jaargang 10 • nummer 1 • jan 2022

ICTRecht in de praktijk

Toegangsbeveiliging:
waarom het zo belangrijk is en
hoe u er grip op houdt

Onrechtmatige informatie
op het internet:
wie stelt u aansprakelijk?

2021: een recap
door onze privacyexperts

ICTRECHT
adviesbureau

ICTRecht: praktisch en deskundig

ICTRecht is hét grootste en meest ervaren fullservice adviesbureau op het gebied van ICT-recht, privacy en security. Met een team van meer dan 70 specialisten voorzien we onze klanten van deskundig en praktisch advies. Van startup tot multinational en van overheidsinstantie tot zorginstelling.

Wij zijn flexibel, innovatief en denken proactief met klanten mee. Onze adviezen zijn altijd concreet en begrijpelijk, en geven blijk van onze technische kennis.

Geen zes pagina's jargon met als conclusie

"dat hangt ervan af", maar een duidelijk antwoord

waarmee de organisatie direct aan de slag kan.

Hier zijn wij goed in:

ICT-recht - Privacy - Security - Legal tech - Academy - Detachering - Werving & selectie

ICTRECHT
adviesbureau

Meer informatie over hoe wij werken? Bezoek ictrecht.nl

Index

Dit is een uitgave van ICTRecht B.V. Telefoonnummer: 020 663 1941, e-mail: info@ictrecht.nl.

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

Aan deze uitgave werkten mee:

Alisa Schurink Marketing adviseur
a.schurink@ictrecht.nl
Arnoud Engelfriet Algemeen directeur/ Opleidingsdirecteur
a.engelfriet@ictrecht.nl
Bram de Vos Juridisch adviseur
b.devos@ictrecht.nl
Britt Telleman Opleidingscoördinator
b.telleman@ictrecht.nl
Isabella Oelz Juridisch adviseur
i.oelz@ictrecht.nl
Jasmine Benning Juridisch adviseur
j.benning@ictrecht.nl
Jonas van Ginkel Juridisch adviseur
j.vanginkel@ictrecht.nl
Koen van Jaarsveld Legal consultant
k.vanjaarsveld@ictrecht.nl
Kors Monster Directeur ICTRecht Security
k.monster@ictrecht.nl
Laura Monhemius Juridisch adviseur
l.monhemius@ictrecht.nl
Marjolein Struik Juridisch adviseur
m.struik@ictrecht.nl
Maxime Leijendekker Juridisch adviseur
m.leijendekker@ictrecht.nl
Menno Konst Juridisch adviseur
m.konst@ictrecht.nl
Nicole Waaijer Marketing adviseur
n.waaijer@ictrecht.nl
Pelçim Kaygusuz Juridisch adviseur
p.kaygusuz@ictrecht.nl
Sten Demon Legal consultant
s.demon@ictrecht.nl
Amanda Butterworth Grafisch ontwerper
info@amandabutterworth.com
Leonard Fäustle Stills & Motion Foto's ICTRecht
info@leonardfaustle.nl

Pelçim Kaygusuz
Juridisch adviseur

E-health Innovatie

AI Act naast MDR: reden tot zorg?

Technologie is altijd een onderdeel geweest van de menselijke evolutie. Door de uitvinding van het wiel konden we onszelf (en onze spullen) ineens een stuk sneller verplaatsen. En zonder de uitvinding van de drukpers was het erg ingewikkeld geweest om wetenschap te bedrijven op de manier waarop wij dat nu doen. Maar waar de hiervoor genoemde uitvindingen heel zichtbaar zijn, vindt technologische innovatie vandaag de dag steeds vaker achter gesloten deuren plaats. Denk bijvoorbeeld aan de opkomst van Artificial Intelligence (AI). Steeds vaker laten we computers (semi-)autonome beslissingen maken, maar hoe zo'n AI werkt en tot zijn beoordeling komt is vaak niet inzichtelijk. Daar kleven vanzelfsprekend ook risico's aan. Denk bijvoorbeeld aan de zorg: wat als AI een bepaalde operatie aanraadt en dit achteraf niet juist blijkt? We worden steeds bewuster van de risico's van AI en onder andere om die reden is de High-Level Expert Group on AI opgericht en zijn de 'Ethics Guidelines for Thrustworthy AI' opgesteld.[1] Daarnaast kent de zorg ook sector-specifieke regelgeving, zoals de Medical Device Regulation (MDR). Hierin staan regels om bijvoorbeeld de kwaliteit van medische technologie te waarborgen. Nu stelt de Europese Commissie een algemene act voor die moet gaan gelden voor elke toepassing van AI in elke sector. Tijd om de AI Act en MDR te vergelijken: hoe verhouden de genoemde wetgevingsinstrumenten zich tot elkaar? En waar zitten mogelijke knelpunten bij de invoering van de AI Act?[2]

1. European Commission, 'Ethics guidelines for trustworthy AI' (Shaping Europe's digital future, 8 April 2019).
2. Wegens de omvang van het onderwerp is de keuze gemaakt om niet uitvoerig inhoudelijk in te gaan op alle vereisten van zowel de MDR als de AI Act.

AI Act

De AI Act is een voorstel met regels die gesteld worden aan het ontwikkelen, in de handel brengen en gebruiken van AI-systemen. De AI Act definieert een AI-systeem als volgt:

'Software die is ontwikkeld aan de hand van een of meer van de technieken en benaderingen die zijn opgenomen in de lijst van bijlage I en die voor een bepaalde reeks door mensen gedefinieerde doelstellingen output kan genereren, zoals inhoud, voorspellingen, aanbevelingen of beslissingen die van invloed zijn op de omgeving waarmee wordt geïnterageerd'.[3]

3. Artikel 3 lid 1 AI Act.

Hieruit kan opgemaakt worden dat het in principe voor alle AI-toepassingen geldt.

De AI Act maakt een onderscheid tussen verschillende risicoklassen waar de AI-systemen onder kunnen vallen. Zo is er een onacceptabel risico (een voorbeeld is *social scoring*[4]), hoog risico (zoals bepaalde medische hulpmiddelen[5]), beperkt risico (zoals chatbots) en minimaal risico (spamfilters). Afhankelijk van de risicoklasse moet er aan meer of minder verplichtingen worden voldaan.

4. Artikel 5 lid 1 sub c AI Act.
5. Artikel 6 lid 1 en Bijlage II AI Act.

Wat houden de eisen in?

Naast dat de AI Act eisen stelt aan het AI-systeem, bevat het ook eisen en verplichtingen over de omgang en ontwikkeling met en van het AI-systeem. Denk daarbij bijvoorbeeld aan verplichtingen als documentatie van de gebruikte techniek en transparante informatieverstrekking aan de gebruikers.[6] Maar er moet ook een kwaliteitsbeheer- en risicobeheersysteem[7] zijn en er moet een conformiteitsbeoordeling worden uitgevoerd.[8]

6. Artikel 6 AI Act.
7. Artikel 9 AI Act.
8. Artikel 45 AI Act.

Het doel van een kwaliteitsbeheersysteem is het waarborgen van de naleving van de AI Act.[9] De AI Act biedt een opsomming van aspecten die het kwaliteitsbeheersysteem minimaal moet omvatten. Het kwaliteitsbeheersysteem bestaat uit beleidslijnen, procedures en instructies. Het risicobeheersysteem is daarentegen een doorlopend iteratief proces. De bekende en voorzienbare risico's moeten in kaart gebracht worden, maar er moet ook een inschatting gemaakt worden van de risico's die zich nog kunnen voordoen bij ingebruikname. Dit laatste wordt ook gedaan door data te analyseren die verzameld wordt door een verplicht monitoringssysteem na het in de handel brengen van het AI-systeem.[10]

9. Artikel 17 AI Act.
10. Artikel 9 AI Act.

Wisselwerking AI Act en MDR

Wanneer een AI-systeem wordt toegepast voor zorgdoeleinden kan naast de AI Act ook de MDR van toepassing zijn. Dit is echter alleen het geval indien het AI-systeem aan een aantal vereisten voldoet. Het AI-systeem moet:

- een eigen medisch doel hebben;[11]
- standalone zijn;[12]
- actie op de data uitvoeren;
- toegepast worden op individuele patiënten.

11. Artikel 2 MDR (EU) 2017/745.
12. Artikel 2 onder 4 MDR (EU) 2017/745.

Als de software gekwalificeerd kan worden als een medisch hulpmiddel dan moet bepaald worden in welke risicoklasse het hulpmiddel valt. Afhankelijk van deze classificatie gelden er bepaalde eisen. Er bestaan vier verschillende risicoklassen (I, IIa, IIb en III), waarbij de laagste risicoklasse (klasse I) ziet op medische hulpmiddelen die weinig risico's meebrengen voor de veiligheid van de patiënt. Denk hierbij aan pleisters. Klasse III is de hoogste risicoklasse, hierbij kan gedacht worden aan pacemakers. Dit getrapte systeem voor de risicoklassen zien we ook terug in de AI Act.

Wanneer we de uitgelichte vereisten van de AI Act vergelijken met de vereisten die al gelden onder de MDR dan zien we dat er hier en daar overlap is.[13] Zo is een risicobeheersysteem onder beide verordeningen vereist, al wordt het onder de MDR een 'risicomanagementsysteem' genoemd. De ISO 14971-norm is de internationale norm voor risicomanagement van medische hulpmiddelen. Onder deze norm is het risicomanagementproces ook voor de gehele productlevenscyclus vereist, net zoals onder de AI Act. Het doel van beide systemen onder de verschillende verordeningen is hetzelfde. Het verschil zit 'm in het specifieke karakter van de AI Act. De AI Act is specifiek geschreven voor AI-systemen en de MDR voor alle medische hulpmiddelen (met of zonder AI). De aanbieder moet onder de MDR de risico's al monitoren. Daar komt nu bij dat het monitoren mogelijk is door de data die verzameld wordt door het AI-systeem zelf, nadat het in de handel is gebracht. Het is dus niet één op één hetzelfde als het risicomanagementsysteem onder de MDR. De aanbieder zal dus naar zowel de AI Act als naar de MDR moeten kijken.

13. Omwille van de leesbaarheid zijn niet alle vereisten van de AI Act en de MDR naast elkaar gelegd.

Voor het kwaliteitsbeheersysteem geldt onder de AI Act dat er een systeem moet zijn voor de monitoring van het AI-systeem. Nadat het in de handel is gebracht, moeten er procedures zijn voor het melden van ernstige incidenten, moeten de verantwoordelijkheden binnen de organisatie uiteen worden gezet en moeten er procedures zijn voor de kwaliteitscontrole van het AI-systeem. Ook op dit punt is er veel overlap met de MDR. Wat wel een opvallend verschil is, is dat de verantwoordelijkheden die uiteengezet moeten worden onder de AI Act verder gaan. Onder de AI Act moeten de verantwoordelijkheden van het management en ander personeel (wat dan zo ongeveer de rest van de organisatie betekent) uiteengezet worden. Terwijl onder de MDR wordt gesproken over 'verantwoordelijkheid van het beheer'. De reden hiervan kan zijn dat er in de praktijk gevreesd wordt dat het moeilijk wordt om iemand aansprakelijk te stellen wanneer AI fouten maakt. Wellicht heeft de Europese Commissie geprobeerd om dat risico op deze manier wat in te perken.

Tot slot dient onder beide verordeningen een conformiteitsbeoordeling uitgevoerd te worden om aan te tonen dat aan de verplichtingen uit de desbetreffende verordening is voldaan. Dit is onder beide verordeningen van belang voor onder andere de CE-markering. Onder beide verordeningen is het mogelijk om de conformiteitsbeoordeling zelf uit te voeren of door een aangemelde instantie (de onafhankelijke derde). Onder de MDR is het zo dat een *notified body* betrokken moet worden bij het proces wanneer het gaat om een medisch hulpmiddel uit klasse IIa of hoger. In de overige gevallen mag de beoordeling intern uitgevoerd worden. Onder de AI Act lijkt het in eerste instantie alsof de aanbieder zelf de keuze mag maken of de beoordeling intern wordt uitgevoerd of door een aangemelde instantie. Maar wanneer we verder lezen blijkt dat er uitzonderingen zijn. Opmerking verdient wel dat het erg omslachtig is om te achterhalen of je als aanbieder zelf de keuze mag maken of niet. Onder de MDR is dit erg duidelijk: risicoklasse IIa of hoger? Schakel een *notified body* in! In tegenstelling tot de AI Act waar van de ene na de andere bijlage wordt verwezen. Een ware puzzel zou je kunnen zeggen.

AI Act: goed idee of weg ermee?

De AI Act heeft een specifieker karakter voor wat betreft AI, dan de MDR. Gezien de AI Act specifiek is ontworpen om te voorzien in vereisten voor de toepassing van AI, zijn er ook vereisten die hierop aansluiten en meer verdiepend zijn dan de vereisten in de MDR. Wanneer een medisch hulpmiddel een AI-systeem kent zal er dus aan extra voorwaarden voldaan moeten worden. Dit brengt wel een vraag met zich mee: wordt het wettelijk kader niet duidelijker als sectorspecifieke wetgeving (zoals de MDR) uitgebreid wordt met vereisten die van toepassing zijn wanneer AI wordt toegepast? De verordening heeft discussies gestart, dus wellicht is een 'wordt vervolgd' hier op z'n plaats?

