jaargang 9 • nummer 3 • juli 2021

ICTRecht in de praktijk

Komen autonome drones ooit van de grond?

Zorginstelling, wat betekent de MDR voor uw dagelijkse bedrijfsvoering?

Pragmatisch omgaan met uw informatiebeveiliging

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:

Alexander Freund Information security consultant
a.freund@ictrecht.nl
Alisa Schurink Marketing adviseur
a.schurink@ictrecht.nl
Arnoud Engelfriet Algemeen directeur en Opleidingsdirecteur
a.engelfriet@ictrecht.nl
Bas Dekker Juridisch adviseur
b.dekker@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
Jay Remmelzwaal Juridisch adviseur
j.remmelzwaal@ictrecht.nl
Johnny Honing Information security consultant
j.honing@ictrecht.nl
Kors Monster Directeur ICTRecht Security
k.monster@ictrecht.nl
Laura Monhemius Juridisch adviseur
l.monhemius@ictrecht.nl
Nicole Waaijer Marketing adviseur
n.waaijer@ictrecht.nl
Sanne Haumersen Legal assistant
s.haumersen@ictrecht.nl
Sten Demon Directeur ICTRecht Legal Tech
s.demon@ictrecht.nl
Steven Ras Algemeen directeur
s.ras@ictrecht.nl
Tess Vonk Juridisch adviseur
t.vonk@ictrecht.nl
Tessa van Schijndel Juridisch adviseur
t.vanschijndel@ictrecht.nl
Valeria Brussé Juridisch adviseur
v.brusse@ictrecht.nl
Eline Pellis Grafisch ontwerper
eline@elinepellis.com
Leonard Fäustle Stills & Motion
Foto's ICTRecht
info@leonardfaustle.nl

Bas Dekker
Juridisch adviseur

Valeria Brussé
Juridisch adviseur

Cloud Overheid Innovatie

Komen autonome drones ooit van de grond?

De drone-industrie en artificial intelligence (AI) zijn volop in ontwikkeling, waardoor drones steeds beter in staat zijn om zelfstandig te opereren. De verschuiving van een menselijke piloot (op afstand) naar een autonome drone betekent dat bestaande regelgeving aangepast dient te worden. Europa is dan ook hard op weg om AI en drones te reguleren: op 21 april 2021 publiceerde de Europese Commissie (EC) en de luchtvaartautoriteit (EASA) beide concept-documenten met nieuwe regels en acties over de aanpak van AI en drones.

De EC presenteert hiermee het allereerste regelgevingskader voor AI.[1] In samenwerking met de lidstaten is het doel de veiligheid en grondrechten van mensen en bedrijven te waarborgen en tegelijkertijd het draagvlak voor AI, investeringen en innovatie in de hele EU te versterken. Tegelijkertijd presenteert de EASA met dit conceptdocument de eerste belangrijke mijlpaal van hun 'AI Roadmap'[2] met een reeks doelstellingen voor AI.[3] Het lijkt erop dat EASA de mogelijkheden van AI wil stimuleren, maar het is de vraag of de EC met nieuwe regulering niet te strenge regels oplegt.

1. https://bit.ly/3xUgXkO
2. https://bit.ly/3tpy4Hm. De AI Roadmap is bedoeld om EASA's visie op de ontwikkeling van AI in de luchtvaart vast te stellen, alsook de basis te leggen voor interactie met zijn belanghebbenden over dit onderwerp.
3. https://bit.ly/3uom6zn

Wat is een autonome drone?

Bestuurbare drones worden op dit moment al gebruikt voor verschillende doeleinden. Het gaat dan voornamelijk om saaie, gevaarlijke en vieze taken. Er zijn ook drones op de markt die uitgerust zijn met autopilot-technologie, waardoor ze 'zelfstandig' kunnen vliegen zonder te allen tijde door de piloot te worden bestuurd. Maar dat het apparaat onbemand en zelfs zonder bestuurd te worden kan vliegen, wil niet zeggen dat het apparaat daadwerkelijk autonoom is. Er is pas sprake van een autonome drone indien de

drone (met gebruik van AI) volledig zelfstandig kan vliegen, de af te leggen route bepaalt en inspeelt op het overige luchtverkeer om zich heen.

Waarom hebben we AI nodig?

Naar verwachting zal komende jaren de hoeveelheid drones blijven toenemen. Integratie van deze grote hoeveelheid drones in het luchtruim en operaties in stedelijke omgevingen zullen alleen mogelijk zijn met hoge mate van automatisering en het gebruik van disruptieve technologieën zoals AI. Daarbij zal voor de ontwikkeling van oplossingen op het gebied van autopilot- en 'detect and avoid' technologie ook de ondersteuning van AI-oplossingen nodig zijn. Denk aan het analyseren van beelden van radar- of camera-systemen. AI zou ook als een vangnet kunnen fungeren, bijvoorbeeld wanneer de verbinding met de drone wegvalt. Bovendien kan gedacht worden aan het pakket- en personenvervoer in de stad. Operaties buiten het zicht en zonder piloot zullen cruciaal zijn om dronevervoer in de stad economisch rendabel te houden. Tot slot wordt verwacht dat autonome systemen op termijn veiliger zullen zijn omdat veel ongelukken ontstaan door menselijke fouten.

Waarom zijn er nog geen autonome drones?

Hoewel er op technisch gebied al veel mogelijk is, zijn er nog vele uitdagingen om autonome drones daadwerkelijk in te zetten. Om veilig te kunnen vliegen zal het luchtruim heringericht moeten worden. Ook zullen er diensten moeten komen die drones op afstand kunnen identificeren en informatie verschaffen waar wel en niet mag worden gevlogen. Daarbij moeten drones in staat zijn om obstakels en elkaar te ontwijken.

Naast de technische beperkingen vereisen autonome drones geheel nieuwe wet- en regelgeving. Er zijn regels nodig die de veiligheid en de privacy rondom het gebruik van autonome drones waarborgen.

Regulering van AI op Europees niveau

In het conceptdocument van de EASA wordt voorlopig alleen aandacht besteed aan relatief eenvoudige toepassingen van AI, waarbij er altijd een mens toezicht houdt op de drone. In de toekomst zullen er mogelijk aanvullende richtsnoeren worden opgesteld voor complexere c.q. autonomere (en daarmee ook risicovollere) toepassingen van AI in drones. De EC heeft al een stap verder gezet: het conceptdocument van de EC heeft betrekking op álle toepassingen van AI, niet alleen op toepassingen waarbij een mens toezicht houdt. Eurocommissaris Margrethe Vestager heeft hier een duidelijke visie over: "Hoe hoger het risico, hoe strenger de regels."

De EC gaat in het conceptdocument uit van een geschaald risicosysteem. Bijna het gehele document ziet op de regulering van de hoogste risicocategorie: 'high risk AI-systems', denk hierbij aan zelfrijdende auto's. Opvallend is dat het gebruik van onbemande luchtvaartuigen niet specifiek is opgenomen in de lijst met hoge risico's van het conceptdocument. Wel geeft de EC zichzelf nu alvast de ruimte om de lijst met 'high risk AI-systems' op termijn uit te breiden. En aangezien ook zelfrijdende auto's als 'high risk' toepassing worden aangemerkt, is het in onze optiek waarschijnlijk dat ook autonome drones hier in de toekomst onder zullen worden geschaard. Als dat het geval is, zullen zij (uitgaande van het conceptdocument) moeten gaan voldoen aan strenge regels, zoals het uitvoeren van een risicoanalyse waarbij de risico's van de inzet van de autonome drone worden gedocumenteerd. Daarnaast dient een high *risk AI-system* geregistreerd te worden in een Europese database.

Het conceptdocument is slechts een eerste poging van de EC om AI te reguleren en onderdeel van een omvangrijk proces met meerdere belangen waarbij veel verschillende partijen betrokken zijn. Vooralsnog zal concrete wet- en regelgeving nog een tijd op zich laten wachten. Te verwachten valt dat bij verdere technologische ontwikkelingen (sector) specifieke regelgeving rondom het gebruik van AI zal worden opgesteld en dus mogelijk ook voor de toepassing van AI bij drones.

Dus: komen autonome drones ooit van de grond?

Als autonome drones in de toekomst als hoog risico worden aangemerkt, zal de strenge regulering weinig ruimte laten voor de toepassing ervan. Hiermee zal de technologische innovatie mogelijk te veel aan banden worden gelegd, iets wat mede van invloed is op de toepassing van autonome drones.

Overigens moet het Europarlement en alle lidstaten van de EC instemmen met de voorstellen uit het conceptdocument. Dit zal naar verwachting nog jaren duren, mogelijk wordt er in de tussentijd een goede werkwijze gevonden waarbij AI kan worden toegepast op drones!

Tess Vonk
Juridisch adviseur

Privacy

Privacy en beeldmateriaal op social media

Op ieder online medium worden dagelijks miljarden foto's en video's (beeldmateriaal) gepubliceerd. Met één druk op de knop wordt beeldmateriaal immers te pas en te onpas gemaakt en gepubliceerd. Iedereen – met een *smartphone* op zak – is tegenwoordig fotograaf. Daarnaast biedt social media tal van mogelijkheden om uw creaties te delen met de wereld. Kortom, het maken en publiceren van beeldmateriaal is nog nooit zo makkelijk geweest. Maar let goed op, als u beeldmateriaal op social media publiceert waarop personen herkenbaar zijn afgebeeld, dan is de Algemene verordening gegevensbescherming (AVG) van toepassing. In dit artikel leg ik uit welke regels uit de AVG van belang zijn voor het publiceren van beeldmateriaal op social media.

Is beeldmateriaal een persoonsgegeven?

Op het maken en publiceren van beeldmateriaal is de AVG van toepassing. Op beeldmateriaal is het immers mogelijk een persoon te identificeren. Het identificeren kan volgens de Autoriteit Persoonsgegevens (AP) zelfs aan de hand van een herkenbare houding of postuur van een persoon.[1] Dit betekent dat een gezicht in beeld in principe niet is vereist. Zo kan ook een persoon die is geblurd of een zwart blokje voor zijn gezicht heeft, worden geïdentificeerd door andere factoren. Dit betekent dat al het beeldmateriaal waarop een persoon is afgebeeld gekwalificeerd kan worden als een persoonsgegeven.

1. https://bit.ly/33XleGn

Kan beeldmateriaal worden aangemerkt als een verwerking van bijzondere categorieën persoonsgegevens?

Bijzondere categorieën persoonsgegevens zijn gegevens die bijvoorbeeld iets zeggen over iemands ras, godsdienst of gezondheid.[2] Op het verwerken van bijzondere categorieën persoonsgegevens gelden strengere regels. Zo geldt in beginsel een verwerkingsverbod, tenzij een uitzondering uit de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) of de AVG van toepassing is.

2. Artikel 9 AVG.

Op beeldmateriaal kan een hoop gevoelige informatie zichtbaar zijn. Zo kan een lichte of donkere huidskleur iets zeggen over iemands ras of etnische afkomst. Bovendien kan een hoofddoek iets zeggen over iemands godsdienst of geloofsovertuiging. Dit betekent echter niet dat al het beeldmateriaal, waarop gevoelige informatie zichtbaar is bijzondere categorieën persoonsgegevens zijn. Volgens de AP kan beeldmateriaal immers worden aangemerkt als een bijzondere categorie persoonsgegevens, indien het beeldmateriaal specifiek is gericht op het maken van onderscheid op basis van een bijzondere categorie persoonsgegevens.[3] Dit is bijvoorbeeld het geval wanneer een school een foto publiceert op social media van biddende kinderen, om te laten zien aan de buitenwereld dat zij het geloof naleeft. Het is dan ook belangrijk om na te gaan wat zichtbaar is op het beeldmateriaal en wat de boodschap is van het beeldmateriaal om te bepalen of het bijzondere categorieën persoonsgegevens betreft.

3. https://bit.ly/33XleGn

Op welke verwerkingsgrondslag kan het publiceren van beeldmateriaal worden gebaseerd?

Op grond van de AVG dient elke verwerking – dus ook het publiceren van beeldmateriaal op social media – te worden gebaseerd op een verwerkingsgrondslag. De in de praktijk meest voorkomende verwerkingsgrondslagen voor het plaatsen van beeldmateriaal op social media zijn toestemming, uitvoering van de overeenkomst of gerechtvaardigd belang.

Toestemming

De verwerkingsgrondslag toestemming houdt in dat je van de personen die zijn afgebeeld op het beeldmateriaal toestemming dient te krijgen om het beeldmateriaal te publiceren. Het verkrijgen van toestemming moet voldoen aan een aantal vereisten. Zo dient de toestemming vrij, ondubbelzinnig en specifiek te worden gegeven. Dit betekent dat het weigeren van toestemming geen negatieve gevolgen mag hebben, de toestemming duidelijk wordt gegeven en degene die toestemming geeft precies weet waarvoor hij toestemming geeft. Het geven van vrije toestemming kan in sommige situaties echter problemen opleveren. Bijvoorbeeld het publiceren van beeldmateriaal van de werknemer in een werknemer-werkgever relatie. Er bestaat immers tussen de werknemer en werkgever een wanverhouding, waardoor de werknemer zich verplicht kan voelen toestemming te verlenen voor het publiceren van beeldmateriaal. Dit kan je als werkgever voorkomen door bijvoorbeeld duidelijk aan te geven dat er geen negatieve gevolgen zijn verbonden aan het weigeren of intrekken van de toestemming.

Bovendien gelden voor kinderen onder de 16 jaar strengere eisen met betrekking tot het geven van toestemming. Op grond van de AVG dienen namelijk de ouders van het kind toestemming te geven voor het publiceren van het beeldmateriaal. Indien het kind boven de 16 is, dan kan de toestemming bij het kind zelf verkregen worden.

Let wel, de gegeven toestemming kan te allen tijde worden ingetrokken. Dit betekent dat het beeldmateriaal verwijderd moet worden van social media, wanneer de toestemming wordt ingetrokken.

Uitvoering van de overeenkomst

Op de verwerkingsgrondslag uitvoering van de overeenkomst kan een beroep worden gedaan, wanneer een overeenkomst is gesloten tussen u en degene die op het beeldmateriaal staat. Denk hierbij bijvoorbeeld aan het sluiten van een overeenkomst voor het maken en publiceren van beeldmateriaal voor een fotoshoot of reclamespot.

Gerechtvaardigd belang

Een andere verwerkingsgrondslag waarop het publiceren van beeldmateriaal op kan worden gebaseerd is het gerechtvaardigd belang. Een beroep op het gerechtvaardigd belang kan onder andere worden gedaan, wanneer je met het beeldmateriaal een belangrijk punt aan de kaak wil stellen of als het beeldmateriaal een bepaalde nieuwswaarde heeft. Het risico dat het publiceren van beeldmateriaal op basis van deze verwerkinggrondslag met zich meebrengt, is dat de op het beeldmateriaal afgebeelde persoon bezwaar kan maken tegen de publicatie.

Uitzondering persoonlijk- en huishoudelijk gebruik

Beeldmateriaal die je in een beperkte kring op social media publiceert valt buiten de scope van de AVG. Dit wordt ook wel de uitzondering voor persoonlijk- en huishoudelijk gebruik genoemd.[4] Hierbij geldt echter wel dat een beperkt aantal personen toegang mag hebben tot het beeldmateriaal. Het beeldmateriaal mag dus niet gepubliceerd worden op een

openbare Facebook- of Instagrampagina. Daarnaast moet het aantal vrienden zijn beperkt tot een duidelijk bepaalbare groep personen.[5] Een social mediapagina met honderden vrienden of waarbij vrienden van vrienden toegang hebben, valt hier niet onder. De groep is dan immers geen bepaalbare groep. In dat geval gelden de regels uit de AVG wel en heb je een verwerkingsgrondslag nodig om het beeldmateriaal te kunnen publiceren.

4. Artikel 2 lid 2 sub c AVG.
5. https://bit.ly/3f32r2z

De journalistieke uitzondering

Om de vrijheid van meningsuiting te waarborgen is in de UAVG een journalistieke uitzondering opgenomen.[6] Dit betekent dat op beeldmateriaal met een journalistiek karakter een gedeelte van de AVG niet van toepassing is. Zo vervalt onder andere het recht om de gegeven toestemming in te trekken of om bezwaar te maken. Daarnaast kan door middel van de journalistieke uitzondering het verwerkingsverbod op bijzondere categorieën persoonsgegevens worden doorbroken. De algemene bepalingen blijven echter wel gelden. Voor het publiceren van beeldmateriaal met een journalistiek karakter is dus nog wel een verwerkingsgrondslag nodig.

