ICTRECHT
adviesbureau

ICTRECHT
IN DE PRAKTIJK

jaargang 9 nummer 1 januari 2021

Grip op leveranciers in de zorg

Wat betekent Strong Customer Authentication voor uw webshop?

Legal tech voor iedereen?

Heeft u uw juridische zaken goed geregeld?

Zeker op het gebied van ICT en privacy is dit geen eenvoudige zaak.
Voorkom juridische ICT- of privacyproblemen en laat ICTRecht u deskundig en praktisch adviseren.
Dat hoeft helemaal niet duur te zijn: naast maatwerk leveren wij standaardproducten en juridische generatoren.

ICTRecht is een flexibel en creatief juridisch adviesbureau. Wij bedienen zowel de grote als de kleine klant. Onze adviezen zijn begrijpelijk, concreet en geven blijk van technische kennis. Onze mensen zijn dan ook juridisch en technisch thuis in onze niche.

Wij kunnen u van dienst zijn met:

Juridische documenten - Juridisch advies - Juridische detachering
Trainingen - Boeken

Meer informatie over hoe wij werken? Bezoek ictrecht.nl

ICTRECHT
adviesbureau

Index

Colofon

Dit is een uitgave van ICTRecht B.V.
020 663 1941, 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:

Arnoud Engelfriet Algemeen directeur en Opleidingsdirecteur
a.engelfriet@ictrecht.nl
Steven Ras Algemeen directeur
s.ras@ictrecht.nl
Kors Monster Directeur ICTRecht Security
k.monster@ictrecht.nl
Sten Demon Manager ICTRecht Detachering
s.demon@ictrecht.nl

Alisa Schurink Marketing adviseur
a.schurink@ictrecht.nl
Anouk van Rijn Juridisch adviseur
a.vanrijn@ictrecht.nl
Ardine Siepman Juridisch adviseur
a.siepman@ictrecht.nl
Beryl Hetharia Juridisch adviseur
b.hetharia@ictrecht.nl
Bram de Vos Juridisch adviseur
b.devos@ictrecht.nl
Britt Telleman Opleidingscoördinator
b.devos@ictrecht.nl

Eline Streefkerk Juridisch adviseur
e.streefkerk@ictrecht.nl
Esther Flierman Juridisch adviseur
e.flierman@ictrecht.nl
Fleur Biegstraaten Juridisch adviseur
f.biegstraaten@ictrecht.nl
Itte Overing Juridisch adviseur
i.overing@ictrecht.nl
Jay Remmelzwaal Juridisch adviseur
j.remmelzwaal@ictrecht.nl
Jorden Bailey Juridisch adviseur
j.bailey@ictrecht.nl
Kim Groot Juridisch adviseur
k.groot@ictrecht.nl
Milan van der Spoel Juridisch adviseur
m.vanderspoel@ictrecht.nl
Nicole Waaijer Marketing adviseur
n.waaijer@ictrecht.nl
Niek Bakker Juridisch adviseur
n.bakker@ictrecht.nl
Tessa van Schijndel Juridisch adviseur
t.vanschijndel@ictrecht.nl
Eline Pellis Grafisch ontwerper
eline@elinepellis.com
Leonard Fäustle Stills & Motion
Foto’s ICTRecht
info@leonardfaustle.nl

Kors Monster
Directeur ICTRecht Security

Itte Overing
Juridisch adviseur

E-health

Grip op leveranciers in de zorg: leveranciers-management conform NEN 7510

Veel zorgaanbieders zijn hard onderweg om zelfs hun primaire proces, het leveren van zorg, digitaal te laten verlopen. Gedwongen door tekorten en de pandemie wordt er flink gesubsidieerd en geïnvesteerd in digitalisering binnen de zorg. De absolute noodzaak van het digitaal uitwisselen van patiëntgegevens werd ineens schrijnend zichtbaar tijdens de eerste lockdown. Voor minister Van Ark reden om flink aan de slag te gaan, het wetsvoorstel Elektronische Gegevensuitwisseling in de Zorg verwacht zij begin 2021 aan de Tweede Kamer toe te sturen.

Wat heb je als gemiddelde zorgaanbieder al in gebruik aan ICT begin 21ste eeuw? Allereerst een zorginformatiesysteem, het bronsysteem waarin de dossiers van patiënten of cliënten worden bijgehouden. Dan, meestal daaraan gekoppeld, een declaratiesysteem waarmee gedeclareerd wordt. Verder, hardware en software in het kader van het leveren van specialistische zorg al dan niet met gebruik van AI, verschillende zorgplansystemen, een applicatie voor veilig mailen, infrastructuur ten behoeve van het uitwisselen van medische gegevens met andere zorgaanbieders, koppelingen met webdiensten van bijvoorbeeld Vecozo en ga zo maar door. De ICT-diensten kunnen op locatie staan/draaien, maar vaker zal gebruik gemaakt worden van de cloud, of anders gezegd: een extern (gevirtualiseerd) datacenter.

Al deze systemen helpen zorgaanbieders anno 2021 om goede zorg te kunnen leveren. Maar je bent er als zorgaanbieder ook afhankelijk van. En niet alleen van de systemen, in het verlengde daarvan, ook van de leveranciers van die systemen. Spannend? De zorgaanbieder blijft immers zelf verantwoordelijk voor het leveren van goede zorg. De zorgaanbieder moet ervoor zorgen dat hij in ieder geval de regie houdt.

Een van de belangrijkste onderwerpen daarbij is informatieveiligheid. Verplichte kost in de zorg in dat kader, is de implementatie van NEN 7510 (en NEN 7512 en NEN 7513). Al sinds 2013 vindt ook de Autoriteit Persoonsgegevens (toen nog CBP) dat NEN 7510 geïmplementeerd moet worden als er medische persoonsgegevens worden verwerkt. Ook voor het gebruik van zorginformatiesystemen en elektronische uitwisselingssystemen geldt dat er moet worden voldaan aan de genoemde normen bij het gebruik van die systemen. En zodra het genoemde wetsvoorstel wet wordt, is te verwachten dat het voldoen aan de norm in steeds meer gevallen verplicht wordt.

