jaargang 10 • nummer 2 • april 2022

ICTRecht in de praktijk

Tips en tricks voor het uitvoeren van een DPIA

Zo leidt u een veilige organisatie effectief

De Legal Tech Map 2022 The Netherlands

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 100 specialisten voorzien we onze klanten van deskundig en praktisch advies. Van startup tot multinational en van overheidsinstantie tot zorginstelling.

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

Geen zes pagina's jargon met als conclusie "dat hangt ervan af", maar een duidelijk antwoord waarmee de organisatie direct aan de slag kan.

Hier zijn wij goed in:

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

ICTRECHT
adviesbureau

Meer informatie over hoe wij werken? Bezoek ictrecht.nl

Index

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

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

Aan deze uitgave werkten mee:

Alisa Schurink Marketing adviseur
a.schurink@ictrecht.nl
Arnoud Engelfriet Algemeen directeur/ Opleidingsdirecteur
a.engelfriet@ictrecht.nl
Bas Dekker Juridisch adviseur
b.dekker@ictrecht.nl
Beryl Hetharia Juridisch adviseur
b.hetharia@ictrecht.nl
Bram de Vos Juridisch adviseur
b.devos@ictrecht.nl
Britt Telleman Opleidingscoördinator
b.telleman@ictrecht.nl
Chantal Sitaram Juridisch adviseur
c.sitaram@ictrecht.nl
Koen van Jaarsveld Legal consultant
k.vanjaarsveld@ictrecht.nl
Laura Monhemius Juridisch adviseur
l.monhemius@ictrecht.nl
Mark Zijlstra Legal consultant
m.zijlstra@ictrecht.nl
Nick Tegelaar Information security consultant
n.tegelaar@ictrecht.nl
Nicole Waaijer Marketing adviseur
n.waaijer@ictrecht.nl
Pelçim Kaygusuz Juridisch adviseur
p.kaygusuz@ictrecht.nl
Ruben van der Geest Juridisch adviseur
r.vandergeest@ictrecht.nl
Tessa van Schijndel Juridisch adviseur
t.vanschijndel@ictrecht.nl
Tim Wokke Juridisch adviseur
t.wokke@ictrecht.nl
Eline Pellis Grafisch ontwerper
eline@elinepellis.com
Leonard Fäustle Stills & Motion
Foto's ICTRecht
info@leonardfaustle.nl

Ruben van der Geest
Juridisch adviseur

Beryl Hetharia
Juridisch adviseur

Privacy

Tips en tricks voor het uitvoeren van een DPIA

Organisaties struggelen er nog wel eens mee: het uitvoeren van een Data Protection Impact Assessment (DPIA). Wanneer is het nodig of zelfs wettelijk verplicht om een DPIA uit te voeren? Hoe ziet een DPIA eruit en wat staat er eigenlijk in? Het moet geen document worden dat in een lade belandt en waar vervolgens niets mee wordt gedaan. Dat is zonde, want uiteindelijk is het de bedoeling dat privacy risico's in kaart worden gebracht, en de eventuele risico's ook worden weggenomen. In dit artikel geven wij tips en tricks voor het uitvoeren van een DPIA.

Wat is een DPIA?

Aan de hand van een DPIA doet een organisatie voorafgaand onderzoek naar de privacy risico's die spelen bij een bepaalde gegevensverwerking. Het is belangrijk om te onderzoeken wat de gevolgen zijn voor de privacy van betrokkenen, en op welke manieren die inbreuk verkleind kan worden. Als een gemeente bijvoorbeeld camera's wil gaan ophangen in een winkelcentrum, dan wordt daarmee inbreuk gemaakt op de privacy van het winkelend publiek. Iedereen die in het winkelcentrum is, wordt immers op camera vastgelegd. Het is de vraag of dat zomaar kan. In een DPIA wordt daar onderzoek naar gedaan.

Dat het belangrijk is om een DPIA uit te voeren en ook kritisch te kijken naar de privacy inbreuk voor betrokkenen, volgt wel uit de zaak van de gemeente Enschede waar wifitracking is gebruikt in de binnenstad. Wat was er aan de hand? De gemeente Enschede liet aan de hand van verschillende sensoren de drukte meten in de binnenstad. Zo werden meetkastjes gebruikt die de wifisignalen van mobiele telefoons opvingen van passerende mensen. Denk bijvoorbeeld aan het winkelend publiek, maar ook het winkelpersoneel dat naar het werk gaat. Mobiele telefoons die binnen het bereik van de meetkastjes kwamen kregen een unieke code, zo kon de gemeente nagaan hoe druk het is in de binnenstad.

Maar als u over een langere termijn bijhoudt welke mobiele telefoon langs een bepaald meetkastje komt, kan dit leiden tot het volgen van mensen. De Autoriteit Persoonsgegevens (AP) oordeelde dat deze manier van handelen niet toelaatbaar is. Er werd een te grote inbreuk gemaakt op de privacy van de burgers. Het gevolg was een boete van € 600.000.[1]

1. Autoriteit Persoonsgegevens, 'Boetebesluit AP gemeente Enschede', 11 maart 2021, https://bit.ly/3tFpDtP

Wanneer moet een DPIA uitgevoerd worden?

Een DPIA moet worden uitgevoerd wanneer een gegevensverwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context, en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen.[2] De norm "waarschijnlijk een hoog risico inhouden" is een open norm. Dit dient u als verwerkingsverantwoordelijke dus zelf vast te stellen.

2. Artikel 35 lid 1 AVG.

Voorbeelden

Gaat uw organisatie gebruik maken van een nieuw CRM-systeem, waarin allerlei klantgegevens worden verwerkt, dan zal een DPIA uitgevoerd moeten worden. Van plan om allerlei databases te combineren en big data-analyses uit te voeren? Ook dat is een geval waarin een DPIA nodig is.

In de Algemene verordening gegevensbescherming (AVG) zijn enkele voorbeelden opgenomen van situaties waarin een DPIA verplicht is:[3]

- Grootschalige besluiten worden genomen gebaseerd op geautomatiseerde verwerkingen van persoonsgegevens, zoals bij profilering
- Grootschalige verwerking van bijzondere persoonsgegevens of strafrechtelijke gegevens
- Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten

3. Artikel 35 lid 3 AVG.

Naast de situaties die in de AVG zijn opgenomen, zijn er nog meer situaties waarin een DPIA uitgevoerd moet worden. De AP heeft een DPIA-lijst gepubliceerd waarin is opgenomen in welke situaties een DPIA in ieder geval verplicht is.[4] In die lijst staan bijna twintig onderwerpen waarbij het dus verplicht is om een DPIA uit te voeren. Denk bijvoorbeeld aan samenwerkingsverbanden waarbij gemeenten met andere organisaties, zoals politie, brandweer maar ook een woningcorporatie persoonsgegevens delen. Er zal dan een DPIA uitgevoerd moeten worden op dat project. Ook in geval van het monitoren van werknemers (of studenten) is het verplicht om een DPIA uit te voeren. Denk bijvoorbeeld aan het gebruik van volgsoftware door werkgevers. Dit kan een flinke inbreuk opleveren op de privacy van medewerkers.

4. Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens (*Stcrt*. 2019, 64418).

To do, or not to do, that's the question!

Of is het toch eigenlijk niet echt een vraag? Stel, uw organisatie is (mogelijk) verplicht om een DPIA uit te voeren en dat wordt niet gedaan. Dan kunt u als organisatie een flinke boete verwachten. De maximale boete voor het niet uitvoeren van een DPIA is tien miljoen euro, of twee procent van de wereldwijde jaaromzet (welke hoger is). Nu zal een maximale boete niet snel voorkomen, maar de basisboete is ook niet mis. De boetebeleidsregels van de AP hebben het basisboete bedrag voor het niet uitvoeren van een DPIA namelijk vastgesteld op €310.000[5] Dit bedrag wordt naar boven of beneden aangepast, afhankelijk van de omstandigheden. Denk hierbij bijvoorbeeld aan de mate van verwijtbaarheid, maar ook om welke (soort) persoonsgegevens het gaat.

5. Boetebeleidsregels Autoriteit Persoonsgegevens 2019 (*Stcrt*. 2019, 14586).

Naast dat het dus flinke boetes kan opleveren, kleven er nog andere risico's aan het niet uitvoeren van een DPIA. De DPIA is, zoals eerder al genoemd, ook bedoeld om risico's van de gegevensverwerking aan het licht te brengen. Uit een DPIA kan bijvoorbeeld volgen dat bepaalde gegevens helemaal niet verwerkt mogen worden. Als dit wel gebeurt kan dit ook flinke boetes opleveren. Deze eventuele boetes kunnen dan boven op de eerdergenoemde boete van €310.000 komen! Dus als u twijfelt of een DPIA wel nodig is, doe het dan gewoon. Niet alleen geeft het u en uw organisatie inzicht in hoe de gegevensverwerking verloopt, het biedt ook zekerheid. U krijgt geen boete voor het "onnodig" uitvoeren van een DPIA!

Wat staat er in een DPIA?

Heeft uw organisatie te maken met een project waarop een DPIA uitgevoerd moet worden, dan rest nog de vraag hoe dat dan moet gebeuren. Wat voor informatie moet u opnemen in een DPIA? Kort gezegd moet uit de DPIA volgen wat voor persoonsgegevens er verwerkt gaan worden, wat er met de gegevens gebeurt en op welke manier de gegevens beveiligd worden.

Er zijn verschillende DPIA-modellen in omloop. U kunt er ook voor kiezen om zelf een template te maken in Word of Excel. Wat u ook gebruikt, let erop dat de DPIA aan alle wettelijke vereisten voldoet. Zo moeten onderstaande onderwerpen terugkomen in de DPIA:

1. Welke persoonsgegevens, en van welke betrokkenen er door welke partijen worden verwerkt
2. Het doel van de gegevensverwerking en de wettelijke grondslag
3. Noodzakelijkheid van de persoonsgegevens die verwerkt worden, en de juistheid van gegevens
4. Bewaartermijnen
5. Verwerkers- of data-uitwisselingsovereenkomsten met derde partijen
6. Verwerkingslocatie (binnen of buiten de Europese Economische Ruimte)
7. Informatieplicht richting betrokkenen
8. Rechten van betrokkenen
9. Beveiligingsmaatregelen

Per onderwerp zullen privacy risico's naar boven komen, en vervolgens is het van belang om ervoor te zorgen dat de risico's verkleind worden. Komt u er tijdens het uitvoeren van de DPIA achter dat er nog geen verwerkersovereenkomst is gesloten met de bouwer van de applicatie, dan is dat een risico. Vervolgens is het dus van belang om alsnog een verwerkersovereenkomst te sluiten. Als er nog geen bewaartermijnen zijn vastgelegd, dan moeten die alsnog bepaald worden. Worden er bijzondere persoonsgegevens verwerkt en is het systeem nog niet met tweefactorauthenticatie beveiligd, dan is dat een actiepunt dat opgepakt moet worden.

Uiteindelijk staan er in de DPIA allerlei risico's, maar ook actiepunten zodat de risico's verkleind kunnen worden. Houd voor ogen dat aan de ene kant alles draait om de privacy van betrokkenen, maar ook de verantwoordelijkheid van de eigen organisatie. Als organisatie moet u immers de AVG naleven, en op zorgvuldige wijze omgaan met persoonsgegevens.

Plan-Do-Check-Act

Na het uitvoeren van een DPIA is het nog niet klaar. Het is de bedoeling dat u periodiek de gegevensverwerking beoordeelt. Er kan immers een hoop veranderen. Worden nog steeds dezelfde persoonsgegevens verwerkt, of worden inmiddels ook bijzondere persoonsgegevens verwerkt? Zijn alle verwerkers nog hetzelfde of is er een overstap gemaakt naar een andere partij? Zijn de beveiligingsmaatregelen nog op orde, of moeten die aangescherpt worden? Zijn er op juridisch vlak nieuwe ontwikkelingen? De DPIA in de lade laten liggen is dan ook niet de bedoeling. Eens in de zoveel tijd moet u toch echt die lade opentrekken, het stof van de DPIA afblazen en er nog eens met een frisse blik naar kijken.

Maak tijdens het uitvoeren van de DPIA een planning voor revisies. Hoe vaak is een revisie nodig? Als het een relatief onveranderlijke verwerking van persoonsgegevens is, dan kunt u mogelijk volstaan met een jaarlijkse revisieronde. Voor sommige verwerkingen kan het per kwartaal of half jaar nodig zijn. Het is in ieder geval vereist om een nieuwe versie van de DPIA te maken als de verwerking van persoonsgegevens (fundamenteel) wijzigt. Door de DPIA regelmatig te bekijken en aan te passen, blijft u als organisatie scherp. Privacy van betrokkenen moet immers gewaarborgd blijven.

Where privacy meets design

Maak privacy aantoonbaar

PRIVACY VERIFIED

Met ons documentcertificeringsprogramma helpen wij uw organisatie om privacydocumenten op een praktische, maar vooral ook leesbare wijze aan klanten aan te bieden. Middels visualisatie van de documenten wordt de juridische context van de documenten voor iedere lezer begrijpelijk gemaakt. Hiermee wordt voorkomen dat klanten lange juridische teksten moeten doorspitten om te controleren op welke wijze privacy wordt gewaarborgd. Daarnaast wordt ieder document voorzien van een samenvatting inclusief een certificaat, zodat klanten in één oogopslag kunnen zien wat de belangrijkste punten uit het document zijn en dat er een aantoonbare controle heeft plaatsgevonden.

Actie: ontvang eenmalig €150,- korting op een van de privacydocumenten uit ons documentcertificeringsprogramma. Actie geldt t/m 15 mei 2022.