6. Artikel 43 UAVG.

Tot slot

Ondanks deze wirwar aan regels is het op grond van de AVG mogelijk om beeldmateriaal op social media te publiceren. Zorg echter wel dat u de privacy van de persoon afgebeeld op het beeldmateriaal waarborgt. Bijvoorbeeld door het vragen van toestemming. Mocht dit niet mogelijk zijn, kunt u er natuurlijk ook voor kiezen om het beeldmateriaal enkel met een beperkte groep te delen of privé te houden.

Tessa van Schijndel
Juridisch adviseur

E-Health Privacy Overheid

Zorginstelling, wat betekent de MDR voor uw dagelijkse bedrijfsvoering?

Het is zo ver, het lang verwachte (en misschien wel gevreesde) moment is aangebroken: de nieuwe Europese wetgeving voor medische hulpmiddelen is vanaf 26 mei 2021 van toepassing. De verordening medische hulpmiddelen (MDR) is na een overgangsperiode van vier jaar van toepassing in alle lidstaten van de Europese Unie.

Vrijwel iedereen in de zorg krijgt te maken met de nieuwe regels. Hoewel de MDR de meeste impact heeft op de fabrikanten[1] van medische hulpmiddelen, is er ook voor de zorginstelling een nieuwe rol weggelegd. Risicoklassen voor medische hulpmiddelen worden (vooral voor medische software) strenger en zorginstellingen kunnen ineens gezien worden als fabrikant. Daarnaast krijgen zorginstellingen een grotere rol in het garanderen van de veiligheid en kwaliteit van de medische hulpmiddelen. In dit artikel zet ik de belangrijkste aandachtspunten voor zorginstellingen op een rij. En ICT-leveranciers, lees ook even mee. Het is altijd nuttig om te weten waar een zorginstelling tegenaan loopt bij de inkoop en het gebruik van medische hulpmiddelen.

1. De fabrikant is degene die de hulpmiddelen onder zijn naam in de handel brengt.

Kwalificatie en risicoclassificatie

Een hulpmiddel (waaronder software) die door de fabrikant bedoeld is om te worden gebruikt voor een medisch doeleinde, zoals voor het diagnosticeren, voorspellen, het stellen van een diagnose of behandelen van een ziekte, letsel of een beperking wordt onder de MDR aangemerkt als een medisch hulpmiddel.[2]

2. https://bit.ly/3f5cfZK

Software dat niet gebruikt wordt voor een individuele patiënt of voor enkel opslag, archivering of het reconstrueren van data, wordt niet beschouwd als een medisch hulpmiddel. Ook software die als communicatiemiddel wordt gebruikt of software die simpele zoekopdrachten uitvoert, valt niet onder de definitie van een medisch hulpmiddel.

Het kwalificeren en classificeren van medische hulpmiddelen is niet alleen een taak van de fabrikant. Voor het verlenen van goede zorg mogen zorginstellingen alleen maar medische hulpmiddelen gebruiken die een CE-markering hebben. Om dit te controleren moeten Zorginstellingen zelf in kaart brengen welke hulpmiddel een medisch hulpmiddel in de zin van de MDR is en in welke risicoklasse het hulpmiddel valt.

Controleer de beschikbaarheid van de medische hulpmiddelen

Niet alleen medische apparatuur valt onder de MDR, maar ook schoonmaak- en sterilisatieproducten voor deze apparatuur, hulpmiddelen voor eenmalig gebruik, intern vervaardigde hulpmiddelen en steeds meer medische software. Deze nieuwe Europese wetgeving zal vooral een grote impact hebben op medische software. Software wordt namelijk sneller aangemerkt als een medisch hulpmiddel en zal tegelijkertijd in een hogere risicoklasse vallen. Hierdoor moeten fabrikanten aan strengere verplichtingen voldoen om hun medische software te voorzien van een CE-markering. Dit is een vereiste voordat ze het hulpmiddel op de markt mogen brengen en mogen blijven leveren.

Medische hulpmiddelen die niet voorzien zijn van een CE-markering mogen niet meer worden gebruikt. Hiervoor geldt echter wel een uitzondering. Fabrikanten kunnen onder omstandigheden gebruikmaken van het overgangsrecht. Hierdoor kan het hulpmiddel tot 26 mei 2024 onder de oude wetgeving nog worden verkocht en gekocht, mits er geen wijzigingen aan het hulpmiddel worden aangebracht. Voor medische software lijkt dit haast onmogelijk, omdat er met een eenvoudige upgrade al zoveel wijzigingen worden doorgevoerd waardoor medische software al snel opnieuw gecertificeerd zou moet worden.

De meeste fabrikanten van medische software zijn druk bezig met het certificeren, maar wij zien ook een trend van fabrikanten die hun aanbod verminderen of veranderen. Vooral voor start-ups in de medische wereld zou de MDR zomaar een strop om de hals kunnen betekenen. Het verkrijgen van een CE-markering is een kostbare en tijdrovende procedure. Dit komt omdat medische software in een hogere risicoklasse valt waardoor een conformiteitsbeoordeling door een aangemelde instantie (notified body) vereist is. Hier stippen we meteen een ander probleem aan: de beschikbaarheid van die notified bodies. Op dit moment zijn er in Nederland drie notified bodies goedgekeurd om de conformiteitsbeoordelingsprocedure voor medische software uit te voeren. Hierdoor moeten fabrikanten rekening houden met een certificeringsprocedure van minimaal drie, maar reken maar zeker op zes maanden. De voorbereidingstijd hebben we hier nog niet meegerekend. Onder de MDR wordt er namelijk veel verwacht van de fabrikant, zoals het inrichten en het in stand houden van een kwaliteits- en risicomanagementsysteem en het treffen van een behoorlijk pakket aan maatregelen op het gebied van cybersecurity.[3]

3. https://bit.ly/3f1yKPm

Gelukkig heeft de Europese Commissie inmiddels wel een uitzondering kunnen maken op het vereiste dat de notified body's de beoordeling altijd op locatie moeten uitvoeren. Met de coronamaatregelen van afgelopen tijd was dat niet altijd mogelijk.[4]

4. https://bit.ly/340uBVO

Intern vervaardigde hulpmiddelen moeten ook aan de MDR voldoen

Onder de MDR mogen medische hulpmiddelen alleen nog worden gebruikt in lijn met het beoogde doel van de fabrikant. Voor dat beoogde doel heeft de fabrikant een CE-markering verkregen en ander gebruik is verboden. Om te voorkomen dat de zorginstelling zelf als fabrikant wordt aangemerkt, kan hij overwegen om het hulpmiddel intern te vervaardigen. De MDR biedt hiervoor namelijk een nieuwe mogelijkheid. Zorginstellingen mogen zelf (of onder eigen verantwoordelijkheid) medische hulpmiddelen (laten) ontwikkelen als er nog geen hulpmiddelen met de vereiste prestatie op de markt verkrijgbaar zijn. De zorginstelling mag dit hulpmiddel enkel intern gebruiken. Op het moment dat het hulpmiddel in de handel wordt gebracht, wordt de zorginstelling als fabrikant aangemerkt. Hierbij maakt het niet uit of het hulpmiddel tegen betaling of gratis wordt aangeboden.

De intern vervaardigde hulpmiddelen moeten echter wel voldoen aan de algemene vereisten voor veiligheid en prestatie in Annex I van de MDR. Afwijkingen hiervan moeten worden onderbouwd. Daarnaast moet de zorginstelling het ontwerp adequaat documenteren in een technisch dossier, over een passend kwaliteitssysteem en risicomanagementsysteem beschikken en klinische evaluaties uitvoeren. Ook hier zal de Inspectie Gezondheidszorg en Jeugd (IGJ) hier toezicht op gaan houden. De IGJ kan steekproefsgewijs documentatie opvragen ter controle.

Meewerken aan de Post market surveillance van de fabrikant is verplicht

Ook de post market surveillance is niet alleen een belangrijk aandachtspunt voor de fabrikant, maar ook voor de zorginstelling. Door de nieuwe verplichtingen in het kader van de post-market surveillance zullen fabrikanten meer informatie van zorginstellingen willen krijgen over de hulpmiddelen die zij leveren. In het kader van medische software hebben ze onder andere informatie nodig over gebruikerservaringen, updates, storingen, datalekken en cyberaanvallen. Welke persoon binnen de organisatie van de zorginstelling onderhoudt het contact met de fabrikanten? Is dat iemand van inkoop, een zorgverlener of een andere medewerker? In ieder geval krijgt deze persoon er een nieuwe taak bij. Fabrikanten zullen snel een beroep op de informatie van de zorginstellingen doen om te voldoen aan de post market surveillance verplichtingen. En dan moet deze informatie wel beschikbaar zijn.

Ook zullen zorginstellingen alle richtlijnen en instructies van fabrikanten over bijvoorbeeld het onderhoud van de medische hulpmiddelen in acht moeten nemen. Denk hierbij aan procedurele afspraken over het uitvoeren van updates aan medische software. Het niet in acht nemen van deze instructies kan tot gevolg hebben dat de zorginstellingzelf als fabrikant wordt aangemerkt, met alle gevolgen van dien.

Meld- en informatieplicht bij problemen

Op grond van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) bestaat er voor zorginstelingen al de verplichting om calamiteiten te melden bij het toezichthoudende orgaan, de IGJ. In de Wet op medische hulpmiddelen is een meer specifieke meldplicht voor medische hulpmiddelen neergelegd.[5] Hoewel de MDR direct geldig is, heeft de Europese wetgever op enkele punten ruimte overgelaten aan de nationale wetgever om invulling te geven aan bepaalde normen, zoals de invulling van de meldplicht. Hiervoor is de Nederlandse Wet op de medische hulpmiddelen aangepast. De nadere invulling van de meldplicht moet echter nog bekend worden gemaakt in een Algemene Maatregel van Bestuur.

5. Artikel 5a Wet op de medische hulpmiddelen.

Gemakkelijke controle van hulpmiddelen door de EUDAMED

Alle medische hulpmiddelen krijgen een unieke identificatiecode (UDI). Wanneer een patiënt een medisch hulpmiddel met deze unieke streepjescode gebruikt, is het voor iedereen onmiddellijk duidelijk om welk hulpmiddel het gaat. Door het invoeren van de UDI zijn hulpmiddelen beter traceerbaar en kunnen vervalsingen beter worden opgespoord. Bovendien worden zorginstellingen verplicht om een register aan te leggen van de UDI's voor hoog risico-implanteerbare medische hulpmiddelen die zij hebben gebruikt bij de behandeling van de patiënt.

Het hulpmiddel met de UDI wordt door de fabrikant ingeschreven in de EUDAMED. De EUDAMED is de Europese databank voor informatie over medische hulpmiddelen en fabrikanten. Zorginstellingen hebben toegang tot dezelfde openbare delen van EUDAMED als patiënten. Deze databank kan erg nuttig zijn om informatie over de medische hulpmiddelen te verzamelen tijdens het inkoopproces. De EUDAMED is nog niet vrijgegeven. Verwacht wordt dat het in mei 2022 in gebruik zal worden genomen. In deze overgangsperiode blijven fabrikanten zich registreren zoals zij dat nu ook doen. Ook voor zorginstellingen gelden dezelfde verplichtingen omtrent de registratie van de hulpmiddelen.

Medisch-wetenschappelijk onderzoek

De MDR heeft niet alleen gevolgen voor het veilig gebruik van medische hulpmiddelen in de patiëntenzorg, maar is ook van toepassing wanneer er medische hulpmiddelen worden gebruikt in medisch-wetenschappelijk onderzoek.[6] Met medisch-wetenschappelijk onderzoek wordt hier bedoeld, onderzoek dat als doel heeft het beantwoorden van een vraag op het gebied van ziekte en gezondheid.[7]

6. Artikel 2.46 MDR.
7. Artikel 1.1.b Wet medisch-wetenschappelijk onderzoek met mensen (en zie verder de website van de Centrale Commissie Mensgebonden Onderzoek).

Zorginstellingen moeten er ook bij een medisch-wetenschappelijk onderzoek rekening mee houden dat zij de hulpmiddelen gebruiken volgens het beoogd doeleind van de fabrikant. Een uitzondering wordt gemaakt voor hulpmiddelen die worden gebruikt in het kader van een conformiteitsbeoordelingsprocedure van artikel 62 MDR of de Post-market Clinical Follow-up zoals is bedoeld in artikel 74 MDR. De zorginstelling moet bij ieder ander medisch-wetenschappelijk onderzoek de fabrikant betrekken. Ook moet de zorginstelling, net zoals bij het ontwikkelen van interne hulpmiddelen, technische documentatie opstellen en dit bij het onderzoeksprotocol voegen. Deze documenten worden vervolgens beoordeeld door een toetsingscommissie.[8]
Ten slotte moet de zorginstelling gedurende het onderzoek incidenten registreren en ernstige incidenten melden bij de IGJ. De zorginstellingen en fabrikanten zullen nauw moeten samenwerken, want op de fabrikant rust de verplichting om het onderzoek aan en af te melden bij de IGJ. Tenzij de zorginstelling het hulpmiddel in een onderzoek buiten de instelling gebruikt, dan wordt de zorginstelling aangemerkt als fabrikant en zal de zorginstelling het onderzoek moeten aanmelden.

8. Artikel 82 AVG.

Plan van aanpak

Voldoet u al aan de MDR? Of moet u nog beginnen? Als zorginstelling moet u in beeld hebben wat de MDR betekent voor het verlenen van goede zorg. Om dit in kaart te brengen, bevat een gedegen plan van aanpak in ieder geval een nulmeting, gap-analyse en een roadmap.

Tijdens de nulmeting beoordeelt u de reeds ingekochte medische hulpmiddelen, stelt u de stand van zaken vast met betrekking tot intern vervaardigde hulpmiddelen en beoordeelt u aan welke verplichtingen u al wel voldoet en welke nog niet. Het is goed mogelijk dat u al aan bepaalde verplichtingen uit de MDR voldoet door de overlap met andere wetgeving, zoals de Algemene verordening gegevensbescherming (AVG) en de Wkkgz. Hierna kan er doormiddel van een roadmap in kaart worden gebracht welke maatregelen er nog genomen moeten worden om te voldoen aan de MDR om ten slotte aan de slag te gaan met de implementatie. In veel gevallen moet u ook een kwaliteitsmanagementsysteem implementeren. Dergelijk systeem kent de plan-do-check-act cyclus. Na de implementatie is dus beheer nodig van de getroffen maatregelen, na de do-fase komt u (na verloop van tijd) in de check-fase. Wellicht heeft u deze cyclus reeds in uw bedrijfsvoering geïmplementeerd. De maatregelen ten behoeve van het veilig gebruik maken (en doorontwikkeling indien relevant) van medische hulpmiddelen moeten hierin worden meegenomen.

26 mei 2021 is verstreken. De MDR is van toepassing. De deadline zal niet meer opschuiven. Na een jaar vertraging als gevolg van de coronapandemie kunnen betrokken partijen niet langer meer wachten. De MDR is van toepassing en die zal worden gehandhaafd. Dit vergt ook voor zorginstellingen een goede voorbereiding, want de MDR bevat harde sancties.

Brengt u medische software op de markt?

ICTRECHT adviesbureau

Vanaf 26 mei 2021 geldt de nieuwe wetgeving over medische hulpmiddelen: de Medical Device Regulation (MDR). Brengt u software met een medisch doeleinde op de markt? Wellicht levert u dan een medisch hulpmiddel. Afhankelijk van de risico's die de medische software met zich meebrengt, wordt het medisch hulpmiddel in een bepaalde risicoklasse ingedeeld. Wanneer niet wordt voldaan aan de MDR, kunnen er boetes worden opgelegd (tot € 870.000 of 10% van de omzet van het laatste boekjaar).