Als je het hebt over regie, dan springt een onderwerp uit de NEN 7510 in het oog: het leveranciersmanagement. Omdat er in de praktijk steeds meer uitbesteding (al dan niet in de cloud) plaatsvindt, en dit wat ons betreft dus een van de kernonderwerpen van de NEN 7510 is, geven wij u graag meer inzicht in wat NEN 7510 precies vereist als het aankomt op leveranciersmanagement.

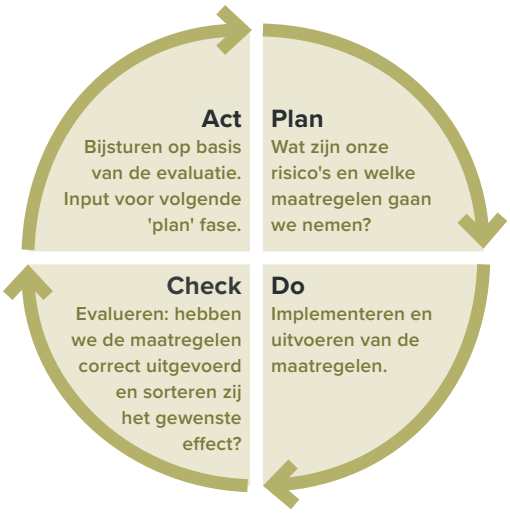
Norm voor informatiebeveiliging in de zorg
NEN 7510 bestaat uit twee delen. Het eerste deel

(NEN 7510-1+A1) gaat niet in op maatregelen om informatie te beschermen, maar beschrijft hoe het managementsysteem voor informatiebeveiliging zou moeten worden ingericht.

Managementsysteem

Het managementsysteem voor informatiebeveiliging wordt ook wel aangeduid als het 'ISMS', wat een acroniem is van *Information Security Management System*.

Met 'systeem' wordt niet gedoeld op een software tool, maar op een gestructureerd geheel aan beleid, processen, procedures en afspraken die zijn ingericht om de doelstellingen met betrekking tot informatiebeveiliging te behalen. De rode draad binnen dit systeem is de 'plan-do-check-act-cyclus'; een procesmatige manier van werken waarmee je de kwaliteit niet alleen op peil houdt, maar ook doorlopend kunt verbeteren. Dat doe je door de processen rond informatiebeveiliging zodanig in te richten dat acties op basis van een bepaald plan worden uitgevoerd. Vervolgens wordt periodiek geëvalueerd of het plan naar behoren wordt uitgevoerd en of daarmee de gestelde doelen worden behaald. Waar nodig wordt bijgestuurd. Vervolgens worden de geleerde lessen meegenomen in de nieuwe 'plan' fase, enzovoort.



Beheersmaatregelen

Deel 2 van NEN 7510 (NEN 7510-2) beschrijft beheersmaatregelen om de risico's rond informatiebeveiliging te beheersen en geeft *best practices* met betrekking tot de implementatie van de maatregelen. De beheersmaatregelen betreffen zowel technische als organisatorische maatregelen en lopen uiteen van maatregelen voor het opstellen van beleid en de aansturing daaromheen, tot aan maatregelen rond het screenen en opleiden van personeel, het beheren van autorisaties, het toepassen en beheren van versleuteling, en het uitvoeren van interne en externe audits. Een onderwerp dat steeds belangrijker wordt is beschreven in hoofdstuk 15: leveranciersrelaties.

Leveranciersrelaties & NEN 7510

NEN 7510 heeft een hoofdstuk geweid aan leveranciersmanagement in de context van informatiebeveiliging in de zorg. De norm beschrijft twee beheersdoelstellingen en koppelt daar in totaal vijf beheersmaatregelen aan.

Doelstellingen

NEN 7510 beschrijft de volgende beheersdoelstellingen in het kader van leveranciersrelaties:

1. **Informatiebeveiliging in leveranciersrelaties**
   De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.[1]
2. **Beheer van dienstverlening van leveranciers**
   Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.[2]

Informatiebeveiliging in leveranciersrelaties

Bij de eerste doelstelling komt het erop neer dat er risico's voor de bescherming van informatie ontstaan, wanneer leveranciers toegang of beschikking krijgen over bedrijfsmiddelen. Bijvoorbeeld een inhuurkracht die een laptop van de zorginstelling ontvangt om haar of zijn werk te doen. Maar ook het netwerk en computersystemen zijn bedrijfsmiddelen waar zo'n inhuurkracht toegang toe kan krijgen. En ook daar kan bewust of onbewust iets gebeuren dat een risico vormt voor de beschikbaarheid, integriteit of vertrouwelijkheid van (zorg)informatie. NEN 7510-2 beschrijft drie maatregelen om deze risico's te beheersen.

Beleid voor leveranciersrelaties

Stap 1 om deze doelstelling te behalen is om beleid te hanteren met betrekking tot leveranciers. De norm schrijft voor dat de organisatie eisen opstelt en met de leverancier afspreekt, waarmee de risico's die samenhangen met de toegang die de leverancier heeft tot bedrijfsmiddelen, worden verkleind.

Met andere woorden: zorg er niet alleen voor dat er duidelijke regels zijn voor de eigen medewerkers, maar leg die regels ook op aan leveranciers. Hiertoe zal dus éérst in kaart moeten worden gebracht welke risico's er zijn, hoe groot de kans is dat de risico's zich voordoen en wat in dat geval de impact is. Vervolgens kunnen maatregelen worden overeengekomen met de betreffende leverancier om op een voor de organisatie passende wijze met die risico's om te gaan.