Kors Monster
Directeur ICTRecht Security

Security

Toegangsbeveiliging: waarom het zo belangrijk is en hoe u er grip op houdt

Bij ‘toegangsbeveiliging’ wordt in eerste instantie misschien vooral gedacht aan de toegangspasjes voor het kantoorgebouw, de beveiliger bij de deur of de receptie, of de slagboom bij de parkeergarage. Maar ook in het digitale domein is ‘toegangsbeveiliging’ een belangrijk middel om uw kroonjuwelen te beschermen. Wanneer een onbevoegde toegang heeft tot uw netwerk, systemen, applicaties en/of informatie kan niet alleen de vertrouwelijkheid van de informatie onder druk komen te staan. Ook de beschikbaarheid en integriteit van de informatie kunnen worden aangetast, waardoor u niet over de informatie kunt beschikken op het moment dat dit nodig is, of waardoor uw informatie aangetast en daardoor onjuist (en onbruikbaar) wordt.

Risico’s bij ongeoorloofde toegang

Als er onvoldoende grip is op toegang tot informatie en faciliteiten waarmee informatie wordt verwerkt (zoals netwerken, systemen en applicaties) loopt u het risico dat onbevoegden daar toegang toe krijgen. Als het om gevoelige informatie gaat, bijvoorbeeld privacygevoelige gegevens of bedrijfsgeheimen, dan levert de enkele inzage in de gegevens al een probleem op. Maar met toegang tot de gegevens kunnen de gegevens ook gewist, aangepast of anderszins onbruikbaar worden gemaakt. Dat kan het gevolg zijn van een bewuste actie, bijvoorbeeld

door cybercriminelen die gegevens versleutelen om losgeld te vragen, maar het kan ook gaan om onbewuste acties zoals menselijke fouten of onkunde. Het is dus belangrijk om niet alleen de inzage in informatie te beperken, maar ook de handelingen die een gebruiker kan uitvoeren met betrekking tot de informatie.

Wat toegangsbeveiliging probeert te bereiken

Het beveiligen van toegang tot informatie en de faciliteiten waarmee informatie wordt verwerkt heeft doorgaans tot doel:

1. Het beperken van toegang tot informatie en de faciliteiten waarmee informatie wordt verwerkt;
2. Ervoor zorgen dat bevoegde gebruikers daadwerkelijk toegang hebben tot de informatie en faciliteiten die zij nodig hebben;
3. Voorkomen van onbevoegde toegang tot informatie en faciliteiten;
4. Gebruikers verantwoordelijk maken voor het geheimhouden van hun inloggegevens en andere geheime authenticatiegegevens.

Het is goed om te realiseren dat deze doelstellingen bestaan tegen de achtergrond van het overkoepelende doel van informatiebeveiliging, namelijk het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie en -systemen om de continuïteit van de informatievoorziening (en daarmee de continuïteit van de organisatie) te waarborgen, plus het beperken van informatiebeveiligingsincidenten tot een vooraf bepaald, acceptabel niveau.

Daarbij geldt dat de 'plan-do-check-act-cyclus' als werkwijze wordt gehanteerd om doelmatig en efficiënt te werk te kunnen gaan, en om het beschermingsniveau continu te verbeteren.

Aan de slag met toegangsbeveiliging

Overtuigd van de toegevoegde waarde van toegangsbeveiliging? Dan wordt het tijd om ermee aan de slag te gaan. Via onderstaand stappenplan geven wij handvatten om op een praktische manier meer grip te krijgen op toegangsbeveiliging. De stappen worden vervolgens per stuk toegelicht.

1. bepalen wat precies beschermd moet worden;
2. formuleren van toegangsbeleid;
3. toekennen, beheren en intrekken van rechten;
4. controleren van toegekende rechten en bijsturen waar nodig;
5. evalueren en verbeteren van beleid en werkwijze.

1. Bepalen wat precies beschermd moet worden en waarom

Het klinkt als een open deur, maar in de praktijk zien wij dat hier vaak nog maar beperkt zicht op is: om aan de slag te gaan met toegangsbeveiliging is het belangrijk om te weten wat u precies in huis heeft. Over welke soorten informatie beschikt de organisatie? Maar ook: met welke netwerken, systemen en applicaties wordt de informatie ontsloten? Stap 1 bestaat dus uit het verkrijgen van inzicht in wat precies beschermd moet worden.

Een tweede punt is bepalen hoe belangrijk de informatie of faciliteit is voor de organisatie. Een risico-inventarisatie, *risk assessment* of Business Impact Assessment (BIA) kan daarin inzicht geven. Enerzijds is dit belangrijk om ervoor te kunnen zorgen dat belangrijke systemen adequaat beschermd worden. Anderzijds is dit ook belangrijk om efficiënt te kunnen werken: informatie en systemen die minder belangrijk of minder risicovol zijn, kunnen met een lager beschermingsniveau alsnog 'veilig genoeg' zijn.

2. Formuleren van toegangsbeleid

Nu er zicht is op de informatie , de informatieverwerkende faciliteiten, en het belang daarvan voor de organisatie, kan beleid worden geformuleerd. Het beleid beschrijft wat de organisatie wil bereiken met toegangsbeveiliging en hoe zij dat voor elkaar wil krijgen. Onderwerpen die thuishoren in een toegangsbeleid zijn o.a.:

- Doelstellingen met betrekking tot toegangsbeveiliging binnen de organisatie.
- Taken en verantwoordelijkheden rond toegangsbeveiliging.
- Toepasselijke uitgangspunten en principes, zoals 'need to know' (u krijgt alleen toegang tot informatie die u nodig heeft voor uitoefening van uw taken) en 'need to use' (u krijgt alleen toegang tot faciliteiten die nodig zijn om uw taak uit te oefenen).
- Scheiding van functies en rollen binnen toegangsbeveiliging, zoals het aanvragen/toekennen/intrekken van rechten.
- Omgang met rollen met bijzondere toegangsrechten (zoals administrators).
- Interne beoordelingen en controles van toegangsrechten.

Daarnaast kan het beleid o.a. de werkwijze m.b.t. het aanvragen, toekennen, wijzigen en intrekken van

rechten beschrijven of verwijzen naar een procedure of ander document waarin dit wordt uitgewerkt.

3. Toekennen, beheren en intrekken van rechten

Inmiddels is bekend welke informatie en faciliteiten moeten worden beschermd en waarom zij het beschermen waard zijn. Vervolgens is het beleid met betrekking tot toegangsbeveiliging bepaald. Nu wordt het tijd om het beleid in de praktijk te gaan toepassen.

Het is daarbij belangrijk om duidelijke taken en verantwoordelijkheden af te spreken. De directie en/of het management zullen ervoor moeten zorgen dat degenen die een taak of verantwoordelijkheid hebben voldoende tijd en middelen beschikbaar hebben om hun taken en verantwoordelijkheden uit te voeren. Denk daarbij overigens ook aan competenties: het is óók de taak van directie/management om taken en verantwoordelijkheden toe te bedelen aan personen die over de juiste competenties beschikken (of om hen op te leiden, zodat ze over de benodigde competenties gáán beschikken).

Maak duidelijke afspraken over de werkwijze, taken en verantwoordelijkheden rondom:

- Het aanvragen van nieuwe accounts en toegangsrechten.
- Het wijzigen van bestaande accounts en rechten, bijvoorbeeld wanneer iemand een nieuwe functie krijgt.
- Het intrekken van accounts en rechten, bijvoorbeeld wanneer iemand de organisatie verlaat.
- De manier waarop inloggegevens en andere geheime authenticatie-informatie worden opgeslagen en beheerd.
- Geaccepteerde procedures voor inloggen.
- Het gebruik van *password managers*.
- De omgang met programma's die verhoogde rechten nodig hebben.
- Het beperken van toegang tot broncode.

Kies daarbij een werkwijze met bijbehorende afspraken die past bij uw organisatie. Een organisatie die bestaat uit 5 man heeft andere behoeften dan een corporate met duizenden medewerkers.

Toets of met de afspraken aan het eerder opgestelde beleid wordt voldaan. Het strekt tot aanbeveling om de gemaakte afspraken op papier te zetten. Zo wordt onduidelijkheid of verwarring voorkomen en wordt het een stuk eenvoudiger om anderen (zoals toekomstige collega's) te informeren en instrueren.

4. Controleren van toegekende rechten en bijsturen waar nodig

Het is belangrijk om regelmatig te controleren of het beleid en de afspraken op juiste wijze zijn nageleefd. Meer concreet: om te controleren of de rechten die gebruikers hebben, conform het beleid en de afgesproken werkwijze zijn toegekend. Schenk daarbij extra aandacht aan accounts met bijzondere toegangsrechten (zoals *administrators*).

Het spreekt voor zich dat hoe vaker gecontroleerd wordt, hoe sneller kan worden ingegrepen als er iets niet klopt. Hoe vaak de controles worden uitgevoerd, kan worden gekoppeld aan het belang van de betreffende informatie/faciliteit en de daarbij horende risico's; bij een groter belang of groter risico wordt dan vaker gecontroleerd dan bij minder belangrijke of minder risicovolle informatie/faciliteiten.

5. Evalueren en verbeteren van beleid en werkwijze

Veel organisaties denken dat ze met bovenstaande stappen klaar zijn. De realiteit is echter dat veranderingen snel gaan, waardoor het beleid en de werkwijze na verloop van tijd verouderen en hun nut en bruikbaarheid verliezen. Bovendien: het beleid en de werkwijze rond toegangsbeveiliging zal altijd mogelijkheden tot verbetering hebben. Dat kan een verbetering zijn die erop gericht is het beveiligingsniveau te verhogen, maar het kan ook een verbetering zijn die (bijvoorbeeld) leidt tot meer efficiëntie, minder fouten of lagere kosten.

Het is daarom belangrijk om zowel het beleid als de werkwijze periodiek tegen het licht te houden. Het strekt tot aanbeveling om dit minstens één keer per jaar te doen, waarbij vervolgens het beleid en de afspraken verbeterd worden conform de uitkomsten van de evaluatie.

Bram de Vos
Juridisch adviseur

Wet- en regelgeving

Tijdelijke verordening ter bestrijding van online kindermisbruik

Op 30 juli 2021 is er een verordening betreffende een tijdelijke afwijking ten aanzien van de e-Privacyrichtlijn bekendgemaakt in het publicatieblad van de Europese Unie (2021/1232). De verordening biedt ruimte aan aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten (zoals webmail en berichtendiensten) om online seksueel misbruik van kinderen op te sporen en te melden bij de bevoegde autoriteiten. Er zijn al verschillende dienstverleners die zich op vrijwillige basis inzetten om online seksueel misbruik via hun diensten op te sporen en aan te pakken. Hoewel deze activiteiten in de basis legitiem zijn, wordt hiermee wel inbreuk gemaakt op de grondrechten van de gebruikers van de dienst. Deze nieuwe verordening voorziet in tijdelijke afwijkingen van de e-Privacyrichtlijn om de opsporing en bestrijding toch mogelijk te maken. Om ervoor te zorgen dat de privacy van de gebruikers voldoende geborgd is, moet wel worden voldaan aan de Algemene verordening gegevensbescherming (AVG) en een aantal aanvullende voorwaarden die in verordening 2021/1232 worden gesteld. Aanvankelijk geldt de verordening voor een periode van 3 jaar. Deze kan eventueel nog worden verlengd of juist eerder komen te vervallen als er binnen deze periode consensus wordt bereikt over definitieve wetgeving.

https://bit.ly/3HFAYA8

Wetsvoorstel verlenging experimentwet stembiljetten en centrale stemopneming

Op 30 augustus 2021 is er een voorstel tot wijziging van de Tijdelijke experimentwet stembiljetten en centrale stemopneming ingediend bij de Tweede Kamer. Deze tijdelijke wet maakt het mogelijk om stembiljetten per e-mail toe te sturen naar stemgerechtigden die in het buitenland wonen. Ook biedt de wet ruimte aan gemeenten om te experimenteren met het centraal tellen van de ingezamelde stembiljetten. De experimentwet zou eigenlijk per 1 januari 2022 komen te vervallen. Via dit wijzigingsvoorstel wordt de duur verlengd tot 1 januari 2024.

https://bit.ly/3kU2roe

Wijziging Richtlijn CE-markering radioapparatuur

Op 23 september 2021 werd een voorstel tot aanpassing van de Richtlijn betreffende de harmonisatie van nationale wetgeving inzake het op de markt aanbieden van radioapparatuur (2014/53/EU) gepubliceerd. De aanpassing moet onder meer de hoeveelheid E-waste terugdringen door verdere harmonisatie van opladers voor mobiele (radio)apparatuur. Het aantal verschillende soorten opladers is de afgelopen jaren al sterk verminderd, maar nog steeds worden er verschillende soorten aansluitingen gebruikt. De Europese Commissie wil daarom USB-C als standaardpoort aanwijzen voor onder meer smartphones, tablets en koptelefoons. Ook stelt de Europese Commissie voor om de verkoop van opladers los te koppelen van de verkoop van elektronische apparaten (“ontbundeling”). Dit om te voorkomen dat er onnodig veel opladers worden geproduceerd. Verder moet de consument beter worden geïnformeerd over de oplaadprestaties van de aangeboden apparaten.

https://bit.ly/3FBYegN

Wet open overheid

Op 5 oktober 2021 heeft de Eerste Kamer ingestemd met het initiatiefvoorstel van de Tweede Kamer voor de Wet open overheid ("Woo"). Het aannemen van de wet heeft zeer veel tijd in beslag genomen: al in 2012 werd het oorspronkelijke voorstel ingediend. De Woo vervangt de reeds bestaande Wet openbaarheid van bestuur ("Wob") en heeft tot doel om (semi-)overheden transparanter te maken. Overheidsorganisaties worden via de Woo aangespoord om actief informatie openbaar te maken. Daarnaast bevat de wet onder meer een aanscherping van de weigeringsgronden voor het verstrekken van informatie aan burgers. Ook worden de beslistermijnen korter en moet elk bestuursorgaan verplicht een Woo-contactfunctionaris aanstellen.

