jaargang 9 • nummer 4 • okt 2021

ICTRecht in de praktijk

Legal tech:
hype of toekomst

Geld of je
bedrijfsgegevens

Uitwisseling
van patiëntgegevens:
de Wet
kwaliteitsregistraties zorg

ICTRECHT
adviesbureau

ICTRecht: praktisch en deskundig

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

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

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

Hier zijn wij goed in:

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

ICTRECHT
adviesbureau

Meer informatie over hoe wij werken? Bezoek ictrecht.nl

Index

Legal tech: hype of toekomst	4
Wet- en regelgeving	6
Geld of je bedrijfsgegevens	8
De technische implementatie van een cookiebanner, wat zijn de valkuilen?	12
Uitwisseling van patiëntgegevens: de Wet kwaliteitsregistraties zorg	16
Internetrechtspraak	20
Geld van de toekomst?	26
Noot bij HR 25 juni 2021 (Dutch Filmworks tegen Ziggo)	30
Van onze blog	32
ICTRecht Academy	38

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

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

Aan deze uitgave werkten mee:

Alisa Schurink Marketing adviseur
a.schurink@ictrecht.nl
Arnoud Engelfriet Algemeen directeur en Opleidingsdirecteur
a.engelfriet@ictrecht.nl
Beryl Hetharia Juridisch adviseur
b.hetharia@ictrecht.nl
Britt Telleman Opleidingscoördinator
b.telleman@ictrecht.nl
Jorien Zwaneveld Juridisch adviseur
j.zwaneveld@ictrecht.nl
Mark Zijlstra Legal consultant
m.zijlstra@ictrecht.nl
Martijn Michael Juridisch adviseur
m.michael@ictrecht.nl
Nicole Waaijer Marketing adviseur
n.waaijer@ictrecht.nl
Ruben van der Geest Juridisch adviseur
r.vandergeest@ictrecht.nl
Sanne Haumersen Legal assistant
s.haumersen@ictrecht.nl
Sari Jansen Juridisch adviseur
s.jansen@ictrecht.nl
Steven Ras Algemeen directeur
s.ras@ictrecht.nl
Valeria Brussé Juridisch adviseur
v.brusse@ictrecht.nl
Vivianne Vermeulen Juridisch adviseur
v.vermeulen@ictrecht.nl
Amanda Butterworth Grafisch ontwerper
info@amandabutterworth.com
Leonard Fäustle Stills & Motion Foto's ICTRecht
info@leonardfaustle.nl

Mark Zijlstra
Legal consultant

Legal tech Innovatie

Legal tech: hype of toekomst

Legal tech startups schieten als hip geklede paddenstoelen uit de grond, de Big 4 investeren veel geld in juridische technologie en elke enigszins ingelezen jurist meent dat er geen weg terug meer is. Legal tech is de toekomst. Inmiddels kun je een bibliotheek vullen met alle artikelen, boeken en studiemateriaal over Legal tech. Maar wat is nu daadwerkelijk de waarde van Legal tech? En is de hype terecht?

Doel en functie

Laten we bij de – vreemd genoeg regelmatig overgeslagen – startvraag beginnen: heeft een organisatie een goede reden om aan de slag te gaan met Legal tech? Legal tech is al enige tijd een hype, maar dat hoeft uiteraard niet te betekenen dat u hier als organisatie in mee hoeft te gaan. Innoveren om het innoveren zal niet leiden tot succesvolle resultaten.

Het is van belang vast te stellen wat het uiteindelijke doel en de functie van legal tech is binnen de organisatie. De voornaamste redenen om legal tech in te zetten, zijn het verbeteren van de (interne) processen en het vergemakkelijken van het werk van de jurist. Daarbij is het uiteindelijke doel – en dat wordt nog wel eens uit het oog verloren – het beter kunnen bedienen van de klant. Of het nu gaat om een interne bedrijfsjurist of een advocaat die zijn cliënt bijstaat, uiteindelijk is het de klant die gebaat is bij een goed functionerende juridische afdeling. Dit nog los van de stijgende behoefte naar een efficiëntere en transparantere juridische wereld.

Technologie en legal

De vervolgvraag is: wat voor oplossingen biedt legal tech hiervoor? En moet dit altijd iets ontzettend futuristisch of baanbrekends zijn? Absoluut niet. Legal tech is een erg breed begrip, dat lastig te vatten is. Legal tech hoeft zeker niet altijd te gaan om disruptieve innovatieve technologie. Het doembeeld dat juristen massaal thuis komen te zitten omdat zij vervangen zijn door intelligente software, of dat procederen over een aantal jaar alleen nog ten overstaan van een robotrechter kan, is onzin – in elk geval op de korte termijn.

Bij de inventarisatie of legal tech een oplossing kan bieden, is het daarom verstandig om niet alleen naar *cutting edge* technologie te kijken. Bestaande – oudere - technologie kan uitstekend dienstdoen als oplossing in het kader van legal tech. Soms biedt Microsoft Excel in eerste instantie een makkelijkere en zeker goedkopere oplossing dan specifiek ontwikkelde software. Daar komt bij dat beproefde legal tech-oplossingen normaliseren en ook niet

langer als innovatief worden gezien. Toch zijn deze voor sommige organisaties juist daarom erg geschikt: de technologie werkt.

Pas op de plaats

Met die kennis moet elke organisatie die op zoek gaat naar een oplossing in de vorm van legal tech, goed kijken naar de interne en externe processen. Als niet duidelijk is welke processen aanwezig zijn binnen de organisatie en waar de kansen liggen, is het ook lastig in te schatten welke verbeteringen er mogelijk zijn.

Legal tech-oplossingen zijn uitermate geschikt voor *commodity* werkzaamheden. Dit zijn repetitieve en veel voorkomende taken die voor een jurist weinig interessant zijn. Denk hierbij aan het beoordelen van een NDA. Het is belangrijk dat een NDA een aantal essentiële onderdelen bevat, maar het is voor de gemiddelde jurist geen uitdaging. Bij dergelijke werkzaamheden kan legal tech een deel van het proces vervangen of er in ieder geval bij ondersteunen. In de praktijk blijkt dat juristen meer van dat soort taken hebben dan zij in eerste instantie denken.

Meer winst

Om bij het voorbeeld van de NDA te blijven: de jurist is geholpen met het geautomatiseerd beoordelen van een NDA, omdat hij deze zo sneller kan verwerken. En er is nog veel meer winst te behalen. Bij grotere organisaties komt een NDA vaak binnen op een andere afdeling dan de juridische, bijvoorbeeld bij sales. De salesmanager heeft er belang bij de NDA zo snel mogelijk getekend te hebben en werpt alvast een eerste blik. Vervolgens zet hij deze door naar Legal, waar de beoordeling door drukte minimaal een dag op zich laat wachten. Vervolgens moet Sales de opmerkingen en suggesties beoordelen en duurt het in het meest gunstige geval twee dagen voordat de NDA wordt teruggestuurd.

Gebruik je een tool om NDA's geautomatiseerd te beoordelen, eventueel in combinatie met enkele *guidelines*, dan hoeft Legal niet meer betrokken te zijn bij dit proces. Hiermee wordt dus niet alleen tijd van de jurist gewonnen, maar kan ook de salesmanager sneller handelen. Zo zijn zowel interne als externe klanten sneller geholpen.

Succesvolle implementatie

Het beoordelen van de processen, het analyseren van de *risk appetite* en het opstellen van *guidelines* is de eerste stap naar succesvolle implementatie van een legal tech-oplossing. Zonder deze stap bestaat het risico dat lukraak software wordt aangeschaft waarvan na verloop van tijd blijkt dat het geen invloed heeft op het proces. Hiermee raken we direct een van de argumenten waarom organisaties niet meer investeren in legal tech: "Het kost veel tijd en uiteindelijk werkt het toch niet".

Om het doel en de functie van legal tech vast te stellen binnen de organisatie is het verstandig een scan te laten uitvoeren van de juridische afdeling. Hieruit zal duidelijk worden waar de kansen liggen en welke technologie geschikt is om de klant nog beter van dienst te zijn. Uiteraard spelen ook andere factoren als verander- en projectmanagement een belangrijke rol bij een succesvolle implementatie.

Valeria Brussé
Juridisch adviseur

Wet- en regelgeving

Wetsvoorstel Uitvoeringswet Cyberveiligheidsverordening

Op 18 mei 2021 werd het wetsvoorstel bij de Tweede Kamer ingediend voor de Uitvoeringswet van de Cyberveiligheidsverordening. Het wetsvoorstel strekt tot de uitvoering van de Verordening (EU) nr. 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatie- technologie en tot intrekking van Verordening (EU) nr. 526/2013 (hierna: de cyberbeveiligingsverordening) welke op 27 juni 2019 in werking is getreden. Het doel van de cyberbeveiligingsverordening is om door middel van een geharmoniseerde certificatiesystematiek de cyberbeveiliging in de Europese Unie te vergroten en de (digitale) interne markt te versterken. Door de uitvoeringswet wordt het mandaat van het Europees Agentschap voor Cyber Security (Enisa) versterkt. Verder wordt er een kader geïntroduceerd op het gebied van cyberbeveiligingcertificering. Daarnaast zal Nederland op grond van deze uitvoeringswet op termijn een cyberbeveiligingscertificeringsautoriteit aanwijzen, welke moet gaan toezien op de certificering van cyberbeveiliging.

https://bit.ly/3BQUXrQ

Wet kwaliteitsregistraties zorg

Op 1 juni 2021 ging de internetconsultatie voor het wetsvoorstel Wet kwaliteitsregistraties zorg van start. Het doel van het wetsvoorstel is om een wettelijke (verwerkings)grondslag te creëren voor kwaliteitsregistratie in de zorg (met uitzondering van de geestelijke gezondheidszorg). In de memorie van toelichting wordt benadrukt dat kwaliteitsregistraties van belang zijn voor de continue kwaliteit van de zorg. Het wetsvoorstel regelt dat het mogelijk wordt om (gepseudonimiseerde) (bijzondere) gegevens zonder toestemming te verwerken, zodat deze kunnen worden opgenomen in het kwaliteitsregister. Het Zorginstituut Nederland krijgt, door deze wet, de taak om het nieuwe openbare register voor kwaliteitsregistraties aan te leggen. De internetconsultatie is gesloten op 13 juli 2021.

https://bit.ly/3yS7nOi

Wijziging van de telecommunicatiewet in verband met de implementatie van Richtlijn (EU) 2018/1972 tot vaststelling van het Europees wetboek van elektronische communicatie (Implementatie Telecomcode)

Op 21 juni 2021 is een wetsvoorstel ingediend ter wijziging van de Telecommunicatiewet. De wijziging ziet op de implementatie van de 'Telecomcode' (Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek van elektronische communicatie). Dit wetsvoorstel strekt onder andere tot een uitbreiding van het begrip 'elektronische communicatiedienst' uit de Telecommunicatiewet. Op deze manier wordt de wet aangepast op het beginsel van technologieneutraliteit. Door de aanpassing van de wet kunnen diensten zoals WhatsApp en Skype hieronder worden geschaard en kunnen gebruikers van deze online diensten beter worden beschermd.

https://bit.ly/2WTWpv6

Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid)
Op 22 juni 2021 is een 'novelle' ingediend op het wetsvoorstel Wet digitale overheid. Het doel van deze novelle is om de bescherming van de privacy in de nieuwe wet beter uit te werken. Enkele punten uit de novelle zijn: het stellen van regels over informatieveiligheid, de verantwoordelijkheid voor het beheer van de voorzieningen en diensten binnen de generieke digitale overheidsinfrastructuur (GDI) en het regelen van de digitale toegang tot publieke dienstverlening voor burgers en bedrijven.

https://bit.ly/3tmH6H5

Wet verwerking persoonsgegevens coördinatie en analyse terrorismebestrijding en nationale veiligheid
Op 23 juni 2021 is het wetsvoorstel voor de Wet verwerking persoonsgegevens in het kader van coördinatie en analyse terrorismebestrijding en nationale veiligheid in consultatie gegaan. Het wetsvoorstel strekt ertoe om de minister van Justitie en Veiligheid meer bevoegdheden te geven op het gebied van terrorismebestrijding en bescherming van de nationale veiligheid. Zo regelt de wet onder andere een grondslag voor het verwerken van bijzondere persoonsgegevens. In het concept van de memorie van toelichting wordt toegelicht dat "het voor het duiden van fenomenen nodig is om het maatschappelijk discours te volgen, dus uitlatingen van ideologische of politie aard op internetfora en (social) media te monitoren en te duiden." De internetconsultatie werd gesloten op 30 juni 2021; het wetsvoorstel is momenteel aanhangig bij de Raad van State.

https://bit.ly/3h9uXjJ

Innovatiewet Strafvordering
Het wetsvoorstel Innovatiewet Strafvordering is op 24 juni 2021 ingediend en dient ertoe om verschillende onderdelen van het Wetboek van Strafvordering aan te passen in lijn met de huidige innovatie. Enkele voorstellen zijn: het erkennen van audiovisuele opnamen als wettig bewijsmiddel, zodat het mogelijk wordt om bijvoorbeeld een proces-verbaal van een opgenomen verhoor te gebruiken, om een regeling op te nemen die het mogelijk maakt om berichten die na inbeslagname van een geautomatiseerd werk (zoals een smartphone) binnenkomen voor een bepaalde periode mogen worden onderzocht in het kader van de opsporing en te voorzien in een regeling die het mogelijk maakt om na inbeslagneming netwerkzoekingen (het onderzoek in een geautomatiseerd werk dat zich elders bevindt) uit te voeren.

https://bit.ly/3tsBdYL

Wijziging Wet beveiliging netwerk- en informatiesystemen i.v.m. uitbreiding bevoegdheid Ministerie van Justitie en Veiligheid
Op 28 juni 2021 is het wetsvoorstel Wijziging Wet beveiliging netwerk- en informatiesystemen i.v.m. uitbreiding bevoegdheid Ministerie van Justitie en Veiligheid ingediend. Met dit nieuwe wetsvoorstel wordt beoogd om de bevoegdheden van het Nationaal Cyber Security Centrum (NCSC) uit te breiden. Hierdoor krijgt het NCSC de mogelijkheid om informatie over dreigingen en incidenten breder te delen. Dit betekent dat zij dit buiten rijksoverheidinstanties en organisaties in vitale sectoren ook kunnen delen met andere organisaties. Op deze manier kunnen zij inspelen op de informatie, en maatregelen nemen om incidenten te voorkomen of de gevolgen van die incidenten zo goed mogelijk te beperken. De consultatie voor dit wetsvoorstel staat open tot 23 augustus 2021.

https://bit.ly/3DQPG5z

Jorien Zwaneveld
Juridisch adviseur &
Information security consultant

Sanne Haumersen
Legal assistant

Security

Geld of je bedrijfsgegevens

Bijna elke organisatie is tegenwoordig afhankelijk van een digitale omgeving, bijvoorbeeld werken in de cloud of product- en dienstspecifieke software. Maar wat als door ransomware uw systemen of de bestanden erop worden vergrendeld door criminelen? In dit artikel leggen we uit wat ransomware is, hoe ransomware kan binnenkomen in uw organisatie, hoe u dit kunt voorkomen en wat (niet) te doen bij een ransomware-aanval.