Beveiligingsaspecten in contracten

Als tweede stap om bedrijfsmiddelen die toegankelijk zijn voor leveranciers te beschermen, schrijft NEN 7510-

1. NEN 7510-2:2017, §15.1.
2. NEN 7510-2:2017, §15.2.

2 voor dat 'alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt'. Oftewel: denk bij elke leverancier die toegang heeft tot informatie of IT na welke beveiligingseisen nuttig zijn en zorg dat de afspraken netjes worden gedocumenteerd in een contract, zodat daar later geen misverstand over kan ontstaan.

Hierbij kan onder andere worden gedacht aan een beschrijving van de informatie of -systemen die toegankelijk zijn, de classificatie die daarop van toepassing is, afspraken met betrekking tot rapportage over naleving van het contract, regels voor aanvaardbaar gebruik, maar bijvoorbeeld ook de omgang met incidenten of procedures voor het oplossen van conflicten.

ICT-toeleveringsketen
Net zoals leveranciers een risico vormen voor de bedrijfsmiddelen van de organisatie, geldt dat ook voor onderaannemers van de leverancier. Het is daarom belangrijk om óók grip te houden op partijen in de keten die minder zichtbaar zijn. Als derde stap om bedrijfsmiddelen die toegankelijk zijn voor leveranciers te beschermen, schrijft NEN 7510-2 daarom voor dat contracten met leveranciers óók eisen moeten bevatten om de risico's in verband met de toeleveringsketen van diensten en producten op het gebied van ICT te beheersen.
Hierbij kan onder andere worden gedacht aan een verplichting om eisen die de leverancier op zich neemt door te leggen aan andere partijen in de keten. Gedacht kan ook worden aan een proces om te monitoren en controleren dat het geleverde aan de gestelde eisen voldoet, of aan regels om informatie over toekomstige kwesties in de keten door te geven.

Beheer van dienstverlening van leveranciers
De tweede doelstelling die NEN 7510 beschrijft met betrekking tot leveranciersrelaties is erop gericht om een vooraf bepaald niveau van beveiliging en dienstverlening te handhaven, in lijn met de gemaakte afspraken. Deze doelstelling draait dus niet in directe zin om het beschermen van bedrijfsmiddelen van de organisatie, maar meer om het in de gaten houden of de leverancier doet wat hij beloofd heeft.

Monitoren en beoordelen dienstverlening
De eerste stap om de doelstelling te behalen, is door regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen. Hierdoor kan ervoor worden gezorgd dat de gemaakte afspraken worden nagekomen en dat eventuele problemen met betrekking tot informatiebeveiliging tijdig en op de juiste manier worden behandeld. Hiertoe dient een proces te worden ingericht om leveranciersrelaties te beheren, en om (onder andere) te verifiëren of wordt geleverd wat is afgesproken conform de contracten, te rapporteren over de dienstverlening, audits uit te voeren en gesignaleerde problemen op te lossen.

Beheer van veranderingen in dienstverlening
De PDCA-cyclus die in het managementsysteem centraal staat, werkt ook door in het leveranciersmanagement. De wereld verandert, en zo ook de diensten die de organisatie afneemt van haar leverancier. Die veranderingen kunnen voortkomen uit (bijvoorbeeld) het doorontwikkelen en verbeteren van de dienst, het opvolgen van afspraken of bevindingen uit leverancierscontroles, of veranderingen in de dienst die voortvloeien uit nieuwe of aangepaste wetgevingsvereisten. Maar het kan natuurlijk ook zijn dat de dienst die initieel geleverd werd dusdanig goed beviel dat na verloop van tijd méér diensten worden afgenomen (of juist andersom: er worden minder diensten afgenomen).

Het is belangrijk om zulke veranderingen in de gaten te houden en om erop in te spelen. Zulke veranderingen kunnen immers risico's met zich brengen. Door regelmatig te beoordelen welke veranderingen er zijn geweest, welke risico's daaraan kleven en hoe groot die risico's precies zijn, kan tijdig worden bijgestuurd om die risico's tot een acceptabel niveau te beperken.

Tot slot
Het hoofdstuk over leveranciersmanagement in NEN 7510 biedt een hoop inspiratie en aanknopingspunten waarmee organisaties ervoor kunnen zorgen dat hun informatie beschermd blijft, óók wanneer er externe leveranciers in het spel zijn. Tegelijkertijd kunnen ook onderwerpen uit de andere hoofdstukken uit NEN 7510 relevant zijn met betrekking tot leveranciers. Een goed voorbeeld is het hoofdstuk over bedrijfscontinuïteit: gezien de toenemende afhankelijkheid van leveranciers zal een goed bedrijfscontinuïteitsbeheer óók leveranciers in scope hebben.

De normen uit NEN 7510 kunnen in de praktijk overweldigend overkomen – zeker wanneer de lijst met alle leveranciers wordt bekeken en men daarbij bedenkt dat al die partijen periodiek beoordeeld en gecontroleerd moeten worden. Houd in dat geval altijd in het achterhoofd dat NEN 7510 tegenwoordig *risk based* is. Focus dus op informatie en -systemen die écht kritisch zijn, en besteed minder energie aan kleine tools die weinig of geen risico met zich dragen. Maar: zorg er wel voor dat je achteraf kunt onderbouwen en aantonen waarom je deze keuzes gemaakt hebt en op basis van welke inzichten en risico-afwegingen de beslissingen zijn genomen.

Anouk van Rijn
Juridisch adviseur

Beryl Hetharia
Juridisch adviseur

E-commerce

Wat betekent Strong Customer Authentication voor uw webshop?

Veiligheid is een essentieel onderdeel van online betalingen. Online fraude komt echter steeds vaker voor. Vanuit Europa wordt dan ook op allerlei manieren gekeken hoe dit probleem kan worden teruggedrongen. Een van deze manieren is Strong Customer Authentication (SCA), zoals vermeld in de tweede Payment Services Directive (PSD2). Vanaf 1 januari 2021 moeten organisaties zich houden aan de SCA. Wat is het en wat betekent het voor uw organisatie?