https://bit.ly/3nEnQn9

Consultatie Implementatiewet DAC7

Op 8 oktober 2021 werd de internetconsultatie van de Wet implementatie EU-richtlijn transparantie inkomsten via de digitale platformeconomie en overige aanpassingen gestart. Al eerder dit jaar heeft de Raad van de Europese Unie deze richtlijn (ook wel bekend onder de naam DAC7) aangenomen. De richtlijn moet bijdragen aan eerlijkere en eenvoudigere belastingheffing in de digitale economie. Zo voorziet de richtlijn in verplichtingen voor online verkoopplatforms om de identiteit van verkopers op hun platform te controleren. Ook worden de platformaanbieders verplicht om (fiscale) informatie te rapporteren aan de bevoegde belastingautoriteiten. Via de implementatiewet moet de richtlijn worden geïncorporeerd in het Nederlandse wet- en regelgevingsstelsel. De implementatiewet leidt tot diverse wijzigingen in de Wet op de internationale bijstandsverlening bij de heffing van belastingen.

https://bit.ly/3xeiBOe

Wetsvoorstel coördinatie en analyse terrorismebestrijding en nationale veiligheid

Op 9 november 2021 heeft minister Grapperhaus van Justitie en Veiligheid het wetsvoorstel coördinatie en analyse terrorismebestrijding en nationale veiligheid ingediend bij de Tweede Kamer. Het voorstel geeft een wettelijke grondslag voor het verwerken van (bijzondere) persoonsgegevens aan de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De NCTV coördineert het beleid op het gebied van terrorismebestrijding en draagt zorg voor analyses van trends en risico's op dit vlak. Voor het uitvoeren van deze taken kan het nodig zijn om (bijzondere) persoonsgegevens te verwerken. Onder meer de Autoriteit Persoonsgegevens heeft zich kritisch uitgelaten over het voorstel. De toezichthouder wijst erop dat de bevoegdheden onvoldoende duidelijk zijn en dat het wetsvoorstel te weinig waarborgen bevat. Het wetsvoorstel is inmiddels controversieel verklaard en zal daarom voorlopig niet in behandeling worden genomen.

https://bit.ly/3cxsSeR

Advies gewijzigd voorstel WGS

Op 9 november 2021 publiceerde de Autoriteit Persoonsgegevens een adviesrapport waarin zij zich (opnieuw) kritisch uitliet over het voorstel voor de Wet gegevensverwerking door samenwerkingsverbanden ("WGS"). Hoewel er al verschillende wijzigingen zijn doorgevoerd, bevat het voorstel in de huidige vorm nog steeds te weinig privacywaarborgen volgens de toezichthouder. Het voorstel maakt het mogelijk voor overheidsorganisaties en private partijen om gegevens met elkaar uit te wisselen ten behoeve van de opsporing van fraude en ondermijnende criminaliteit. Volgens AP-voorzitter Wolfsen gaat het huidige voorstel verder dan het sterk bekritiseerde SyRI. Het is onvoldoende duidelijk voor welke doeleinden de gegevens gedeeld en geanalyseerd mogen worden. Daarnaast ziet het voorstel op ruime categorieën persoonsgegevens. Het wetsvoorstel moet nog behandeld worden door de Eerste Kamer.

https://bit.ly/3FAwoBn

Jonas van Ginkel
Juridisch adviseur

Menno Konst
Juridisch adviseur

Cloud E-commerce

Platformarbeiders: zelfstandigen met arbeidscontract?

Commerciële platforms spelen in de huidige digitale samenleving een steeds grotere rol. Een platform laat zich simpelweg omschrijven als een organisatiemodel waarbij op een efficiënte wijze vraag en aanbod bij elkaar worden gebracht. De rol van het platform laat zich daarbij typeren als die van een bemiddelaar.
Het platform maakt het mogelijk voor aanbieders van producten of diensten om transacties aan te gaan met klanten. Via platformen komen dus allerlei overeenkomsten tot stand, waarbij het platform in beginsel zelf geen partij is.

De via het platform gesloten overeenkomsten moeten uitgevoerd worden. Zo heeft het platform Uber, waarmee reizigers taxiritten kunnen boeken, chauffeurs nodig om de tot stand gekomen taxiritten uit te voeren. Ook via het platform Deliveroo kunnen maaltijdbezorgers aan de slag om ervoor te zorgen dat bestellingen van restaurants bij klanten bezorgd worden. De vraag die al geruime tijd voor discussie zorgt, is of de verhouding tussen het personeel en het platform valt te kwalificeren als een arbeidsovereenkomst. Zowel bij Deliveroo en Uber hebben verschillende rechters zich gebogen over deze vraag. In het verdere verloop van dit artikel wordt ingegaan over wanneer een overeenkomst kan worden gekwalificeerd als een arbeidsovereenkomst. Vervolgens worden de twee uitspraken behandeld. Aan de hand daarvan wordt bekeken of daaruit een bepaalde trend voortvloeit.

Wanneer is er sprake van een arbeidsovereenkomst?

De arbeidsovereenkomst is volgens de wet een overeenkomst waarbij een werknemer zich *in dienst van* een andere partij, de werkgever, verbindt om *arbeid* te verrichten *gedurende een zekere tijd* waar *loon* tegenover staat.[1] Deze definitie geeft vier elementen die een rol spelen om een overeenkomst te kwalificeren als een arbeidsovereenkomst:

- er moet arbeid worden verricht die bijdraagt aan het primaire doel van de onderneming;
- voor deze arbeid moet de werkgever een vergoeding verschuldigd zijn;
- tussen werknemer en werkgever moet een zekere gezagsverhouding bestaan; en
- de arbeid geschiedt gedurende een zekere tijd.

1. Art. 7:610 lid 1 BW.

Voor de beoordeling of sprake is van een arbeidsovereenkomst, worden de bovenstaande elementen als 'totaalplaatje' beoordeeld. Daarbij weegt een bepaald element niet zwaarder ten opzichte van een ander element. Wanneer de conclusie luidt dat de overeenkomst onder de definitie van een arbeidsovereenkomst valt, zijn alle (semi-)dwingendrechtelijke regels uit het arbeidsrecht van kracht. Zo moet een werkgever onder andere een werknemer doorbetalen in het geval van ziekte, is de werkgever verplicht loonbelasting af te dragen en heeft de werknemer ontslagbescherming.

Voor de kwalificatie van een arbeidsovereenkomst is het niet van belang hoe partijen de overeenkomst precies definiëren en wat partijen precies bedoelen.[2] Alle omstandigheden die feitelijk een rol spelen tussen de partijen worden meegenomen in de beoordeling van de kwalificatie.[3] Daarbij gaat 'wezen voor schijn'. Met andere woorden: als partijen afspreken om te werken met een overeenkomst van opdracht, maar de feitelijke uitvoering is in overeenstemming met een arbeidsovereenkomst, dan is van laatstgenoemde sprake.

2. HR 6 november 2020, ECLI:NL:HR:2020:1746 (zaak X/Gemeente).
3. HR 14 november 1997, ECLI:NL:HR:1997:ZC2495 (Groen/Schroever).

Maaltijdbezorgers van Deliveroo: zzp'ers of werknemers?

De eerste zaak die besproken wordt is die van Deliveroo.[4] Zij is één van de vele digitale platformen op het gebied van bezorgdiensten voor restaurants. Het idee is simpel: men bestelt bij een restaurant een maaltijd en deze wordt vervolgens door een bezorger afgeleverd bij de klant. De bezorgers hebben met Deliveroo een overeenkomst afgesloten met als aanhef 'Opdrachtovereenkomst'. Dit duidt erop dat de bezorgers als zzp'ers de opdrachten uitvoeren voor Deliveroo. Voordat een bezorger aan de slag gaat, moet hij/zij een aantal instructievideo's bekijken. Om daadwerkelijk de werkzaamheden uit te voeren, dient de bezorger in te loggen op het door Deliveroo beschikbaar gestelde portaal. Vervolgens wordt door een algoritme bepaald welke bestellingen de bezorger aangeboden krijgt om op te halen en te bezorgen. Voor het afleveren van een bestelling keert Deliveroo gemiddeld € 5 uit aan de bezorger. In deze zaak stelt vakbond FNV, de vakbond die opkomt voor de belangen van werknemers op het gebied van werk en inkomen, dat de bezorgers van Deliveroo werken op basis van een arbeidsovereenkomst.

4. Gerechtshof Amsterdam 16 februari 2021, ECLI:NL:GHAMS:2021:392.

Het arrest

Het gerechtshof Amsterdam gaat in op de verschillende elementen van de arbeidsovereenkomst. Daarbij wordt vastgesteld dat allereerst sprake is van 'arbeid'. In het arrest wordt daarnaast besproken dat Deliveroo het mogelijk maakt dat een bezorger zich kan laten vervangen door een ander. Dit staat de kwalificatie van een arbeidsovereenkomst niet in de weg omdat ook een werkgever toestemming kan geven aan een werknemer om zich te laten vervangen.

Ten tweede wordt ingegaan op het element 'loon'. De bezorger ontvangt een bepaalde vergoeding van Deliveroo. De hoogte van deze vergoeding wordt eenzijdig bepaald door het platform. Deliveroo keert deze vergoedingen eens per twee weken uit zonder dat de bezorger hiervoor een factuur hoeft te sturen. De bezorger hoeft daarnaast geen omzetbelasting af te dragen, waardoor het voor hem eerder hobbymatig voelt dan dat hij een echte ondernemer is. De beloning die de bezorger verkrijgt is ontoereikend om daarmee verzekeringen af te sluiten. Verder speelt mee dat Deliveroo een vergoeding uitbetaalt tijdens ziekte.

Tot slot wordt het element 'in dienst van' besproken waarbij gekeken wordt of sprake is van een zekere gezagsverhouding. Voor het werk als maaltijdbezorger geeft het hof aan dat niet veel instructies nodig zijn. Dit betekent niet dat geen sprake is van gezag. Het hof benoemt dat de vrijheid van een bezorger om een precieze route te bepalen gering is, omdat een bezorger meestal kiest voor de snelste route. Dit doet hij mede gelet op het feit dat Deliveroo middels een GPS-tracker de bezorger in de gaten kan houden. Dit kan eventueel weer invloed hebben op het algoritme van Deliveroo en welke bezorgdiensten de bezorger krijgt aangeboden.

Op basis van bovenstaande omstandigheden concludeert het hof dat de bezorgers van Deliveroo werkzaam zijn op grond van een arbeidsovereenkomst.

Vallen taxichauffeurs van Uber onder de CAO-Taxivervoer?

De tweede zaak is de Uber-zaak.[5] Uber is een partij die – zo zeggen zij zelf – bemiddelt tussen chauffeurs en klanten via de Uber-app. Daarmee is de dienst die de chauffeurs uitvoeren vergelijkbaar met taxivervoer. De chauffeur kan inloggen via de Uber-app en krijgt vervolgens ritten aangeboden door middel van een

algoritme. In de app kan de chauffeur alvorens hij/zij de rit accepteert of weigert, onder meer zien hoelang de rit duurt, waar hij de passagier moet ophalen en wat de *rating* is van de passagier. Als een chauffeur inlogt in de app en drie keer achter elkaar een aangeboden rit negeert, wordt hij automatisch uitgelogd. Een chauffeur die een rit accepteert kan deze daarna ook nog annuleren. Als de chauffeur meer dan 20 procent van de geaccepteerde ritten vervolgens annuleert, kan Uber de toegang tot de Uber-app aan de chauffeur weigeren.

5. Rechtbank Amsterdam 13 september 2021, ECLI:NL:RBAMS:2021:5029.

Voor elke uitgevoerde rit krijgt de Uber-chauffeur een bepaald percentage van de ritprijs. De passagier betaalt in eerste instantie aan Uber. Uber Pay zorgt er vervolgens voor dat het toegekende bedrag wordt uitbetaald. Het bedrag wordt elke week (of soms elke dag) overgemaakt aan de chauffeur.

In deze zaak stelt vakbond FNV dat Uber-chauffeurs onder de CAO-Taxivervoer vallen. Voor deze vraag moet eerst worden gekeken of chauffeurs een arbeidsovereenkomst hebben met Uber.

De uitspraak

Volgens de rechtbank Amsterdam vormen de vervoerdiensten de kern van de activiteiten van Uber. De chauffeur dient akkoord te gaan met de voorwaarden van Uber indien hij ritten wil uitvoeren via de Uber-app. Hij moet de arbeid persoonlijk verrichten en hiervoor vraagt het platform om een *selfie* te maken ter controle. De chauffeur is gebonden aan de Uber-app om personen te kunnen vervoeren.

Verder krijgt de chauffeur zijn loon uitbetaald in de vorm van een ritprijs. De rechtbank geeft aan dat het niet uitmaakt hoe het loon wordt genoemd en dat niet Uber zelf, maar Uber Pay dit uitbetaalt.

Daarnaast zijn de voorwaarden waaronder de chauffeur ritten moet uitvoeren niet onderhandelbaar. Bij wijzigingen kunnen chauffeurs deze dan ook niet weigeren als zij willen blijven rijden via Uber. Wat ook meespeelt is dat de ritprijs vaststaat voor de voorgestelde route, omdat chauffeurs anders van passagiers een negatieve *rating* krijgen. Daarmee verkrijgt het ratingsysteem een disciplinerende werking. Tot slot leidt het niet oppakken of annuleren van ritten tot uitsluiting van de app. Daarmee zit Uber dus eigenlijk aan de knoppen van de app. De rechtbank geeft aan dat hier sprake is van een 'moderne gezagsverhouding' en beslist dat door de samenhang van de feitelijkheden de overeenkomst in wezen een arbeidsovereenkomst is.

