jaargang 11 · nummer 1 · januari 2023

ICTRecht in de praktijk

In vier stappen compliant digitale zorg verlenen

Het gaat snel, maar is het ook genoeg? Een visie op legal tech

Impact van de nieuwe ISO 27001 versie voor uw organisatie

ICTRECHT

ICTRecht: praktisch en deskundig

ICTRecht is hét grootste en meest ervaren fullservice adviesbureau op het gebied van Legal, Security en Tech. 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

Meer informatie over hoe wij werken?
Bezoek **ictrecht.nl**

ICTRECHT

Index

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

Aan deze uitgave werkten mee:

Arnoud Engelfriet Algemeen directeur/ Opleidingsdirecteur
a.engelfriet@ictrecht.nl
Bram de Vos Juridisch adviseur
b.devos@ictrecht.nl
Caroline van Ekeren Juridisch adviseur
c.vanekeren@ictrecht.nl
Dimmen Smolders Juridisch adviseur
d.smolders@ictrecht.nl
Emily Swens Legal Assistant
e.swens@ictrecht.nl
Isabella Oelz Juridisch adviseur
i.oelz@ictrecht.nl
Itte Overing Juridisch adviseur
i.overing@ictrecht.nl
Kors Monster Directeur ICTRecht Security
k.monster@ictrecht.nl
Mark Zijlstra Legal consultant
m.zijlstra@ictrecht.nl
Raoul van de Laak Partnermanager & juridisch adviseur
r.vandelaak@ictrecht.nl
Salmaan Khan Information security consultant
s.khan@ictrecht.nl
Sanne van Esterik Juridisch werkstudent
s.vanesterik@ictrecht.nl
Simon Hagen Content marketeer
s.hagen@ictrecht.nl
Eline Pellis grafisch ontwerp
Ontwerp en opmaak layout
eline@elinepellis.com
Leonard Fäustle Stills & Motion
Foto's ICTRecht
info@leonardfaustle.nl
Ronald Zijlstra Fotografie
Foto's ICTRecht
info@ronaldzijlstra.nl
Saskia Bakker Fotografie
Foto's ICTRecht
contact@saskiabakkerfotografie.nl

Itte Overing
Juridisch adviseur

E-health

In vier stappen compliant digitale zorg verlenen

In 2010 trad ik in dienst bij ICTRecht. Vlak daarna stierf het landelijk EPD een politieke dood. Niet voldoende waarborgen voor de privacy, niet voldoende regie bij de veldpartijen. Fast Forward naar maart 2020, corona en de eerste lockdown. De digitalisering van de zorg in een stroomversnelling. De wetgever is gevraagd om (weer) de regie te nemen bij de digitalisering.
Nu is er een integraal zorgakkoord, met digitalisering (en standaardisering) als bouwsteen en versneller voor het samen werken aan gezonde zorg. Want de gedachte is, we moeten nu aan de slag voor een toekomstbestendige zorg.
Maar waar begint u?

Integraal Zorgakkoord

In het Integraal Zorgakkoord (IZA) wordt aandacht besteed aan welke digitalisering bij kan dragen aan arbeidsbesparende en passende zorg. In 2025 is het de bedoeling dat elektronische gegevens-uitwisseling de standaard is in de zorg en dat elke inwoner toegang heeft tot zijn of haar medische gegevens middels een persoonlijke gezondheids-omgeving (PGO). Het doel is dat in 2026 gebruik kan worden gemaakt van zogenaamde hybride zorgpaden (binnen sectoren).

Mede om passende en arbeidsbesparende zorg te faciliteren, om de gewenste samenwerking uitvoerbaar te maken, dienen data (of beter gezegd gegevens) digitaal, eenduidig en gestandaardiseerd geregistreerd te worden in het zorgproces. Natuurlijk is het op deze manier registreren ook zeer nuttig voor het gewenste gebruik van data voor diverse secundaire doelen: denk aan zorg-, management- en stuurinformatie, maar ook het gebruik van data voor innovaties zoals AI-toepassingen.
Bij het gebruik van al deze informatie van de inwoners moet uiteraard rekening worden gehouden met - zeker als het gaat om deze secundaire doelen - proportionaliteit, doelbinding, de bescherming daarvan en de zeggenschap van de burger over zijn gegevens.

Waarom nu aan de slag?

Een zorgaanbieder koopt over het algemeen ICT-toepassingen in voor een periode van 5 jaar of langer. Zodra u in beeld heeft wat u nodig heeft voor de door u gewenste digitalisering, kunt u dit meenemen bij uw inkoop of onderhandeling. Stel dat u verplicht bent om bepaalde uitwisselingen digitaal te doen over een jaar of over 4 jaar, dan kunt u dit nu bespreekbaar maken. Of als een

bepaalde standaardisatie al heeft plaatsgevonden, denk aan NEN 7503:2022 'Gegevensuitwisseling in de zorg - Elektronische verwerking en uitwisseling van gegevens voor het voorschrijven en ter hand stellen van medicatie'. Dan moet een leverancier wel voldoen aan de eisen die voor zijn systeem gelden op basis van een dergelijke norm. Denk hierbij bijvoorbeeld aan de standaardisatie van koppelvlakken door de ICT-leverancier, in het kader van de interoperabiliteit.

Een andere reden is het feit dat voor de transformatiemiddelen geldt: *"use it or lose it"*. De transformatiemiddelen (geld) zijn enkel komende 5 jaar beschikbaar, aldus het IZA. Deze middelen zijn bedoeld om een transformatie te maken naar arbeidsbesparende passende zorg. Gebruikt u ze niet? Dan kunt u ze niet ten goede laten komen aan uw eigen vermogen.
En uiteindelijk geldt natuurlijk algemeen het nijpende tekort aan mensen in de zorg en de stijging van de belasting van de zorg. Naar alle waarschijnlijkheid zult u dus moeten besparen op de inzet van mensen, of vooral op de inzet van mensen met een bepaalde opleiding, bij het verlenen van zorg. Als u het IZA onderschrijft, en de daar genoemde stappen wilt ondernemen om tot passende en arbeidsbesparende zorg te komen, waar begint u dan met deze enorme opgave?

Vanuit ons perspectief kunnen wij u een **plan van aanpak** aanreiken. Ons doel daarbij is dat u de transformatie kunt inzetten, dus hybride zorgpaden kunt ontwikkelen en standaarden kunt implementeren zonder daarbij bestaande en nieuwe wetgeving uit het oog te verliezen.

Afgelopen jaren is er nogal wat regelgeving bij gekomen of aangepast op het gebied van ICT-gezondheidsrecht, de in onze ogen meest belangrijke onder elkaar:
- Algemene verordening gegevensbescherming (AVG)
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)
- Besluit elektronische gegevensuitwisseling door Zorgaanbieders
- Wet op de geneeskundige behandelingsovereenkomst (WGBO)
- Medical Device Regulation (en IVDR)
- Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)

De volgende relevante wet- en regelgeving is in de maak:
- Wet elektronische gegevensuitwisseling in de zorg (Wegiz)
- Verordening tot oprichting van een Europese ruimte voor gezondheidsgegevens (EHDS)
- AI Verordening

Plan van aanpak

Ons plan van aanpak is een **totaalaanpak**. Waarom? Omdat er anders grote kans is dat het werk dubbel gedaan wordt binnen een zorginstelling, of dat bepaalde onderwerpen de agenda nooit halen. Vaak zijn er binnen een grote instelling namelijk meerdere initiatieven om te digitaliseren. Ook ziet u binnen een instellingen vaak verschillende functionarissen of experts die vanuit hun invalshoek bezig zijn met het (gaan) voldoen aan wet- en regelgeving of normen, denk bijvoorbeeld aan de FG en de CISO. Communicatie is hier nodig om overlap te voorkomen. Een totaalaanpak, waarbij goed gekeken wordt welke stakeholders moeten worden betrokken, zorgt voor meer waarde voor de zorginstelling als geheel.

Voordat de zorginstelling kan beginnen, moet het plan van aanpak en de scope van het project besproken worden met het bestuur van de instelling. Er is commitment vanuit het bestuur nodig om een dergelijk project tot een succes te kunnen maken. En de kennis van de verschillende initiatieven die al lopen is essentieel. Het bestuur heeft daar overzicht van. Samen met het bestuur wordt de scope van het project bepaald. Het plan van aanpak kent de volgende fases:

1. Analysefase
2. Implementatiefase
3. Audit-fase
4. Duurzaam onderhoud-fase

Analyse

De analysefase start met een **inventarisatie** van de online diensten, applicaties en on premises software (hierna: het applicatielandschap of de applicaties) zoals in gebruik bij de zorginstelling en de data (gegevens) die daarin worden verwerkt. Indien bekend, is het goed om ook te inventariseren met welk doel gegevens worden verwerkt. Dan moeten de datastromen in kaart worden gebracht. Extern naar intern en van intern naar extern. Nadat applicatie, data en datastromen in beeld zijn, moet gekeken worden naar de roadmap of strategie: welke applicaties zijn end of life, of welke worden juist aangekocht of geïmplementeerd? Hoe gaat de zorginstelling de hybride zorgpaden vormgeven, welke samenwerkingen zijn op handen? Dan moet beoordeeld worden welke zorg er nu en in de toekomst geleverd gaat worden door de instelling.

Na deze inventarisatie moet **gekwalificeerd** worden aan de hand van de wet. Applicaties kunnen kwalificeren als zorginformatiesysteem (EPD, ECD), als uitwisselingssysteem maar daarnaast ook als medisch hulpmiddel. Want ja, software kan een medisch hulpmiddel zijn. Staat de ontwikkeling van een AI-toepassing op de roadmap? Goed om te beoordelen of de AI Act in de toekomst relevant zal zijn of dat bijvoorbeeld de ‘Leidraad kwaliteit AI in de zorg’[1] nog meegenomen kan worden bij ontwikkeling van AI.
De gegevens zijn mogelijk te kwalificeren als persoonsgegevens of bijzondere (medische) persoonsgegevens; als onderdeel van het medisch dossier of financieel dossier van de instelling; of zijn bedoeld voor het kwaliteitsonderzoek van de instelling; of datasets zoals gebruikt voor onderzoek.
Kwalificeer de datastromen waar mogelijk en nuttig, zijn de stromen toegestaan op grond van de wet en waarom? Goed om vast te stellen op welke grond en met welk doel data uitgewisseld wordt, bijvoorbeeld in het kader van verwijzing of het doen van onderzoek of ten behoeve uitbetaling door de zorgverzekeraar. Ten aanzien van de verwerking van persoonsgegevens (zoals onderdeel van de data en uitgewisseld middels datastromen) moet vastgesteld worden welke rol de zorginstelling heeft op grond van de AVG.
Vervolgens is het belangrijk de zorg te kwalificeren om vast te stellen welke wet (of wetten) van toepassing is. En om vast te stellen welke van de gegevensuitwisselingen van de “Meerjarenagenda” relevant zijn. Er staan er nu elf op de lijst[2], begin 2023 wordt de lijst uitgebreid met een selectie van gegevensuitwisselingen uit de richtlijn acute zorg.

1. Leidraad voor kwalitatieve diagnostische en prognostische toepassingen van AI in de zorg, https://www.leidraad-ai.nl/
2. https://www.gegevensuitwisselingindezorg.nl/gegevensuitwisseling/uitleg-over-de-wet/meerjarenagenda-wegiz

Aan de hand van de inventarisatie en kwalificatie (en de afgesproken scope) moet een **kader** worden opgesteld. In dit kader staat, kort door de bocht, aan welke normen en welke wetgeving

“Mede om passende en arbeidsbesparende zorg te faciliteren, om de gewenste samenwerking uitvoerbaar te maken, dient data (of beter gezegd gegevens) digitaal, eenduidig en gestandaardiseerd geregistreerd te worden in het zorgproces.”

uw organisatie en uw applicatielandschap moet voldoen bij de gewenste digitalisering gezien de zorg die de instelling verleent of zal verlenen. Bij de **nulmeting en GAP-analyse** wordt vastgesteld, wat reeds geïmplementeerd is en welke GAP er is. Goed is altijd om daarbij vast te stellen waar dubbel werk kan worden voorkomen: is voor een bepaalde applicatie al privacybeleid geschreven of zijn autorisatieprofielen ontwikkeld; of is er al een groep aan de slag met de vertaling van een bepaalde standaardisatie naar wat dat betekent voor de instelling. Goed om in kaart te brengen in de GAP-analyse welk werk reeds gedaan is en elders in de organisatie gekopieerd kan worden.

De analysefase bestaat dus uit de inventarisatie en kwalificatie van het applicatielandschap, de data, datastromen en de zorg, nu en in de toekomst. Vervolgens moet het kader (juridisch- en normenkader) worden opgesteld op basis waarvan de nulmeting en GAP-analyse kan worden uitgevoerd.

Op de GAP-analyse kunt u een risicoanalyse doen. Mede op basis daarvan kunt u dan gedurende de implementatiefase de roadmap invullen.

Implementatie

Op basis van de nulmeting en GAP-analyse kan de zorginstelling starten met de implementatiefase. Deze fase bestaat uit het opstellen van een projectplan, een roadmap met prioritering en dan de daadwerkelijke implementatie.

Uiteraard hangt het af van de snelheid van de ontwikkeling van standaarden door NEN of het uitdenken van een hybride zorgpad, wanneer u daadwerkelijk aan de slag kunt met de implementatie. Het maken van een gedegen projectplan en een roadmap zorgt er wel voor dat u niet voor verrassingen komt te staan. Dat u bij inkoop bewust zult zijn van uw verplichtingen komende jaren. Ook krijgt u inzichtelijk welke transitie u moet doormaken om aan wet- en regelgeving te kunnen blijven voldoen. En daarnaast, als u ook aan de slag bent of gaat met bijvoorbeeld hybride zorgpaden of het samenwerken met andere instellingen om uw krachten en data te bundelen om tot inzichten te kunnen om arbeid te besparen, dan kunt u daar prioriteit aan geven binnen uw projectplan en roadmap.