Wat is het?

Ransomware is kwaadaardige software, oftewel malware, die ervoor zorgt dat gegevens op een laptop of smartphone vergrendeld worden voor de gebruiker, zodat hij er niet meer bij kan. Door ransomware worden de gegevens als het ware gegijzeld. Ransomware is een probleem omdat kwaadwillenden ten eerste door de ransomware vertrouwelijke bedrijfsgegevens ongemerkt kunnen inzien of stelen. Ten tweede eisen de kwaadwillenden achter de gijzeling van de software losgeld in ruil voor het opheffen van deze vergrendeling. Dit losgeld wordt vaak geëist in de vorm van cryptocurrencies zoals Bitcoin en loopt snel op tot in de honderden of duizenden - soms zelfs miljoenen - euro's. Ransomware hoeft tegenwoordig niet ontwikkeld te worden door de kwaadwillende zelf. Diensten als Ransomware-as-a-Service, waarbij de gijzelsoftware als dienst wordt verkocht, zijn steeds meer de norm, waardoor ransomware op steeds grotere schaal voorkomt.

Hoe komt u eraan?

Er zijn verschillende manieren waarop ransomware uw organisatie kan binnendringen. Ransomware wordt vaak onbewust geïnstalleerd en bevindt zich in veel gevallen enkele weken of maanden op het apparaat of bedrijfsnetwerk voordat het geactiveerd wordt. Een vorm waarbij medewerkers een grote rol spelen is als een gebruiker op een geïnfecteerde link klikt, waardoor de malware op een apparaat wordt gedownload. Deze link wordt bijvoorbeeld in een e-mail verzonden die afkomstig is van een schijnbaar betrouwbare (persoon in de) organisatie. Een dergelijke mail heet phishing, dit is een vorm van digitale oplichting. Een andere veelvoorkomende oorzaak van ransomware is dat de hacker voorafgaand aan de infectie onderzoek doet naar de kwetsbaarheden (vulnerabilities) van een server of applicatie. Op het moment dat de kwaadwillende in een entry point van een server of applicatie een kwetsbaarheid heeft gevonden, is het voor de hacker mogelijk om op afstand de ransom-

ware op het apparaat te installeren. De ransomware kan dan op afstand geactiveerd worden.

Hoe voorkomt u (gevolgen van) ransomware?

Ransomware-infecties hebben een enorme impact op een organisatie, en herstel van een ransomware-aanval kost veel tijd. Daarom is het verstandig om ook voldoende voorzorgsmaatregelen te nemen om de kans op een aanval en de impact ervan zo klein mogelijk te houden.

Cruciale systemen

Het ene systeem is belangrijker voor uw organisatie dan het andere. Bepaal welke systemen écht cruciaal zijn, zodat u weet waar u uw energie en maatregelen op moet vestigen bij het beschermen van uw organisatie tegen ransomware.

Updates en patches

Hackers kunnen kwetsbaarheden in software, apps of operating systems gebruiken om binnen te komen in het bedrijfsnetwerk. In verouderde software zijn de specifieke vulnerabilities bij hackers algemeen bekend, waardoor het binnendringen in het bedrijfsnetwerk gemakkelijk wordt. Op het moment dat de uitgever van de software op de hoogte is van de vulnerabilities, worden patches ontwikkeld om de fouten in de software op te lossen en de beveiliging te verbeteren. Het up-to-date houden van alle softwaresystemen is daardoor bijzonder belangrijk.

Anti-virussoftware

Anti-virussoftware kan bijzonder nuttig zijn om verborgen malware te herkennen en aan de deur te weren. Schakel de anti-virussoftware daarom niet uit wanneer de software het downloaden van bestanden belemmert of tegenhoudt.

Social engineering

Ransomware of andere malware kan op vele manieren worden geïnstalleerd. Denk aan het klikken op een link of document in een mail van een schijnbaar betrouwbare afzender (phishing), maar de malware kan zich ook bevinden in (gratis) software, illegaal gedownloade films, doorgestuurde afbeeldingen, en ook het bezoeken van een schijnbaar betrouwbare website kan genoeg zijn om de malware te installeren. Wat bovenstaande voorbeelden met elkaar gemeen hebben is dat de medewerkers een cruciale rol spelen in het binnenhalen van de ransomware. Dit fenomeen wordt ook wel ‘social engineering’ genoemd.

Wanneer alle technische maatregelen in orde zijn, kan social engineering er alsnog voor zorgen dat ransomware binnenkomt op het bedrijfsnetwerk. Een mix van technische maatregelen en awareness kan ervoor zorgen dat de medewerker niet meer als beveiligingsrisico hoeft te worden gezien.[1] Voorbeelden hiervan zijn een spamfilter en internetblokkades, gecombineerd met regelingen over het privégebruik van werkeigendommen en awarenesstrainingen. Ook phishing-simulaties kunnen hier onderdeel van zijn.

1. Zie ook https://bit.ly/3A4PhdH

Informatie vrijgeven

Hackers en andere kwaadwillenden kunnen gebruikmaken van onschuldige informatie die door het bedrijf wordt vrijgegeven. De beschrijving van werkprocessen en de partijen waarmee informatie wordt gedeeld in de privacyverklaring, nieuwsberichten via LinkedIn, maar ook informatie in vacatureteksten kunnen worden gebruikt om meer informatie te krijgen over de gang van zaken binnen het bedrijf. Zoekt het bedrijf een IT-er, dan blijkt uit de vacaturetekst vaak welke programmeertaal en frameworks worden gebruikt. Bij gerichte aanvallen is dit zeer waardevolle informatie. Omdat het delen van de informatie noodzakelijk is voor een goede werving, of in het geval van de privacyverklaring zelfs wettelijk verplicht is, is het weglaten van deze informatie vaak praktisch onmogelijk. Wees er wel van bewust dat alle informatie die naar buiten wordt gebracht, hoe onschuldig de informatie in eerste instantie ook lijkt, ingezet kan worden door kwaadwillenden.

Back-up

Het onderhouden van een back-upsysteem waarin alle kwetsbare informatie is opgeslagen is aan te raden. Door een back-upsysteem te onderhouden kan informatie worden teruggezet van het moment voor de aanval, zodat doorgewerkt kan worden aan de lopende opdrachten en de belangrijke informatie niet definitief verloren gaat. Wees er echter wel op bedacht dat de malware vaker langere tijd op het bedrijfsnetwerk aanwezig is voordat de aanval wordt uitgevoerd. Met het terugzetten van een back-up kan daardoor ook de malware worden teruggezet. Back-ups voorkomen ransomware niet, maar kunnen er wel voor zorgen dat de gevolgen (tijdelijk) beperkt blijven. Voor de back-ups kan de *3-2-1-regel* worden toegepast: er dienen drie

kopieën van de data te zijn, op twee verschillende locaties of dragers met minimaal één offline versie.

Disaster Recovery Plan

Een andere manier om het bedrijf voor te bereiden op incidenten zoals ransomware, is het beschikken over een disaster recovery plan. Ransomware kan de continuïteit van het bedrijf in gevaar brengen waarbij de schade kan oplopen tot in de miljoenen euro's. In een disaster recovery plan wordt uitgewerkt hoe en welke kritieke processen binnen het bedrijf moeten doorgaan wanneer sprake is van een technische verstoring van buitenaf zoals een ransomware-aanval. In de tussentijd kan adequaat gereageerd worden op de situatie en de schade worden beperkt. Vergeet niet om het disaster recovery plan regelmatig te testen en oefenen (vergelijkbaar met de periodieke brandoefening), zodat u het vertrouwen hebt dat het plan ook daadwerkelijk werkt.

Andere maatregelen

Naast bovenstaande onderdelen kunnen ook de volgende maatregelen bijdragen in een betere weerbaarheid tegen malware:

- monitoring;
- netwerksegmentatie;
- autorisatiebeheer;
- beperken van USB-gebruik;
- uitvoeren van vulnerability scans en pentesten;
- samenwerking met ketenpartners;
- cyberverzekering;
- regelmatige evaluatie en controle van getroffen maatregelen.

Welke maatregelen u het beste kunt nemen en in welke vorm, is grotendeels afhankelijk van wat er precies beschermd moet worden binnen uw organisatie (zie ook 'cruciale systemen') en de mate waarin de organisatie bereid is om risico's te accepteren.

Security officer

Een security officer heeft als taak om (informatie binnen) de organisatie te beveiligen. Een security officer kan ingezet worden om een beveiligingsbeleid op te stellen met onder andere bovenstaande onderdelen, en ziet toe op de uitvoering van dit beleid. Ook een business recovery plan, een incident response plan of het implementeren van standaarden zoals de ISO27001 zijn werkzaamheden die de security officer op zich kan nemen.

Geïnfecteerd! En nu?

Ook al zijn de bovenstaande maatregelen genomen, dan nog kunt u slachtoffer worden van een ransomware-aanval. Het is belangrijk om in ieder geval kalm te blijven en u niet gek te laten maken door de (tijds)druk die de aanvallers gebruiken.

Betalen of niet?

Het betalen van het geëiste losgeld geeft géén garantie dat de criminelen de decryptie-sleutels verschaffen en dat u de toegang tot uw bestanden terugkrijgt. Sommige criminelen vragen na het betalen van de ransom zelfs nogmaals om een betaling. Daarbij is het betalen van de ransom ook geen garantie dat uw organisatie niet nog een keer slachtoffer wordt van een ransomware-aanval, omdat de kwetsbaarheden in de systemen of in uw organisatie mogelijk blijven bestaan. Bovendien houdt betaling deze vorm van digitale criminaliteit in stand. Over het algemeen wordt daarom afgeraden om het 'losgeld' te betalen, ondanks dat er situaties denkbaar zijn waarin betalen de enige of beste optie lijkt te zijn.

Code beschikbaar

Hoe krijgt u zonder te betalen toch toegang tot de systemen en bestanden? De ransomware is vaak een vergrendeling door het gebruik van encryptie. Juist omdat de kwaadwillenden zelf niet altijd de ransomware zelf hoeven te maken, zijn de codes om de bestanden te kunnen ontgrendelen vaak online al beschikbaar. Kijk bijvoorbeeld of de ransom op nomoreransom.org staat, een site van onder andere Europol en de politie.

Aangifte

Ongeacht de oorzaak of vorm ransomware: doe altijd aangifte van de ransomware bij de politie, ook wanneer u inmiddels weer bij uw bestanden kan! Door aangifte te doen krijgt de politie inzicht in de soorten ransomware die worden gebruikt en kunnen meer slachtoffers worden voorkomen. Daarnaast is aangifte vaak een verplichting vanuit uw verzekering, indien u daarop aanspraak doet.

ICTRECHT
security

Uw organisatie goed beschermd met ICTRecht Security

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

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

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

Ruben van der Geest
Juridisch adviseur

Privacy

De technische implementatie van een cookiebanner, wat zijn de valkuilen?

Het internet staat er vol mee: blogs en artikelen over wat wel en niet mag met cookies. Logisch, want online tracking is een belangrijk onderwerp voor veel bedrijven. Sommige bedrijven, zoals Google en Facebook, danken er zelfs hun bestaansrecht aan! Vaak wordt er (onterecht) alleen geschreven over cookies, maar de ePrivacy richtlijn en de Algemene verordening gegevensbescherming (AVG) zien op veel meer dan alleen cookies. De regels gaan namelijk over alle vormen van online tracking, dus ook het gebruik van web beacons of device fingerprinting. Voor het leesgemak zal in dit artikel de term 'online tracking' of 'cookies' gebruikt worden voor alle technieken die gebruikt worden om gebruikers online te volgen.

Cookies in vogelvlucht

Voor de meeste cookies is toestemming vereist. Deze toestemming moet vrij, specifiek, geïnformeerd en ondubbelzinnig gegeven worden, via een ondubbelzinnige actieve handeling. Hierdoor is het gebruik van cookie walls (niet vrijelijk gegeven), vooraf aangevinkte vakjes (geen actieve handeling) en "bij gebruik van deze website bent u akkoord" (geen specifieke ondubbelzinnige handeling) geen geldige vorm van toestemming. Let erop dat de cookiebanner aan de vereisten voldoet. Waarschuwingen en boetes liggen op de loer!

De cookiebanner is af, en nu?

De eerste stap is de cookiebanner. De tweede stap is alles technisch goed regelen. Die tweede stap blijkt in de praktijk een stuk ingewikkelder. Veel bedrijven zijn afhankelijk van andere partijen. Denk bijvoorbeeld aan een externe webdeveloper, cookiedienstverleners of YouTube, voor het plaatsen van de 'Over

ons bedrijf'-video. Al die partijen moeten hun medewerking verlenen om de tweede stap tot een succes te maken. Er komt heel wat kijken bij deze tweede stap. In dit artikel bespreken we een paar valkuilen die u tegen kunt komen (of juist over het hoofd ziet) bij het uitvoeren van stap twee.