Het klassieke begrip 'arbeidsovereenkomst' kan niet ontweken worden

De twee aangehaalde zaken laten zien dat veel omstandigheden een rol spelen bij de kwalificatie van een arbeidsovereenkomst. Onzes inziens vat de rechtbank Amsterdam het in de Uber zaak goed samen. Op platformen is een nieuwe vorm van gezagsverhouding ontstaan, maar dit betekent niet dat daarmee het klassieke begrip 'arbeidsovereenkomst' ontweken kan worden. De trend die daarbij opvalt is dat rechters platformarbeiders onder het beschermingsregime van het arbeidsrecht laten vallen. Over dit onderwerp zal het laatste woord nog niet geschreven zijn, maar het is zeker een ontwikkeling om in de gaten te blijven houden.

“Ik vond de opleiding prettig en gestructureerd. De docenten kwamen kundig en goed voorbereid op mij over. Er was ruimte voor vragen en we werden goed verzorgd. Al met al vind ik het een top opleiding die ik zeker zal aanraden!”

Danielle Putman
Letselschadejurist bij Brunel
Deelnemer opleiding
ICT-jurist 2020/2021

ICTRecht Academy biedt u een praktijkgerichte opleiding tot ICT-jurist op twee niveaus:

ICT-jurist
ICT-jurist: de verdieping

In één jaar (start april 2022) doet u gespecialiseerde juridische én technische kennis op over het ICT-vakgebied. U leert onder meer over: ICT-contracten, platforms en tussenpersonen, softwarerecht, AI, privacy en persoonsgegevens en ICT-security.

Kijk voor meer informatie op:
ictrecht.nl/opleiding-ict-jurist

Enkel geïnteresseerd in het opdoen van alomvattende kennis en skills over privacy en recht? Volg onze opleiding tot allround privacy jurist.

Kijk voor meer informatie op:
ictrecht.nl/opleiding-allround-privacy-jurist

NEDERLANDSE ORDE VAN ADVOCATEN

iapp CPE credits approved

Marjolein Struik
Juridisch adviseur

Cloud E-commerce Privacy

Onrechtmatige informatie op het internet: wie stelt u aansprakelijk?

Stelt u zich eens voor dat u een socialmedia-website beheert waarop gebruikers door het plaatsen van video's hun dagelijks leven kunnen delen met de rest van de wereld. Dit is tegenwoordig zo normaal dat de bezoekersaantallen al snel oplopen en daarmee de video's die dagelijks geüpload worden ook. Maar wat doet u als blijkt dat een van de gebruikers een auteursrechtelijk beschermde video op de website uploadt, zonder toestemming van de auteursrechthebbende, en de auteursrechthebbende hierdoor meent schade te lijden? De auteursrechthebbende zal hiervoor schadevergoeding willen vorderen. Vanwege de anonimiteit op het internet zal de auteursrechthebbende veelal niet beschikken over de persoonsgegevens van de inbreukmakende gebruiker, waardoor een vordering instellen lastig wordt. Kan de auteursrechthebbende in dit geval de websitebeheerder aansprakelijk stellen voor deze mogelijk illegale video? En zo niet, kan de websitebeheerder dan worden verplicht om de persoonsgegevens van de inbreukmakende gebruiker af te staan, zodat de auteursrechthebbende een vordering kan instellen tegen deze gebruiker?

Aansprakelijkheid van providers

Wanneer inbreuk wordt gemaakt op iemands rechten door het plaatsen van onrechtmatige informatie op bijvoorbeeld een website, zal moeten worden bepaald wie hiervoor aansprakelijk is. Een rechthebbende zal immers de vermeende schade die hij hierdoor heeft geleden vergoed willen zien. Omdat via het internet veelal anoniem informatie wordt geplaatst, zal de rechthebbende zich hiervoor in eerste instantie richten tot de beheerder van een website of de webhoster, die vallen onder de algemene noemer provider. Providers zijn tussenpersonen die informatie van anderen opslaan of doorgeven. De E-commerce richtlijn (Richtlijn inzake elektronische handel 2000/31/EG) kent een beperking van aansprakelijkheid voor providers met betrekking tot de opgeslagen of doorgegeven informatie. Deze beperking van aansprakelijkheid is in Nederland uitgewerkt in artikel 6:196c van het Burgerlijk Wetboek ('BW'). De aansprakelijkheidsbeperking is belangrijk, omdat het voor providers onmogelijk is om alle content vooraf te screenen. Daarnaast moet het internet vrij en toegankelijk zijn voor het delen van informatie, zonder dat een provider zich met deze informatie bemoeit. Om onder deze aansprakelijkheidsbeperking te kunnen vallen is het van belang dat een provider zich passief opstelt. De wet onderscheidt twee verschillende soorten providers die zich kunnen beroepen op de beperking van aansprakelijkheid voor schade als gevolg van het plaatsen van onrechtmatige informatie door gebruikers:

Beperking van aansprakelijkheid van de access provider

Een access provider is de schakel tussen de gebruiker van het internet en de informatie die vervolgens gevonden wordt. Access providers bieden toegang tot een communicatienetwerk of geven enkel informatie door dat afkomstig is van een ander. Een voorbeeld van een access provider is de klassieke internetprovider. Op grond van de wet is een access provider in beginsel niet aansprakelijk voor de doorgegeven informatie, mits de access provider geen actieve rol speelt bij het uitwisselen van informatie. Voorwaarde hiervoor is dat een access provider geen initiatief neemt tot het doorgeven van de informatie en ook niet bepaalt aan wie de informatie wordt doorgegeven. Daarnaast mag een access provider de informatie niet zelf selecteren of wijzigen. Om zich dus op de beperking van aansprakelijkheid te kunnen beroepen moet een access provider slechts als doorgeefluik fungeren.[1]

1. Artikel 12 E-commerce richtlijn en artikel 6:196c lid 1 Burgerlijk Wetboek.

Bij het doorgeven van informatie is het onvermijdelijk dat er tijdelijke kopieën van die informatie worden opgeslagen, wat ook wel caching wordt genoemd. Een access provider is dan ook niet aansprakelijk voor deze tijdelijke kopieën van informatie, indien deze slechts zijn bedoeld voor het doorgeven van informatie en wanneer deze kopieën niet langer dan nodig worden bewaard. Hierbij is het wederom van belang dat een access provider de doorgegeven informatie niet selecteert of wijzigt.[2]

2. Artikel 13 E-commerce richtlijn en artikel 6:196c lid 3 Burgerlijk Wetboek.

Aansprakelijkheid van de hosting provider

Een hosting provider slaat informatie van een ander op en geeft deze informatie door wanneer anderen daarom vragen. Een voorbeeld van een hosting provider is een webhosting dienst. Maar ook een hobbyforum waarop mensen knutselideeën kunnen uitwisselen valt onder de noemer hosting provider. Het kan voorkomen dat een gebruiker van een website daarop onrechtmatige informatie plaatst. Een hosting provider kan in theorie alle informatie die op de website wordt geplaatst checken op onrechtmatigheid, voordat het wordt opgeslagen en doorgegeven. In de praktijk zou dit echter veel tijd en moeite kosten en daarnaast moet het internet vrij en toegankelijk zijn voor het delen van informatie, zonder dat een hosting provider zich met deze informatie bemoeit. Een hosting provider is daarom niet aansprakelijk voor informatie opgeslagen door derden indien zij niet weet, of redelijkerwijs niet behoorde te weten, van de onrechtmatige informatie. Wanneer een hosting provider op de hoogte wordt gesteld van onrechtmatige informatie, dient de hosting provider deze onrechtmatige informatie te verwijderen.[3] Deze procedure wordt ook wel notice-and-takedown genoemd.

3. Artikel 14 E-commerce richtlijn en artikel 6:196c lid 4 Burgerlijk Wetboek.

Het verstrekken van NAW-gegevens door een provider

Zoals uit het voorgaande blijkt kan een provider niet altijd aansprakelijk gesteld worden voor onrechtmatig geplaatste informatie. Een andere mogelijkheid is degene die de informatie geplaatst heeft hiervoor aansprakelijk te stellen, zoals de plaatser van de auteursrechtelijk beschermde video uit de inleiding. Vaak is het op een website niet direct duidelijk wie bepaalde informatie heeft geplaatst en om een vordering tegen iemand in te kunnen stellen zijn echter wel naam en contactgegevens nodig. De provider beschikt over het algemeen over de gegevens van zijn klanten. In een dergelijk geval kan de provider klem komen te zitten tussen de rechthebbende die de schade vergoed wil zien en de klant waarvan zijn of haar privacy beschermd moet worden. In sommige gevallen kan een provider echter verplicht worden om de NAW-gegevens af te staan van de klant die de onrechtmatige informatie heeft geplaatst.

De wet schrijft geen verplichting aan providers voor tot afgifte van persoonsgegevens van klanten. In de jurisprudentie zijn echter wel richtlijnen te vinden over afgifte van persoonsgegevens, die in de volgende alinea's worden besproken.

De zorgplicht uit het Lycos/Pessers-arrest

In het Lycos/Pessers arrest uit 2005[4] bepaalde de Hoge Raad aan de hand van een aantal criteria dat een provider verplicht was om NAW-gegevens af te geven aan eiser. De Hoge Raad overwoog dat het kan voorkomen dat er op een website onrechtmatige informatie aanwezig is, die jegens een derde onrechtmatig kan zijn en waardoor deze derde schade kan lijden. In dit arrest werd bepaald dat wanneer dit het geval is, het ongewenst zou zijn indien deze derde geen reële mogelijkheid heeft om de provider daarop aan te kunnen spreken. Indien de provider weigert om de NAW-gegevens van diegene die inbreuk maakt te verstrekken aan een derde, dan kan dit onder bepaalde omstandigheden in strijd zijn met de zorgvuldigheid die de provider jegens een derde in acht moet nemen. In dit arrest werd bepaald dat aan een viertal vereisten moet worden voldaan om een provider tot afgifte van persoonsgegevens van de klant te dwingen:

a) de mogelijkheid dat de informatie, op zichzelf beschouwd, jegens de derde onrechtmatig is, is voldoende aannemelijk;
b) de derde heeft een reëel belang bij de verkrijging van de NAW-gegevens;
c) aannemelijk is dat er in het concrete geval geen minder ingrijpende mogelijkheid bestaat om de NAW-gegevens te achterhalen;
d) afweging van de betrokken belangen van de derde, de serviceprovider en de websitehouder (voor zover kenbaar) brengt mee dat het belang van de derde behoort te prevaleren.

4. Hoge Raad, 25 november 2005, ECLI:NL:HR:2005:AU4019.

In het Promusicae-arrest[5] van het Europese Hof van Justitie is het bovenstaande bevestigd. In dit arrest werd bepaald dat Europese landen geen verplichtingen aan providers mogen opleggen om persoonsgegevens van hun klanten af te geven, noch mogen er regels worden opgesteld dat afgifte van persoonsgegevens altijd in strijd is met het privacyrecht van de klant. De afgifte van persoonsgegevens zal derhalve moeten afhangen van de betrokken belangen en er zal een juist evenwicht moeten worden gezocht tussen de betrokken grondrechten.

5. Hof van Justitie van de Europese Unie, 29 januari 2008, C-275/06.

Afgifte van NAW-gegevens en de Algemene verordening gegevensbescherming

De vraag rijst of de criteria uit het Lycos/Pessers arrest nog wel kunnen rijmen met de vereisten uit de Algemene verordening gegevensbescherming ('AVG'). Overeenkomstig de AVG mogen persoonsgegevens namelijk slechts worden verwerkt op basis van een van de zes grondslagen genoemd in de AVG. Deze grondslag kan worden gevonden in artikel 6 lid 1 onder f AVG. De verplichting tot afgifte van persoonsgegevens kan voortvloeien uit het gerechtvaardigd belang van de provider om het verspreiden van onrechtmatige informatie te bestrijden.[6] Ook in de uitspraak DFW/Ziggo uit 2019[7] gaat het Hof in op deze belangenafweging. Het Hof oordeelt dat Ziggo slechts tot afgifte van persoonsgegevens kan worden verplicht indien a) er sprake is van een gerechtvaardigd belang, b) de verwerking noodzakelijk is en c) het belang van DFW prevaleert boven het belang van de klanten van Ziggo. Mijns inziens rijmen de criteria uit het Lycos/Pessers arrest derhalve met de AVG, de criteria uit het arrest schrijven immers ook een belangenafweging voor. Wanneer de op grond van de AVG vereiste belangenafweging wordt uitge-

voerd, zouden naar mijn mening hierin de criteria uit het Lycos/Pessers arrest moeten worden meegenomen. Het is overigens niet uitgesloten dat de afgifte van NAW-gegevens op een andere grondslag uit de AVG kan worden gebaseerd, maar in de rechtspraak wordt de afgifte over het algemeen gebaseerd op de grondslag gerechtvaardigd belang.

6. Zie ook: Parket bij de Hoge Raad, 29 januari 2021 en ECLI:NL:PHR:2021:83 en Rechtbank Den Haag, 17 maart 2021, ECLI:NL:RBDHA:2021:2422.
7. Gerechtshof Arnhem-Leeuwarden, 5 november 2019, ECLI:NL:GHARL:2019:9352.

Slotsom

Concluderend bestaan er, in het geval er sprake is van een inbreuk, voor een rechthebbende verschillende wegen om zijn aangetoonde schade vergoed te krijgen. De rechthebbende kan hiervoor de provider aansprakelijk stellen, welke zich echter op de wettelijke aansprakelijkheidsbeperking kan beroepen mits de provider zich passief opstelt. Er bestaat dan nog een mogelijkheid om een vordering in te dienen bij degene die de onrechtmatige informatie heeft geplaatst. Omdat hiervoor NAW-gegevens zijn vereist, kan een provider onder bepaalde omstandigheden worden verplicht om de NAW-gegevens van die persoon af te staan.