PSD2
De PSD2 is een Europese richtlijn voor het betalingsverkeer van consumenten en bedrijven. Deze richtlijn is in elke EU-lidstaat opgenomen in de nationale wetgeving. In Nederland is de PSD2 geïmplementeerd in het Burgerlijk Wetboek en de Wet op het financieel toezicht. Ook wordt de PSD2 verder uitgewerkt in richtlijnen voor banken en andere bedrijven die betaaldiensten aanbieden en hun toezichthouders.

Strong Customer Authentication
In de PSD2 wordt gesproken over 'sterke cliëntauthenticatie' (de SCA). Bij SCA draait het erom dat er zekerheid bestaat dat de klant die een online aankoop doet en hier ook voor betaalt, daadwerkelijk deze persoon is. Wordt een creditcard gebruikt of een betaling via iDEAL verricht, dan is het van belang dat de kaartgegevens ook worden gebruikt door de kaarthouder. Hoe meer u over iemand te weten komt, hoe zekerder u hierover kunt zijn.

Er zijn in totaal drie manieren om iets over uw klant te weten te komen. De PSD2 vereist dat u bij elektronisch betalen en bankieren kiest voor tenminste twee van deze controles. Daarbij kan het gaan om:
1. iets wat je bezit, zoals je telefoon, kenteken of bankpas;
2. iets wat je weet, bijvoorbeeld een pincode, wachtwoord of een geheim feit; of
3. iets wat je bent, denk aan je vingerafdruk, gezichtsherkenning via Face ID of je stem.

In Nederland kennen we SCA eigenlijk al veel langer, bij veel betalingen gebeurt dit namelijk al. Denk bijvoorbeeld aan betalingen met de pinpas. Daarbij gebruik je immers zowel je pincode als je bankpas. Ook bij iDEAL betalingen gebruik je jouw geregistreerde telefoon en je toegangscode. In het kader van PSD2 moet deze dubbele authenticatie nu dus ook gebeuren bij betalingen met creditcards.

Uitzonderingen
De juridische wereld staat bekend om haar regels, maar natuurlijk ook de uitzonderingen. Zo kent de PSD2 ook een aantal uitzonderingen voor het gebruik van SCA. Hieronder worden de uitzonderingen kort uitgewerkt.

Betalingen geïnitieerd vanuit de verkoper
Wanneer een betaling wordt geïnitieerd door de webshop, bijvoorbeeld via een automatische incasso, dient alleen voor de eerste betaling aan SCA-verificatie te worden voldaan.

Abonnementen of terugkerende transacties
Wanneer het gaat om terugkerende transacties met een vast bedrag, zijn deze vanaf de tweede transactie

vrijgesteld van SCA. Vrij logisch ook, aangezien abonnementskosten of terugkerende transacties vaak automatisch worden afgeschreven. Indien het te betalen bedrag verandert, zal SCA weer nodig zijn.

Transacties met een lage waarde
Transacties onder de 30 euro zijn vrijgesteld van SCA. Deze vrijstelling is beperkt en SCA wordt door de bank altijd vereist als een klant vijf van deze transacties achter elkaar uitvoert of de som van de transacties van de klant bij elkaar een waarde van meer dan 100 euro bereikt.

Postorder- en telefoonorder-transacties
Deze transacties zijn vrijgesteld van SCA, omdat ze niet worden beschouwd als 'elektronische' betalingen en daarmee buiten het toepassingsgebied van de richtlijn vallen.

Transactie met een laag risico
Daarnaast zijn transacties met een laag risico vrijgesteld van SCA. De vraag is natuurlijk hoe je een betaling kunt bestempelen als zijnde een 'laag risico'. Dit bepaalt de bank die de betaling verwerkt en dient te worden gebaseerd op het gemiddelde fraudeniveau van de kaartuitgever die de transactie verwerkt en de acquirer (de verwerker van de transactie). Daarbij wordt gekeken naar het aantal fraudegemiddelden van deze partijen. Als de bank tot de conclusie komt dat dit een laag risico oplevert, kan de transactie vrijgesteld worden van SCA.

Interregionale transacties
De regels uit de PSD2 gelden niet wereldwijd. Betalingen waarbij de uitgever of de acquirer niet in Europa gevestigd is, worden ook vrijgesteld. Als de klant echter buiten Europa is gevestigd, maar de uitgever van de kaart en de acquirer wél allebei in Europa zijn gevestigd, zal dit niet als een interregionale transactie worden bestempeld en kan SCA erop van toepassing zijn.

De witte lijst-handelaren
Doet een klant bijvoorbeeld regelmatig aankopen bij uw webshop, dan heeft deze klant de mogelijkheid om uw webshop toe te voegen aan de witte lijst. Daarvoor kunnen de klanten zelf kiezen na het afronden van een betaling. Ook in dat geval is er geen SCA meer nodig voor deze vaste klant.

B2B-transacties
Voor specifieke betalingsproducten op het gebied van zakelijke betalingen zijn ook uitzonderingen om zo complicaties bij B2B-betalingen te voorkomen. De gebruikte betaalmethode moet in dat geval een betaalinstrument zijn dat is bedoeld om B2B-betalingen uit te voeren.

Veiligheid versus privacy
Wanneer SCA wordt gebruikt, dan worden er persoonsgegevens van klanten verzameld. In sommige gevallen zelfs bijzondere persoonsgegevens. Een voorbeeld hiervan is een Face ID. Daarbij speelt het recht op privacy, zoals vastgelegd in de Algemene verordening gegevensbescherming (AVG) een rol. De beveiliging van deze persoonsgegevens dient gewaarborgd te zijn. Daarnaast zal de klant voor het gebruik van deze bijzondere persoonsgegevens expliciet gevraagd moeten worden om zijn toestemming.

Wat dient u voor uw website te regelen?
Vanaf 1 januari 2021 dienen online betalingen te allen tijde met tweestapsverificatie voltooid te worden. De genoemde uitzonderingen daar gelaten. Voldoet een betalingstransactie niet aan de voorwaarden van de SCA, dan kan de bank de transactie weigeren.