Embedded content

Veel cookie-management oplossingen bieden de mogelijkheid om cookies die u zelf plaatst, pas in te laden als de gebruiker toestemming geeft. Het belangrijkste in de voorgaande zin is "zelf plaatst". Cookies die u niet zelf plaatst zijn het probleem bij het embedden van content.

Een goed voorbeeld van het embedden van content is het plaatsen van een YouTube-video op uw website. In dit artikel wordt YouTube gebruikt als voorbeeld omdat het een bekende partij is, maar het probleem speelt bij veel meer content hosting platforms (en niet alleen bij video's). Bij het embedden van een video, lijkt het alsof de video op uw website staat, maar in feite wordt de video afgespeeld vanaf de servers van YouTube. Het is als het ware een raampje met uitzicht op de servers van YouTube.

Het voordeel hiervan is dat u de video niet zelf hoeft te hosten op uw server. Dat scheelt opslagruimte en uw webpagina wordt er sneller van. Het probleem is alleen dat dit raampje twee kanten op werkt. De bezoeker van een website kan de video op de server van YouTube zien en YouTube kan ondertussen cookies plaatsen op het apparaat van de websitebezoeker. Het vervelende is dat u als website-eigenaar verantwoordelijk bent onder de AVG! Dan heeft u dus netjes een cookiebanner laten opstellen en die ook ingevoerd, komt YouTube opeens roet in ~~de koekjes~~ het eten gooien!

Het antwoord van YouTube op dit probleem is YouTube Nocookies. Maar let op, dit is op zijn zachtst gezegd een beetje misleidend. YouTube Nocookies plaatst geen cookies totdat de websitebezoeker op de play-knop drukt. Nog steeds niet AVG-proof dus! Maar er is een oplossing. Dit is een technisch verhaal en daarom misschien beter om over te laten aan uw webdeveloper. Het embedden van een video gebeurt vaak door middel van een iframe. Dit is een stukje HTML-code die de link naar de video bevat. Door dit linkje te verplaatsen van het 'src'-onderdeel naar een 'data-src'-attribute wordt de video niet geladen bij het openen van de website. U kunt dan een placeholder plaatsen met een link naar de privacyverklaring en de cookie instellingen. Met javascript kan de link weer naar de originele locatie in het iframe worden geplaatst op het moment dat de cookies zijn geaccepteerd.

De bovenstaande oplossing is niet 100% juridisch sluitend. De AVG vereist namelijk dat er geen nadelige gevolgen mogen zitten aan het weigeren van toestemming. Het niet kunnen zien van een YouTube-video is een nadelig gevolg. Dus strikt gezien is dit geen geldige toestemming. Het zelf hosten van video's is eigenlijk de enige juridisch correcte oplossing, maar dit stuit soms op praktische bezwaren.

Cookies sans

Comic sans, wie kent het lettertype niet? Dit lettertype heeft zelfs een eigen pagina op Reddit.[1] Sans komt van het Franse woord 'zonder'. Als het in de naam van een lettertype staat, betekent dit dat het een schreefloos lettertype is. Dus zonder (sans) dwarsstreepjes aan de uiteinden van letters, zoals bij **Times New Roman** te zien is. Maar het gaat in dit artikel toch over cookies? Dat klopt, dus zorg ervoor dat de lettertypes die u gebruikt "sans cookies" zijn.

1. https://www.reddit.com/r/comicsans/

Het gaat bij lettertypen niet echt om cookies, maar om een andere manier van online tracking: web beacons. Een web beacon is een element op een webpagina (kan zelfs een enkele pixel zijn, zoals de Facebook Pixel) die bij het laden van de webpagina een signaal stuurt naar de bijbehorende server. Dit signaal bevat informatie over de websitebezoeker en maakt het mogelijk om die websitebezoeker op meerdere websites te volgen.

Nu weer terug naar lettertypen. Om een website goed uit de verf te kunnen laten komen, is het belangrijk om mooie lettertypes te gebruiken. Het is mogelijk om een lettertype te kopen of te laten maken en dat vervolgens te hosten op uw eigen website. Het nadeel is dat dit kostbaar kan zijn en het maakt uw webpagina trager. Het alternatief is om gebruik te maken van een (gratis) 'lettertype-bibliotheek', zoals Google Fonts. Het probleem is hierbij: niets in het leven is gratis. Door gebruik te maken van de Google Fonts API's wordt contact gelegd met de servers van Google. En daar komen de web

beacons en de lettertypen samen. Door de lettertypen op te vragen via de server van Google, kan Google interessante informatie verzamelen over gebruikers van uw website. Google zegt zelf dat ze daarbij het minimale aan gegevens verwerken.[2] Minimaal is niet niets helaas.

2. https://developers.google.com/fonts/faq

De volgende oplossingen zijn denkbaar:
- Toestemming vragen. De website zal eerst geladen worden met 'saaie' standaard lettertypen. Als de gebruiker dan akkoord gaat, kan de pagina geladen worden met de gewenste lettertypen. Zo niet, dan zal de gebruiker het moeten doen met de standaard lettertypen.
- Zelf hosten. De licentie voor het gebruik van Google Fonts staat het toe om de lettertypen te downloaden en zelf te hosten. Dit gaat wel ten koste van de snelheid, maar er is geen toestemming vereist.
- Zelf hosten en toestemming vragen. Een combinatie van de eerste twee oplossingen is ook mogelijk. De eerste stap is dat u de lettertypen op uw eigen server host. De webpagina kan dan naar de lettertypen op uw server verwijzen. Als de gebruiker dan akkoord gaat, dan kan een script de verwijzing naar uw eigen server vervangen door de API van Google Fonts. De rest van de webpagina's zal dan sneller laden.

U heeft ongelezen cookies

E-mail, wie kan nog zonder? Vooral bedrijven niet, zelfs de bakker op de hoek heeft tegenwoordig een eigen digitale nieuwsbrief met nieuwe producten, aanbiedingen en cookies. En met cookies bedoel ik niet die lekkere roomboterkoeken die bij de bakker in de vitrine liggen!

Het woord cookies is ideaal voor anekdotes zoals hierboven, maar in deze situatie gaat het wederom over web beacons. E-mails bevatten tegenwoordig mooie afbeeldingen, links en tracking pixels. Die afbeeldingen worden niet allemaal meegestuurd in de e-mail zelf, die staan op een server van de verzender. De verzender kan dus zien of de mail geopend wordt, hoe vaak dit gebeurt, of de mail wordt doorgestuurd en welk apparaat gebruikt wordt om de mail te openen.

De meeste e-mailmarketingsoftware heeft dergelijke functionaliteiten ingebouwd. Er zijn dus bedrijven die hun klanten tracken zonder dat ze dit door hebben of weten dat ze hier toestemming voor moeten vragen. Het vragen om een nieuwsbrief te mogen versturen is dan niet voldoende. De in het begin aangehaalde voorwaarden voor toestemming sluiten dit namelijk uit.

In een toestemmingsvraag voor een nieuwsbrief dient het volgende te staan:
- wie de nieuwsbrief verstuurt;
- hoe vaak dit zal gebeuren;
- wat voor soort informatie verstuurd gaat worden en hoe dit gebeurt (via e-mail);
- een link naar de privacyverklaring.

Een dergelijke vraag zal er dan als volgt uit kunnen zien: "Ik wil graag twee keer per maand een e-mail ontvangen met de nieuwste aanbiedingen en acties van bedrijf X. Klik hier voor onze privacyverklaring." Met toestemming verkregen op basis van deze vraag mag een nieuwsbrief verstuurd worden, maar daar mogen geen tracking mechanismes inzitten.

Uit de toestemmingsvraag blijkt namelijk niet dat de nieuwsbrief ook bijhoudt of de ontvanger de e-mail opent of doorstuurt. Er is dus geen specifieke en ondubbelzinnige toestemming verkregen. Er zal dus apart toestemming voor gevraagd moeten worden door een extra aanvinkvakkje toe te voegen. De toestemming moet namelijk vrij en specifiek gegeven kunnen worden. Een gebruiker moet dus de nieuwsbrief kunnen ontvangen zonder toestemming te geven voor het gebruik van web beacons, anders is het geen vrije keuze. Toestemming krijgen is hier de enige oplossing.

☐ I'm not a robot

Vraag een website-eigenaar wat het grootste probleem is met contactformulieren en ze zullen allen zeggen: "Spam". Het spammen gebeurt vaak door algoritmen, ook wel spam-robots genoemd. Het is daarom handig voor website-eigenaren om te weten wie een echte gebruiker is en wie een spam-robot is. De eerste oplossing die voor dit probleem gevonden werd was de captcha, het overtypen van lastig te lezen letters en cijfers. De spam-robots worden echter steeds beter, dus de captcha's moeten steeds moeilijker gemaakt worden. Een constante online-wapenwedloop tussen goed en kwaad! De nieuwste ontwikkelingen zijn de technieken zoals die door Google gebruikt worden voor reCAPTCHA.

Er zijn twee versies van reCAPTCHA in omloop. De

twee versies kennen weer verschillende vormen, maar het principe is hetzelfde. Een algoritme monitort het gedrag van een websitebezoeker en beslist aan de hand van die gegevens of het gaat om een robot of een mens. Hoe werkt dit precies? De websitebezoeker laadt een webpagina waar een contactformulier op staat. De webpagina laadt de API van reCAPTCHA. Vervolgens gaat reCAPTCHA het gedrag van de websitebezoeker in de gaten houden. Het gaat dan bijvoorbeeld om: hoe snel worden de velden ingevuld, hoeveel tijd zit er tussen het invullen van de verschillende velden, waar klikt u in het volgende invulveld, etc. Een robot zou de velden namelijk heel snel kunnen invullen of elke keer op precies dezelfde plek in het volgende invulveld kunnen klikken. De websitebezoeker krijgt vervolgens een score toegekend, een 'robot-score'. Vervolgens vinkt de websitebezoeker het vakje "I'm not a robot" aan. Als de robot-score laag is, dan komt er een groen vinkje in beeld en kan het formulier verzonden worden. Als de robot-score hoog is, en de bezoeker misschien een robot is, komt er een extra test. Dit kan bijvoorbeeld het herkennen van auto's in Google Maps afbeeldingen zijn. Tijdens het oplossen van deze puzzel wordt weer nauwkeurig bijgehouden of de websitebezoeker dit robotachtig doet. Als de websitebezoeker slaagt, dan kan het formulier verstuurd worden. De websitebezoeker helpt Google ook direct met het labelen van data voor AI-systemen. Het labelen van data is duur, dus dat is mooi meegenomen!

ReCAPTCHA maakt dus een digitale vingerafdruk van de websitebezoeker, inclusief een schermafbeelding, waar de muis is geweest en waar is geklikt. Dit maakt het mogelijk om een uniek profiel aan te maken van websitebezoekers. Voor device fingerprinting, en dus het gebruik van reCAPTCHA, is toestemming vereist. Ik gok dat de spam-robot geen toestemming zal geven!

Spam voorkomen moet dus op een andere manier. Er zijn privacyvriendelijke alternatieven beschikbaar. Er is dan wel een grote kans dat uw websitebezoekers meer puzzeltjes moeten oplossen om aan te tonen dat ze geen robot zijn. Het beste is om een combinatie van een privacyvriendelijke captcha, honeypots en een goed spam-filter te gebruiken. Honeypots zijn onzichtbare invulvelden die mensen niet kunnen zien, maar waarbij het voor robots lijkt of er iets ingevuld moet worden. Wanneer een dergelijk honeypot-veld wordt ingevuld, dan is dat door een robot gedaan. Een privacyvriendelijke captcha samen met honeypots en u bent al een heel eind op weg. Mochten er alsnog robots door uw beveiliging heen komen, dan doet een spam-filter vaak ook wonderen!

Conclusie

Cookies in lijn met de wetgeving brengen is makkelijker gezegd dan gedaan. Het is een technisch onderwerp en de partijen die de cookies leveren, vinden het vaak niet zo belangrijk om alles in lijn met de AVG in te richten. Laat u daarom altijd goed adviseren, ook over de technische aspecten.

Sari Jansen
Juridisch adviseur

E-health Overheid Privacy

Uitwisseling van patiëntgegevens: de Wet kwaliteitsregistraties zorg

Voor het leveren van de juiste zorg op de juiste plek is het nodig dat hulpverleners tijdig beschikken over de correcte patiëntinformatie. Regelmatig schrijven we over de ontwikkelingen op wetgevingsgebied omtrent de (elektronische) uitwisseling van patiëntdata. U heeft bijvoorbeeld kunnen lezen over het Wetsvoorstel elektronische gegevensuitwisseling in de zorg (Wegiz), de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) en het Besluit elektronische gegevensverwerking door zorgaanbieders. In het kader van gegevensuitwisseling in de zorg verdient ook het wetsvoorstel over het aanleveren van patiëntgegevens voor kwaliteitsregistraties een bespreking. In dit artikel gaan we in op de inhoud en reikwijdte van het voorstel Wet kwaliteitsregistraties zorg (Wkz)[1], en de verhouding tot de huidige wetgeving.

1. Raadpleegbaar via: https://bit.ly/3lpQrtS

Doel en reikwijdte

De overheid heeft op grond van de Wet kwaliteit klachten en geschillen zorg (Wkkgz) de wettelijke opdracht om zorg te dragen voor een stelsel van goede zorg. Om de kwaliteit van zorg te borgen en te verbeteren is het van belang om zorgaanbieders in staat te stellen om van elkaar te leren. Er bestaat daarom een grote behoefte aan het gebruik van medische gegevens van patiënten voor algemene kwaliteitsregistraties. De Wkz zou dit moeten vereenvoudigen en is een wijziging op de Wkkgz. Het voorstel beoogt het regelen van regie op kwaliteitsregistraties in de zorg en het creëren van grondslagen om ten behoeve van die kwaliteitsregistraties bijzon-

dere persoonsgegevens te kunnen verwerken. In de Wkz wordt een specifieke wettelijke grondslag gecreëerd voor kwaliteitsregistraties om gepseudonimiseerde (bijzondere) persoonsgegevens te mogen verwerken. Deze grondslag geldt alleen voor kwaliteitsregistraties die het Zorginstituut Nederland heeft opgenomen in het, ook bij dit wetsvoorstel te regelen, nieuwe openbare register voor kwaliteitsregistraties. De reikwijdte van de Wkz ziet verder nu nog alleen op de medisch specialistische zorg, maar het is de bedoeling dat dit de komende jaren wordt uitgebreid.

