018/1725/EU). Omdat deze instellingen, organen en instanties niet onder het toepassingsbereik van de Algemene Verordening Gegevensbescherming (AVG) vallen, is er een afzonderlijke wettelijke regeling nodig om de privacy van EU-onderdanen te waarborgen. Hiervoor werd reeds in 2001 een verordening (45/2001/EG) aangenomen, maar vanwege de inwerkingtreding van de AVG was er een vernieuwingsslag nodig.

<https://bit.ly/2Egufzh>



De ICTRecht Academy biedt u diverse praktijkgerichte opleidingen. Specialiseer u tot:



Functionaris Gegevensbescherming (FG)

Start: eind januari 2019



ICT-jurist, niveau juridisch adviseur

Start: maart 2019

56
PUNTEN
PO
ADVOCATEN

NEDERLANDSE ORDE VAN ADVOCATEN



ICT-jurist, niveau senior adviseur

Start: maart 2019

52
PUNTEN
PO
ADVOCATEN

NEDERLANDSE ORDE VAN ADVOCATEN



Senior privacy jurist

Start: maart 2019

36
PUNTEN
PO
ADVOCATEN

NEDERLANDSE ORDE VAN ADVOCATEN

Meer weten of inschrijven?

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



Alisa Schurink
Opleidingscoördinator
en Marketing Assistant



Beryl Hetharia
Juridisch adviseur

Aandachtspunten bij (online) verkoop van vouchers

Tegenwoordig geven bedrijven steeds meer (digitale) vouchers uit. Vouchers blijken een populair cadeau. Er zijn verschillende soorten vouchers, maar meestal is het een tegoed dat gedurende een bepaalde periode bij een ondernemer ingewisseld kan worden. In de praktijk is gebleken dat bedrijven die deze vouchers (willen) uitgeven tegen juridische vragen aanlopen. Wat voor soorten vouchers zijn er, hoe zit het met het afdragen van btw, geldt het herroepingsrecht voor aanschaf van en aankoop met een voucher, en wat is de geldigheidsduur van een voucher? Nieuwe regelgeving op dit gebied is de aanleiding om deze onderwerpen in dit artikel te bespreken.

De nieuwe Voucherrichtlijn geeft duidelijkheid over btw-verplichtingen

Binnen de Europese lidstaten was er onduidelijkheid over btw-heffing wanneer vouchers werden verkocht of daarmee werd betaald. Dit speelde voornamelijk in grensoverschrijdende situaties, waarbij in lidstaat A de voucher was verkocht en in lidstaat B werd ingewisseld. Ondernemers wisten niet of en wanneer btw-heffing moest plaatsvinden. Daarom was op Europees niveau regelgeving nodig. Dat heeft geresulteerd in de Voucherrichtlijn¹, die in Nederland in de Wet op de omzetbelasting 1968 (hierna: Wet OB 1968) is omgezet, en welke regels per 1 januari 2019 gelden.² De nieuwe regels hebben onder andere betrekking op de soorten vouchers en het tijdstip van btw-heffing. De regels gelden alleen voor vouchers die ingewisseld kunnen worden voor goederen of diensten. De voucher is het betaalmiddel waarmee goederen of diensten kunnen worden gekocht. Kortingsvouchers die een prijsverlaging geven, vallen buiten de Voucherrichtlijn.

1. Richtlijn (EU) 2016/1065 tot wijziging van Richtlijn 2006/112/EG wat de behandeling van vouchers betreft.

2. *Stb.* 2018, 82.

3. *Kamerstukken II, 2016/17, 34 755, nr. 3, p. 12.*

Soorten vouchers

Een voucher kan een fysieke vorm hebben, bijvoorbeeld een papieren boekenbon. Tegenwoordig hebben veel vouchers een digitale vorm, zoals een e-mail met daarin een barcode waarmee aankopen gedaan kunnen worden. In de Wet OB 1968 wordt onderscheid gemaakt tussen *vouchers voor enkelvoudig gebruik* en *vouchers voor meervoudig gebruik*. Het soort voucher bepaalt wanneer btw-heffing moet plaatsvinden; bij verkoop of bij verzilvering van de voucher.

1. Voucher voor enkelvoudig gebruik

Bij een voucher voor enkelvoudig gebruik, zijn de plaats van de goederenlevering of dienstverrichting waarop de voucher betrekking heeft en het bedrag van de over die goederen of diensten verschuldigde belasting bekend op het moment van uitgifte van de voucher.³ Bijvoorbeeld een saunabon die toegang geeft tot een sauna in Nederland. Deze dienst valt onder het btw-tarief van 6%. Aangezien de plaats en het btw-tarief bekend zijn op het moment van verkoop, vindt via de gebruikelijke wijze btw-heffing plaats bij verkoop van de voucher.

2. Voucher voor meervoudig gebruik

Een voucher voor meervoudig gebruik, kan voor verschillende goederen of diensten worden gebruikt, of

kan worden ingewisseld in verschillende lidstaten. Bij verkoop van vouchers voor meervoudig gebruik zijn de plaats en bijbehorend btw-tarief nog niet bekend. Dat kan doordat nog niet duidelijk is waar de voucher wordt ingewisseld, of het is nog niet bekend welk btw-tarief geldt voor de goederen of diensten die worden afgenomen.⁴ Denk aan een hotelbon die te verzilveren is in Nederland en Duitsland. In Nederland geldt voor hotelovernachtingen een btw-tarief van 6%, terwijl in Duitsland het btw-tarief 7% is. Daarom geldt dat btw-heffing plaatsvindt wanneer de voucher wordt ingewisseld.

Geldt het herroepingsrecht bij aanschaf van en aankopen met vouchers?

Het kopen van een voucher of cadeaukaart

Een voucher is te kwalificeren als een recht aan toonder. Bij verkoop van een voucher verstrekt de verkoper een voucher (toonderpapier) aan de consument waarmee de consument zijn vorderingsrecht (aankoop doen ter waarde van cadeaubon) kan uitoefenen.⁵ Nu een voucher niet echt gezien kan worden als een product of als dienst, is de vraag of het herroepingsrecht geldt wanneer een voucher online is gekocht. De Autoriteit Consument & Markt heeft zich hierover uitgelaten.⁶ Kruidvat bood online reisvouchers aan, maar consumenten mochten de overeenkomst niet binnen de bedenktijd ontbinden. Dit was onterecht volgens de toezichthouder; herroepingsrecht geldt zolang de voucher niet is ingewisseld.

Ervan uitgaande dat consumenten bedenktijd hebben bij online aankoop van vouchers, zouden ondernemers onder die bedenktijd uit kunnen komen door bijvoorbeeld een cadeaukaart te personaliseren (zoals de kaart laten bedrukken met een afbeelding die de consument kiest)? Maatwerk is namelijk uitgesloten van het herroepingsrecht. Dit gaat waarschijnlijk niet op.

4. *Kamerstukken II, 2016/17, 34 755, nr. 3, p. 12.*

5. Artikel 93 van boek 3 van het Burgerlijk Wetboek.

6. S. Bierling, Kruidvat past voorwaarden actie reisvouchers aan in opdracht van ACM, Den Haag: ACM 2017.

7. Artikel 230r lid 2 van boek 6 van het Burgerlijk Wetboek.

8. Artikel 307 lid 1 boek 3 van het Burgerlijk Wetboek.

9. Artikel 236 sub g van boek 6 van het Burgerlijk Wetboek.

10. Plenaire vergadering, 24036-430, 13 november 2018.

Wanneer voor de gepersonaliseerde cadeaukaart een gering bedrag is betaald en daarop € 50 is gestort, dan zou naar maatstaven van redelijkheid en billijkheid de verkoper bij een beroep op het herroepingsrecht het gestorte bedrag minus de kosten van de kaart kunnen terugbetalen. Zo lijdt de verkoper weinig schade en ontvangt de consument toch een gedeeltelijke terugbetaling.

Het kopen met een voucher of cadeaukaart

Stel, een consument koopt schoenen en betaalt met een cadeaukaart, geldt dan het herroepingsrecht voor de gekochte schoenen? Ja, schoenen vallen niet onder de uitzonderingsclausules. Bij een beroep op het herroepingsrecht moet de verkoper de aankoopprijs terugstorten op de cadeaukaart. De verkoper moet namelijk terugbetalen via hetzelfde betaalmiddel als waarmee de consument heeft betaald, tenzij de consument akkoord gaat met een ander betaalmiddel (geld).⁷

Geldigheidsduur van cadeaukaarten

De geldigheidsduur van cadeaukaarten hangt af van de informatie die je over die cadeaukaart ontvangt. Staat er een uitgiftedatum (datum waarop de consument de cadeaukaart heeft gekocht) op, dan is de cadeaukaart 5 jaar geldig.⁸ Is geen uitgiftedatum vermeld, dan heeft de cadeaukaart een onbepaalde geldigheidsduur. De kaart is dan te gebruiken zolang het bedrijf bestaat. Het is ook mogelijk dat de kaart een beperkte geldigheidsduur heeft. Ondernemers mogen zelf de geldigheidsduur bepalen, maar deze mag niet korter zijn dan 1 jaar. Dat is in Nederland wettelijk geregeld.⁹

Tweede Kamerlid Van den Berg heeft voorgesteld dat de minimale geldigheidsduur van cadeaukaarten twee jaar wordt. Dit ter bescherming van de consument, aangezien cadeaukaarten vaak worden vergeten en dus niet tijdig worden verzilverd. Van den Berg heeft in begin november 2018 een motie ingediend, welke inmiddels door de Tweede Kamer is aangenomen.¹⁰

Bij de verkoop van vouchers moeten ondernemers rekening houden met een aantal zaken. Het soort voucher bepaalt het moment van btw-heffing. Daarnaast hebben consumenten in sommige gevallen bedenktijd bij de aankoop van een voucher en bij de aankoop met de voucher. Tot slot zal de minimale geldigheidsduur van cadeaukaarten waarschijnlijk worden verlengd naar 2 jaar.



Demi Grandiek
Juridisch adviseur



Lisette Chew-Meij
Directeur
ICTRecht privacy

Marketing

E-commerce

Direct marketingrecht

Handelen in data is een lucratieve business. We hebben allemaal weleens een mail of poststuk ontvangen van partijen waarvan wij ons afvroegen hoe zij aan onze gegevens zijn gekomen. Relatief weinig handelingen zijn nodig om data te (ver)kopen en in te zetten voor direct marketing doeleinden. Ook het hergebruiken van zelf verworven data is geen uitzondering. Data is tenslotte geld waard. U mag data (ver)kopen of gebruiken voor andere doeleinden, maar let wel: de wet stelt voorwaarden aan deze manieren van het gebruik van data.

Data & direct marketing

Om te illustreren hoe data gebruikt kan worden voor direct marketing doeleinden, een simpel voorbeeld: iemand die een abonnement heeft op een voetbalzender op TV zal wellicht ook geïnteresseerd zijn in een voetbalreisje. De voetbalreisaanbieder wil daarom graag abonneehouders van de desbetreffende voetbalzender benaderen om te vragen of ze inderdaad geïnteresseerd zijn in zijn voetbalreis. Direct marketing dus. Het enige wat hij hiervoor nodig heeft is de data van de voetbalzender.

Is handel in data nog mogelijk onder de AVG?

Aan het verkopen van data aan derde partijen zijn middels de AVG regels gebonden. Allereerst moet u de data op een rechtmatige wijze verkrijgen. Dat houdt in dat er een grond moet zijn om de data te verzamelen en vervolgens te verhandelen. Voor de doorgifte van data aan derde partijen zal dit de welbekende toestemmingsgrond zijn. De betrokkene, degene over wie de data gaat, moet toestemming gegeven hebben aan de partij die de data verzamelt, voor het verkopen van de data aan een derde partij. Daarnaast moet de betrokkene toestemming hebben gegeven voor het gebruik van de verkochte data door deze derde partij. De betrokkene moet dus bij het verstrekken van zijn data al weten wie de derde partij is die de data gaat kopen en wat hij met de data gaat doen. Die zogeheten voorafgaande geïnformeerde toestemming is een groot struikelblok bij het verhandelen van data. De verkoper van data weet doorgaans niet wat zijn koper met de data gaat doen. De koper weet dat mogelijk zelf nog niet eens.

Inzetten van data voor direct marketing

Het doel van het verkrijgen en verhandelen van data is vaak het gebruik voor direct marketing, oftewel: reclame

maken voor een product of dienst. Direct marketing kan op allerlei verschillende manieren plaatsvinden. Veel gebruikte manieren zijn telemarketing (het telefonisch benaderen van potentiële klanten om een product of dienst aan te prijzen), e-marketing (het benaderen van potentiële klanten via een elektronisch bericht, zoals een e-mail of app, met daarin een mooi aanbod) en reclamepost.

Zodra is vastgesteld dat de persoonsgegevens rechtmatig zijn verkregen, door middel van de hierboven beschreven procedure met toestemming of via de klantrelatie onder bijvoorbeeld uitvoering van de overeenkomst, kan worden nagegaan of de gegevens voor direct marketingdoeleinden ingezet mogen worden. Hiervoor gelden niet alleen de regels uit de AVG, maar ook uit de Telecommunicatiewet. Voor telemarketing, e-marketing en marketing via reclamepost gelden verschillende regels.