Runt u een webshop? Kies dan voor een betaaltechniek die voldoet aan de SCA-vereisten. In Europa wordt 3D Secure als tweestapsverificatie het meest toegepast. Dit komt doordat de twee grootste kaartaanbieders van Europa, Visa en MasterCard, 3D Secure gebruiken. Het is verstandig om daarnaast ook bekende betaalmethoden zoals Google Pay of Apple Pay te ondersteunen. Daarmee zullen uw klanten al snel aan SCA voldoen zonder dat ze dat zelf doorhebben. Om deze diensten te kunnen gebruiken moeten zij zich namelijk al identificeren.

Uiteindelijk is het belangrijk dat webshops voldoende onderzoek doen naar de geschikte SCA-methode en deze voor 1 januari 2021 implementeren. Deze dubbele controle is niet alleen bedoeld om fraude tegen te gaan, maar zorgt er ook voor dat de algemene veiligheid van online betalingen wordt versterkt!

ICTRECHT
academy

Opleiding FG/DPO

De schakel tussen theorie en praktijk binnen de opleiding is essentieel en maakt dat de opleiding zowel relevant is voor beginnende als ervaren FG's.

Specialiseer u tot FG/DPO
Start 25 maart 2021

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

Deelnemer opleiding FG/DPO september 2019

Schrijf u nu in via
ictrecht.nl/fg-opleiding

Bram de Vos
Juridisch adviseur

Wet- en regelgeving

EDPB Richtsnoeren inzake verwerkings-verantwoordelijke en verwerker
In de periode van 7 september tot en met 19 oktober 2020 heeft de EDPB een consultatie gehouden over nieuwe richtsnoeren met betrekking tot de begrippen 'verwerkingsverantwoordelijke' en 'verwerker'. Hierover waren in het verleden al richtsnoeren vastgesteld door de Artikel 29 Werkgroep, maar deze dateren uit 2010 en zijn dus nog van vóór de invoering van de Algemene verordening gegevensbescherming. In de tussentijd zijn er allerhande nieuwe vragen ontstaan, bijvoorbeeld rondom de gezamenlijke verantwoordelijkheid (artikel 26 AVG) en de specifieke verplichtingen die gelden voor de verwerker (artikel 28 AVG). In de nieuwe richtsnoeren probeert de EDPB meer duidelijkheid te bieden.

https://bit.ly/3nTML3s

Wetsvoorstel toetsing economie en nationale veiligheid
Van 8 september tot en met 7 oktober 2020 is er een internetconsultatie over de Wet toetsing economie en nationale veiligheid gehouden. Het voorstel heeft tot doel om te voorkomen dat de nationale veiligheid wordt bedreigd door internationale investeringen, fusies of andere economische activiteiten. De wet richt zich primair op aanbieders van vitale infrastructuur in Nederland en op ondernemingen die zich toeleggen op sensitieve technologie. Deze bedrijven worden verplicht om een melding te doen aan de minister van Economische Zaken en Klimaat bij activiteiten die gevolgen hebben voor de zeggenschap over – of invloed op – de onderneming. Naar aanleiding van deze melding wordt vervolgens een risicoanalyse gemaakt. Indien blijkt dat de activiteiten een risico opleveren voor de nationale veiligheid, kan de minister een verbod opleggen, dan wel aanvullende eisen of voorschriften stellen.

https://bit.ly/3lPi1zD

Tijdelijke wet notificatieapplicatie COVID-19
Op 6 oktober 2020 heeft de Eerste Kamer ingestemd met het voorstel voor de Tijdelijke wet notificatie-applicatie COVID-19. Daarmee wordt een wettelijke grondslag gecreëerd voor het verwerken van persoonsgegevens via de CoronaMelder-app. Hoewel de applicatie in het oorspronkelijke ontwerp al uitdrukkelijke toestemming vroeg aan gebruikers voor het verwerken van gegevens, concludeerde de Autoriteit Persoonsgegevens eerder dat een wettelijke grondslag logischer zou zijn. Dit mede vanwege de ingrijpende impact van de applicatie. Op deze conclusie van de toezichthouder kwam de nodige kritiek. Desondanks heeft men besloten om de verwerking van persoonsgegevens via de applicatie wettelijk te verankeren.

https://bit.ly/2ISWMhW

Implementatiewet richtlijn modernisering consumentenbescherming
Van 23 oktober tot en met 22 november 2020 is er een internetconsultatie gehouden met betrekking tot de Implementatiewet richtlijn modernisering consumentenbescherming. Het wetsvoorstel bevat onder andere nieuwe transparantieverplichtingen voor online-marktplaatsen en aanbieders van online zoekfuncties. Zo worden marktplaatsen verplicht om consumenten vóór het sluiten van de overeenkomst te informeren over de hoedanigheid (handelaar of particulier) van de persoon die een product of dienst aanbiedt. Ook moeten aanbieders van online zoekfuncties informatie beschikbaar stellen over hoe de rangschikking van advertenties of zoekresultaten wordt bepaald. Verder komen er onder meer regels om valse reviews van online platforms te weren. De wet verplicht ondernemers om maatregelen te nemen om nepreviews te voorkomen. De genomen maatregelen moeten ook inzichtelijk zijn voor de consument.

https://bit.ly/3mdEfeQ

Mediawet
Op 1 november 2020 is een gewijzigde versie van de Mediawet in werking getreden. Daarmee wordt de herziene Richtlijn audiovisuele mediadiensten (2010/13/EU) in het Nederlandse wetgevingskader geïmplementeerd. Via deze herziening worden de verschillen in wetgeving voor lineaire mediadiensten (zendertelevisie) en mediadiensten op aanvraag (zoals Netflix) grotendeels gelijkgetrokken. Daarnaast worden online videoplatforms (zoals YouTube) onder het toepassingsbereik gebracht. Deze platforms moeten daardoor maatregelen gaan treffen om te zorgen dat het voor gebruikers duidelijk is als er in een video sprake is van reclame, sponsoring of productplaatsing.