ICTRecht biedt MDR-specialisten aan met kennis van regelgeving en kwaliteitsmanagementsystemen voor medische hulpmiddelen die u kunnen helpen met:

- het kwalificeren en classificeren van medische software;
- het bieden van ondersteuning bij de voorbereiding op de conformiteitsbeoordeling door een notified body; en
- het vervullen van de rol van een "Person Responsible for Regulatory Compliance" (PRRC) op afstand of op locatie; en
- het opleiden van uw eigen PRRC.

Meer weten?
Lees onze factsheet op: ictrecht.nl/factsheet-MDR
Of neem contact op via: zorg@ictrecht.nl

Isabella Oelz
Juridisch adviseur

Jay Remmelzwaal
Juridisch adviseur

Privacy

Een ongeluk zit in een klein hoekje: hoe om te gaan met datalekken?

In vergelijking met de rest van Europa was Nederland samen met Duitsland in 2020 koploper in de hoeveelheid gemelde datalekken. Zo meldt Financial Times, naar aanleiding van een onderzoek van DLA Piper.[1] Het aantal datalek meldingen in Europa stijgt nog steeds. Het totaal van 121.165 meldingen in 2020 is een stijging van bijna 20 procent vergeleken met dezelfde periode in 2019. Ook de daarmee gepaard gaande boetes die zijn opgelegd op grond van de Algemene verordening gegevensbescherming (AVG) zijn afgelopen jaar flink gestegen. Gelukkig voorkom je met de juiste omgang met datalekken zowel financiële- als imagoschade. Het is zaak om zorgvuldig te handelen als een datalek zich voordoet. Maar hoe doet u dat?

1. Financial Times, GDPR fines jump as EU regulators raise pressure on business, 19-01-2021.

Wat is een datalek ook alweer?

Koopt u wel eens een ticket voor een pretpark, museum of een dierentuin? Brengt u uw auto wel eens naar de garage? Heeft u Facebook? Of bent u wel eens patiënt in het HagaZiekenhuis geweest? Grote kans dat uw persoonsgegevens in dat geval gelekt zijn. De laatste tijd zijn er veel omvangrijke datalekken in de media terecht gekomen. Het blijkt wel dat een ongeluk in een klein hoekje zit.

Natuurlijk is voorkomen beter dan genezen. Maar ongelukjes met data gebeuren nu eenmaal. Daarom dienen organisaties scherp te zijn op het constateren van (mogelijke) datalekken. Temeer omdat de Autoriteit Persoonsgegevens (AP) veel waarde hecht aan een zorgvuldige afhandeling van datalekken. Een zorgvuldige afhandeling begint bij weten wat een datalek is. Er moet een belletje gaan rinkelen indien zich een (mogelijk) datalek voordoet.

In de volksmond wordt gesproken van een datalek. De AVG spreekt echter van een 'inbreuk in verband met persoonsgegevens'.[2]

2. Art. 4 lid 12 AVG.

Een datalek begint met een beveiligingsincident. Denk aan een hacker die zich toegang verschaft tot een database of een kwijtgeraakte USB-stick. Een beveiligingsincident is nog geen datalek. Er is pas sprake van een datalek als er persoonsgegevens in het spel zijn: een inbreuk op de persoonsgegevens. Er bestaan drie soorten inbreuken:

1. 'Inbreuk op de vertrouwelijkheid' – als er sprake is van ongeoorloofde of onbedoelde verstrekking van of toegang tot persoonsgegevens. Bijvoorbeeld een hacker die toegang heeft tot een database met persoonsgegevens.
2. 'Inbreuk op de integriteit' – als er sprake is van een ongeoorloofde of onopzettelijke wijziging van persoonsgegevens. Bijvoorbeeld een hacker die persoonsgegevens in een database heeft gewijzigd.
3. 'Inbreuk op de beschikbaarheid' – als er sprake is van een onopzettelijk of ongeoorloofd verlies van toegang tot persoonsgegevens of een onopzettelijke of ongeoorloofde vernietiging van persoonsgegevens. Bijvoorbeeld een hacker die een database met gijzelsoftware heeft versleuteld.

Een combinatie van inbreuken is mogelijk. Datalekken kunnen verregaande gevolgen hebben voor de privacy van betrokkene(n). Er is daarom een meldplicht in het leven geroepen. Afhankelijk van het privacyrisico van het datalek moet er een melding worden gedaan aan de AP en de betrokkene(n). Bovendien kunnen datalekken in de media terecht komen, wat kan zorgen voor imagoschade.

Om een datalek zorgvuldig af te handelen is het verstandig een procedure te implementeren in de organisatie, zodat alle medewerkers weten wat hen te doen staat wanneer een datalek zich voordoet. Een dergelijke procedure kan worden vastgelegd in een zogeheten 'calamiteitenplan datalekken'. De volgende stappen kunnen helpen bij het opstellen van een calamiteitenplan datalekken.

Stappenplan voor het afhandelen van een datalek

Stap 1: inventarisatie en registratie

Is er een vermoeden van een datalek, dan is het belangrijk om *direct* te onderzoeken of dit vermoeden juist is. Aanleiding kan een melding van een journalist zijn die een datalek heeft ontdekt, zoals het geval was bij de datalekken bij RDC en Ticketcounter. Ook als een oplettende betrokkene je als organisatie op de hoogte stelt van een verdacht mailtje van een onbekende partij, zoals bij Booking gebeurde, is dat een reden om meteen tot actie over te gaan. Is het vermoeden juist en is er een redelijke mate van zekerheid dat een inbreuk in verband met persoonsgegevens zich heeft voorgedaan, dan is dat tevens het moment dat de tijd gaat tikken om het datalek (als verwerkingsverantwoordelijke) binnen 72 uur te melden. Ondertussen dient het datalek in ieder geval intern te worden geregistreerd. De verwerkingsverantwoordelijke is verplicht een datalekregister bij te houden.[3] Ook als sprake is van een datalek dat niet gemeld hoeft te worden moet deze wel geregistreerd worden. Als verwerker is het de bedoeling dat je het datalek zonder onredelijke vertraging meldt bij de verwerkingsverantwoordelijke.

3. Art. 33 lid 5 AVG.

Stap 2: damage control

Vervolgens is het belangrijk dat de aard en omvang van het datalek in kaart wordt gebracht. Om welke persoonsgegevens gaat het en hoe heeft het lek kunnen ontstaan? Dit onderzoek kan worden uitgevoerd in samenwerking met de ICT-afdeling en de functionaris gegevensbescherming. Een goede samenwerking tussen verwerkingsverantwoordelijke en verwerker is belangrijk. De verwerker heeft in de meeste gevallen meer informatie over het datalek. De verwerker is volgens de AVG verplicht om bijstand te verlenen aan de verwerkingsverantwoordelijke.

Als de aard en omvang van het datalek bekend is, dan is het zaak om eventuele schade zo veel mogelijk te beperken. Ook als de pers op het datalek duikt is het belangrijk dat er een mediaprotocol klaarligt om reputatieschade te voorkomen. Laat medewerkers bijvoorbeeld doorverwijzen naar de aangewezen persoon met een (juridisch) doordacht verhaal op zak.

Stap 3: melding Autoriteit Persoonsgegevens

Indien het datalek een risico inhoudt voor de privacyrechten van betrokkenen dient de verwerkings-

verantwoordelijke binnen 72 uur na ontdekking, een melding te doen bij de AP. Ook indien nog niet alle informatie compleet is over het datalek is het belangrijk de melding binnen 72 uur te doen. In dat geval is het mogelijk informatie later aan te vullen in een vervolgmelding.

Stap 4: informeren betrokkenen

Behalve het melden van het datalek aan de AP moet ook worden nagegaan of betrokkene(n) over het datalek moeten worden geïnformeerd. Informeren over het datalek aan de betrokkene(n) is verplicht als het datalek een hoog privacyrisico met zich meebrengt voor de rechten en vrijheden van de betrokkene(n).[4] Indien een melding aan de betrokkene(n) wordt gedaan kan ook informatie worden meegestuurd over de maatregelen die betrokkene(n) zelf nog kunnen nemen om de schade te beperken. Bijvoorbeeld het wijzigen van een wachtwoord, of extra alert zijn voor phishing mails.

4. Art. 34 AVG

Stap 5: evaluatie

Het is een open deur, maar hoe kon het datalek ontstaan en wat is er goed en wat is fout gegaan? Zijn er lessen te leren uit het datalek zodat herhaling kan worden voorkomen? Het is belangrijk om datalekken te evalueren.

Wie moet het datalek afhandelen?

Een verwerkersverantwoordelijke is ook verantwoordelijk voor de afhandeling van het datalek. De verwerker dient bijstand te leveren, en heeft een faciliterende rol. In de praktijk gaat dit nog wel eens mis als een datalek ontstaat bij de verwerker. De verwerker kan de neiging hebben om het heft in eigen handen te nemen, door bijvoorbeeld betrokkene(n) te informeren of een melding doen bij AP. Als verwerker neem je in dat geval een risico door opeens wel de verantwoordelijke rol op je te nemen. Begrijpelijk, maar als verwerker niet handig om te doen.

Lever als verwerker de bijstand die wordt gevraagd, en neem een faciliterende houding aan. Het is belangrijk om de bepalingen na te leven die zijn opgenomen in de verwerkersovereenkomst. Zet aanvullend op papier welke bijstand de verwerker levert aan de verwerkingsverantwoordelijke. De verwerker kan bijvoorbeeld helpen met het opstellen van een bericht met alle relevante informatie voor verwerkingsverantwoordelijke(n) om betrokkene(n) op de hoogte te stellen van het datalek. Pas er als verwerker wel mee op dat je niet te veel op stoel gaat zitten van verwerkingsverantwoordelijke.

Waar let de AP op?

Als een datalek zich voordoet let de AP op verschillende zaken. Wij lichten er een aantal uit.

Ten eerste of de organisatie 'passend beveiligingsmaatregelen' heeft genomen.[5] Had een datalek voorkomen kunnen worden door middel van encryptie en het versleutelen van gegevens en was de juiste autorisatie ingesteld? De AP heeft in 2019 een boete opgelegd aan het HagaZiekenhuis omdat het ziekenhuis onvoldoende passende maatregelen had genomen medische dossiers van patiënten te beschermen.[6]

5. Art. 32 AVG.
6. https://bit.ly/3bHHUyt. Deze boete heeft de rechtbank in Den Haag onlangs gematigd van € 460.000 naar € 350.000 (zie Rb. Den Haag 31 maart 2021, zaak AWB 20-1516).

Ten tweede is het van belang of het datalek op tijd is gemeld aan de AP.[7] Booking werd een flinke boete opgelegd omdat het datalek 22 dagen te laat is gemeld. Belangrijke les is dat ieder signaal dat mogelijk sprake is van een datalek serieus moet worden opgepikt. Bewustzijn bij medewerkers speelt daarbij een belangrijke rol.

7. Art. 33 AVG

Andere zaken waar de AP op let zijn bijvoorbeeld welke persoonsgegevens zijn gelekt en waar deze terecht zijn gekomen. Een Burgerservicenummer is bijvoorbeeld gevoeligere informatie dan een e-mailadres. Naar aanleiding van het datalek bij de GGD, waar adressen, telefoonnummers en Burgerservicenummers zijn gelekt, heeft de AP geadviseerd burgers goed en snel te informeren over de diefstal. De persoonsgegevens zijn namelijk in handen van onbekende criminelen gekomen, dat is een extra reden voor betrokkenen om alert te zijn.

Indien gegevens eenmaal gelekt zijn, is het soms lastig om het lek te dichten. Toch is dat ook iets waar de AP op let, of het datalek voldoende adequaat is beëindigd en of er voldoende vervolgmaatregelen worden genomen. Ons devies is: probeer zoveel mogelijk te doen om de schade te beperken.

Een datalek, wat te doen?

ICTRecht biedt eerste hulp bij datalekken

ICTRECHT
adviesbureau

Hoewel het voorkomen van datalekken altijd beter is dan het beperken van de schade achteraf, is het kwaad soms al geschied. Heeft uw organisatie te maken met (de dreiging van) een datalek? De privacy experts van ICTRecht schieten u direct te hulp. Onze hulp stopt niet bij het plakken van de broodnodige pleisters, maar richt zich ook op het voorkomen van toekomstige datalekken.

Meer weten?

Ga naar: bit.ly/331nuM7

Of neem contact op via: 020 663 1941

Bram de Vos
Juridisch adviseur

Wet- en regelgeving

Motie verhoging budget Autoriteit Persoonsgegevens

Op 9 februari 2021 heeft de Tweede Kamer een motie aangenomen met een verzoek aan de regering om meer budget toe te kennen aan de Autoriteit Persoonsgegevens (AP). De motie werd mede gebaseerd op een onderzoek dat afgelopen jaar door KPMG werd uitgevoerd in opdracht van het Ministerie van Veiligheid en Justitie en de AP gezamenlijk. Mede op basis van dit onderzoek heeft de AP een groeiplan vastgesteld. Daarin wordt als uitgangspunt genomen dat de capaciteit van de toezichthouder zal moeten groeien van 184 naar 470 fte in 2025 om haar wettelijke taken goed te kunnen uitoefenen. Sander Dekker (demissionair minister voor Rechtsbescherming) heeft inmiddels via een kamerbrief laten weten dat hij de beslissing over de toekenning van extra budget overlaat aan het volgende kabinet. In zijn brief plaatst hij wel de nodige kanttekeningen bij de aangenomen motie onder verwijzing naar het KPMG-rapport.

https://bit.ly/33gPJqd

https://bit.ly/3eplDaF

Implementatiewet richtlijnen verkoop goederen en levering digitale inhoud

Op 16 februari 2021 werd het voorstel voor de Implementatiewet richtlijnen verkoop goederen en levering digitale inhoud ingediend bij de Tweede Kamer. Het voorstel strekt tot implementatie van twee nieuwe Europese richtlijnen (EU 2019/770 en EU 2019/771). Met de implementatie worden verschillende aanpassingen doorgevoerd in de bestaande regels over consumentenkoop. Deze wijzigingen zien onder meer op de conformiteitseis, de verhaalsmogelijkheden van de consument en de vereisten voor commerciële garanties. Ook wordt er een nieuwe titel aan Boek 7 van het Burgerlijk Wetboek toegevoegd over de levering van digitale inhoud en digitale diensten. De belangrijkste verandering die hieruit voortvloeit, is de verplichting van handelaars om (binnen bepaalde kaders) updates aan de consument te verstrekken.

https://bit.ly/3nO7eaS

Wetsvoorstel verkorting wettelijke betaaltermijn tot 30 dagen

Op 16 maart 2021 werd een wetsvoorstel tot verkorting van de wettelijke betaaltermijn ingediend bij de Tweede Kamer. Het voorstel strekt tot aanpassing van artikel 6:119a van het Burgerlijk Wetboek. Op grond van dat artikel mogen grote ondernemingen richting het mkb momenteel nog een betaaltermijn van maximaal 60 dagen bedingen. Na de invoering van het wetsvoorstel geldt een maximumtermijn van 30 dagen. Als partijen toch een langere betaaltermijn afspreken, is deze afspraak nietig en geldt van rechtswege een termijn van 30 dagen. Het toepassingsbereik van de regeling blijft ongewijzigd en geldt alleen in handelsrelaties waarbij een grote onderneming als schuldenaar optreedt en een mkb-ondernemer als schuldeiser.

https://bit.ly/3uq87J6

Wet implementatie richtlijnen elektronische handel

Op 6 april 2021 heeft de Eerste Kamer ingestemd met de Wet implementatie richtlijnen elektronische handel. De inhoud van dit wetsvoorstel kwam in editie 2020-4 van dit tijdschrift al aan bod. Kort samengevat wordt middels het wetsvoorstel de heffing van btw op grensoverschrijdende internetverkopen gemoderniseerd en vereenvoudigd. De wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip (naar verwachting 1 juli 2021).