Telemarketing

De Telecommunicatiewet gaat ervan uit dat u iedereen in uw (rechtmatig verkregen) CRM-bestand telefonisch mag benaderen, tenzij deze persoon zich heeft aangemeld bij het Bel-me-niet Register. Hierbij geldt overigens wel een uitzondering voor het bellen van betalende klanten. Uw klanten mag u, ondanks dat zij in het Bel-me-niet Register staan, bellen over soortgelijke producten of diensten, die lijken op of goed aansluiten bij hetgeen door de klant in de afgelopen periode (bijvoorbeeld de afgelopen twee jaar) bij u is aangekocht.

E-marketing

Voor e-marketing gelden ook regels uit de Telecommunicatiewet, maar dit zijn andere regels dan voor telemarketing. Deze regels uit de Telecommunicatiewet

hebben betrekking op ongevraagde elektronische berichten (zoals e-mail en sms) met commerciële inhoud, die via een automatisch oproep- of communicatiesysteem worden verzonden.

Waar je bij telemarketing je CRM-systeem kan gebruiken zolang geen van je klanten verzet heeft geboden, geldt voor het versturen van een commercieel elektronisch bericht, bijvoorbeeld een digitale nieuwsbrief, dat in de meeste gevallen voorafgaande uitdrukkelijke toestemming nodig is van de ontvanger. De toestemming moet vrij, specifiek, geïnformeerd en ondubbelzinnig zijn. Een simpel 'ik ontvang graag de nieuwsbrief' is onvoldoende. In enkele gevallen kan echter ook gewerkt worden met een zogenaamde opt-out. Die opt-out mogelijkheid is aan voorwaarden gebonden en moet worden geboden op het moment dat u de gegevens van de betrokkene verkrijgt. Voor e-marketing bestaat dus geen algemeen opt-out register.

Reclamepost

Net als bij telemarketing, is het voor het verzenden van reclamepost belangrijk om de regels uit de AVG te volgen. De Telecommunicatiewet is op het verspreiden van reclame via post niet van toepassing. Er geldt een minder streng regime voor het verzenden van reclamepost, dan voor telemarketing en e-marketing. Toestemming is geen vereiste. Het telkens vermelden van het register waarin een ontvanger zich kan aanmelden om zich te verzetten tegen reclame, hoeft niet.

Wel is vereist dat de verzender van de reclamepost een wettelijke grondslag heeft. Een wettelijke grondslag kan toestemming zijn, maar kan ook het gerechtvaardigd belang zijn of de uitvoering van de overeenkomst. De AP stelt dat toestemming nodig is voor het verzenden van reclamepost aan niet-klanten. Maar, net als voor bestaande klanten, kan de grondslag voor niet-klanten ook zeker het gerechtvaardigd belang zijn. Volgens de AVG is een direct marketingbelang namelijk een gerechtvaardigd belang, mits de privacy-afweging in het voordeel van het direct marketingbelang uitvalt. Daarvoor is onder andere belangrijk dat het direct marketingbelang goed wordt onderbouwd, de ontvanger het gebruik van persoonsgegevens voor reclamepost had kunnen verwachten en er geen ander minder ingrijpend middel mogelijk is om het direct marketingdoel te behalen.

Reclamepost: zelf vergaarde gegevens van klanten

Voor klanten kan volgens verschillende partijen, waaronder de AP, ook nog sprake zijn van het feit dat verzenden van reclamepost voldoende verband houdt met het doel waarvoor de adresgegevens van de klant zijn verzameld. Wanneer je via de webshop een bestelling hebt ontvangen en afgewikkeld, heb je de persoons-

gegevens rechtmatig verkregen voor het uitvoeren van de overeenkomst. Als je de klant vervolgens reclame wilt sturen over soortgelijke producten of diensten, dan is dit volgens de AP onder voorwaarden verenigbaar met het doel waarvoor je de persoonsgegevens in eerste instantie had verzameld: de uitvoering van de overeenkomst. Je mag dan onder doelbinding de reclamepost, zonder afweging van het gerechtvaardigd belang en zonder toestemming, versturen aan de klant. De meningen zijn hierover echter verdeeld. Het is namelijk moeilijk vast te stellen in welke gevallen de reclame voldoende verband houdt met het doel waarvoor de gegevens in eerste instantie zijn verzameld.

Wat te doen bij 'verzet'?

Bellen, berichten sturen, of reclame per post toesturen aan zowel klanten als niet-klanten mag uiteraard niet als de ontvanger heeft aangegeven dit niet te willen. Wanneer persoonsgegevens voor direct marketingdoeleinden worden gebruikt, heeft de ontvanger altijd de mogelijkheid om bezwaar aan te tekenen tegen dit gebruik. Dit wordt ook wel 'verzet' genoemd. Je moet de ontvanger altijd de gelegenheid bieden om verzet aan te tekenen en de ontvanger ook op de hoogte brengen van het feit dat dit kan, gescheiden van alle andere informatie. Telefonisch betekent dit de gelegenheid geven om aan te melden bij het Bel-me-niet Register, bij elektronische berichten moet een ontvanger zich op een gemakkelijke wijze kunnen afmelden en bij reclamepost wordt de ontvanger uit de adressenlijst verwijderd als hij daarom verzoekt. Vanuit zelfregulering zijn in de Nederlandse Reclame Code ook regels opgenomen over het gebruik van een register voor reclamepost: het Postfilter, en het gebruik van Ja-Nee en Nee-Nee stickers. Het is zaak voor de gebruiker van persoonsgegevens voor direct marketingdoeleinden om de registers te raadplegen, en gemaakte bezwaren te respecteren.

E-Privacyverordening komt eraan

Het is nog maar de vraag of bovengenoemde regels blijven bestaan. Al lange tijd wordt in Europa gesteggeld over de inhoud van de e-Privacyverordening. De e-Privacyverordening regelt onder andere zaken ten aanzien van e-marketing, over cookies en over telemarketing. Het is heel goed mogelijk dat de hierboven beschreven regels in de toekomst gaan veranderen. Een van de voorspelde veranderingen is het regime voor telemarketing. De Staatssecretaris van Economische Zaken heeft bekendgemaakt dat zij zich zal inzetten voor een gelijktrekking van de regels voor offline en e-marketing. Ook voor e-marketing is het mogelijk dat de spelregels gaan veranderen. De definitieve tekst van de e-Privacyverordening is er echter nog niet. Het kan dus allemaal nog anders uitpakken.



Arend Jan Wiersma
Juridisch adviseur

Cloud

Privacy

Coinrecht – Jaaroverzicht 2018

Het afgelopen jaar was voor crypto een jaar van bezinning. Na het vierde kwartaal van 2017 is de manie afgezwakt en is het sentiment teruggekeerd naar een niveau dat ruimte biedt voor reflectie. Dit betekent niet dat er in het afgelopen jaar niks is gebeurd. In tegendeel. Deze perioden waarin de prijs niet dagelijks op de voorgrond staat, zijn juist productieve tijden in de cryptowereld. Daarom gebruiken we dit stuk om terug te kijken op 2018 en tevens een blik vooruit te werpen.

“

*“Bitcoin is not currency;
it’s the internet of money!”*

– Andreas Antonopoulos

Wetgeving

Veel van onze financieel rechtelijke wetgeving is afkomstig uit Europa. Het is daarom niet verwonderlijk dat de eerste wetgeving die specifiek betrekking heeft op crypto, op Europees niveau is vormgegeven. Het resultaat, de vijfde anti-witwas richtlijn (5AMLD), erkent het bestaan van cryptogeld en integreert deze onder de noemer *Virtuele Valuta*.

Voordat de 5AMLD praktische gevolgen gaat hebben, dient deze eerst te worden omgezet in Nederlands recht. Dit proces dient begin 2020 te zijn voltooid. In grote lijnen worden crypto-partijen na de inwerkingtreding onderworpen aan gelijke verplichtingen als de traditionele varianten van deze dienstverleners.

“De lidstaten waarborgen dat aanbieders van diensten voor het wisselen tussen virtuele valuta en fiduciaire valuta en aanbieders van bewaarportemonnees worden geregistreerd, dat wisselkantoren en kantoren voor het omwisselen van cheques, en aanbieders van trustdiensten of vennootschappelijke diensten over een vergunning beschikken of geregistreerd zijn, en dat aanbieders van kansspeldiensten worden gereguleerd.” (wijziging 29 5AMLD)

Naast de registratie/vergunning betekent dit dat crypto-partijen nieuwe processen zullen moeten gaan inrichten. Het gaat om: interne gedragslijnen, controlemaatregelen en procedures, daaronder begrepen model-risico-

beheerpraktijken, cliëntenonderzoek, rapportage, bewaring van bewijsstukken, interne controle, nalevingsbeheer en doorlichting van medewerkers. Hoewel enige regulering op zijn plaats is, bevat de richtlijn tevens enkele ambities die doen denken aan Orwell’s 1984:

“Om de aan de anonimiteit verbonden risico’s te bestrijden, moeten nationale financiële inlichtingeneenheden (FIE’s) in staat zijn informatie te verkrijgen waarmee ze virtuelevaluta-adressen kunnen koppelen aan de identiteit van de eigenaar van de virtuele valuta. Bovendien zou de mogelijkheid om gebruikers in staat te stellen zich op vrijwillige basis zelf bekend te maken aan aangewezen autoriteiten, verder moeten worden onderzocht.” (overweging 9 5AMLD)

Dergelijke verplichtingen zijn vooralsnog niet opgenomen, maar worden voor nadere uitwerking in 2022 neergelegd bij de Europese Commissie. Gezien het tempo waarin crypto zich ontwikkelt, vraag ik me af of een dergelijk register er ooit gaat komen. Zoals we al jaren zien, loopt technologie mijlenver vooruit op wetgeving. Enkele aanpassingen in de source-code kunnen dergelijke plannen immers snel onmogelijk maken.

Gevolgen van wetgeving

De aankomende wetgeving betekent dat wetgevers gaan proberen om pseudonieme en anonieme systemen toch inzichtelijk te maken. Dit betekent dat iedereen die virtuele valuta gaat gebruiken zal worden geïdentificeerd, geclassificeerd en geregistreerd. Dit is beter bekend als know your customer (KYC) en anti-money laundering (AML) beleid en is al geruime tijd onderdeel van onze financiële wetgeving. Echter, traditionele valuta verschilt op belangrijke punten van virtuele valuta.



Traditionele valuta vs. virtuele valuta

Het is met name belangrijk om in te zien dat de eigenschappen van virtuele valuta het resultaat zijn van software in plaats van beleid van een centrale bank. Dit betekent dat eigenschappen als uitgifte, inflatie en privacy aangepast kunnen worden of in nieuwe softwarelagen kunnen worden geïmplementeerd naarmate hier noodzaak voor is. Dergelijke wijzigingen zijn overigens niet eenvoudig om door te voeren. Met name in het geval van Bitcoin zal er een brede consensus nodig zijn.

Wanneer wetgevers (in Europa en daarbuiten) inzetten op vergaande inperking van financiële vrijheden door identificatie, classificatie en registratie, hebben de verschillende valuta, anders dan traditionele valuta, de mogelijkheid om de software hierop aan te passen. Dit kan betekenen dat nieuwe privacy-features aan een virtuele valuta kunnen worden toegevoegd waardoor de link tussen de virtuele valuta en het individu niet langer betrouwbaar is vast te stellen. Deze technieken bestaan al maar zijn, vanwege het ontbreken van een directe noodzaak, momenteel nog niet geactiveerd.

De hoop is dat wetgevers inzien dat ingrijpende regulering kan leiden tot meer geharde virtuele valuta die daardoor minder vatbaar zijn voor die regulering.

Een analogie met het internet is op zijn plaats: iedereen die het internet gebruikt, doet dit met een IP-adres. In de vroege tijden van het internet wist men niet wie achter welk IP-adres zit. Tegenwoordig bestaan er real-time registers waarin IP-adressen aan individuen worden gekoppeld. Deze zijn op ieder moment te bevragen door verschillende (opsporings)instanties. Dit heeft gevolgen gehad voor de vrijheid van meningsuiting en informatievergaring. Omdat het internet voor een groot deel functioneert aan de hand van software, is er een tegenbeweging ontstaan die deze afbreuk aan privacy wil corrigeren. Het is hierom dat er nieuwe diensten ontstaan zoals virtual private networks (VPN) en the onion router (TOR), die het individu meer privacy geven door het gebruik van encryptie en software. De verwachting is dat dit ook zal gebeuren met crypto wanneer regulering en privacy op gespannen voet komen te staan.

Is KYC/AML doeltreffend?

Privacy is belangrijk, maar we ontkomen niet aan de mogelijke nadelen van virtuele valuta. Snelle, pseudo- of anonieme en grensoverschrijdende transacties zijn nou eenmaal aantrekkelijk voor criminelen. Maar is het identificeren, classificeren en registreren aan de poort wel doeltreffend?

Het virtuele valuta equivalent van IBAN-nummers zijn (hashes van) publieke sleutels. Anders dan IBAN-nummers, kunnen virtuele valuta adressen gratis en onbeperkt worden gegenereerd door iedere gebruiker. Dit betekent dat, in theorie, iedere gebruiker voor iedere transactie een nieuw rekeningnummer/adres kan gebruiken. Wanneer de controle aan de poort plaatsvindt bij de conversie van euro naar virtuele valuta, is dit het laatste moment waarop de virtuele valuta met enige zekerheid kan worden gevolgd. Wat gebeurt er bijvoorbeeld als de geïdentificeerde persoon A bitcoin koopt en dit doorverkoopt aan persoon B. Moet persoon A dan ook persoon B identificeren en rapporteren? En wat als persoon B de bitcoin aanwendt voor criminele doeleinden. Komt dit voor rekening van persoon A aangezien alleen deze is geïdentificeerd? Persoon A kan ook zijn eigen bitcoin naar een ander eigen adres sturen en dit 10 keer herhalen. De oorspronkelijke identificatie aan de poort heeft al snel zijn waarde verloren en de bitcoin is niet meer (betrouwbaar) te koppelen. Hoewel de maatregelen in de 5AMLD een logisch verlengstuk zijn van de eerder ingeslagen weg en gekozen methoden, is dit waarschijnlijk niet het geschikte middel om criminaliteit tegen te gaan waar het gaat om virtuele valuta.