De “noodzaak” van het wetsvoorstel

Op dit moment ontbreekt een toereikende wettelijke grondslag om als zorgaanbieder patiëntgegevens aan te leveren voor een kwaliteitsregistratie.[2] De Wkz neemt dit knelpunt weg door een specifieke grondslag te bieden. Het gevolg is dat voor het aanleveren en verwerken van (medische) gegevens, géén toestemming van de betreffende patiënt (meer) nodig is. Het is de bedoeling dat op die manier de regeldruk wordt verlicht: de zorgaanbieder hoeft geen toestemming meer te vragen en de patiënt hoeft niet telkens (opnieuw) toestemming te geven. Daarnaast geldt dat indien een deel van de patiënten geen toestemming verleent, een verleende toestemming later weer intrekt of niet in staat is om toestemming te verlenen (bijvoorbeeld omdat de patiënt te ziek is en er geen wettelijke vertegenwoordiger toestemming kan geven), tot gevolg heeft dat niet alle relevante gegevens kunnen worden verwerkt. En dat is, in het kader van de kwaliteit van zorg en de volledigheid van de registraties, onwenselijk.

2. Met de wettelijke grondslag wordt een uitzondering gecreëerd op het verwerkingsverbod van artikel 9 van de Algemene verordening gegevensbescherming voor bijzondere (medische) persoonsgegevens.

In de toelichting op het voorstel wordt als tweede knelpunt de toename van de registratielasten en beheerskosten voor zorgaanbieders genoemd. Die stijging zou het gevolg zijn van de toename van het aantal kwaliteitsregistraties en de toenemende omvang van de gegevensset van de registraties. Ook is sprake van overlap van nieuwe registraties met bestaande registraties. De Wkz beoogt dit knelpunt op te lossen door het stellen van eisen aan de kwaliteitsregistratie en het verplicht toetsen aan die eisen door een externe onafhankelijke partij (het Zorginstituut Nederland). Voor opname in het register moet de kwaliteitsregistratie worden getoetst op onder meer noodzaak en proportionaliteit. Wordt hieraan niet voldaan, dan is er geen opname in het register voor kwaliteitsregistraties.

Doorbreken van het medisch beroepsgeheim

De gegevens ten behoeve van een kwaliteitsregistratie worden doorgaans aangeleverd door een arts of andere hulpverlener. Op grond van de Wet op de geneeskundige behandelingsovereenkomst (WGBO)

is de hulpverlener verplicht geheimhouding te betrachten ten aanzien van de gegevens van zijn patiënt. Doorbreking van dit beroepsgeheim, zonder toestemming van de patiënt, kan geschieden op grond van een wettelijk voorschrift. Daarnaast kunnen gegevens op basis van de WGBO onder meer gedeeld worden met degene die rechtstreeks is betrokken bij de behandeling en, voor zover dit noodzakelijk is, voor de in dat kader door hem te verrichten werkzaamheden.

In de praktijk worden er regelmatig gegevens verzameld en aangeleverd ten behoeve van kwaliteitsregistraties, zónder toestemming van de patiënt. Een argument wordt dan gevonden in de stelling dat kwaliteitsregistraties noodzakelijk zijn voor de behandeling. Kwaliteitsregistraties kunnen uiteraard ten goede komen aan de kwaliteit van zorgverlening, maar zijn echter niet noodzakelijk voor de behandeling van de specifieke patiënt. Ook de Europese Algemene verordening gegevensbescherming (AVG) en de nationale Uitvoeringswet AVG bieden geen ruimte voor het veronderstellen van toestemming, zoals op grond van de WGBO onder omstandigheden wel kan. Gevolg: een wettelijke grondslag óf toestemming is nodig. Voor de gevallen waar de registratie niet binnen het toepassingsbereik van de Wkz valt, moet dus alsnog toestemming worden verkregen.

Verminderde druk op zorgaanbieders?

De Wkz regelt niet alleen een wettelijke grondslag, maar roept daarnaast ook een wettelijke verplichting in het leven om gegevens aan te leveren voor kwaliteitsregistraties. De Wkz verplicht zorgaanbieders namelijk om, in het geval dat een kwaliteitsregistratie is opgenomen in het register voor kwaliteitsregistraties van het Zorginstituut Nederland, de gevraagde informatie aan (de gegevensverwerker van) de betreffende kwaliteitsregistratie aan te leveren. Blijkens de toelichting op het voorstel heeft het vrijwillige karakter van deelname door zorgaanbieders aan een kwaliteitsregistratie inmiddels plaatsgemaakt voor de opvatting dat alle zorgaanbieders en patiënten moeten meedoen om tot betrouwbaar leren en verbeteren te komen. Dat betekent dat aanbieders die nog geen gegevens aanleverden, dit nu wel moeten doen. Het is dus de vraag of de totale regeldruk voor alle zorgaanbieders daadwerkelijk wordt verlicht: zorgaanbieders hoeven geen toestemming meer te vragen, maar moeten wel actief aan de slag met het aanleveren van gegevens.

Gegevensbeveiliging

Voor medische gegevens is vanwege de gevoelige (en bijzondere) aard een hoog niveau van beveiliging vereist. Het anonimiseren van de gegevens, waarbij geen enkele herleidbaarheid naar het individu bestaat, is volgens de toelichting op het voorstel echter geen optie. Anonimisering wordt problematisch geacht omdat het juist nodig is om individuele patiënten van een bepaalde patiëntenpopulatie met een specifieke aandoening, ziekte, zorgtype of complicatie te kunnen volgen. Daarom voorziet het voorstel erin dat er alleen met gepseudonimiseerde gegevens wordt gewerkt: de gegevens zijn dan in ieder geval niet direct herleidbaar naar een individu. Dit vermindert het privacyrisico voor de betrokken patiënten. Overigens voorziet het voorstel niet in (de verplichting tot) andere specifieke beveiligingsmaatregelen, zoals we bijvoorbeeld wel zien bij de wetgeving omtrent zorginformatie- en elektronische uitwisselingssystemen (denk aan NEN 7510, 7512 en NEN 7513).[3] Wel kent het voorstel een delegatiegrondslag op basis waarvan bij lagere regelgeving nadere eisen kunnen worden gesteld. Het gaat dan om bij ministeriële regeling te bepalen regels ten aanzien van het gebruik van bijvoorbeeld NEN-normering en/of andere passende technische en organisatorische maatregelen om de persoonsgegevens te beveiligen tegen verlies of enige andere vorm van onrechtmatige verwerking.

3. Besluit elektronische gegevensverwerking door zorgaanbieders.

Ook worden in de toelichting al enkele voorbeelden van technische en organisatorische waarborgen genoemd, zoals het voorschrift om alleen te rapporteren op voldoende geaggregeerd niveau. Verder wordt aangeraden om voor de aanlevering van de persoonsgegevens gebruik te maken van een (onafhankelijke) aanbieder van vertrouwde pseudonimiseringsdiensten (TTP).

Waar staan we nu?

U bent als zorgaanbieder op dit moment nog niet verplicht om gegevens aan te leveren ten behoeve van de kwaliteitsregistraties. De consultatie ten aanzien van de Wkz is afgelopen juli gesloten. De uitkomsten daarvan zullen worden besproken en mogelijk verwerkt in een nieuwe versie van de Wkz. Of en zo ja, wanneer de Wkz vervolgens in werking zal treden, is nog niet bekend. Vanzelfsprekend houden we u op de hoogte.

Wij staan op de Zorg & ICT beurs!

ICTRECHT
adviesbureau

2, 3 en 4 november 2021, Jaarbeurs Utrecht.

Verder met ons praten over de (elektronische) uitwisseling van medische persoonsgegevens? Wilt u weten hoe u nu echt grip krijgt op uw informatiebeveiliging? Of bent u geïnteresseerd in het volgen van een training over thema's die u als zorgprofessional aangaan? Bezoek ons op de Zorg & ICT beurs!

Wij staan u graag te woord en praten u bij over de laatste ontwikkelingen op het gebied van het ICT-recht, de privacywetgeving (AVG) en informatiebeveiliging.

Registreer u nu via: zorg-en-ict.nl

Graag tot dan!

Arnoud Engelfriet
Algemeen directeur / Opleidingsdirecteur

Internetrechtspraak

Bevrijdende betaling valse factuur
(Hoge Raad 28 mei 2021)

Devante is een dochtermaatschappij van Yildirim Holding, een onderneming die zich bezighoudt met de handel in onder meer ferrochroom. Hascor bestelde in 2015 een hoeveelheid van dit ferrochroom. Vanuit het juiste e-mailadres werd er, na de eerste e-mail, een tweede gestuurd met de inhoud dat de vorige e-mail fouten bevatte. Een derde e-mail verkondigde dat de fouten eruit waren gehaald en dat de factuur kon worden voldaan. Dit bleek achteraf een valse factuur. In de vraag of er bevrijdend is betaald, oordeelde het hof dat er sprake is van bijzondere omstandigheden van dien aard dat het aan Devante valt toe te rekenen dat Hascor de e-mail met factuur voor echt heeft gehouden. Devante mocht dit redelijkerwijze ook doen. Met bijzondere omstandigheden wordt in dit geval geduid op het feit dat er telkens een andere verkopende partij vanuit Yildirim naar voren werd geschoven en de e-mails verstuurd zijn vanuit het juiste e-mailadres. Ook gezien de inhoud van de e-mails had Hascor geen reden om te twijfelen aan de echtheid hiervan. Het oordeel van het hof wordt door de Hoge Raad in stand gehouden.

https://bit.ly/3BRnPAy

Onduidelijke software-eigendom
(Rechtbank Rotterdam 31 mei 2021)

Twee bedrijven werken samen aan softwareontwikkeling maar krijgen ruzie. De vraag ontstaat wie eigenaar is van het resultaat: hiervoor zijn geen eenduidig vastgelegde afspraken voorhanden. Wat de juridische situatie is met betrekking tot het eigendom van het intellectueel eigendomsrechten op de huidige versie van de software is gelet op het voorgaande onduidelijk. Op voorhand kan evenwel niet worden uitgesloten dat er sprake is van een gezamenlijk auteursrecht. De onderhavige zaak leent zich bij uitstek tot het treffen van een ordemaatregel. Eiser in verzet moet daarom binnen 24 uur de blokkade van (de medewerkers van) gedaagde in verzet tot de voor de uitoefening van haar bedrijfsactiviteiten vereiste (computer) systemen opheffen en opgeheven te houden totdat het onderzoek van de Ondernemingskamer is afgerond, of tot dat een gerechtelijk bodemvonnis is gewezen en in kracht van gewijsde is gegaan.

https://bit.ly/3toUvhx

Teruggave dongels (Gonen tegen Ikea)
(Hof Amsterdam 8 juni 2021)

In 1995 hebben Gonen en Ikea een overeenkomst gesloten die ertoe strekt dat Gonen software aan Ikea ter beschikking stelt. Gonen heeft in de loop van de tijd ook dongels aan Ikea ter beschikking gesteld. In dit geding vordert Gonen dat Ikea dongels aan haar teruggeeft of anders schade vergoedt. Ikea betwist dat dit in het ontvangstformulier is bepaald. Het hof acht Ikea onder omstandigheden verplicht tot teruggave van de dongels, maar geeft aan Gonen de opdracht om te bewijzen

dat dit het geval is. Ook krijgt Gonen de gelegenheid om te bewijzen dat er sprake is van schade, wanneer de dongels niet worden teruggegeven.

https://bit.ly/2YD77qf

Onrechtmatige uitingen op Twitter
(Rechtbank Midden-Nederland 17 juni 2021)

Eiser stelt dat gedaagde onrechtmatige uitlatingen over hem heeft gedaan op Twitter. Gedaagde heeft aangegeven dat zij met deze berichten andere vrouwen wil waarschuwen voor het, volgens haar, manipulatieve en grensoverschrijdende gedrag van eiser. Eiser vordert van de rechtbank dat gedaagde bevolen wordt om de berichten van haar Twitteraccount te verwijderen en dat zij deze berichten uit verschillende zoekmachines laat verwijderen. De rechtbank weegt in deze zaak het belang van vrijheid van meningsuiting af tegen het belang van het recht op eerbiediging van de eer en goede naam. Omdat de op Twitter geuite beschuldigingen van gedaagde genoeg steun vinden in andere feiten en verklaringen en een deel van de berichten inmiddels verwijderd zijn, oordeelt de rechtbank dat het belang van gedaagde zwaarder weegt. Ze wijst de vorderingen van eiser af.

https://bit.ly/3tpmLRk

Onware google reviews
(Rechtbank Rotterdam 17 juni 2021)

Eiser is de rechtsopvolger van een budgetbeheer bedrijf. Gedaagde was klant bij het bedrijf en heeft een aantal keer Google reviews geschreven die onwaarheden bevatten. Eiser vordert dat het gedaagde verboden wordt om nog langer zulke uitlatingen te doen. Op het moment dat deze zaak voor de rechter komt, staan er geen uitlatingen van gedaagde op internet. Mede om deze reden wordt geoordeeld dat eiser geen belang bij de vordering heeft. Ook staat gedaagde inmiddels weer onder professionele begeleiding, waardoor het aannemelijk wordt geacht dat gedaagde zich niet langer negatief zal uitlaten op internet over eiser.

https://bit.ly/2VppwWh

Inzageverzoek te algemeen
(Rechtbank Noord-Holland 18 juni 2021)