https://bit.ly/3eia8S9

Verordening geharmoniseerde regels inzake kunstmatige intelligentie

Op 21 april 2021 heeft de Europese Commissie een concept van de Verordening geharmoniseerde regels inzake kunstmatige intelligentie gepubliceerd. In de verordening worden verschillende toepassingen van kunstmatige intelligentie expliciet verboden. Denk aan toepassingen waarbij real time biometrische identificatie plaatsvindt in de openbare ruimte. Verder richt de Europese Commissie zijn pijlen hoofdzakelijk op toepassingen van kunstmatige intelligentie waar een 'hoog risico' aan vastzit. Of er sprake is van een hoog risico, moet worden vastgesteld aan de hand van verschillende criteria, zoals de impact op grondrechten van burgers en veiligheids- en gezondheidsaspecten. Wordt een bepaalde toepassing met een hoog risico bestempeld, dan gelden allerlei inhoudelijke eisen om de veiligheid daarvan te waarborgen. Zo moet er een risicomanagementsysteem worden ingericht en worden er eisen gesteld aan de datasets die voor de toepassing worden gebruikt. Zie ook het artikel op bladzijde 4.

https://bit.ly/3fauwEb

Advies EDPB inzake adequaatheidsbesluiten

Op 13 april 2021 heeft het European Data Protection Board (EDPB) twee adviezen gepubliceerd met betrekking tot de voorgenomen adequaatheidsbesluiten voor de doorgifte van persoonsgegevens naar het Verenigd Koninkrijk. Op 31 december 2020 stapte het Verenigd Koninkrijk definitief uit de Europese Unie. Daarmee kwalificeert het Verenigd Koninkrijk voortaan als 'derde land' onder de Algemene verordening gegevensbescherming (AVG) en de Richtlijn politie en justitie. Doorgifte van persoonsgegevens is daardoor niet zonder meer mogelijk. Eén van de mechanismen om deze doorgifte juridisch toch mogelijk te maken, is middels een zogeheten adequaatheidsbesluit van de Europese Commissie. Het EDPB heeft nu advies uitgebracht aan de Europese Commissie over de voorgenomen besluiten. Volgens het EDPB is de privacy ook na de Brexit goed beschermd in het Verenigd Koninkrijk. Wel ziet het EDPB ook aandachtspunten, met name als het gaat om de mogelijkheid dat persoonsgegevens straks – via het Verenigd Koninkrijk – in andere landen terecht komen (zoals de Verenigde Staten).

https://bit.ly/33oCrI9

https://bit.ly/3eWaw7Z

Implementatiewet richtlijn representatieve vorderingen voor consumenten

Op 1 mei 2021 ging de internetconsultatie voor de Implementatiewet richtlijn representatieve vorderingen voor consumenten van start. Dit wetsvoorstel strekt tot implementatie van de Europese richtlijn (EU 2020/1828). Het wetsvoorstel bevat een aantal aanpassingen van de Wet afwikkeling massaschade in collectieve actie (WAMCA). Zo gaan er bijvoorbeeld nieuwe eisen gelden als het gaat om het financieren van de collectieve actie. Ook voorziet het wetsvoorstel in aanvullende voorschriften voor deelname aan de actie. De consultatie staat nog open tot 31 mei 2021.

https://bit.ly/2Rmoub7

Sten Demon
Directeur ICTRecht Legal Tech

Innovatie

Legal tech
Weerstand tegen vooruitgang

De impact van nieuwe technologieën op de banenmarkt is een soort glijdende schaal. Toch? Banen op mbo-niveau zullen eerder last hebben van automatisering dan banen op hbo- of wo-niveau. Want 'makkelijke' banen zijn natuurlijk 'makkelijk' te automatiseren en 'complexe' werkzaamheden van juristen en advocaten zijn daarom zeer bestand tegen veranderingen door nieuwe technologieën. Althans, veel juristen en advocaten hebben volgens mij deze verwachting. Maar is dit wel zo? Zijn onze juridische werkzaamheden niet veel makkelijker te automatiseren dan de werkzaamheden van bijvoorbeeld een loodgieter of klusjesman?

De voornoemde vraag is wat mij betreft makkelijk te beantwoorden. Ik verwacht eigenlijk dat veel van mijn juridische werkzaamheden eerder overgenomen zullen worden door slimme software, dan dat een robot de taken van een loodgieter kan overnemen. Veel juristen en advocaten schieten echter automatisch in de verdediging als het gaat om innovaties en technologieën voor de juridische sector. Bijna dagelijks hoor ik van juristen dat er wellicht een klein percentage van de werkzaamheden geautomatiseerd kan worden, maar dat ze zich verder bezighouden met *uniek maatwerk* dat echt niet geautomatiseerd kan worden.

Deze reacties van juristen zijn begrijpelijk. Mensen houden nou eenmaal niet van verandering en al helemaal niet als het *hun* werk is dat geautomatiseerd wordt. Als legal tech te dichtbij komt, wordt het algauw eng. Want geen enkele jurist wil zonder werk komen te zitten. Was rechtsgeleerdheid immers niet die studie die ongetwijfeld zou leiden tot baanzekerheid? De jurist kan toch onmogelijk overbodig worden? Hoewel ik niet denk dat het zover komt, denk ik wel dat het onvermijdelijk is dat legal tech een deel van de menselijke werkzaamheden overbodig zal maken. Software kan op dit moment al meer dan mensen denken en gaat in de toekomst alleen maar meer kunnen. Maar, wees gerust, er zit

wel een kern van waarheid in de genoemde reacties. Uniek maatwerk is inderdaad moeilijk te automatiseren.

Als ik aan juristen vraag wat dan het unieke maatwerk is dat niet te automatiseren valt, dan lopen de antwoorden erg uiteen. Nee, ik zie een robot niet zo snel een emotioneel pleidooi houden of *out of the box* denken bij moeilijke contractonderhandelingen. Dit is echt mensenwerk, maar bij welke jurist vormt dit momenteel het merendeel van de dagelijkse werkzaamheden? Sommige juristen noemen het opstellen en controleren van contracten ook als het mensenwerk dat nog lang niet vervangen kan worden door software. Nu een groot deel van alle contracten bestaat uit standaardafspraken, wordt het opstellen en controleren van contracten echter sneller geautomatiseerd dan je zou verwachten. Zie bijvoorbeeld reeds bestaande oplossingen als NDA Lynn en DPA Lynn die geheimhoudingsovereenkomsten en verwerkersovereenkomsten kunnen controleren en becommentariëren.

Weerstand tegen deze vooruitgang is echter nergens voor nodig. Uw juridische werkzaamheden zullen niet allemaal van de ene op de andere dag verdwijnen. Wel gaat legal tech ervoor zorgen dat uw werkzaamheden veranderen. Sterker nog, legal tech gaat uw werkzaamheden verbeteren. Het gaat er namelijk voor zorgen dat u minder tijd kwijt bent aan standaardwerkzaamheden en u meer tijd kunt besteden aan de interessante vraagstukken waarbij wat creativiteit komt kijken. Wat overblijft zijn dus de leemtes in de wet en de zoektocht naar wat 'afhankelijk is van de omstandigheden van het geval'. Laat DPA Lynn bijvoorbeeld de standaardopmerkingen plaatsen in de verwerkersovereenkomst, zodat u, u kunt focussen op valkuilen die software niet gemakkelijk herkent, zoals de onderlinge samenhang tussen een hoofdovereenkomst, verwerkersovereenkomst en eventuele andere bijbehorende overeenkomsten. Door deze focus ontdekt u misschien wel knelpunten die u over het hoofd zou zien als u ook alle standaardclausules zou moeten voorzien van steeds dezelfde soort opmerkingen.

Voor de gepassioneerde juristen blijft er dus niet alleen genoeg werk over, maar zelfs meer ruimte om zich te focussen op het uitdagende werk. Een mooi vooruitzicht, vind ik zelf. Maar een vooruitzicht waar wel nog wat voor nodig is. Dit bereiken wij niet vanzelf. Net als andere sectoren, zal ook de juridische sector innovatie moeten omarmen. De jurist zal zijn – of haar – angst voor verandering moeten overwinnen en het voorbeeld van de wetgever moeten volgen. Immers huppelen wetten ook altijd technologische ontwikkelingen achterna, hoewel dat nooit snel genoeg gaat.

Naast de weerstand tegen verandering merk ik ook dat juristen niet gemakkelijk nieuwe technologieën omarmen vanwege perfectionisme. Alle omstandigheden en kleine nuances zijn tenslotte zeer belangrijk in het recht. Een minimaal misverstand kan grote gevolgen hebben. Software die in 90% van de gevallen juiste adviezen geeft omdat het niet alle nuances kan toepassen, is voor de jurist niet goed genoeg en wordt daarom niet geaccepteerd. Dit terwijl juristen ook maar mensen zijn die fouten maken. Waarom moet software dan perfect zijn? Zelfs als de software niet perfect is, kan het enorme tijdwinst opleveren als de jurist alleen wat foutjes in het advies van de software hoeft te verbeteren in plaats van het compleet zelf opstellen van een advies. Daarnaast kan de software juist snel verbeterd worden als het veel wordt gebruikt en er veel feedback wordt gegeven.

Kortom, het is tijd om ergens te starten en de leiding van de andere sectoren te volgen. Legal tech wordt dan steeds beter en normaler. Denk aan de HR-afdeling. Dient u vakantieverzoeken nog steeds in per e-mail of gaat dat via een portal? En bij een verhuizing; geeft u dan uw nieuwe adres door per e-mail of wijzigt u uw adres zelf in een portal? Volgens mij zijn deze portals nu de norm. Dit terwijl alle juridische vragen nog op één hoop binnenkomen bij de juridische afdeling. Aan de slag dus.

Hopelijk laat dit artikel u inzien dat terughoudendheid ten aanzien van innovatie niet nodig is. Natuurlijk kan en hoeft u nu niet direct allerlei legal tech in gebruik te nemen. De eerste stap is het bespreken en opstellen van een agenda of plan voor de komende jaren. Welke strategie zou u willen toepassen als het gaat om legal tech en welke veranderingen kunnen uw organisatie het meeste voordeel opleveren? Met een goed plan en duidelijke tijdlijnen, kunt u de komende jaren stap voor stap innoveren. Dat doen uw concurrenten immers ook.

Kors Monster
Directeur ICTRecht Security

Johnny Honing
Information security consultant

Security

Pragmatisch omgaan met uw informatiebeveiliging

In onze huidige samenleving is data niet meer weg te denken en het wordt voor de meest uiteenlopende toepassingen verzameld, verwerkt en gedeeld. Denk aan social media, aanraden van nieuwe films en series & dating. Aan de andere kant ook voor bijvoorbeeld rampenbestrijding, rijstrookbeheer, marketingcampagnes, verkiezingen, virusbestrijding en ga zo maar door.

Ook binnen uw organisatie is de kans groot dat er een grote verscheidenheid aan data verwerkt wordt. Denk hierbij bijvoorbeeld aan klant- en leveranciersgegevens, financiële gegevens, maar ook informatie over producten en diensten én vergeet natuurlijk niet de informatie van u en uw personeel! Als u er even over nadenkt komt u waarschijnlijk tot de conclusie dat er méér informatie binnen de organisatie aanwezig is dan u op het eerste gezicht dacht. En dat deze informatie om verschillende redenen van waarde is.

Het topje van de ijsberg

Onlangs zult u er vast over gehoord hebben: “Grote kwetsbaarheden gevonden in Microsoft Exchange”, “3,6 miljoen klantgegevens op straat door omvangrijke hack bij allekabels.nl”, “500 miljoen gegevens van LinkedIngebruikers op straat” en “Kwetsbaarheden in OpenSSL”.

Dit zijn zomaar een aantal nieuwberichten die het afgelopen kwartaal de revue zijn gepasseerd. Dan hebben we het natuurlijk over de grootschalige hacks en kwetsbaarheden waar we van weten. Door dit soort berichtgeving zien wij ook een steeds grotere bewustwording over de gevoeligheid van informatie en hoe hier mee wordt omgegaan. Logischerwijs betekent dit ook dat men kritischer wordt over wie toegang heeft tot welke data én voor welk doel de informatie wordt ingezet.

Perspectief op informatiebeveiliging verandert

U en uw organisatie worden kritischer, maar ook uw klanten worden dat! Daarom is het van groot belang dat u uw informatiebeveiliging goed op orde heeft. Klinkt logisch, maar hoe doet u dat op een goede manier en hoe is dat momenteel bij uw organisatie gerealiseerd?

Vaak wordt informatiebeveiliging gezien als een belemmering van de huidige bedrijfsprocessen. Immers: er moeten verscheidene maatregelen genomen worden om gegevens te beschermen, of om te voldoen aan wet- en regelgeving. Dit kost tijd, middelen en geld en vanuit een commercieel oogpunt is dit veelal een doorn in het oog. Ook lijkt dit vaak een zeer gecompliceerd onderwerp. Het oogt daarom verleidelijk om nog maar even af te wachten: "In de afgelopen tijd is het ook altijd goed gegaan, dus we kunnen vast nog even zo door."

Om een andere kijk op het geheel te krijgen, is het wellicht goed om vanuit een ander perspectief naar informatiebeveiliging te kijken.

Als we het zouden omdraaien en u zouden vragen; wat zou het u kosten, als u X periode geen toegang heeft tot uw gegevens? Of, wat zou de imagoschade voor uw onderneming zijn als uw klantgegevens op straat komen te liggen? Wat zijn de consequenties als u er niet meer vanuit kunt gaan dat uw informatie juist en actueel is?

Informatiebeveiliging dient uw bedrijf, en niet andersom

De vraagstukken die in de vorige alinea worden opgeworpen, zijn typisch de vragen die het eerst worden gesteld als u aan de slag gaat met informatiebeveiliging. Het uitgangspunt moet zijn, dat uw informatiebeveiliging in lijn moet zijn met uw bedrijfsprocessen. Door uw informatiebeveiliging vóór u te laten werken, bespaart u dus op de langere termijn kosten door een zekerheid in te bouwen ten aanzien van de continuïteit van uw bedrijfsprocessen.

Dit illustreert ook meteen het doel van informatiebeveiliging; uw gegevens moeten te allen tijde bereikbaar zijn voor diegene die deze informatie nodig heeft. De informatie moet volledig en correct zijn en deze informatie mag niet toegankelijk zijn voor derden. Stel uzelf daarom ook de vraag; wat is cruciaal voor de bedrijfsvoering? Met andere woorden: wat is voor óns van belang om te kunnen blijven functioneren? Gefeliciteerd! Wanneer u dit inzichtelijk heeft, is de eerste stap naar een betere informatiebeveiliging gezet.

Word bewust van risico's en neem er controle over

Nu u weet welke informatie en -systemen voor u van waarde zijn, is het van belang om te bekijken waar de kwetsbaarheden in uw organisatie zich (kunnen) voordoen. Door deze risicoanalyse heeft u duidelijk inzichtelijk welke risico's acceptabel zijn voor uw organisatie en voor welke risico's u een plan de campagne op dient te stellen.

Een risicoanalyse kan op verschillende manieren plaatsvinden. Er zijn verschillende normen en standaarden beschikbaar, maar uiteindelijk kiest elke organisatie zelf hoe zij dit inregelt. Het is van belang dat de analyse aansluit op de wens en behoefte van uw onderneming, zodat er organisatiebreed een draagvlak ontstaat. Betrek bij deze analyse ook alle informatie-eigenaren! Denk hierbij aan bijvoorbeeld de IT-manager, inkoopmanager, salesmanager en de boekhouding, maar vergeet ook niet de warehouse manager en de HR-manager. Uiteindelijkis de directie verantwoordelijk voor de acceptatie of minimalisering van de risico's, maar de genoemde informatie-eigenaren, kunnen u een duidelijk beeld geven van de risico's die zij binnen uw organisatie zien. Last but not least; breng ook in kaart welke externe partijen (leveranciers, Cloud-providers, CRM-provider) een mogelijk risico vormen voor uw informatiebeveiliging!

Selecteren van 'passende technische en organisatorische beveiligingsmaatregelen'

De volgende stap is het kiezen van adequate maatregelen voor de risico's. Er zijn veelal meerdere maatregelen te implementeren voor één en hetzelfde risico. Daarnaast zijn er maatregelen die meerdere risico's kunnen reduceren. Denk hierbij bijvoorbeeld aan een slot op de deur naar een serverruimte, maar ook een persoonsgebonden login voor de server. Ander voorbeeld is een back-up maken van uw data op een andere locatie, of in de Cloud werken, zodat uw informatie altijd toegankelijk blijft.