Virtuele valuta vooralsnog ongrijpbaar

De in dit stuk beschreven wetgeving lijkt crypto te behandelen als een digitaal/virtueel equivalent van reeds gedefinieerde wettelijke figuren. Dit is niet per se de juiste aanpak. Vanwege de korte bestaansgeschiedenis van deze technologie weten we simpelweg nog niet welke rol het op het internet en in de maatschappij gaat vervullen.

Iedereen benadert virtuele valuta vanuit zijn eigen wereldbeeld. Voor sommigen is het een nieuw systeem om de dagelijkse boodschappen mee af te kunnen rekenen (betaalmiddel). Voor anderen is het een veilige haven voor vermogen die niet samenhangt met de prestaties van de traditionele economie (waarde opslag). Voor weer anderen is het een manier om vertrouwen opnieuw vorm te geven op een globale schaal.

Afgezien van het uiteindelijke nut, is het afgelopen jaar een goede periode geweest om de daadwerkelijke intenties van de geïnteresseerden te ontdekken. De opgedreven prijs uit het laatste kwartaal van 2017 werd gedomineerd door speculanten. De groep die na het inzakken door is blijven werken begrijpt wat er op het spel staat. Wat betreft wetgeving zullen we in Nederland nog even geduld moeten hebben en de praktische uitwerking hiervan is nog onzeker. De doorontwikkeling en adoptie van crypto is daarentegen niet onzeker. Dit zal onverminderd doorgaan en we zijn ontzettend benieuwd naar alles wat 2019 ons gaat brengen!

Welkom bij de financiële revolutie (de waarde van één Bitcoin (BTC) is op dit moment - december 2018 - € 3729).





Esther Flierman
Juridisch adviseur
ICTRecht Groningen

Contracteren

Overheid

E-commerce

Recht uit de praktijk: conflictoplossing

Regelmatig worden wij benaderd door ondernemers die in een conflict zijn geraakt met een leverancier of een partner. Gezamenlijk wordt in goed vertrouwen een IT-project ontwikkeld. Ergens in het proces ontstaat een kink in de kabel en raken partijen gefrustreerd. Hoe dan verder?

Ook worden wij vaak benaderd inzake schending intellectueel eigendomsrechten (IE-rechten). Op internet wordt veel gedeeld en gekopieerd, zoals teksten en foto's. Dit gebeurt vaak zonder toestemming. Velen zijn zich niet bewust van de risico's hiervan. Als men door een advocaat wordt aangeschreven op schending IE-rechten dan gaat dit meestal gepaard met een zeer hoge vordering tot schadevergoeding. Dergelijke sommaties veroorzaken paniek en onrust. Wat kunt u in zo'n geval doen? En andersom, als uw IE-rechten of andere afspraken worden geschonden, wilt u uiteraard hiertegen opkomen. Waar begint u?

Het is raadzaam in bovengenoemde zaken snel deskundig advies in te winnen. Wij bieden voor genoemde zaken rechtshulp, begeleiding en bemiddeling. Hoe dat in zijn werk gaat wordt hieronder besproken met enkele voorbeelden uit onze praktijk.

Conflict

Conflicten hebben een grote impact, ze zijn immers per definitie negatief beladen en houden u af van waarmee u wel bezig wilt zijn: ondernemen!

Als u een conflict aan ons voorlegt, zullen wij de zaak met u bespreken en beoordelen welke mogelijkheden er zijn. Daarna wordt de strategie uiteengezet. Meestal vangt de zaak aan met het verzenden van een gemotiveerde brief, waarin ofwel uw eisen worden uiteengezet ofwel uw verweer. Op basis van de briefwisseling komt er beweging in de zaak. Meestal volgen er onderhandelingen. Ook kan er een bemiddelingstraject of mediation volgen. In het uiterste geval kan er geprocedeerd worden. De ervaring is evenwel dat de meeste zaken buiten de rechtbank worden opgelost.

Een voorbeeld uit onze praktijk

Een webshopleverancier neemt de volledige ontwikkeling en beheer van een webshop ter hand voor een grote winkelier. De webshop wordt in 3 fases opgeleverd conform een uitgebreid plan van aanpak, met de bedoeling van partijen daarna een langdurige samenwerking aan te gaan in abonnementsvorm. In de ontwikkelings- en testfase verzoekt de afnemer om aanvullende functionaliteiten, die buiten de offerte vallen. Uiteraard was de leverancier bereid een en ander aan te vullen en te wijzigen, voorzover mogelijk. Hierdoor liep het traject evenwel vertraging op en werd niet binnen de overeengekomen termijn opgeleverd. De webshop gaat op enig moment live en werkt naar behoren. De afnemer is evenwel van mening dat de webshop niet voldoet aan zijn verwachtingen en dat hij schade had geleden omdat de webshop te laat was opgeleverd. Hij meende de laatste termijn niet te hoeven betalen. Daarnaast stopte hij ook met het betalen van de maandelijkse abonnementskosten en de jaarlijkse licentiekosten. De afnemer werd in gebreke gesteld, maar bleef zijn standpunt handhaven, wel betaalde hij voortaan de abonnementskosten en de licentiekosten. Hiermee was het stopzetten van de dienstverlening een groot risico. De webshop draaide goed en de maandelijkse omzet was een veelvoud van de openstaande factuur. De afnemer breidde zijn klachtenzang wekelijks uit en legde op alle slakken zout.

Van de relatie tussen deze partijen was weinig over, eigenlijk wilde de partijen niet met elkaar verder. De webshop-eigenaar wilde wel het ontwerp van de website behouden en dit overdragen tot verdere ontwikkeling aan een derde. De leverancier wilde uiteraard wel dat zijn openstaande facturen en extra geleverde werkzaamheden (support) zouden worden betaald. Geen van beide was

genegen iets toe te geven aan de ander. De kosten voor een procedure waren twee keer zo hoog als de openstaande eindtermijn. Dit was voor beide partijen een doorn in het oog, zodat zij akkoord gingen met een bemiddelingsgesprek. Hierbij werd afgesproken dat alles wat werd besproken geheim zou blijven. Mochten partijen er niet uitkomen in het gesprek, dan kon hetgeen dat was gedeeld niet tegengeworpen worden in een eventuele procedure. ICTRecht trad op als bemiddelaar/mediator en begeleidde het gesprek. Door verschillende scenario's te bespreken en door te vragen op de belangen van de partijen, zijn de partijen tot een oplossing gekomen. De ene partij ging over tot betaling van de openstaande termijn en de andere partij heeft alle medewerking verleend om de webshop aan een derde over te dragen. Alles is keurig vastgelegd in een vaststellingsovereenkomst en de partijen hebben de zaak daarmee snel kunnen afwikkelen.

Sommatie ontvangen

Sommaties tot staken van bepaalde activiteiten vanwege inbreuk op het gebied van databankrecht, merkenrecht, auteursrecht, handelsnaamrecht of domeinnaam gebruik, komen vaak als donderslag bij heldere hemel. Dergelijke sommaties gaan veelal gepaard met een enorme vordering tot schadevergoeding. De schrik zit er dan goed in. In de meeste gevallen kunnen wij de zorg wegnemen en de sommatie weerspreken danwel hulp en begeleiding bieden in de oplossing van het conflict.

Een voorbeeld uit onze praktijk

Een startende ondernemer in de affiliate marketing-branch probeerde voor opdrachtgevers c.q. publishers

uiteeraard zoveel mogelijk personen op internet te bewegen om op advertenties te klikken en het liefst ook tot het bestellen van het product over te gaan. Om het zichzelf enigszins makkelijk te maken had hij soortgelijke advertenties van een grote partij, werkzaam in dezelfde branche, gekopieerd en op zijn eigen relatief onbekende website geplaatst. Hij meende dat publicaties op internet wel gekopieerd en gedeeld mochten worden.

In paniek belde hij ICTRecht. Hij had een brief ontvangen, waarin hij gesommeerd werd per direct de advertenties te verwijderen en zijn inbreukmakende activiteiten te staken en gestaakt te houden. Ook werd er een schadevergoeding van van € 150.000 gevorderd, te voldoen binnen drie werkdagen na ontvangst van de brief. In ons telefoongesprek konden wij direct zijn zorgen wegnemen, al was het wel op zijn minst onhandig wat hij had gedaan. Dat er van een inbreuk op auteursrecht sprake was, was helder. De schadevergoeding die werd gevorderd was evenwel buitenproportioneel. De klant heeft direct zijn website offline gehaald en alle gekopieerde advertenties verwijderd. Wij hebben een uitgebreid gemotiveerd verweer opgesteld met verwijzing naar een recente rechtspraak, op basis waarvan ook de tegenpartij wel tot de conclusie moest komen dat de schadevergoeding buitenproportioneel was. Dat werkte. De zaak was binnen twee weken opgelost en er is uiteindelijk nog geen 10% van de gevorderde schadevergoeding betaald aan de tegenpartij. Voor onze klant voelde het als leergeld. Hij was zeer tevreden over de uitkomst.





**Een dreigend conflict met uw klant of leverancier?
Een meningsverschil over de dienstverlening of
een contract wat dreigt te escaleren? Moeite
met het betaald krijgen van facturen? Snel een
juridische beoordeling, een verweer tegen een
claim of een goed gemotiveerde sommatie nodig?
Dit kan met de conflictoplossing en rechtshulp
van ICTRecht.**

ICTRecht kan uw organisatie ontlasten in conflictsituaties en biedt deskundige rechtshulp door ervaren juridische adviseurs.

De voordelen van conflictoplossing en rechtshulp door ICTRecht:

-  Direct deskundige ondersteuning
-  Creatieve oplossingen voor uw conflict
-  Betrouwbaar door onze ervaren adviseurs

Meer weten of direct een geschil voorleggen
in een vrijblijvend gesprek?

Neem contact op met **Esther Flierman** via
050 209 3499 of e.flierman@ictrecht.nl



Esther Flierman
Juridisch adviseur
ICTRecht Groningen



Samantha van de Stouwe
Juridisch adviseur
ICTRecht Groningen

Contracteren

Innovatie

Blockchain en recht: nieuwe vraagstukken voor juristen

Voor velen is blockchain bekend van de cryptocurrency bitcoin, maar de blockchain kan voor veel meer doeleinden gebruikt worden dan enkel voor het overdragen van bitcoins. Verschillende (internationale) bedrijven en overheden maken al gebruik van de blockchain om bijvoorbeeld internationale contracten bij te houden en auto's te registreren om fraude tegen te gaan. De blockchain technologie belooft te zorgen voor onder meer transparantie en betrouwbaarheid, maar zorgt ook voor vragen op juridisch gebied. Hoe sterk sta je in je schoenen als je afgesproken hebt om te betalen met cryptocurrencies en de ander komt deze afspraak niet na? En kunnen smart contracts in een blockchain gebruikt worden voor juridische contracten? Dit zijn zomaar wat vragen die juristen zichzelf stellen en gevolgen kunnen hebben voor de praktijk. In dit artikel behandel ik deze vragen in het kort.

Wat is de blockchain?

Blockchain kan je het beste vergelijken met grootboeken waarin lijsten van gegevensmutaties worden bijgehouden. Denk bijvoorbeeld aan de grote hoeveelheden databases die in de praktijk gebruikt worden en fungeren als grootboeken. Deze grootboeken zijn echter vaak in handen van één centrale organisatie en voor het gebruik/wijzigen hiervan is toestemming nodig van deze organisatie. Men moet erop vertrouwen dat deze beheerders correct met deze grootboeken omgaan.

De blockchain kan juist hier zorgen voor een uitkomst. De blockchain is een onveranderbaar, openbaar, en nog belangrijker: decentraal grootboek. Er is dus niet één beheerder of centrale organisatie, maar alle deelnemers aan de blockchain verdelen het 'eigendom' samen. Deze deelnemers, 'nodes' genoemd, hebben identieke kopieën van de blockchain opgeslagen op hun computers. De transacties van deze blockchain zijn voor iedere deelnemer aan de blockchain, waar hij of zij zich ter wereld ook bevindt, toegankelijk. Aan de blockchain kunnen enkel transacties worden toegevoegd.

Ze kunnen dus niet verwijderd of aangepast worden.

Toevoegingen worden pas daadwerkelijk doorgezet als bijvoorbeeld de deelnemers, kort gezegd, hiermee akkoord gaan. Hoe de toevoeging precies doorgezet wordt, hangt af van het consensusmechanisme dat bij elke blockchain kan verschillen.

Cryptocurrencies $\neq$ geld?

In Nederland zijn steeds meer mogelijkheden om te betalen met cryptocurrencies, met dank aan de blockchain. Met name het betalen met bitcoin wordt steeds meer geaccepteerd. Zo bieden verschillende online winkels en bezorgservices de mogelijkheid aan om te betalen met bitcoin, kan je in een toenemend aantal winkels met bitcoin betalen en vind je op steeds meer plekken in Nederland crypto-automaten. Een voorbeeld hiervan is Schiphol waar onlangs in één van de aankomsthallen een crypto-automaat is geplaatst waar je, je euro's kan omwisselen naar bitcoin of ethereum. Hoewel cryptocurrencies dus steeds meer als betaalmiddel geaccepteerd worden, is het de vraag of ze juridisch gezien als geld gezien kunnen worden.