Het opstellen van het projectplan en de roadmap zal u dus helpen om zicht te krijgen op uw verplichtingen (en risico's) en koers te bepalen bij deze enorme opgave.

De implementatie kan bijvoorbeeld bestaan uit het uitwerken van beleid, het implementeren van normen, het opstellen van juridische documenten, maar ook aan het geven van trainingen aan medewerkers, en het creëren van awareness op bepaalde onderwerpen. Gedrag is immers altijd een grote factor waar u mee aan de slag moet bij een digitalisering.

Audit en duurzaam onderhoud

Een voorbeeld van wanneer u bij digitalisering een interne of externe audit niet voorkomt. Bij het gebruik van een elektronisch patiëntdossier, oftewel een zorginformatiesysteem, moet u voldoen aan onder andere NEN7510. 'Voldoen aan' is niet hetzelfde als 'gecertificeerd zijn voor'. Een interne audit is dan wel op zijn plaats, al wordt ook voor de instelling certificering steeds meer de norm als het gaat om informatiebeveiliging. Indien uw software kwalificeert als medisch hulpmiddel, en al gebruikt u dit enkel intern, dan nog is het kwaliteitsmanagementsysteem (bij medische hulpmiddelen: ISO 13485) verplichte kost.

Dus na implementatie, is een audit waarschijnlijk nodig. Onderdeel van dergelijke managementsystemen is altijd de 'plan do check act'-cyclus. Deze cyclus vormt ook de basis van duurzaam onderhoud van hetgeen er geïmplementeerd is en het uitvoeren en waar nodig aanpassen van de roadmap. De strategie van de instelling kan wijzigen, denk aan nieuwe samenwerkingen of wijziging van de zorg die verleend zou gaan worden. Wetgeving is in beweging. Een en ander heeft effect op waaraan het applicatielandschap moet voldoen. De roadmap wordt dan aangepast zodat de zorginstelling grip houdt op deze enorme opgave.

Kunt u ondersteuning gebruiken bij de totaalaanpak? Vanuit ICTRecht hebben we expertise op het gebied van IT-gezondheidsrecht, privacy, security en tech. Wij ondersteunen u graag met advies of doorlopende ondersteuning.

Blended: de moderne manier van leren

Tijdgebrek: hét probleem van de juridisch professional. Iedereen wil bijblijven en zich ontwikkelen, maar het werk gaat ook door. Dan is een hele dag op cursus wel een grote investering. Daarom kijken steeds meer mensen naar blended learning, een nieuwe vorm van leren, waarin klassikale en online elementen gecombineerd worden.

Bij blended learning worden de voordelen van klassikaal en afstandsonderwijs gecombineerd. Zo leert u bijvoorbeeld een groot deel van de stof zelfstandig in eigen tijd en tempo via een digitale leeromgeving, maar ontmoet u ook regelmatig docenten en medestudenten in een klaslokaal. Hier kan gericht en verdiept worden gewerkt, omdat u de basis immers al online verworven hebt.

Voor professionals is deze manier van werken ideaal. U heeft meer flexibiliteit, een betere benutting van de tijd en mogelijkheden, en een grotere controle over het leerproces. Een grootschalig onderzoek bij de faculteit Rechtsgeleerdheid van de Open Universiteit in 2021 laat zien dat blended learning helpt bij het afronden van een kennisgerichte opleiding, bijdraagt aan een betere studiebegeleiding en uiteindelijk leidt tot hogere scores.

Hoe ziet blended leren er nu praktisch uit?
Neem een cursus ICT-contracten als voorbeeld. Zo'n cursus heeft een aantal leerdoelen, zoals het benoemen van de belangrijkste elementen van dergelijke contracten, het herkennen van valkuilen, het kunnen lezen van typische clausules en het toepassen van terugvalposities in het contracteringsproces. Dit alles in een klaslokaal verwerven kan, maar wordt vaak als langdradig ervaren: de basisstof staat ook in het boek, sommige studenten leren sneller dan andere en discussies gaan alle kanten op.

Bij blended learning begint u in eigen tijd met de basis. U bekijkt webinars (met daarin toetsvragen) over de basis zoals contractsstructuur en belangrijkste elementen. Via e-learning oefent u met het spotten van valkuilen. Denk aan puzzels waarin u deze moet aanwijzen tussen 'gewone' clausules, of opdrachten waarbij u clausules sorteert op "neutraal", "voordelig" of "gevaarlijk". U kunt deze opdrachten zo vaak herhalen als u wilt, in uw eigen tempo.

In het klaslokaal wordt het online geleerde in de praktijk gebracht. Alle aanwezigen zitten nu op hetzelfde niveau, dus de docent kan meteen de diepte in: hier is een contract, wie spot de grootste risico's voor de leverancier en wie heeft een voorstel voor de afnemer? Zo kan in minder tijd dezelfde stof worden verworven.

Kortom, blended learning is een moderne vorm van leren die ideaal is voor drukke professional. Laat u uitdagen en ervaar zelf hoe u betere resultaten boekt met een flexibel schema.

Mark Zijlstra
Legal consultant

Legal tech

Het gaat snel, maar is het ook genoeg? Een visie op legal tech

De afgelopen jaren is er veel gebeurd op het gebied van Legal Tech. Het aantal aanbieders van software die het leven van de jurist vergemakkelijkt is exponentieel gegroeid en ook in de functionaliteit van deze aangeboden software zijn mooie stappen gemaakt. Producten worden steeds completer en gebruiksvriendelijker. Daarnaast lijkt de belofte van kunstmatige intelligentie langzaam maar zeker te worden ingelost.
Is er daarmee ook niets meer te wensen over? Zeker wel! Dit artikel is een keer geen introductie van een nieuw soort tooling of verdieping van een specifiek onderwerp. Wel delen we onze visie op de nabije toekomst van Legal Tech en de invloed hiervan op het leven van de hedendaagse jurist.

Ontwikkelingen: sneller en slimmer

Vierde revolutie

Laten we de opkomst van Legal Tech eerst even kort in historisch perspectief plaatsen. De eerste revolutie was de opkomst van water en stoom om machines te laten draaien. De tweede revolutie was het gebruik van elektriciteit en de derde revolutie zag op het gebruik van informatietechnologie voor het automatiseren van eenvoudige taken.

Inmiddels zijn we langzaam begonnen aan de vierde revolutie. Die sluit feitelijk aan bij de derde, maar is in een aantal opzichten toch anders.
De vierde evolutie zal sneller gaan en de omvang maar ook vooral de impact zal groter zijn.

Het World Economic Forum voorspelde eerder dat in 2025 ongeveer 50% van het werk dat we verrichten geautomatiseerd is.[1] Dit is het gevolg van de vierde revolutie, waarbij kennis en technologie nog dichter bij elkaar komen en robots en kunstmatige intelligentie een belangrijke rol spelen.

1. https://www3.weforum.org/docs/WEF_Future_of_Jobs_2018.pdf

De continue technologische ontwikkeling maakt dat verandering in bedrijfsvoering noodzakelijk én wenselijk is. De behoefte verandert mee met de ontwikkeling en de eisen die een jurist nu stelt aan een legal tech-oplossing zijn binnenkort achterhaald. Dit vereist flexibiliteit en processen die aan verandering onderhevig zijn. Afhankelijk van de

ontwikkelingen kan het zo zijn dat bepaalde delen van een proces op dit moment volledig handmatig zijn, over twee jaar ondersteund worden door techniek en over vijf jaar wellicht volledig geautomatiseerd zijn. Dit maakt dat de focus van de jurist kan verschuiven van deels administratieve taken naar volledig inhoudelijk (maat)werk.

Aanpassingsvermogen

Toen de stoommachine zijn intrede deed, werd deze door vele gezien als een duivelse machine. De reacties op de eerste mobiele telefoon kennen we ook allemaal: “Ik zie er het nut niet van in” en “ik heb een gewone telefoon, ik hoef niet altijd bereikbaar te zijn” klonk het eind jaren 90 sceptisch. Inmiddels kunnen we stellen dat de mobiele telefoon niet meer is weg te denken uit ons straatbeeld. Veel hedendaagse technologie die nu vanzelfsprekend is, maakte een soortgelijk proces door. Dit artikel is geschreven met tekstverwerkingsoftware, dat is tegenwoordig doodnormaal. Vertel dat maar aan de mensen die ineens op een computer moesten gaan werken.

Met de komst van de computer en de exponentiële groei van de rekenkracht, gaat de ontwikkeling aanzienlijk sneller. Voor de oudere generatie juristen onder ons zal het wellicht lastig zijn om bij te blijven bij alle nieuwe ontwikkelingen. Voor de aankomende generatie juristen wordt het meer vanzelfsprekend. Zij zijn immers opgegroeid met smartphones, apps en een wereld die bereikbaar is met één druk op de knop.

En jawel, wie de vierde revolutie kent ook zijn weerslag op het gebied van legal tech. De voornaamste ontwikkeling zit in de intelligentie van de legal tech-oplossingen. Waar kunstmatige intelligentie nu mondjesmaat wordt gebruikt in software voor de juridische markt (denk aan Lynn Legal, Bluetick of Contractify) verwachten we dat dit de komende jaren exponentieel toeneemt.

Met flexibelere bedrijfsprocessen en toekomstige juristen die meer gewend zijn aan snelle technologische ontwikkeling, is de weg vrij voor een nieuwe generatie legal tech-tools. Hierin gaat kunstmatige intelligentie een grote(re) rol spelen en neemt de software ook complexere taken over en een centrale plek in in de organisatie. Dit brengt dus naast een ontwikkeling op de werkvloer ook een verandering in de instelling van de jurist (en het management van de organisatie) teweeg.

Uitdagingen

Uiteraard brengt de komst van slimmere software, net zoals eerdere revoluties, ook uitdagingen met zich mee. Los van de inhoudelijke discussie omtrent de vooroordelen, ondoorzichtigheid en (soms) het gebrek aan menselijke invloed, zijn er ook andere uitdagingen. Zo moet ook het management van organisaties zich voorbereiden op de komst van slimmere software. Vroegtijdige omarming kan vele voordelen hebben, maar in de praktijk gaat dit traag.

Anderzijds vraagt het een aanpassing in de wijze waarop toekomstige juristen worden opgeleid. Ook hier is al een kleine verschuiving merkbaar, maar met name de universiteiten besteden op dit moment nog te weinig aandacht aan de technologische ontwikkelingen in het juridisch werkveld. Het hoger beroepsonderwijs is hierin al verder. Ten slotte zijn er nog toezichthouders die terughoudend zijn met de omarming van legal tech, denk bijvoorbeeld aan de orde van advocaten. Ook hier is zeker nog winst te behalen.

Ecosysteem: veel aanbod maar weinig samenwerking

Aanbod

Maar dan zijn we er nog niet. Naast de ontwikkeling richting slimmere en snellere technologie, is namelijk een andere ontwikkeling wenselijk. Want waarom is de legal tech-markt op dit moment zo ontzettend versnipperd?

De vraag naar legal tech wordt steeds groter, om over het aanbod maar te zwijgen. Selectie van het juiste product hangt vaak af van de nuanceverschillen tussen de vele aanbieders. Dan is het nog de vraag hoe groot de ontwikkeldrang van de leverancier is. Het is lastig in te schatten of het product bij de tijd kan blijven. Dit terwijl er wel veel tijd en geld wordt gestoken in implementatie en langdurige licenties. Ook is er nog de vraag: wat te doen bij een veranderende interne behoefte? De overstap naar een alternatieve of aanvullende leverancier is vaak onwenselijk. Ook merken we in de praktijk vaak de afweging tussen het aanschaffen van een groot systeem met veel functionaliteiten of het klein beginnen met een puntoplossing - of toch misschien een *no code*-

oplossing? Hierbij spelen factoren als kosten, implementatie(tijd) en toekomstbestendigheid een grote rol.

Voor elk onderdeel van het werk van een jurist is anno 2023 wel een oplossing. Er zijn echter weinig oplossingen die volledig voldoen aan de specifieke wens van de klant. Perfectie bestaat logischerwijs (nog) niet en er zal altijd ontwikkeling blijven. Het is een kwestie van het best mogelijke product selecteren.

Matter

In november 2023 is Matter[2] officieel geïntroduceerd. Het is inmiddels redelijk normaal om een lamp, thermostaat of de deurbel op afstand te bedienen. Om de communicatie tussen het slimme apparaat en (bijvoorbeeld) een smartphone mogelijk te maken, worden diverse protocollen gebruikt. Zo zijn er ZigBee, Z-Wave, Bluetooth, wifi en Thread. Het verschilt per leverancier welke 'taal' het slimme product spreekt. Omdat niet alle producten dezelfde taal spreken, is het lastig om deze aan elkaar te verbinden. Met de introductie van Matter moet hier een einde aan komen. Door een samenwerking van veel (grote) leveranciers van slimme producten, is er nu een universeel protocol ontwikkeld. Voor de oudere generatie: vergelijk het met Esperanto. Het idee is dat je met de komst van Matter een willekeurig slim product kunt kopen en aansluiten en dat deze direct goed samenwerkt met de overige slimme producten in je huis.