Kijk voor meer informatie en onze prijzen op:
www.privacyverified.nl/documentcertificering

Chantal Sitaram
Juridisch adviseur

Cloud Overheid

To infinity and beyond!

Ooit overwogen om voor eigen amusement een reis naar de ruimte te maken? De ruimtevaart was gedurende lange tijd volledig in handen van overheidsinstanties als de Amerikaanse NASA en Europese ESA. Hier is echter een verschuiving in gekomen door de opkomst van commerciële ruimtevaartbedrijven die ruimtereizen voor gewone burgers toegankelijker willen maken. Een moment van gewichtloosheid, ronddwalen in een donkere sterrenhemel en het zien van de ronding van onze aarde. Deze unieke ervaring en het verlangen naar het onbekende heeft ertoe geleid dat het grensverleggende fenomeen 'ruimtetoerisme' zich is gaan ontwikkelen. Hierbij rijzen natuurlijk de nodige juridische vragen. Hoe dient ruimtetoerisme juridisch te worden gekwalificeerd? En hoe zit het met de veiligheid aan boord en de aansprakelijkheid voor schade aan ruimtetoeristen?

Het concept 'ruimtetoerisme'

Ruimtetoerisme kan worden omschreven als het reizen van mensen naar de ruimte voor recreatieve doeleinden. Er kunnen verschillende soorten ruimtereizen worden gemaakt, waaronder orbitaal en suborbitaal. Bij een orbitale vlucht blijft het voertuig in hoge snelheid gedurende een aantal dagen in een baan om de aarde, terwijl er bij een suborbitale vlucht met een lagere snelheid binnen twee tot drie uur een ruimtesprong wordt gemaakt. Maar wanneer spreken we van 'de ruimte'? Hoewel dit nergens officieel is vastgelegd, ligt de denkbeeldige grens tussen de lucht- en ruimtevaart, bekend als de Kármánlijn, op een hoogte van ongeveer 100 kilometer boven de aarde.

De Amerikaanse multimiljonair Dennis Tito bracht in 2001 als eerste ruimtetoerist bijna acht dagen door aan boord van het internationale ruimtestation ISS. Hij werd hier met het Russische Sojoez TM-32 naartoe gebracht en betaalde ongeveer 20 miljoen dollar voor het waarmaken van deze jongensdroom. Sindsdien zijn er dankzij diverse miljardairs commerciële ruimtevaartbedrijven uit de grond geschoten

om gehoor te geven aan de groeiende publieke interesse in de ruimte. Hiervan hebben Blue Origin, Virgin Galactic en SpaceX in de afgelopen jaren veel naamsbekendheid gekregen. Zo maakte de 18-jarige Nederlandse miljardairszoon, Oliver Daemen, samen met Amazon-oprichter en eigenaar van Blue Origin, Jeff Bezos, in juli 2021 een suborbitale vlucht naar de Kármánlijn. Richard Brandson richt zich met Virgin Galactic ook op het maken van suborbitale vluchten en heeft vorig jaar zijn eerste volledig bemande testvlucht naar de rand van de ruimte voltooid. SpaceX, waar Elon Musk de oprichter en CEO van is, verwacht dit jaar juist orbitale vluchten te kunnen maken met het ruimtevaartuig Starship.

Welk recht is van toepassing?

Om vragen omtrent de veiligheid van ruimtetoeristen en aansprakelijkheid voor schade te kunnen beantwoorden, is het allereerst noodzakelijk om te bepalen welk recht van toepassing kan worden verklaard. Gezien het gaat om ruimtevluchten lijkt het voor de hand liggend om internationaal ruimterecht toe te passen. Uit artikel VII van de *Outer Space Treaty* vloeit voort dat lidstaten internationaal aansprakelijk zijn voor schade veroorzaakt in de ruimte. Dit geldt ook voor schade door private commerciële ruimteactiviteiten. Echter, schade die ruimtetoeristen lijden aan boord van een voertuig wordt hiervan uitgezonderd.[1] Dit is een reden om terug te vallen op luchtvaartverdragen en -regelingen. De ontwikkeling van de luchtvaartindustrie is immers op een vergelijkbare manier begonnen. Het is namelijk niet altijd gebruikelijk geweest dat een luchtvaartmaatschappij aansprakelijk kan worden gesteld voor schade aan haar passagiers inclusief de verplichting om hier een redelijke vergoeding voor uit te keren.

1. Artikel VII van de Convention on International Liability for Damage Caused by Space Objects.

Vliegtuig, ruimtevaartuig of iets ertussenin

De International Civil Aviation Organisation (ICAO) heeft aan de hand van het Verdrag van Chicago internationale veiligheidsnormen en richtlijnen opgesteld voor de burgerluchtvaart. Een 'vliegtuig' wordt hierin gedefinieerd als een gemotoriseerd luchtvaartuig met vleugels.[2] De vleugels kunnen een recht- of driehoekige vorm hebben en worden gemaakt van materialen als doek, hout of metaal. Dit resulteert in het feit dat bijna de helft van de voertuigen die wordt gemaakt voor het uitvoeren van suborbitale ruimtevluchten niet onder de definitie van een vliegtuig valt. Hierdoor vervalt de mogelijkheid om de ICAO-veiligheidsnormen toe te passen, simpelweg omdat deze voertuigen geen vleugels hebben.[3] Ook bestaat er een hybride variant waarin een voertuig opstijgt als een luchtvaartuig, maar gedurende de vlucht de vleugels zal verliezen en uiteindelijk zal landen als een ruimtevaartuig.

2. Glossary of Terms ICAO.
3. Handbook of Space Law, Chapter 12, 2015.

Gezien de toepassing van internationale wet- en regelgeving afhankelijk is van het soort voertuig, valt een grote categorie voertuigen hierbuiten. Het gevolg hiervan is dat staten hun eigen regelingen opstellen om zo invulling te geven aan dit grijze gebied.[4] De Verenigde Staten, waar de Federal Aviation Administration (FAA) bevoegdheden heeft in zowel de lucht- als ruimtevaart, zijn hier het meest gevorderd in. Er is gekozen om een vergunningenbeleid te voeren in combinatie met een *informed consent* door de deelnemende ruimtetoeristen.[5] In laatstgenoemde wordt in nogal vage bewoordingen gewezen op de mogelijke gevaren van de ruimtevlucht, waarmee de ruimtetoerist door ondertekening een deel van de risico's op zich neemt. In Europa heeft de EASA de wens om alles rondom ruimtevluchten te certificeren vóór de eerste commerciële vlucht.[6]

4. Handbook of Space Law, Chapter 12, 2015.
5. CRS Report, The Future of Space Tourism, 2020.
6. Introduction to Space Law, 2019.

Binnenkort op reis naar de ruimte?

Ruimtetoerisme is zich sterk aan het ontwikkelen. Vooralsnog treft noch het internationale ruimterecht, noch de luchtwetgeving sluitende voorzieningen op het gebied van veiligheid en aansprakelijkheid. Voorts is er geen uitsluitsel over de vraag onder welke juridische definitie de voertuigen horen te vallen. Daarom lijkt toepassing naar analogie van de bestaande verdragen en regelingen in de lucht- en ruimtevaart momenteel het meest geschikt. Nationale regelingen spelen hier ook een leidende rol in. De verwachting is dat dezelfde lijn gevolgd zal worden als binnen de luchtvaartindustrie. Het maken van een betaalbare reis naar de ruimte die ook nog eens volledig juridisch is afgedekt, zal echter voorlopig nog even op zich laten wachten.

Bram de Vos
Juridisch adviseur

Wet- en regelgeving

Wetsvoorstel Archiefwet 2021

Op 17 november 2021 heeft toenmalig minister Slob van Basis- en Voortgezet Onderwijs en Media een voorstel voor een nieuwe Archiefwet ingediend bij de Tweede Kamer. De huidige Archiefwet, die regels stelt aan de informatiehuishouding van de overheid, dateert nog uit 1995. Omdat digitalisering van de overheid toen nog in de kinderschoenen stond, zijn de regels en toelichtingen uit de Archiefwet 1995 vooral toegespitst op papieren archieven. In de Archiefwet 2021 wordt juist aansluiting gezocht bij de digitale samenleving van vandaag. Het wetsvoorstel voorziet in significante wijzigingen in zowel de structuur als de inhoud van de Archiefwet. Zo voorziet het voorstel in een geheel nieuwe hoofdstukindeling en worden de eisen die gelden voor de toegankelijkheid van informatie gemoderniseerd en aangescherpt.

https://bit.ly/3BFuMFS

Richtsnoeren doorgifte persoonsgegevens naar derde landen

Op 18 november 2021 heeft het European Data Protection Board (EDPB) nieuwe richtlijnen gepubliceerd over de doorgifte van persoonsgegevens naar derde landen. Op grond de Algemene verordening gegevensbescherming (AVG) mogen persoonsgegevens vrijelijk worden doorgegeven naar landen binnen de Europese Economische Ruimte (EER). Doorgifte naar landen buiten de EER (derde landen) is alleen toegestaan als er aan aanvullende eisen is voldaan. Het is daarbij niet altijd duidelijk wanneer er sprake is van een “doorgifte” in de zin van de AVG. Met de nieuwe richtsnoeren van het EDPB wordt hier nadere invulling aan gegeven.

https://bit.ly/3v7JLqJ

Richtlijnvoorstel ter verbetering van de arbeidsvoorwaarden bij platformwerk

Op 9 december 2021 hebben het Europees Parlement en de Raad een voorstel voor de Richtlijn betreffende de verbetering van arbeidsvoorwaarden bij platformwerk gepubliceerd. De afgelopen jaren is er veel commotie geweest over de platformeconomie en de manier waarop met platformwerkers wordt omgegaan. Er werden diverse rechtszaken gevoerd tegen exploitanten van online platforms. Echter bestaan ook in veel andere situaties zorgen over schijnzelfstandigheid. Met de invoering van de nieuwe richtlijn moet er meer duidelijkheid komen over de arbeidsrechtelijke status van de platformwerkers. Daarnaast bevat de richtlijn diverse regels die specifiek op de platformeconomie zijn gericht, onder andere op het gebied van geautomatiseerde monitoring en besluitvorming.

https://bit.ly/3sWQGAC

Verlenging Tijdelijke wet notificatieapplicatie COVID-19

Op 10 december 2021 heeft toenmalig minister De Jonge van Volksgezondheid, Welzijn en Sport besloten om de wet voor de CoronaMelder-app te verlengen tot april 2022. Ondertussen loopt het gebruik van de app terug. Volgens NU.nl waarschuwde in de periode van januari tot en met mei 2021 nog 12 procent van de mensen na een positieve coronatest anderen via de

app. Inmiddels is dit percentage teruggezakt naar 6,5 procent. Daarmee neemt ook de effectiviteit van het systeem af.

https://bit.ly/3LOHsyN https://bit.ly/3JLa1vf

Intrekking voorstel tijdelijke wet informatie-verstrekking RIVM

Op 17 januari 2022 heeft minister-president Mark Rutte het voorstel voor de Tijdelijke wet informatie-verstrekking RIVM ingetrokken. De wet zou aanbieders van openbare mobiele telecommunicatienetwerken gaan verplichten om informatie te delen met het Rijksinstituut voor volksgezondheid en milieu (RIVM) in het kader van de bestrijding van COVID-19. De verkeers- en locatiegegevens van deze aanbieders zouden belangrijke inzichten kunnen bieden bij de bestrijding van het virus. Onder meer burgerrechten-organisatie Bits of Freedom was tegen de invoering van de wet, omdat het om een vorm van massasurveil-lance gaat waarbij de noodzakelijkheid van de wet onvoldoende werd aangetoond. Mede in het licht van het nieuwe coalitieakkoord heeft het nieuwe kabinet besloten om het wetsvoorstel in te trekken.

https://bit.ly/35iipTT

Richtsnoeren inzagerecht betrokkenen

Op 18 januari 2022 heeft het EDPB nieuwe richt-snoeren gepubliceerd over het recht op inzage van betrokkenen. Op grond van artikel 15 AVG hebben betrokkenen een wettelijk recht om inzage te vragen in alle persoonsgegevens die een organisatie van hem of haar verwerkt. Blijken de gegevens niet te kloppen of bijvoorbeeld onterecht verwerkt te worden, dan kan de betrokkene onder meer verzoeken om de gegevens aan te passen of te verwijderen. Met deze richtsnoeren worden verschillende praktische vragen over het inzagerecht beantwoord.

https://bit.ly/3HbxV1p

Aankondiging wetsontwerp voor standaardpoort elektronische apparaten

De Raad van de Europese Unie heeft op 26 januari 2022 aangekondigd dat er gewerkt wordt aan een wet voor de invoering van een standaardpoort voor allerhande elektronische apparaten (onder andere smartphones, tablets en draagbare audioapparaten). Op dit moment worden er door marktpartijen nog verschillende oplaadinterfaces toegepast. Denk aan de verschillende USB-interfaces en de eigen Lightningaansluiting van Apple. De Europese Unie wil er naartoe dat straks alle elektronische apparaten gebruik gaan maken van USB-C. Op die manier kunnen consumenten met één universele lader uit de voeten en wordt de hoeveelheid elektronisch afval beperkt. Onder meer Apple heeft zich kritisch uitgelaten over het voorstel. Het bedrijf wijst er onder meer op dat de markt vanzelf al richting USB-C beweegt. Zo zijn de nieuwere generaties MacBooks ook van deze poort voorzien. Daarnaast zou een dergelijke wet onder meer de ontwikkeling van nieuwe, innovatieve oplaadinterfaces kunnen frustreren volgens Apple.