Om te bepalen of cryptocurrencies als geld gekwalificeerd kunnen worden, moeten we eerst kijken naar wat de betekenis is van geld. In Nederland kennen we vier definities van geld: chartaal, elektronisch, gangbaar en giraal geld. Het chartale geld is niet zozeer gedefinieerd in de wet zelf, maar staat bekend als het tastbare geld, oftewel de euromunten en het briefgeld in je portemonnee.¹ Het begrip giraal geld is eveneens niet opgenomen in de wet, maar wordt gezien als een vorderingsrecht van de rekeninghouders op hun bank bij een positief banksaldo. Het elektronische geld is daarentegen wel gedefinieerd: het gaat om geldswaarde die elektronisch of magnetisch is opgeslagen en een vordering op de uitgever vertegenwoordigt.² Denk hierbij aan een PayPal rekening of voor de wat ouderen onder ons; de Chipknip. Het begrip gangbaar geld omvat zowel de munten als bankbiljetten in de hoedanigheid van wettig betaalmiddel, maar laat ook de ruimte voor het betalen in fysieke of virtuele geldsoorten die hun bestaan niet aan de Staat ontleenen. Of een betaalmiddel gezien kan worden als gangbaar geld en

een wettig betaalmiddel, wordt bepaald door het recht van het land van de betrokken valuta.³

De rechtbank Overijssel heeft in 2014 uitspraak gedaan over een bitcoin kwestie waar de vraag centraal stond of de bitcoin gezien kan worden als geld.⁴ In deze zaak hadden A en B een overeenkomst gesloten op 8 augustus 2012 voor de koop en verkoop van 2.750 bitcoin. B zou deze verkopen aan A voor € 8,05 per bitcoin. Het ging om een totaalbedrag van € 22.137,50. A heeft deze koopprijs betaald, maar vervolgens heeft B maar 990 bitcoin geleverd. A heeft vervolgens B in gebreke gesteld en uiteindelijk op 25 oktober 2012 de overeenkomst ontbonden voor het gedeelte dat B niet was nagekomen. A vordert onder meer een schadevergoeding van € 132.792,00, omdat A stelt schade te hebben geleden als gevolg van de (flinke!) koersstijging van de bitcoin in de tussentijd. Deze vordering is gebaseerd op wetsartikel 6:125 Burgerlijk Wetboek. Dit artikel geeft de schuldeiser het recht op vergoeding van de schade die hij heeft geleden, doordat na het intreden

1. Van Dale Groot woordenboek van de Nederlandse taal.

2. Artikel 1.1. Wet financieel toezicht

3. T&C Burgerlijk Wetboek

4. Rb Overijssel 14 mei 2014, NL:RBOVE:2014:2667.

van het verzuim van de schuldenaar de koers van het geld dat de schuldenaar had moeten betalen, is gewijzigd.

De rechtbank heeft de verschillende definities van geld vergeleken met bitcoin. Zo concludeert de rechtbank dat het bewaren van bitcoin in wallets op het eerste oog lijkt op een bankrekening, maar deze wallets worden niet beheerd door een derde partij (de giro-instelling), maar door de gebruiker zelf. Er is dus geen sprake van giraal geld. De rechtbank merkt met betrekking tot gangbaar geld op dat de wetgever destijds heeft gekozen voor het begrip gangbaar geld in plaats van het begrip wettig betaalmiddel. Zo heeft de wetgever proberen te vermijden dat onnodig partij gekozen wordt voor de theorie dat geld zijn hoedanigheid enkel aan de Staat kan ontlelen. Er is dus ruimte voor betaling in geldsoorten die hun bestaan niet aan de Staat ontlelen.⁵

Desondanks maakt de rechtbank korte metten met de mogelijkheid bitcoin te beschouwen als gangbaar geld. Hierbij worden kamerstukken aangehaald, waarin is opgenomen dat voor de vraag of sprake is van gangbaar geld, eerst gekeken dient te worden of het een wettig betaalmiddel is. Op grond van de Nederlandse wet is enkel de euro een wettig betaalmiddel in Nederland. Ook benoemt de rechtbank het standpunt van de Minister van Financiën dat bitcoin niet onder de definitie van (elektronisch) geld valt in de zin van de Wet financieel toezicht en eveneens niet als wettig betaalmiddel, maar als een ruilmiddel tussen particulieren kan worden gezien.⁶ De rechtbank vergelijkt verder de handel in bitcoin met de handel in edelmetalen wat ook niet op grond van bovenstaande maatstaven gezien kan worden als gangbaar geld. De conclusie van de rechtbank is dan ook dat bitcoin gezien dient te worden als een ruilmiddel zodat de vordering van A werd afgewezen. Dit vonnis is vervolgens in hoger beroep door het gerechtshof Arnhem-Leeuwarden bekrachtigd.⁷

Hoewel ik het ermee eens ben dat de wet geen ruimte laat voor het kwalificeren van de bitcoin als giraal of elektronisch betaalmiddel vanwege het ontbreken van een centrale instelling zoals een bank, vind ik de argumentatie dat er geen sprake is van een gangbaar geld te kort door de bocht. De rechtbank maakt gebruik van

een cirkelredenering. Er wordt aangegeven dat gangbaar geld ruimte laat voor andere vormen van geld en daardoor niet gekwalificeerd dient te worden als wettig betaalmiddel, maar vervolgens wordt gezegd dat het geen gangbaar geld is, omdat het geen wettig betaalmiddel is. Zoals eerder is aangegeven worden bitcoins net als onze euro gebruikt om betalingen te verrichten (zowel online als in winkels) - al is het nog in mindere mate dan de euro. Maar waarom maakt dat het niet gangbaar? Interessant is dat het Hof van Justitie van de Europese Unie de bitcoin in 2015 wel gelijk heeft gesteld aan traditionele valuta met betrekking tot de btw-richtlijn.⁸ We zullen nog wel moeten afwachten of (bepaalde) cryptocurrencies in de toekomst door jurisprudentie of de wet ook als gangbaar geld worden aangewezen. Let in de tussentijd dus goed op of de tegenpartij bij transacties met cryptocurrencies betrouwbaar is.

Smart contracts

Om geldtransacties of bijvoorbeeld contracten op de blockchain uit te kunnen voeren zijn smart contracts nodig. Smart contracts zijn niet tegelijkertijd met de blockchain ontstaan. In de jaren 90 werd door Nick Szabo (een van de mensen die ervan wordt verdacht om Satoshi Nakamoto, de grondlegger van de bitcoin te zijn) al geschreven over de uitvoering van een smart contract.

Een smart contract is niet meer dan programmeercode dat is opgenomen in een blockchain en hier wordt uitgevoerd. In een smart contract zijn rechten/verplichtingen opgenomen die aan voorwaarden gekoppeld worden. Zodra deze voorwaarden (zoals een termijn die is verstreken) vervuld worden, zullen de rechten/verplichtingen automatisch door het smart contract worden uitgevoerd. Smart contracts zijn opgenomen op blockchains en hiermee transparant. Je kan als partij de code van het contract altijd controleren. Bovendien biedt een smart contract zekerheid. De blockchain met haar nodes zorgt ervoor dat de uitkomst voortdurend wordt bevestigd. Bij papieren contracten kunnen partijen, wat hen volgens het contract is opgedragen, nalaten. Dit is niet mogelijk bij een smart contract, wat een groot voordeel is.

5. Rb Overijssel 14 mei 2014, NL:RBO-VE:2014:2667, r.o. 4.8.

6. Zie Brief Minister van Financiën van 19 december 2013 aan de Voorzitter van de Tweede Kamer der Staten Generaal, FM/2013/1939 U.

7. Hof Arnhem-Leeuwarden 31 mei 2016, ECLI:NL:GHARL:2016:4219.

8. Hof van Justitie van de Europese Unie 22 oktober 2015, C-264/14 (Hedqvist).



Sari Jansen
Juridisch adviseur

Privacy

Overheid

Cloud

ICT en zorg: vragen uit de praktijk

Personen die werkzaam zijn in de zorg krijgen te maken met een grote verscheidenheid aan wet- en regelgeving, gedragscodes en richtlijnen. De hoeveelheid aan documenten is enorm en de daarin opgenomen bepalingen zijn vaak aan verandering onderhevig. Dit leidt tot het onoverkomelijke gevolg dat er veel onduidelijkheid bestaat over de interpretatie van de relevante regels en handreikingen. Hoe moet er bijvoorbeeld worden omgegaan met e-mailverkeer in de zorg nu de AVG van toepassing is? In dit artikel worden de drie meestgestelde vragen aan ICTRecht uit het zorgveld behandeld.

Ben ik een zorgaanbieder zoals bedoeld in de wetgeving over het elektronisch uitwisselingssysteem?

Sinds 1 juli 2017 is de nieuwe Wet cliëntenrechten bij elektronische verwerking van gegevens van toepassing. Deze wet regelt de voorwaarden waaronder zorgaanbieders middels een elektronisch uitwisselingssysteem medische gegevens kunnen uitwisselen. Voor opname in het systeem is uitdrukkelijke en per 2020 gespecificeerde toestemming van de patiënt vereist. De wet geeft de patiënt onder andere het recht om zijn dossier elektronisch in te zien en een elektronisch afschrift van het dossier te krijgen. Op welke manier dit gebeurt, is aan de zorgaanbieder. Maar wanneer is men te kwalificeren als een zorgaanbieder zoals bedoeld in deze wet?

Voor de definitie van zorgaanbieder vinden we in verscheidene gezondheidszorgwetten een handreiking. In de relevante wet- en regelgeving wordt het begrip zorgaanbieder, zorgverlener of hulpverlener -afhankelijk van de betreffende wet- gebruikt. Ieder van deze begrippen kent haar eigen definitie. Enige verwarring over de begrippen en de betekenis ervan lijkt daardoor onvermijdelijk. In de Wet cliëntenrechten wordt bijvoorbeeld in de artikelen zelf meestal het begrip “zorgaanbieder” gehanteerd, terwijl in de definitielijst slechts het begrip “zorgverlener” wordt gedefinieerd.¹ Het Besluit elektronische gegevensverwerking door zorgaanbieders, welke ziet op de beveiliging van elektronische uitwisselingssystemen, definieert het begrip zorgaanbieder weer wel. Voor de definitie van zorgaan-

bieder verwijst het Besluit naar een andere wet, namelijk de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.

In deze andere wet staat beschreven wat er onder zorgaanbieder moet worden verstaan, namelijk een natuurlijk persoon (dus niet een rechtspersoon, zoals een bedrijf). Deze natuurlijke persoon moet ingeschreven staan in een register zoals bedoeld in de Wet op de beroepen in de individuele gezondheidszorg. Dit zijn artsen, tandartsen, apothekers, gezondheidszorgpsychologen, psychotherapeuten, fysiotherapeuten, verloskundigen en verpleegkundigen. Als de natuurlijke persoon niet in een register staat, dan moet het gaan om een persoon die een beroep uitoefent waarvan de opleiding bij een algemene maatregel van bestuur wordt geregeld of aangewezen. Dit is dezelfde definitie als de Wet cliëntenrechten hanteert bij het begrip “zorgverlener”.

En waarom is het belangrijk om te weten wie bedoeld wordt? Is er niet aan de voorwaarden uit de definitie voldaan, dan is er dus geen sprake van een zorgverlener of zorgaanbieder zoals bedoeld in de Wet cliënten-

1. Slechts in artikel 15b lid 3 en artikel 15i Wet cliëntenrechten wordt gesproken van “zorgverlener”. In de overige artikelen wordt het begrip “zorgaanbieder” gehanteerd.



rechten. Het gevolg is dat de betreffende partij dan niet aan de vereisten uit deze wet hoeft te voldoen.

Mag ik als zorgaanbieder in de correspondentie met mijn patiënt gebruikmaken van e-mail?

Het gebruik van e-mail in de zorg is een heikel en gevoelig punt, omdat er in het e-mailverkeer tussen zorgaanbieder en patiënt medische gegevens van de patiënt kunnen worden verzonden. Mag een zorgaanbieder gebruik maken van conventionele e-mail in de correspondentie met zijn patiënt?

Het al dan niet gebruiken van conventionele e-mail in de correspondentie tussen zorgaanbieder en patiënt hangt dan af van de inhoud van de e-mail. Bij online gegevensuitwisseling dienen maatregelen getroffen te worden die de privacy van de patiënt en de veiligheid en de betrouwbaarheid van de gegevensuitwisseling waarborgen. Zowel de zorgaanbieder als de patiënt dienen zich te realiseren dat online communicatie vooralsnog niet volledig veilig is. De zorgaanbieder dient de patiënt op grond van zijn zorgplicht hierop te wijzen.²

Wanneer er medische gegevens (gezondheidsgegevens) in de e-mail worden verzonden, dan raden wij het gebruik van conventionele e-mail af. Op grond van de AVG moeten er namelijk passende technische en organisatorische maatregelen zijn getroffen ter

beveiliging van de persoonsgegevens.³ Dat betekent dat de e-mail een hoog niveau van beveiliging moet hebben, als hier medische gegevens in staan. Medische gegevens zijn bijvoorbeeld gegevens die wat zeggen over de ziekte die de patiënt heeft of gegevens die wat zeggen over welke specialist de patiënt behandelt (zoals een neuroloog of psychiater). Bij een onversleutelde e-mail is er dan geen sprake van voldoende beveiliging.