2. https://www.xda-developers.com/matter-devices-are-coming-in-2023/

Interoperabliteit

Matter is natuurlijk een mooie ontwikkeling, maar heeft op het eerste oog niets met legal tech te maken. De reden waarom er in 2019 is begonnen met het ontwikkelen van Matter, is echter wel vergelijkbaar met de legal tech-markt. Hier is nu sprake van veel verschillende producten, van verschillende aanbieders, die in principe goed op elkaar aansluiten, maar niet eenvoudig samenwerken. Er is sprake van een een versnipperde markt met veel aanbieders en weinig interoperabiliteit. Juist dat laatste, interoperabiliteit, is waar de kansen voor softwareleveranciers liggen.

Het is nu al mogelijk bepaalde software te laten communiceren met andere software middels een API. Een goede werking van een API vereist echter in de praktijk nog wel wat werk. Van een *plug and play*-situatie zoals bij Matter is nog lang geen sprake.

In een ideale wereld maakt het niet uit welke legal tech-oplossing er wordt aangeschaft; deze werkt moeiteloos samen met de reeds bestaande systemen. Zo moet het eenvoudig zijn om een documentgenerator van de ene leverancier te combineren met het documentmanagementsysteem van een ander. En koppel je moeiteloos de juridische database als naslagwerk of komen de gegevens uit de privacy-tool samen met alle informatie die te maken heeft met corporate housekeeping. Op die manier heb je alle juridisch relevante informatie bij elkaar en ontwikkel je een *single point of truth* (ook niet onbelangrijk).

Uitdagingen

Uiteraard brengt de ontwikkeling van een goede interoperabiliteit de nodige uitdagingen met zich mee. Draagvlak onder de leveranciers is hier essentieel. Dergelijke initiatieven werken alleen als marktleiders meewerken. Is dit niet het geval, dan wordt er wéér een extra optie toegevoegd aan de markt – iets dat juist voorkomen moet worden.

Daarnaast kent legal tech-software veel meer en complexere 'waarden' dan waar Matter mee te maken heeft. Het zal niet eenvoudig zijn een dergelijke standaard te ontwikkelen. Sommige metadata leent zich hier prima voor, maar uitwisselen van complexe contractmodules of kennis brengt technische uitdagingen met zich mee.

De technologie zal veranderen, zoveel is duidelijk. Dit betekent ook dat er genoeg kansen liggen en sommige juristen staan te springen om hiermee aan de slag te gaan. De vraag is echter of we de technologische ontwikkelingen kunnen bijbenen. Zijn we er klaar voor?

Opleiding
Specialist ICT-recht

ICTRECHT ACADEMY

In 1 jaar uw focus op het snijvlak van **legal, tech en security**

start: april 2023 · duur: 1 jaar

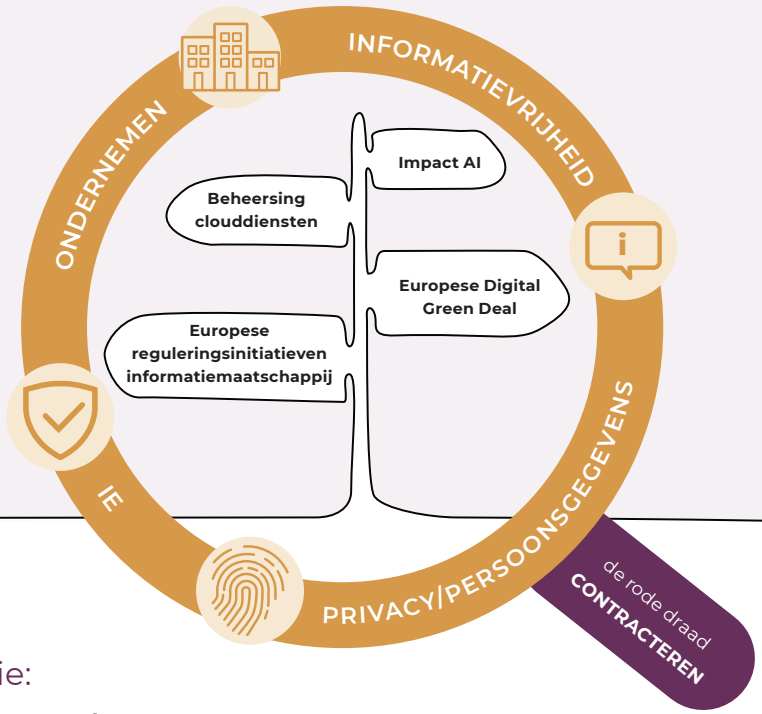
Vergroot uw kennis op het gebied van ict-technologie, software, security, privacy, digitaal ondernemen, blockchain, marktregulering (DSA/DMA) en artificial intelligence.

In het kort

- Flexibel leren (middels webinars en e-Learning) met 15 praktijkmiddagen op locatie in Utrecht;
- Gemiddeld beoordeeld met een 8.3;
- 56 PO punten. ICTRecht is NOvA-erkende opleidingsinstelling;
- Prijs: € 5.895 excl. BTW (inclusief boekenpakket).

Voor wie

Deze opleiding is toegankelijk voor wo-juristen die zich willen specialiseren in het ICT-recht. Verdere specifieke voorkennis is niet noodzakelijk.



56 PUNTEN PO ADVOCATUUR

NEDERLANDSE ORDE VAN ADVOCATEN

Kijk hier voor meer informatie:

ictrecht.nl/academy/opleidingen/specialist-ict-recht

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Nieuws

DAS en JuriBlox **bundelen krachten** voor transformatie juridische dienstverlening

Op 24 november 2022 sloten juridisch dienstverlener DAS en legal-techspecialist JuriBlox een exclusieve strategische samenwerking. Hun eerste speerproduct is de VSO checker, een volledig door artificiële intelligentie gedreven oplossing voor het controleren van en adviseren over vaststellingsovereenkomsten. Een primeur in Europa. Wat betekent dit voor de markt?

Een vaststellingsovereenkomst is een document dat in het arbeidsrecht veelvuldig nodig is. Als werkgever en werknemer afscheid nemen van elkaar, worden de afspraken met dit document geformaliseerd. Het document is enerzijds heel standaard, maar anderzijds elke keer net weer anders, met genoeg voetangels en klemmen om zelfs een ervaren jurist tot voorzichtigheid te manen.

De VSO checker, ontwikkeld met de Lynn technologie van JuriBlox en de marktkennis en data van DAS, heeft het potentieel de markt voor juridische dienstverlening te transformeren. De checker controleert op alle belangrijke punten, en doet suggesties voor verbetering waar nodig. En dat in een minuut, waar een jurist gemiddeld toch al gauw een uur nodig heeft voor een standaard controle.

Technisch is de VSO checker een cloudoplossing waarin een vaststellingsovereenkomst tussen werknemer en werkgever wordt geüpload, en deze vervolgens automatisch wordt gecontroleerd door de applicatie. Inclusief het doen van commentaar en desgewenst aanpassingen in de tekst. Hierdoor hebben de juristen van DAS meer tijd om de klant bij de hand te nemen; meer persoonlijke aandacht te bieden, en bijvoorbeeld de overeenkomst samen met de cliënt te doorlopen. Dat is de toekomst van juridische dienstverlening: laat computers het standaardwerk doen en de basischecks uitvoeren, zodat mensen hun unieke toegevoegde waarde kunnen laten zien.

“De VSO checker, ontwikkeld met de Lynn technologie van JuriBlox en de marktkennis en data van DAS, heeft het potentieel de markt voor juridische dienstverlening te transformeren.”

DAS wil in de toekomst toepassingen als de VSO-checker ook aan consumenten aanbieden – in plaats van de applicatie enkel door de eigen juristen te laten gebruiken. Daarmee kunnen werknemers zelf de mogelijkheid hebben om een vaststellingsovereenkomst te laten controleren. Dit kan als je verzekerd bent bij DAS, maar de applicaties worden in de toekomst ook beschikbaar gesteld tegen directe betaling – via iDeal bijvoorbeeld. On-demand juridisch advies: hoe gaat u daar als jurist mee om?

Foto: DAS-cco Charles Staats (links), Niels Winters (midden Juriblox) en Steven Ras van JuriBlox tekenen voor de nieuwe samenwerking

Meer informatie:
juriblox.nl

Wet- en regelgeving

Bram de Vos
Juridisch adviseur

Emily Swens
Legal Assistant

Datagovernanceverordening

Op 30 mei 2022 is de Datagovernanceverordening tot stand gekomen. Deze verordening moet onder andere het hergebruik van overheidsinformatie door overheidsinstanties gaan faciliteren. De verordening introduceert ook een nieuw bedrijfsmodel, de zogeheten 'databemiddelingsdienst' die ervoor moet zorgen dat burgers en bedrijven op een veilige manier hun gegevens kunnen delen. Organisaties die gegevens van burgers of organisaties willen gebruiken, kunnen zich daarnaast laten registreren als erkende organisatie op het gebied van data-altruïsme. Op die manier hoopt de Europese Unie de uitwisseling van gegevens voor doeleinden van algemeen belang te bevorderen. Op basis van de verordening zal er ook een Europees Comité voor gegevensinnovatie worden opgericht, in de vorm van een deskundigengroep. De verordening is van toepassing per 24 september 2023.

https://bit.ly/3ACQrPK

E-Codexverordening

Op 30 mei 2022 is de Verordening over een geautomatiseerd systeem voor de grensoverschrijdende elektronische gegevensuitwisseling op het gebied van justitiële samenwerking in civiele en strafzaken (e-Codex) tot stand gekomen. Het doel van de verordening is om grensoverschrijdende gerechtelijke procedures sneller te laten verlopen. Dit door de procedures voor de betekening en kennisgeving van gerechtelijke en buitengerechtelijke stukken in de Europese Unie te vereenvoudigen en te stroomlijnen. De verzendende en ontvangende instanties zullen voor moeten aansluiten op e-Codex. Dit systeem moet ervoor zorgen dat de IT-systemen die door justitiële autoriteiten worden gebruikt interoperabel zijn.

https://bit.ly/3gq6Vno

Voorstel Uitvoeringswet verordening terroristische online-inhoud

Op 20 juni 2022 is de voorgestelde uitvoeringswet over het tegengaan van de verspreiding van terroristische online-inhoud bij de Tweede Kamer ingediend. Deze uitvoeringswet hangt samen met de Europese Verordening terroristische online-inhoud, die misbruik van hostingdiensten voor terroristische doeleinden moet tegengaan. Het wetsvoorstel regelt primair de instelling van een nieuw zelfstandig bestuursorgaan genaamd de Autoriteit Online Terroristisch en Kinderpornografisch Materiaal (ATKM). Ook voorziet de uitvoeringswet in een mogelijkheid voor de ATKM om voor zijn handhavingstaken bijzondere (strafrechtelijke) persoonsgegevens te verwerken.

https://bit.ly/3VgXJAz

Wijziging Grondwet inzake de onschendbaarheid van het brief- en telecommunicatiegeheim

Op 6 juli 2022 is artikel 13 van de Grondwet gewijzigd. De wijziging zorgt ervoor dat de onschendbaarheid van het brief-, telefoon- en telegraafgeheim technieonafhankelijk wordt gemaakt, met als doel om alle huidige en toekomstige communicatiemiddelen onder het toepassingsbereik te laten vallen.

https://bit.ly/3Ve2bzY

Voorstel strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden

Op 7 juli 2022 is een voorstel voor de strafbaarstelling van het gebruik persoonsgegevens voor intimiderende doeleinden bij de Tweede Kamer ingediend. Dit wetsvoorstel voegt twee bepalingen toe aan het Wetboek van Strafrecht die het strafbaar stellen om persoonsgegevens voor intimiderende doeleinden te gebruiken. Het gaat hierbij om het verschaffen, verspreiden of anderszins ter beschikking stellen van identificerende persoonsgegevens van een ander of een derde met het oogmerk om die ander vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of ernstig te (laten) hinderen in hun dagelijks leven. Deze strafbaarstelling is behulpzaam als een beroep wordt gedaan op een internetplatform om gegevens te verwijderen omdat hiermee het verboden karakter van het gebruik van persoonsgegevens voor intimiderende doeleinden tot uitdrukking wordt gebracht.

https://bit.ly/3EOVrCj

Voorstel Wet Adviescollege ICT-toetsing

Op 12 september 2022 is het wetsvoorstel Wet Adviescollege ICT-toetsing bij de Tweede Kamer ingediend. Het voorstel betreft de instelling van een permanent adviescollege voor toetsing van informatiesystemen, ICT-projecten en onderhoud- en beheeractiviteiten van de centrale overheid. Het adviescollege heeft tot taak grote ICT-projecten en informatiesystemen van ministeries, politie en de Raad voor de rechtspraak te toetsen. Het college zal bestaan uit een voorzitter en ten hoogste vier andere leden. De leden hebben zitting op persoonlijke titel worden benoemd voor ten hoogste vier jaar. Herbenoeming kan eenmaal voor ten hoogste vier jaar plaatsvinden.

https://bit.ly/3Vi6TN9

Digital Markets Act

Op 12 oktober 2022 is de Digital Markets Act ("DMA") gepubliceerd in het Publicatieblad van de Europese Unie. De DMA biedt een regelgevend kader voor de 'poortwachters' van het internet. Deze bedrijven zijn van een dusdanige omvang dat zij een groot deel van het digitale domein beheersen. De DMA bevat onder meer een regels voor fusies en overnames. Daarnaast zijn hierin bepalingen over 'self-preferencing' opgenomen, waarmee het voortrekken van eigen producten en diensten ten opzichte van producten en diensten van concurrenten wordt bedoeld. Het grootste deel van de verordening wordt van toepassing vanaf 2 mei 2023.