https://bit.ly/3pQlv7M

EDPB Richtsnoeren doorgifte persoonsgegevens
Op 11 november 2020 heeft de EDPB een consultatie gestart voor nieuwe richtsnoeren over de doorgifte van persoonsgegevens naar derde landen. De richtsnoeren zijn opgesteld naar aanleiding van het recente Schrems II arrest (ECLI:EU:C:2020:559). In dat arrest werd het Privacy Shield (dat als juridische basis dient voor veel gegevensuitwisselingen tussen Europa en de Verenigde Staten) ongeldig verklaard. Ook benadrukte het Europese Hof van Justitie dat men bij doorgifte van persoonsgegevens niet zonder meer mag vertrouwen op bijvoorbeeld de *Standard Contractual Clauses* (SCC). Volgens het Hof moet voor iedere doorgifte een risicoanalyse worden gemaakt. Afhankelijk van de uitkomst kunnen er aanvullende maatregelen nodig zijn om persoonsgegevens op een verantwoorde manier te verwerken buiten de Europese Economische Ruimte. In de nieuwe richtsnoeren geeft de EDPB handvatten om partijen hierbij te helpen. De richtsnoeren bieden een stappenplan, een overzicht van relevante informatiebronnen en voorbeelden van aanvullende maatregelen die genomen kunnen worden.

https://bit.ly/3pQkTip

Regeling veiligheid en integriteit telecommunicatie
Op 11 november 2020 is de internetconsultatie van de Regeling veiligheid en integriteit telecommunicatie gestart. In de regeling zijn aanvullende beveiligingsmaatregelen opgenomen voor aanbieders van mobiele telecomnetwerken in Nederland. De maatregelen moeten de weerbaarheid van de netwerken vergroten in het licht van actuele dreigingen, zoals spionage door statelijke actoren uit het buitenland. Belanghebbenden kunnen tot 16 december op de conceptversie reageren.

https://bit.ly/3lOcsBC

Codebesluit over voorstel wijziging eisen gegevensuitwisseling
Op 12 november 2020 heeft de Autoriteit Consument & Markt een besluit genomen over de gegevensuitwisseling tussen netbeheerders (onderling en met andere partijen). Met het besluit worden ook de kwaliteitseisen en de bewaartermijnen van opgeslagen gegevens gewijzigd. Het besluit resulteert in wijzigingen in de Netcode elektriciteit, de Meetcode elektriciteit en de Begrippencode elektriciteit.

https://bit.ly/2UI8iPZ

Digital Services Act en Digital Markets Act
Op 2 december 2020 worden de conceptversies van de Europese Digital Services Act en de Digital Markets Act verwacht. Deze nieuwe wetgeving moet een duidelijk en modern juridisch kader bieden voor online dienstverlening. De huidige regels hieromtrent zijn vastgelegd in onder andere de Richtlijn elektronische handel (2000/31/EG). Deze dateert echter nog uit 2000 en sinds die tijd is er veel veranderd in het digitale landschap. Hoewel de invulling van de Digital Services Act en de Digital Markets Act op dit moment nog niet volledig duidelijk is, zullen zij naar verwachting tot belangrijke veranderingen leiden. De Europese Commissie wil in ieder geval een eerlijker speelveld creëren voor aanbieders van online diensten. Zo rapporteerde verschillende media eerder (op basis van uitgelekte documenten) dat er mogelijk een verbod gaat gelden voor grote technologiebedrijven (zoals Google en Apple) om eigen software en diensten vooraf te installeren op hun apparaten. Ook krijgen online platforms naar verwachting aanvullende verantwoordelijkheden als het gaat om het bestrijden van illegale inhoud.

https://bit.ly/2UVjTLB

Wet kansspelen op afstand
De Wet kansspelen op afstand zal naar verwachting op 1 maart 2021 in werking treden, zo blijkt uit een nieuwsbericht op de website van de Rijksoverheid. Dat is twee maanden later dan gepland. Minister Dekker wil met deze nieuwe planning meer ruimte geven aan alle betrokken partijen om zich voor te bereiden op de nieuwe wetgeving. De opening van de online kansspelmarkt staat nu gepland op 1 september 2021.

https://bit.ly/3lQCkwC

Esther Flierman
Juridisch adviseur

Overheid Cloud

De voor- en nadelen van de SGOA-procedure

Recent zijn de nieuwe ICT-branchevoorwaarden gepubliceerd. De opvolger van de Nederland ICT Voorwaarden, de NLdigital Voorwaarden. In deze voorwaarden is bepaald dat alle geschillen met een financieel belang van € 25.000 of meer alleen aanhangig gemaakt kunnen worden bij Stichting Geschillenoplossing Automatisering (SGOA).

Tijd voor een inkijkje, wat zijn de voor- en nadelen in vergelijking tot een procedure bij de burgerlijk rechter? Is het verstandig om op voorhand akkoord te gaan met een arbitragebeding?

De geschillenregeling is vastgelegd in artikel 22 van de NLdigital Voorwaarden. Alle geschillen worden beslecht middels Arbitrage door SGOA op basis van het arbitragereglement.

De kosten
De kosten bestaan uit administratiekosten en het honorarium. De hoogte van de kosten is afhankelijk van het financiële belang van de zaak (zie de tabel hiernaast). Hierbij zij opgemerkt dat vooraf een urenbegroting wordt gemaakt. Complexe zaken worden begroot op tenminste 60 uur. Onder complexe zaken wordt verstaan, zaken met een belang van tenminste € 50.000.

Ook de kosten van een gerechtelijke procedure zijn afhankelijk van het financiële belang waarover de kwestie gaat. Er wordt enkel griffierecht inrekening gebracht en dus geen kosten voor het aantal te besteden uren. Het verschuldigde griffierecht kent drie staffels bij de sector civiel:

- Onbepaalde belang kost € 656;
- Een zaak met een financieel belang tot € 100.000 kost € 2.042;
- Een zaak met een financieel belang van meer dan € 100.000 kost € 4.131.