https://bit.ly/3v84XNE https://bit.ly/3H9Uq6H

Aanpassing procesreglement wegens uitfasering faxcommunicatie

Met ingang van 1 februari 2022 zijn er diverse proces-reglementen aangepast, waarmee de Rechtspraak definitief afscheid heeft genomen van communicatie via de fax. Omdat KPN volgend jaar stopt met het aanbieden van de ISDN-dienstverlening voor tradi-tioneel faxen, stapt de Rechtspraak over op Veilig Mailen (Zivver). Het systeem zoekt aansluiting bij NTA 7516, een bestaande NEN-norm voor veilig mailverkeer in de zorg. Op die manier moet de beschikbaarheid, integriteit en vertrouwelijkheid van het mailverkeer geborgd worden.

https://bit.ly/3BGFeNo

Tessa van Schijndel
Juridisch adviseur

Pelçim Kaygusuz
Juridisch adviseur

E-health

Nieuwe wetgeving voor voorspellende diagnostische tests (en andere in-vitro diagnostica)

Het zal u vast niet ontgaan zijn: de wijzigingen in de regelgeving rondom medische hulmiddelen. Vanaf 26 mei 2022 gaat ook de nieuwe Europese verordening voor in-vitro diagnostica (IVDR) in.[1] De IVDR vervangt de bestaande EU Richtlijn voor medische hulpmiddelen voor in-vitro diagnostiek.[2] Kort gezegd zijn hulpmiddelen voor in-vitro diagnostiek hulpmiddelen om diagnostische testen uit te voeren waarmee monsters uit het lichaam worden onderzocht. Als een fabrikant een medisch hulpmiddel voor in-vitro diagnostiek op de markt wil brengen, heeft hij een CE-markering nodig. Die CE-markering geeft aan dat het product voldoet aan de wettelijke veiligheids- en kwaliteitseisen. Ook voor andere marktdeelnemers, zoals distributeurs en importeurs gaan er regels gelden. Ten slotte verkrijgt ook de zorginstelling een speciale vermelding in de IVDR op het moment dat de instelling in eigen huis gaat ontwikkelen.

1. (EU) 2017/746 Verordening In-vitro diagnostiek.
2. 98/79/EG Richtlijn In-vitro diagnostiek.

De MDR (Verordening medische hulpmiddelen) is van toepassing op medische hulpmiddelen die in direct contact komen met de mens. De IVDR is van invloed op een kleiner scala van producten en heeft een langere implementatieperiode. Maar is de IVDR om die reden een ondergeschoven kindje van de MDR? Think again! In dit artikel lichten wij een aantal belangrijke aandachtspunten toe voor software voor in-vitro diagnostiek.

Achtergrond IVDR

De van toepassing wordende wet maakt een einde aan de gefaseerde inwerkingtreding van de wetgeving omtrent medische hulpmiddelen. Zowel de MDR als IVDR zijn op 25 mei 2017 in werking getreden, maar de regels voor medische hulpmiddelen gelden vanaf 26 mei 2020. Vanaf 26 mei 2022 gaan de regels voor medische hulpmiddelen voor in-vitro diagnostiek gelden. De wetgeving heeft de vorm van een verordening, wat betekent dat zowel de MDR als de IVDR rechtstreeks van toepassing is in de Europese Unie en niet omgezet hoeft te worden in nationale wetgeving.

Met de inwerkingtreding van de IVDR is het complete regelgevend kader voor medische hulpmiddelen afgerond. Voor alle marktdeelnemers ligt er een complete set aan dwingende spelregels om medische hulpmiddelen op de markt te brengen en te gebruiken.

Toepassingsbereik en opzet IVDR

De opzet van de IVDR lijkt enorm veel op de opzet van de MDR. De regels uit de IVDR gelden voor fabrikanten van hulpmiddelen, importeurs en distributeurs. Afhankelijk van de rol die de zorginstelling inneemt, kunnen er ook eisen voor zorginstellingen gelden. Voor zorginstellingen gelden namelijk dezelfde regels uit de MDR. Zorginstellingen hoeven geen CE-markering te verkrijgen als de in-vitro diagnostiek geheel in eigen huis wordt ontwikkeld en toegepast. Wel moet er een kwaliteitsmanagementsysteem zijn en moet de zorginstelling haar uitzonderingspositie kunnen rechtvaardigen door aan te tonen dat er geen gelijkwaardig hulpmiddel op de markt is.

Een medisch hulpmiddel voor in-vitro diagnostiek

Een medisch hulpmiddel is een hulpmiddel dat door de fabrikant is bestemd voor een medisch doel, zoals de behandeling van een ziekte, de verlichting van een handicap of het onderzoek van een fysiologisch proces. In-vitro diagnostiek is een subtype van een medisch hulpmiddel dat specifiek bestemd is voor onderzoek van specimen die afkomstig zijn van het menselijk lichaam. Het heeft een medisch doel, bijvoorbeeld om een diagnose te stellen of een behandeling te volgen. In tegenstelling tot de medische hulpmiddelen die onder de MDR vallen, zijn zij niet bestemd om rechtstreeks in contact te komen met de patiënt, maar wel om in contact te komen met specimen die afkomstig zijn van de patiënt (zoals bloed of urine) of om gegevens te analyseren die afkomstig zijn van een specimen.

Software valt ook onder de IVDR als de software door de fabrikant bestemd is om te worden gebruikt voor het in-vitro onderzoek met het doel om medische informatie te verschaffen over bijvoorbeeld een ziekte, letsel of behandeling. Denk hierbij aan voorspellende diagnostische software om ziektes te voorspellen of om een behandelplan gerichter op te stellen. Dit kan gaan over biomarkers, vormen van artificial intelligence (AI) zoals machine- en/of deep learning of andere diagnostische tests.

De risicoclassificatie

In tegenstelling tot de MDR verandert de IVDR veel met betrekking tot de indeling in de verschillende risicoklassen. Om deze reden heeft de Medical Device Coordination Group (MDCG) een guidance gepubliceerd om het classificeren van in-vitro diagnostica makkelijker te maken.[3] De MDCG is een door de Europese Commissie ingestelde werkgroep voor medische hulpmiddelen.

3. MDCG 2020-16.

De IVDR voert een heel nieuw classificeringsmechanisme in. Onder de oude wetgeving wordt er een onderscheid gemaakt tussen in-vitro diagnostica die wel of niet in bijlage II van de Richtlijn zijn opgenomen. In-vitro diagnostica uit bijlage II moesten worden gecertificeerd door een aangemelde instantie (Notified Body) en de overige in-vitro diagnostica konden door de fabrikanten zelf worden gecertificeerd. Omdat maar een beperkt aantal in-vitro diagnostica is opgenomen in de bijlage, zijn de meeste in-vitro diagnostica door de fabrikanten zelf gecertificeerd.

Het nieuwe systeem voor risicoclassificatie in de IVDR is vergelijkbaar met het systeem in de MDR. De IVDR kent ook vier risicoklassen (A, B, C en D). Ook hier kunnen enkel klasse A in-vitro diagnostica doormiddel van een self-assesment worden gecerti-

ficeerd. De meerderheid van de in-vitro diagnostica zal dus door een Notified Body moeten worden beoordeeld. Er zullen dus een groot aantal in-vitro diagnostica die momenteel op de markt zijn, alsnog een CE-certificaat van een Notified Body moeten verkrijgen vóór 26 mei 2022.

De regels aan de hand waarvan de risicoklassen bepaald worden, werken ook op dezelfde wijze als bij de MDR, maar bevatten minder regels. De IVDR kent 7 regels en de MDR kent er 22. Software wordt ingedeeld volgens de klasse van het hulpmiddel dat zij vergezelt of beïnvloedt. De IVDR kent geen specifieke indelingsregel voor stand alone software.[4]

4. Annex VII, artikel 1.4 IVDR.

De verschillen met de MDR

De bepalingen uit de IVDR over medische software overlappen grotendeels met de bepalingen uit de MDR, maar zijn in een enkel geval ook verschillend. Op het etiket van een medisch hulpmiddel voor in-vitro diagnostiek moet worden vermeld dat het bestemd is voor in-vitrogebruik, zodat het kan worden onderscheiden van een medisch hulpmiddel. Ook moet in de ontwerpinformatie van software "een beschrijving van de methode voor de interpretatie van de gegevens, namelijk het algoritme" opgenomen worden, terwijl dit voor medische software onder de MDR geen vereiste is.[5]

5. Annex I, 3.1 IVDR en MDR.

Overgangsrecht

Ook bij de IVDR geldt dat fabrikanten nog steeds gebruik mogen maken van het overgangsrecht voor in-vitro diagnostica met een CE-markering die is verkregen onder de oude regels op de markt. Tot 27 mei 2024 mogen fabrikanten gebruikmaken van het overgangsrecht, mits er geen significante wijzigingen zijn in het beoogde gebruik of het ontwerp van de in-vitro diagnostiek.[6]

6. Artikel 110 lid 3 IVDR.

Gelukkig maar, want voor de MDR en IVDR moest na de inwerkingtreding van de verordeningen op 25 mei 2017 nog veel gebeuren voordat de wet uitvoerbaar zou zijn. Zo moest bijvoorbeeld het systeem voor de Unique Device Identifier (UDI-code) nog worden opgestart, de implementatie van de EUDAMED nog worden voltooid en misschien wel het het belangrijkst: het aanstellen van Notified Bodies die bevoegd zijn om een CE-markering af te geven. Dit heeft geleid tot veel vertraagde beschikbaarheid van de Notified Bodies waardoor bedrijven niet volledig gebruik hebben kunnen maken van deze overgangsperiode. Voor velen was het ook niet mogelijk om een hulpmiddel op tijd te laten markeren vóór de vereiste datum. Dit is een groot probleem gebleken voor alle fabrikanten die zelf de conformiteitsbeoordelingsprocedure hebben doorlopen, een CE-markering hebben aangebracht, nu een hulpmiddel hebben in een hogere risicoklasse en geen gebruik kunnen maken van het overgangsrecht. Voor in-vitro diagnostica wordt dit probleem nog groter verwacht, omdat de meeste fabrikanten van in-vitro diagnostiek zelf een CE-markering hebben aangebracht en op grond van de IVDR een CE-certificaat van een Notified Body moeten hebben.

Tot 26 mei 2022

Hoewel er nog veel voorbereidingsmaatregelen getroffen moeten worden, komt 26 mei 2022 steeds dichterbij. Veel fabrikanten van in-vitro diagnostica moeten hun hulpmiddel nog laten beoordelen door een Notified Body. Anders lopen deze partijen het risico dat zij hun hulpmiddel vanaf 26 mei 2022 niet meer op de markt mogen brengen.

Bovendien mogen de bestaande hulpmiddelen geen significante wijzigingen ondergaan zolang zij niet van een vernieuwde CE-markering zijn voorzien. Dit betekent geen belangrijke software-upgrades op in-vitro diagnostiek, omdat dit bijna altijd een significante wijziging teweegbrengt.

Gezien het relatief grote aantal in-vitro diagnostica waarvoor een eerste CE-markering nodig is in verhouding tot de beschikbare capaciteit van de enkele beschikbare Notified Body, is er geen tijd meer om te wachten met het implementeren van de nieuwe regels!

“De IVDR is van invloed op een kleiner scala van producten en heeft een langere implementatieperiode. Maar is de IVDR om die reden een ondergeschoven kindje van de MDR? Think again!”

Tessa van Schijndel
Juridisch adviseur

Pelcim Kaygusuz
Juridisch adviseur

Nick Tegelaar
Information security consultant

Security Privacy

Zo leidt u een veilige organisatie effectief

Afgelopen maand hebben wij een poll gedeeld op LinkedIn (395 stemmen) en Twitter (55 stemmen). Hierin vroegen wij wie uiteindelijk verantwoordelijk zou moeten zijn voor informatiebeveiliging. In deze vraag stonden vier opties:
1. De Directie (91% en 90.0% van de stemmen)
2. De CISO (7% en 5,5% van de stemmen)
3. De FG (1% en 1,8% van de stemmen)
4. De IT-manager (1% en 1,8% van de stemmen)

Een overweldigende meerderheid gaf aan dat de directie verantwoordelijk zou moeten zijn. Mijns inziens is dit het enige juiste antwoord op de vraag, maar toch is dit in de praktijk niet altijd terug te zien. Ondanks dat voor de meerderheid in ons netwerk wellicht al duidelijk is dat de directie uiteindelijk verantwoordelijk is voor informatiebeveiliging, wil ik deze vraag toch op een analytische wijze beantwoorden.

RASCI-model

Een belangrijke noot is dat er wordt gevraagd naar wie 'uiteindelijk' verantwoordelijk is. Om de verantwoordelijkheidsvraag helder te krijgen wil ik het RASCI-model uitlichten. Dit model bestaat uit vijf verantwoordelijkheden:

1. **Responsible**, de rol die verantwoordelijk is. Dit is minimaal één persoon.
2. **Accountable**, de rol die eindverantwoordelijk is. Dit is maar één rol, en is altijd (onderdeel van) senior management.
3. **Support**, de rol die ondersteuning levert.
4. **Consult**, de rol die kan adviseren.
5. **Inform**, de rol die moet worden geïnformeerd.

Aan de hand van het RASCI-model kunnen we bepalen dat wordt gevraagd wie 'accountable' is. Dit zal leiden tot een ander antwoord dan wanneer wordt gevraagd wie verantwoordelijk (responsible) is. Om de vraag te beantwoorden wie eindverantwoordelijk is voor informatiebeveiliging kijken we naar de ISO 27001 en de NEN 7510. De ISO 27001/NEN 7510 zijn standaarden voor een 'Information Security Management System' (ISMS).