https://bit.ly/3ETsdDh

Digital Services Act

Op 27 oktober 2022 is de Digital Services Act ("DSA") gepubliceerd in het Publicatieblad van de Europese Unie. De verordening bevat uiteenlopende verplichtingen voor verschillende soorten online dienstverleners, waaronder online (handels)platforms en zoekmachines. De DSA heeft als doelstelling het verbeteren van mechanismen voor het verwijderen van illegale inhoud en bescherming van de grondrechten van gebruikers. Het grootste deel van de verordening wordt van toepassing per 17 februari 2024.

https://bit.ly/3TTZ8Md

Voorstel implementatie Richtlijn betalingsdienstaanbieders

Op 21 oktober 2022 is het wetsvoorstel Wet implementatie Richtlijn betalingsdienstaanbieders bij de Tweede Kamer ingediend. Op grond van deze richtlijn worden betalingsdienstaanbieders verplicht om onder voorwaarden alle betaaldata van grensoverschrijdende transacties te delen met de Belastingdienst. Deze gegevens worden gebruikt in de bestrijding van btw-fraude bij grensoverschrijdende internetverkopen van goederen en diensten (e-commerce).

https://bit.ly/3GIple1

Isabella Oelz
Juridisch adviseur

Dimmen Smolders
Juridisch adviseur

Privacy

Digitalisering in het onderwijs: kansen en risico's

Het onderwijs is in het digitale tijdperk ingrijpend veranderd. Digiborden en laptops of tablets zijn al lange tijd onderdeel van het interieur van scholen. School- of studievoortgang wordt keurig bijgehouden in grafieken en vergeleken met klas- of studiegenoten. Onder invloed van de Covid-19 pandemie en de noodzaak om les op afstand te faciliteren kwam die ontwikkeling in een stroomversnelling.
Ondanks dat het onderwijs nu weer helemaal is teruggekeerd in de klaslokalen, gaat digitalisering in het onderwijs in volle vaart door. De techniek biedt kansen op allerlei terreinen, en daarvan maken onderwijsinstellingen graag gebruik. Educational Technology, kortaf EdTech genoemd, is dan ook een bloeiende industrie. In dit artikel leggen we uit wat EdTech inhoudt en wat deze technologieën kunnen betekenen voor de privacy van gebruikers.

Wat is EdTech?

Een algemeen gebruikte definitie van EdTech is er niet. Onder EdTech vallen onder andere: technologieën die onderwijsvoortgang meten, zoals leermanagementsystemen, technologieën die worden ingezet als nieuwe onderwijsvormen en technologieën waarmee technologisch onderwijs wordt gegeven. In alle gevallen dient de technologie om het werk van een onderwijsinstelling te verbeteren. Sommige van deze innovaties zijn bedoeld om de communicatie met scholieren of studenten te verbeteren, of studieresultaten bij te houden en te analyseren. Er zijn ook technologieën met veel meer potentiële impact, zoals het gebruik van kunstmatige intelligentie (AI) of zogenaamde immersive (letterlijk: 'onderdompelende') technologie, ten behoeve van onderwijs.

Het concept EdTech is de laatste jaren in opkomst vanwege de kansen die het biedt aan onderwijsinstellingen. Het onderwijs kan efficiënter of beter worden aangeboden, dankzij de hulp van technologische toepassingen. Grote aanbieders van clouddiensten, zoals Google en Microsoft, sprongen al vroeg op deze kansen. In Europa wordt ondertussen ook driftig gewerkt aan een bloeiende EdTech-industrie, mede omdat de doorgifte van persoonsgegevens naar de Verenigde Staten sinds de Schrems II-uitspraak bij voorbaat verdacht is.

De Nederlandse overheid ondersteunt digitale innovatie in het onderwijs, waaronder EdTech, van harte. Er lopen op dit moment al veel uiteenlopende initiatieven in het onderwijs, van basisscholen tot hoger onderwijs. Zo wordt vanuit het Nationaal Groeifonds (NGF) het *Nationaal Onder-*

wijslab gefinancierd. Dit om de toepassing van innovatieve producten op het gebied van kunstmatige intelligentie (AI) in het basis- en voortgezet onderwijs te bevorderen.[1] Voor het hoger onderwijs investeert de Rijksoverheid, samen met hogescholen en universiteiten, in het *Versnellingsplan Onderwijsinnovatie met ICT*.

1. https://www.rijksoverheid.nl/actueel/nieuws/2021/10/27/nationaal-groeifonds-financiert-ai-innovatie-voor-gebruik-in-onderwijs

Welke negatieve effecten kan EdTech hebben op privacy?

Wat alle categorieën van technologie gemeen hebben, is dat er grote hoeveelheden gegevens kunnen worden verzameld over de gebruikers. Dat betekent logischerwijs een risico voor de privacy van de gebruikers.

In het rapport "Naar hoogwaardig digitaal onderwijs" van het Rathenau instituut, worden aanbevelingen gedaan om de effecten van digitalisering de juiste kant op te sturen.[2] Onder meer ongewenst datagebruik, zoals profilering, moet worden tegengegaan, aldus het rapport. Wanneer bijvoorbeeld wordt gewerkt met grote hoeveelheden studiedata, ligt de mogelijkheid van profilering op de loer. Er wordt daarnaast ook gewaarschuwd voor een 'chilling effect': het onderdrukken van bepaald menselijk gedrag door continue monitoring tijdens het onderwijs.

2. https://www.rathenau.nl/sites/default/files/2022-02/Rathenau%20Instituut_Rapport_Naar_hoogwaardig_digitaal_onderwijs-24feb2022.pdf

SURF heeft als ICT-onderwijsvertegenwoordiger in 2021 een DPIA laten uitvoeren op de Google Workspace for Education diensten. Daaruit kwamen risico's naar voren, waaronder dat Google teveel vrijheid had om te doen wat het wilde met de verzamelde metadata.

Juridisch zijn er al kaders om de hierboven beschreven negatieve effecten van digitalisering te beperken. Op grond van de Algemene verordening gegevensbescherming (AVG) hebben betrokkenen het recht om niet onderworpen te worden aan een besluit puur op basis van profilering, "dat hem in aanmerkelijke mate treft". Anders gezegd: negatieve gevolgen op basis van een geautomatiseerd toegekend profiel, zonder menselijke tussenkomst, zijn verboden. Daarnaast gelden er strengere regels rond het informeren van betrokkenen over het gebruik van geautomatiseerde besluitvorming. Voor het volgen van het gedrag van studenten geldt dat in bepaalde gevallen een DPIA verplicht is. Hoe dan ook zijn de beginselen van noodzakelijkheid en proportionaliteit van essentieel belang: kan het doel met minder ingrijpende middelen worden bereikt, dan moet daarvoor worden gekozen.

Een leverancier mag tot slot niet zelf bepalen wat hij kan doen met de verzamelde informatie over gebruikers van een onderwijsinstelling. In de verwerkersovereenkomst wordt afgesproken onder welke voorwaarden de leverancier de persoonsgegevens mag of moet verwerken.

Ethische normen voor het gebruik van EdTech

Onderwijsinstellingen zijn de verwerkingsverantwoordelijke voor de verwerkingen van persoonsgegevens middels EdTech, dus rusten op hen de hierboven genoemde verplichtingen. Minstens even belangrijk is het dat onderwijsinstellingen zichzelf ook steeds afvragen wat ethisch verantwoord is bij het gebruik van EdTech. Ook al mag iets strikt genomen op grond van de wet, kan een instelling dan nog steeds aan ouders, scholieren of studenten uitleggen wat er aan informatie wordt verzameld, en wat er vervolgens mee gebeurt?

Om richting te geven aan de ethische keuzes die instellingen moeten maken, hebben Kennisnet en SURF een WaardenWijzer voor digitalisering in het onderwijs opgesteld.[3] Daarin worden als drie hoofdwaarden voor het onderwijs bestempeld: rechtvaardigheid, menselijkheid en autonomie.

3. https://www.kennisnet.nl/app/uploads/kennisnet/digitale-geletterdheid/documenten/waardenwijzer_def.pdf

Ondersteuning EdTech op het terrein van privacy

Onderwijsinstellingen worden als dat nodig is ondersteund door verschillende informatiebronnen, als het gaat om privacy. Kennisnet voorziet het

basis- en voortgezet onderwijs van informatie en handreikingen over – onder meer – digitalisering en privacy. Kennisnet biedt verschillende templates aan voor beleidsstukken, registraties en handreikingen. Leveranciers in het basis- of voortgezet onderwijs kunnen het privacyconvenant ondertekenen en de bijbehorende model-verwerkersovereenkomst gebruiken, om te laten zien dat zij privacy serieus nemen. Voor het hoger onderwijs is er SURF, wat op haar beurt het Versnellingsplan ondersteunt, om digitalisering in het hoger onderwijs te stimuleren, binnen de kaders van privacy.

Hoe het onderwerp privacy in de EdTech-community wordt aangekaart, wordt nader behandeld in onderstaande case study.

Conclusie

Er bestaat geen twijfel dat technologische innovatie in het onderwijs kansen biedt. EdTech wordt al grootschalig ingezet om onderwijs efficiënter of beter te maken. De Covid-19 pandemie heeft de laatste jaren duidelijk gemaakt dat het massale, klassikale onderwijs niet in alle omstandigheden mogelijk is. Onder druk van personeelstekorten in het onderwijs worden de krachten richting digitalisering alleen maar sterker.

Zoals met alle vormen van technologische innovatie waarbij gebruikersgegevens worden verzameld, kleven er privacyrisico's aan EdTech-toepassingen. Het is uiteindelijk aan de instellingen die deze technologie inzetten, om te zorgen dat de wet wordt nageleefd en, misschien nog belangrijker, aan gebruikers kan worden uitgelegd wat er met hun persoonsgegevens gebeurt.

Om te zorgen dat er een bloeiende lokale EdTech-industrie bestaat, zijn diverse organisaties actief met het delen van informatie en het initiëren van projecten. Uiteindelijk is het aan de aanbieders van EdTech om een privacyvriendelijk product aan te bieden, wat de afnemer tegelijk kansen biedt om het onderwijs te verbeteren. Inspiratie opdoen, of aanhaken bij, de landelijke projecten die op dit moment lopen, kan helpen bij het maken van de noodzakelijke keuzes rondom het verzamelen en het gebruik van persoonsgegevens in het onderwijs.

Case study: Startup in Residence

Instellingen, SURF en de Rijksoverheid investeren samen in de ontwikkeling van EdTech, middels een speciale EdTech-werkgroep van het *Versnellingsplan Onderwijsinnovatie met ICT*. "Doel is om onderwijsinnovatie binnen het hoger onderwijs te vergroten", aldus Liselotte Westerveld van Startup in Residence in een toelichting. Startup in Residence is één van de projecten die onder het Versnellingsplan Onderwijsinnovatie met ICT worden uitgevoerd. De bedoeling is om EdTech-startups en opdrachtgevers, in dit geval hogescholen en universiteiten, met elkaar in contact te brengen. Startup in Residence selecteert startups op basis van een opdracht vanuit een instelling en koppelt bedrijf en instelling vervolgens aan elkaar. Startup in Residence begeleidt daarna zowel de startup als de instelling, om het product te verbeteren en het bedrijf klaar te stomen voor de markt waar zij hun product willen aanbieden. Privacy is één van de vraagstukken waar aandacht aan wordt besteed: hoe kun je als startup tegemoet komen aan de hoge eisen die instellingen stellen, als het gaat om de bescherming van persoonsgegevens?

ICTRECHT

Ook uw **ISO 27001 certificering** behalen? ICTRecht helpt u!

ISO 27001 is een wereldwijd erkende norm op het gebied van informatiebeveiliging. Het behalen van het ISO 27001 certificaat geeft aan dat uw organisatie serieus omgaat met de beveiliging van informatie. Dit straalt vertrouwen uit naar (potentiële) klanten, investeerders en partners.

Wist u al dat er een nieuwe versie van de ISO 27001 is? In het artikel op de volgende bladzijde leest meer over de wijzigingen die zijn doorgevoerd.

Meer weten? Kijk dan op onze website:
ictrecht.nl/security/iso-27001-certificering

Salmaan Khan
Information security consultant

Kors Monster
Directeur ICTRecht Security

Security

Impact van de nieuwe **ISO 27001 versie** voor uw organisatie

Wellicht heeft u er de laatste tijd al wat over gehoord of gelezen: de internationale norm voor informatiebeveiliging ISO/IEC 27001 (hierna kortweg 'ISO 27001') heeft een update gehad. De nieuwste versie[1] vervangt de versie uit 2017. Wij vertellen u graag wat dit betekent voor uw organisatie, of u nou ISO 27001 gecertificeerd bent of niet. Want: ook voor partijen die zelf niet gecertificeerd zijn, maar die zaken doen met gecertificeerde partijen (ofwel als leverancier, ofwel als afnemer), kunnen met veranderingen te maken krijgen.

1. Voluit: ISO/IEC 27001:2022.

Hoe zat het ook alweer: ISO 27001 in een notendop

ISO 27001 is een internationale norm op basis waarvan organisaties een werkwijze rond informatiebeveiliging kunnen inrichten. Het doel hiervan is om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te waarborgen en om de impact van eventuele incidenten tot een acceptabel niveau te beperken. De norm draait in eerste instantie om het inrichten van een managementsysteem voor informatiebeveiliging (ook wel: 'information security management system' of kortweg 'ISMS'), waarmee de werkwijze procesmatig wordt geborgd. De risico's voor de organisatie vormen daarbij het uitgangspunt.