Er zijn zeker wel beveiligde mailsystemen voorhanden waarmee wel “gewoon” gemaild mag worden, ook als er gezondheidsgegevens met de e-mail worden verzonden. Het is dan altijd goed om als klant aan uw leverancier te vragen: “Is uw systeem passend beveiligd voor het verwerken van bijzondere persoonsgegevens?”. De Koninklijke Nederlandsche Maatschappij ter bevordering der Geneeskunst geeft een aantal handvaten. Zo kan er voor versleuteling gebruik worden gemaakt van de in de markt beschikbare ‘secure-email’ oplossingen. Daarnaast adviseert zij onder andere het gebruik van een encrypted server en het gebruik van Virtual Private Networks (VPN).⁴

Wanneer er tussen de zorgverlener en de patiënt gemaild wordt zonder dat er gezondheidsgegevens (of andere bijzondere of gevoelige persoonsgegevens) in de e-mail staan, dan kan conventionele e-mail voldoende zijn. Hier geldt wel, zoals voornoemd, de zorgplicht van de zorgaanbieder om de patiënt te wijzen op de risico's.

2. KNMG Richtlijn online arts-patiënt contact, herziene versie september 2007.

3. Artikel 32 AVG.

4. KNMG Richtlijn online arts-patiënt contact, herziene versie september 2007.

Hoe verhoudt de intrekking van toestemming voor het verwerken van persoonsgegevens tot de bewaarplicht van het medisch dossier?

In de Wet op de geneeskundige behandelingsovereenkomst (WGBO) is bepaald dat zorgaanbieders, in deze wet aangeduid als “hulpverleners”, een medisch dossier moeten inrichten.⁴ In dit dossier moet de hulpverlener onder andere aantekeningen maken omtrent de gegevens van de patiënt en de ten aanzien van de patiënt uitgevoerde verrichtingen. Dat betekent dat een medisch dossier ook persoonsgegevens van de betrokken patiënt bevat. De hulpverlener is op grond van de WGBO verplicht om dit medisch dossier gedurende vijftien jaren te bewaren.⁵ Voor de verwerking (waaronder tevens opslaan wordt verstaan) van de persoonsgegevens in het medisch dossier is een uitzonderingsgrond en grondslag vereist. Het verwerken van medische gegevens is op grond van de AVG namelijk verboden, tenzij er sprake is van een uitzondering op dit verbod.⁶ Daarnaast moet er een verwerkingsgrondslag aanwezig zijn.⁷ In de AVG zijn de uitzonderingsgronden op het verwerkingsverbod en de grondslagen limitatief opgesomd.

Een van de uitzonderingsgronden en grondslagen onder de AVG voor het verwerken van persoons-

gegevens is de uitdrukkelijke toestemming van de betrokkene.⁸ Onder de AVG is de betrokkene gerechtigd om zijn toestemming weer in te trekken. Het gevolg is dat de verwerking van de persoonsgegevens waarvoor toestemming is gegeven, gestaakt dient te worden. Maar hoe verhoudt deze bevoegdheid van de betrokkene zich tot de bewaarplicht van de hulpverlener?

Een veelgemaakte denkfout is dat de uitzonderingsgrond en de grondslag voor het aanleggen van een medisch dossier de *toestemming van de betrokkene* is. Dit is echter niet het geval. Het aanleggen van een medisch dossier en het gedurende vijftien jaar bewaren van het medisch dossier is namelijk een *wettelijke plicht*.⁹ Onder de AVG is het verwerkingsverbod niet van toepassing indien de verwerking noodzakelijk is voor het uitvoeren van een wettelijke plicht.¹⁰ Ook de grondslag voor de verwerking is het voldoen aan deze plicht. Dat betekent dat de hulpverlener géén toestemming hoeft te verkrijgen voor het aanleggen van het medisch dossier en het bewaren daarvan. De patiënt kan dus ook geen toestemming voor het aanleggen en bewaren van een medisch dossier intrekken. Wel kan hij een verzoek tot verwijdering van (specifieke) persoonsgegevens of vernietiging van het medisch dossier indienen.

5. Artikel 7:454 lid 1 WGBO.

6. Deze bewaarplicht kan overigens wel doorbroken worden, indien de betrokken patiënt een verzoek tot vernietiging van het medisch dossier doet.

7. Artikel 9 AVG.

8. Artikel 6 AVG.

9. Artikel 9 lid 2 sub a AVG en artikel 6 lid 1 sub a AVG.

10. Artikel 9 lid 2 sub g AVG en artikel 6 lid 1 sub c AVG.





Raoul van de Laak
Juridisch adviseur

E-commerce

Contracteren

Innovatie

Digitaliseren en elektronische handtekening

Tegenwoordig stappen steeds meer organisaties over op elektronische processen en elektronisch contracteren. Elektronische processen zijn snel en eenvoudig waardoor overeenkomsten direct gesloten kunnen worden. Denk aan het sluiten van een verkoop of het in dienst nemen van een werknemer. Niet langer hoeven documenten eerst geprint, dan ondertekend, gescand en gepost te worden. Toch zijn bedrijven terughoudend met het overstappen op een elektronisch proces. Dit komt met name door de onzekerheid of de overeenkomst wel rechtsgeldig elektronisch gesloten kan worden en of daarmee overtuigend bewijs kan worden geleverd.

Bijna alle overeenkomsten kunnen elektronisch

Het uitgangspunt in het contractenrecht is vormvrijheid. Een overeenkomst kan zowel schriftelijk, mondeling als dus ook elektronisch tot stand komen, zolang er maar sprake is van aanbod en aanvaarding. Voor sommige overeenkomsten eist de wet echter dat deze op schrift moet. Denk aan het kopen van een huis of overdragen van auteursrechten. Maar ook als er een schriftelijkheidsvereiste geldt, kan de overeenkomst meestal elektronisch gesloten worden. De wet vereist dat dan wel aan de volgende voorwaarden voldaan moet zijn:

- De overeenkomst moet raadpleegbaar zijn voor partijen;
- De authenticiteit moet in voldoende mate gewaarborgd zijn;
- Het moment van totstandkoming (aanvaarding aanbod) moet vastliggen;
- De identiteit van partijen kan met voldoende zekerheid worden vastgesteld;
- En indien ondertekening een wettelijke eis is: een betrouwbare elektronische handtekening. Het is wel erg belangrijk om goed te (laten) onderzoeken of er voor een bepaalde overeenkomst specifieke wettelijke bepalingen gelden.

Welke elektronische handtekening?

1. Gewone elektronische handtekening

De gewone elektronische handtekening is de eenvoudigste variant. Denk hierbij aan een gescande handtekening op papier, die bijvoorbeeld onder een e-mail geplakt kan worden als afbeelding. Deze variant wordt meestal niet aangeraden omdat hij eenvoudige vervalsen is. Maar als de betrouwbaarheid voldoende vaststaat (bijvoorbeeld bij e-mail binnen een bedrijf), dan is zo'n handtekening rechtsgeldig.

2. Geavanceerde elektronische handtekening

De geavanceerde elektronische handtekening maakt gebruik van wiskundige technieken om een unieke code aan een bericht te koppelen. Deze code wordt afgeleid uit het bericht zelf en uit de identiteit van de afzender. Daarmee is de code niet te gebruiken bij een vervalst bericht, zodat zo'n geavanceerde elektronische handtekening al snel als betrouwbaar en dus rechtsgeldig wordt gezien. Deze vorm wordt ook wel aangeduid als de "digitale handtekening".

3. Gekwalificeerde elektronische handtekening

De gekwalificeerde elektronische handtekening is de zwaarste variant. Hierbij wordt een geavanceerde elektronische handtekening gecontroleerd met behulp van

een certificaat dat door een erkende certificatiedienstverlener wordt uitgegeven. Erkenning en inschrijving van zulke dienstverleners gebeurt door het Agentschap Telecom.

Rechtsgeldigheid

Europese wetgeving (eIDAS) bepaalt dat het rechtsgevolg van de gekwalificeerde elektronische handtekening gelijk is aan dat van een handgeschreven handtekening. In Nederland hebben de gewone en de geavanceerde elektronische handtekening ook dezelfde rechtsgevolgen als de handgeschreven handtekening mits de gebruikte methode voor ondertekening voldoende betrouwbaar is. Daar is niet één specifiek criterium voor, maar hoe groter het (bewijs)belang van de overeenkomst, hoe zwaarder het betrouwbaarheidsniveau moet zijn.

In Nederland is een ondertekend stuk dat dient als bewijs een “akte” en levert dwingend bewijs op tussen partijen. Dit kan ook gelden voor de elektronische akte. Dwingend bewijs betekent dat een rechter dan gehouden zal zijn uit te gaan van de juistheid van de inhoud van de akte, tenzij de tegenpartij slaagt in het leveren van tegenbewijs.

Digitaliseringstraject en advies elektronische handtekening

ICTRecht adviseert veel organisaties die overstappen op elektronische processen en elektronisch ondertekenen. Bij een dergelijk digitaliseringstraject inventariseren wij eerst alle relevante processen en overeenkomsten binnen een organisatie. In het advies zullen wij per document of proces aangeven of deze handelingen elektronisch plaats kunnen vinden, wat de eventuele juridische voorwaarden zijn (welk type elektronische handtekening is vereist) en hoe dit ingericht kan worden.

Enkele voorbeelden van klanten:

“

Met het advies van ICTRecht konden wij met een gerust hart een keuze maken om over te stappen op digitaal ondertekenen. Wij willen ICTRecht graag bedanken voor de prettige samenwerking!

Rockstart

Rockstart is een startup accelerator, waarbij veel verschillende overeenkomsten worden gesloten met betrekking tot de oprichting en begeleiding van startups (onder andere sponsor-, licentie-, joint-venture-, arbeids- en financieringsovereenkomsten). ICTRecht heeft Rockstart geadviseerd over hoe zij alle overeenkomsten volledig kunnen digitaliseren.

“

ICTRecht geeft helder en praktisch advies. Ze hebben niet alleen goede juridische kennis, maar zeker ook kennis van de techniek en begrijpen dus ook de processen en werkwijzen.

Evidos/ondertekenen.nl

Evidos biedt een dienst aan voor elektronisch ondertekenen (ondertekenen.nl). ICTRecht heeft deze elektronische handtekening beoordeeld en getoetst of deze aan de (juridische) vereisten voldoet.

Uiteraard kan ICTRecht ook adviseren of een bepaald type overeenkomst digitaal gesloten kan worden en welke handtekening hiervoor gebruikt dient te worden. Of beoordelen of een bepaald proces of systeem voor elektronisch contracteren geldig is en op de juiste manier is ingericht. Adviezen worden altijd zoveel mogelijk praktisch ingestoken en waar mogelijk met tips om het proces gebruiksvriendelijk(er) in te richten.





Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Internetrechtspraak

Rechtbank Midden-Nederland 25 juli 2018

(Inzage personeelsdossier)

Bij ziekte van een werknemer ontstaat een geschil over de afwikkeling van de leaseauto, tankpas en dergelijke. Als onderdeel van het geschil vordert de werknemer inzage in zijn personeelsdossier onder de AVG. Weinig verrassend oordeelt de rechtbank dat zo'n dossier onder de AVG valt. Een elektronisch personeelsdossier moet sowieso worden afgegeven, en een papieren dossier zal aan de definitie van 'bestand' voldoen en dus ook moeten worden afgegeven. In casu bevat het dossier uitsluitend een kopie van de arbeidsovereenkomst, deze moet desondanks gewoon worden verstrekt.

<https://bit.ly/2QuvFsL>

Hoge Raad 17 augustus 2018

(Geen black box algoritmes)

Wanneer een door het bestuursorgaan genomen besluit geheel of ten dele het resultaat is van een geautomatiseerd proces - zoals in casu de modelmatige waarde-bepaling in het kader van de uitvoering van de Wet WOZ - en de belanghebbende de juistheid van de bij dat geautomatiseerde proces gemaakte keuzes en van de daarbij gebruikte gegevens en aannames wil controleren en zo nodig gemotiveerd betwisten, moet het bestuursorgaan zorgdragen voor de inzichtelijkheid en controleerbaarheid van die keuzes, aannames en gegevens. Zonder die inzichtelijkheid en controleerbaarheid dreigt een ongelijkwaardige procespositie van partijen te ontstaan. Een belanghebbende kan in geval van besluitvorming op basis van een computerprogramma dat vanuit zijn perspectief is te beschouwen als een zogenoemde "black box" immers niet controleren op basis waarvan tot een bepaald besluit wordt gekomen. Zie de noot op pagina 37.

<https://bit.ly/2Ec2M0S>

Rechtbank Den Haag 31 augustus 2018

(Inzage personeelsdossier)

Een werkgever voert een loonstop door, waar de werknemer het mee oneens is. Als onderdeel van het geschil

vordert de werknemer inzage in zijn personeelsdossier. De werkgever weigert dit onder meer met de opmerking dat de werknemer de gegevens daaruit al heeft. De rechtbank accepteert dit terecht niet: de AVG voorziet niet in de weigeringsgrond dat de betrokkene de gegevens reeds heeft. De werkgever moet de stukken afgeven, op straffe van een dwangsom omdat ze niet bij eerste verzoek reeds zijn verstrekt.