Sten Demon
Legal consultant

Koen van Jaarsveld
Legal consultant

Innovatie

Wat is legal operations?

Jarenlang was de juridische afdeling een enigszins mysterieuze plek en fungeerde de jurist als een alwetende poortwachter met uiterst genuanceerde, soms onnavolgbare, adviezen. Hier is inmiddels verandering in gekomen. Het juridische landschap is aan het bewegen en van de jurist wordt tegenwoordig andere dingen verwacht dan voorheen. Zelf zien we ook dat organisaties steeds meer de behoefte krijgen om de rol van legal te verschuiven van laatste obstakel naar eerste aanspreekpunt.

Ontstaan legal operations

Legal is een laatbloeier als het gaat om verandering. Waar afdelingen als Finance, HR, en IT al veel langer vanuit een operations-gedachte werken, bleef legal lang vasthouden aan een meer traditionele functie in organisaties. Deze traditionele functie zag voornamelijk op het inhoudelijk adviseren van de organisatie met betrekking tot juridische vraagstukken en had een sterk reactief karakter. Sinds de financiële crisis van 2008 worden er strengere eisen gesteld aan de kosten voor juridische afdelingen. Hierdoor komt er steeds meer nadruk te liggen op het efficiënt uitvoeren van werkzaamheden binnen legal. Dit heeft ervoor gezorgd dat de noodzaak is ontstaan tot optimalisatie over te gaan en steeds slimmer te gaan werken. De methodiek die dit mogelijk maakt wordt legal operations genoemd.

Doel legal operations

Legal operations, ook wel legal ops genoemd, staat voor de discipline die gericht is op het optimaliseren van de juridische afdeling. Het doel hiervan is om legal zo in te richten dat de hindernissen worden weggenomen die het juristen moeilijk maken om hun werk te doen. Door deze optimale inrichting van legal krijgen juristen meer gelegenheid om hun tijd te besteden aan hoogwaardige juridische taken. Of zoals wij samengevat zeggen: legal operations maakt organisaties efficiënter, sneller, goedkoper en inhoudelijk beter.

De te realiseren efficiëntie binnen legal is voor de meeste organisaties, juristen en managers nu misschien nog een droom. Welke jurist wil nou niet meer tijd hebben om in complexe materie te duiken in plaats van eenvoudige (administratieve) werkzaamheden? En welke manager wil er nou geen grip hebben op de kosten en het functioneren van legal? Kortom allemaal winnaars bij het juist uitvoeren van legal operations. Maar daar zit direct de crux: het juist uitvoeren van legal operations. Dit is specialistisch werk en dient systematisch te gebeuren.

CLOC-model

Er zijn verschillende manieren om met legal operations aan de slag te gaan. Het Corporate Legal Operations Consortium (CLOC) heeft een model ontwikkeld met twaalf kerncompetenties op het gebied van legal

operations. Het model biedt een overzicht van de verschillende competenties binnen het verzamelbegrip legal operations. ICTRecht gebruikt dit model om te inventariseren hoe een organisatie op verschillende juridische vlakken presteert en om vervolgens te adviseren over optimalisatie.

Hieronder worden de twaalf kerncompetenties van het CLOC-model beschreven. Houd er rekening mee dat elke organisatie anders is en de ene competentie daarom misschien relevanter kan zijn dan de andere. Elke organisatie heeft zo zijn eigen verbeterpunten.

1. Business intelligence

Business intelligence is niet nieuw. Bij veel organisaties en binnen verschillende afdelingen wordt dit al veelvuldig toegepast. De juridische afdeling loopt hier in het algemeen op achter. Juristen focussen zich op de inhoudelijke juridische vraagstukken die worden voorgelegd en maken weinig gebruik van de processuele data. Als u bijvoorbeeld vraagt hoeveel NDA's afgelopen kwartaal zijn beoordeeld, dan kan hier geen antwoord op gegeven worden. Dit is zonde, want met dergelijke data kunt u sturen op verbetering.

2. Financial management

Juristen worden vaak gezien als kostenpost. Daarnaast zijn de meeste juristen geen rekenwonders. De budgetten vanuit legal worden regelmatig overschreden. Dit kan relatief eenvoudig verbeterd worden. Bijvoorbeeld door samen met de financiële afdeling meer inzichten te genereren in de uitgaven van de juridische afdeling. Maar ook door inzicht te generen in de waarde die vanuit legal juist is toegevoegd aan de organisatie. Denk aan de geboden juridische ondersteuning bij een grote deal. Met dergelijke gegevens en inzichten kan er beter gepland en gebudgetteerd worden. Tevens is dit het fundament om te sturen op kostenefficiëntie.

3. Firm and vendor management

Het managen van leveranciers wordt al door veel organisaties gedaan. Met name de grotere ondernemingen hebben hier beleid of zelfs een aparte afdeling voor. Hoe zit het echter met de leveranciers die de juridische afdeling inschakelt? We zien regelmatig dat externe ondersteuning wordt ingeschakeld op basis van gevoel of verleden in plaats van objectieve criteria. Daarnaast wordt expertise ingekocht bij kantoor X vanwege persoonlijke voorkeuren, in plaats van bij het kantoor met de beste prijs-kwaliteitverhouding.

4. Information governance

Informatie en kennis is het meest waardevolle bezit van een juridische afdeling. Toch hebben weinig juridische afdelingen een concreet beleid voor het managen van informatie. Welke informatie heeft de afdeling? Wie moet hier toegang tot hebben? Hoe en hoelang wordt bepaalde informatie bewaard? Veel juridische afdelingen hebben deze inzichten niet en dat leidt tot risico's. Het meest voorkomende risico is het herhalen van een kostbare inhoudelijke exercitie omdat informatie niet meer gevonden kan worden.

5. Knowledge management

Op het gebied van kennismanagement valt er veel winst te behalen. Organisaties groeien en wanneer er te veel werk ligt voor een jurist, wordt er nog een aangenomen die op een eigen eilandje of met een eigen expertise aan de slag gaat. Juristen duiken in complexe vraagstukken, zonder hun kennis goed vast te leggen of te delen. Dit leidt niet alleen tot risico's, maar ook tot onnodige kosten en vertragingen binnen de organisatie. Door kennismanagement goed in te richten kan iedere medewerker ongeacht eigen kennis of ervaring van de organisatie enorm veel waarde toevoegen. Tevens voorkomt het dat kennis onnodig verloren gaat wanneer iemand vertrekt of uitvalt.

6. Organization, optimization and health

Als general counsel streeft u natuurlijk naar een effectieve en gemotiveerde juridische afdeling. Dit kunt u alleen bereiken als de juiste personen op de juiste plek zitten. Maak dit daarom bespreekbaar. Wie heeft welke ambities en talenten? Zijn de juristen tevreden of moet er verandering komen? Laat u hierin niet leiden door korte termijn doelen. Ja het is nu druk, maar is het daadwerkelijk verstandig om het contract met deze jurist te verlengen? Door hier goed op te sturen, kunt u een efficiënt team opbouwen.

7. Practice operations

Als bedrijfsjurist heeft u veel verschillende petten op en houdt u u bezig met veel verschillende rechtsgebieden. Meestal ontstaat dit uit noodzakelijkheid en is het bijvoorbeeld niet efficiënt om bepaalde taken door een stagiair uit te laten voeren omdat u dan alsnog veel nakijkwerk heeft. Het gevolg is dat we regelmatig zien dat bedrijfsjuristen te veel tijd steken in een onderwerp buiten hun expertise of zich zelfs bezighouden met werkzaamheden die meer administratief van aard zijn dan juridisch. Door

taken op de juiste plek te beleggen of te automatiseren met legal tech, kan de jurist focussen op de complexere juridische vraagstukken en zo efficiënt mogelijk werken.

8. Project / program management

Juristen hebben veelal een adviserende rol binnen projecten. Iemand anders leidt het project en zorgt ervoor dat doelen behaald worden. Dit is niet vreemd, projectmanagement is tenslotte een andere expertise. Toch zien we bij veel organisaties de verwachting dat de jurist ook projectmanagement doet. Met name als het gaat om projecten met een juridische inslag, zoals het implementeren van nieuwe wetgeving of het leiden van een fusie. Het gevolg is dat er inefficiënt gewerkt wordt en projecten rommelig verlopen. Door de juristen te trainen in projectmanagement of ervaren projectmanagers te koppelen aan de juridische afdeling, kunnen projecten tot een goed einde worden gebracht zonder te veel effectiviteit te verliezen van de juristen.

9. Service delivery models

Bedrijfsjuristen zijn interne dienstverleners. De juridische afdeling helpt de organisatie bij juridische vraagstukken en ondersteunen afdelingen met compliance. Binnen grote organisaties wordt de juridische afdeling vaak met gelijksoortige vragen bestookt. Hier gaat veel werk in zitten en kan praktischer. Is er bijvoorbeeld nagedacht over hoe de juridische afdeling benaderd kan of mag worden? Beantwoordt de juridische afdeling telkens dezelfde soort vragen of is er ook al nagedacht over hetgeen de andere afdelingen zelf kunnen (self service)?

10. Strategic planning

Vrijwel iedere juridische afdeling heeft met elkaar gemeen dat er gewerkt wordt in de waan van de dag. Vandaag staan deze afspraken en moeten deze vraagstukken afgerond worden. Het grote plaatje raakt snel uit beeld, waardoor er op directieniveau onvoldoende rekening gehouden kan worden met de ambities van de juridische afdeling en andersom. Daarnaast ontstaat er niet een cyclus van continue verbetering, maar blijven pijnpunten lang doorzeuren en loopt de afdeling telkens tegen dezelfde problemen aan. Door een goede strategische planning kan dit voorkomen worden.

11. Technology

Wat tegenwoordig niet mag ontbreken is technologie. Nu is het niet de bedoeling om direct allerlei innovatieve oplossingen aan te schaffen, maar het is wel noodzakelijk om te starten met een digitale strategie. Welke oplossingen bestaan er? Wat zijn de behoeften van de afdeling? Welke stappen willen we de komende drie jaar maken als afdeling binnen een organisatie en welke technologieën sluiten hierop aan? Het inzetten van de juiste technologie kan enorm veel efficiëntie opleveren en risico's verminderen. Met name administratieve en repetitieve taken waar juristen zich mee bezig houden kunnen goed geautomatiseerd worden.

12. Training and development

Stilstaan is achteruitgaan. Dit geldt ook voor juridische afdelingen die geen beleid hebben rondom het trainen en verbeteren van de juristen. Is er nagedacht over hoe nieuwe medewerkers het beste ingewerkt kunnen worden? Hoe houden deze personen vervolgens hun kennis op peil en verbeteren ze hun vaardigheden? Ook dit zijn belangrijke onderwerpen om rekening mee te houden als u een effectief en gemotiveerde juridische afdeling wil neerzetten en behouden.

Concluderend

Juridisch werk kan meestal efficiënter, sneller, goedkoper en inhoudelijk beter. Om een effectieve juridische afdeling neer te zetten, moet er verder worden gekeken dan de juridische inhoud. De afdeling zal aan de slag moeten met legal operations en de twaalf kerncompetenties van het CLOC-model geven hierbij houvast. Legal operations is essentieel om de juridische afdeling zoveel mogelijk waarde te kunnen laten toevoegen aan een organisatie.

ICTRECHT
legal tech

Maak uw juridische afdeling toekomstbestendig met legal tech

Legal tech staat voor de technologie die juridische taken versimpelt of compleet automatiseert. Het stelt organisaties in staat om juridische werkprocessen efficiënter in te richten. Uw organisatie kan zo tijd besparen, de werkdruk verminderen en tegelijkertijd meer juridische waarde creëren. Ervaren wat de juiste technologie kan betekenen voor uw juridische processen? ICTRecht helpt organisaties innoveren met behulp van legal tech.