Kies daarom een maatregel die aan de volgende criteria voldoet:

1. De maatregel brengt het risico naar een acceptabel niveau.
2. De maatregel is meetbaar effectief voor het/de risico('s).
3. De maatregel is in lijn met uw bedrijfsvoering.

Uiteraard zijn er nog meer criteria te bedenken en deze kunt u naar gelang uw organisatie dit verlangt aanpassen.

Nadat de maatregelen geselecteerd zijn, dienen deze

natuurlijk ook geïmplementeerd te worden in uw organisatie. Stem daarom duidelijk af wíe er verantwoordelijk is voor de implementatie en monitoring van de maatregelen. Het kan zo zijn dat bepaalde maatregelen van toepassing zijn voor meerdere informatie-eigenaren en het is daarom van belang dat iedereen weet waar de verantwoordelijkheid ligt om toekomstige interne complicaties te voorkomen.

Continu verbeteren door regelmatig te evalueren

Om de cyclus rond te maken, is het natuurlijk wel van belang dat u periodiek evalueert of de maatregelen nog steeds het gewenste resultaat bieden en of uw risicoanalyse nog relevant is voor uw organisatie. Per slot van rekening leven we in een continu veranderend (digitaal) landschap en iedere dag komen er nieuwe kwetsbaarheden en beveiligingsmaatregelen beschikbaar.

Vergeet ook niet de veranderingen van uw eigen organisatie; groeit u explosief? Slaat uw onderneming een compleet andere weg in? Is er een fusie of overname aanstaande? Is er een wijziging in het personeelsbestand? Al deze factoren hebben invloed op de risico's én voor de maatregelen die u voor uw organisatie heeft gerealiseerd. Plan daarom periodiek een evaluatie van uw informatiebeveiliging. Dit kunt u intern doen, of bijvoorbeeld door het laten plaatsvinden van een externe audit.

Wie moet het overzicht houden over informatiebeveiliging?

Nu u grip hebt op de risico's en passende maatregelen hebt geïmplementeerd volgt natuurlijk een nog belangrijker vraagstuk; wie gaat er binnen uw organisatie zorg voor dragen dat uw informatiebeveiliging op orde is? De directie? De IT/ICT-manager? De informatie-eigenaren zelf? Er zijn een hoop stakeholders rond informatiebeveiliging, en om uw informatie adequaat te beschermen moet de hele organisatie meedoen. Maar het is belangrijk dat iemand daarop het overzicht houdt en het voortouw neemt. Informatiebeveiliging is, net als vele andere functies, een vak apart. Het vraagt iemand die zich continu bezighoudt met nieuwe ontwikkelingen binnen de industrie en die pragmatisch kijkt naar uw informatiebeveiliging, in lijn met de visie en processen van uw bedrijf.

De Chief Information Security Officer (CISO) is de aangewezen persoon om u hierin te ondersteunen. Het NCSC (Nationaal Cyber Security Centrum) onderscheid drie hoofdtaken voor de CISO[1] :

1. Adviseren: antwoord geven op vragen over informatiebeveiliging binnen de organisatie.
2. Coördineren: verantwoordelijkheid over specifieke acties op het gebeid van informatiebeveiliging, zoals het beheren van het ISMS, het begeleiden van risicoanalyses, penetratietesten of awareness-campagnes en het bijhouden van een register voor beveiligingsincidenten.
3. Controleren: nagaan of de organisatie zich houdt aan de regels over informatiebeveiliging die door de directie zijn opgesteld en de directie hierover informeren.

1. www.NCSC.nl – Factsheet Risicomanagement – CISO.

Feitelijk gezien is de CISO uw oor en oog betreffend de informatiebeveiliging binnen de organisatie. Het is dan ook raadzaam om deze als zodanig te positioneren! Een veelgemaakte misvatting is dat uw CISO onder de IT/ICT-manager valt, omdat informatiebeveiliging veelal als "technisch" te boek staat. Helaas zorgt deze positionering van de CISO voor een mogelijke belangenverstrengeling binnen uw organisatie. Neem dit in overweging bij uw besluitvorming.

Conclusie

Deze beknopte roadmap geeft u een illustratie van hoe u, uw informatiebeveiliging kunt benaderen. Ondanks dat sommige factoren best gecompliceerd zijn, is het geen "hogere wiskunde", maar wel degelijk een noodzaak om op orde te hebben. De stappen kunnen leiden tot een volwassen organisatie ten opzichte van informatiebeveiliging, maar zijn natuurlijk niet allesomvattend en zullen specifiek afgestemd moeten worden op de missie en visie van uw organisatie.

Eerder vroegen wij u: hoe brengt u de informatiebeveiliging goed op orde en hoe is dat bij u geregeld? Wij hopen dat u aan de hand van dit artikel voldoende munitie heeft om deze vraag voor uw organisatie te beantwoorden en de benodigde stappen te kunnen initiëren.

ICTRECHT
security

Uw organisatie goed beschermd met ICTRecht Security

ICTRecht Security werkt samen met u aan een veilige organisatie. Wij helpen u om grip te krijgen én te houden op informatiebeveiliging. Zo zorgt u ervoor dat uw security aantoonbaar op orde is en waarborgt u de continuïteit van uw bedrijfsprocessen.

Altijd beschikken over deskundige security ondersteuning? Kies dan voor ICTRecht Security. Wij zijn direct inzetbaar en altijd beschikbaar (24/7). ICTRecht Security staat voor flexibiliteit: u bepaalt wat wij voor u doen en onze abonnementen zijn per maand opzegbaar.

Meer weten?
Ga naar: ictrecht.nl/security
Of neem contact op via:
020 663 1941

Arnoud Engelfriet
Directeur / Opleidingsdirecteur

Internetrechtspraak

Tekortkoming in ICT-onderhoudscontract toegewezen

(Gerechtshof Amsterdam 16 februari 2021)

Appellante heeft voor haar onderneming een ICT-onderhoudscontract afgesloten met geïntimeerde. Nadat dit contract is beëindigd en appellante op het punt staat om een nieuw ICT-onderhoudscontract af te sluiten met een andere partij, wordt de onderneming van appellante gehackt. Appellante lijdt hierdoor schade. Die schade is met name het gevolg van een tekortkoming in de nakoming (door geïntimeerde) van de verplichting om naar behoren te zorgen voor adequate back ups. Geïntimeerde betoogt dat een groot deel van de schade niet aan haar kan worden toegerekend, maar juist aan appellante zelf. Het Hof stelt geïntimeerde in het ongelijk omdat zij wel degelijk een causaal verband ziet tussen de tekortkoming en de geleden schade.

https://bit.ly/3o8p48w

KPN niet verplicht tot afgifte NAW-gegevens

(Rechtbank Rotterdam 1 maart 2021)

Eiser stond voorheen ingeschreven in het Register beëdigde tolken en vertalers. Hij wordt verweten dat hij op frauduleuze wijze niet bestaande tolkopdrachten heeft uitgezet, geaccepteerd en weer geannuleerd om zo annuleringsvergoedingen op te strijken. Als gevolg hiervan is zijn inschrijving uit het Register gehaald. Eiser is tegen deze beslissing in beroep gegaan. Het is hem namelijk opgevallen dat de fraude vanaf verschillende IP-adressen is gepleegd. Gelet hierop vordert hij de NAW-gegevens van de gebruiker van een van deze IP-adressen van KPN. Het bedrijf weigert de gegevens namelijk af te geven. De voorzieningenrechter wijst de vordering af en oordeelt dat de weigering van KPN niet in strijd is met de ongeschreven zorgvuldigheidsnorm vervat in artikel 6:162 BW, omdat het belang van eiser niet opweegt tegen het belang van KPN bij de bescherming van de persoonsgegevens en persoonlijke levenssfeer van haar klant(en).

https://bit.ly/3o8spoj

HvJ EU: toegang tot communicatiegegevens dient beperkt te blijven

(Hof van Justitie van de Europese Unie 2 maart 2021)

H.K. wordt vervolgd in Estland wegens diefstal, gebruik van de bankpas van een ander en geweldpleging tegen betrokkenen bij een gerechtelijke procedure. De Estse rechter heeft H.K. schuldig verklaard aan deze feiten op grond van informatie die zij verkreeg van een aanbieder van elektronische- communicatiediensten. H.K. ging hiertegen in hoger beroep. De hoogste Estse rechterlijke instantie besloot een aantal prejudiciële vragen te stellen aan het Hof van Justitie van de Europese Unie (Hof). De verwijzende rechter vroeg zich af in hoeverre een nationale regeling, in het kader van strafrechtelijk onderzoek, aan een overheidsinstantie toegang mag verlenen tot elektronische-communicatiegegevens die een gedetailleerd beeld van een gebruiker kunnen scheppen. Het Hof verklaart dat een dergelijke regeling niet is toegestaan indien

deze niet is beperkt tot het bestrijden van zware criminaliteit of het voorkomen van *ernstige* bedreigingen van de openbare veiligheid. Daarnaast moet de toetsing van een rechtmatige toegang tot gegevens niet gedaan worden door een organisatie zoals het openbaar ministerie, maar door een (meer) onafhankelijke instantie.

https://bit.ly/33w5w4v

Vrij en Sociaal Nederland krijgt domein terug
(Rechtbank Den Haag 9 maart 2021)

Vrij en Sociaal Nederland (VSN) is een politieke partij. In januari heeft de partij te maken gehad met bestuursperikelen die leidden tot een afsplitsing waaruit de partij Lijst 30 is ontstaan. Een aantal van de afgesplitste leden had echter nog de controle over het domein dat VSN gebruikte. De leden hebben dit om weten te zetten in een *redirect*-link naar de site van Lijst 30. Hierop vorderde VSN dat Lijst 30 het domein terug aan haar moest overdragen. De voorzieningenrechter stelt VSN in het gelijk en beveelt twee bestuursleden van Lijst 30 tot volledige medewerking aan de overdracht van het domein.

https://bit.ly/3o80KUD

Inzage bij Uber : Uber moet (gedeeltelijk) meer persoonsgegevens overleggen aan Britse chauffeurs
(Rechtbank Amsterdam 11 maart 2021)

Verzoekers in deze zaak zijn (voormalig) chauffeurs van Uber. De chauffeurs willen weten welke informatie Uber over hen verzamelt en hoe deze gegevens worden gebruikt. Zij verlangen inzage in interne notities van klantenservicemedewerkers, tags waarmee het gedrag van een chauffeur wordt beoordeeld, *reports* gebaseerd op feedbackmeldingen van passagiers, de start- en eindlocatie van ritten, individuele ratings door passagiers, gegevens over rijgedrag (bijvoorbeeld GPS-data, informatie over versnelling en remmen) en informatie over het *upfront pricing*-systeem. Verder verlangen de chauffeurs inzage in het bestaan van geautomatiseerde besluitvorming en profilering op grond van artikel 15(1)(h) AVG. De rechtbank wijst de vordering tot inzage in de genoemde gegevens slechts gedeeltelijk toe voor wat betreft de individuele ratings. Voor het overige wijst de rechtbank de verzoeken af, onder meer gelet op de privacyrechten van passagiers en algemeen/vaag omschreven verzoeken. Ten aanzien van de geautomatiseerde besluitvorming oordeelt de rechter dat de chauffeurs niet hebben toegelicht dat Uber ten aanzien van hen besluiten heeft genomen op basis van geautomatiseerde besluitvorming. Daarnaast is niet gebleken dat sprake is van een rechtsgevolg of een aanmerkelijk effect hiervan op de chauffeurs. Het verzoek om inzage in dergelijke besluitvorming wordt derhalve afgewezen.

https://bit.ly/3xVQSl8

Facebook moet gegevens van advertentie-accounts afgeven
(Rechtbank Den Haag 17 maart 2021)

PVH is een groot kleding- en modebedrijf dat verschillende merken exploiteert, waaronder Tommy Hilfiger. PHV ontdekte op Facebook en Instagram een aantal advertenties voor kleding en schoeisel met de naam “Tommy Hilfiger” die niet van haar afkomstig waren, dit terwijl zij met Facebook een advertentieovereenkomst had gesloten ten behoeve van haar eigen merk. Een en ander leidde tot een bevel van de voorzieningenrechter jegens Facebook om de nodige maatregelen te nemen tegen de inbreukmakende advertenties. Facebook is hiertegen in beroep gegaan en weigerde om de gegevens van de advertentie-accounts aan PVH te geven. De rechtbank oordeelt dat Facebook deze gegevens alsnog moet afgeven en benadrukt daarbij dat zij het plaatsen van de inbreukmakende advertenties gestaakt dient te houden.

https://bit.ly/3bUSRN8

Implementatie anti-witwasrichtlijn behoeft geen buitenwerkstelling

(Rechtbank Den Haag 18 maart 2021)

In het licht van de implementatie van de vierde en vijfde anti-witwasrichtlijn heeft de Staat wetgeving aangenomen die verplicht tot het registreren van persoonsgegevens van *Ultimate Beneficial Owners* (UBO's) in het UBO-register en vaststelt dat deze gegevens (deels) openbaar toegankelijk zijn. Privacy First vordert (voorlopige) buitenwerkingstelling van deze wetgeving. De voorzieningenrechter wijst de vordering af, omdat er volgens hem geen grond is voor een buitenwerkingstelling.

https://bit.ly/3eBRhSn

Inzagerecht dient beperkt te blijven tot eigen persoonsgegevens

(Rechtbank Rotterdam 19 maart 2021)

Deze zaak gaat in op de omvang van het inzagerecht van betrokkenen zoals neergelegd in artikel 15 van de AVG. Eiser had de staatssecretaris van Justitie en Veiligheid verzocht om inzage in de verwerking van zijn persoonsgegevens. De staatssecretaris heeft daarna aan eiser een overzicht verstrekt. Eiser was echter van mening dat hij ook recht had op achterliggende informatie c.q. onderliggende stukken (waaronder gespreksverslagen en documenten met daarin persoonsgegevens van zijn moeder). De rechtbank overweegt dat het inzagerecht is beperkt tot de persoonsgegevens die de betrokkene zelf betreffen. De uitleg van het begrip 'persoonsgegevens' is dus bepalend voor de reikwijdte van het inzagerecht. Volgens de rechtbank heeft eiser gekregen waar hij recht op heeft, namelijk een overzicht, in begrijpelijke vorm, van alle hem betreffende persoonsgegevens die zijn verwerkt. Artikel 15 AVG geeft immers geen recht op afschriften van originele documenten waarin persoonsgegevens staan, wanneer aan het inzageverzoek kan worden voldaan met een andere vorm van verstrekking. Nu eiser niet aannemelijk heeft gemaakt dat er méér persoonsgegevens dienen te zijn, verwerpt de rechtbank het beroep.

https://bit.ly/3y5JNhV

Begrip 'verwerkingsverantwoordelijke' vereist ruime uitleg

(Rechtbank Rotterdam 19 maart 2021)

Eiser uit de hiervoor genoemde zaak had tevens een inzageverzoek ingediend bij de minister van Buitenlandse Zaken. Aanleiding voor dit verzoek was een e-mail die eiser had ontvangen van de Dienst Terugkeer en Vertrek (DT&V). Daarin stonden persoonsgegevens opgenomen die volgens DT&V afkomstig zouden zijn van de minister van Buitenlandse Zaken. De minister heeft het verzoek afgewezen, mede omdat hij stelde niet de verwerkingsverantwoordelijke van de gegevens te zijn. De rechtbank oordeelt echter dat de minister wel degelijk verwerkingsverantwoordelijke van de gegevens is. Het begrip 'verwerkingsverantwoordelijke' dient namelijk ruim te worden uitgelegd. Volgens de rechtbank heeft de minister niet afdoende (met stukken) onderbouwd dat hij zelf geen feitelijke invloed heeft gehad op de verwerking van de persoonsgegevens van eiser. Dat een identiteitsonderzoek in opdracht van DT&V altijd wordt uitgevoerd door inschakeling van een vertrouwenspersoon en dat de minister slechts een kleine rol heeft bij het doorgeven van een onderzoeksvraag aan deze vertrouwenspersoon, doet daaraan niet af.

https://bit.ly/3twIiGc

Ziekenhuis hoeft identiteit zaaddonor niet prijs te geven

(Rechtbank Gelderland 24 maart 2021)