<https://bit.ly/2B4Gs6j>

Gerechtshof Arnhem-Leeuwarden 4 september 2018

(Gebrek RSA tokens)

De Nederlandse politie koopt bij beveiligingsbedrijf RSA een set tokens voor tweefactorauthenticatie. Het bedrijf Motiv levert deze feitelijk, plus voorziet in aanvullende dienstverlening. Op zeker moment blijkt RSA gehackt waardoor de tokens als onveilig worden gezien. De politie verwijt dit Motiv, die als leverancier in hoort te staan voor de veiligheid van de geleverde producten. Het hof wijst dit af. De politie koos zelf de tokens, dus is het moeilijk van Motiv te verlangen dat deze de veiligheid ervan garandeert. Bovendien is de omstandigheid waar de onveiligheid uit volgt, geheel aan RSA toe te schrijven zodat ook dit Motiv moeilijk in de schoenen te schuiven valt. Zoals de politie zelf aangeeft(!), dit is te vergelijken met de koop van een slot dat op zichzelf goed functioneert, maar waarvan derden door een inbraak bij de fabrikant kopieën van de sleutels in handen hebben gekregen. Is dat de fout van de winkel die het slot verkocht?

<https://bit.ly/2A3sr9b>

Gerechtshof Amsterdam 18 september 2018

(Verlenging domeinnaam)

Een bedrijf registreert een domeinnaam. Op zeker moment meldt hij de domeinnaamregistrar dat "ik alle onderstaande domeinnamen wens op te zeggen op het einde van de registratieperiode. Ik wens dus ALLE domeinnamen in mijn account niet te verlengen op de vervaldatum." Het bedrijf laat vervolgens een aantal domeinnamen vervallen nog vóór de betreffende

vervaldata. Het Hof ziet dit als wanprestatie. De brief is duidelijk genoeg dat de klant de domeinnamen wilde behouden maar niet stilzwijgend wilde verlengen. Opzegging had dus pas na de juiste vervaldata mogen gebeuren.

<https://bit.ly/2QLpZh5>

Gerechtshof Arnhem-Leeuwarden 25 september 2018 (Bewijswaardering)

In een geschil rijst de vraag of een e-mailbericht op een zeker tijdstip is verzonden. Een deskundige wordt benoemd, die op basis van *message headers* de conclusie doet dat met 99,9% zekerheid de mail op 1-10-2013 om 19:46:50 is verzonden. Hij noemt daarbij het theoretisch voorbehoud dat de klokken van alle betrokken internet-providers (mailproviders) fout stonden, maar sluit dit uit op basis van zijn deskundigheid. Hierover heeft hij echter geen onderzoek bij de providers gedaan. In hoger beroep wordt dit niet nodig geacht.

<https://bit.ly/2ROIShE>

Gerechtshof Den Haag 25 september 2018 (Phishing)

De verdachte heeft met valse mails de indruk gewekt dat de ontvanger voor overstappen naar het SEPA betaalsysteem en/of overgang naar 4G mobiel internet moest inloggen en betaalgegevens verstrekken. Met valse inlogpagina's werden vervolgens betaalgegevens verkregen die werden gebruikt om bankrekeningen te plunderen. Vanwege de omvang (enkele tienduizenden euro's) wordt een gevangenisstraf van 18 maanden waarvan zeven maanden voorwaardelijk, opgelegd.

<https://bit.ly/2EnLzCE>

Raad van State 26 september 2018 (Online kansspelen)

Bij besluit van 22 december 2014 heeft de Ksa aan appelante een boete opgelegd van € 180.000 voor het zonder vergunning aanbieden van online kansspelen. Appelante beklaagt zich over het feit dat zijn website in het buitenland gevestigd is. De Ksa wijst op betaal-mogelijkheden met iDeal en een Nederlandstalige site. Ook teksten als "Onze spelers komen uit heel Nederland. Dus kom je uit Amsterdam, Groningen, Doetinchem,

Maastricht, Breda of Den Haag, we houden het simpel en duidelijk." Helpen natuurlijk niet. Het boetebesluit blijft in stand.

<https://bit.ly/2QG0yO5>

Rechtbank Limburg 26 september 2018 (Telefonische verkoop domeinnaam)

Vordering uit hoofde van een telefonisch tot stand gekomen overeenkomst met betrekking tot het leveren van een domeinnaam. Gedaagde betwist primair dat een vordering tot stand is gekomen. Dit verweer wordt gepasseerd. Subsidiair voert gedaagde aan dat er sprake is van bedrog en/of dwaling. De kantonrechter verweegt dat het algemeen bekend is dat er veel fraude wordt gepleegd bij telefonisch acquisitie. Er is echter geen sprake van bedrog omdat niet vast staat dat eiseres onjuiste mededelingen heeft gedaan. De vordering wordt echter toch afgewezen, bij gebrek aan een deugdelijke onderbouwing. Eiseres heeft immers niet een transcriptie van het gehele gesprek overgelegd, maar alleen van dat deel van het gesprek waarin de overeenkomst is gesloten.

<https://bit.ly/2PyIqK4>

Rechtbank Rotterdam 27 september 2018 (Bedreiging via WhatsApp)

Verdachte zou de aangeefster hebben bedreigd met een vuurwapen. Een getuige heeft beelden gemaakt en aan de politie overhandigd. Deze laten echter geen daadwerkelijke confrontatie zien en ook geen voorwerp dat wordt gericht op de aangeefster. Dit levert vrijspraak op. Anders ligt dit bij de vele bedreigende en beledigende WhatsApp-berichten die de verdachte verstuurde, waarbij concreet geweld wordt aangezegd. Er volgt twee weken gevangenisstraf en een contact-verbod voor twee jaar.

<https://bit.ly/2G9dszQ>

Rechtbank Noord-Holland 27 september 2018 (ICT-fraude)

De verdachte heeft zich gedurende een reeks van jaren, en vanaf het moment dat hij hoofd ICT werd, in toenemende mate schuldig gemaakt aan grootschalige en langdurige benadeling van zijn werkgever, Stichting OCK het Spalier, door middel van het opmaken van

valse Vobis-facturen. Daarnaast heeft verdachte een grote rol gespeeld bij het valselijk (doen) opmaken van Computerlab-facturen. Verdachte heeft tezamen met een ander of anderen door middel van twee verschillende, deels naast elkaar bestaande, oplichtingsconstructies miljoenen euro's aan OCK het Spalier onttrokken, waardoor OCK het Spalier, een maatschappelijke instelling gespecialiseerd in opvoedhulp en psychische hulp voor kinderen en jongvolwassenen met ontwikkelings-, gedrags- en gezinsproblemen, welke instelling volledig werd gefinancierd met overheidsgeld, fors is gedupeerd.

<https://bit.ly/2B9nkUr>

Rechtbank Noord-Holland 3 oktober 2018

(Particulier onderwijs annuleren)

Gedaagde heeft via internet zich voor een particuliere opleiding ingeschreven. Vervolgens wil zij de startdatum diverse malen verschuiven. Daarna wil zij annuleren, waarop de instelling 25% van de opleidingskosten in rekening brengt. De kantonrechter bepaalt allereerst dat de overeenkomst rechtsgeldig via internet gesloten is, inclusief de algemene voorwaarden. Weliswaar kon de instelling niet bewijzen dat het 'vinkje' is aangevinkt, maar de bevestigingsmail verwijst duidelijk naar de AV. Deze zijn dus bindend. De annuleringsregeling is echter onredelijk bezwarend, omdat ze ingaan tegen art. 7:408 lid 1 en 7:411 BW, met name omdat annuleren ná aanvang van de cursus goedkoper is dan annuleren daarvóór. Wel moet redelijk loon voor administratieve werkzaamheden worden voldaan.

<https://bit.ly/2B8Frpd>

Rechtbank Limburg 8 oktober 2018

(Vaststellingsovereenkomst domeinnamen)

In het verleden hebben twee partijen geschikt omtrent het gebruik van gelijkende handelsnamen, waarbij wordt afgesproken dat ze elk een toevoeging doen om de namen uniek te maken. Nu blijkt dat één van hen een domeinnaam voert zonder de toevoeging. Na feitenonderzoek blijkt dat de naam slechts doorvoert naar de nieuwe naam van gedaagde, en eigenlijk al opgeheven had moeten zijn maar om technische redenen nog niet is. De eis is afgewezen.

<https://bit.ly/2UuXXWe>

Rechtbank Rotterdam 11 oktober 2018

(Gekloonde modems)

Naar aanleiding van informatie van de Canadese politie is op 29 mei 2017 onder de naam 26Cicero een opsporingsonderzoek gestart naar het klonen van modems van Vodafone Ziggo. Daarbij is de verdenking gerezen dat in Nederland in georganiseerd verband op illegale wijze (met gebruikmaking van speciaal daartoe ontwikkelde software) modems van betalende klanten van Ziggo werden uitgelezen en gekloond. Afnemers van deze gekloonde modems zouden zonder betaling gebruik kunnen maken van de internetdiensten van Ziggo. In dit onderzoek zijn drie personen aangehouden, waaronder de verdachte.

<https://bit.ly/2zU5tkJ>

Rechtbank Amsterdam 12 oktober 2018

(Portret van BN'er versus AVG)

In een roddelblad worden foto's van de partner van een bekende Nederlander geplaatst. De foto was gemaakt door een bekende roddelfotograaf, die onder meer aankondigde "Alle verloven zijn ingetrokken en de klike's met kijkgaten zijn de garage uitgereden". De man ziet dit als hinderlijk volgen en een inbreuk op zijn privacy, artikel 8 EVRM. Ook wordt de AVG in stelling gebracht, omdat de foto als (bijzonder) persoonsgegevens aan te duiden is. De rechtbank stelt voorop dat noch onder artikel 8 EVRM, noch onder het portretrecht, noch onder de AVG sprake is van een absoluut verbodsrecht bij een foto als deze, maar dat de grondrechten van vrijheid van meningsuiting en privacy als gelijkwaardige rechten tegenover elkaar moeten worden afgewogen. Het beroep op de AVG wordt afgewezen vanwege artikel 43 Uitvoeringswet (journalistieke exceptie). In het algemeen volgt uit de belangenafweging dat de foto mocht worden gepubliceerd.

<https://bit.ly/2G981RE>

Rechtbank Noord-Holland 15 oktober 2018

(Kansspelbelasting via internet)

De eiser is inwoner van Nederland en heeft vanuit Nederland via een website met een .eu domeinnaam in de maanden maart, april en mei 2016 deelgenomen aan internetpokerspelen. De eiser heeft voor de gewonnen bedragen aangifte gedaan en hij heeft de kansspelbelasting voldaan. Vervolgens maakt hij

bezwaar omdat hij ten onrechte zou zijn belast met kansspelbelasting aangezien de aanbieder van het spel binnen de Europese Unie is gevestigd. Afgaande op HR-arrest ECLI:NL:HR:2018:356 moet worden gekeken waar de organisator van het kansspel daadwerkelijk is gevestigd. Dit dient te worden beoordeeld aan de hand van alle omstandigheden van het geval. Het zijn van aanbieder van het spel is een van de factoren die dient te worden meegewogen bij de beantwoording van de vraag wie houder is van het spel. Het enkel zijn van aanbieder van het spel is echter onvoldoende om ook als houder van het spel te kunnen worden aangemerkt. De omstandigheden afwegend komt men tot de conclusie dat de houder van het spel in de EU was gevestigd.

<https://bit.ly/2B8ANvO>

Rechtbank Zeeland-West-Brabant 17 oktober 2018 (Liefdadigheidsbingo)

Gedaagde is in oktober 2016 op Facebook een crowdfundingactie gestart voor de aanschaf van een rolstoelbus voor zijn gehandicapte zoon. De vrouw van de eiser had daarna op internet aangekondigd een liefdadigheidsbingo voor de zoon te organiseren. Deze is er niet van gekomen, waarna gedaagde op Facebook haar én hem in diverse bewoordingen oplichtster “ik heb bewijzen genoeg” noemde. Dit bericht is verwijderd en de rechtbank veroordeelde gedaagde tot een rectificatie. In november werd aandacht besteed aan het geschil in het tv-programma “Stegeman op de Bres”, wat de eiser onrechtmatig vindt. Door een en ander wordt hij als taxichauffeur geconfronteerd met klanten die hem als ‘die oplichter van zieke kinderen uit Arnemuiden’ herkennen. De rechtbank ziet geen aanleiding voor onrechtmatig handelen.

<https://bit.ly/2rsWGI8>

Hof van Justitie EU 18 oktober 2018 (Aansprakelijkheid verleggen filescharing)

In Duitsland geldt bij geschillen over illegaal downloaden een harde bewijsregel: wanneer een thuisnetwerk toegankelijk is voor derden, kan de eigenaar niet aansprakelijk worden gesteld voor de inbreuk tenzij hij erkent deze zelf gedaan te hebben. Het HvJ acht deze regel in strijd met de belangen van auteursrechtheb-

benden. Enkel opperen dat huisgenoten de inbreuk hadden kunnen plegen, behoort niet genoeg te zijn om aansprakelijkheid te ontlopen.

<https://bit.ly/2rFuFHh>

Gerechtshof Amsterdam 19 oktober 2018

(Shooterspel geen bedreiging)

Verdachte had op internet een schietspel gepubliceerd met daarin personages voorzien van foto's van een derde, waarop geschoten moest worden. De derde deed aangifte van bedreiging. Na cassatie bij de HR oordeelt het Hof nu dat geen sprake is van bedreiging, omdat het spel op een afgeschermd gedeelte van internet beschikbaar werd gesteld aan een aantal 'lotgenoten' van de derde. De bedreiging heeft daarmee deze derde nooit bereikt.