Lees meer op:
ictrecht.nl/legal-tech

Arnoud Engelfriet
Algemeen directeur / Opleidingsdirecteur

Internetrechtspraak

Haatdragende reacties op Facebookpost

(Europees Hof voor de Rechten van de Mens 2 september 2021)

Aanhangers van de Franse politicus Julien Sanchez hadden in 2011 haatdragende reacties geschreven onder een bericht op zijn openbare Facebookprofiel. De berichten werden door Sanchez niet verwijderd, maar hij postte wel een bericht waarin stond dat gebruikers de inhoud van hun opmerkingen moesten controleren en matigen. De Franse rechtbank overwoog dat de beledigende commentaren aan Sanchez kunnen worden toegerekend, alsof hij deze zelf heeft geschreven. Sanchez vond dat zijn mensenrechten hierdoor waren geschonden (op basis van artikel 10 EVRM). Dit omdat het niet zijn commentaren waren en een post had geplaatst met een verzoek naar de gebruikers. Het EHRM is het eens met de veroordeling. Sanchez had moeten modereren wat derden op zijn pagina zeiden. Vooral omdat hij een bericht over een politieke tegenstander had geplaatst en hij dus kon verwachten dat hierop heftige reacties kwamen.

https://bit.ly/32FwGsx

Omvang bescherming BOB "Champagne"

(Hof van Justitie EU 9 september 2021)

GB maakt gebruik van het teken CHAMPANILLO. CIVC behartigt de belangen van champagneproducenten. Zij wijzen GB erop dat inschrijving van dit teken onverenigbaar is met de Beschermende oorsprongsbenaming (BOB) "Champagne". GB stelt dat het gebruik van het teken geen gevaar oplevert voor verwarring met producten waarop de BOB "Champagne" betrekking heeft en dat hij niet de bedoeling heeft om de reputatie van BOB "Champagne" uit te buiten. De vraag die het Hof van Justitie moet beantwoorden is of de omvang van BOB "Champagne" ook bescherming mogelijk maakt voor niet-soortgelijke producten. Het Hof antwoordt daarop bevestigend. Ook stelt het Hof dat de reputatie van het BOB "Champagne" wordt beschermd en dat diensten die hier enigszins mee te maken hebben ook onder de bescherming vallen. Het BOB "Champagne" beschermt dus tegen handelingen die betrekking hebben op zowel diensten als producten.

https://bit.ly/31cvQms

Uber is een werkgever

(Rechtbank Amsterdam 13 september 2021)

Uber biedt taxichauffeurs de mogelijkheid om taxiritten aangeboden te krijgen via het Uber-platform. De passagier betaalt Uber en Uber betaalt wekelijks de chauffeur. FNV behartigt belangen van werknemers. Zij hebben Uber aangesproken op het naleven van de CAO Taxivervoer. Uber heeft dat geweigerd, omdat – volgens Uber – de chauffeurs geen werknemers zijn, en dat ook niet worden doordat zij de Uberapp gebruiken. Uber zegt daarnaast dat zij geen werkgever is, maar een technologiebedrijf is dat een platform runt. De rechtbank oordeelt echter dat Uber wel een werkgever is. Dit omdat het samenstel van het door Uber opgetuigde systeem ertoe leidt dat de feitelijke uitvoering alle kenmerken van een arbeidsovereenkomst bevat. Hierdoor moet de overeenkomst tussen Uber en de chauffeurs worden gekwalificeerd als een arbeidsover-

eenkomst. Uber is hierdoor verplicht om de bepalingen van de CAO Taxivervoer na te leven ten opzichte van de chauffeurs die zich in persoon met Uber hebben verboden. Zie ook het artikel op pagina 12.

https://bit.ly/3xDIB5I

Datadiefstal GGD

(Rechtbank Midden-Nederland 14 september 2021)
Twee mannen zijn schuldig bevonden aan datadiefstal uit een GGD-systeem. De rechtbank Midden-Nederland heeft het tweetal tot een (deels voorwaardelijke) gevangenisstraf veroordeeld. De twee werkten voor het callcenter van de GGD en planden coronatesten in. Begin dit jaar raakte de GGD op de hoogte van een mogelijk datalek. Persoonsgegevens uit het GGD-systeem werden namelijk online verkocht. Uit onderzoek bleek dat één van de mannen de gegevens verkocht en de andere man in het GGD-systeem naar gegevens zocht en deze via WhatsApp naar een vriend stuurde. De gegevens waren onder andere van twee misdaadjournalisten, die ernstig worden bedreigd. De rechtbank is dan ook van oordeel dat er sprake is van een ernstige inbreuk op de privacy. De man die gegevens te koop aanbood, is veroordeeld tot een straf van tien maanden waarvan vijf voorwaardelijk. De andere man krijgt een gevangenisstraf van 60 dagen, waarvan 34 dagen voorwaardelijk, opgelegd en een taakstraf voor de duur van 180 uur.

https://bit.ly/32zG0y7

Elektronisch geleverde software is een goed

(Hof van Justitie EU 16 september 2021)
Het Europees Hof van Justitie heeft twee vragen van het High Court of Justice beantwoord. The Software Incubator handelde voor rekening van Computer Associates om potentiële klanten in het VK en Ierland te benaderen om de software van Computer Associates te promoten, in de handel te brengen en te verkopen. De vraag die tussen beide speelde was of The Software Incubator een handelsagent was en dus recht had op een schadevergoeding na beëindiging van de overeenkomst. De vragen die het High Court of Justice hiervoor stelde waren: (1) Als computersoftware elektronisch wordt geleverd, valt dit dan onder 'goederen'? en (2) indien de software aan klanten van een principaal wordt geleverd door een licentie van onbepaalde tijd toe te kennen, valt dit dan onder 'verkoop van goederen'? Het Hof legt uit dat software als een goed kan worden aangemerkt en dat er sprake is van verkoop, aangezien bij het sluiten van de overeenkomst de IE-rechten van een kopie worden overgedragen. De vragen worden dus door het Hof bevestigend beantwoord.

https://bit.ly/3EfO712

Schoonmakers via Helping zijn uitzendkrachten

(Gerechtshof Amsterdam 21 september 2021)
Helping exploiteert een online platform waar schoonmakers en huishouders afspraken kunnen maken over het uitvoeren van huishoudelijke werkzaamheden. Een schoonmaker heeft zich ziekgemeld en bij Helping inlichtingen ingewonnen over mogelijk doorbetaling bij ziekte. Helping stelt dat er geen dienstverband is. FNV behartigt belangen van werknemers en zij stellen dat er sprake is van een arbeidsovereenkomst dan wel uitzendovereenkomst is tussen Helping en de schoonmakers. Het hof oordeelt dat er sprake is van een uitzendovereenkomst, waardoor de cao voor uitzendkrachten van toepassing is. De schoonmakers die via Helping werken hebben daarom recht op pensioen, vakantiegeld, doorbetaling bij ziekte en andere werknemersrechten.

https://bit.ly/31fbaKP

Jeugddetentie en leerstraf voor phishing en pakketfraude

(Rechtbank Amsterdam 21 september 2021)
De Rechtbank heeft geoordeeld dat de 15-jarige verdachte zich schuldig heeft gemaakt aan phising en pakketfraude. Dit omdat hij goederen bestelde via gekaapte webshop-accounts – welke door phising tot stand kwamen – en vervolgens zocht naar leegstaande woningen waarop de pakketjes konden worden bezorgd. Dit laatste wordt ook wel pakketfraude genoemd. Daarnaast stuurde hij deze adressen door naar andere leden van de organisatie. De tiener heeft

dus een uitvoerende als een faciliterende rol gehad ten aanzien van pakketfraude. Voor dit aandeel heeft de rechter de verdachte tot een jeugddetentie van 135 dagen, waarvan 90 voorwaardelijk, veroordeeld. Daarnaast is de leerstraf 'Tools4U Online Delicten' voor een duur van 25 uur opgelegd. Tools4U is een leerstraf voor jongeren in de leeftijd van 12 tot 23 jaar die één of meerdere delicten hebben gepleegd.

https://bit.ly/3o9C7sh

Digitaal versturen van aanmaningen

(Rechtbank Zeeland-West-Brabant 23 september 2021)

De rechtbank heeft geoordeeld dat de gemeente de aanslag gemeentelijke belasting rechtsgeldig bekend maakt als deze naar de mailbox van de belanghebbende wordt gestuurd en deze belanghebbende ervoor heeft gekozen om post van de gemeente digitaal te ontvangen. Het eventueel niet ontvangen van een e-mailnotificatie doet hier niet aan af. De wet voorziet namelijk in het digitaal verzenden van post, mits de belastingplichtige hiervoor toestemming geeft. Ook aanmaningen mag de gemeente digitaal versturen.

https://bit.ly/3paRKyY

LinkedIn tegen Van Haga

(Rechtbank Noord-Holland 6 oktober 2021)

Om gebruik te kunnen maken van het social media platform LinkedIn moeten gebruikers bij hun registratie een gebruikersovereenkomst sluiten met LinkedIn. Van Haga heeft op het platform berichten gedeeld waarin onder meer stond dat mondkapjes niet werken en de coronamaatregelen niet proportioneel zijn. Ook noemde hij een verkeerd sterftepercentage en heeft hij andere berichten gedeeld waarin misinformatie stond. Hierdoor is zijn account beperkt, omdat deze berichten in strijd zouden zijn met de gebruikersvoorwaarden van LinkedIn. Van Haga heeft hiertegen bezwaar gemaakt en geëist dat zijn profiel inclusief berichten moesten worden teruggeplaatst. De rechter oordeelt dat LinkedIn het beleid voor misinformatie op het platform nauwelijks heeft uitgeschreven in de gebruikersvoorwaarden. Ook heeft LinkedIn niet genoeg uitschreven waarom het bezwaar had tegen de berichten van Van Haga. Het account moet daarom binnen drie werkdagen worden teruggeplaatst, zo oordeelt de rechtbank. De verwijderde berichten blijven wel verwijderd en LinkedIn hoeft haar handelen niet te rectificeren.

https://bit.ly/3EaSVo7

Decompileren van computerprogramma's

(Hof van Justitie EU 6 oktober 2021)

Het Belgische softwarebedrijf Top System SA had in de end-user license agreement gezet dat de software niet mocht worden gedecompileerd. Software decompileren betekent dat de taal van de software waarin het is geschreven wordt veranderd in iets wat begrijpelijker is voor mensen. Selor, een Belgische openbare instelling, heeft het geleverde computerprogramma van Top System SA gedecompileerd. Dit heeft Selor gedaan om een bug op te lossen. Aan het Hof van Jusitie is de vraag gesteld of de rechtmatige verkrijger van een computerprogramma dit programma mag decompileren om fouten te verbeteren en zo ja, of er dan nog aan voorwaarden moet worden voldaan. Het Hof heeft geoordeeld dat de rechtmatige verkrijger van een computerprogramma het recht heeft een programma geheel of gedeeltelijk te decompileren om fouten te verbeteren. Er hoeft daarbij niet te worden voldaan aan enige voorwaarden.

https://bit.ly/3d1jJva

Webshop maakte geen back-ups

(Gerechtshof Arnhem-Leeuwarden 12 oktober 2021)

Eiser exploiteert een webshop en heeft met verweerder een overeenkomst gesloten over een koppeling tussen de webshop en het door haar gebruikte boekhoudprogramma van Exact Online. In 2018 werden de gegevens van de crediteuren overschreven door debiteurenboekingen. Verweerder heeft de koppeling aangepast, waarna de problemen zijn verholpen. Aangezien er geen back-up was, heeft eiser de overgeschreden data handmatig hersteld.

Deze kosten wil eiser vergoed zien van verweerder, omdat verweerder – volgens eiser – tekort is geschoten in de nakoming van de overeenkomst. In de algemene voorwaarden van verweerder staat echter dat klanten zelf verantwoordelijk zijn voor het regelmatig maken van back-ups. Dat eiser dit achterwege heeft gelaten, is aan eiser zelf toe te rekenen, aldus het hof. Daarnaast stellen de voorwaarden dat de verweerder in geen enkel geval aansprakelijk is voor de kosten van de verloren gegane gegevens. Het gerechtshof stelt eiser daarmee in het ongelijk.

https://bit.ly/3d1NNXJ

Functioneringsgesprek opnemen

(Rechtbank Noord-Holland 28 oktober 2021)

In een zaak tussen een werknemer van Blooming en de werkgever heeft de werkgever een verzoek gedaan om de arbeidsovereenkomst tussen partijen te ontbinden. Dit naar aanleiding van het functioneringsgesprek dat door de werknemer is opgenomen, zonder voorafgaande toestemming van de werkgever. De werkgever stelt om deze reden dat de werknemer verwijtbaar heeft gehandeld en dat daardoor de arbeidsverhouding is verstoord. De werknemer stelt ook dat de arbeidsverhouding is verstoord, maar dan vanwege ernstig verwijtbaar handelen of nalaten van Blooming. De rechtbank oordeelde dat er inderdaad sprake was van een verstoorde arbeidsverhouding en ontbind daarmee de overeenkomst. De rechter vindt echter niet dat het handelen van de werknemer ernstig verwijtbaar is. Een werknemer is namelijk gerechtigd een gesprek met zijn werknemer op te nemen, zelfs zonder voorafgaande toestemming. De werknemer hoeft alleen van tevoren te bevestigen dat hij het gesprek opneemt. Het bleek dat de werknemer dat laatste had gedaan.

https://bit.ly/3FVaYiw

Bescherming van (onder)delen van een model

(Hof van Justitie EU 28 oktober 2021)

Ferrari heeft haar topmodel FXX K voor het eerst aan het publiek gepresenteerd in een persbericht dat twee foto's bevatte waarop een zij- en vooraanzicht van dit voertuig te zien waren. Mansory Design verkoopt pakketten met montagestukken voor personalisatie die zijn bedoeld om de verschijningsvorm van een ander Ferrari-model te veranderen en op de Ferrari FXX K te laten lijken. Ferrari stelt dat Mansory Design een inbreuk maakt op Ferrari's niet-ingeschreven gemeenschapsmodellen die betrekking hebben op het model FXX K. Het Bundesgerichtshof heeft aan het Hof gevraagd of de beschikbaarheidstelling voor het publiek van afbeeldingen van een voortbrengsel met zich meebrengen dat een (onder)deel van het model een eigen karakter heeft. Het Hof antwoordt hierop dat de formele voorwaarde voor bescherming als niet-ingeschreven gemeenschapsmodel is dat dit model voor het publiek beschikbaar is gesteld. De beschikbaarstelling voor het publiek van afbeeldingen van het model in zijn geheel kan slechts de beschikbaarstelling van het model van een deel met zich brengen, indien bij die beschikbaarstelling de verschijningsvormen van dat deel duidelijk herkenbaar is. Daarnaast benadrukt het Hof dat het begrip 'eigen karakter' niet ziet op de verhouding tussen het model van een voortbrengsel en de modellen van de delen waaruit het voortbrengsel bestaat, maar op de verhouding tussen deze en andere, oudere modellen. Dit veronderstelt dat de verschijningsvorm van een (onder)deel op zichzelf een algemene indruk kan wekken en niet volledig opgaat in het voortbrengsel als geheel.

https://bit.ly/32FX3P7

Leerlingvolgsysteem

(Rechtbank Oost-Brabant 2 november 2021)