Het ministerie van Financiën wijst een inzageverzoek onder de AVG af met het argument dat het te algemeen is, zodat sprake is van een “fishing expedition”. Eiser stelt daar tegenover dat men ten onrechte van hem vraagt zijn verzoek te preciseren, omdat hij daardoor niet al zijn persoonsgegevens kan controleren. Verweerder heeft aangevoerd dat zij in meerdere systemen op zoek moet gaan naar de betreffende persoonsgegevens en dat voor sommige systemen slechts autorisatie aan een beperkt aantal personen is toegekend. De rechtbank oordeelt: naarmate een verzoek meer concreet is, mag van de verwerkingsverantwoordelijke meer inspanning worden verwacht, maar ook bij een algemeen geformuleerd verzoek mag naar het oordeel van de rechtbank worden verwacht dat de verwerkingsverantwoordelijke een zoekslag verricht naar de meest gangbare persoonsgegeven (bijvoorbeeld aan de hand van de NAW-gegevens en het BSN-nummer) in de meest gangbare gegevensbestanden en/of computersystemen/applicaties. Dat zou slechts anders zijn als van de zijde van de verwerkingsverantwoordelijke inzichtelijk gemotiveerd wordt dat ook zo’n beperkte zoekslag onevenredig veel inspanning vergt.

https://bit.ly/3hceYS1

Strafpunten-systeem Letland
(Hof van Justitie EU 22 juni 2021)

Het Hof geeft in deze uitspraak een antwoord op een aantal door het Letse grondwettelijk hof gestelde prejudiciële vragen. De persoonsgegevens van natuurlijk persoon B staan bij de Letse directie verkeersveiligheid geregistreerd, omdat hij een

aantal verkeersovertredingen heeft begaan. Op basis van deze overtredingen zijn er zogenaamde strafpunten aan B toegekend. Vervolgens is het door middel van deze regeling ook voor eenieder mogelijk om zonder belang inzage te krijgen in dit soort gegevens. B betwist dat deze regeling in overeenstemming is met de AVG, omdat de regeling het recht op eerbiediging van het privéleven zou schenden. In de eerste plaats merkt het Hof op dat de informatie over strafpunten zich kwalificeert als persoonsgegevens, die binnen de werkingssfeer van de AVG valt. Verder oordeelt het Hof dat deze regeling niet proportioneel is in verhouding tot het doel; namelijk het verbeteren van de verkeersveiligheid. Het feit dat het om een min of meer openbaar register gaat, doordat iedereen zonder direct belang persoonsgegevens van anderen kan inzien, leidt bovendien tot onverenigbaarheid met de AVG.

https://bit.ly/3CeGTZJ

Dutch Filmworks tegen Ziggo
(HR 25 juni 2021)

In een langlopend geschil eist Dutch Filmworks dat Ziggo structureel NAW-gegevens verstrekt van consumenten die via Ziggo illegaal films downloaden waar DFW producent of distributeur van is. Rechtbank en hof hebben deze eisen beiden afgewezen, met name omdat DFW te zeer op de vlakte blijft bij de vraag wat men precies gaat eisen van deze consumenten. DFW spreekt in de media bijvoorbeeld van het “opleggen van boetes” en schermt met bedragen als 150 euro, wat wringt met de opstelling in de rechtszaal waarin men zegt consumenten op constructieve manier aan te willen spreken en een reële schadevergoeding wil verzoeken. Mede hierdoor oordeelde het hof dat Ziggo zo niet op een fatsoenlijke manier haar klanten kan informeren over de voorgenomen verstrekking van persoonsgegevens. De HR bekrachtigt de uitspraak zonder nadere motivatie (art. 81 RO). Zie de noot op pagina 30.

https://bit.ly/3BOebhW

100% beschikbaarheid
(Gerechtshof Arnhem-Leeuwarden 29 juni 2021)

Accountantskantoor Nagtzaam heeft bij een ICT-dienstverlener een online Citrix-werkomgeving afgenomen. Nagtzaam ging er daarbij vanuit dat zij een 100% gegarandeerde toegang had tot deze systemen. Het hof neemt de 21 pagina’s tellende SLA ter hand en ziet weliswaar in de inleiding mooie woorden over gegarandeerde toegang, maar verderop genoeg uitzonderingen, zoals grootschalige calamiteiten, gepland en ongepland onderhoud, slecht beveiligde werkplekken et cetera. Daar komt bij dat Nagtzaam heeft gekozen voor het laagste niveau (zilver), waarbij expliciet de verschillen met het hogere niveau (goud) genoemd zijn en dus duidelijk hadden moeten zijn. Er blijkt geen sprake te zijn van wanprestatie door Arcus. Nagtzaam mocht er (onder andere) op grond van de zorgplicht en het door Nagtzaam gekozen support-niveau niet ervan uitgaan dat ze te allen tijde storingvrije beschikbaarheid tot de werkomgeving zou krijgen. Nagtzaam heeft namelijk niet voor het hoogste support-niveau gekozen en ook was niet het gehele ICT-systeem ondergebracht bij Arcus.

https://bit.ly/3hcRxYy

Phishing panels
(Rechtbank Den Haag 1 juli 2021)

Verdachte wordt onder andere verdacht van oplichting, phishing en computervredebreuk. Hij heeft op internet zogenaamde panels verkocht. Met deze panels kunnen gemakkelijk webpagina’s van banken worden nagemaakt. Ook heeft de verdachte zelf slachtoffers gemaakt door oplichting. Naar aanleiding van gegevens die zijn aangetroffen op de computer van de verdachte, in het bijzonder Telegramchats, is de verdenking ontstaan dat de verdachte niet alleen panels heeft ontworpen en verkocht, maar ook zelf, samen met anderen, van de door hem ontworpen panels gebruik heeft gemaakt om fraude te plegen. De politie heeft verbanden gelegd met de gegevens op de computer van de verdachte en diverse aangiftes van fraude. Ook heeft de politie bij ING Bank fraudedossiers opgevraagd waarin het IP-adres van het huisadres van de verdachte voorkwam. Hij wordt veroordeeld

voor een gevangenisstraf van 36 maanden, waarvan 12 voorwaardelijk. Daarnaast wordt hij veroordeeld tot de gedragsinterventie Hack_Right, omdat gebleken is dat verdachte een talent voor programmeren heeft.

https://bit.ly/3jUn4Ra

Probegin tegen Communiq
(Rechtbank Overijssel 7 juli 2021)

Probegin is een softwareontwikkelaar. Communiq houdt zich bezig met de marketing voor franchises. Partijen hebben een softwareovereenkomst gesloten waarbij is afgesproken dat Probegin een integraal platform voor Communiq zou gaan ontwikkelen, die Communiq voor al haar klanten kan gebruiken. Communiq is vervolgens ontevreden over kwaliteit van het geleverde werk en is van mening dat de overschrijding van de ureninschatting buitenproportioneel is. Ze heeft daarop haar betalingen aan Probegin opgeschort. Probegin vordert betaling van de facturen en stelt daarbij dat er een afnameverplichting van vijf ontwikkelaars is overeengekomen. De rechter gaat hier niet in mee en oordeelt dat uit de feiten en omstandigheden gedurende de onderhandelingen is gebleken dat een afnameverplichting van een ontwikkelaar is overeengekomen. Probegin heeft echter telkens nagelaten om slechts een ontwikkelaar ter beschikking te stellen en aangevoerd dat alleen in teamverband kan worden gewerkt. Volgens de rechtbank is dit niet wat partijen overeengekomen zijn en heeft Communiq dus terecht de overeenkomst buitengerechtelijk ontbonden.

https://bit.ly/3niEaKB

Schadeclaim sjoemelsoftware
(Rechtbank Amsterdam 14 juli 2021)

Collectieve claimorganisatie Car Claim komt in een collectieve actie op voor de belangen van bezitters van auto's van de merken Volkswagen, Audi, Škoda en Seat met een dieselmotor met sjoemelsoftware: software die ervoor zorgde dat het bij de test leek alsof aan de normen voor uitstoot werd voldaan, terwijl de motor in feite meer uitstootte dan was toegestaan. De rechtbank oordeelt dat de autofabrikanten onrechtmatig hebben gehandeld, doordat zij met de sjoemelsoftware de toezichthouder en de kopers van de auto's opzettelijk hebben misleid. De autodealers hebben auto's verkocht die door de sjoemelsoftware niet aan de redelijke verwachtingen van de kopers voldeden. Daarom hebben de kopers jegens de autodealers recht op prijsvermindering van 3000 (nieuwe auto) of 1500 (tweedehands) euro.

https://bit.ly/38Rq9uE

Softwarefouten versus SLA
(Rechtbank Noord-Holland 14 juli 2021)

Het bedrijf Quadrant heeft aan afnemen Bioworqz software geleverd en deze geïmplementeerd. Hiervoor heeft zij zes facturen aan Bioworqz gestuurd, waarvan maar twee zijn betaald. De klant voert als reden aan dat Quadrant wanprestatie pleegt, doordat de software volgens hen niet goed werkt. Zij onderbouwt dit echter onvoldoende: volgens de rechtbank had het op de weg van Bioworqz gelegen om, al dan niet aan de hand van bevindingen van deskundigen, aan te tonen dat de door Quadrant geleverde software niet aan de te stellen eisen voldeed. Ook had Bioworqz Quadrant onder vermelding van de geconstateerde gebreken, schriftelijk in gebreke moeten stellen, al dan niet gevolgd door ontbinding van de overeenkomst. Ook faalt het verweer van Bioworqz dat de door haar van Quadrant gevraagde herstelwerkzaamheden onder de werkzaamheden vielen, waarvoor Bioworqz een serviceabonnement had en waarvoor zij maandelijks een bedrag van € 159,00 betaalde.

https://bit.ly/3l6RFKq

Pepperflow tegen SEP

(Rechtbank Gelderland 14 juli 2021)

Het bedrijf Pepperflow is een softwareontwikkelaar, die met het bedrijf SEP (een adviesorgaan over informatiesecurity) wilde samenwerken voor reselling. Nadat de samenwerking mislukt bleek, hadden wel een aantal klanten via SEP software van Pepperflow geleverd gekregen. Er ontstaat ruzie over de facturen: SEP meent dat de software van Pepperflow ernstige gebreken vertoont, dat klanten ontevreden zijn en dat om die redenen de al betaalde facturen onverschuldigd aan Pepperflow zijn betaald. De rechtbank stelt SEP in het ongelijk en oordeelt dat Pepperflow gedurende de onderhandelingen te goeder trouw heeft gehandeld. Het benaderen van een klant van SEP door Pepperflow wordt niet als onrechtmatig handelen gekwalificeerd, omdat SEP de betreffende klant ook te kennen had gegeven dat zij haar werkzaamheden zou opschorten. Pepperflow heeft enkel in deze leemte voorzien en heeft zich niet negatief uitgelaten over SEP. De vorderingen van SEP worden afgewezen en Pepperflow wordt grotendeels in het gelijk gesteld.

https://bit.ly/2Yx4rKB

Kinderfilmpjes door vader

(Rechtbank Gelderland 26 juli 2021)

Een vader van drie kinderen heeft geen contact meer met hen, maar probeert toch de herinnering aan zijn kinderen levend te houden door foto's en filmpjes van hen te delen op social media. Onder toezicht van de gecertificeerde instelling (GI) heeft de vader een schriftelijke aanwijzing ontvangen om deze te verwijderen op grond van ernstige ontwikkelingsbedreiging wegens achterliggend trauma. De vader verzoekt om vervallenverklaring van de schriftelijke aanwijzing onder meer met een beroep op zijn recht op vrijheid van meningsuiting. De kinderrechter wijst het verzoek van de vader af. De kinderen zijn onder behandeling voor trauma's die weer opleven bij het zien van de filmpjes, hetgeen deze behandeling in de weg staat. Het belang van de kinderen om hun persoonlijke levenssfeer te eerbiedigen, weegt zwaarder dan het belang van de vader.

https://bit.ly/3hcIneU

Eiser tegen GBLT

(Rechtbank Overijssel 11 augustus 2021)

Een burger heeft bij het gemeenschappelijke belastingkantoor Lococensus-Tricijn (GBLT) inzage gevorderd in zijn persoonsgegevens, en geëist dat zijn e-mailadres werd verwijderd, dit naar aanleiding van een datalek bij het GBLT. Echter, de burger constateert dat niet alle door hem verzochte persoonsgegevens aan hem zijn toegestuurd. Verder zegt hij dat hij geen toestemming heeft gegeven voor het gebruik van zijn mailadres voor klantonderzoek. Ten derde is volgens eiser tijdens een digitale hoorzitting een geluidsopname gemaakt door GBLT, die men weigert af te geven. De rechter gaat echter mee met het bestuursorgaan, en merkt de beslissing om de geluidsopname niet te verstrekken niet aan als een besluit. Wat betreft het gebruik van zijn e-mailadres voor klantonderzoek, oordeelt de rechtbank dat verweerder aan zijn verplichtingen heeft voldaan door het e-mailadres op verzoek van eiser te verwijderen. Het verzoek van eiser wordt ongegrond verklaard.

https://bit.ly/3E13fQa

Youtube-overtreding

(Rechtbank Amsterdam 18 augustus 2021)

Een Tweede Kamerlid beheert een YouTube-nieuwskanaal samen met een bestuurder. Op dit kanaal plaatsen zij een video met daarin het Kamerlid dat kritische vragen stelt aan de directeur infectieziektenbestrijding van het RIVM, en een interviewvideo die hierop volgde, waarin een deel van de Kamervideo is te zien. In de servicevoorwaarden van YouTube staat dat content verwijderd mag worden indien deze de overeenkomst schendt. Volgens het COVID-beleid is het niet toegestaan om misleidende medische informatie te verspreiden via het platform. Eisers stellen dat dit beleid niet geschonden is, omdat de Nederlandse gezagheb-

bende autoriteit op het gebied van infectieziekten aan het woord komt. De rechtbank stelt voorop dat Google met haar COVID-beleid in beginsel rechtmatig handelt, omdat zij de officiële kanalen omtrent informatie hierover volgt. Omdat de video verboden uitingen bevat over mondkapjes, social distancing en de vergelijking met griep, en bovendien ten onrechte beweert dat vaccins het risico op COVID-19 niet verkleinen en de bepaling die verbiedt te beweren dat kinderen geen COVID-19 kunnen krijgen, mag Google deze blokkeren.

https://bit.ly/38MMrOe

Martijn Michael
Juridisch adviseur

Jorien Zwaneveld
Juridisch adviseur &
Information security consultant

Innovatie Overheid

Geld van de toekomst?