ISMS en leiderschap

Wanneer een organisatie een ISMS conform een van deze standaarden inricht, komt zij in aanmerking voor certificering. Certificering kan leiden tot talloze voordelen omdat u als organisatie aantoonbaar in control bent van informatiebeveiliging, waaronder een nieuwe aanwas van klanten. Daarnaast kan certificering verplicht zijn vanuit leveranciers, of vanuit overheidsinstellingen om, bijvoorbeeld, in aanmerking te komen voor subsidies.

Niet alleen organisaties die een certificering ambiëren hebben baat bij een juiste inrichting van een ISMS. Ook andere organisaties kunnen hiervan profiteren. Bovendien dwingt de AVG organisaties om voldoende technische en organisatorische beveiligingsmaatregelen te nemen. Met de implementatie van een ISMS zet u hiervoor belangrijke stappen. De inrichting van een ISMS hoeft niet te betekenen dat u direct moet overgaan tot certificering van de ISO 27001/NEN 7510. Een dergelijke certificering vraagt namelijk meer van organisaties dan het enkel inrichten van een ISMS. Zo moet bijvoorbeeld ook een interne audit zijn uitgevoerd.

Hoe de implementatie van het ISMS er in zijn volledigheid uitziet valt buiten de scope van dit artikel, maar ik wil wel graag inzoomen op de onderdelen die zien op het stukje leiderschap om de vraag die voorhanden ligt te beantwoorden.

In hoofdstuk 5 van de ISO 27001/NEN 7510 komen harde vereisten terug voor leiderschap. In het kort:

- Directie moet het informatiebeveiligingsbeleid vaststellen dat passend is voor de organisatie. Dat beleid moet concrete informatiebeveiligingsdoelstellingen bevatten of een kader bieden voor het vaststellen van dergelijke doelstellingen.
- De directie moet de verantwoordelijkheden en bevoegdheden met betrekking tot informatiebeveiliging toekennen en communiceren.
- Een hoop concrete verantwoordelijkheden, waaronder:
  - het bewerkstelligen dat het informatiebeveiligingsbeleid en de informatiebeveiligingsdoelstellingen worden vastgesteld en aansluiten op de strategie van de organisatie;
  - het belang van informatiebeveiliging en het ISMS te communiceren aan de organisatie;
  - het bewerkstelligen dat er voldoende resources beschikbaar zijn en dat de beoogde resultaten worden behaald;
  - mensen aan te sturen en te ondersteunen om een bijdrage te leveren aan de doeltreffendheid van het ISMS; en
  - andere relevante managementfuncties te ondersteunen om hun leiderschap te tonen binnen hun verantwoordelijkheidsgebieden.

In hoofdstuk 9.3 wordt de directie op nog een verantwoordelijkheid gewezen. Ze moet namelijk het ISMS met geplande tussenpozen beoordelen om de continue geschiktheid, toereikendheid en de doeltreffendheid van het ISMS te waarborgen.

Aan de hand van bovenstaande vereisten is het niet onlogisch om te concluderen dat de directie eindverantwoordelijk (accountable) is voor informatiebeveiliging. Wat er ook gebeurt in de lagen daaronder, de directie is hiervoor verantwoordelijk. Een vraag waar ik me nu niet aan wil wagen is of directieleden persoonlijk aansprakelijk zijn als de informatiebeveiliging niet op orde is, maar ik kan me voorstellen dat dergelijke scenario's bestaan.

De directie zal hoogstwaarschijnlijk de verantwoordelijkheden van informatiebeveiliging (in bepaalde mate) delegeren. Een rol die daar vaak voor wordt gebruikt is de CISO of de (I)SO. Het gebruik van deze rol kan echter verwarrend zijn, omdat de CISO vaak wel de verantwoordelijkheden krijgt van informatiebeveiliging, maar niet de invloed om het werk effectief te verrichten. In een ideale situatie heeft de CISO wel voldoende bevoegdheden, de CISO zou dan verantwoordelijk zijn (responsible). Wanneer de CISO een directiefunctie betreft dan is er misschien eerder sprake van gedelegeerde eindverantwoordelijkheid (accountable) vanuit de directie aan de CISO.

Uitdagingen

Als we inzoomen op informatiebeveiliging stuiten we ook op andere verantwoordelijkheidsvragen: 1) welke risico's loopt mijn informatie? 2) hoe kan ik deze risico's het beste mitigeren? 3) wie mag toegang hebben tot mijn informatie?

In principe is een informatie-eigenaar verantwoordelijk voor zijn 'eigen' informatie. De CISO zou hier een adviserende en controlerende rol in moeten spelen. Het kan dus zo zijn dat een informatie-eigenaar responsible is, terwijl de CISO een meer consult/inform rol aanneemt. Omdat de mate van beveiliging uiteindelijk toch de verantwoordelijkheid is van de CISO lijkt het mij echter logischer om de CISO dan als medeverantwoordelijk te benoemen (responsible). In beide gevallen is de directie eindverantwoordelijk (accountable).

Een aantal uitdagingen met betrekking tot verantwoordelijkheid die ik vaak terugzie bij organisaties zijn:

- Directie heeft een CISO aangesteld, die geen onderdeel is van directie. De CISO mist daarnaast een passend directiemandaat om het ISMS goed te sturen en de informatiebeveiligingsdoelstellingen te halen. Bovendien mist de communicatie binnen de organisatie over deze belangrijke rol. Met als gevolg dat de CISO geen draagkracht heeft van andere afdelingen en de medewerkers, waardoor de implementatie van het ISMS niet van de grond komt.

- Informatiebeveiliging is direct onder IT gepositioneerd. Dit betekent dat de CISO of de Security Officer, en in sommige gevallen de Privacy Officer, rapporteert aan de IT-manager. De IT-manager rapporteert vervolgens aan een directielid over informatiebeveiliging. Bij de uitvoering van werkzaamheden in de rol van Security Officer zal u in deze verhoudingen allerlei obstakels tegenkomen. Informatiebeveiliging betreft namelijk meer dan de technische invulling van beveiligingsmaatregelen. Denk aan verplichte awareness trainingen voor nieuwe medewerkers, exitgesprekken, controles op IT, de beveiliging van het pand, etc. Daarnaast kan het voorkomen dat de IT-manager en jij belangen hebben die tegenstrijdig zijn, zo kan de IT-manager, bijvoorbeeld, een bepaalde applicatie van een leverancier willen terwijl jij de leverancier niet veilig genoeg acht.
- De reden dat informatiebeveiliging toch vaak onder IT komt te vallen heeft te maken met het feit dat informatiebeveiliging te veel als een IT-gelegenheid wordt gezien, en het initiatief om informatiebeveiliging serieus op te pakken vaak van de IT-afdeling komt.
  Deze bottom-up benadering van informatiebeveiliging is misschien een goed begin, maar zal nooit kunnen leiden tot een gedegen en complete aanpak van informatiebeveiliging. U zou zelfs kunnen beargumenteren dat IT aan de CISO of de Security Officer zou moeten rapporteren, omdat zij 'responsible' zijn voor informatiebeveiliging.
- Informatie-eigenaren worden niet of onvoldoende betrokken bij de beveiliging van hun informatie of informatiewerkende middelen. Helaas komt het ook vaak genoeg voor dat informatie-eigenaren geen idee hebben hoe hun informatie is beveiligd, en waarom.

Kies voor een top-down werking!

De hierboven omschreven uitdagingen zijn een kleine greep uit de praktijk die ik regelmatig tegenkom bij organisaties. Het geeft aan hoe incorrecte organisatorische verhoudingen binnen informatiebeveiliging kunnen leiden tot onwenselijke situaties. Ik pleit dan ook voor een top-down werking van informatiebeveiliging, waarbij de initiële en uiteindelijke verantwoordelijkheid ligt bij de directie. De directie kan een directeur aanwijzen als portefeuillehouder van informatiebeveiliging en eventueel privacy). Die directeur moet ervoor zorgen dat informatiebeveiliging tijdens het directieoverleg wordt geagendeerd, en houdt de overige directieleden op de hoogte van de stand van zaken.

Mijn advies is om vervolgens een directieverklaring uit te brengen naar de organisatie om aan te geven wat de intentie is van de organisatie met betrekking tot informatiebeveiliging. U kunt bijvoorbeeld denken aan de intentie om te certificeren, of gewoon om informatiebeveiliging serieus op te pakken. Communiceer dan direct wie waarvoor verantwoordelijk is, en vraag om medewerking van de organisatie. De aanpak van informatiebeveiliging valt of staat bij de draagkracht van de medewerkers. Als de medewerker weet dat het bericht vanuit directie komt dan wordt dit serieus genomen.

Daarnaast luidt mijn advies om een ISMS conform de ISO 27001/NEN 7510 in te richten zodat commitment en leiderschap over een langere termijn, in een verbetercyclus, kan worden gegarandeerd. Certificering is uiteraard niet verplicht.

Het antwoord op de vraag

Voor een effectieve aanpak van informatiebeveiliging is dus een duidelijk, gestructureerde leiderschap nodig. Over het antwoord op de vraag 'wie is uiteindelijk verantwoordelijk voor informatiebeveiliging?' kunnen we het volgende zeggen:

- De directie is eindverantwoordelijkheid, zij kan de verantwoordelijk aan een directielid delegeren.
- Een CISO is niet eindverantwoordelijkheid, tenzij het een gedelegeerde bevoegdheid betreft van de directie en de CISO zelf een directielid is.
  De CISO kan ook gemandateerd worden door directie, maar is dan eerder 'responsible'.
- De FG moet onafhankelijk zijn en de organisatie kunnen controleren. In die zin is het niet logisch dat ze verantwoordelijkheid draagt.
- Dit IT-manager is niet eindverantwoordelijkheid. Ze speelt weliswaar een 'responsible' rol bij de implementatie van technische maatregelen, maar hierover zou ze het best kunnen rapporteren aan een (C)ISO, die dan medeverantwoordelijke (responsible) zou zijn.

Bas Dekker
Juridisch adviseur

Tim Wokke
Juridisch adviseur

Cloud

Digital Services Act: nieuwe regels voor internettussenpersonen

Op 20 januari 2022 heeft het Europees Parlement (EP) ingestemd met de Digital Services Act[1] (DSA). De DSA is een verordening en bevat in het bijzonder spelregels hoe internetproviders, hosters en online platforms om moeten gaan met illegale content. Momenteel geldt hiervoor de meer dan 20 jaar oude Richtlijn inzake elektronische handel. Met instemming van de EP is een stap gezet in de update van deze regels. Deze regels bevatten een verfijning van het huidige kader met als doelstelling bij te dragen aan verbetering en verhoging van vertrouwen in de Europese digitale markt.

1. https://bit.ly/3vyq63B

Momenteel wordt er op Europees niveau nog verder onderhandeld over de definitieve tekst van de DSA. Dit zal ongetwijfeld leiden tot verdere wijzigingen, maar de verwachting is dat dit eerder op detailniveau zal zijn. De verplichtingen die we nu al teruglezen zullen in bepaalde vorm ook in de definitieve versie terugkomen. In dit artikel wordt ingegaan op de impact van de DSA, voor wie geldt de DSA, welke verplichtingen zijn er, en per wanneer.

Voor wie geldt de DSA?

Het begrip 'tussenhandelsdienst'

De DSA zal van toepassing zijn op aanbieders van *tussenhandelsdiensten*. Het gaat daarbij om diensten op het gebied van louter doorgifte van informatie ('mere conduit'), zeer tijdelijke opslag van informatie ('caching') en het langduriger opslaan van informatie ('hosting'). Bij *mere conduit* kunt u denken aan internet-providers of VOIP-aanbieders. Bij *caching* aan content distributie diensten, zoals CDN van Cloudflare.

Anders dan bij mere conduit en caching, gaat het bij *hosting* om het opslaan van informatie voor langere duur. De DSA is voornamelijk relevant voor partijen die zich hiermee bezighouden. Het gaat daarbij echter niet alleen om de klassieke cloud- of webhoster, maar ook om andere partijen die derden in staat stellen informatie op te slaan, zoals online fora, -marktplaatsen en social media platforms.

De drie type diensten zijn overigens overgenomen uit de Richtlijn inzake elektronische handel. Qua definiëring vallen geen wijzigingen op.

Aanbieder met 'aanzienlijke band met de EU'

De DSA zal van toepassing zijn op tussenhandelsdiensten die worden verleend aan afnemers die gevestigd zijn in de EU. Het maakt daarbij niet uit of de aanbieder van de dienst zelf gevestigd is in de EU, maar de DSA bepaalt wel dat er een *aanzienlijke band met de EU* moet zijn. Een aanzienlijke band wordt verondersteld te bestaan als de aanbieder zelf ook gevestigd is in de EU. Als dat niet zo is, kan er gekeken worden naar andere feitelijke criteria, zoals het aantal gebruikers in de EU of het feit dat een aanbieder marketingactiviteiten richt op de EU. Dit is verder niet uitgewerkt, maar duidelijk is wel dat de DSA niet alleen van toepassing zal zijn op EU-aanbieders.

Gelaagde structuur van de DSA

De DSA introduceert zekere verplichtingen voor aanbieders, maar ook bepaalde rechten voor gebruikers. Het type dienst bepaalt welke verplichtingen e r gelden. De DSA hanteert hierbij een gelaagde structuur, waarbij laag 1 voor elke aanbieder geldt en laag 2 specifiek voor hosters. Laag 3 en laag 4 roepen respectievelijk voor online platforms en zeer grote online platforms nog enkele bijzondere verplichtingen in het leven. De DSA heeft hierbij een cumulatief karakter, zodat een zeer groot online platform zich moet houden aan alles wat uit laag 1 t/m 4 voortvloeit.