Binnen deze werkwijze staat de plan-do-check-act-cyclus centraal. Dat houdt in dat in eerste instantie een plan wordt gemaakt om de beveiligingsrisico's voor de organisatie te beteugelen. In de 'do-fase' wordt dit plan ten uitvoer gebracht door de maatregelen te implementeren die zijn bedacht om de risico's aan te pakken. Vervolgens wordt in de 'check-fase' geëvalueerd of de maatregelen op de juiste wijze zijn doorgevoerd en of zij ook het effect hebben dat van tevoren was bedacht. Daar waar dat nodig is wordt op basis van de evaluatie in de 'act-fase' bijgestuurd. Vervolgens vormen de ervaringen en inzichten die gedurende de cyclus zijn opgedaan input voor de volgende cyclus. Op die manier wordt het ISMS continu een stukje verbeterd.

Lezers die thuis zijn in andere ISO-normen, zoals de norm voor kwaliteit (ISO 9001), zullen de plan-do-check-act-cyclus herkennen. Zij zullen hierin de High Level Structure ('HLS') herkennen die ISO toepast in verschillende normen die betrekking hebben op het inrichten van een management-systeem.

Certificering

Organisaties kunnen hun ISMS laten certificeren, waarmee zij een instrument in handen hebben om te kunnen aantonen dat zij een werkwijze voor informatiebeveiliging hebben die is ingericht conform de norm. Dit instrument wordt met name gebruikt om aan diverse stakeholders (zoals klanten, aandeelhouders en toezichthouders) te kunnen laten zien dat informatiebeveiliging de nodige aandacht krijgt en dat dit door een onafhankelijke externe auditor is getoetst.

Om gecertificeerd te kunnen worden dient de organisatie minstens éénmaal aantoonbaar de plan-do-check-act-cyclus te hebben doorlopen. Bij de certificeringsaudit controleert de externe auditor of het ISMS conform de norm is opgezet, en of deze opzet ook in de praktijk wordt toegepast. Als het certificaat wordt toegekend, is dat voor een periode van drie jaar. In die periode wordt jaarlijks door een externe auditor middels een tussentijdse audit gecontroleerd of het ISMS nog steeds voldoet. Na drie jaar vindt een hercertificering plaats waarbij weer het volledige ISMS wordt getoetst.

Relatie tussen ISO 27001 en ISO 27002

Wie denkt dat ISO 27002 de opvolger is van ISO 27001, komt bedrogen uit. Beide normen behoren tot de 27xxx-reeks en hangen daarom samen met informatiebeveiliging, maar de aard en strekking van beide normen is anders. Waar ISO 27001 gaat over de inrichting van een managementsysteem voor informatiebeveiliging, bevat ISO 27002 maat-regelen om risico's in dit kader te beheersen. Kort samengevat schrijft ISO 27001 voor dat organisaties hun risico's ten aanzien van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie moeten beheersen via een werkwijze die is gestoeld op de plan-do-check-act-cyclus en dat zij op basis van een risicoanalyse passende maat-regelen moet selecteren en implementeren om die risico's te beheersen. ISO 27002 geeft een opsomming van mogelijke beheersmaatregelen, plus een richtlijn hoe die beheersmaatregelen kunnen worden toegepast. Een samenvatting van die beheersmaatregelen is in een annex van ISO 27001 opgenomen, waarmee ISO 27002 gekoppeld wordt aan ISO 27001.

Eerder dit jaar heeft ISO 27002 een behoorlijke update gehad. Net als bij wetgeving het geval is, is aanpassing van een norm een vrij bureaucratische en tijdrovende aangelegenheid. Omdat ISO 27002 via de annex van ISO 27001 ook onderdeel uitmaakt van die norm, moest ook de annex van ISO 27001 grondig worden herzien. Maar tegelijkertijd zijn ook enkele wijzigingen doorgevoerd in andere hoofdstukken van ISO 27001.

De belangrijkste wijzigingen van ISO 27001

Om met de minst spannende wijzigingen te beginnen, starten we met de wijzigingen die niet samenhangen met de wijzigingen van ISO 27002. ISO heeft kleine updates doorgevoerd in de High Level Structure, die het uitgangspunt vormt voor normen die betrekking hebben op het inrichten en onderhouden van managementsystemen. Omdat de vorige versie van ISO 27001 één van de eerste normen was die de HLS integreerde, zijn de wijzi-gingen erg beperkt. De wijzigingen kunnen vooral worden gevonden in taalgebruik en leesbaarheid. Zo zijn er correcties die sinds het uitkomen van de vorige versie zijn uitgebracht, nu integraal door-gevoerd in de nieuwe versie.

Nieuwe indeling

De grootste wijziging zit, zoals eerder gezegd, in de afstemming van ISO 27001 op ISO 27002. De meest in het oog springende wijziging is de nieuwe indeling die ISO 27002 (en dus de annex van ISO 27001) heeft gekregen. Waar de vorige versie nog veertien categorieën kende waarin de beheersmaatregelen waren ingedeeld, kent de nieuwe versie slechts vier categorieën. De cate-gorieën zijn ook anders ingedeeld, waarbij een logica is nagestreefd die het koppelen van beheersmaatregelen aan afdelingen of verant-woordelijkheidsgebieden eenvoudiger moet maken.

Een vergelijking:

Categorieën beheersmaatregelen oude versie	Categorieën beheersmaatregelen nieuwe versie
Informatiebeveiligingsbeleid	Organisatorische beheersmaatregelen
Organiseren van informatiebeveiliging	Mensgerichte beheersmaatregelen
Veilig personeel	Fysieke beheersmaatregelen
Beheer van bedrijfsmiddelen	Technologische beheersmaatregelen
Toegangsbeveiliging	
Cryptografie	
Fysieke beveiliging en beveiliging van de omgeving	
Beveiliging bedrijfsvoering	
Communicatiebeveiliging	
Acquisitie, ontwikkeling en onderhoud van informatiesystemen	
Leveranciersrelaties	
Beheer van informatiebeveiligingsincidenten	
Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	
Naleving	

Aantal beheersmaatregelen

Daarnaast is het aantal beheersmaatregelen teruggebracht, doordat een aantal beheersmaatregelen is samengevoegd. De oude versie kende in totaal 114 beheersmaatregelen; de nieuwe versie telt er 93.

Nieuwe beheersmaatregelen

Er zijn ook nieuwe beheersmaatregelen toegevoegd, in antwoord op de ontwikkelingen die de afgelopen jaren hebben plaatsgevonden binnen het domein van informatiebeveiliging. Het gaat in totaal om elf nieuwe beheersmaatregelen. Deze maatregelen leggen met name aandacht op preventie en monitoring. Hieronder volgt een opsomming van de nieuw toegevoegde beheersmaatregelen.

- Organisatorische beheersmaatregelen:
  - 5.7: Informatie en analyses over dreigingen
  - 5.23: Informatiebeveiliging voor het gebruik van clouddiensten
  - 5.30: ICT-gereedheid voor bedrijfscontinuïteit
- Fysieke beheersmaatregelen:
  - 7.4: Monitoren van de fysieke beveiliging
- Technologische beheersmaatregelen:
  - 8.9: Configuratiebeheer
  - 8.10: Wissen van informatie
  - 8.11: Maskeren van gegevens
  - 8.12: Voorkomen van gegevenslekken
  - 8.16: Monitoren van activiteiten
  - 8.23: Toepassen van webfilters
  - 8.28: Veilig coderen

Attributen van beheersmaatregelen

Een andere wijziging die in het oog springt, is het gebruik van attributen om beheersmaatregelen te kenmerken. Het doel hiervan is om meer overzicht te kunnen creëren, door beheersmaatregelen in overzichten te kunnen filteren of sorteren. Het staat organisaties vrij om de attributen naar eigen inzicht te gebruiken en om bijvoorbeeld bepaalde attributen te vervangen, of om 'eigen' attributen toe te voegen. De attributen die in de norm worden gebruikt, zijn:

1. **Type beheersmaatregel**. Dit attribuut beschrijft wanneer en hoe de maatregel leidt tot verandering van het risico waarop de maatregel is gericht. Typen beheersmaatregelen zijn preventief, detectief of corrigerend.
2. **Informatiebeveiligingseigenschappen**. Dit attribuut beschrijft aan welk kenmerk van informatie de beheersmaatregel bijdraagt. Kenmerken zijn beschikbaarheid, integriteit en vertrouwelijkheid.
3. **Cybersecurityconcepten**. Dit attribuut legt een verband tussen de beheersmaatregelen uit ISO 27002 (en de annex van ISO 27001) en cybersecurityconcepten uit een aanverwante norm (ISO/IEC TS 27110). Het gaat om identificeren, beschermen, detecteren, reageren en herstellen.
4. **Operationele capaciteiten**. Dit attribuut bekijkt de beheersmaatregelen vanuit het

perspectief van beroepsbeoefenaren op capaciteiten die nodig zijn om informatie te beschermen. Hierbij kan o.a. worden gedacht aan governance, personeelsbeveiliging, fysieke beveiliging, systeem- en netwerkbeveiliging, en beveiliging in leveranciersrelaties.

5. **Beveiligingsdomeinen**. Dit attribuut bekijkt beheersmaatregelen vanuit het oogpunt van vier domeinen, te weten governance & ecosysteem, bescherming, verdediging, veerkracht.

Impact van de wijzigingen op uw organisatie

Welke impact de wijzigingen in de norm op uw organisatie heeft, is o.a. afhankelijk van uw relatie tot de norm. Heeft uw organisatie een gecertificeerd managementsysteem, dan is er werk aan de winkel om uw ISMS aan te passen op de nieuwe norm. Maar ook wanneer uw organisatie zelf niet gecertificeerd is, kunt u impact ervaren.

Gevolgen voor certificering

Als uw organisatie een ISMS heeft dat gecertificeerd is conform ISO 27001, dient het ISMS op de nieuwe norm te worden afgestemd. Hiervoor geldt een transitieperiode van 36 maanden vanaf het moment van publicatie.[2] Binnen deze periode moeten dus het beleid, de procedures en andere documentatie worden bijgewerkt in lijn met de nieuwe versie van de norm. En de aangepaste opzet dient vanzelfsprekend ook zo te worden geïmplementeerd dat zij ook in praktijk wordt gebracht.

Kortom: het certificaat moet vóór 1 november 2025 zijn omgezet naar de nieuwe versie.

2. Op het moment van schrijven is de Engelstalige norm van ISO 27001 reeds gepubliceerd (publicatiedatum: oktober 2022). De Nederlandse vertaling is op het moment van schrijven nog niet gepubliceerd.

Het ligt voor de hand om de overstap naar de nieuwe versie gelijk te laten vallen met uw hercertificering.[3] Het is echter ook mogelijk om de overgangsaudit te laten plaatsvinden tijdens een tussentijdse audit.[4] Tot slot kan ook een 'losse' overgangsaudit worden gepland. Dat is echter de minst praktische oplossing, omdat dit tot een (onnodige) extra audit leidt, wat onnodig impact op de bedrijfsvoering heeft.

3. Zie ook par. 'Certificering': een certificaat heeft een geldigheid van drie jaar, waarbij jaarlijks een tussentijdse audit plaatsvindt. Na die drie jaar wordt een hercertificeringsaudit uitgevoerd.
4. Idem.

Gevolgen voor organisaties die leveren aan gecertificeerde partijen

Als uw organisatie producten of diensten levert aan klanten die gecertificeerd zijn, kunt u vanuit uw klanten impact verwachten. Zij zullen wijzigingen in hun ISMS en beheersmaatregelen gaan doorvoeren, die direct of indirect bij u terecht komen. Zo las u in de paragraaf 'Nieuwe beheersmaatregelen' dat er meer aandacht komt voor het gebruik van clouddiensten en monitoring, maar ook voor andere aandachtsgebieden waar uw klanten u wellicht bij nodig hebben. Om niet overvallen te worden door vragen van uw klanten, verdient het aanbeveling om in kaart te brengen welke aspecten van de norm raakvlak hebben met de diensten of producten die u levert. Zo kunt u inzichtelijk maken met welke vragen klanten zich waarschijnlijk tot u gaan richten, en daarop anticiperen. Door dit tijdig te doen kunt u niet alleen tijd en kosten besparen, maar kunt u ook een commercieel voordeel behalen door uw diensten en producten af te stemmen op de verwachtingen, eisen en wensen van uw klanten.

Gevolgen voor organisaties die afnemen van gecertificeerde partijen

Als uw organisatie zelf niet gecertificeerd is, maar wel klant is van partijen die gecertificeerd zijn, kunt u verwachten dat deze leveranciers bepaalde wijzigingen doorvoeren. Deze kunt u o.a. terugvinden in de Verklaring van Toepasselijkheid (een overzicht van de beheersmaatregelen uit de norm, waarbij is beschreven of die maatregel toepasselijk is voor desbetreffende organisatie).

De wijzigingen in de norm kunnen leiden tot aanpassingen in de producten of diensten die u afneemt, of in de afspraken en voorwaarden die daarvoor gelden. Welke impact dit voor uw organisatie heeft is uiteraard afhankelijk van (o.a.) de diensten en producten die worden afgenomen, de wijzigingen die worden doorgevoerd, en de relatie die u hebt met desbetreffende leverancier.

Hoe nu verder?

De transitieperiode van 36 maanden lijkt lang, maar om onnodig extra werk te voorkomen adviseren wij organisaties die zelf gecertificeerd zijn om op tijd te beginnen met de overgang. Dit begint met het kiezen van een logisch moment voor de overgang en met het in kaart brengen wat daarvoor moet gebeuren.