Eiseressen, een moeder en een dochter, eisen van een ziekenhuis dat het de identiteit van de biologische vader van de dochter bekendmaakt. De vader is zaaddonor. Hij had aanvankelijk gezegd dat zijn donorkinderen zijn identiteit mochten weten als zij dat wilden, maar bedacht zich later. De rechtbank oordeelt dat de biologische vader dit terecht heeft mogen doen. Ondanks dat in 2004 de Wet donorgegevens kunstmatige bevruchting (WDKB) is

ingesteld die anoniem doneren heeft verboden, mag de man zich bedenken omdat hij vóór de invoering van deze wet heeft gedoneerd. Daarnaast zijn er veel kinderen met het zaad van de man verwekt. Een plotselinge bekendmaking van zijn identiteit kan grote gevolgen voor hem hebben, die niet goed gewogen kunnen worden door de rechtbank omdat de man geen partij is bij deze procedure.

https://bit.ly/3tFaald

Gerecht EU: uiterlijk Lego-blokjes is wel beschermd

(Gerecht EU 24 maart 2021)

In 2010 liet Lego een legoblokje als Gemeenschapsmodel registreren bij het Bureau voor de Intellectuele Eigendom van de Europese Unie (EURIPO). In 2016 diende Delta Sport Handelskontor – een Duitse speelgoedmaker die óók langwerpige, rechthoekige blokjes produceert welke door de rondjes en puntjes in elkaar kunnen worden geklikt – een verzoek in tot nietigverklaring van dit Gemeenschapsmodel. Hiertoe voerde Delta Sport aan dat de kenmerken van het product louter worden bepaald door haar technische functie. In 2019 verklaarde het Third Board of Appeal van het EUIPO het Gemeenschapsmodel nietig. Lego is tegen deze beslissing in beroep gegaan bij het Gerecht. Het Gerecht oordeelt, anders dan het EUIPO, dat niet álle kenmerken van het legosteentje technisch zijn bepaald en vernietigt daarom de EUIPO-beslissing. Het legosteentje wordt aldus beschermd door het modellenrecht.

https://bit.ly/3bPZTCS

Verweerder moet een kopie van een identiteitsbewijs betrekken bij de identificatie van eiser

(Rechtbank Den Haag 22 maart 2021)

Eiser heeft op grond van artikel 17 lid AVG de gemeente verzocht om zijn persoonsgegevens te verwijderen. Bij het verzoek heeft de gemachtigde van eiser een kopie van het identiteitsbewijs van eiser en een volmacht overgelegd. De gemeente heeft het verzoek van eiser niet-ontvankelijk verklaard omdat zij eiser naar eigen zeggen niet heeft kunnen identificeren. In het bestreden besluit heeft de gemeente zich op het standpunt gesteld dat een persoon zich moet identificeren aan het gemeenteloket of via DigiD om een verzoek in de zin van de AVG in te dienen. In de uitspraken van de Afdeling bestuursrechtspraak van de Raad van State van 9 december 2020 (ECLI:NL:RVS:2020:2833 en ECLI:NL:RVS:2020:2915) is echter bepaald dat een kopie van een identiteitsbewijs op zichzelf voldoende kan zijn om de identiteit te controleren. In het bestreden besluit heeft de gemeente niet gemotiveerd waarom het overleggen van een kopie van het identiteitsbewijs van eiser in dit geval onvoldoende was om zich te identificeren. De rechtbank ziet desondanks aanleiding om dit motiveringsgebrek te passeren met toepassing van artikel 6:22 van de Algemene wet bestuursrecht. Tijdens de zitting heeft de gemeente toegelicht dat de handtekeningen op de kopie en de volmacht van elkaar afwijken. Door deze redelijke twijfel over de identiteit van eiser is een kopie van het identiteitsbewijs inderdaad onvoldoende. De rechtbank oordeelt dat de verweerder het bezwaar van eiser ongegrond heeft mogen verklaren.

https://bit.ly/3twM02A

Boete voor ziekenhuis wegens overtreding AVG door rechter verlaagd

(Rechtbank Den Haag 31 maart 2021)

In 2019 legde de Autoriteit Persoonsgegevens (AP) een hoge boete op aan het HagaZiekenhuis. Het ziekenhuis kreeg de boete wegens overtreding van de AVG. Persoonsgegevens van patiënten – één patiënte in het bijzonder, bekend van de reality tv-serie Oh Oh Cherso – werden onvoldoende beschermd. De boete bedroeg €460.000, maar de rechtbank Den Haag heeft deze teruggebracht naar €350.000. De rechtbank is van mening dat de verhogingen op de basisboete hebben geleid tot een disproportioneel boetebedrag. Het ziekenhuis had ten tijde van de inbreuk reeds diverse maatregelen genomen om te voorkomen dat persoonsgegevens in het digitale patiëntendossier worden ingezien door

onbevoegde medewerkers. Ook had het ziekenhuis tijdens de bezwaarfase bij de AP tweefactorauthenticatie voor toegang tot patiëntendossiers ingevoerd en de logging van inzage in patiëntendossiers geïntensiveerd. Volgens de rechtbank tonen de door het ziekenhuis getroffen maatregelen de bereidwilligheid om met de problematiek in de organisatie aan de slag te gaan en nuanceren die de nalatigheid die het ziekenhuis wordt verweten. De beperkte financiële draagkracht van het ziekenhuis vindt de rechtbank overigens geen grond voor een verdere matiging van de boete.

https://bit.ly/3tCvJck

Foto's van minderjarigen op sociale media en toestemming onder de AVG

(Rechtbank Overijssel 7 april 2021)

In deze uitspraak bevestigt de Rechtbank Overijssel dat derden niet zomaar foto's van minderjarigen op sociale media kunnen plaatsen zonder de toestemming van één of beide wettelijk vertegenwoordigers. De zaak draaide om een ex-stiefmoeder (gedaagde) van een minderjarige jongen die foto's van de jongen, maar ook van hem en zijn halfzusje, op Facebook had geplaatst. De moeder van de minderjarige jongen (eiseres) was het hier niet mee eens en verzocht de ex-stiefmoeder om de foto's van het platform te verwijderen. De vader van de jongen (de heer X) – die volgens gedaagde zelf eerder had meegewerkt aan de gezamenlijke Facebookpagina met haar – had zich later achter het verzoek van de moeder geschaard. De ex-stiefmoeder weigerde echter de foto's weg te halen. De rechter toetst aan de AVG en UAVG. De zogenaamde 'huishoudexceptie' – een uitzondering op de privacyregels bij zuiver persoonlijke of huishoudelijke activiteiten – acht de rechter niet van toepassing, omdat het een openbare Facebookpagina betreft. In de UAVG is een bepaling opgenomen die stelt dat voor de verwerking van persoonsgegevens van een kind jonger dan 16 jaar de toestemming van zijn wettelijk vertegenwoordiger is vereist. Nu is gebleken dat zowel moeder als vader geen toestemming (meer) hebben gegeven voor het plaatsen van de foto's, oordeelt de rechter dat de ex-stiefmoeder het beeldmateriaal dient te verwijderen. Het gestelde belang van de ex-stiefmoeder dat zij aan de jongen is gehecht omdat hij een halfzusje heeft, maakt het oordeel van de rechter niet anders.

https://bit.ly/3y3mFkb

Geen daadwerkelijk misbruik = geen aansprakelijkheid voor gehackte gegevens

(Rechtbank Gelderland 7 april 2021)

Eiser heeft zich als woningzoekende ingeschreven bij NederWoon. Daarbij heeft eiser persoonsgegevens verstrekt, zoals een kopie van zijn paspoort, loonstroken en bankafschriften. Op een gegeven moment werd het computersysteem van NederWoon gehackt. De hacker heeft allerlei gegevens van accounthouders kunnen inzien, maar het is niet bekend welke gegevens precies zijn gelekt. PrivacyPunt heeft namens eiser NederWoon aansprakelijk gesteld voor de schade die is veroorzaakt doordat NederWoon vermoedelijk in strijd heeft gehandeld met de AVG. De rechtbank wijst de vordering af omdat er niet is gebleken dat er daadwerkelijk misbruik is gemaakt van de gegevens die bij de hack zijn betrokken. De hacker had de persoonsgegevens immers nog niet aan derden verkocht of overgedragen.

https://bit.ly/3txNTw1

Domeinnaamhouder niet aansprakelijk voor beelden huwelijk minister Grapperhaus

(Rechtbank Amsterdam 9 april 2021)

Eiser is fotograaf. Op 22 augustus 2020 heeft hij foto- en filmopnames gemaakt van het huwelijk van Ferdinand Grapperhaus. Op 2 september 2020 is op de website commonsensetv.nl een post geplaatst met de titel "Nieuwe foto's handenschuddende en knuffelende Grapperhaus" waarin o.a. beelden, gemaakt door eiser, zijn opgenomen. Op de beelden is het logo van CommonSenseTV te zien. De domeinnaam commonsensetv.nl is door Hostnet als registrar bij SIDN geregistreerd. Eiser is van mening dat Hostnet hierdoor inbreuk maakt op de auteursrechten die hij

over zijn beelden beschikt. De rechtbank oordeelt dat wanneer iemand een inbreukmakend foto of filmpje op een website post, de domeinnaamhouder daarmee niet automatisch óók inbreuk maakt op dat auteursrecht.

https://bit.ly/3bdSddt

E-mail staat schriftelijkheidsvereiste niet in de weg

(Rechtbank Rotterdam 14 april 2021)

Aemstel heeft aan Mejoro een appartementsrecht verkocht. In de overeenkomst is een bepaling opgenomen met de voorwaarde dat een schriftelijke verklaring nodig is om de overeenkomst te ontbinden. Aemstel heeft per e-mail laten weten dat zij de koopovereenkomst wil ontbinden. Mejoro meende dat Aemstel hiermee niet aan het schriftelijkheidsvereiste had voldaan. De rechtbank stelt dat het van belang is dat vastgesteld moet kunnen worden of de mededeling de geadresseerde heeft bereikt. Of dit digitaal of fysiek is daarbij niet van belang.

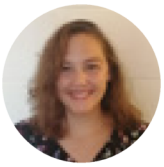
https://bit.ly/2RHu20b

Bol.com trapte in phishingmail en maakte €750.000 over naar oplichters

(Rechtbank Midden-Nederland 14 april 2021)

In 2019 heeft Bol.com €750.000 gestort op een Spaanse bankrekening van oplichters. De webwinkel dacht het geld over te maken naar het Nederlandse Brabantia, nadat Bol.com een mail in gebrekkig Nederlands en met een snufje Engels had ontvangen waarin werd medegedeeld dat Brabantia haar rekeningnummer had gewijzigd. Het echte Brabantia wilde alsnog geld zien en stapte daarom naar de rechter. Bol.com vond dat haar werknemers toentertijd voldoende reden hadden om aan te nemen dat de Brabantia's rekeningnummer inderdaad was gewijzigd. Volgens Bol.com leken het e-mailadres, de lay-out van de brief en de handtekeningen van de directie authentiek. De rechtbank oordeelt anders. Het verzoek om het rekeningnummer te wijzigen had bij Bol.com tot 'gezonde' argwaan moeten leiden. Bovendien had er een belletje moeten gaan rinkelen als een Brabantse producent opeens zijn rekeningnummer wijzigt naar een Spaanse rekening. Ten slotte hadden ook de spelfouten tot argwaan moeten leiden.

https://bit.ly/3uQy19r



Sanne Haumersen
Legal assistant

Cloud

Aanpak van nepnieuws: aansprakelijkheid of zelfcensuur?

Op vrijdag 8 januari 2021 bracht Twitter het nieuws naar buiten dat het Twitter-account van Donald Trump voorgoed verwijderd zou blijven van het medium. Twitter geeft in een verklaring aan dat zij het account hebben geblokkeerd omdat dat de tweets van de oud-president aanzetten tot geweld.[1] Deze permanente blokkade is het gevolg van het feit dat Trump verschillende Tweets de wereld in stuurde die onjuistheden bevatten. Twitter heeft hier gedurende de presidents-verkiezingen al op ingegrepen door waarschuwingen bij de Tweets te zetten dat de inhoud mogelijk misleidend zou zijn. Sociale mediaplatformen zoals Twitter hebben, zoals ook hieruit blijkt, een grote impact op ons dagelijkse leven. Hun rol in de aanpak van dergelijke desinformatie is daarom erg interessant. Toch moeten zij ervoor waken om zelf niet aansprakelijk te worden gesteld voor de onrechtmatige inhoud op hun platform.

1. 'Permanent suspension of @realDonaldTrump', 8 januari 2021, www.blog.twitter.com (laatst geraadpleegd: 4 mei 2021).

Inleiding

De aanpak van Twitter om Trump te blokkeren en zijn Tweets als misleidend te labelen, zou op het eerste oog toegejuicht moeten worden. De actieve houding ten aanzien van nepnieuws en andere onrechtmatige inhoud is de meest effectieve manier om ervoor te zorgen dat de digitale media een positieve bijdrage leveren aan de nieuwsvorming van burgers, in plaats van dat burgers mogelijk worden beïnvloed door misleidende informatie. Het publiek is immers steeds meer afhankelijk van nieuwsvoorziening via sociale media. Bovendien is er bij sociale mediaplatformen vaak geen redactionele controle. Het gebrek aan controle kan leiden tot de verspreiding van nepnieuws, ook wel bekend als desinformatie. Dit is informatie die wordt verspreid met het

oogmerk het publiek te misleiden, om de publieke opinie te beïnvloeden of om winst te maken.[2]

2. M. de Cock Buning, 'Nepnieuws, bubbels en clickbait: over consumentenvertrouwen en advertentiebeleid', IER 2018/32, afl. 4, p. 31-38.

Het is de vraag of en hoe we ons kunnen wapenen tegen de verspreiding van desinformatie. De invloedrijke rol van platformen kan bij deze strijd tegen desinformatie juist goed van pas komen. Voor platformen is de manier waarop zij desinformatie aanpakken echter een groot dilemma. Twitter en andere sociale mediaplatformen zijn namelijk in juridische zin een dienst van de informatiemaatschappij. Deze diensten kunnen mogelijk een beroep doen op de vrijwaring van aansprakelijkheid op het moment dat onrechtmatige informatie op hun platform wordt geplaatst, dit is de vrijwaringsregeling van artikel 6:196c lid 4 BW. Dit is een 'safe harbor'-bepaling uit de e-Commercerichtlijn. Desondanks zijn zij onder bepaalde voorwaarden toch aansprakelijk, wat voor de platformen niet wenselijk is. Deze aansprakelijkheid weerhoudt platformen er mogelijk van om zich actief te bemoeien met de informatie op het platform. Een andere kant van het probleem is dat indien sociale mediaplatformen rechtmatige inhoud onnodig verwijderen, dit een vorm van censuur is. Het platform mag immers niet bepalen welke rechtmatige inhoud geplaatst wordt en welke blijft.

Aansprakelijkheid van platformen

De rol van sociale mediaplatformen wordt steeds groter in de digitale maatschappij. Deze ontwikkeling gaat gepaard met de verantwoordelijkheid van dergelijke platformen om onrechtmatige informatie te verwijderen van het platform. Voor dergelijke platformen is het onder voorwaarden mogelijk om te worden gevrijwaard van aansprakelijkheid. Dit is de vrijwaringsregeling van artikel 6:196c BW. Deze bepalingen zijn van toepassing op 'diensten van de informatiemaatschappij'. Volgens de Memorie van Toelichting zijn dit alle diensten die normaal tegen vergoeding, op afstand, via elektronische apparatuur voor de verwerking en de opslag van gegevens, op individueel verzoek van een afnemer van de dienst worden verricht.[3]

3. *Kamerstukken II* 2001/02, 28197, nr. 3, p. 12.

Sociale mediaplatformen zoals Twitter en Facebook zijn hostingdiensten in de zin van lid 4 van artikel 6:196c BW. Dit zijn user-generated contentdiensten, waarbij gebruikers van de dienst zelf de content zoals foto's, video's of tekst leveren. De platformen fungeren hierbij als tussenpersoon en verzorgen de opslag van de gegevens. De vrijwaringsbepaling bevat twee maatstaven. Ten eerste is de hostingprovider volgens artikel 6:196c lid 4 sub a BW niet aansprakelijk als hij van de informatie met het onrechtmatige karakter geen kennis heeft. Echter, de vrijwaringsbepaling is al niet meer van toepassing op het moment dat de hostingprovider al een vermoeden heeft van onrechtmatige content. De tweede maatstaf volgt uit sub b. De hostingdienstverlener kan alsnog een beroep op de vrijwaring doen als onrechtmatige informatie prompt verwijdert op het moment dat hij op de hoogte raakt van de onrechtmatige content. Hostingproviders gebruiken hiervoor vaak een Notice-and-takedown procedure (NTD-procedure) om aan deze verwijderingsplicht te voldoen.