In de zin van de DSA is sprake van een *online platform* als het gaat om een hostingdienst waarbij de informatie op verzoek van de afnemer wordt verspreid bij een publiek van een mogelijk onbeperkt aantal ontvangers. Dat kan een social media platform, een doorsnee verkoopplatform, maar ook een appstore. Van een zeer groot online platform is sprake als het platform gemiddeld 45 miljoen actieve gebruikers per maand heeft in de EU. In dit artikel wordt verder niet op laag 4 ingegaan.

Hieronder worden enkele verplichtingen (en rechten) nader uitgewerkt. Voor ondernemingen met minder dan 50 werknemers of minder dan 10 miljoen euro omzet/balanstotaal per jaar zullen aardig wat regels niet van toepassing zijn. Dat is hieronder dan aangegeven met '*MKB uitgezonderd'.

Verplichtingen per niveau

Laag 1: regels die gelden voor iedere aanbieder

De regels uit laag 1 gelden voor iedere aanbieder, dus naast hosting-, ook voor caching- en mere conduit-diensten.

1.Inrichten contactpunt

Iedere aanbieder moet een contactpunt aanstellen waarmee, onder meer, toezichthoudende autoriteiten uit (andere) Europese lidstaten eenvoudig via elektronische weg contact kunnen leggen. Denk aan het online publiceren van een e-mailadres. Ook moet er worden vermeld in welke talen communicatie mogelijk is.

2. Aanstellen wettelijk vertegenwoordiger

Als de aanbieder niet gevestigd is in de EU, dan moet deze een wettelijke vertegenwoordiger aanstellen en de gegevens van deze vertegenwoordiger verstrekken aan een nationaal aangewezen coördinator. De gekozen vertegenwoordiger kan ook aansprakelijk gesteld worden voor niet-naleving van de DSA door de aanbieder.

3. Vereisten algemene voorwaarden

Algemene voorwaarden moeten eventuele beperkingen bevatten ten aanzien van informatie die via de dienst gedeeld mag worden. Ook moet er duidelijk worden vermeld welke procedures en regels er gelden ten aanzien van moderatie en de wijze waarop dit plaatsvindt (menselijk of via algoritmes).

*4. Transparantierapportage**

Minimaal 1 keer per jaar moet gepubliceerd worden over eventuele toegepaste moderatie, met details over het aantal ontvangen bevelen van nationale autoriteiten (denk aan informatievorderingen van de politie of een takedown vonnis), gecategoriseerd per soort illegale inhoud, en de gemiddelde tijd die nodig is deze bevelen op te volgen. Hosters moeten daarnaast ook jaarlijks publiceren over het aantal takedown-verzoeken dat ze hebben ontvangen, gecategoriseerd, met beschrijving van getroffen acties en de gemiddelde tijd die ze daarvoor nodig hadden. Als er op eigen initiatief gemodereerd is, dan moet dit ook worden benoemd, met informatie over het aantal keer, de aard en aanleiding.
*MKB uitgezonderd

Laag 2: aanvullende regels voor hosters

De regel uit laag 2 geldt naast laag 1 ook voor hosters.

5. Notice and takedown procedure
Hosters worden verplicht toegankelijke en gebruiksvriendelijke procedures te hanteren die het voor derden mogelijk maakt om uitsluitend via elektronische weg melding te maken van, naar hun mening, illegale inhoud.

De meldingsprocedure moet uitvragen naar: een verklaring waarom de melder van mening is dat er sprake is van illegale inhoud, de online locatie waar de inhoud zich bevindt (exacte URL), eventueel aangevuld met informatie om de locatie te achterhalen. Daarnaast moet de melder zijn naam en e-mailadres achterlaten en een verklaring afgeven dat hij te goeder trouw is bij de indiening.

Hosters worden ook verplicht direct na ontvangst van een melding, een ontvangstbevestiging te sturen per mail aan de melder. Hetzelfde moet een hoster doen zodra hij een besluit heeft genomen. Dat bericht moet dan ook vermelden of en welke beroepsmogelijkheden er zijn.

Als een hoster actie onderneemt, dan wordt hij verplicht de getroffen gebruiker te informeren en uiterlijk op het moment van actie. Die kennisgeving moet specifiek zijn gemotiveerd en daarmee informatie bevatten over: de reden tot, aard en gevolgen van het besluit, of er geautomatiseerde middelen zijn ingezet tot aan het besluit, de vermelding van de rechtsgrond wanneer het gaat om illegale inhoud en waarom de hoster denkt dat dit eronder valt. Als het gaat om overtreden van algemene voorwaarden moet dit ook worden geduid. Dit kennisgevingsbericht moet informeren over eventuele beroepsmogelijkheden.

Het is verder de bedoeling dat deze besluiten (geanonimiseerd) in een openbare databank van de Europese Commissie worden opgenomen en gepubliceerd.

Laag 3: aanvullende regels online platforms*

*MKB uitgezonderd

De regels uit laag 3 gelden in aanvulling op laag 1 en 2, specifiek voor online platforms.

6. Voorrang betrouwbare flaggers
Online platforms moeten meldingen van onafhankelijke en daartoe geautoriseerde en betrouwbare 'flaggers' met voorrang behandelen. Een flagger is een bedrijf gespecialiseerd in het opsporen van illegale inhoud en moet onafhankelijk zijn van enig online platform. Geautoriseerde flaggers worden door de Europese Commissie in een openbare database opgenomen.

7. Transparantie van onlinereclame voor gebruiker
Platforms moeten reclame duidelijker gaan duiden: dat het om reclame gaat, van welke persoon of onderneming het afkomstig en welke parameters relevant zijn voor het tonen van de reclame.

8. Kennisgeving bij strafbare feiten
Een online platform zal verplicht worden de lokale autoriteiten te informeren als hij op de hoogte is gesteld van informatie die aanleiding is voor een vermoeden van een ernstig strafbaar feit ten aanzien van bedreiging van iemands leven. Daartoe moet het platform alle beschikbare informatie verstrekken. Het is niet duidelijk of het echt een aangifteplicht betreft.

Aansprakelijkheid en filterplicht

De DSA brengt geen echte verschuiving in aansprakelijkheidsrecht met zich mee. Internettussenpersonen kunnen zich nog steeds beroepen op een vrijwaring onder meer als zij zich niet inhoudelijk met de illegale informatie hebben bemoeid, of als ze er geen kennis van hebben.

Verder bepaalt de DSA uitdrukkelijk dat een *algemene* monitoringsplicht voor illegale inhoud niet mag worden opgelegd. Wel laat dit ruimte voor het opleggen van een specifieke 'stay down'-verplichting; zorgen dat bepaalde illegale inhoud offline blijft.

Inwerkingtreding

De DSA is nog niet definitief, maar de verwachting is dat in 2022 een definitieve tekst wordt aangenomen. Vanwege de impact op voornamelijk grotere partijen, is het de bedoeling deze circa anderhalf jaar de tijd te geven voor te bereiden. De verwachting is dus dat de DSA niet eerder dan in 2024 effect zal hebben.

Uw organisatie goed beschermd met ICTRecht

ICTRecht 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. Wij zijn direct inzetbaar en altijd beschikbaar (24/7). ICTRecht staat voor flexibiliteit: u bepaalt wat wij voor u doen en onze abonnementen zijn per maand opzegbaar.

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

Koen van Jaarsveld
Legal consultant

Mark Zijlstra
Legal consultant

Legal tech

De Legal Tech Map 2022 The Netherlands

Op donderdag 10 februari 2022 werd tijdens de Legal Tech Heroes Round Table 2022 de Legal Tech Map 2022 gepresenteerd. Evenals de vorige versie in 2018 is de map ook dit keer weer ontwikkeld door Dutch Legal Tech in samenwerking met Advocatie en het legal innovation agency NOUN. De map geeft een overzicht van de bepalende Nederlandse legal tech bedrijven. In één oogopslag is te zien met welk onderwerp binnen legal tech deze bedrijven zich bezighouden.

De map

Op de map is een mooi landschap te zien van uitsluitend Nederlandse legal tech bedrijven. Het feit dat deze map er is laat zien dat de juridische sector structureel blijft innoveren en dat legal tech veel meer is dan een hype. Het is een permanente verandering in de juridische wereld die nog maar aan het begin staat. Het gegeven dat een groot aantal bedrijven die in 2018 op de kaart stond er in 2022 ook weer op staat laat zien dat de juridische softwaremarkt in Nederland steeds volwassener wordt. De pioniers van een paar jaar terug zijn inmiddels de gevestigde namen in Nederland geworden.
De producten zijn de afgelopen jaren ook sterk doorontwikkeld waardoor deze beter, betrouwbaarder en gebruiksvriendelijker zijn geworden.
Kaarten als deze zijn voor juristen altijd nuttig.
In één oogopslag is te zien welke tech bedrijven er in Nederland zijn en waar zij zich mee bezighouden.
Hoewel sommige partijen meerdere keren hadden kunnen voorkomen op de map, hebben de makers ervoor gekozen om iedere partij maar één keer terug te laten komen.

ICTRecht Legal Tech

Waar de Legal Tech map van 2018 vooral nog handvatten bood, is deze map ook een vorm van erkenning van de diensten die wij zelf aanbieden. ICTRecht Legal Tech staat namelijk zelf in de categorie legal tech consultancy. ICTRecht heeft in 2021 veel werk verricht om de bestaande diensten

aan te vullen met legal tech consultancy dienstverlening. Het legal tech team binnen ICTRecht ondersteunt uiteenlopende organisatie bij het optimaliseren van juridische (werk) processen. De dienstverlening van ICTRecht Legal Tech is drieledig en bestaat uit 1. Consultancy; 2. Legal tech implementaties en 3. Legal proces outsourcing.

ICTRecht Legal Tech werkt nauw samen met een groot aantal bedrijven die op de map staat en combineert juridische werkervaring met technische kennis over de producten. De komende periode zal ICTRecht Legal Tech blijven ontwikkelen voor wat betreft haar dienstverlening.

Juriblox

Waar ICTRecht Legal Tech als een nieuwkomer op de kaart is gekomen zijn Juriblox en Lynn Legal inmiddels gevestigde namen. Juriblox heeft zich, sinds het uitkomen van de vorige map, sterk doorontwikkeld en zal dat de komende periode ook blijven doen. Juriblox biedt het stabiele cloud platform voor diverse tech oplossingen.

Recente ontwikkelingen als no-code automation, realtime onderhandelen en contract lifecycle management laten zien dat dit platform terecht een gevestigde naam is op de Legal Tech Map 2022. ICTRecht Legal Tech en Juriblox werken regelmatig met elkaar samen om opdrachtgevers optimaal te bedienen.

Lynn Legal

In 2018 stond Lynn Legal nog op de map als NDA Lynn. Nu Lynn Legal op de map prijkt geeft dit aan dat ook deze lawyerbot zich blijft doorontwikkelen. Inmiddels beoordeelt Lynn niet alleen meer de geheimhoudingsovereenkomsten maar biedt het ook uitkomst voor verwerkersovereenkomsten en inkoopvoorwaarden. De hoge mate van standaardisering in deze specifieke juridische documenten maakt het voor Lynn mogelijk om deze op basis van kunstmatige intelligentie te reviewen en te annoteren. Ook Lynn Legal zal de komende jaren blijven ontwikkelen en in staat zijn om steeds meer juridische documenten te kunnen beoordelen en daar continu beter in te worden.

Internetrechtspraak

Opname persoonsgegevens in 'Treiteraanpak' is rechtmatig

(Rechtbank Amsterdam 15 november 2021)

De gemeente Amsterdam is in 2013 gestart met de Treiteraanpak om intimidatie in de woon- en werkomgeving tegen te gaan. Hierin werkt de gemeente samen met onder andere de politie en woningbouwcorporaties om herhaaldelijke intimidatie tegen specifieke personen zo snel mogelijk te beëindigen. In 2015 is eiseres als dader in deze Treiteraanpak opgenomen. Zij werd door de burgemeester middels een notificatie van de opname op de hoogte gesteld, maar vindt deze opname onterecht. Volgens haar is de verwerking onrechtmatig en daarom verzoekt ze de verwerking van haar gegevens te staken en de opgebouwde dossiers aan haar te overhandigen. Dit verzoek is door de burgemeester afgewezen.
De rechtbank oordeelde dat de gegevensverwerking zowel noodzakelijk als rechtmatig was. De verwerking is noodzakelijk voor het handhaven van de openbare orde, waarmee de burgemeester is belast.
Verder is de verwerking niet onverenigbaar met de oorspronkelijke verwerking van de bewuste gegevens. Om de privacy van betrokkenen bij de Treiteraanpak te waarborgen is met de betrokken instanties een convenant gesloten. Hierin zijn vijf criteria opgenomen waaraan een persoon moet voldoen om in de aanpak te worden opgenomen. Eiseres voldeed ook aan al deze criteria.

https://bit.ly/3Bqz0ku

BKR-registratie door kredietaanbieder DEFAM hoeft niet verwijderd te worden

(Rechtbank Den Haag 18 november 2021)