De Europese Centrale Bank ("ECB") is voornemens om een eigen digitale munt in te voeren: de digitale euro, ook wel 'e-euro' of 'deuro' genoemd. In dit artikel praten we u – aan de hand van de gepubliceerde onderzoeken van de ECB – bij over de deuro, mogelijke aanleidingen voor de digitale munt en verschillende aandachtspunten en uitdagingen bij de uitwerking ervan.

D'euro, quoi?

Naast de digitale yuan en digitale dollar moet de digitale euro vanaf 2026 het licht zien. Net als zijn Amerikaanse en Chinese tegenhangers is de deuro een 'digitale centralebankvaluta'.

Kenmerkend voor centralebankvaluta is dat deze direct worden uitgegeven door een centrale bank. Het Verdrag voor de Werking van de Europese Unie ("VWEU") stelt dat het de taak is van het Europees Stelsel van Centrale Banken ("ESCB") om prijsstabiliteit na te streven.[1] Met andere woorden: ervoor te zorgen dat uw euro, met inachtneming van bepaalde marges, morgen nog steeds een euro waard is. De vraag is dan: "wanneer heeft u een euro?".

1. Art. 127(1) VWEU.

Met betrekking tot contant geld, of geld dat op een rekening staat bij het ESCB, is die vraag makkelijk te beantwoorden. Deze zijn immers direct uitgegeven door het ESCB. Met betrekking tot geld op een rekening bij een commerciële bank ligt het ingewikkelder – dat betreft in principe namelijk slechts een vordering op een private partij, niet een daadwerkelijke euro.

Een vierde soort geld

Momenteel bestaan er drie soorten geld: (i) contant geld (ii) centralebankreserves en (iii) commerciële-bankgeld. Reserves worden ingezet om betaalverkeer tussen overheden, banken en andere financiële instellingen te bewerkstelligen, terwijl contanten en commerciëlebankgelden samen de bulk van het reguliere betaalverkeer vormen. Commerciëlebankgeld wordt niet uitgegeven door het ESCB, maar gecreëerd door commerciële banken, bijvoorbeeld door het aanbieden van leningen. Geld op een commerciële bankrekening correspondeert daardoor niet 1:1 met contant geld in de bankkluis en is, zoals beschreven, niet hetzelfde als bezit van een gelijk bedrag in contanten. Het idee achter de deuro is het ontwikkelen van een vierde soort, die de zekerheid kan bieden van (i) en (ii), met het gebruiksgemak van (iii).[2]

2. https://bit.ly/3l1xihC (p.7)

Een digitale centralebankvaluta biedt dus dezelfde zekerheid als contante valuta en centralebankreserves en kan worden gezien als een digitale versie van contant geld. Omdat deze direct door het ESCB wordt uitgegeven zijn er hiermee voor gebruikers

minder risico's gemoeid dan wanneer zij dat bedrag onderbrengen bij een commerciële bank.[3] Naarmate we weg bewegen van contant geld, is men namelijk steeds afhankelijker van commerciële partijen zoals creditcardmaatschappijen, betaaldienstverleners en banken om deel te kunnen nemen aan het digitale betaalverkeer. Hoewel die partijen gereguleerd zijn, is er sprake van extra kosten, vertragingen en andere risico's (zie het faillissement van verschillende banken in 2008) die kunnen inhouden dat tegoeden op essentiële momenten niet beschikbaar zijn. Arme burgers worden hier vaak het hardst door geraakt.[4] De stabiliteit van het ESCB en haar centrale rol in de centralebankvaluta maakt deuro-investeringen een veiligere keuze. Toch is het niet de bedoeling om commerciële banken buiten spel te zetten of daarmee te concurreren. De ECB erkent de belangrijke rol van commerciële banken bij niet alleen de uitrol en uitvoer van centraal bepaald monetair beleid (waaronder een eventuele deuro), maar ook bij de werking van het financieel systeem op zich.[5]

3. https://bit.ly/3hdRA6C (p.21,32)
4. https://bit.ly/3E84gG6
5. https://bit.ly/3hdRA6C (p.32)

Deuro ≠ crypteuro

Die genoemde taak van het ESCB zou ook van toepassing zijn op een deuro. Daarmee verschilt het van crypto-assets en crypto-currency ("crypto"). De term 'digitale euro' wekt misschien de indruk dat Europa voorbereidingen treft voor zijn eigen crypto. Dit is zeker niet het geval. De hoofdgedachte achter crypto is, in tegenstelling tot het eerdergenoemde, juist het omzeilen van centraal beheer en facilitering van een betaalmiddel dat onafhankelijk is van commerciële en centrale bankinstellingen. Het feit dat beheer van de digitale centralebankvaluta voor rekening van het ESCB dient te komen is hierbij het leidende verschil.

Waarom?

Het algemene doel van de deuro is het bieden van *"costless access to a simple, universally accepted, safe and trusted means of payment"*. Verder moeten deuro's toegankelijk, betrouwbaar, veilig, efficiënt, privacyvriendelijk en in overeenstemming met wet- en regelgeving zijn.[6]

6. https://bit.ly/3hfw69A

De ECB beschrijft verschillende scenario's die aanleiding kunnen geven tot de uitgifte van deuro's.[7] Op basis van deze scenario's formuleert de ECB telkens vereisten waaraan de deuro moet voldoen.

7. https://bit.ly/3hdRA6C (p.9-15)

Digitalisatie

Als eerst stelt de ECB dat de invoer van een deuro in het algemeen kan bijdragen aan de digitalisatie van de Europese economie. Zo zou het bijvoorbeeld de ontwikkeling van innovatieve pan-Europese betaalnetwerken kunnen stimuleren en Europa in dat opzicht autonomie bieden ten opzichte van concurrerende oplossingen. Om te antwoorden op dit scenario is het volgens de ECB vereist dat de digitale efficiëntie en moderniteit van het deuro-systeem voorop staat.

Afname contante betalingen

Als tweede stelt de ECB dat het gebruik van contant geld verder zal afnemen. Dit betekent dat de voordelen van contant geld zoals anonimiteit, eenvoudigheid, gebruiksgemak, gebrek aan risico's gerelateerd aan commerciële banken en de mogelijkheid tot het doen van kosteloze, offline betalingen voor gebruikers wegvallen. In dit kader is het belangrijk dat een deuro die kenmerken van contant geld zo veel mogelijk spiegelt.

Concurrerende ruil- en betaalmiddelen

In het derde scenario krijgt een buitenlandse digitale centralebankvaluta of een ongereguleerd alternatief zoals 'stablecoin'[8] vaste voet op de Europese markt. Zo'n situatie zou onder andere de mogelijkheden tot toezicht en regulering met betrekking tot de financiële markt en economie en (huidige) uitrol van monetair beleid in Europa flink in de weg zitten. Een deuro moet dus aantrekkelijker zijn dan ongereguleerde of buitenlandse alternatieven.

8. https://bit.ly/3tsqz4q

Monetair beleid

Hoewel de ECB nog geen concrete voorbeelden kan formuleren, acht zij het als vierde denkbaar dat een deuro ingezet kan worden als instrument om monetair beleid te bewerkstelligen. Zo zou een eventuele mogelijkheid om deuro-rente te bepalen haar in staat stellen om, naast haar huidige invloed op de Europese financiële sector, ook de consumptie en investeringen van de niet-financiële sector te beïnvloeden.[9]

9. https://bit.ly/3hd9o1O

Noodsituaties

Het vijfde scenario omvat situaties waarin private digitale betalingsinfrastructuur wordt belemmerd. Naarmate we meer richting digitale betaalsystemen bewegen nemen ook de cybersecurityrisico's toe.[10] Dergelijke infrastructuren zijn tevens vatbaar voor natuurrampen en andere onverwachte omstandigheden. Dit kan ertoe leiden dat private betaaloplossingen niet beschikbaar zijn. Een deuro kan in die gevallen soelaas bieden. Om te antwoorden op dit scenario dient de deuro-infrastructuur gescheiden te worden van de bestaande betalingsinfrastructuren, offline gebruikt te kunnen worden en dusdanig weerbaar te zijn dat het extreme situaties kan doorstaan.

Ondersteuning doelstellingen EU in brede zin

Naast de doelstelling van prijsstabiliteit, volgt uit artikel 127 VWEU dat het ESCB bijdraagt aan de doelstellingen van de Europese Unie zoals beschreven in artikel 3 van het verdrag. In dat kader formuleert de ECB twee aanvullende scenario's die aanleiding kunnen geven tot een deuro.

Internationale rol

In het zesde scenario gaat groei van buitenlandse digitale centralebankvaluta ten koste van de relevantie en status van de euro. Een internationale rol voor de euro kan bijdragen aan Europese economische autonomie.[11] Dit scenario kan worden beantwoord door buitenlandse deuro-investeerders aan te trekken. Ook kan de internationale rol van de euro worden versterkt zónder deuro's aan te bieden aan niet-ingezetenen van de Unie, maar juist door interoperabiliteit van deurosystemen met buitenlandse systemen te bewerkstelligen.

11. https://bit.ly/3zTypXa

Ecologische voetafdruk

Het onderhouden van betalingsinfrastructuren is vaak kostbaar en slecht voor het milieu.[12] In het zevende scenario kunnen deuro's een rol spelen bij het nastreven van de klimaat-gerelateerde doelstellingen van de Europese Unie. Daarvoor is het vereist dat de uitwerking ervan een kostenbesparing inhoudt ten opzichte van de bestaande betalingsinfrastructuren en een kleinere ecologische voetafdruk heeft.[10]

12. https://bit.ly/3hdfCOW

Uitwerking en uitdagingen

Over de praktische uitwerking van de deuro, alsmede welke doelstellingen en aanleidingen bij die uitwerking voorop moeten staan, bestaat discussie. Zo blijkt dat de ECB doelen, aanleidingen en mogelijke praktische uitwerkingen van de deuro stelt, waarbij vaak sprake is van onderlinge tegenstrijd en uiteenlopende mogelijkheden.

Technische aanpak

De ECB onderzoekt welke technische aanpak het passendst is voor de deuro. Daarbij zijn gecentraliseerde ('target instant payment settlement'[13]) en gedecentraliseerde ('distributed ledger technology') systemen, een combinatie van beide, alsmede het gebruik van offline systemen uitgebreid getest.[10] De hierin gemaakte keuzes hebben invloed op verschillende scenario's en doelstellingen. Zo staan gedecentraliseerde ledgersystemen berucht om hun ecologische voetafdruk en betekent het niet-faciliteren van offline gebruik dat de deuro minder geschikt is als back-up voor contanten.

13. https://bit.ly/2Yxq5hP

Eindgebruik

Kunnen we binnenkort de opening van loketten van de ECB verwachten? Waarschijnlijk niet. De ECB is niet ingericht als consumentenbank. Het is waarschijnlijk dat commerciële banken of andere tussenpersonen naast de huidige dienstverlening deuro's gaan aanbieden aan gebruikers.[10] Dit wringt met de doelstelling dat gebruik van de deuro kosteloos moet zijn. Immers willen partijen waarschijnlijk een vergoeding voor deuro-gerelateerde dienstverlening.[10] Het gebruik van commerciële intermediairs betekent dat verschillende genoemde centralebankvaluta-gerelateerde zekerheidsvoordelen (zie het noodsituatie-scenario) wegvallen naarmate men voor de deuro-infrastructuur afhankelijk is van commerciële partijen. Zo lang het onmogelijk is om rechtstreeks bij het ESCB een bankrekening te openen, kunnen de doelstellingen 'safe, risk-free en cost-free' niet gegarandeerd worden: dit is afhankelijk van de handelswijze en weerbaarheid van de tussenpersoon.

Bankruns?

Naarmate een deuro meer van de genoemde zekerheidsvoordelen kent, bestaat er risico dat commerciële banken worden gepasseerd. Waar er voorheen bij aanwijzingen van instabiliteit van een bank bankruns waren, biedt een deurosysteem de moge-

lijkheid om commerciëlebankgeld om te zetten naar deuro's. Dergelijke transfers verschillen niet veel van een fysieke bankrun. In beide gevallen vertegenwoordigen de commerciëlebankgelden niet een aanwezige hoeveelheid fysieke/digitale (d)euro's en kan grootschalige omzetting de economie ontwrichten.

Om dit te voorkomen en de rol van commerciële banken te waarborgen zijn er volgens het ECB verschillende oplossingen mogelijk – waaronder stellen van een deuro-limiet (€3.000,-), of bij overschrijding van een deuro-limiet negatieve rente te hanteren.[14] Buiten de praktische uitdagingen, levert dit problemen op met de genoemde toegankelijkheid- en eenvoudigheidsdoelstellingen.[10]

14. https://bit.ly/3hdRA6C (p.28)

Privacy, veiligheid en gecontroleerde anonimiteit

Bij de uitrol van een digitaal betaalsysteem komen privacybelangen kijken. Fabio Panetta, ECB-bestuurslid, gelooft dat inachtneming van Europese privacywetgeving in combinatie met een FG in beginsel voldoende is om de privacy van betrokkenen te waarborgen.[10] Vooralsnog blijft het bij de geruststelling dat privacybelangen beter gewaarborgd worden bij de deuro dan bij commerciële banken, omdat er geen commerciële belangen spelen bij het opslaan, analyseren en doorgeven van de verwerkte gegevens. Hoewel dit een goed uitgangspunt is, geeft het geen garanties.

10. https://bit.ly/2Yrvmr9

Dat kan problematisch zijn. Vertrouwen in de deuro en het ESCB is belangrijk. Gebruikers moeten erop vertrouwen dat transacties niet worden gecontroleerd en er geen misbruik wordt gemaakt van verzamelde data. De Chinese digitale centralebankvaluta is uitgegeven met als opgegeven doel om witwassen, gokken, corruptie en terrorismefinanciering te bestrijden. Uitgangspunt hierbij was zogeheten 'controllable anonymity': persoonlijke informatie is afgeschermd, tenzij er verdachte transacties worden verricht.[15] Critici zien het echter vooral als middel om individuen te controleren.