De regeling van artikel 6:196c lid 4 BW heeft echter iets tegenstrijdigs in zich. Zo is een platform die zich bemoeit met de inhoud, dus door actief uit eigen beweging onrechtmatige inhoud te verwijderen, geen neutrale tussenpersoon en dus geen host in de zin van dit artikel. Dat houdt in dat dit platform zich niet kan beroepen op de vrijwaring. Toch is het, zoals uit de volgende paragraaf zal blijken, wel belangrijk dat sociale media een sturende rol hebben in het nieuwsaanbod op hun platform.

Het gevaar van nepnieuws voor platformen

Door de digitalisering van de maatschappij is het informatieaanbod op digitale media enorm toegenomen. Dit is enerzijds een goede ontwikkeling. Burgers kunnen door pluriformiteit van de media beter een eigen mening vormen. Bovendien krijgt een medium niet een monopolypositie, waardoor het nieuwsaanbod divers blijft. Aan de andere kant heeft de digitalisering van het nieuwsaanbod tot gevolg dat nieuwsberichten veel sneller verspreid kunnen worden. Dit geeft ook de verspreiding van desinformatie vrij spel. Door de verspreiding van desinformatie via sociale mediakanalen wordt het voor burgers lastig(er) om het echte nieuws te onderscheiden van desinformatie. Het gevolg is dat het publiek wordt belemmerd in het vormen van een goed geïnformeerde mening.

Een recent bekend voorbeeld uit de Nederlandse rechtspraak is de zaak van John de Mol tegen

Facebook uit 2019 bij de rechtbank van Amsterdam.[4] John de Mol heeft Facebook gedagvaard omdat sinds oktober 2018 tot maart 2019 advertenties op Facebook verschenen waarin bekende Nederlanders, waaronder John de Mol, in verband werden gebracht met Bitcoin. In deze zaak had John de Mol daarvoor geen toestemming gegeven. De mensen die op de advertenties in zijn gegaan en bedragen betaalden, kregen geen Bitcoins. De rechter zegt hierover dat Facebook onrechtmatig heeft gehandeld omdat zij de mogelijkheid bieden om dergelijke advertenties te tonen. Facebook kan dus geen beroep doen op de vrijwaringsbepaling. Het primaire verdienmodel van Facebook is namelijk het faciliteren van advertenties en het genereren van inkomsten daaruit. Facebook heeft bovendien een uitgebreid advertentiebeleid waardoor de advertenties voor plaatsing uitvoerig worden gecontroleerd. De rechtbank oordeelt dat Facebook geen neutrale tussenpersoon meer is en het dus geen beroep kan doen op de vrijwaringsbepaling.

4. Rb. Amsterdam 11 november 2019, ECLI:NL:RBAMS:2019:8415.

De zojuist besproken advertenties zijn een vorm van desinformatie omdat de advertenties erop gericht zijn om het publiek te misleiden en daarmee winst te maken. Toch kan Facebook in het geval van de onderhavige zaak geen beroep doen op de vrijwaringsregeling zoals hierboven besproken. Dit leidt ertoe dat Facebook mogelijk te streng gaat controleren op desinformatie in advertenties en rechtmatige advertenties voor de zekerheid bij twijfel ook verwijdert. Het aanpakken van de verspreiding van desinformatie middels platformen lijkt daarom de meest logische en eenvoudige optie. Toch gaat dit gepaard met mogelijk grote bezwaren. Door mensen te verbieden op een bepaalde manier informatie te delen kan dit een inbreuk op de vrijheid van meningsuiting opleveren. Als de overheid door middel van wetgeving platformen verplicht informatie van hun platform te verwijderen, kan dit leiden tot censuur. Platformen zullen in dat geval namelijk 'op safe spelen' en mogelijk ook rechtmatige inhoud verwijderen van hun platform.

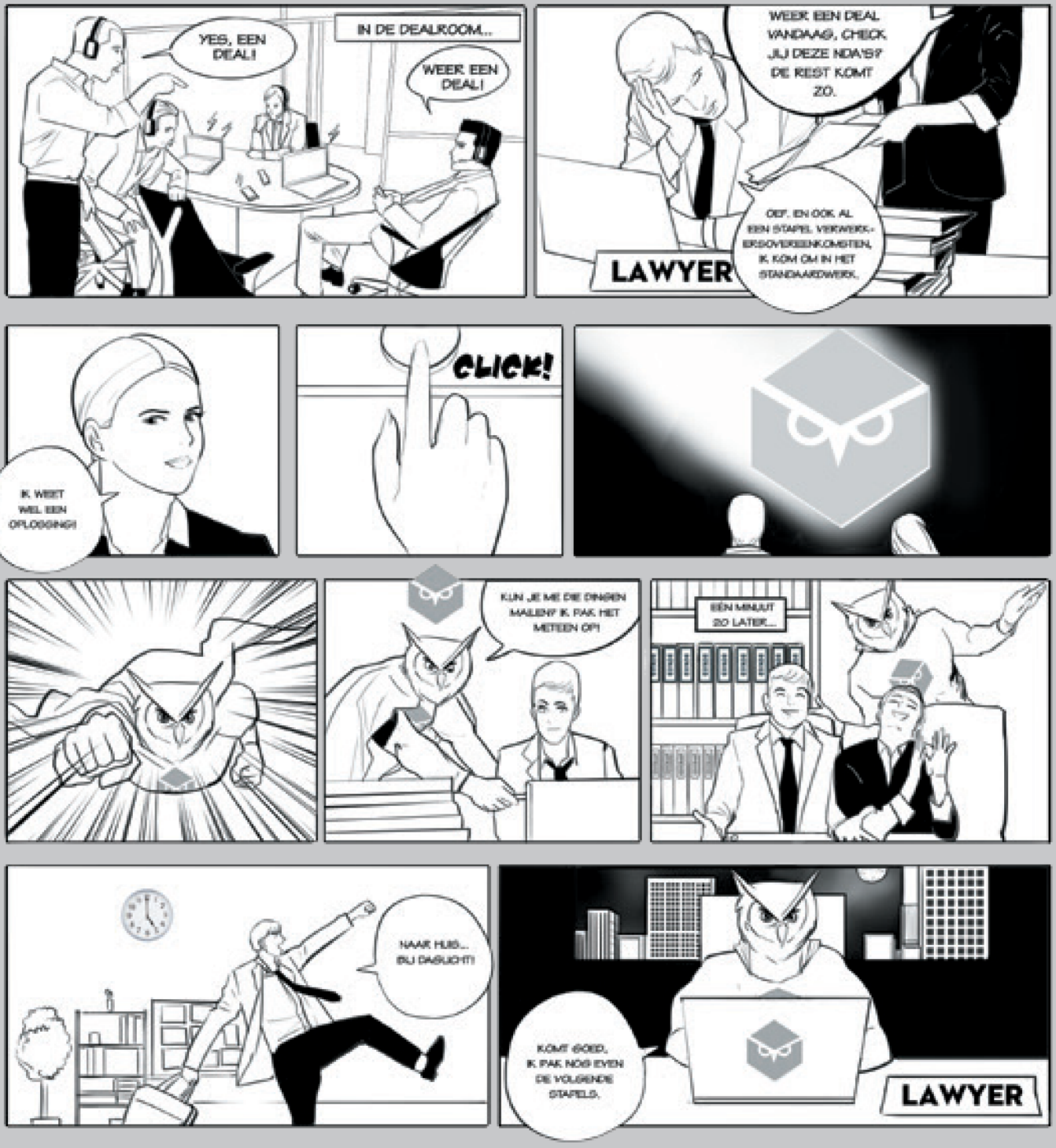
Conclusie

Recente voorbeelden van Facebook en Twitter illustreren de impact van desinformatie op de maatschappij perfect. Sociale mediaplatformen maken het voor burgers mogelijk om op ieder moment het nieuwsaanbod te bekijken. De verspreiding van het nieuws gaat hierdoor razendsnel. Dit heeft ook tot gevolg dat de verspreiding van nepnieuws, of desinformatie, niet te stoppen is. Het gevaar van desinformatie is dat het publiek wordt beïnvloed door onjuistheden en burgers niet meer een mening gebaseerd op juiste feiten kunnen vormen.

Platformen kunnen zelf ook een rol spelen in de bestrijding van dergelijke desinformatie. De vrijwaringsbepaling van artikel 6:196c lid 4 BW motiveert platformen om onrechtmatige inhoud te verwijderen. Platformen moeten echter wel waken voor censuur, omdat ze mogelijk te veel (rechtmatige) informatie verwijderen om aansprakelijkheid te voorkomen. De NTD-procedure lijkt de meest effectieve oplossing tegen de verspreiding van desinformatie. Dit voorkomt dat een platform actief informatie moet verwijderen en dus mogelijk censureert.

Een kanttekening hierbij is dat de gebruikers van het platform de onrechtmatige informatie moeten melden bij de hostingprovider. Echter, dergelijke advertenties zoals in de zaak van John de Mol worden door gebruikers waarschijnlijk niet gezien als desinformatie. Omdat de advertenties zo echt lijken, wordt het publiek dusdanig beïnvloed dat zij denken dat de advertentie echt is, en maken gebruikers geen melding van de onrechtmatig inhoud. Op dit moment is er geen kant en klare oplossing voor het verwijderen van desinformatie op internet, terwijl dit probleem er wel om vraagt.

- DE AVONTUREN - VAN LAWYERBOT LYNN



Een lawyerbot is allang geen stripverhaal meer. Contracten reviewen is standaardwerk, en dat is precies waar computers goed in zijn.
De lawyerbots van Lynn Legal nemen u graag werk uit handen: een geheimhoudingscontract of verwerkersovereenkomst is binnen een minuut gecontroleerd op standaardpunten, waarna u de belangrijke zaken kunt overnemen.

lynn legal

Meer weten?
Bezoek onze website: **lynnlegal.nl**
Of neem contact met ons op
via telefoonnummer: 020 229 3345

Arnoud Engelfriet
Directeur / Opleidingsdirecteur

Cloud Innovatie

Noot bij Google LLC v. Oracle America, inc.[1]

De zaak Google/Oracle draait om de universele programmeertaal Java, die begin jaren negentig is ontwikkeld door Sun Microsystems. Door ontwikkelaars een gestandaardiseerd platform te bieden zouden zij eenvoudig applicaties kunnen maken die op iedere computer kunnen werken. Een belangrijk onderdeel van Java is haar *application programming interface* (API)[2]: een voor software gemaakte wijze van toegang tot een applicatie.

1. US Supreme Court, 7 oktober 2020, zaaknr. 18–956.

2. Jacobson, D.; Brail, G.; and Woods, D. APIs: A Strategy Guide. Sebastopol, CA, USA: O'Reilly, 2011. In het Nederlands taalgebied wordt ook wel de term koppeling of koppelvlak gebruikt, maar de Engelse term API is meer ingeburgerd.

In 2007 kwam het voor mobiele apparaten ontwikkelde besturingssysteem Android op de markt. Om ontwikkelaars over de streep te trekken Android-applicaties te maken, had Google daarin verschillende API's opgenomen. Deze API's bevatten elementen die ook aanwezig waren in de API's van Java en droegen bovendien dezelfde namen. De software zelf was echter niet uit Java gekopieerd, maar geheel zelfstandig door Google gemaakt.

In 2010 startte softwaregigant Oracle – de rechtsverkrijger van Sun wat betreft Java – een rechtszaak tegen Google. Overname van die API's – of beter gezegd: de namen van de functionaliteiten daarvan – vormde volgens Oracle auteursrechtinbreuk. Oracle vorderde daarin maar liefst acht miljard dollar aan schadevergoeding vanwege gederfde licentiekosten. De claims van Oracle maakten veel los, omdat een uitspraak conform haar eis zou betekenen dat het interface-conform ontwikkelen van een implementatiekloon juridisch onmogelijk zou zijn. Het langlopende traject, inclusief tweemaal hoger beroep en ook twee trips naar de Supreme Court, maakte dat de zaak langdurig in de belangstelling stond (en staat).

In eerste instantie werden de vorderingen van Oracle afgewezen. De rechtbank oordeelde dat het overnemen van functie-aanroepen geen inbreuk op het auteursrecht oplevert zolang men een eigen implementatie daarvan toevoegt. In hoger beroep oordeelde het Hof van Beroep echter dat de API van Java moest worden gezien als een door Sun zelf bedachte taxonomie die naar Amerikaans recht auteursrechtelijk te beschermen valt. Een API was daarmee dus auteursrechtelijk beschermd. Google trachtte vervolgens om de zaak in behandeling te laten nemen door het Supreme Court, maar dit verzoek werd afgewezen.

In de vervolgprocedure stond de vraag centraal of het gebruik van een API uitgezonderd was van auteursrecht omdat dit als *fair use* zou kunnen worden aangemerkt. De rechtbank in eerste aanleg oordeelde dat zulks het geval was. In hoger beroep werd dit echter ongedaan gemaakt. Het Hof van Beroep oordeelde dat niet was aangetoond dat aan de vier *fair use*-criteria was voldaan. Daarop stapte Google (wederom) naar de Supreme Court. De belangstelling voor de zaak was ondertussen zo gegroeid dat tientallen *amici curiae* hun kijk op de zaak aandroegen.

De reden voor deze belangsteling voor een op zich achterhaalde kwestie – de API's zitten al lang niet meer in Android en Java heeft fors aan relevantie ingeboet – is fundamenteel: zou het oordeel van het Hof van Beroep in stand blijven, dan zou het inmiddels wijdverbreide gebruik van API's van andermans software toestemming vereisen van de auteursrechthebbende.

Totdat de Google/Oracle zaak de IE-insteek weer op de kaart zette, werd toegang tot API's voornamelijk gezien als een kwestie van het mededingingsrecht. Kern van de discussie is daarbij of de ontwerper van een API concurrenten kan dwingen de markt met een geheel andere API te bedienen. In de praktijk lijkt dit meestal tot weinig problemen te leiden, juist omdat door marktwerking een concurrent dan een effectievere implementatie aanbiedt met dezelfde API aanroepen. Het auteursrecht zou dat laatste verhinderen, en dat is waar de schoen wringt bij deze zaak.

In de Europese Unie lijkt het een uitgemaakte zaak dat er geen auteursrecht op API functie-aanroepen kan bestaan. Artikel 1 lid 2 van de Softwarerichtlijn bepaalt dat "ideeën en beginselen die aan enig element van een computerprogramma ten grondslag liggen, met inbegrip van de ideeën en beginselen die aan de interfaces daarvan ten grondslag liggen, niet krachtens deze richtlijn auteursrechtelijk [worden] beschermd." En in het SAS/WPL-arrest oordeelde het Hof van Justitie dat "noch de programmeertaal en de indeling van gegevensbestanden die in het kader van een computerprogramma worden gebruikt om bepaalde van de functies van dat programma te kunnen benutten" onder het auteursrecht op dat programma kunnen vallen. Het gebruiken van functies van een programma kan maar op een manier, en dat is met functie-aanroepen - precies zoals dat met een API gebeurt. Daarmee lijkt het onvoorstelbaar dat een functie-aanroep in een API in Europa onder het auteursrecht van de bedenker daarvan zou vallen.

In de VS oordeelt nu de Supreme Court dat Google inderdaad een beroep op *fair use* mocht doen. Google had alleen die regels broncode gekopieerd – die API definities overgeschreven – die ze echt nodig had om haar eigen herimplementatie van de Java API te maken. Het probleem is alleen: geldt dit voor íedere herimplementatie van andermans API? Hoe ver gaat dat "what was needed", hoe anders moet jouw eigen programmeeromgeving zijn en moet het gaan om een "bekende" (familiar) programmeertaal? Als ik de API van zeg de elearning-provider op de hoek kopieer, val ik dan hieronder? En dat is dan alleen nog maar wat ik in vijf seconden kan bedenken na het lezen van deze zin; kun je nagaan wat een advocaat van Oracle daarvan maakt als hij zes maanden fulltime 800 dollar per uur daarvoor mag rekenen.