Verzoeker heeft in 2014 een lening afgesloten bij kredietaanbieder DEFAM, die na een lange periode van problematisch betaalgedrag in 2019 is afbetaald. De betaalachterstanden van verzoeker zijn destijds geregistreerd bij het BKR en deze registratie wordt in 2024 verwijderd. De BKR-registratie zorgt er volgens verzoeker voor dat hij geen huurwoning kan vinden, terwijl hij hier dringend naar op zoek is. Daarom beroept hij zich op de AVG en vraagt hij DEFAM om de verwerking van zijn persoonsgegevens te staken en de registratie te verwijderen. DEFAM heeft dit verzoek afgewezen.
De rechtbank oordeelde dat het belang van verzoeker bij vroegtijdige verwijdering van de gegevens niet opweegt tegen dat van DEFAM. De doelen van BKR-registraties zijn namelijk het behoeden van consumenten voor overcreditering en het beperken van de financiële risico's van kredietverleners. Hierbij merkte de rechtbank wel op dat als de persoonlijke omstandigheden van verzoeker wijzigen, DEFAM een nieuwe belangenafweging moet maken wanneer hij opnieuw om verwijdering vraagt.

https://bit.ly/33t9aQs

Microsoft moet erfgenamen toegang tot accounts verlenen

(Rechtbank Amsterdam 1 december 2021)

De erfgenamen van een overleden man hebben Microsoft verzocht hen toegang te verlenen tot zijn Hotmail-account. Zonder vonnis wilde Microsoft echter niet aan dit verzoek voldoen. Microsoft stelde dat het Hotmail-account en de inhoud hiervan niet overgaan op erfgenamen en dat hij rekening moest houden met privacybelangen van derden.
De rechtbank oordeelde dat niet uit de wet of de gebruikersovereenkomst van Microsoft blijkt dat het Hotmail-account niet over mag gaan op de erfgenamen. Verder deelde zij de mening van de Duitse rechter met betrekking tot belangen van derden. Bij leven van de accounthouder moeten 'vrienden' op een sociaal netwerk rekening houden met derden die, door misbruik of toestemming, toegang kunnen krijgen tot het account; bij zijn overlijden met de

vererving van de overeenkomst. Microsoft moest de erfgenamen toegang geven tot het account. Zie de noot op pagina 32.

https://bit.ly/3pfDdD1

Privacy First geen spoedeisend belang bij buitenwerkingstelling Wet ANPR

(Rechtbank Den Haag 1 december 2021)

Op basis van de Wet ANPR kunnen opsporingsambtenaren met ANPR-camera's kentekengegevens van passerende voertuigen vastleggen voor een periode van 28 dagen. Stichting Privacy First had een kort geding aangespannen omdat zij van mening is dat er door deze wet op dagelijkse basis sprake is van een stelselmatige ernstige inbreuk op de grondrechten van alle burgers in Nederland. Zij vorderde dat de Wet ANPR buiten werking moest worden gesteld en dat, op grond van deze wet, kentekens niet mogen worden verzameld of geraadpleegd totdat het totale systeem is onderworpen aan onafhankelijk rechterlijk toezicht.

De voorzieningenrechter oordeelde dat er geen sprake was van een spoedeisend belang en wees daarom het gevorderde af. De Wet ANPR is namelijk op 1 januari 2019 in werking getreden, dus deed de gestelde inbreuk zich al ruim tweeëneenhalf jaar voor. In deze periode heeft Privacy First blijkbaar niet eerder aanleiding gezien om zich op deze inbreuk te beroepen. De rechter neemt geen spoedeisend belang aan vanwege dit tijdsverloop en het feit dat Privacy First niet op andere manieren een spoedeisend belang heeft aangetoond.

https://bit.ly/356JcCU

Koop van paard via marktplaats.nl kan ontbonden worden

(Rechtbank Zeeland-West-Brabant 8 december 2021)

Eiser heeft gereageerd op een advertentie op marktplaats.nl waarin door gedaagde, een paardenhandelaar, een paard te koop werd aangeboden. Hierop is hij langsgegaan bij gedaagde om het paard te komen bekijken. Telefonisch en per WhatsApp is onderhandeld over de prijs waarna, met een aanbetaling van € 3.000, de koop gesloten werd. Vijf dagen na het sluiten van de overeenkomst ontbond eiser de aankoop echter. Gedaagde wilde de aanbetaling niet terugbetalen en stelt dat het herroepingsrecht niet van toepassing is omdat het hier geen koop op afstand betreft. Daarnaast zijn volgens haar de regels voor koop op afstand niet werkbaar bij de verkoop van paarden.

De rechtbank oordeelde dat het hier wel koop op afstand betrof omdat het onderhandelen, de deal sluiten en het betalen allemaal per telefoon zijn gegaan. Ook oordeelde de rechtbank dat er sprake was van een georganiseerd systeem voor verkoop op afstand omdat gedaagde regelmatig op deze wijze paarden verkoopt via haar eigen website en marktplaats.nl. Verder worden dieren niet wettelijk uitgezonderd van het recht op ontbinding. De eiser mocht de koop daarom ontbinden.

https://bit.ly/351fSNM

Laptop kan kansspelautomaat zijn

(Rechtbank Rotterdam 10 december 2021)

Verdachte exploiteert een café waar verbalisanten een opengeklapte en actieve laptop aantroffen op een tafel. Op de laptop was de website betsball.com geopend waarop verscheidene voetbalwedstrijden met bijbehorende quoteringen werden genoemd. Achter de bar werd een printer gevonden met een lange bundel wedtickets, die overeenstemden met wedtickets die in grote hoeveelheden op andere locaties in het café lagen. Omdat de caféhouder geen vergunning had voor het aanwezig hebben van een speelautomaat is hij vervolgd voor het overtreden van de Wet op de kansspelen. De caféhouder stelde echter dat de laptop niet is aan te merken als een kansspelautomaat en dat er daarom geen sprake was van een overtreding.

De rechtbank overwoog dat de bestemming die aan een apparaat wordt gegeven doorslaggevend is. Uit verklaringen van de caféhouder blijkt dat de laptop van hem is, maar hoofdzakelijk door klanten werd gebruikt om te gokken op voetbalwedstrijden. De wedtickets printte de caféhouder daarna voor de gokkende klanten uit. Gecombineerd met de waarnemingen van de verbalisanten leidt dit ertoe dat

deze laptop kon worden aangemerkt als kansspelautomaat. De caféhouder is veroordeeld tot een maand voorwaardelijke gevangenisstraf.

https://bit.ly/3HXpAQ6

Dansgezelschap mag zelftestweigeraar van werk weren

(Rechtbank Amsterdam 14 december 2021)

Eiser is werkzaam als danser en bij repetities en uitvoeringen komt hij in nauw contact met mededansers. Omdat hij niet is ingeënt tegen het coronavirus vroeg zijn werkgever hem wekelijks een zelftest te doen en de uitslag daarvan met haar te delen. Eiser weigert dit onder andere omdat hij dit beschouwt als inbreuk op zijn grondrechten op privacy en lichamelijke integriteit. Hij is daarom door zijn werkgever verzocht niet meer op werk te verschijnen. Eiser wilde dat werkgever hem weer toe zou laten op zijn werk. De rechtbank wees de vordering af en overwoog dat de maatregel, naast de normale bij gedaagde geldende veiligheidsregels, als (minimaal) noodzakelijk kan worden aangemerkt om een veilige werkomgeving te scheppen voor de dansers gedurende de coronapandemie. Een minder verstrekkend middel om hetzelfde doel te bereiken is niet genoemd en ook niet goed voorstelbaar. Het doel van gedaagde om door de maatregel een veilige werkomgeving te scheppen woog in dit geval zwaarder dan het bezwaar van de eiser tegen het testen en het delen ervan. Verder is de AVG niet van toepassing op het laten zien van de testuitslag, omdat werkgever deze niet opslaat in een bestand ter verwerking.

https://bit.ly/3HVlSqd

Coolblue mag foto's ex-werknemer blijven gebruiken

(Rechtbank Rotterdam 17 december 2021)

Eiser was drie jaar lang bij Coolblue werkzaam, maar is op staande voet ontslagen. Tijdens zijn dienstverband heeft Coolblue, met zijn toestemming, foto's gemaakt die zijn afgebeeld op bestelbussen van het bedrijf. Daarnaast komt eiser voor in een promotievideo die op YouTube is geplaatst. Na zijn ontslag stelt eiser dat Coolblue inbreuk maakt op zijn portretrechten en de AVG. Hij vordert schadevergoeding en dat Coolblue wordt bevolen de inbreuk op zijn portretrechten te staken en gestaakt te houden.
De rechtbank heeft de vordering afgewezen. Hierbij speelde onder andere een rol dat in de arbeidsovereenkomst die door eiser was ondertekend specifiek was bepaald dat Coolblue foto's van medewerkers mag gebruiken, ook na het dienstverband. Verder heeft eiser medewerking verleend aan het maken van de bewuste foto's en opnamen en is hem op voorhand het doel hiervan duidelijk gemaakt. Nu Coolblue al had toegezegd de foto's niet verder te gebruiken, de bestelbussen uit te faseren en dat de kosten van het direct vervangen van de busjes heel hoog zouden zijn, weegt het belang van eiser niet op tegen dat van Coolblue.

https://bit.ly/3513tte

KvK heeft geen databankenrecht op het handelsregister

(Rechtbank Midden-Nederland 22 december 2021)

Nieuwe gebruiksvoorwaarden voor het handelsregister bepaalden dat voor sommige soorten gebruik databankrechtelijke toestemming van de KVK is vereist. Hiermee wil de KVK zogeheten 'schaduwregistraties' aanpakken die worden aangelegd met kopieën van gegevens uit het handelsregister. Commerciële marktpartijen leveren hiermee tegen een gereduceerd tarief soortgelijke informatiediensten als de KVK. De KVK stelt dat schaduwregistraties een negatieve impact hebben op de rechtszekerheid, privacy van personen en zijn inkomsten. Belangenvereniging VVZBI meent dat de KVK geen databankenrecht heeft op het handelsregister. Zij vordert dit voor recht te verklaren en de KVK te verbieden zich hierop te beroepen.
De rechtbank oordeelde dat het handelsregister als databank kwalificeert. Hiervan kan de KVK echter niet als producent worden aangemerkt. De KVK draagt namelijk niet het financiële risico van de investeringen; kosten die hij niet uit zijn inkomsten kan voldoen, worden gedekt door de Rijksoverheid. Verder is met het databankenrecht beoogd investe-

ringen te stimuleren. De KVK behoeft deze stimulans niet, want die heeft hij al in de vorm van een wettelijke taak. De vordering van de VVZBI is toegewezen.

https://bit.ly/3h7r3Yp

Collectieve actie tegen Oracle en Salesforce strandt bij "like"-knop

(Rechtbank Amsterdam 29 december 2021)

The Privacy Collective (TPC), een organisatie die opkomt voor de privacyrechten van internetgebruikers, heeft met een beroep op de Wet afwikkeling Massaschade in collectieve actie (WAMCA) een zaak aangespannen tegen softwarebedrijven Oracle en Salesforce. Zij stelt dat deze bedrijven de privacy van tien miljoen Nederlandse internetgebruikers heeft geschonden door persoonsgegevens in gedetailleerde profielen te verwerken en te verkopen voor advertentiedoeleinden. TPC eist een schadevergoeding van € 5 miljard.
De rechtbank heeft TPC niet-ontvankelijk verklaard. Voor een beroep op de WAMCA moet de organisatie die de collectieve actie op zich neemt voldoende representatief zijn. Om dit aan te tonen heeft TPC onder andere een steunknop op haar site geplaatst waarop websitebezoekers konden klikken om hun steun aan de vordering te laten blijken. Deze was door 75.000 mensen aangeklikt. De tekst bij de knop was echter summier, waardoor volgens de rechter niet bleek waarvoor exact steun kenbaar werd gemaakt. Daarnaast waren van de 'likers' geen contactgegevens opgeslagen waardoor TPC ze niet kon betrekken bij de besluitvorming, wat ook verplicht is.

https://bit.ly/3GObyig

Reclame voor Ariel All-in-1 pods mag niet meer worden uitgezonden

(Rechtbank Rotterdam 6 januari 2022)

P&G, eigenaar van het wasmiddelmerk Ariel, liet sinds 2021 reclames uitzenden waarin Ariel impliciet met het wasmiddelmerk Robijn van Unilever wordt vergeleken. In de reclame werd geïmpliceerd dat je twee doses Robijn nodig zou hebben om de vlekverwijderingsprestaties van een Ariel All-in-1 pod te evenaren. Unilever vond deze vergelijking misleidend en spande daarom een kort geding aan.
De rechtbank oordeelde dat er inderdaad sprake was van een misleidende vergelijkende reclame, omdat de onjuiste indruk wordt gewekt dat je voor iedere wasbeurt met Robijn twee doses nodig hebt. Deze vergelijking is ook in strijd met de richtlijnen die de wasmiddelproducenten normaliter volgen met betrekking tot vergelijkende testen. Daarom is er een uitzendverbod opgelegd voor de betreffende reclame.

https://bit.ly/3sQc2iQ

Belastingadviseur moet inzage geven in agenda met daarin ook privéafspraken

(Gerechtshof 's-Hertogenbosch 12 januari 2022)

Naar aanleiding van een boekenonderzoek heeft een belastinginspecteur inzage gevraagd in de gemengde agenda's van de onderzochte belastingadviseur. Hierin noteerde de adviseur, naast privéafspraken, ook (betaalde) afspraken met particulieren. Omdat de adviseur de agenda's niet wilde overleggen, heeft de belastinginspecteur een informatiebeschikking gegeven, waartegen door de adviseur bezwaar is ingediend. Na ongegrondverklaring van dit bezwaar is belanghebbende een juridische procedure gestart. Hij beroept zich hierbij onder andere op zijn recht op privacy.
Het gerechtshof heeft geoordeeld dat de belastinginspecteur de beschikking terecht had gegeven. Het recht op privéleven dat in artikel 8 EVRM is neergelegd maakt dit oordeel niet anders. De bevoegdheid van de belastinginspecteur om informatiebeschikkingen te geven is namelijk vastgelegd in de wet, en deze is noodzakelijk in het belang van het economisch welzijn van ons land.