Voor beide procedures geldt dat de kosten vooraf betaald moeten worden door de eisende partij. De kosten van een civiele procedure zijn overzichtelijk en te overzien. De kosten van SGOA zijn vele malen groter.

Belang		Administratiekosten
Van	tot en met	
€ 0	€ 10.000	€ 800
€ 10.001	€ 50.000	€ 1.000
€ 50.001	€ 1.000.000	€ 1.400
€ 1.000.001	€ 2.500.000	€ 7.100
€ 2.500.001	€ 5.000.000	€ 13.100
€ 5.000.001	€ 7.500.000	€ 14.350
€ >7.500.000		€ 15.100

Uurtarief	Belang
€ 210	van € 50.000 of minder
€ 220	tussen de € 50.000 en de € 200.000
€ 250	tussen de € 200.001 en de € 500.000
€ 275	tussen de € 500.001 en de € 5.000.000
€ 300	tussen de € 5.000.001 en de € 30.000.000
€ 325	tussen de € 30.000.001 en de € 50.000.000
€ 350	van meer dan € 50.000.000

De kosten van de procedure komen voor rekening van de verliezende partij. Een groot verschil tussen civiel en SGOA betreft het feit dat in een SGOA-procedure ook de kosten van ingeschakelde rechtshulp voor rekening van de verliezende partij komen, terwijl in civiele procedures slechts een klein deel hiervan zal worden toegewezen op basis van vastgestelde staffels

"salaris gemachtigden" (uitzonderingen daargelaten, zoals bij IE-zaken).

Hierbij wordt nog opgemerkt dat in een civiele procedure procesvertegenwoordiging door een advocaat verplicht is, terwijl partijen bij SGOA ook in persoon kunnen procederen dan wel zich kunnen laten bijstaan door een juridisch adviseur of advocaat.

De kosten van de SGOA-procedure zijn erg hoog. Dit is een groot nadeel van de SGOA-procedure.

De duur van procedure
Zowel de SGOA-procedure als de civiele procedure vangen aan met schriftelijke stukken van de eisende partij. Hierop kan verweerder vervolgens schriftelijk reageren en eventueel een tegenvordering indienen. Vervolgens wordt een zitting bepaald en volgt er een uitspraak. Indien onvoldoende informatie is uitgewisseld om een einduitspraak te kunnen doen, kan worden besloten tot nadere opdrachten, bewijsopdracht, getuigenverhoor, deskundige bericht, nog een schriftelijke ronde etc.

De SGOA-procedure is beschreven in het Arbitrage reglement van SGOA. De civiele procedure is vastgelegd in wet- en regelgeving, het wetboek van rechtsvordering en het rolreglement.

De termijnen tussen de verschillende processuele stappen zijn bij SGOA kort, meestal vier weken. In civiele procedures is dit ook het geval alleen kan ieder der partijen uitstel vragen, wat meestal ook wordt verleend. Daarnaast kent de civiele procedure meer mogelijke proceshandelingen dan de SGOA-procedure, wat een langere doorlooptijd met zich brengt.

De gemiddelde doorlooptijd van een SGOA-procedure is dan ook veel korter dan een civiele procedure. De gemiddelde doorlooptijd betreft drieënhalve maand, terwijl de gemiddelde doorlooptijd van een civiele procedure 12 maanden bedraagt. Bovendien kan een SGOA-vonnis niet aangetast worden door een vervolgprocedure. Hoger beroep is niet mogelijk. Dus de zaak komt tot een einde na uitspraak SGOA. Tegen uitspraken in civiele procedures staat altijd hoger beroep open en kan dus een vervolgprocedure volgen van een jaar of meer.

De SGOA-procedure is relatief kort. Dit is een groot voordeel.

De expertise
De arbiters van SGOA zijn allemaal experts binnen de ICT-branche ofwel juridisch experts ofwel technisch experts. De lijst van arbiters is openbaar en beide partijen kunnen een arbiter voordragen voor benoeming van de arbitragecommissie. Dit geeft dus enige invloed op de commissie die de zaak zal gaan beoordelen.

Rechters in civiele procedures hebben deze achtergrond (meestal) niet. Een rechter zal ook geen oordeel kunnen geven of een ICT-product, zoals een app, deugdelijk is opgeleverd. Rechters zullen ter beantwoording van dergelijke vragen experts uit de branche benoemen. Dit is overigens in alle soorten zaken, zoals bouwzaken, autozaken en dierenzaken. Ook zijn rechters in het civiele proces lijdelijk. Dit betekent dat het aan partijen is om de zaak goed voor het voetlicht te brengen. Als feiten niet worden betwist worden deze dan ook (meestal) als juist aangenomen. De vragen van de rechter op zittingen zien veelal op de feiten, beide partijen kunnen mondeling de zaak toelichten.

Partijen hebben op dergelijke zitting nogal eens het gevoel dat de rechter de zaak niet begrijpt en daar dus ook geen beslissing over zou kunnen nemen. Zo heb ik in mijn praktijk veelvuldig gehoord dat de ICT-dienstverlener zelfs moest uitleggen wat een IP-adres was. De rechter stelt vragen en vraagt door doch het is aan partijen om een en ander goed uit te leggen. Bij een dispuut over ondeugdelijkheid van een product of dienst zal dan ook bijna altijd na de zitting (comparitie van partijen) nog een deskundige worden benoemd om dit te onderzoeken en vast te stellen. De rechter volgt dit oordeel en beoordeelt vervolgens wat dit juridisch betekent.

Zowel binnen de gerechtelijke procedure als binnen de SGOA-procedure is expertise op het terrein van ICT-gerelateerd zaken aanwezig of wordt in de procedure gebracht middels benoeming van deskundigen. Wat expertise betreft heeft de ene procedure niet per se een voordeel ten opzichte van de andere procedure. De betrokken partijen ervaren de expertise van de arbiters zelf overigens wel als zeer positief, vooral de ICT-dienstverlener.