Het Hof danst om de vraag heen of haar vorige uitspraak over auteursrecht op API definities terecht was. Dat is ook lastig want zelfs de Supreme Court kan niet zomaar haar eigen precedenten opzij zetten.

Men houdt het dan ook bij: *"We shall assume, but purely for argument's sake, that the entire Sun Java API falls within the definition of that which can be copyrighted. … As part of an interface, the copied lines are inherently bound together with uncopyrightable ideas (the overall organization of the API) and the creation of new creative expression (the code independently written by Google)."*

Dit laat dus het principe overeind dat er best auteursrecht op een API als zodanig kan zitten. Weliswaar

niet heel veel, maar kennelijk net genoeg. En hoe je het idéé van een API hergebruikt zonder de letterlijke functienamen en dergelijke te gebruiken, daar laat men zich wijselijk niet over uit.

We kunnen dus nu wel roepen dat Google gewonnen heeft, maar de conclusie die op lange termijn blijft staan is dat vrijwel iedere API auteursrechtelijk beschermd is, met als gevolg dat interoperabiliteit vrijwel onmogelijk wordt. Immers, wil je die herimplementeren dan heb je toestemming nodig tenzij je in een beperkte uitzondering valt.

Dit versterkt de macht van rechthebbenden enorm. En ja, ik maak me daar ook bij Europese bedrijven zorgen over. De meeste innovatieve softwaredienstverleners opereren immers vanuit de VS. De ervaring leert dat hun gedrag (en contractuele voorwaarden) sterk Amerikaans georiënteerd zal zijn, waarbij men niet snel Europeesrechtelijk water bij de wijn zal doen. Daar komt bij dat een concurrent binnen dit juridisch kader geen API-compatibele eigen dienst kan aanbieden, omdat dit op auteursrechtelijke bezwaren zal stuiten in de VS – en de dienst aldaar niet aanbieden is commercieel dan geen optie.

Daar staat natuurlijk tegenover dat zeker de web API's vaak al onder bepaalde voorwaarden worden aangeboden, zodat de praktijk niet direct zal wijzigen. Maar API-aanbieders hebben nu wel een stuk steviger fundament voor hun voorwaarden, namelijk dat wie deze schendt, tevens het auteursrecht te buiten gaat. Een app die jouw voorwaarden schendt, kun je afsluiten van de API en dat is het. Een app die jouw auteursrecht schendt, kun je van de markt halen onder opvordering winst en een verbod voor de toekomst. Dus nee, ik vind deze 'overwinning' best zorgelijk.


EAD>
TLE><?PHP ECHO $PAGE_TITLE; ?></TITLE>
ETA NAME="KEYWORDS" CONTENT="<?PHP ECHO SPAG
ETA NAME="DESCRIPTION" CONTENT="<?PHP ECHO SPA
ETA NAME="CONTENT-LANGUAGE" CONTENT="ENGLISH
ETA NAME="REVISIT-AFTER" CONTENT="56 DAYS">
ETA NAME="DISTRIBUTION" CONTENT="GLOBAL">
ETA NAME="ROBOTS" CONTENT="ALL">
"STYLESHEET" TYPE="TEXT/CSS" HREF="TDS.CS
TEXT/CSS">
CENTER;

Innovatie Security

Deepfakes: of u even een paar gekke bekken wilt trekken?

Van onze blog
29 april 2021

De laatste jaren hebben “deepfake” video’s de nodige aandacht gehad en zijn er een aantal (griezelig) goed gelukte video’s voorbijgekomen. Zo zagen wij een video[1] waarin Boris Johnson en Jeremy Corbyn elkaar steunen en gaf de Engelse Queen een wel heel bijzondere kersttoespraak[2]. Recentelijk nog dachten Nederlandse Tweede Kamerleden via Zoom gesproken te hebben met een medewerker van de Russische oppositieleider Navalny. Zij kwamen echter bedrogen uit, want de man die ze daadwerkelijk spraken bleek een deepfake-imitatie te zijn.

1. https://bbc.in/3onDxxO
2. https://bit.ly/3eKRz9B

Deepfake-technologie

Door middel van deepfake-technologie kan een gezicht of een stem vervangen worden door het gezicht of een stem van iemand anders. Hierdoor kun je iemand van alles laten zeggen, terwijl in werkelijkheid dit helemaal niet door deze persoon is gezegd. Dit brengt tal van risico’s met zich mee, zo kunnen deepfakes bijvoorbeeld gebruikt worden om desinformatie te verspreiden om politieke processen te beïnvloeden. Deepfakes kunnen in de praktijk ook gebruikt worden om bedrijfsprocessen te manipuleren om fraude of oplichting te plegen. Zo is er al een bedrijf slachtoffer geworden van CEO-fraude doordat de CEO een telefoontje ontving van de CEO van de moedermaatschappij met het verzoek om een overboeking van € 220.000 te doen. De stem van de CEO die om de overboeking verzocht bleek uiteindelijk nagebootst door middel van deepfake-technologie. Een volgend geval, waarbij iemand via een videocall probeert de boel te manipuleren door middel van deepfake zal vermoedelijk niet lang op zich laten wachten.

Waar moet u op letten?

De ontwikkelingen op het gebied van deepfakes gaan razendsnel en de techniek om goed lijkende video’s te maken wordt steeds verfijnder. Op dit moment lijkt het erop dat detectiesoftware die gebaseerd is op artificial intelligence een goede mogelijkheid zal bieden om er snel achter te komen of een video echt of nep is. Tot de tijd dat dit gemeengoed is geworden zijn er een aantal punten welke gebruikt kunnen worden om na te gaan of er sprake is van een deepfake video of niet:

- Let goed op de ogen van de persoon, wordt er raar met de ogen geknipperd of knippert de persoon helemaal niet?
- Kijk goed naar het schaduwpatroon van het gezicht, komt dit waarheidsgetrouw over of is er sprake van rare vlekken of schaduwen in het gezicht?
- Let goed op de vervaging van de beeldkwaliteit indien er armgebaren worden gemaakt.

Is er sprake van een live gesprek en vertrouwt men het echt niet? In dat geval is het raadzaam om te vragen of de persoon in kwestie helemaal met het hoofd wil ronddraaien, gekke bekken wil trekken of even het gezicht wil aanraken.

Auteur
Alexander Freund
Information security consultant

Privacy

De ePrivacy Verordening: tijd voor de eindsprint

Van onze blog
21 april 2021

Wij schreven eerder[1] al over het langslepende dossier dat de ePrivacy Verordening heet. Na bijna vier jaar lijkt er eindelijk weer beweging in het vastgeroeste wetgevingsproces te komen. Op 10 februari 2021 publiceerde de Raad van de Europese Unie (de Raad) namelijk een nieuw wetsvoorstel[2], waarmee het startsein werd gegeven voor de onderhandelingen tussen de Raad, het Europees Parlement en de Europese Commissie. Hoog tijd voor een update dus.

1. https://bit.ly/3uMACky
2. https://bit.ly/3hvOGv7

Hoe zat het ook alweer?

Laten we even teruggaan naar het begin. De ePrivacy Verordening wordt in het leven geroepen om de verouderde ePrivacyrichtlijn, welke in Nederland is geïmplementeerd in de Telecommunicatiewet, te vervangen. Als broertje van de Algemene verordening gegevensbescherming (AVG) zal de ePrivacy Verordening zich richten op de bescherming van de persoonlijke levenssfeer op het gebied van elektronische (online) communicatie. Het eerste wetsontwerp[3] van de Europese Commissie voor de Verordening dateert van 10 januari 2017. Vrij snel daarna nam het Europees Parlement een resolutie[4] aan waarmee zij flink wat wijzigingen aan het voorstel aanbracht. Eenmaal bij de Raad konden de vertegenwoordigers van de lidstaten het – mede onder invloed van sterke lobbycampagnes door grote bedrijven – jarenlang niet eens worden over de in te nemen standpunten. Daarbovenop zorgden de Europese verkiezingen in 2019 en de COVID-pandemie in 2020 voor extra vertraging. Onder de nieuwe voorzitter Portugal kwam de Raad dit jaar dan eindelijk met een aangepast voorstel.

3. https://bit.ly/3fI9KBs
4. https://bit.ly/3uQmwP5

Wat verandert er?

In vergelijking met de Telecommunicatiewet komt het nieuwe (let op: niet definitieve!) wetsvoorstel met onder andere de volgende wijzigingen:

Versoepeling cookieverbod

De Telecommunicatiewet kent een cookieverbod[5] waarop beperkte wettelijke uitzonderingen van toepassing zijn. In het wetsvoorstel worden deze uitzonderingen enigszins opgerekt. Zo mogen ook derde partijen analytische cookies plaatsen en hoeft niet te worden voldaan aan het vereiste van 'privacyvriendelijkheid'. Daarnaast laat het voorstel toe dat informatie over eindapparatuur, verzameld door cookies, ook voor ándere, maar wel verenigbare doeleinden wordt verwerkt dan waarvoor deze was vergaard ("verdere verwerking"). Tot slot biedt het voorstel gebruikers de mogelijkheid om *vooraf* toestemming te geven voor het plaatsen van cookies door middel van *whitelisting*, oftewel het samenstellen van lijsten van goedgekeurde websites en websitediensten via de browserinstellingen.

5. https://bit.ly/3uOO07A

Verbod op cookiewalls?

Tegelijkertijd lijkt het Raadsvoorstel juist iets strenger dan de Telecommunicatiewet ten aanzien van 'cookiewalls': meldingen waarbij de toegang tot (een deel van) een website afhankelijk wordt gemaakt van toestemming voor het plaatsen van trackingcookies. Hoewel de Autoriteit Persoonsgegevens cookiewalls in zijn algemeenheid afwijst, is het cookiewallverbod in de Telecommunicatiewet beperkt tot publieke (overheids-)diensten. Het Europese voorstel lijkt dit verbod breder te trekken, al blinkt de tekst niet uit in helderheid. Zo wordt overwogen dat cookiewalls toelaatbaar zijn wanneer de dienstverlener een cookievrij alternatief aanbiedt dat de gebruiker toegang geeft tot een equivalente dienst. Hierbij kan worden gedacht aan het betalen van een geldbedrag voor vergelijkbare content. Verder schrijft de Raad dat cookiewalls niet geoorloofd zijn wanneer geen redelijke alternatieven voorhanden zijn, bijvoorbeeld bij dominante marktpartijen, of wanneer sprake is van een duidelijke machtsongelijkheid tussen de gebruiker en de dienstverlener, zoals in het geval van publieke diensten geleverd door overheidsinstanties.

Terugkeer bewaarplicht verkeersgegevens?

In een viertal uitspraken uit 2014-2020 heeft het Hof van Justitie van de Europese Unie geoordeeld dat een algemene en ongedifferentieerde bewaar-

plicht van metadata in strijd is met het Europese recht. Er klinkt echter kritiek, onder andere van de Duitse privacytoezichthouder, dat het Raadsvoorstel de deur naar algemene gegevensbewaring juist weer openzet. De EDPB heeft benadrukt dat het creëren van een wettelijke grondslag voor ongerichte data-retentie, zonder de juiste waarborgen, niet is toegestaan. Wat de precieze bedoeling is van de Raad en wat de eventuele gevolgen voor Nederland zijn is nog onduidelijk, maar dat dit onderwerp debat zal opleveren staat vast.

Direct marketing

Tot slot laat het voorstel ten aanzien van direct marketing relatief veel zaken aan de lidstaten over. Mogelijke wijzigingen op dit gebied zullen dus veelal afhangen van de Nederlandse wetgever. Volgens het Raadsvoorstel mogen lidstaten zelf bepalen of zij het bellen met een herkenbaar prefix (bijvoorbeeld 088-) verplicht stellen, een maximale termijn invoeren waarin klantgegevens voor direct marketing mogen worden gebruikt, en een opt-out systeem voor tele-marketing aanleggen. Voor wat betreft dit laatste heeft de Eerste Kamer recent een nieuwe wet[6] aangenomen waarbij het opt-out systeem in de vorm van het Bel-me-niet Register wordt omgezet naar een opt-in systeem waarbij personen in beginsel met telemarketing moeten instemmen.

Vooruitblik

De rest van 2021 zal in het teken staan van de onderhandelingen tussen de Europese Commissie, het Europees Parlement en de Raad om tot een definitieve tekst van de Verordening te komen. Het is geenszins zeker dat bovengenoemde bepalingen uit het Raadsvoorstel stand zullen houden; daarvoor wijkt het te sterk af van het voorstel van het Europees Parlement, dat een strengere privacykoers vaart. Ook de EDPB heeft veel op het ontwerp aan te merken. De verwachting is dat een definitieve wettekst pas in 2022 op tafel zal liggen. Laten we desondanks hopen dat de drie instanties de vaart erin zetten zodat de ePrivacy Verordening vóór 2024 – na een overgangsperiode van twee jaar – van kracht wordt.

6. https://bit.ly/3odrByy

Auteur
Laura Monhemius
Juridisch adviseur

Deze blog is geschreven in samenwerking met stagiaire Arlette Meiring

“De EDPB heeft benadrukt dat het creëren van een wettelijke grondslag voor ongerichte dataretentie, zonder de juiste waarborgen, niet is toegestaan.”

Laura Monhemius
Juridisch adviseur

ICTRecht Academy

Trainingsoverzicht juli - september 2021

Donderdag 8 juli 2021

Identiteit en veiligheid online (2 PO)

Online contracteren vindt steeds vaker plaats. Een aandachtspunt daarbij blijft het identificeren en valideren van handtekeningen. Leer in deze training onder meer te beoordelen of, en met gebruik van welke vertrouwensdienst elektronisch overeenkomsten gesloten kunnen worden.

De training vindt online plaats.
Lees meer!
https://bit.ly/2SjNiBf

Dinsdag 21 september 2021

Contracteren: belangrijke ICT-contracten nader bekeken (6 PO)

Wilt u veel voorkomende ICT-contracten in detail leren te behandelen? In deze training delen onze experts al hun praktijktrucs en wordt er ingegaan op nieuwe aspecten, zoals Agile ontwikkeling van software.

De training vindt plaats in Amsterdam indien mogelijk, anders online. Lees meer!
https://bit.ly/3nxqv0f

Donderdag 23 september 2021

Cybercrime (2 PO)

Computercriminaliteit is een belangrijk risico voor iedere activiteit op internet. Leer in deze training alles over *cybercrime* (computervredebreuk, aftappen, *denial of service*, *phishing*, virussen, gegevensdiefstal) en het fenomeen ethisch hacken te plaatsen.

De training vindt plaats in Amsterdam indien mogelijk, anders online. Lees meer!
https://bit.ly/3vumhsX

Donderdag 23 september 2021

Aanbesteden ICT-dienstverlening (4 PO)

Het aanbestedingsrecht zit vol met bijzondere valkuilen en randvoorwaarden. Bijzondere aandacht geldt daarbij voor ICT-diensten en de daarbij gebruikte inkoopvoorwaarden. Leer te signaleren dat er aanbesteed dient te worden en de valkuilen bij ARBIT, GIBIT en andere standaard overheidsvoorwaarden te benoemen.

De training vindt plaats in Amsterdam indien mogelijk, anders online. Lees meer!
https://bit.ly/2QBNUlc

Volg nu ook uw CIPP/E, CIPM en CIPT training bij ICTRecht Academy!

Op zoek naar een privacy certificering waarmee u uzelf kunt onderscheiden en kennis van zaken kunt aantonen?

Als 'Official Training Partner' van IAPP, de grootste internationale vakvereniging voor privacy professionals, bieden wij nu ook CIPP/E, CIPM en CIPT trainingen aan. Zo wordt u een nationaal en internationaal gecertificeerde privacy professional.

De eerste trainingen starten als zomercursus in augustus. Lees meer!
https://bit.ly/34gOhVq

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 20 september. Lees meer!
https://bit.ly/3u5C7tT

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

ICTRECHT
adviesbureau

Meer informatie over hoe wij werken? Bezoek ictrecht.nl