<https://bit.ly/2PsMFOT>

Rechtbank Midden-Nederland 26 oktober 2018

(Domeinnaamhouder onrechtmatig)

Een bedrijf faciliteert het beheer van domeinnamen maar laat de hosting door de klant elders uitvoeren. Een derde is gedupeerd door een publicatie van een klant, en spreekt het domeinnaambedrijf aan. Die weigert, terwijl de publicatie in kwestie zonder twijfel onrechtmatig is. Het domeinnaambedrijf betwist dit ook niet, maar vindt nooit gehouden te zijn tot verwijdering omdat hij niet de publicaties op internet host. De rechter beslist anders. Omdat door het handelen van het domeinnaambedrijf de houder van de website buiten beeld blijft – de registratie was op eigen naam van het bedrijf, en niet op naam van de klant – is daarmee effectief onmogelijk om de publicatie aan te pakken zonder het domeinbedrijf aan te spreken. Hem wordt bevolen de website ontoegankelijk te maken, en het vonnis wordt tevens aangemerkt als een verzoek aan SIDN tot buitengebruikstelling van de website.

<https://bit.ly/2B6aLcN>

Rechtbank Noord-Holland 31 oktober 2018

(Foto broodjeszaak)

In de categorie kleine inbreuk. Een fotograaf maakt en verkoopt culinair getinte foto's, waaronder een foto van

een bord erwtensoep (met rookworst en katenspek). Hij publiceert de foto's zonder duidelijk voorbehoud op internet. Een van deze foto's wordt op internet gevonden door gedaagde, die bij een uitnodiging op Facebook de foto gebruikt ter verfraaiing. De fotograaf spreekt haar hierop aan, waarna hij ontdekt dat ook twee andere foto's worden gebruikt. In totaal eist hij 1.740 euro schadevergoeding en 2.518 euro proceskosten. De rechtbank wijst 1.195 euro schadevergoeding toe en sluit daarbij aan bij de vrijwaringstarieven van Foto Anoniem, onder verwijzing naar de licentiewaarden van vakvereniging DuPho.

<https://bit.ly/2qX01Zz>

Rechtbank Gelderland 6 november 2018

(Reclame voor niet-geneesmiddelen)

Een ondernemer krijgt een boete opgelegd wegens overtredingen van de Geneesmiddelenwet. Hij heeft reclame gemaakt voor de producten Boldocynara forte en Glucosamine + Alchemilla als zijnde geneesmiddelen waarvoor geen handelsvergunning is verleend. Bij het intypen in Google van de zoektermen leveraandoening, leverproblemen, pijn aan de lever en leververvetting verscheen een advertentie van deze ondernemer met een link naar de productpagina's op zijn website. Het verweer luidt dat hij niet actief de producten als geneesmiddel promoot, maar de rechtbank ziet de koppeling tussen zoekwoorden, advertentie en productpagina als genoeg om van promotie van geneesmiddelen te spreken. Het is daarbij niet nodig dat de toezichthouder aantoonde dat een gemiddelde consument de indruk moet krijgen dat het om een geneesmiddel gaat. Iedere consument verdient bescherming tegen reclame maken via internet zoals de eiseres heeft gedaan. Niet bewezen hoeft in dit geval te worden dat bij gemiddelde consumenten daadwerkelijk de indruk is gewekt dat het om een geneesmiddel gaat.

<https://bit.ly/2RJkY5X>

Autoriteit Persoonsgegevens 6 november 2018

(Datalek Uber)

De AP legt een boete van 600.000 euro op aan taxibedrijf Uber vanwege het te laat melden van een datalek bij haar dochter Uber Technologies. In 2016 vond een datalek plaats waarbij gegevens van ongeveer 174.000 Nederlandse klanten en taxichauffeurs werden

buitgemaakt. Uber betaalde de hackers 100.000 'tipgeld' inclusief belofte dit onder de pet te houden, in strijd met de Nederlandse Wet meldplicht datalekken. Onderdeel van het besluit is de aanwijzing van Uber Technologies als verantwoordelijke voor de verwerking, wat opmerkelijk is nu Uber Technologies in principe slechts als hostingpartij optrad. Echter, zij bemoeit zich inhoudelijk met de ontwikkeling van de app, bepaalt zelf het beveiligingsbeleid en heeft zodoende inspraak in doel en middelen.

<https://bit.ly/2DNBmhO>

Rechtbank Midden-Nederland 14 november 2018

(Google-verwijderverzoek)

Eiser ontdekt in Google diverse zoekresultaten gekoppeld aan zijn naam, betreffende een beschuldiging van het valselijk voeren van academische titels. De rechtbank constateert dat het Hof Den Bosch in 2013 heeft geoordeeld dat eiser academische titels had gevoerd die hem niet toekwamen, zodat berichtgeving over het onderwerp in beginsel rechtmatig is. Dat het Hof daarbij een misslag zou hebben begaan omdat kopieën van de diploma's niet werden aangenomen ter griffie, doet daarbij niet ter zake. Mede weegt bij de rechtbank dat eiser als publiek persoon kan worden beschouwd, zodat hij eerder negatieve berichtgeving moet tolereren.

<https://bit.ly/2zNZxtl>

Rechtbank Amsterdam 15 november 2018

(Museumjaarkaart)

De Belastingdienst vordert van de stichting Museumjaarkaart gegevens over het museumbezoek van een van haar kaarthouders, omdat deze wordt verdacht van belastingfraude en er moet worden vastgesteld waar deze woonachtig is. Veelvuldig bezoek aan musea rond een zekere plaats kan worden gebruikt voor dat bewijs. De stichting weigert dit met een beroep op de plicht de privacy van haar klanten te moeten beschermen. Zij ziet het niet als proportioneel en vreest voor een glijdende schaal waarbij de Belastingdienst straks vrijelijk kan neuzen in al haar klantgegevens. De rechtbank gaat daaraan voorbij; het gaat hier om één concreet verzoek met duidelijke aanleiding. De gegevens moeten worden verstrekt.

<https://bit.ly/2zSnAaO>

The future of legal automation

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

Begin vandaag met juridische innovatie!

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

juriblox.nl



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

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



JuriBlox

Documenten op maat

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



JuriBlox

Toegang tot kennisbank

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



JuriBlox

Slimme workflows

Maak gebruik van de workflows om eenvoudig een validatieproces op te zetten en de kwaliteit te bewaken. Hierdoor houdt u grip op de documenten die gemaakt worden door uw collega's. Zo wordt u bijvoorbeeld op de hoogte gebracht wanneer er in een document wordt afgeweken van de standaardtekst.



Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Noot bij Hoge Raad 17 augustus 2018 (Geen black box algoritmes)

De zwarte doos roept steeds meer zorgen op. En dan bedoel ik niet de (overigens feloranje) kast in vliegtuigen waar informatie over crashes te vinden is, maar de zogeheten *black box algorithms* die zonder inzicht in hun werking een uitkomst geven. In het jargon van de ‘meme’ of internetgrap: “Computer says no”. Een zorgelijke ontwikkeling immers als men bedenkt dat steeds meer besluitvorming dankzij dergelijke algoritmes plaatsvindt. Een gebrekkige motivatie zou men bij menselijk genomen besluiten niet accepteren, dus waarom dan wel bij computers?

De term ‘algoritme’ is in dit verband een tikje misleidend. Een algoritme is een eindige reeks instructies die vanuit een gegeven begintoestand naar een beoogd doel leidt. Meestal worden deze instructies door een computer uitgevoerd. In beginsel is er dus niets ondoorzichtigs of mysterieus aan een algoritme. “Ga na of betrokkene de leeftijd van 67 jaar heeft bereikt en zo ja ga over tot AOW-uitkering” is een volkomen transparant algoritme, dat iedere SVB-ambtenaar kan uitvoeren.

De meeste algoritmes zijn echter een stuk complexer, en drijven steeds vaker op zogeheten *machine learning* constructies in plaats van ouderwets ontworpen procedures. Klassieke algoritmes worden opgezet als stappenplannen van bovenaf, en verfijnd of uitgebreid als de regels ingewikkelder worden of uitzonderingen moeten worden ingevoerd. In bovengenoemd voorbeeld zou eigenlijk de deelregel horen “als betrokkene na 31 december 1954 en voor 1 oktober 1955 is geboren, neem dan de leeftijd van 67 jaar en 3 maanden”. Latere wetgeving kan nog meer regels doorvoeren, zoals wat te doen als iemand vele jaren in het buitenland heeft gewoond. Dit alles blijft relatief overzichtelijk.

Machine learning algoritmes werken van onderaf. Zij analyseren bestaande historische gegevens en destilleren daaruit patronen, die vervolgens worden omgezet in regels. Een dergelijk algoritme zou bij-

voorbeeld uitkeringsfraude kunnen detecteren door in uitgavenpatronen van gerechtigden te zoeken naar voor fraude typische handelingen, zoals op onregelmatige momenten grote bedragen ontvangen of vanaf de 15^e van de maand niets meer te pinnen (omdat dan het zwart geld handje contantje wordt ontvangen).

Deze algoritmes zijn dus niet met vooraf opgestelde regels geformuleerd, maar kunnen uitsluitend vaststellen of een nieuwe casus voldoet aan het gedetecteerde patroon. Zo’n patroon is dan niet eenvoudig verklaarbaar, althans niet in een vorm waar mensen genoeg mee nemen. Effectief komt het algoritme niet verder dan “uw gedrag lijkt heel sterk op dat van fraudeurs, dus bent u volgens ons een fraudeur”. Nadere uitleg waaróm men dat lijkt, blijft vaak achterwege of komt neer op een opsomming van factoren waar moeilijk een voor juristen herkenbare regel van te maken is.

Een bijkomstigheid is dat dergelijke algoritmes vaak worden ontwikkeld door private bedrijven, die de effectiviteit van hun algoritme als belangrijkste verkoopargument aandragen. Het is dan ook essentieel voor hen dat zij geen inzicht hoeven te geven in de details van het algoritme, anders doet de concurrent morgen hetzelfde. Ook daardoor is sterk het beeld ontstaan dat algoritmes ondoorzichtige dozen zijn, er mag namelijk niet in worden gekeken.

Wanneer dergelijke algoritmes worden ingezet voor juridische besluitvorming, ontstaat een groot probleem. Een bestuursorgaan of rechtbank neemt dan een besluit, waarbij een deel van de motivatie gebaseerd is op een ondoorzichtige doos die ja of nee zegt. Een heldere motivatie is kern van een goede besluitvorming. Immers het is de motivatie waarop men een besluit in hoger beroep aanvecht.

Terecht dan ook dat de Hoge Raad bij het arrest van 18 augustus een duidelijke streep in het zand trekt: wanneer een bestuursrechtelijk besluit geheel of ten dele het resultaat is van een geautomatiseerd proces, moet het bestuursorgaan zorgdragen voor de inzichtelijkheid en controleerbaarheid van die keuzes, aannames en gegevens. Anders kan een belanghebbende de juistheid van de bij dat geautomatiseerde proces gemaakte keuzes en van de daarbij gebruikte gegevens en aannames niet controleren en betwisten.

De zaak betrof de modelmatige waardebepaling in het kader van de uitvoering van de Wet WOZ. Deze waardebepaling vindt in eerste aanleg geautomatiseerd plaats. Hiertoe worden door (nagenoeg uitsluitend externe) softwareontwikkelaars taxatiemodellen ontworpen die per gemeente worden gevuld met de relevante objectgegevens en de beschikbare verkoopinformatie. Op grond van modelmatige analyse worden in het taxatiemodel onder meer staffels berekend die kunnen worden gebruikt voor het bepalen van de grondwaarde van het te taxeren object, met inachtneming van het type object en de ligging van de onroerende zaak. De staffels zijn opgenomen in de software en dus niet inzichtelijk voor de ambtenaren die ermee werken, laat staan voor de betrokkenen die de waardebepaling aangezegd krijgen.

De Hoge Raad ziet een dergelijke manier van werken in strijd met fundamentele beginselen van een goede besluitvorming. Een belanghebbende kan in geval van besluitvorming op basis van een computerprogramma dat vanuit zijn perspectief is te beschouwen als een zogenoemde “black box” immers niet controleren op basis waarvan tot een bepaald besluit wordt gekomen. Het is dan onmogelijk een fatsoenlijk bezwaar daartegen te formuleren. Het verbaast dan ook niet dat de HR de betrokkene gelijk geeft.

Terug naar de tekentafel, of eigenlijk rekentafel dus voor de gemeente. Echter, dat roept de vraag op hoe een nieuw besluit dan wél fatsoenlijk tot stand kan komen. Het is namelijk het gewone werkproces waarbij deze gegevens als black box worden gebruikt. In feite zou de gemeente nu de staffels opnieuw moeten construeren en als transparante tabellen moeten aanbieden, zodat ze als duidelijke onderbouwing en grondslag kunnen dienen. Dat zal buitengewoon veel werk kosten, en dat was nu precies waarom men die software van derden afnam.

Een ander probleem is dat dergelijke nieuwe staffels mogelijk minder van kwaliteit zullen zijn. De bestaande ontransparante staffels voldoen namelijk vaak wel in hoge mate. Dat is de keerzijde van zo’n breed computer-algoritme dat op basis van data-analyse tot stand komt: het werkt wel heel goed. Het is immers gebaseerd op de feitelijke situatie, niet op hoe men op papier bedenkt dat dingen zouden kunnen zijn. Het dilemma van de algoritmes: wil men een mooi model dat niet past bij de werkelijkheid, of een passend model dat onverklaarbaar is?