15. https://on.wsj.com/3yOb3AM

De anonimiteit van cashbetalingen is, ondanks de eerdergenoemde doelstellingen, met de invoering van de deuro waarschijnlijk verleden tijd. Volledige anonimiteit bij digitale betalingen is door de huidige wetgeving niet toegestaan. Volgens de ECB kunnen privacybelangen echter ook zonder anonimiteit gewaarborgd worden, omdat het delen van transactie- en persoonsgegevens met derde partijen niet nodig is voor het afwikkelen van betalingen.[16]

16. https://bit.ly/3hdRA6C (p.27)

Wettelijke basis

Er moet een wettelijke basis bestaan voor de uitgifte van een deuro. Hier bestaat volgens de ECB voldoende keuze in, afhankelijk van de gekozen vormgeving.[17]

17. https://bit.ly/3hdRA6C

De grondslag die het meest in lijn ligt met de deuro zoals besproken is vervat in artikel 128(1) VWEU en artikel 16 van de statuten van het ESCB. In dit kader worden deuro's als bankbiljet-equivalenten beschouwd. Andere door de ECB genoemde grondslagen zijn volgens de ECB passender voor een beperkt bruikbare deuro, zonder status van wettig betaalmiddel. Noch de wet noch de statuten sluiten uit dat het ESCB wettige betaalmiddelen uitgeeft in een andere vorm dan bankbiljetten. De vraag of het recht tot "uitgifte van bankbiljetten" zoals bedoeld in artikel 128(1) VWEU ook het recht zou kunnen omvatten om te bepalen in welke vorm deze bankbiljetten worden uitgegeven, wordt door de ECB daarnaast bevestigend beantwoord.

Voor uitrol, toezicht en regulering van de deurosystemen en eventueel daarbij ingezette tussenpersonen, kan op basis van artikel 133 VWEU wetgeving worden vastgesteld.

Warm welkom?

Hoewel 2026 relatief dichtbij is, is er nog veel onduidelijkheid rondom de deuro. De ECB overweegt verschillende uitwerkingen en genoemde doelstellingen en de antwoorden op beschreven scenario's spreken elkaar regelmatig tegen. Pas als er concretere plannen op tafel komen kan worden vastgesteld of de deuro een warm welkom zal krijgen. Een prangende vraag blijft: is dit dé verandering van het financiële systeem waar we op zaten te wachten, of wordt de deuro alleen ingevoerd omdat Europa bang is om achter te blijven op China, Amerika of crypto?

Arnoud Engelfriet
Algemeen directeur / Opleidingsdirecteur

Cloud

Noot bij HR 25 juni 2021 (Dutch Filmworks tegen Ziggo)

Wat kost een auteursrechtinbreuk? Met die vraag worstelen rechters (en rechthebbenden) al vele jaren. De problematiek van de "Getty-claim" is bij juridische professionals al langer bekend: een vaak kleine ondernemer of consument publiceert een foto van een stockbeelddienst zoals Getty of Masterfile, en krijgt een rekening van vele duizenden euro's met vele toegevoegde posten. Met dit arrest is er weer een mijlpaal(tje) bij: wie zich te zeer op de vlakte houdt over de te claimen vergoeding, krijgt ook nul op het rekest.

Bepalen van schade bij (online) inbreuk

Het concreet bepalen van de schade door een auteursrechtinbreuk is en blijft een moeilijke zaak. In de regel berust de berekening van een schadevergoeding op een concrete schadebegroting, waarbij de begroting zo veel mogelijk is gebaseerd op de concrete, individuele omstandigheden van de benadeelde. Dat werkt echter niet bij dit soort claims, onder meer omdat er geen officiële prijslijsten of taxateurs zijn die een concreet bedrag kunnen aanwijzen. Abstracte begroting is dan ook de enige reële optie. De rechter begroot dan de schade op de wijze die het meest met de aard ervan in overeenstemming is (art. 6:97 BW). Bij auteursrechtinbreuken wordt de wijze van begroting nader ingevuld door artikel 27(2) Auteurswet dat aan de rechter de basis geeft om een forfaitair bedrag vast te stellen.

Het forfaitair bedrag als schadevergoeding dient in beginsel, zo blijkt uit overweging 26 van de Handhavingsrichtlijn, te worden vastgesteld rekening houdend met alle omstandigheden van het geval. De overweging noemt als voorbeelden van dergelijke omstandigheden "het door de rechthebbende geleden inkomensverlies of de door de inbreukmaker onrechtmatig gemaakte winst".[1] Als alternatieve bepalingswijze noemt de overweging de vaststelling van "het bedrag aan royalty's of vergoedingen [dat] verschuldigd zou zijn geweest indien de inbreukmaker toestemming had gevraagd". Hierbij mag tevens rekening worden gehouden met kosten voor de rechthebbende, zoals voor opsporing en onderzoek.[2] In Nederland is bij de implementatie van de Handhavingsrichtlijn over deze bepalingswijze het volgende opgemerkt: "Dit bedrag kan bijvoorbeeld vastgesteld worden op basis van de licentievergoeding die verschuldigd zou zijn geweest indien de auteursrechthebbende toestemming zou hebben gegeven".[3]

Opmerking verdient nog dat de Handhavingsrichtlijn in diezelfde overweging 26 spreekt van een schadevergoedingsplicht voor "de inbreukmaker die wist of redelijkerwijs had moeten weten dat hij inbreuk pleegde". Hierin zien diverse rechters een aanknopingspunt om bij een niet-opzettelijke en kleinschalige inbreuk een lagere vergoeding toe te wijzen dan gevorderd.[4]

Dit kan worden gerechtvaardigd als een impliciet gebruik van de bevoegdheid tot matiging (art. 6:109 lid 1 BW). Om de schade te bepalen is een eerste belangrijke vraag welk bedrag aan royalty's of vergoedingen verschuldigd zou zijn geweest indien er om toestemming was gevraagd. Hoofdregel hierbij is dat het gaat om de vergoeding die aan deze rechthebbende verschuldigd zou zijn geweest, niet om enkel een marktconforme vergoeding.

Kanttekening daarbij is dat strafrechtelijke handhaving in het auteursrecht vrijwel volstrekt afwezig is. Hoewel formeel de opzettelijke schending van het auteursrecht een misdrijf is, komt het Openbaar Ministerie slechts in zeer uitzonderlijke gevallen in actie.[5] Er moet sprake zijn van grootschalige inbreuk die verband houdt met georganiseerde misdaad of de volksgezondheid bedreigt. Het soort inbreuken dat in dit onderzoek centraal staat, voldoet volstrekt niet aan dit criterium.

1. Richtlijn 2004/48 EG PbEU 2004, L 157/45, hierna de "Handhavingsrichtlijn".
2. Art. 6:96 lid 2 BW.
3. MvT bij het voorstel voor de omzettingswet, Kamerstukken II, 2005/06, 30392, nr. 3, p. 27.
4. Rb. Noord-Holland (ktr.) 27 mei 2015, IEF 14990, Rb. Rotterdam 10 augustus 2012, 12-8738, Rb. Rotterdam (ktr.) 18 oktober 2013, IEF 13604, Rb. Rotterdam (ktr.) 10 augustus 2012, ECLI:NL:RBROT:2012:BY3179.
5. Aanwijzing intellectuele-eigendomsfraude (2005A022), Stcrt. 2006, nr. 6. Verlengd bij besluit tot 31 januari 2016, Stcrt. 2012, nr. 1754. Zie ook Spoor/Verkade/Visser 2005, p. 534.

Dutch Filmworks op zoek naar schade

In een langlopend geschil eist Dutch Filmworks dat Ziggo structureel NAW-gegevens verstrekt van consumenten die via Ziggo illegaal films downloaden waar DFW producent of distributeur van is. Rechtbank en Hof hebben deze eisen beiden afgewezen, met name omdat DFW te zeer op de vlakte blijft bij de vraag wat men precies gaat eisen van deze consumenten. DFW spreekt in de media bijvoorbeeld van het "opleggen van boetes" en schermt met bedragen als 150 euro, wat wringt met de opstelling in de rechtszaal waarin men zegt consumenten op constructieve manier aan te willen spreken en een reële schadevergoeding wil verzoeken. Mede hierdoor oordeelde het Hof dat Ziggo zo niet op een fatsoenlijke manier haar klanten kan informeren over de voorgenomen verstrekking van persoonsgegevens. De HR bekrachtigt de uitspraak zonder nadere motivatie (art. 81 RO). De rechtszaak was het logisch gevolg van DFW's plan downloaders aan te spreken op illegaal downloaden, inclusief boete, pardon schikkingsvoorstel van 50, pardon 150 euro, pardon een nader te bepalen maatregel per download. Nodig daarvoor is dat providers NAW-gegevens verstrekken wanneer DFW een IP-adres verstrekt en een rapportje dat er daarmee gedownload is. Maar, zoals de rechtbank in eerste instantie[6] opmerkte: "De opmerking van DFW ter zitting dat er een brief zal worden gestuurd en dat er dan rustig zal worden afgewacht wat de reactie zal zijn, is erg mager, zeker in de omstandigheid dat de inhoud van de brief niet (voldoende) bekend is."

Het Gerechtshof ging er eens goed voor zitten[7] en bekeek de vier criteria uit dat arrest nog eens streng. Het gaat hier om een 'kleine' inbreuk (één keer een film), onduidelijk is hoe DFW aan het bedrag komt en wat doe je als de IP-adreshouder niet zelf de downloader blijkt? Je moet echt een goede onderbouwing geven van deze zaken alvorens een provider NAW-gegevens moet geven, en DFW had die niet overlegd: "Het bedrag dat DFW thans wenst te ontvangen, vermoedelijk € 150,–, is echter op geen enkele wijze onderbouwd en niet is uitgesloten dat in het door DFW te vragen schadebedrag ook elementen van een boete zitten". In het door DFW opgestelde Protocol waarin zij een toelichting geeft, vermeldt zij slechts dat zij steeds per geval zal beoordelen welke acties of vervolgstappen zij tegen een betrokkene wenst te ondernemen. Dat is te makkelijk; DFW kan zo nadat zij de persoonsgegevens heeft gekregen, eenzijdig en zonder enige motivering of toelichting de actie te kiezen die haar goeddunkt. Dat leidt naar het oordeel van het Gerechtshof tot een verstoring van het te vinden evenwicht, met name in de situatie dat onzeker is of de betrokken Ziggo-klant ook daadwerkelijk de inbreukmaker is, wat een reëel risico is. Onder die omstandigheden hoeft Ziggo niet mee te werken, aldus het Hof. De HR vindt dit zo vanzelfsprekend dat zij er niet eens een motivering aan wijdt.

6. Rechtbank Midden-Nederland 8 februari 2019, ECLI:NL:RBMNE:2019:423.
7. Gerechtshof Arnhem-Leeuwarden 5 november 2019, ECLI:NL:GHARL:2019:9352.

Privacy

Data Transfer Impact Assessment: weer een nieuw begrip!

Van onze blog
4 augustus 2021

Nee, in deze blog gaan we het niet weer hebben over het Privacy Shield. Dat weten we inmiddels wel. Persoonsgegevens kunnen doorgegeven worden aan leveranciers uit de Verenigde Staten, en andere derde landen, op basis van de nieuwe Standard Contractual Clauses (SCC's). Maar dan bent u er nog niet. Er zal ook een Data Transfer Impact Assessment uitgevoerd moeten worden. "Een wat?" denkt u misschien, wat dat is leggen we uit in deze blog.

Passende waarborgen

Persoonsgegevens mogen worden doorgegeven naar een land buiten de Europese Economische Ruimte (EER) als daar passende waarborgen voor zijn getroffen. Welke passende waarborgen organisaties kunnen treffen volgt uit hoofdstuk V van de Algemene verordening gegevensbescherming (AVG).

Een van de meest gebruikte passende waarborgen is het sluiten van de SCC's. Onlangs zijn de SCC's vernieuwd. Voortaan kunnen de SCC's in onderstaande gevallen gesloten worden:

1. Verwerkingsverantwoordelijke naar verwerkingsverantwoordelijke
2. Verwerkingsverantwoordelijke naar verwerker
3. (Sub)verwerker naar (sub)verwerker
4. (Sub)verwerker naar verwerkingsverantwoordelijke

De Europese Commissie heeft de verschillende sets in één lang document gepubliceerd, dat organisaties zelf op maat dienen te maken. Dat is niet zo handig. Daarom hebben we met onze zusterorganisatie JuriBlox een tool ontwikkeld, waarmee je zelf de juiste SCC's kunt genereren, met zowel een Nederlandse[1] als een Engelse[2] vragenlijst (de SCC's zelf zijn altijd in het Engels). Helemaal gratis!

1. https://jrbx.nl/EwQzdrxzBUo6APXu
2. https://jrbx.nl/mj5M2CCCnd0XQXTP

Risicoanalyse voor doorgifte van persoonsgegevens

Met het sluiten van de SCC's bent u er nog niet. Per doorgifte zal een risicoanalyse gedaan moeten worden: een contractuele afspraak is niet meer voldoende, vooral niet als de wetgeving in het ontvangende land niet beschermend genoeg is. Dit wordt ook wel de Data Transfer Impact Assessment (DTIA) genoemd. Uit de DTIA moet volgen waarom de organisatie gebruik maakt van een leverancier die gevestigd is in een derde land, en op welke wijze ervoor wordt gezorgd dat de privacy van betrokkenen wordt gewaarborgd.

Welke onderwerpen komen aan bod in de DTIA?

Dienstverlening

De DTIA moet een omschrijving bevatten van de diensten die worden aangeboden door de leverancier die gevestigd is in een derde land. Gaat het bijvoorbeeld om een hostingprovider, softwareleverancier of marketingpartij? Wordt er support geleverd vanuit een derde land of is het misschien mogelijk om aan de hand van een bepaalde tool nieuwsbrieven te versturen?