De ouders van minderjarige kinderen verzoeken de rechtbank om de voormalige basisschool van hun kind te bevelen om persoonsgegevens inzake de sociaal-emotionele ontwikkeling van hun kind te verwijderen, met inbegrip van de (gespreks)notities en aantekeningen zoals die in het leerlingvolgsysteem zijn opgeslagen. De rechtbank oordeelt dat de basisschool verplicht is een leerling- en onderwijssysteem te gebruiken. Dit staat in artikel 8 lid 6 van de Wet op het primair onderwijs. De basisschool heeft daarom een voldoende rechtsgrondslag voor het behouden van de persoonsgegevens van de kinderen.

https://bit.ly/3D65wrp

Camera's in appartement

(Rechtbank Amsterdam 9 november 2021)
De Vereniging van eigenaren (VvE) in een appartementsgebouw heeft een besluit genomen om een nieuw camerasysteem te plaatsen in het flatgebouw. De bewoonster is het daarmee niet eens en heeft de Autoriteit Persoonsgegevens gevraagd om handhavend op te treden tegen het betreffende besluit. Volgens de AP heeft de VvE een gerechtvaardigd belang, omdat de VvE op deze manier haar eigendommen kan beveiligen. Het bezwaar wordt daarom door de AP ongegrond verklaard, waardoor de bewoonster vervolgens beroep heeft ingesteld tegen het besluit van de AP. De rechtbank kijkt onder andere naar de rechtmatigheid van de besluitvorming, de proportionaliteit en subsidiariteit en of het belang van cameratoezicht prevaleert boven het privacyrecht van de bewoonster. Op basis daarvan oordeelt de rechtbank dat de besluitvorming door de VvE in 2012 rechtmatig is genomen, de manier van beveiliging van haar eigendommen door de VvE niet op een andere en minder ingrijpende manier kan worden gerealiseerd en dat het beveiligen van de eigendommen van de VvE zwaarder wegen dan het belang van de bewoonster ten aanzien van bescherming van haar privacy. De bewoonster wordt derhalve door de rechtbank in het ongelijk gesteld.

https://bit.ly/3xBeaNm

UBO-wetgeving

(Gerechtshof Den Haag 16 november 2021)
In deze zaak heeft het Gerechtshof Den Haag in een kort geding procedure uitgemaakt dat de UBO-wetgeving niet buiten werking hoeft te worden gesteld. De UBO-wetgeving is in september 2020 in werking getreden naar aanleiding van de Europese anti-witwas richtlijn. Op basis van deze wetgeving is het voor een vennootschap verplicht om een aantal persoonsgegevens over de 'Ultimate Beneficial Owners' (UBO) van de betreffende vennootschap in het handelsregister op te nemen. Daarmee wordt de identiteit van de UBO vastgesteld. Volgens Privacy First is dit in strijd met de privacy en met het recht op bescherming van persoonsgegevens van de UBO's. Privacy First heeft daardoor geëist dat de UBO-wetgeving buiten werking dient te worden gesteld. Om wetgeving – dat is gebaseerd op een Europese richtlijn – buitenwerking te stellen, is vereist dat betrokkenen op korte termijn ernstige schade zullen lijden. Privacy First heeft dat echter niet voldoende aannemelijk gemaakt ten aanzien van UBO's. Daarnaast kan een UBO bij blootstelling aan een onevenredig risico, vrees van ontvoering, chantage, afpersing, minderjarigheid en andere soorten van handelingsonbekwaamheid – na de openbaarmaking van zijn gegevens – zijn gegevens op verzoek afschermen. De voorzieningenrechter heeft daarom de vordering afgewezen. Het uiteindelijke oordeel zal moeten worden genomen door de rechtbank Den Haag.

https://bit.ly/32BuTES

ICTRECHT

Van artificial intelligence tot zoekmachine

Legal tech, het is een van de grootste hypewoorden de laatste jaren. Technologie om de juridische sector te ondersteunen, maar vooral te transformeren. Legal tech gaat ons vele veranderingen brengen, maar op een heel andere manier dan we denken.

€ 46,50

Inclusief btw en verzendkosten

Bestel het boek nu!

https://bit.ly/2Yz8bf9

Maxime Leijendekker
Juridisch adviseur

Laura Monhemius
Juridisch adviseur

Jasmine Benning
Juridisch adviseur

Privacy

2021: een recap door onze privacyexperts

Het begin van het nieuwe jaar is een goed moment om eens terug te blikken op de verschillende gebeurtenissen die wij in het afgelopen jaar (2021) op het gebied van privacy zijn tegengekomen. Dat privacy belangrijk is, en blijft, in alle onderdelen van de samenleving, hebben we het afgelopen jaar wel gezien. Niet alleen zagen we het onderwerp privacy vaak voorbij komen in de discussies rondom het coronavirus, ook speelde privacy bij het gebruik van Google Workspace for Education een cruciale rol. Daarnaast kunnen we de nieuwe Standard Contractual Clauses, met de DTIA als nieuw begrip, natuurlijk niet vergeten. In dit artikel blikken we terug op de ontwikkelingen rondom deze thema's.

Corona

In 2020 kregen we voor het eerst te maken met het coronavirus (COVID-19). Dit virus zorgde voor een pandemie met zeer ingrijpende gevolgen. Het coronavirus domineerde ons leven en verlangde aanpassing en flexibiliteit van de samenleving. En nog steeds, want hoewel we gehoopt hadden dat het coronavirus inmiddels tot het verleden zou horen, is dit nog altijd niet het geval. De aanpassingen die gemaakt moesten worden, ziet u bijvoorbeeld ook terug in de wetgeving en onze privacy. Zo is er een tijdelijk wet maatregelen COVID-19 in het leven geroepen en speelt de vraag weer of een QR-code op de werkvloer verplicht mag worden gesteld.

Hoewel we begin vorig jaar hadden verwacht dat er met de start van het vaccineren licht aan het einde van de tunnel was, lijkt niets minder waar. Nu de cijfers weer omhooggaan en de ziekenhuizen overbelast raken, wordt er gezocht naar andere maatregelen om het coronavirus opnieuw onder controle te krijgen. Eén van deze maatregelen is het verplicht stellen van een QR-code op de werkvloer. Dit zou betekenen dat de werkgever moet vragen naar de

vaccinatiestatus van een werknemer, maar mag dit wel? De Autoriteit Persoonsgegevens (AP) was eind 2020 heel duidelijk in haar standpunt: een werknemer hoeft niet te vertellen of hij/zij wel of niet gevaccineerd is. Sterker nog, de werkgever mocht hier volgens de AP niet eens naar vragen.

Gezondheidsgegevens

De QR-code bevat namelijk informatie die aan te merken is als een gezondheidsgegeven. Middels de QR-code is namelijk niet alleen af te lezen van wie de QR-code is, maar ook is inzichtelijk of u gevaccineerd bent. En of u gevaccineerd bent, zegt iets over uw gezondheid.

Het verwerken van gezondheidsgegevens is in principe verboden. Dit komt doordat gezondheidsgegevens op grond van de Algemene verordening gegevensbescherming (AVG) bijzondere persoonsgegevens zijn. Voor bijzondere persoonsgegevens geldt dat deze niet mogen worden verwerkt, tenzij de verwerkingsverantwoordelijke een beroep kan doen op een uitzonderingsgrond. Voor de QR-code op de werkvloer is dat op dit moment (nog) niet het geval.

Wetgeving

Een mogelijke uitzondering zou kunnen zijn dat het vragen en registreren van de vaccinatiestatus noodzakelijk is vanwege een zwaarwegend algemeen belang of de volksgezondheid. Hierbij dient rekening te worden gehouden met de rechten, vrijheden en fundamentele (privacy)belangen van de werknemer. Om gebruik te maken van een uitzondering, dient dit echter wel bij wet geregeld te zijn. Zo werd eerder al wettelijk vastgelegd dat bezoekers van horeca en sportwedstrijden een QR-code moeten kunnen laten zien. Hierbij werd expliciet benoemd dat deze uitzondering niet geldt voor de werkvloer. Dat deze uitzondering niet geldt voor de werkvloer zou dus eerst weer opgeheven moeten worden om de QR-code op de werkvloer mogelijk te maken.

Het invoeren van de QR-code op de werkvloer is een lastige afweging voor het kabinet. Anders dan een bezoek aan het theater of de horeca, kan een persoon tenslotte niet de afweging maken om niet naar werk te gaan. Denk bijvoorbeeld aan docenten of artsen. Op dit moment wordt de wetgeving, waarmee werkgevers het recht krijgen om naar de QR-code te vragen van medewerkers die naar het werk komen, voorbereid door het kabinet. Of er een meerderheid in de Tweede en Eerste Kamer komt, is lastig te zeggen. Het is daarom nog afwachten hoe de maatregelen zich verder ontwikkelen en of de politiek het nodig acht om zo ver te gaan.

Google Workspace for Education

Dan van de werkvloer naar het onderwijs. In 2021 was Google Workspace for Education een veel besproken onderwerp binnen het onderwijs.

Google Workspace is een pakket van applicaties, waarmee in de cloud kan worden samengewerkt. Google Workspace for Education is een uitbreiding op de “gewone” Google Workspace en specifiek bedoeld voor onderwijsinstellingen.

Data Protection Impact Assessment

SURF (ICT-coöperatie van onderwijs en onderzoek) en SIVON (coöperatie van en voor het primair en voortgezet onderwijs) hebben in opdracht van de Rijksuniversiteit Groningen (RUG) en de Hogeschool van Amsterdam (HvA) onderzoek gedaan naar de privacyrisico’s van het gebruik van Google Workspace for Education. Aan de hand van een Data Protection Impact Assessment (DPIA) werden de risico’s in kaart gebracht. Onderzocht is hoe gegevens via Google Workspace for Education verzameld worden, wat er met de gegevens gedaan wordt en wat de risico’s zijn.

Naar aanleiding van deze DPIA is de AP als onafhankelijk toezichthouder, door SURF en SIVON, namens de individuele schoolbesturen, om een advies gevraagd. Vervolgens heeft de AP aan de hand van de DPIA geoordeeld dat de geconstateerde risico’s zien op fundamentele beginselen, die gelden voor elke verwerking van persoonsgegevens, die valt onder de AVG. Volgens de AP kan de gegevensverwerking niet rechtmatig plaatsvinden, omdat er veel onduidelijkheid bestaat over de rolverdeling en de verwerking van persoonsgegevens door Google.

Uit de DPIA kwamen twee grote risico’s naar voren. Ten eerste was het niet duidelijk welke persoonsgegevens door Google worden verwerkt. Ook ontbrak een specificatie van de doeleinden en grondslagen voor de verwerking van deze persoonsgegevens. Het tweede risico was gelegen in de onduidelijkheid over de rolverdeling tussen onderwijsinstellingen en Google. Tussen partijen kon niet worden bepaald wie voor de diverse verwerkingen verwerkingsverantwoordelijke en wie verwerker was.

De AP gaf onderwijsinstellingen daarom het advies om te stoppen met het gebruik van Google Workspace for Education. Het vaststellen van het doel en de grondslag van een verwerking en het bepalen van de rolverdeling zijn namelijk essentieel voor een rechtmatige verwerking van persoonsgegevens onder de AVG.

Nieuwe afspraken

Het is Google echter al gelukt om snel nieuwe afspraken te maken met SURF en SIVON. Begin juli 2021 is overeenstemming bereikt met Google over de maatregelen, die genomen dienen te worden, ten aanzien van de met de DPIA geconstateerde risico's. De afspraken tussen SURF, SIVON en Google bevatten een uitgebreide set contractuele, organisatorische en technische maatregelen. Dit houdt in dat scholen gebruik kunnen blijven maken van Google Workspace for Education, mits zij zelf ook enkele acties uitvoeren. Zo dienen scholen zelf een aantal instellingen binnen de Google Workspace for Education omgeving aan te passen, dienen zij de aangepaste privacyvoorwaarden van Google te accepteren en zijn scholen als verwerkingsverantwoordelijke voor de gegevens van de leerlingen, zelf verantwoordelijk voor het uitvoeren

van een definitieve DPIA. Om deze aanpassingen gemakkelijker te maken voor onderwijsinstellingen hebben SURF, SIVON en Kennisnet een ondersteuningspakket gemaakt dat te vinden is via Kennisnet. In het ondersteuningspakket worden de door scholen uit te voeren handelingen nader toegelicht. Ook bevat het ondersteuningspakket een technische handleiding voor het instellen van de Google Workspace for Education omgeving en een handreiking ter ondersteuning bij het uitvoeren van een eigen risicoanalyse en het vaststellen van additionele risico's in specifieke situaties die per onderwijsinstelling kunnen verschillen.

Nieuwe SCC's

Ook is 2021 het jaar waarin de nieuwe Standard Contractual Clauses (SCC's) zijn aangenomen door de Europese Commissie. Met deze nieuwe sets, zijn de oude versies van de SCC's vervangen. Dit houdt in dat de oude SCC's per 27 september 2021 niet meer gesloten kunnen worden met nieuwe partijen. Daarnaast hebben organisaties tot 27 december 2022 de tijd om de nieuwe SCC's te implementeren in hun huidige contracten.

Passende waarborgen

De AVG stelt strenge eisen aan de verwerking van persoonsgegevens buiten de Europese Economische Ruimte (EER). Dit komt doordat de bescherming van persoonsgegevens niet in alle landen hetzelfde geregeld is en er buiten de EER vaak zwakkere of geen privacywetgeving van toepassing is. Er zijn vier mogelijkheden om persoonsgegevens door te geven naar een derde land. Dit kan op basis van een adequaatheidsbesluit, passende waarborgen, binding corporate rules (BCR's) en specifieke uitzonderingen.

Indien er bijvoorbeeld geen sprake is van een adequaatheidsbesluit, moet er een ander passend doorgiftemechanisme zijn. Dit kan door gebruik te maken van de SCC's. De SCC's zijn algemeen inzetbaar en zorgen er in principe voor dat iedere doorgifte van persoonsgegevens buiten de EER voldoende beschermd is.