https://bit.ly/3LGC5So

Man veroordeelt tot dertig maanden cel wegens grootschalige phishing

(Rechtbank Overijssel 18 januari 2022)

De rechtbank Overijssel heeft een 21-jarige man schuldig bevonden aan het medeplegen van computervredebreuk, oplichting en diefstal door middel van een valse sleutel. Samen met anderen heeft hij in een periode van acht maanden tijd een grote groep personen opgelicht door fraudeleuze links te sturen aan slachtoffers die producten op marktplaats.nl verkochten. De slachtoffers dachten dat zij hiermee de verzendkosten konden betalen, maar in werkelijkheid kregen de man en zijn medeplegers de bankgegevens van deze personen in handen.
Volgens de rechtbank heeft de man op grootschalige wijze slachtoffers financieel benadeeld en hun vertrouwen in de handel van digitale goederen beschadigd. Zijn handelen vormde een inbreuk op het privéleven van de slachtoffers en heeft geleid tot grote gevoelens van onveiligheid, wat de rechtbank de man zwaar aanrekent. De eis van de officier van justitie werd passend en geboden geacht: een gevangenisstraf van dertig maanden waarvan twaalf voorwaardelijk met een proeftijd van drie jaar.

https://bit.ly/3BsVDol

Ziggo hoeft geen waarschuwingsbrieven namens BREIN te versturen

(Rechtbank Midden-Nederland 2 februari 2022)

Stichting Brein, die zich bezighoudt met de collectieve bestrijding van auteursrechtinbreuken, is in 2020 een waarschuwingscampagne gestart voor 'Frequente en Langdurige Uploaders' (FLU) die illegaal aanbod ter beschikking stellen op BitTorrent. Deze campagne is erop gericht waarschuwingsbrieven te sturen aan houders van IP-adressen die door Brein zijn geïdentificeerd als FLU. Omdat Brein echter alleen beschikking heeft over de IP-adressen en niet over de bijbehorende NAW-gegevens heeft zij internetserviceprovider Ziggo gevraagd waarschuwingsbrieven door te sturen aan de FLU wiens IP-adressen hij beheert. Omdat Ziggo niet vrijwillig wilde meewerken heeft Brein een kort geding aangespannen. Hierin is door de rechter bepaald dat Ziggo niets hoeft door te sturen. De voornaamste reden hiervoor was dat tegen de houders van de bewuste IP-adressen een gegronde verdenking bestaat dat zij inbreuk hebben gepleegd op het auteursrecht. Dit maakt de IP-adressen tot strafrechtelijke gegevens en Ziggo heeft voor het verwerken van dergelijke gegevens geen grondslag. De rechter benoemde wel dat Ziggo onrechtmatig zou handelen door de brieven niet te sturen wanneer hij een grondslag zou hebben in de vorm van een vergunning van de AP.

https://bit.ly/3LDKgPj

Sparren over privacyvraagstukken?
Bel onze gratis FG-hotline

Bent u een FG, DPO of privacy professional en krijgt u te maken met vragen waar u zelf niet direct een eenduidig antwoord op kunt geven? Of krijgt u te maken met weerstand? Voor deze momenten bieden de privacy juristen van ICTRecht gratis de helpende hand middels de FG-hotline. Tijdens het telefoongesprek proberen we direct antwoord te geven op uw vragen.

De hotline is bereikbaar op woensdag tussen 14:00 en 15:00 uur.

Lees meer op: www.ictrecht.nl/fg-hotline
Of bel gratis naar: 020 244 3122

Arnoud Engelfriet
Directeur / Opleidingsdirecteur

Cloud Privacy

Toegang mailbox door nabestaanden

Noot bij Rechtbank Amsterdam
1 december 2021

De juridische status van mailboxen en online accounts wordt steeds vaker onderzocht in de rechtspraak. Dit blijft een heikele kwestie, omdat er geen juridisch recht direct van toepassing lijkt. We hebben niet te maken met eigendom of zelfs maar gehuurde zaken, of een mailbox een vermogensrecht is lijkt ook niet waarschijnlijk. Wat is het dan wel? En waarom zou een nabestaande er toegang toe moeten krijgen? Een recent Amsterdams vonnis[1] biedt mogelijk soelaas.

1. https://bit.ly/3pfDdD1

Online account opeisen, een lastige zaak

De feiten van de zaak zijn relatief simpel. Een man overleed in juli 2021, en had daarvoor een Hotmail-account (e-mail) en een OneDrive-account (cloud-opslag) bij Microsoft. De ouders en zussen wilden daar toegang toe krijgen. Redenen worden niet genoemd, maar voor de hand ligt het kunnen opheffen van online diensten. Hiervoor is immers vaak een wachtwoordreset nodig, en daarvoor toegang tot de mailbox. Maar ook simpelweg de "schoenendoos" met oude correspondentie en bestanden van de overledene willen hebben, is natuurlijk een prima motivatie.

Een schoenendoos opeisen is niet zo moeilijk. Het eigendomsrecht daarop kan eenvoudig worden uitgeoefend, zodra vaststaat wie de erfgenamen zijn. Maar een online account 'is' niets, geen zaak in ieder geval en waarschijnlijk ook geen vermogensrecht. Dus revindicatie of een andere vorm van toegang eisen is niet mogelijk op die grond.

Wat is het dan wel? In ieder geval een overeenkomst, het gaat immers om dienstverlening (art. 7:401 BW). In beginsel is een overeenkomst persoonlijk, en in de toepasselijke voorwaarden is overdracht expliciet uitgesloten. Maar er is een uitweg in het Nederlands recht, namelijk de saisine-regeling van art. 4:182 BW: "Met het overlijden van de erflater volgen zijn erfgenamen van rechtswege op in zijn voor overgang vatbare rechten en in zijn bezit en houderschap."

Samengevat komt het erop neer dat de ouders en zussen als erfgenamen aan te merken zijn als rechtsopvolgers onder algemene titel van de accounts van hun zoon en broer en de inhoud ervan en dus ook de nieuwe wederpartij van Microsoft met betrekking tot de desbetreffende overeenkomsten. Een overdracht is niet nodig, immers van rechtswege is de overeenkomst overgegaan. De erfgenamen zetten de overeenkomst voort alsof zij de overledene waren.

De (te verwachten) reactie van Microsoft

Microsoft reageert geheel zoals ik zou verwachten, namelijk naar Amerikaans recht met de dooddoener (sorry) dat men maar met een gerechtelijk bevel moet komen. In de VS laat je namelijk de rechter in vrijwel ieder geval beslissen wat je moet doen, ongeacht de juridische kwestie. In Nederland doen we dat anders. Daar vinden we het logisch dat mensen zélf nazoeken hoe de wet zit en dat dan in alle redelijkheid gaan toepassen. Niet voor ieder gevalletje eerst de rechter bellen.

Natuurlijk had Microsoft ook wel juridische argumenten. Allereerst dat saisine niet zou gelden, voor dit soort dienstverleningsovereenkomst. Een op zich mogelijk argument, omdat voor “hoogstpersoonlijke” overeenkomsten zoals huur of arbeid het voortzetten door erfgenamen uitgesloten is. Maar de rechtbank veegt dit van tafel, een online dienst is daarmee niet op één lijn te stellen.

Een tweede argument van Microsoft was de privacy en de omgang met persoonsgegevens van de correspondenten van deze meneer wiens persoonsgegevens dus in de mailbox zitten. De nabestaanden zouden daar dan zomaar toegang toe krijgen, en dat zou onder de AVG niet toegestaan zijn. Ook dat gaat niet op, aldus de rechtbank. Weliswaar waren deze mensen niet de beoogde ontvanger van die mails, maar zij hebben naast de rechten ook alle plichten uit de dienstvoorwaarden overgenomen. Deze gelden natuurlijk net zo goed voor de erfgenamen, inclusief dus de plicht om de privacy van anderen niet zomaar te schenden.

Als derde argument had Microsoft nog aangedragen dat er rare dingen aan de hand waren met het account. Dat zou een extra reden zijn om het account op slot te mogen houden. Het vonnis lezend lijkt het meest waarschijnlijk dat de nabestaanden hadden geprobeerd in te loggen vanaf de laptop van de overledene (met bijvoorbeeld een bewaard wachtwoord) maar dat het wachtwoord toch niet juist was, of een sms-code nodig was. In ieder geval, dat is geen reden om een saisine te weigeren.

Rechter oordeelt: toegang moet verleent worden

De conclusie van de rechter is dan ook rechttoe rechtaan: Microsoft moet toegang verlenen en wel zo snel mogelijk. Niet moeilijk doen, deze mensen zijn juridisch gezien gewoon de eigenaren na het overlijden van de eigenlijke eigenaar. Microsoft krijgt twintig dagen en verbeurt daarna dwangsommen van tienduizend euro per dag. Dat is een fors bedrag, wat voor mij dus de indicatie is dat de rechtbank het handelen van Microsoft als onnodig moeilijk doen zag.

Een bezwaar dat van diverse kanten is aangedragen, is dat het hiermee voor nabestaanden mogelijk is om toegang te krijgen tot een mailbox die u toch bij leven als privé mocht beschouwen. Deze zouden daarbij dan bijvoorbeeld de liefdesbrieven naar uw partner (of uw minnaar m/v/x) kunnen zien, of discussie met uw therapeut of wat maar zeer privé is en u niet wil dat uw erfgenamen zien. Daar valt wat voor te zeggen, maar dat is mijns inziens niet anders dan bij die spreekwoordelijke schoenendoos met liefdesbrieven, pikante foto’s of wat dan ook die men op zolder of de dossierkast op het werk kan aantreffen.

Ik zie de bijbehorende risico’s dan ook hetzelfde: soms zijn er dingen die u als nabestaande liever niet had geweten, of niet had moeten weten, maar een dienstverlener als Microsoft is niet de partij die daar het oordeel in moet vellen. Wie bang is voor wat hij kan aantreffen, kan maar beter niet kijken.

En wie bezorgd is over wat de nabestaanden kunnen vinden, kan overwegen een zogeheten social media testament of digitaal testament op te stellen. Dit is een vastlegging bij de notaris van alle online accounts, met wachtwoorden indien mogelijk, inclusief aanduiding wat daarmee moet gebeuren. Denk aan verwijderen zonder in te zien, omzetten naar gedenkpagina, archiveren en gebruiken voor afhandeling testament en ga zo maar door. Deze instructies kan de notaris dan bij het voorlezen van het testament meegeven.

Natuurlijk kan het ook zonder notaris, alleen is er dan het nadeel dat de persoon met de codes niet tijdig hoort van het overlijden. Of dat die ze voor eigen doeleinden gebruikt. Maar dat is een kwestie van vertrouwen, niet iets waar het recht voor bedoeld is.

Privacy

Einde Google Analytics in zicht?

Van onze blog
14 januari 2022

Vele websites zetten Google Analytics in om te kijken hoe de website wordt gebruikt en hoe de ervaring van de bezoeker kan worden verbeterd. Dit gebeurt aan de hand van cookies. Het gebruik van de meest populaire analytics tool lijkt echter op losse schroeven te staan. Afgelopen week oordeelde[1] de Oostenrijkse privacytoezichthouder (Datenschutzbehörde of DSB) namelijk dat het gebruik van Google Analytics in strijd is met de Algemene verordening gegevensbescherming (AVG). En nu?

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

Oordeel van de DSB

Sinds de Schrems II-uitspraak[2] in de zomer van 2020 is het juridisch gezien lastig rond te krijgen om vanuit Europa persoonsgegevens in de Verenigde Staten (VS) te verwerken. Lang verhaal kort: het Privacy Shield is ongeldig verklaard en de Standard Contractual Clauses (SCC's) zijn niet meer voldoende zonder risicoanalyse[3] en eventuele aanvullende technische, organisatorische en contractuele maatregelen. Of organisaties hier daadwerkelijk gehoor aan geven, is maar de vraag. Degene achter deze uitspraak, Max Schrems, heeft via zijn organisatie NOYB daarom 101 klachten bij verschillende Europese privacytoezichthouders ingediend over mogelijke schendingen van de uitspraak.

2. https://bit.ly/3MjbgnH
3. https://bit.ly/3Cb2zqM

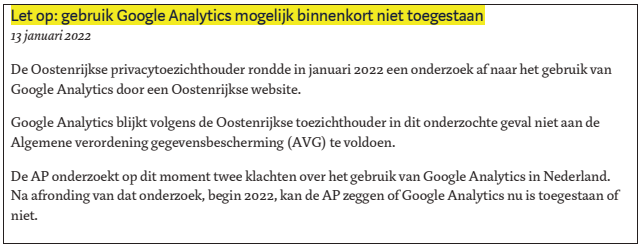
De eerste beslissing is nu genomen. Google Analytics geeft standaard gegevens, waaronder persoonsgegevens, door naar Google in de VS. Hoewel Google stelt technische en organisatorische maatregelen te nemen om persoonsgegevens te beschermen tegen de Amerikaanse overheid, ziet de DSB niet in hoe deze moeten beschermen tegen surveillance. Duidelijke taal. Maar wat betekent dit nou voor Nederland?