Theoretisch gezien zouden de wijzigingen in uw ISMS vooral in de documentatie moeten zitten en niet zozeer in het implementeren van aanvullende beheersmaatregelen. Ook in de huidige versie van de norm vormt immers de risicoanalyse het uitgangspunt voor de selectie en implementatie van beheersmaatregelen. Als u dit op orde hebt, beschikt u dus al over de beheersmaatregelen die u nodig hebt om de risico's voor uw organisatie in toom te houden. Zodoende zal uw aandacht vooral moeten uitgaan naar het bijwerken van documentatie. Het kan echter ook goed zijn dat de nieuwe beheersmaatregelen uit de norm een nieuwe blik werpen op uw risico's en de behandeling daarvan. In dat geval is er ook werk aan de winkel op het niveau van de beheersmaatregelen.

Raoul van de Laak
Information security consultant

Sanne van Esterik
Juridisch werkstudent

Cloud

De European Accessibility Act (EAA): Nieuwe regels voor digitale toegankelijkheid

Op dit moment zijn er in Europa circa 80 miljoen mensen met een beperking. In Nederland gaat het om circa 4 miljoen mensen. Hierdoor kunnen websites of apps voor hen minder toegankelijk zijn. Het is van belang dat, mede in het licht van inclusiviteit, ook mensen met een fysieke, mentale, intellectuele of zintuiglijke beperking toegang hebben tot (digitale) producten en diensten. Vandaar dat in juni 2019 de European Accessibility Act (EAA) is aangenomen door de lidstaten van de Europese Unie.
Op dit moment is digitale toegankelijkheid al verplicht voor alle (semi-)overheidsinstanties, zoals vastgelegd in de Richtlijn 2016/2102, de Wet digitale overheid en het Tijdelijk besluit digitale overheid. De EAA zorgt er dus voor dat niet langer alleen overheidsinstanties aan toegankelijkheidsvoorschriften moeten voldoen, maar ook producten en diensten van bedrijven en andere organisaties. De regels van de EAA gaan gelden vanaf juni 2025.

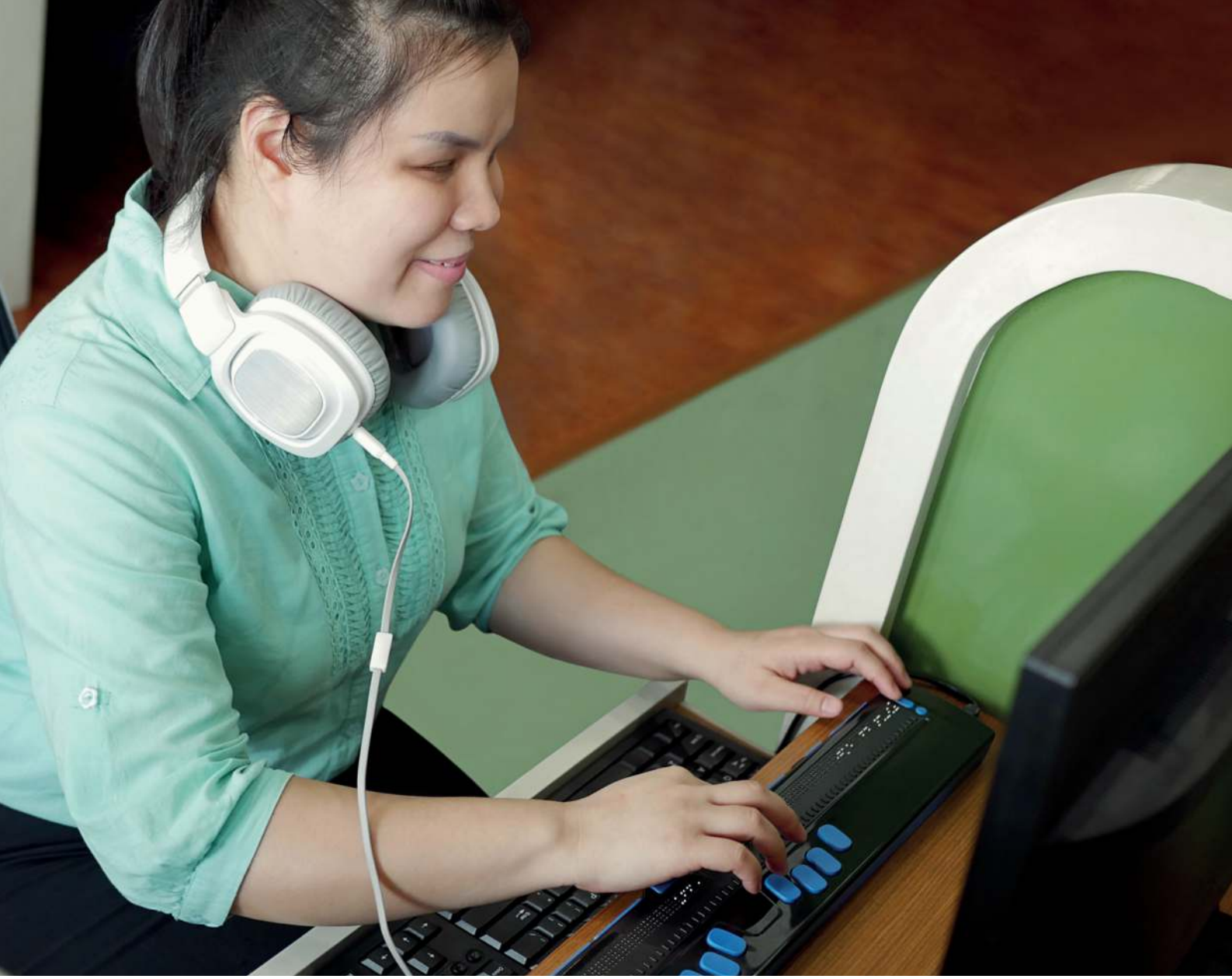
Reikwijdte van de EAA

Producten en diensten aan consumenten

In de EAA staan zoals gezegd verschillende toegankelijkheidsvoorschriften.
Deze verplichtingen zijn van toepassing op de volgende producten en diensten:

- computers en besturingssoftware;
- e-books;
- webshops;
- pinautomaten, ticketservices en incheckmachines;
- smartphones
- TV-apparatuur met betrekking tot digitale televisiediensten;
- Telecommunicatiediensten;
- Audiovisuele mediadiensten, zoals Netflix, Videoland en Spotify;
- Online en offline diensten die te maken hebben met transport, zoals kaartjesautomaten, apps en websites;
- Alle financiële diensten, zoals internetbankieren.

De regels gelden alleen als de producten en diensten worden aangeboden aan consumenten.



Aanbieders, fabrikanten, importeurs en distributeurs

Niet alleen de aanbieders van de bovenstaande producten en diensten moeten rekening houden met de toegankelijkheidsvoorschiften. De EAA bevat namelijk ook verplichtingen aan fabrikanten, gemachtigden, importeurs en distributeurs van de producten. Zo moeten fabrikanten ervoor zorgen dat de producten zo zijn ontworpen dat zij voldoen aan de toegankelijkheidsvoorschriften en mogen importeurs alleen conforme producten in de handel brengen.

Uitzonderingen

De EAA bevat een aantal uitzonderingssituaties waarvoor de toegankelijkheidsvoorschriften niet gelden:

- **Micro-ondernemingen**: Ondernemingen die diensten aanbieden met minder dan 10 werknemers of een omzet lager dan 2 miljoen euro per jaar hoeven niet aan de regels te voldoen.
- **Fundamentele wijziging of onevenredige last**: De toegankelijkheidsvoorschriften zijn ook niet van toepassing als deze een ingrijpende wijziging van een product of dienst vereisen. Hetzelfde geldt als de voorschriften een onevenredige last opleveren voor de betrokken marktdeelnemers (bijvoorbeeld aan een marktdeelnemer extra buitensporige organisatorische of financiële last opleggen). In principe zullen alleen kleinere ondernemingen hierop een beroep kunnen doen.

De toegankelijkheidsvoorschriften

Het belangrijkste onderdeel van de EAA zijn de toegankelijkheidsvoorschriften die gaan gelden voor de bovengenoemde producten en diensten. Uitgangspunt is hierbij dat de producten en diensten zo worden ingericht/aangeboden dat ze toegankelijk zijn voor mensen met een handicap. Er zijn vier beginselen van toegankelijkheid die van belang zijn voor de EAA:

1. **Waarneembaar**: De informatie en componenten van de gebruikersinterface moeten zodanig aan gebruikers worden gepresenteerd dat zij kunnen worden waargenomen.
   Voorbeeld: het moet duidelijk zijn hoe/waar een gebruiker de geschreven tekst kan laten voorlezen via een schermlezer of laten vertalen naar braille.
2. **Bedienbaar**: De gebruiker moet de interactieve elementen van een website of app daadwerkelijk kunnen gebruiken.
   Voorbeeld: als er voorlees-optie via schermlezer wordt aangeboden, dan moet die ook daadwerkelijk werken.
3. **Begrijpelijkheid**: De informatie of gebruiksinterface moet begrijpelijk zijn.
   Voorbeeld: Er moet een logische structuur in website of app zitten.
4. **Robuust**: De inhoud (van informatie of navigatiestructuur van een website) moet universeel en blijvend toegankelijk zijn.

Bij de concrete voorschriften wordt een onderscheid gemaakt tussen enerzijds producten en anderzijds diensten. Onderstaande zijn slechts enkele voorbeelden van de verplichtingen; de bijlage bij de EAA bevat een lijst alle voorschriften.

Producten

- **Informatieverstrekking**: De informatie over het gebruik van het product moet bijvoorbeeld beschikbaar zijn gesteld via meer dan één zintuigelijk kanaal, begrijpelijk zijn en gepresenteerd worden met lettertypes in de juiste grootte en vorm.
- **Gebruikersinterface en functionaliteit**: Als een product bijvoorbeeld visuele elementen heeft, dan moeten er functies zijn voor flexibele vergroting, helderheid en contrast. Ook moeten e-lezers voorzien zijn van technologie voor het omzetten van tekst in spraak.

Diensten

- **Informatie over het functioneren van de dienst**: Deze informatie moet beschikbaar worden gesteld via meer dan één zintuigelijk kanaal, begrijpelijk zijn en gepresenteerd worden met lettertypes in de juiste grootte en vorm.
- **Websites en apps**: Websites en apps van diensten die onder de EAA vallen moeten toegankelijk worden gemaakt op een consistente en geschikte manier waardoor ze waarneembaar, bedienbaar, begrijpelijk en robuust zijn.
- **Callcenters**: Ondersteunende diensten zoals callcenters en helpdesk moeten informatie verstrekken over de toegankelijkheid van een bepaalde dienst.

Gevolgen voor webshops

Bovenstaande verplichtingen zullen ook impact hebben op webshops. In de EAA worden “e-handelsdiensten” namelijk expliciet genoemd als dienst die onder het bereik van de richtlijn vallen. Dat betekent onder andere dat de website van een webshop dusdanig waarneembaar, bedienbaar, begrijpelijk en robuust moet zijn. Bovendien geldt enkel voor webshops ook dat de methoden van identificatie, elektronische ondertekening en betalingsdiensten aan deze vier begrippen moet voldoen. In de komende tijd zal duidelijk(er) worden hoe deze begrippen moeten worden ingevuld.

Conclusie

Het is belangrijk om goed te beoordelen of de aangeboden producten en diensten onder het bereik van de EAA vallen en aan welke concrete toegankelijkheidsvoorschriften moet worden voldaan. De voorschriften kunnen namelijk een flinke impact hebben op aanbieders van de producten en diensten die onder de EAA vallen.

Internetrechtspraak

Raad van State vernietigt boeteoplegging VoetbalTV

(Raad van State 27 juli 2022)

VoetbalTV is een inmiddels failliete website die opnames en uitzendingen van amateurvoetbalwedstrijden verzorgde. Hierbij werden beelden van onder andere minderjarige voetballers beschikbaar gesteld. De Autoriteit Persoonsgegevens (hierna: AP) stelde dat dit een privacyschending opleverde. In beroep werd de boeteoplegging door de rechtbank vernietigd. Ook in hoger beroep schaart de Raad van State (hierna: RvS) zich niet achter de boeteoplegging.

Volgens de RvS heeft de AP de boete onvoldoende gemotiveerd. De AP had het beroep van VoetbalTV op een gerechtvaardigd belang op basis van art. 6 lid 1 sub f verworpen. De AP stelt dat het commerciële belang van VoetbalTV nooit een gerechtvaardigd belang met zich mee kan brengen, maar de rechtbank is hier niet in meegegaan. De RvS gaat hier in hoger beroep evenmin in mee. De RvS stelt dat de AP ten onrechte niet verder heeft gekeken dan de eerste stap van haar toetsing, namelijk het kijken naar gerechtvaardigd belang. Ook was de toetsing te beperkt, zo stelt de RvS. De belangen die VoetbalTV heeft geopperd zijn ten onrechte niet zijn meegewogen in de besluitvorming van de AP. VoetbalTV stelt namelijk een aantal belangen die breder gaan dan enkel het commerciële belang, zoals het dienen van technische analyses door trainers en het vergroten van het genot voor voetballiefhebbers en spelers die graag de wedstrijden (terug)kijken. De RvS stelt dat de AP, door het ontbreken van motivering en onderzoek naar deze stappen, onzorgvuldig haar besluit heeft genomen en dat de boeteoplegging hierdoor niet in stand kan blijven. Zie de noot op pagina 34.

https://bit.ly/3G4Lwsy

Publiceren persoonsgegevens medewerkers Belastingdienst

(Gerechtshof Den Haag 9 augustus 2022)

Appellant heeft zonder toestemming gegevens van twee medewerkers van de belastingdienst op een website en op Twitter openbaar gemaakt. De rechtbank heeft appellant veroordeeld alle persoonsgegevens te verwijderen en een verbod gegeven om zonder expliciete toestemming persoonsgegevens van ambtenaren te publiceren. Het Hof maakt in hoger beroep een belangenafweging tussen het recht op vrijheid van meningsuiting uit artikel 7 EVRM en het recht op privacy uit artikel 8 EVRM. Het Hof is van mening dat het recht op privacy van de ambtenaren in dit geval zwaarder moet wegen. Het Hof beperkt het verbod wel. Deze strekt zich alleen uit over de medewerkers die betrokken waren bij de gebeurtenissen rondom de camping. Het verbod geldt niet meer voor alle ambtenaren met een bestuurlijke functie, zoals de rechtbank had opgelegd.

https://bit.ly/3voNqzx

GGD-medewerker veroordeeld voor datadiefstal uit coronasysteem

(Rechtbank Midden-Nederland 5 september 2022)

Verdachte, een medewerker van de GGD, heeft honderden keren gegevens uit dossiers van de GGD gehaald en deze in een aantal gevallen via WhatsApp gedeeld. Daarnaast zocht hij samen met twee medeverdachten persoonsgegevens van bekende Nederlanders op. Dit alles deed hij zonder dat hij bevoegd was om de dossiers in te zien.