Van onze blog

Privacy

Overheid

14 november 2018

Sporters en blessures: staat de persconferentie buitenspel?

Recentelijk zag ik 'm weer voorbijkomen: de uitspraak dat op grond van de AVG geen informatie meer gegeven mag worden over een opgelopen blessure bij een sporter. Dit keer was het Mark van Bommel, oud-voetballer en inmiddels trainer van voetbalclub PSV, die tijdens een persconferentie aangaf geen details te kunnen geven over de kwetsuur van één van zijn aanvallers. Waar dit een uitmuntend staaltje van 'de tegenpartij niet wijzer maken dan dat deze al is' zou kunnen zijn, is het goed mogelijk dat Mark deze instructies intern heeft meegekregen. Dit zijn echter instructies waar op z'n zachtst gezegd vraagtekens bij te plaatsen zijn.

Voetbalclubs zwijgen liever

Waar voetbalclubs en andere sportverenigingen vroeger uitvoerig (pers)informatie naar buiten brachten over hun sporters en de blessures waar deze sporters mee kampten, lijkt dit sinds enige tijd een stuk minder te zijn geworden. De reden voor de koerswijziging van sportclubs met betrekking tot het informeren van het algemeen publiek over medische ongemakken van sporters is de AVG. Hoewel niet nieuw in vergelijking met onze voorgaande privacywetgeving, de Wet bescherming persoonsgegevens (Wbp), kennen medische persoonsgegevens onder de AVG een strikter regime dan 'gewone' persoonsgegevens zoals NAW-gegevens of een telefoonnummer. Dit strikte regime houdt in dat gegevens die iets zeggen over iemands gezondheid, niet zondermeer verstrekt mogen worden.

Sterker nog, in principe is het verwerken van deze categorie gegevens simpelweg verboden.

Journalistieke exceptie is mogelijk

Echter, de wet zou de wet niet zijn, als hier niet een aantal uitzonderingen op van toepassing waren. Een relevante is hierbij: de journalistieke exceptie – opgenomen in de Uitvoeringswet AVG. Dit is de Nederlandse wet die op een aantal punten nadere invulling geeft aan de AVG. Kort gezegd houdt deze exceptie in dat partijen vrij zijn bijzondere gegevens zoals medische gegevens te verwerken in het geval dit bijdraagt aan een journalistieke uiting. Bij een persconferentie of interview aangeven dat 'speler X' aankomende week niet bij de selectie hoort, omdat hij of zij een enkelblessure heeft of dat 'tennisster Y' een toernooi moet laten schieten, vanwege een kwetsuur aan haar schouder past dus prima in dit plaatje.

Wel is het zoals bij elke verwerking van persoonsgegevens van belang om alleen de gegevens te verwerken die noodzakelijk zijn. De naam van de geneesmiddelen die aan de sporter zijn voorgeschreven, is in veel gevallen dus een duidelijke brug te ver om het doel van informatievoorziening te dienen.

Spelers kunnen media-aandacht verwachten

Ook andere gegevens mag je voor journalistieke uitingen rustig blijven verwerken. Op grond van hun bekendheid en bovengenoemde uitzondering in de wet mogen spelers ook best verwachten dat ze hier en daar in de media verschijnen. Hoewel terughoudendheid in het verspreiden van persoonsgegevens een goede zaak is, moeten we dus niet 'ineens' elke journalistieke uiting de spreekwoordelijke 'doodschop' geven.



Auteur
Jorden Bailey
Juridisch adviseur

14 november 2018

Doet 'de Wet arbeidsmarkt in balans' haar naam eer aan?

Afgelopen 7 november is het wetsvoorstel van de Wet arbeidsmarkt in balans (WAB) naar de Tweede Kamer gestuurd. Nog niet zo lang geleden trad de Wet Werk en Zekerheid (WWZ) in werking. Opnieuw zijn er dus wijzigingen in het arbeidsrecht in de maak. De WAB moet vanaf 1 januari 2020 zorgen voor meer balans tussen vaste werknemers en flexwerkers. Hoe? Lees verder voor het antwoord.

Vast minder vast & flex minder flex

Werkgevers zijn vaak huiverig om werknemers in vaste dienst te nemen. De risico's bij het hebben van een werknemer in vaste dienst zijn bijvoorbeeld hoge kosten door langdurige ziekte of het niet kunnen ontslaan van een werknemer door het strenge ontslagrecht. Werknemers in vaste dienst genieten veel bescherming. Werknemers met een tijdelijk contract, oftewel flexwerkers, genieten daarentegen veel minder bescherming. Van flexwerkers kan bijvoorbeeld gemakkelijker afscheid genomen worden. Op die manier loopt een werkgever minder risico en zo kunnen hoge kosten worden voorkomen. Werkgevers kiezen daarom eerder voor flexwerkers. Het wetsvoorstel, de WAB, moet het verschil tussen vast en flex verkleinen; oftewel 'vast minder vast' en 'flex minder flex' maken. Net als met de WWZ is het doel dat meer mensen een vaste baan krijgen.

Wat houdt de WAB in?

Belangrijke maatregelen uit de voorgestelde wet zijn:

- **Ruimere ontslagmogelijkheden:** er komt een extra ontslaggrond bij. De nieuwe negende grond maakt het mogelijk om de bestaande ontslaggronden te combineren. De ontslaggrond 'disfunctioneren' kan dus bijvoorbeeld gecombineerd worden met de ontslaggrond 'verwijtbaar handelen van de werknemer'. Dit moet ontslag makkelijker maken.
- **Transitievergoeding vanaf de eerste dag:** momenteel heeft men pas na twee jaar recht op een transitievergoeding. Dit is de vergoeding die de werkgever verplicht aan de werknemer moet betalen, wanneer hij de werknemer ontslaat. Onder de WAB krijgen werknemers vanaf de eerste dag recht op een transitievergoeding, ook bij een ontslag tijdens de proeftijd.
- **Minder hoge transitievergoeding bij lange dienstverbanden:** de opbouw van de transitievergoeding wordt verlaagd bij lange dienstverbanden. De hoogte wordt één derde maandsalaris per gewerkt jaar. Momenteel is dat na tien jaar een half maandsalaris per gewerkt jaar.
- **Lagere WW-premie voor vaste werknemers:** de WW-premie wordt voor werkgevers voordeliger als ze een werknemer een vaste baan aanbieden in plaats van een tijdelijk contract. De hoogte van de WW-premie gaat afhangen van het soort arbeidsovereenkomst. Momenteel is de hoogte van de WW-premie afhankelijk van de sector waar een bedrijf in actief is.
- **Regeling voor kleine werkgevers (< 25 werknemers):** er komt een regeling voor kleine werkgevers om de transitievergoeding te compenseren als ze hun bedrijf moeten beëindigen wegens pensionering of ziekte.
- **Langere proeftijd mogelijk voor werknemers in vaste dienst:** er komt een verlenging van de proeftijd voor werknemers die meteen een vast contract krijgen, van twee maanden naar vijf maanden.
- **Drie jaar tijdelijke contracten:** werkgevers mogen weer (voor inwerkingtreding van de WWZ was dat ook al zo) drie jaar lang maximaal drie tijdelijke contracten sluiten (ketenregeling). Momenteel is dat twee jaar en maximaal drie tijdelijke contracten.
- **Gelijke behandeling voor payrollwerknemers:** werknemers die op payrollbasis werken, krijgen minimaal dezelfde arbeidsvoorwaarden als de werknemers die in dienst zijn bij de opdrachtgever. Ook krijgen ze recht op een adequaat pensioen.
- **Meer rechten voor oproepkrachten:** er worden maatregelen genomen om verplichte permanente beschikbaarheid van oproepkrachten te voorkomen. Zo moet een werknemer minstens vier dagen van tevoren worden opgeroepen door de werkgever. Ook houden oproepkrachten recht op loon als het werk minder dan vier dagen van tevoren wordt afgezegd. De termijn van vier dagen kan bij cao worden verkort tot één dag.



Kritiek op het maatregelenpakket

Vanuit verschillende hoeken – zowel vanuit werkgeverskant als werknemerskant – is onvrede geuit over dit maatregelenpakket, zoals voorgesteld door minister Koolmees. Werkgeversorganisaties VNO-NCW en MKB-Nederland spreken van een stap vooruit, maar niet van balans. Volgens werkgeversvereniging AWWN ontbreekt het aan visie en zit er te weinig samenhang in de voorstellen. Werknemersorganisatie FNV ziet niet in hoe de WAB meer vaste banen gaat opleveren. Terwijl andere werknemersorganisatie CNV zelfs een petitie is gestart om de WAB tegen te houden, omdat er volgens hen nog meer flexbanen bij zullen komen. Ook de Raad van State heeft kritiek op het wetsvoorstel en zegt dat de voorgestelde maatregelen ontoereikend zijn om de problemen op de arbeidsmarkt op te lossen.

Grondige opknopbeurt van de arbeidsmarkt?

Uit dit wetsvoorstel, dat kort volgt op de inwerkingtreding van de WWZ, blijkt maar weer dat de werking van de wetten om de arbeidsmarkt te reguleren nauwgezet in de gaten worden gehouden. Dat is iets om toe te juichen. De vraag blijft of de maatregelen inderdaad zullen gaan zorgen voor een grondige opknop-

beurt van de arbeidsmarkt. Het wetsvoorstel ligt nu bij de Tweede Kamer. Dit betekent dat het wetsvoorstel zal worden besproken door de Kamerleden en dat er over het wetsvoorstel zal worden gestemd. De voorgestelde maatregelen zijn dus nog niet definitief. Er kan nog van alles wijzigen. Wanneer het wetsvoorstel definitief is en het duidelijk is wanneer de regels inwerkingtreden, is het belangrijk om de bedrijfsvoering en de arbeidsovereenkomsten waar nodig aan te passen. ICTRecht houdt u op de hoogte.



Auteur
Jay Rimmelzwaal
Juridisch adviseur



Auteur
Demi Grandiek
Juridisch adviseur

Trainingsoverzicht januari - juli 2019



Dinsdag 22 januari en dinsdag 9 april

Privacy en persoonsgegevens: verwerkers-overeenkomst (3 PO - 22 januari, 4 PO - 9 april)

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

<https://bit.ly/2EeNfy3>

Donderdag 24 januari 2019

Contracteren: software-overeenkomst (3 PO)

Software is onderdeel van vrijwel ieder ICT-contract. Beheersen van licentieaspecten is dan ook een vereiste voor een senior adviseur. Welke modellen voor licentieverlening zijn er, wat vereisen deze contractueel en welke randvoorwaarden zijn van belang vanuit zowel de positie van licentiegever als licentienemer? Tevens worden de beginselen van contracteren bij software-ontwikkeling tijdens deze masterclass software-overeenkomst behandeld.

<https://bit.ly/2IXRBhF>

Dinsdag 2 april 2019

Contracteren: ICT-valkuilen bij contractenrecht (4 PO)

Het contractenrecht is een kerndeel van het werk als ICT-jurist. Binnen en buiten de ICT kent elk contract standaard onderwerpen in het kader van het vermogensrecht en het verbintenissenrecht zoals ontbinding, opschorting en (fatale) termijnen. Binnen de ICT kennen deze onderwerpen specifieke valkuilen.

<https://bit.ly/2Rv5MJD>

Dinsdag 16 april 2019

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 (kwaliteit, aansprakelijkheid, intellectueel eigendom, datatoegang, continuïteit en persoonsgegevens) en daarnaast specifieke aspecten.

<https://bit.ly/2rjRy19>

Dinsdag 14 mei 2019

Privacy en persoonsgegevens: de basis (6 PO)

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

<https://bit.ly/2s4yA12>

Donderdag 16 mei 2019

Legal tech: modulair contracteren II (4 PO)

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

<https://bit.ly/2QDgn81>

Dinsdag 21 mei 2019

Ondernemen: verdienmodellen en financiering (4 PO)

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

<https://bit.ly/2BSrEJG>

Dinsdag 18 juni 2019

Contracteren: de verdieping (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!

<https://bit.ly/2rjPeqH>

Donderdag 27 juni 2019 (4 PO)

Legal tech: slimme contracten en blockchain

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

<https://bit.ly/2m3TyK8>

Dinsdag 2 juli 2019

Privacy en persoonsgegevens: de verdieping (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. Tijdens de training leert u onder meer over binding corporate rules, de verwerkersovereenkomst, registers en de Functionaris Gegevensbescherming (FG).

<https://bit.ly/2rk8VPi>

Donderdag 4 juli 2019

Contracteren: onderhandelen

ICT-dienstovereenkomst (4 PO)

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

<https://bit.ly/2PmnuwP>

Overzicht themadagen FG-opleiding januari - mei 2019

Binnen onze FG-opleiding onderscheiden wij diverse themadagen. Op een themadag wordt één specifiek thema behandeld. De themadagen zijn ook los afneembaar.

24 januari	Themadag FG en privacywetgeving
7 februari	Themadag soft skills
14 februari	Themadag inventariseren en registreren
7 maart	Themadag internet en security
14 maart	Themadag datalekken
21 maart	Themadag rechten van betrokkenen
4 april	Themadag verantwoordelijke en verwerker
11 april	Themadag online marketing en cookies
9 mei	Themadag FG in de zorg (optioneel)

ictrecht.nl/fg-opleiding

Heeft u vragen of wilt u meer weten?

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



Alisa Schurink

Opleidingscoördinator
en Marketing Assistant



ICTRECHT
adviesbureau