De nieuwe SCC's zijn – in tegenstelling tot de oude modelcontracten – modulair opgebouwd. Hierdoor kunnen ze in meerdere situaties worden gebruikt. De nieuwe SCC's bestaan nu uit een algemeen gedeelte en vier specifieke situaties:

- doorgifte van verwerkingsverantwoordelijke naar verwerkingsverantwoordelijke;
- doorgifte van verwerkingsverantwoordelijke naar verwerker;
- doorgifte van (sub)verwerker naar (sub)verwerker;
- doorgifte van (sub)verwerker naar verwerkingsverantwoordelijke.

Met deze vier specifieke situaties sluiten de SCC's beter aan bij de AVG. Zo is het nu bijvoorbeeld ook mogelijk om SCC's te sluiten tussen een verwerker en een (sub)verwerker. Met de oude SCC's was het enkel mogelijk om een contract te sluiten tussen twee verwerkingsverantwoordelijke of een verwerkingsverantwoordelijke en een verwerker. Daarnaast vormen de nieuwe SCC's nu ook een integrale verwerkersovereenkomst, waarin alle eisen van artikel 28 (3) AVG verwerkt zijn. Hierdoor is het in principe niet meer nodig om nog een aparte verwerkersovereenkomst te sluiten.

Een nieuw begrip: DTIA

Daarnaast zijn er in 2021 niet alleen nieuwe SCC's aangenomen, maar is hiermee ook een nieuw begrip binnen privacyland geboren: een Data Transfer Impact Assessment (DTIA).

Voor doorgifte naar de Verenigde Staten zijn de nieuwe SCC's van groot belang. Zoals inmiddels wel bekend, is het Privacy Shield, wat gold tussen Europa en de Verenigde Staten, in 2020 ongeldig verklaard in de Schrems II-uitspraak. Naast het oordeel dat het Privacy Shield onvoldoende bescherming biedt tegen het datagraaien van de Amerikaanse inlichtingendiensten, heeft het Europese Hof zich in 2020 ook uitgelaten over de SCC's. Het Europese Hof heeft geoordeeld dat enkel het sluiten van SCC's niet voldoende is. Iedere organisatie die persoonsgegevens doorgeeft buiten de EER, dient via een case-by-case assessment te toetsen of de wetgeving in het ontvangende land niet afdoet aan het beschermingsniveau dat de SCC's creëren. Dit case-by-case-assessment wordt ook wel een Data Transfer Impact Assessment (DTIA) genoemd. Uit een DTIA moet volgen waarom de organisatie gebruik maakt van een leverancier die gevestigd is in een derde land en op welke wijze ervoor wordt gezorgd dat de privacy van betrokkenen wordt gewaarborgd. Deze verplichting is ook expliciet opgenomen in de nieuwe SCC's.

Benieuwd wat ons in 2022 te wachten staat?

Via onze website www.ictrecht.nl plaatsen wij maandelijks meerdere blogs over de ontwikkelingen op het gebied van ICT, cloud, privacy, recht én meer.

Privacy

Het woonadres en tegelijkertijd vestigingsadres van de zzp'er blijft openbaar

Van onze blog
11 oktober 2021

Een van de meest opvallende ontwikkelingen op de arbeidsmarkt van de afgelopen decennia is de opkomst van de zelfstandige zonder personeel (zzp'er). Een journalist of kunstenaar, de digital nomad of de kruidenier op de hoek, zzp'ers vormen een diverse groep in de samenleving. Wat zzp'ers met elkaar gemeen hebben is dat hun persoonsgegevens vaak makkelijk vindbaar zijn. De openbaarheid van woonadressen van zzp'ers kan gepaard gaan met ongewenste gevolgen, zoals ongevraagde direct marketingactiviteiten of erger nog, bedreigingen aan huis. De Autoriteit Persoonsgegevens (AP) heeft daarom geadviseerd[1] dat adresgegevens van zzp'ers moeten worden afgeschermd, zodat deze niet zomaar vindbaar zijn. De vraag is nu hoe dat het best geregeld kan worden voor zzp'ers waarvan het vestigingsadres gelijk is aan het woonadres.

1. https://bit.ly/3yt36Cn

Van motie tot wetswijziging

Op grond van de Handelsregisterwet moeten ondernemingen en rechtspersonen zich registreren in het handelsregister van de Kamer van Koophandel (KVK). De woonadressen van zzp'ers, vennoten van personenvennootschappen en bestuurders van verenigingen van eigenaars zijn op dit moment openbaar. Dat is natuurlijk niet wenselijk. Begin dit jaar werd met een ruime Kamermeerderheid een motie aangenomen dat de KVK voortaan geen privéadressen meer mag verstekken van ingeschrevenen die aangeven dat niet te willen. De wetgever, het ministerie van Economische Zaken en Klimaat, geeft gedeeltelijk uitvoering aan deze motie met een wetswijzing van de Handelsregisterwet.

Wetswijziging Handelsregisterwet

Vanaf 1 januari 2022 moet de KVK woonadressen gaan afschermen. Woonadressen zijn dan alleen nog in te zien door overheidsorganisaties of beroepsgroepen die daar wettelijke toestemming voor hebben, zoals de Belastingdienst, advocaten en deurwaarders. Een vestigingsadres dat tegelijkertijd een woonadres van een zzp'er is, blijft echter nog wel zichtbaar. Volgens het kabinet is het afschermen van deze vestgingsadressen praktisch onhaalbaar en doet dat af aan de rechtszekerheid in het economische verkeer.

In navolging van het advies van de AP wil het kabinet echter nog wel nadenken over andere mogelijke oplossingen voor het probleem. Het ministerie van Economische Zaken en Klimaat is daarom ondertussen een zogenaamd Datavisie Handelsregister gestart. De Datavisie heeft als doel het evenwicht tussen het recht op privacy van de zzp'ers en de economische belangen in het economisch verkeer opnieuw te beoordelen, en waar nodig, bij te stellen. Dit traject is in het voorjaar gestart met een consultatie waarbij bedrijven, burgers en overheden konden aangeven hoe ze gebruik maken van het Handelsregister en hoe het Handelsregister invloed op hen heeft.

Advies: alternatief vestigingsadres

Wij houden de ontwikkelingen uiteraard nauwlettend in de gaten. In afwachting van de definitieve uitkomst van het Datavisie Handelsregister kunnen wij tot nu toe enkel adviseren dat de oplossing vooral bij de zzp'er zelf ligt. Gaat u als zzp'er aan de slag, denk dan van tevoren na hoe u uzelf registreert in het Handelsregister. Heeft u bezwaren tegen het bekendmaken van uw woonadres, ook al werkt u voornamelijk vanuit huis, overweeg dan de mogelijkheden om u in te schrijven op een ander vestigingsadres.

Heeft u tussentijds vragen?

Neem contact met ons op via onze website: ictrecht.nl/contact

Auteur
Isabella Oelz
Juridisch adviseur

Innovatie

Wij stellen aan u voor: ons legal tech team

Van onze blog
8 november 2021

Sinds 1 november hebben wij bij ICTRecht onze dienstverlening uitgebreid met een nieuwe dienst: legal tech.[1] In dit interview vragen we het legal tech team - bestaande uit Koen van Jaarsveld, Mark Zijlstra en Sten Demon (v.l.n.r.) - het hemd van het lijf. Over wat legal tech nu precies inhoudt, waar hun drang tot innovatie vandaan komt en hoe het team tot stand is gekomen. Lees snel verder!

1. https://bit.ly/3m7DRAD

Allereerst, wat is legal tech?
Sten: ''Sinds een aantal jaar hoor je de term legal tech[2] steeds vaker in de juridische wereld. Softwareleveranciers schieten als paddenstoelen uit de grond, legal innovators spreken steeds vaker op juridische events en elke jurist wil mogelijkheden ontdekken om het werk efficiënter te maken. Op dit moment is er nog geen formele definitie van legal tech. Wij leggen legal tech uit als de technologie die ondersteunt bij juridische taken of deze zelfs geheel automatiseert. Legal tech is daarmee een verzamelnaam voor alle innovatieve mogelijkheden bij juridische processen.''

2. https://www.ictrecht.nl/legal-tech

Op welke manier gaat legal tech het verschil maken?
Mark: ''Op verschillende vlakken! Primair zorgt deze vorm van innovatie binnen legal voor meer efficientie. Doordat eenvoudige juridische taken worden versimpeld of geautomatiseerd, kunnen juridische werkzaamheden veel efficiënter worden uitgevoerd. Van deze efficiëntieslag heeft niet alleen legal profijt, maar ook alle met legal samenwerkende organisatieonderdelen. Doordat de jurist efficiënter kan werken zal de juridische afdeling steeds minder vaak snelle deals vertragen. De jurist gaat daarnaast binnen de eigen werkzaamheden meer waarde kunnen toevoegen, aangezien er simpelweg meer gelegenheid is voor het echte inhoudelijke juridische werk.''

Waar komt jullie drang naar innovatie vandaan?
Koen: ''Wij zijn alle drie juristen. Ieder van ons heeft als jurist regelmatig op grote schaal standaard juridische werkzaamheden verricht voor opdrachtgevers. Hierdoor zijn wij van mening dat juridisch werk veel efficiënter kan. Vanuit deze gedachte is de drang naar innovatie ontstaan. Uiteindelijk vonden wij zelf steeds slimmere manieren om ons werk als jurist uit te voeren. Nu bundelen wij deze manieren en delen we dit met organisaties die ook behoefte hebben aan een efficiëntere juridische afdeling.''

Hoe is jullie legal tech team eigenlijk tot stand gekomen?
Sten: ''Ons team is in het voorjaar van 2021 ontstaan. Ik werk zelf ruim zes jaar als juridisch adviseur bij ICTRecht en heb een privacyrechtelijke achtergrond. Ik ben al langere tijd bezig met de ontwikkeling van legal tech binnen ICTRecht. Mark en Koen zijn recentelijk in dienst getreden bij ICTRecht. Eerder waren zij al drie jaar collega's, waarbij ze veel hebben samengewerkt op het gebied van legal tech en legal operations. Door onze krachten te bundelen, hebben wij in korte tijd een volwaardig dienstverleningsmodel kunnen ontwikkelen. Ons team is volledig tech gedreven. Wij geloven dan ook heilig in de legal tech-revolutie die inmiddels gestart is.''

Lees deel 2 van het interview op onze website https://bit.ly/3rxp3Pe

Auteur
Nicole Waaijer
Marketing adviseur

ICTRecht Academy

Trainingsoverzicht jan. - mrt. 2022

Donderdag 13 januari 2022
AI en de wet (4 PO-punten)
Leer de werking van AI op hoofdlijnen te schetsen en de mogelijkheden voor AI in het recht en de risico's te duiden.

Deze vindt online plaats.
Lees meer!
https://bit.ly/3F1suS2

Dinsdag 25 januari 2022
Privacy: AVG in ICT nader bekeken (6 PO-punten)
In de training gaan we uitgebreid in op binding corporate rules, de verwerkersovereenkomst, registers en de FG.

Deze vindt plaats in Utrecht.
Lees meer!
https://bit.ly/3F3qf0A

Dinsdag 1 februari 2022
Contracteren: e-commerce informatieplichten (2 PO-punten)
Word bekend met de e-commerce informatieplichten en weet hoe er in de praktijk aan voldaan kan worden.

Deze vindt plaats in Amsterdam en online. Lees meer!
https://bit.ly/30giSUG

Dinsdag 22 maart 2022
ICT & gezondheidsrecht (6 PO-punten)
Weten welke regels gelden bij het uitwisselen van medische gegevens online? Leer alles over ICT en gezondheidsrecht.

Deze vindt plaats in Utrecht.
Lees meer!
https://bit.ly/3H6kp05

Dinsdag 29 maart 2022
Cloud en software: merken en domeinnamen (2 PO-punten)
Leer de werking van het domeinnaam-systeem (DNS) uitleggen en de inbreuk van een domeinnaam op een merk vaststellen.

Deze vindt plaats in Amsterdam en online. Lees meer!
https://bit.ly/30fMe5y

Dinsdag 29 maart 2022
FG in de zorg(praktijk)
Tijdens deze training wordt specifiek ingegaan op de rol, werkzaamheden en bevoegdheden van de FG in de zorg.

Deze vindt plaats in Utrecht.
Lees meer!
https://bit.ly/3o9qwbm

Specialiseer u tot FG/DPO!

ICTRecht Academy biedt u een opleiding tot Functionaris Gegevensbescherming (FG) – ook wel bekend als Data Protection Officer (DPO). In 12 trainingsdagen, verspreid over vier maanden, doet u gespecialiseerde kennis op over de Europese privacywetgeving (AVG/GDPR) en de vertaling van deze wet naar de dagelijkse praktijk. Wij stomen u klaar voor de positie van FG/DPO.

De opleiding start op 17 maart 2022.
Lees meer!

ictrecht.nl/fg-opleiding

Leer in 10 weken AI te beheersen met onze e-learning AI compliance & governance!

Wordt Artificial Intelligence ook in uw praktijk steeds belangrijker? In deze e-learning leert u in 10 weken wat de regels rond AI zijn en hoe daarmee om te gaan. Daarnaast doet u mee aan een unieke serious game die u AI compliance en governance in de praktijk laat zien. Neemt u de uitdaging aan?

De e-learning start op 7 februari 2022.
Lees meer!

ictrecht.nl/apcg

Heeft u vragen of wilt u meer weten?

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

Britt Telleman
Opleidingscoördinator

Meer informatie over hoe wij werken? Bezoek ictrecht.nl