De rechtbank veroordeelt verdachte voor computervredebreuk. Verdachte was weliswaar geautoriseerd, maar onbevoegd om de gegevens van de personen op eigen initiatief op te zoeken, zo geeft de rechtbank aan. Daarnaast wist verdachte dat hij zich in een beveiligd systeem bevond en heeft hij doelbewust de beveiliging van dat systeem doorbroken, zonder dat zijn werkzaamheden dit van hem

vergden. De rechtbank legt verdachte een voorwaardelijke gevangenisstraf van één maand en een onvoorwaardelijke taakstraf van 120 uur op.

https://bit.ly/3i0MYV4

Rechtbank toetst bestelknop bol.com

(Rechtbank Noord-Nederland 13 september 2022)

Bol.com meent op grond van een gesloten koopovereenkomst met de consument recht te hebben op het aankoopbedrag van een geleverd matras. Voor een op afstand gesloten koopovereenkomst gelden informatieverplichtingen waar bol.com aan moet voldoen. Dit betreft onder meer de verplichting uit art. 6:230v lid 3BW. Dit betekent dat het bestelproces van bol.com zo moet worden ingericht dat het duidelijk is voor de consument dat de bestelling een betalingsverplichting inhoudt.
De rechter toets de tekst 'bestelling plaatsen' aan het criterium dat het Hof van Justitie van de Europese Unie in het arrest 'Fuhrmann' heeft geformuleerd. De kantonrechter komt tot de conclusie dat het woord 'bestellen' van een product in de Nederlandse taal doorgaans met een betalingsverplichting in verband wordt gebracht. De kantonrechter oordeelt dat de knop met 'bestelling plaatsen' voldoende moet zijn om te realiseren dat een betalingsverplichting wordt aangegaan.

https://bit.ly/3jvJuu1

Verdachte veroordeeld voor installeren spyware op laptop ex-partner

(Rechtbank Midden-Nederland 23 september 2022)

Verdachte heeft zijn ex-partner een Macbook Pro cadeau gedaan en hierop, zonder medeweten van de ex-partner, spyware geïnstalleerd. Hij had toegang tot de webcam en microfoon van de laptop, en ook tot alle toetsaanslagen en bestanden die op het systeem stonden. Daarnaast exporteerde verdachte grote hoeveelheden data naar een online dashboard, waar hij deze gegevens van zijn ex-partner kon inzien.
Volgens de rechtbank wist de ex-partner niet dat deze spyware op de laptop geïnstalleerd was. De rechtbank volgt het verweer van verdachte dat het in de gaten houden van elkaar deel uitmaakte van de relatie niet. Met zijn handelen heeft verdachte een grote inbreuk gemaakt op de privacy van het slachtoffer en deze inbreuk heeft over een lange periode plaatsgevonden. De rechtbank rekent verdachte dit aan en veroordeelt verdachte tot een taakstraf van tachtig uur.

https://bit.ly/3WTDGsT

Geen schending zorgplicht bij belegging in crypto als vriendendienst

(Rechtbank Noord-Holland 12 oktober 2022)

Gedaagde is een kennis van eiser en handelt met het vermogen van eiser in cryptovaluta. Op een zeker moment zijn de cryptorekeningen van eiser leeggehaald. De gedaagde geeft aan dat de cryptorekeningen van eiser zijn gehackt en daardoor zijn leeggehaald. Eiser betwist dit en is van mening dat gedaagde zijn zorgplicht heeft geschonden en spreekt hem aan op grond van een tekortkoming in de nakoming van de overeenkomst.
De rechtbank oordeelt dat er geen sprake is van een bijzondere zorgplicht, omdat gedaagde geen professionele beleggingsdienstverlener is. Dit wordt volgens de rechtbank bevestigd door de vriendschappelijke wijze van omgang tussen de partijen. Bovendien heeft gedaagde voldoende beveiligingsmaatregelen genomen met betrekking tot de cryptoaccounts. Het betreffen beveiligingsmaatregelen die in het algemeen bekend zijn en aanvaard worden door particuliere cryptohandelaren. Om deze redenen trekt de rechtbank de conclusie dat gedaagde zijn zorgplicht tegenover eiser niet heeft geschonden. Met betrekking tot de hack geeft de rechtbank aan dat enkel het feit dat enkele e-mailaccounts van gedaagde niet beveiligd waren, onvoldoende is om te kunnen spreken van onrechtmatig handelen door de gedaagde. Het beveiligen van de e-mailaccounts was tussen partijen niet besproken en ook is niet gebleken dat een dergelijke beveiliging in het algemeen gebruikelijk is, zo stelt de rechtbank.

https://ap.lc/xgKk1

Internetprovider hoeft brieven niet door te sturen aan illegale downloaders

(Gerechtshof Arnhem 13 oktober 2022)

Stichting Brein weet door eigen onderzoek dat er vanaf bepaalde IP-adressen illegaal wordt gedownload en geüpload via BitTorrent. Stichting Brein wil graag waarschuwingsbrieven sturen om de illegale handelingen te stoppen. Alleen de internetproviders, waaronder Ziggo, weten de NAW-gegevens die bij de IP-adressen horen. Stichting Brein heeft de internetproviders gevraagd om namens hen de inbreukmakers waarschuwingsbrieven te sturen. Ziggo wil hier niet aan meewerken.

De conclusie van het hof is dat niet kan worden aangenomen dat op Ziggo een rechtsplicht rust om Breins waarschuwingsbrieven door te sturen aan klanten die houder zijn van een IP-adres dat uit de steekproef komt. De weigering van Ziggo om mee te werken is niet onrechtmatig en Ziggo is niet aansprakelijk voor mogelijk daaruit voortvloeiende schade. Dit zou anders kunnen zijn als het opvragen van de NAW-gegevens de enige manier zou zijn om een civiele procedure te kunnen starten. In dat geval zou sprake kunnen zijn van het onthouden van effectieve rechtsbescherming. Van die situatie is nu geen sprake, omdat het slechts gaat om het verzenden van waarschuwingsbrieven, zo stelt het hof.

Daarnaast heeft Ziggo geen grondslag uit de AVG om de gegevens te verwerken. Ook om die reden kan niet van Ziggo worden gevraagd om medewerking te verlenen aan het verzoek van Stichting Brein.

https://bit.ly/3YPxa8h

Ziekenhuis aansprakelijk voor inzien patiëntendossier

(Rechtbank Zeeland-West Brabant 21 september 2022)

Eiseres is diverse malen als patiënt behandeld in het Bravis Ziekenhuis in Roosendaal. De ex-partner van eiseres heeft een boek geschreven waarin hij de echtscheiding tussen hem en eiseres beschrijft. In dit boek staan ook medische gegevens van eiseres. Deze huidige partner was tussen 2007 en 2018 werkzaam in het Bravis Ziekenhuis. Eiseres stelt het Bravis Ziekenhuis aansprakelijk voor de schade die zij heeft geleden doordat het ziekenhuis haar medische gegevens onvoldoende heeft beschermd.

De rechtbank is van oordeel dat het Bravis Ziekenhuis aansprakelijk is voor de schade die door eiseres is geleden. Volgens de rechtbank heeft het ziekenhuis geen passende maatregelen genomen met betrekking tot de controle van de logging in patiëntendossiers. De controle van logbestanden betreft een zeer belangrijke beveiligingseis als het gaat om het beschermen van persoonlijke medische gegevens, zo stelt de rechtbank. In de situatie van eiseres is haar patiëntendossier over een aantal jaren veelvuldig ingezien. Er is om deze reden niet voldaan aan de normen die hiervoor gelden en aan artikel 32 AVG.

https://bit.ly/3Wy9zXZ

Uitlatingen in WhatsAppgroep niet onrechtmatig

(Rechtbank Den Haag 25 oktober 2022)

Gedaagden hebben een aannemingsovereenkomst met eiser met als doel het plaatsen van een aantal dakkappellen. De gedaagden zijn ontevreden over de werkzaamheden en er is een WhatsAppgroep opgericht waarin negatieve uitlatingen over eiser zijn gedaan. Ook hebben gedaagden in deze WhatsAppgroep klanten van eiser bewogen om hun relatie met eiser te verbreken.

Volgens de rechter zijn de uitlatingen door gedaagden in de WhatsAppgroep als zodanig niet onrechtmatig aan te merken. De WhatsAppgroep is een besloten groep en alleen de leden van de WhatsAppgroep kunnen de daarin gedeelde berichten lezen. Bovendien is het voor de leden van de groep vrij om binnen die groep ervaringen en meningen over eiser met elkaar te delen. De rechtbank geeft aan dat er niet is gebleken dat gedaagden door de WhatsAppgroep berichten over oplichting of fraude geopenbaard hebben met als doel om schade toe te brengen aan eiser. Evenmin is gebleken dat gedaagden in de WhatsAppgroep klanten van eiser ertoe hebben bewogen om hun relatie met eiser te verbreken.

https://bit.ly/3C9h13K

YouTube-filmpjes door influencers geen schending vaststellingsovereenkomst
(Rechtbank Noord-Holland 9 november 2022)
Gedaagde is de voormalige buurman van eiseres. Zij hadden een vaststellingsovereenkomst gesloten waarin onder meer werd bedongen dat gedaagde zijn weiland met paardenbak niet bedrijfsmatig mocht exploiteren. De gedaagde moest deze verplichting ook aan zijn rechtsopvolger opleggen. Op het schenden van deze overeenkomst rust een boete. Eiseres is van mening dat gedaagde deze boete moet betalen, omdat de huidige bewoners als influencers gebruikmaken van de paardenbak. De huidige bewoners van het perceel zijn influencers die elkaar filmen bij alledaagse of speelse activiteiten, zoals het houden en verzorgen van hun eigen paarden, zo stelt de rechtbank. Zij zetten deze filmpjes vervolgens online. Het feit dat zij hiermee mogelijk geld verdienen, betekent niet dat er sprake is van bedrijfsmatige exploitatie van de paardenbak, overweegt de rechtbank. Zij hadden de filmpjes ook online kunnen zetten zonder dat er iemand geïnteresseerd zou zijn.

https://bit.ly/3C43ACb

Het NRC hoeft geen rectificatie te plaatsen
(Rechtbank Amsterdam 18 november 2022)
Eisers werken als adviseur bij Taxeco. Na enkele gebeurtenissen worden zij vervolgd wegens poging tot afdreiging. Over deze gebeurtenissen heeft NRC een kritisch artikel geschreven waarin onder meer wordt gesproken over eisers. Eisers zijn van mening dat NRC het artikel moet rectificeren, maar NRC gaat hier niet in mee. Vervolgens eisen eisers bij de rechtbank dat NRC veroordeelt moet worden tot het rectificeren van het artikel. De rechtbank weigert het gebod tot rectificatie. De voorzieningenrechter stelt dat eisers aangemerkt kunnen worden als publieke figuren. Deze positie brengt met zich mee dat eisers meer kritiek dulden te hebben dan een willekeurig persoon. Daarnaast vindt de negatieve afschildering voldoende steun in de feiten, zodat het artikel niet onrechtmatig is. Om deze reden valt het artikel binnen de grenzen van de journalistieke vrijheid.

https://bit.ly/3GqOYPO

Toestemming voor persoonsgegevens in openbare telefoongids
(Hof van Justitie van de Europese Unie 27 oktober 2022)
De klager in deze procedure is een abonnee van Telenet. Telenet opereert telefoondiensten in België. Telenet zendt de contactgegevens van haar abonnees door naar aanbieders van abonneelijsten. Het geschil richt zich met name op de vraag of het doorzenden van de contactgegevens valt onder de toestemming die door een abonnee is gegeven. Het Hof bevestigt dat de toestemming, zoals genoemd in art. 12 van richtlijn 2002/58, van een naar behoren geïnformeerde abonnee noodzakelijk is om zijn persoonsgegevens te kunnen publiceren in een openbare telefoongids. Deze toestemming vereist een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting van de betrokkene waaruit blijkt dat hij de verwerking van de persoonsgegevens aanvaardt. Het Hof voegt hieraan toe dat niet opnieuw toestemming van die abonnee hoeft te worden verkregen als wordt gewaarborgd dat de betrokken gegevens niet voor andere doeleinden zullen worden gebruikt dan die waarvoor zij met het oog op de eerste publicatie ervan zijn verzameld. Telenet mag de gegevens dus doorsturen naar andere aanbieders onder de voorwaarde dat dit met hetzelfde doel geschiedt als waar de toestemming voor is verkregen.

https://bit.ly/3C8c1MQ

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Privacy

Noot bij Raad van State 27 juli 2022 (Boete VoetbalTV)

Het definitieve oordeel voor VoetbalTV is gevallen: de Autoriteit Persoonsgegevens (AP) had niet op deze manier de voorgenomen videoregistraties mogen verbieden. De boete van een dik half miljoen is daarmee van tafel. Een nieuw oordeel zal er niet komen, want initiatiefnemers Talpa en KNVB trokken de stekker er ondertussen uit. Maar het is wel een goede bevestiging van de invulling van het "legitiem belang" uit de AVG.