Passende waarborgen

Welke passende waarborgen worden getroffen? Denk aan het sluiten van de SCC's of wellicht worden persoonsgegevens doorgegeven op basis van Binding Corporate Rules.

Technische, organisatorische en contractuele maatregelen

Niet geheel onbelangrijk is natuurlijk welke maatregelen er worden getroffen om persoonsgegevens te beschermen, aanvullend op de SCC's. Denk aan dataminimalisatie, encryptie en het pseudonimiseren of misschien wel anonimiseren van persoonsgegevens. Een andere maatregel is dat partijen contractueel afspreken dat persoonsgegevens binnen de EER worden gehost.

Wetgeving in het ontvangende land

Om tot een gedegen DTIA te komen is het van belang dat de nationale wetgeving van het land van de leverancier wordt bekeken. Het is vrijwel onmogelijk om kennis te hebben van alle wet- en regelgeving. Als u gebruik maakt van een Amerikaanse leverancier dan speelt bijvoorbeeld de Foreign Intelligence Surveillance Act (FISA) een belangrijke rol. Elke ICT-dienstverlener die gevestigd is in de VS, is gebonden aan de FISA. In een van de bepalingen is opgenomen dat een speciale rechtbank een bevel kan geven tot surveillance. Naast de FISA staan in de USA Freedom Act ook allerlei bepalingen inzake surveillance.

Elke organisatie dient zelf te bepalen of zij verwacht onderwerp te zijn van deze wetgeving, of dat dat risico verwaarloosbaar is. Het Amerikaanse Ministerie van Handel heeft bijvoorbeeld wel aangegeven dat veruit de meeste commerciële doorgiften van persoonsgegevens naar de VS niet van belang zijn voor de Amerikaanse inlichtingen- en veiligheidsdiensten.

Risicobeoordeling

Uiteindelijk volgt er een risicobeoordeling. Is de inzet van bijvoorbeeld een Amerikaanse leverancier noodzakelijk? Of kan er gebruik worden gemaakt van een partij die in Europa of misschien zelfs wel in Nederland gevestigd is? Welke risico's spelen er in het derde land en zijn die risico's aanvaardbaar?

Hulp nodig met het uitvoeren van een Data Transfer Impact Assessment? Laat het ons weten!

Auteur
Beryl Hetharia
Juridisch adviseur

Bent u goed voorbereid op uw cloudtransitie?

ICTRECHT
adviesbureau

WIECK MOLENDIJK
CONSULTANTS

Doe de quickscan!

Uw organisatie gaat over naar de cloud. Hoe pakt u een cloudtransitie aan die zoveel impact heeft? Wieck Molendijk consultants en ICTRecht hebben samen alle kennis in huis om u op alle fronten te ondersteunen bij een prettige overgang naar de cloud.

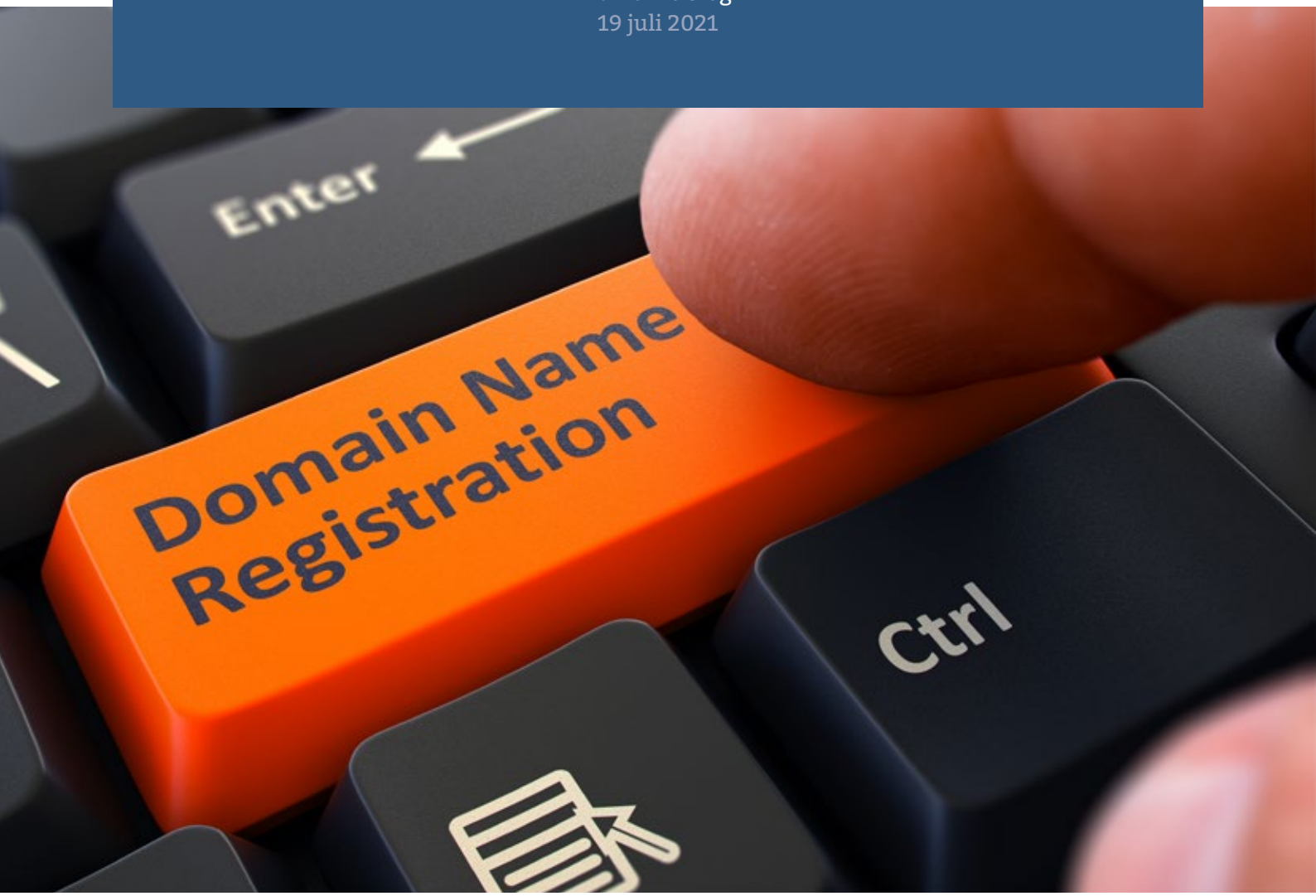
Krijg binnen 5 minuten inzicht in uw uitgangspositie
en de te nemen vervolgstappen met onze online quickscan.

Ga nu aan de slag!
ictrecht.nl/cloudtransitie-quickscan

Cloud

Domeinnaam overdragen of houden? Check uw kans van slagen met deze 4 stappen

Van onze blog
19 juli 2021



Regelmatig zien we houders van een of meerdere domeinnamen die gesommeerd zijn om die over te dragen. Deze klanten hebben de domeinnaam soms al jaren en betalen dus ook al tijdenlang instandhoudingskosten. Een ander, vaak een merkhouder, claimt nu recht te hebben op deze domeinnaam. Moet u hier zomaar aan toegeven?

Of u gehouden bent uw domeinnaam over te dragen is afhankelijk van heel veel verschillende factoren. Op basis van het topleveldomein (extensie) wordt bepaald welke regels van toepassing zijn. In grote lijnen lijken de meeste regels op elkaar, maar het beleid is lang niet altijd hetzelfde. Natuurlijk is het verstandig om een check te laten doen door ICTRecht, maar het is ook zeker mogelijk om zelf alvast uw kans van slagen te beoordelen aan de hand van onderstaande stappen.

Domeinnaam houden? Controleer het volgende

1. Heeft de sommerende partij een geregistreerd merk? U kunt het bijvoorbeeld checken via www.boip.int/nl of in de EUIPO Global Brand database.[1] Vaak zal het merk ook genoemd worden in de sommatiebrief. Controleer of dit een geldig merk is. Zit dit merk ook in uw domeinnaam? Dan heeft u kans dat een van de voorwaarden voor overdracht van een domeinnaam vervuld is. Misschien is het echter zo dat het merk ook een eigennaam is waaronder u algemeen bekend bent of dat het merk een algemeen woordenboekwoord is; dat kan zaken veranderen.

1. https://bit.ly/3ngJA8F

2. Controleer op welke datum het merk geregistreerd is en vergelijk dit met de registratiedatum van uw eigen domeinnaam. Als u uw domeinnaam wilt behouden helpt het als uw domeinnaam niet jonger is dan het geregistreerde merk.
3. Gebruikt u de domeinnaam voor een website? Zo ja, wat gebeurt er op die website? Verkoopt u producten van het merk waar het om draait? Biedt u misschien ook andere merken aan? Misschien gebruikt u de domeinnaam helemaal niet voor een website maar alleen om mailtjes vanaf te kunnen sturen. Misschien verwijst uw domeinnaam door naar een andere domeinnaam en website? De activiteit op de website kan van belang zijn bij de beoordeling of u een legitiem belang heeft bij de domeinnaam.
4. Gebruikt u de domeinnaam niet voor een website? Wat is uw intentie met de domeinnaam? Sommige mensen kopen domeinnamen van opkomende merken met het doel ze voor een flink bedrag te verkopen. Weer anderen doen niets inhoudelijks met de domeinnaam, maar hebben wel affiliate links geplaatst op de bijbehorende website. De intentie die blijkt uit het (niet-)gebruik van de domeinnaam is een belangrijke indicatie voor de vraag of u er al dan niet recht op heeft.

ICTRecht assisteert u graag bij uw domeinnaamzaak

Wanneer u een brief ontvangt waarin u gesommeerd wordt de domeinnaam over te dragen is het vrijwel altijd van belang hierop te reageren. ICTRecht heeft ruime ervaring op het gebied van domeinnaamgeschillen en kan vaak snel en kosteloos beoordelen of de zaak kans van slagen heeft. We begeleiden bij verkoop van domeinnamen, onderhandelingen, domeinnaammediation en het opstellen van klacht- en verweerschriften. We leveren hierbij altijd maatwerk en assisteren ook graag bij uw domeinnaamzaak.

Auteur
Vivianne Vermeulen
Juridisch adviseur

ICTRecht Academy

Trainingsoverzicht okt. - dec. 2021

Dinsdag 12 oktober 2021
Contracteren: contracten in ICT (6 PO)
Elk type ICT-contract vereist algemene aandachtspunten en daarnaast specifieke aspecten. Leer de verschillen tussen ICT-contracten te benoemen en een ICT-contract op te zetten.

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

Donderdag 14 oktober 2021
ICT & gezondheidsrecht (6 PO)
Weten welke regels gelden bij het uitwisselen van medische gegevens online? Of welke rechten patiënten hebben? Onze zorgexpert leert u alles over ICT en gezondheidsrecht.

Deze vindt plaats in Utrecht.
Lees meer!
https://bit.ly/2U6eSTz

Donderdag 4 november 2021
Security en datalekken (4 PO)
Tijdens deze training gaan we onder meer in op het melden van datalekken, het stappenplan voor afhandeling van een datalek en het plan van aanpak om een lek preventief te dichten.

Deze vindt plaats in Amsterdam en online. Lees meer!
https://bit.ly/2VLa0Uc

Dinsdag 9 november 2021
FG zorg en informatiebeveiliging
Privacy en informatiebeveiliging zijn nauw met elkaar verbonden. Waartegen dient informatie eigenlijk te worden beschermd, en wanneer zijn de maatregelen 'passend'?

Deze vindt plaats in Utrecht.
Lees meer!
https://bit.ly/3izK0o7

Donderdag 11 november 2021
Privacy: AVG op hoofdlijnen voor niet-juristen
Heeft u in uw werk (als niet-jurist) te maken met persoonsgegevens en wilt u meer over de privacywetgeving weten? In deze praktijkgerichte training komt de AVG uitgebreid aan bod.

Deze vindt plaats in Utrecht.
Lees meer!
https://bit.ly/37B33ru

Dinsdag 16 november 2021
FG in de zorg(praktijk)
Tijdens deze training wordt specifiek ingegaan op de rol, werkzaamheden en bevoegdheden van de FG in de zorg in relatie tot de privacywetgeving en wetgeving binnen de zorgsector.

Deze vindt plaats in Utrecht.
Lees meer!
https://bit.ly/3CwqG2S

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

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

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

De trainingen vinden plaats op locatie in Utrecht en Zwolle & online. De eerstvolgende trainingen starten in oktober 2021. Lees meer!
https://bit.ly/38Mv3t7

Schrijf u gratis in voor onze live webinars!

Maandag 1 november 2021
AVG rechtspraak update (1 PO)
Op de hoogte blijven van actuele privacy rechtspraak en benieuwd welke lessen hieruit kunnen worden getrokken voor de praktijk? Volg dan onze live webinar: AVG rechtspraak update! Gedurende een uur worden de belangrijkste uitspraken én de essenties hiervan besproken onder leiding van onze privacy adviseurs.

Deze vindt online plaats.
Lees meer!
https://bit.ly/3zgw6fE

Maandag 8 november 2021
FG Newsflash
Laat u gedurende een uur bijpraten over de belangrijkste actuele ontwikkelingen die voor een FG relevant zijn. Deze live webinar wordt verzorgd door onze privacy adviseurs die tevens zelf werkzaam zijn als FG. Aan bod komt onder meer de belangrijkste rechtspraak, berichtgeving van de AP en *best practices*. Daarbij wordt een vertaalslag naar de praktijk gemaakt.

Deze vindt online plaats.
Lees meer!
https://bit.ly/2VM4EbZ

Heeft u vragen of wilt u meer weten?
Neem contact op met onze opleidingscoördinator Britt Telleman via e-mail: academy@ictrecht.nl of telefoonnummer: 020 663 1941.

Britt Telleman
Opleidingscoördinator

ICTRECHT
adviesbureau

Meer informatie over hoe wij werken? Bezoek ictrecht.nl