Reactie Autoriteit Persoonsgegevens

In Nederland zit het net iets anders in elkaar. Tenminste, op het eerste gezicht. De Autoriteit Persoonsgegevens (AP) heeft namelijk een handleiding gepubliceerd over hoe Google Analytics privacyvriendelijk gebruikt kan worden. U zou daarom zeggen: probleem opgelost, wij kunnen Google Analytics gewoon blijven gebruiken. Helaas niet. Gisteren werd er al een extra alinea aan de handleiding toegevoegd (zie afbeelding 1).

Let op: de handleiding heeft een nieuwe vindplaats[4]. De AP is dus aan het onderzoeken of Nederlandse websites Google Analytics mogen blijven gebruiken. Maar eerlijk is eerlijk: het ziet er niet rooskleurig uit.

Handleiding privacyvriendelijk instellen van Google Analytics



Let op: gebruik Google Analytics mogelijk binnenkort niet toegestaan

13 januari 2022

De Oostenrijkse privacytoezichthouder rondde in januari 2022 een onderzoek af naar het gebruik van Google Analytics door een Oostenrijkse website.

Google Analytics blijkt volgens de Oostenrijkse toezichthouder in dit onderzochte geval niet aan de Algemene verordening gegevensbescherming (AVG) te voldoen.

De AP onderzoekt op dit moment twee klachten over het gebruik van Google Analytics in Nederland. Na afronding van dat onderzoek, begin 2022, kan de AP zeggen of Google Analytics nu is toegestaan of niet.

Afbeelding 1: Uitsnede pagina 1 handleiding

De European Data Protection Board (EDPB), het Europese verbond van privacytoezichthouders, is de genoemde 101 klachten ook via een gezamenlijke taskforce aan het behandelen.

4. https://bit.ly/3txt6dO

Wat kan nog wel?

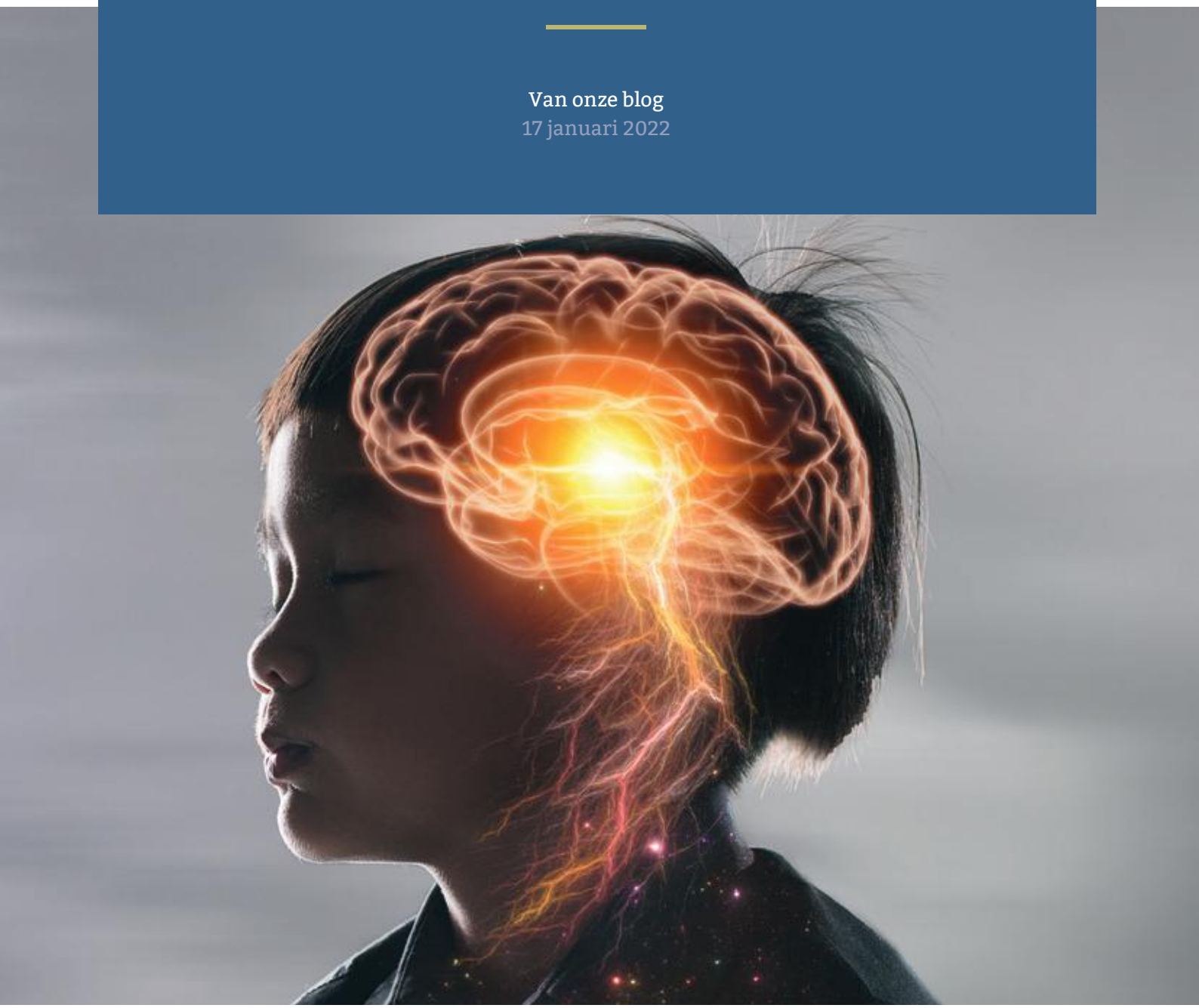
Dat gezegd hebbende, Google Analytics is niet de enige manier om te kijken hoe uw website wordt gebruikt. Er zijn genoeg Europese alternatieven. De Franse toezichthouder, de Commission nationale de l'informatique et des libertés (CNIL), heeft een voorbeeldfunctie ingenomen voor andere privacytoezichthouders. Zo heeft de CNIL een lijstje gepubliceerd met privacyvriendelijke analytics tools. Hiervoor hoeft én geen toestemming te worden gevraagd (want de Cookiewet geldt nog steeds), én er zijn (vooralsnog) geen Schrems II-problemen. Zweert u echter bij Google Analytics, dan is het nog even afwachten of dit zonder problemen blijft. To be continued...

Auteur
Laura Monhemius
Juridisch adviseur

Overheid Artificial Intelligence

Leidraad kwaliteit AI in de zorg

Van onze blog
17 januari 2022



Een aantal weken geleden is in opdracht van het ministerie van Volksgezondheid, Wetenschap en Sport een leidraad gepubliceerd: 'Leidraad kwaliteit AI in de zorg'[1]. Deze leidraad is ontwikkeld door en voor het veld met het oog op voorspellende AI-gestuurde algoritmen. Voor het veld is het een goede stap om met meer vertrouwen AI toe te passen in de dagelijkse zorgpraktijk.

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

AIPA en medisch hulpmiddel

De leidraad geeft de toepassing als volgt aan: 'het ontwikkelen, toetsen en toepassen van een Artificial Intelligence Prediction Algorithm (AIPA) dat deel uitmaakt van een hulpmiddel die bedoeld is voor gebruik in de gezondheidszorg'. Maar wat zijn AIPA? De leidraad geeft een definitie:
'Algoritmen die leiden tot een voorspelling van een gezondheidsuitkomst bij individuele personen. Dit betreft tenminste het voorspellen van de kans op, of classificatie van, het hebben (diagnostisch) of het in de tijd optreden (prognostisch) van gewenste of ongewenste gezondheidsuitkomsten.'

Een voorbeeld hiervan is software die gemaakte longfoto's beoordeeld. In zo een beoordeling wordt aangegeven of er sprake is van een afwijking. Daarnaast wordt de afwijking geclassificeerd, afhankelijk van de ernst van de afwijking.

Het doel van de leidraad

In de gezondheidszorg zijn er al best veel wetten en normen van toepassing. Denk bijvoorbeeld aan de Medical Device Regulation (MDR), de Algemene verordening gegevensbescherming (AVG) of de verschillende ISO-NEN-normen. Waarom is deze leidraad dan nog nodig? In de leidraad wordt de indruk gewekt dat het veld behoefte had aan aanvulling. Hier is zeker een voorstelling bij te maken; een applicatie gebruiken zonder volledig te begrijpen hoe het werkt geeft niet voldoende vertrouwen om het te gaan gebruiken. Vooral niet in de zorg waar levens op het spel staan. Hierom schetst de leidraad binnen het toepassingsbereik (het AIPA) de wettelijke kaders en werkt de toepasselijke wet- en regelgeving nader uit. Dit met als doel dat erop vertrouwd kan worden dat het AIPA kwalitatief hoogwaardig en veilig is. Let wel, de leidraad is geen juridisch bindend document.

De verschillende fasen

In de leidraad worden zes fasen benoemd voor de ontwikkeling, validatie en implementatie van AI-voorspelmodellen. Fase 1 tot en met 3 gaan voornamelijk over het voorbereidende werk voordat de AI-voorspelmodellen in de praktijk worden gebruikt. Fase 4 tot en met 6 komen steeds dichter bij de medische praktijk. De leidraad voorziet van een beschrijving hoe de AIPA veilig en effectief in de medische praktijk gebruikt kunnen worden.

Goede aanvulling?

De leidraad geeft duidelijk weer wat van belang is in de verschillende fasen en benoemd ook vereisten uit relevante wet- en regelgeving. Er wordt aangegeven wat een verplichting is door een vetgedrukte 'moet' en wat geen verplichting is maar wel 'sterk aanbevolen' wordt. Het is wel van belang dat ook de sterk aanbevolen aspecten breed gedragen worden door het veld. Is de leidraad toch wat overweldigend, dan kan er gebruik worden gemaakt van een online leeromgeving[2] die is opgezet vanwege de leidraad.

2. https://www.leidraad-ai.nl/

Zoals eerder aangegeven is de leidraad geen juridisch bindend document. Het is geen uitputtende opsomming van toepasselijke wet- en regelgeving. Dit hoeft niet gelijk negatief te zijn, maar is wel van belang om te realiseren wanneer de leidraad gebruikt wordt door ontwikkelaars of gebruikers. De ontwikkelaar of gebruiker moet zeker proactief blijven en kan niet volledig leunen op de leidraad. De leidraad geeft wel een goede eerste voorzet en handvatten om wegwijs te worden in het juridische woud dat intimiderend kan zijn voor zowel ontwikkelaars als gebruikers. Daarnaast kan het zorgverleners helpen om de kwaliteit van het AIPA te beoordelen en het vertrouwen te vergroten.

Auteur
Pelçim Kaygusuz
Juridisch adviseur

ICTRecht Academy

Trainingsoverzicht
april - juni 2022

Dinsdag 19 april 2022
AVG op hoofdlijnen
Heeft u in uw werk (als niet-jurist) te maken met persoonsgegevens en wilt u meer over de AVG weten? Volg deze training en ontvang praktische handvatten.

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

Dinsdag 26 april 2022
FG zorg en informatiebeveiliging
Belangrijk is dat de FG in de zorg over basiskennis beschikt op het gebied van informatiebeveiliging. Tijdens deze training komt o.a. een hacker aan het woord.

Deze training vindt plaats in Utrecht. Lees meer!
https://bit.ly/3rR7BVU

Donderdag 28 april 2022
Themadag inventariseren en registreren
Leer in deze training wat de belangrijkste onderdelen zijn van een privacyinventarisatie en plan van aanpak. En wat is het doel van het verwerkingsregister?

Deze training vindt plaats in Amsterdam. Lees meer!
https://bit.ly/3HTHfqM

Donderdag 12 mei 2022
Themadag rechten van betrokkenen
Leer in deze training hoe betrokkenen geïnformeerd moeten worden over de verwerkingen van hun persoonsgegevens en welke rechten zij hebben.

Deze training vindt plaats in Amsterdam. Lees meer!
https://bit.ly/3Bo24ZS

Dinsdag 17 mei 2022
AVG-thema's nader bekeken
Privacywetgeving kent open normen en grijze gebieden. Tijdens deze training gaan we o.a. in op de DPIA en de export van gegevens buiten de EER.

Deze training vindt plaats in Utrecht. Lees meer!
https://bit.ly/3hMwex9

Woensdag 25 mei 2022
Themadag online marketing en cookies
Het is voor de FG onmisbaar om kennis paraat te hebben over direct marketing, profiling en de werking van cookies. Leer in deze dagtraining over het juridisch kader.

Deze training vindt plaats in Amsterdam. Lees meer!
https://bit.ly/3HTGdMv

Schrijf u gratis in voor onze live webinars

Maandag 25 april 2022
FG Newsflash
Laat u door onze privacy experts die tevens zelf werkzaam zijn als FG, bijpraten over de belangrijkste actuele ontwikkelingen die voor een FG relevant zijn.

Lees meer!
https://bit.ly/3LGInST

Maandag 2 mei 2022
AVG rechtspraak update
Onze privacy experts praten u bij over de belangrijkste privacy uitspraken, de essenties hiervan én de vertaal-slag naar de praktijk. De insteek is praktijkgericht.

Lees meer!
https://bit.ly/3BqUjCG

Maandag 13 juni 2022
IT en recht Newsflash
Laat u bijpraten over de belangrijkste rechtspraak, best practices én de vertaalslag naar de praktijk. Deze live webinar wordt verzorgd door onze IT-juristen.

Lees meer!
https://bit.ly/33tkn3n

Meld u aan voor onze CIPP/E, CIPM en CIPT trainingen

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 u CIPP/E, CIPM en CIPT trainingen aan. Zo wordt u een nationaal en internationaal gecertificeerde privacy professional.

De trainingen vinden plaats in Utrecht, Zwolle en online. Lees meer!
www.ictrecht.nl/iapp-trainingen

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