Het doel van VoetbalTV was om een platform aan te bieden waar een ieder amateurvoetbalwedstrijden uit heel Nederland kon bekijken. Dergelijke beelden vallen natuurlijk onder de AVG, maar onduidelijk was of dit onder de grondslag eigen gerechtvaardigd belang gebracht kon worden. Men vroeg de AP om een voorafgaand onderzoek, en stapte naar de rechter toen dit maar bleef en bleef wachten. Uiteindelijk kwam het oordeel toch, en dat was verbazingwekkend: er was geen sprake van een dergelijk belang, want VoetbalTV had enkel "zuiver commerciële motieven".

Het standpunt van de AP schokte velen in juridisch privacyland, want in geen enkele wettekst of juridisch commentaar is ooit "zuiver commercieel" op zichzelf een criterium geweest om een verwerking af te keuren. Het is een factor die meeweegt in de belangenafweging die artikel 6 lid 1 sub f AVG vereist, en ook nog eens eentje waar een verwerkingsverantwoordelijke weinig aan heeft. Uiteindelijk gáát het om een afweging, en dat vereist meer dan enkel controleren of van één criterium sprake is.

De AP nam echter een nóg fundamenteler standpunt in. Om als "gerechtvaardigd" belang te tellen, moest het belang eigenlijk gewoon tot een wettelijk recht te herleiden zijn. Vrijheid van meningsuiting bijvoorbeeld, dat is een grondrecht dus daar kun je op gaan zitten. Vervolgens krijg je dan een belangenafweging die al dan niet pro-uitingsvrijheid kan uitvallen. Denk aan een reportage over een ernstig ongeval, de afweging zal dan zijn dat uitzenden kan (want nieuwswaarde) maar dat het slachtoffer geblurd wordt (want privacy). Volgens de AP was het voornemen van Talpa geen journalistieke productie en derhalve niet binnen het grondrecht van de uitingsvrijheid te brengen. Daarmee ontbrak ieder recht dat Talpa kon aanvoeren om haar belang te rechtvaardigen.

De Raad van State verwijst nu dit standpunt naar de prullenbak. In de rechtspraak van het Hof van Justitie van de Europese Unie wordt geen duidelijke omschrijving gegeven wat een gerechtvaardigd belang precies is en de interpretatie van de AP dat het - kort gezegd - zou moeten gaan om een rechtsbelang, is in die jurisprudentie dan ook niet

als zodanig terug te vinden. Het is juist dat het belang niet tegen de wet mag zijn (art. 5 lid 1 sub a AVG) maar daaruit volgt niet dat het dus tot een specifieke wet te herleiden moet zijn.

Uit het Fashion ID-arrest (ECLI:EU:C:2019:629) volgt dat het gerechtvaardigd belang een open norm is waarbij te allen tijde een driestappentoets moet worden gevolgd. De eerste stap is dat het belang dat VoetbalTV nastreeft een gerechtvaardigd belang is. Als dat zo is, moet vervolgens worden beoordeeld of de verwerking van de persoonsgegevens noodzakelijk is voor de behartiging van dat gerechtvaardigde belang (de tweede stap). Daarbij wordt getoetst aan de proportionaliteit en subsidiariteit: is de inbreuk voor de betrokkenen in verhouding tot het met de verwerking te dienen doel en kan het doel op een minder voor de betrokkenen nadelige wijze worden bereikt? De derde stap is dat er een afweging moet plaatsvinden tussen de belangen van de verantwoordelijke en de betrokkenen.

De Raad van State ontwijkt de discussie of een “zuiver commercieel belang” reden genoeg kan zijn om een verwerking af te wijzen. Zij ziet in de documentatie van VoetbalTV namelijk meer dan enkel zo’n commercieel belang: spelers en trainers kunnen beelden gebruiken om de training effectiever te maken, familie en vrienden krijgen zo meer binding met de speler en zijn/haar team, en het kanaliseren van dergelijke beelden op een privacywaarborgende manier om zo willekeurig verspreiden door derden af te remmen. Gelet op de aard van de activiteiten van VoetbalTV - het maken van beelden van voetbalwedstrijden en deze ter beschikking stellen aan derden, waaronder degenen die in beeld gebracht willen worden - is de verwerking van persoonsgegevens noodzakelijk voor meer dan alleen de commerciële belangen van VoetbalTV.

De AP heeft hiermee inderdaad een gebrekkig besluit genomen. Zij zal een nieuw besluit moeten nemen, zij het dat dit niet doorgaat vanwege het faillissement van VoetbalTV. Maar een volgende ondernemer staat nu sterker.

Privacy

Van onze blog ictrecht.nl/blog · 13 december 2022

Mag de EU eindelijk met de VS spelen? **Bijna!** Maar nog niet helemaal.

De Europese Commissie heeft een concept adequaatheidsbesluit voor het EU-US Data Privacy Framework[1] gepubliceerd! Hoezee! Het Privacy Shield heeft eindelijk (bijna, misschien) een opvolger. Een concept? Wat voor besluit? Wat kunnen we hier eigenlijk mee?

1. https://bit.ly/3jCbHQ3
2. https://bit.ly/3Q1BHAq
3. https://bit.ly/3Q39d9C
4. https://bit.ly/3VA9SQK
5. https://bit.ly/3i20Qyn

Data Privacy Framework?

Eerst een klein beetje context (mocht je dat niet willen, scroll door naar “En nu?”). Als je als organisatie binnen de Europese Economische Ruimte (“EER”) werkt en persoonsgegevens uitwisselt, of wil uitwisselen, met een organisatie daarbuiten, moet er gekeken worden of het niveau van gegevensbescherming op die andere locatie wel een beetje in orde is. De Algemene verordening gegevensbescherming (“AVG”) stelt voorwaarden aan zo’n “internationale data doorgifte”. Die voorwaarden zouden ervoor moeten zorgen dat de gegevensbescherming voor een individu “essentieel equivalent” is. Oftewel dat het enigszins dichtbij de AVG-lat komt.

Een van die manieren om dat te doen is als de Europese Commissie heeft onderzocht en besloten dat dat land een adequaat niveau van gegevensbescherming kent (artikel 45 AVG). Zij neemt daarover een adequaatheidsbesluit[2]. Als dat er is, kan je met een organisatie in dat derde land met een gerust hart persoonsgegevens doorgeven. Zoals dat nu bijvoorbeeld met het Verenigd Koninkrijk het geval is.

Op 7 oktober tekende President Biden de “Executive Order”[3] die toeziet op het versterken van waarborgen voor de Verenigde Staten op het gebied van inlichtingendiensten. Dat vormt de basis voor het EU-US Data Privacy Framework waar de Europese Commissie nu z’n zegje over heeft gedaan.

Het idee is dat deze “EU-US DPF” de zorgen wegneemt die het Hof van Justitie van de Europese Unie uitte[4] over hoe de VS met persoonsgegevens van Europese burgers omgaat.

En nu?

De Europese Commissie publiceerde een concept adequaatheidsbesluit van 134 pagina’s. Daarin staat waarom de Europese Commissie de EU-US DPF adequaat acht in de zin van artikel 45 AVG.

Caroline van Ekeren
Juridisch adviseur

De belangrijkste wijzigingen waar naar is gekeken gaan over:

- de mogelijkheid voor Europese burgers bezwaar te maken in geval van surveillance door de Amerikaanse overheid door het gebruik van een tweelaags mechanisme:
  - de eerste laag is de “Civil Liberties Protection Officer”. Die is verantwoordelijk dat de Amerikaanse inlichtingendiensten in lijn met privacy en mensenrechten te werk gaan, en kan je klachten bij indienen als Europees burger;
  - de tweede laag is de nieuwe “Data Protection Review Court” waar je in beroep kan gaan als de beslissing van de “Civil Liberties Protection Officer” je niet zint.
- wanneer Amerikaanse inlichtingendiensten surveillance kunnen inzetten. Dit was volgens het Hof van Justitie van de Europese Unie te breed. In het nieuwe EU-US DPF zou noodzakelijkheid en proportionaliteit beter geborgd moeten zijn, zoals we dat ook in ons Europees rechtssysteem zien in geval dat er een inbreuk op een grondrecht plaatsvindt (alleen als het écht niet anders kan, en het is voor bepaalde doeleinden, dan mag het).

Als deze beslissing finaal is, geldt dat als rechtmatige grondslag voor internationale data doorgifte met de VS.

Zijn we er al bijna?

Helaas niet. Dit concept wordt voorgelegd aan de Europese toezichthouders (European Data Protection Board) en vervolgens aan een commissie met vertegenwoordigers van de EU lidstaten. Als sluitstuk moet het Europees Parlement nog zijn zegen geven voordat de Europese Commissie dit adequaatheidsbesluit mag adopteren, en het in werking treedt als rechtmatige basis voor internationale data doorgifte.

Lang verhaal kort: het gaat op z’n minst nog maanden duren voordat er gemakkelijker persoonsgegevens met de VS gedeeld kunnen worden. Het is wat dat betreft een stap in de goede richting. Maar Schrems is de messen ondertussen ook weer aan het slijpen[5].

Wij houden de ontwikkelingen in ieder geval in de gaten!

Opleiding

Senior Specialist ICT-recht

ICTRECHT ACADEMY

Verdiep uw kennis en kunde als **Senior Specialist ICT-recht**

start: april 2023 · duur: 1 jaar

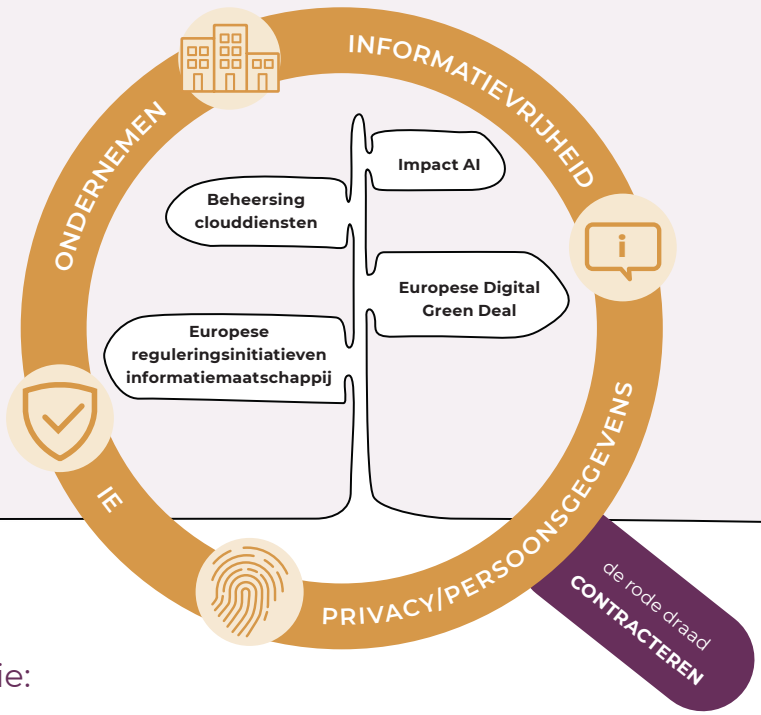
Specialiseer u tot Senior Specialist ICT-recht en verdiep uw kennis rondom technologie, AI en security. Leer fundamentele vragen diepgaand te beantwoorden, aannames uit het recht ter discussie te stellen en nieuwe technologie te vangen in bestaande en nieuwe regels tijdens deze eenjarige opleiding.

In het kort

- Flexibel leren (middels webinars en e-Learning) met 13 middagen op locatie in Utrecht;
- Gemiddeld beoordeeld met een 8;
- 56 PO punten. ICTRecht is NOvA-erkende opleidingsinstelling;
- Prijs: € 5.750 excl. BTW (inclusief boekenpakket).

Voor wie

Ervaren ICT-recht juristen die hun kennis en kunde willen verdiepen. U dient aantoonbaar te beschikken over gedegen voorkennis, bijvoorbeeld door het certificaat van de opleiding Specialist ICT-recht.



56 PUNTEN PO ADVOCATUUR

NEDERLANDSE ORDE VAN ADVOCATEN

Kijk hier voor meer informatie:

ictrecht.nl/academy/opleidingen/senior-specialist-ict-recht

ICTRECHT

Doe de **legal quickscan**

Benieuwd hoe uw juridische afdeling efficiënter ingericht kan worden? Weten waar de concrete innovatiekansen liggen? Laat de consultants van ICTRecht de legal quickscan uitvoeren voor uw organisatie en u komt erachter.

Met de quickscan geven wij - aan de hand van een aantal korte interviews met max. 3 van uw medewerkers - inzicht in de status van uw organisatie en op welke wijze er winst te behalen valt met de inzet van de juiste technologie.

Na het uitvoeren van de quickscan ontvangt u een beknopt rapport met:

- De operationele status van de juridische afdeling.
- De innovatiekansen van de afdeling inclusief toelichting op de mogelijkheden rondom legal tech.

Meer weten? Ga naar:
ictrecht.nl/legal-tech/legal-quickscan

“ICTRecht is dé specialist
op het snijvlak van
Legal, Security en **Tech**.”

ICTRECHT

Amsterdam, Groningen, Eindhoven,
Maastricht, Enschede en Brussel

Meer informatie over hoe wij werken?
Bezoek **ictrecht.nl**