Slotsom
Hoe men de voor- en nadelen tegen elkaar afweegt, is een kwestie van smaak. Over het algemeen zijn hoge kosten toch iets wat partijen c.q. ondernemers wensen te vermijden. Het probleem met contractsluiting op basis van de NLdigital Voorwaarden is evenwel dat partijen verplicht zijn de zaak te laten beslechten door SGOA. Er is geen keuzenvrijheid. In veel zaken is deskundigheid op ICT-gebied niet vereist. Persoonlijk vind ik het onverstandig bij voorbaat de gang naar de burgerlijk rechter uit te sluiten en raad ik aan bij contractsluiting op basis van de NLdigital Voorwaarden de geschillenregeling van artikel 22 buiten toepassing te verklaren.

Jorden Bailey
Juridisch adviseur

Jay Remmelzwaal
Juridisch adviseur

Privacy

Autoriteit Persoons-gegevens teruggefloten in de zaak "VoetbalTV"

Op 23 november 2020 heeft de rechtbank Midden-Nederland een uitspraak[1] gedaan in de zaak "VoetbalTV". De rechtbank oordeelde dat VoetbalTV een door de Autoriteit Persoonsgegevens opgelegde boete van € 575.000 niet hoeft te betalen. De Autoriteit Persoonsgegevens heeft, zo oordeelde de rechtbank, een verkeerd besluit genomen ten aanzien van de grondslag 'gerechtvaardigd belang'. Inmiddels is de speeltijd van VoetbalTV verstreken, want het platform is in september 2020 failliet verklaard. Dat neemt echter niet weg dat de uitspraak van wezenlijk belang is voor de praktijk. In dit artikel nemen wij de uitspraak onder de loep.

VoetbalTV en de grondslag gerechtvaardigd belang
VoetbalTV was een online platform waarop amateur-wedstrijden werden uitgezonden. Ruim 500.000 gebruikers konden deze beelden terugkijken, analyseren en delen met anderen. Leuk als je op zondagmiddag een hattrick hebt gescoord, en je je kunsten middels beeld kunt etaleren. Maar waar beelden worden gemaakt komt privacy om de hoek kijken. Meer specifiek de AVG. Er stonden immers mensen herkenbaar op beeld. Wat betekent dat er persoonsgegevens werden verwerkt.

Om persoonsgegevens te verwerken heb je volgens artikel 6 van de AVG een grondslag nodig, waarvan de AVG er in totaal 6 kent. Toestemming is de bekendste grondslag. Echter, gezien het juridisch en praktisch onmogelijk is om van iedereen toestemming te vragen, kom je al gauw uit bij de grondslag 'gerechtvaardigd belang'. Deze grondslag vraagt een belangenafweging van de verwerkingsverantwoordelijke (is mijn belang groter dan dat van zij wiens gegevens verwerkt gaan worden) en vereist daarmee een gezonde dosis aan inschattingsvermogen. Al eerder hebben wij een blog[2] geschreven over de grondslag gerechtvaardigd belang.

In deze blog noemde wij het gerechtvaardigd belang niet voor niets een oplossing voor privacy hordes, omdat het soelaas biedt voor gegevensverwerkingen waar andere grondslagen – juridisch en praktisch gezien – onhaalbaar zijn. VoetbalTV beriep zich daarom geheel begrijpelijk op deze grondslag. Dit was in strijd met de AVG, aldus de Autoriteit Persoonsgegevens. Daarom besloot de Autoriteit Persoonsgegevens een boete op te leggen.

De strikte uitleg van de Autoriteit Persoons-gegevens
De Autoriteit Persoonsgegevens hanteerde altijd een strikte uitleg van de grondslag gerechtvaardigd belang. Zo staat in de normuitleg grondslag 'gerechtvaardigd belang'[3] van de Autoriteit Persoonsgegevens – wat kan worden gezien als de visie van de Autoriteit Persoons-gegevens – dat belangen pas gerechtvaardigd zijn als deze in (algemene) wetgeving of elders in het recht zijn benoemd als rechtsbelang. Uit rechtsoverweging 14 van onderhavige uitspraak blijkt dat de Autoriteit Persoonsgegevens in dit kader het volgende tijdens de procedure naar voren heeft gebracht:

1. https://bit.ly/3o6FRYA
2. https://bit.ly/3mmniit
3. https://bit.ly/2KSeUcS

"Zuiver commerciële belangen en het belang van winstmaximalisatie zijn niet specifiek genoeg en missen een dringend 'wettelijk' karakter, zodat zij niet kunnen worden aangemerkt als gerechtvaardigde belangen. De kern van de activiteiten van eiseres bestaat uit de verwerking van persoonsgegevens en met die verwerking verdient zij geld. Zij heeft daarmee een zuiver economisch belang bij het verwerken van persoonsgegevens. Dit kan volgens verweerder nooit een gerechtvaardigd belang zijn."

De rechtbank kan zich echter niet vinden in deze strikte uitleg van de Autoriteit Persoonsgegevens en tikt de Autoriteit Persoonsgegevens dan ook op de vingers. De toetsing van de Autoriteit Persoonsgegevens gaat volgens de rechtbank uit van een verkeerde interpretatie van de grondslag 'gerechtvaardigd belang'.

Rechtbank fluit de Autoriteit Persoonsgegevens terug

De rechtbank overweegt aan de hand van rechtspraak van het Europese Hof van Justitie waarom de Autoriteit Persoonsgegevens een onjuist maatstaf hanteert. In rechtsoverweging 14 refereert de rechtbank aan de uitspraak Fashion ID[4], waarin drie voorwaarden naar voren komen voor een geslaagd beroep op de grondslag gerechtvaardigd belang. In het kort komt het erop neer dat moet zijn voldaan aan de volgende drie voorwaarden:

1. Heeft u een gerechtvaardigd belang (doel)?
2. Is de voorgenomen verwerking van persoonsgegevens *noodzakelijk* om het doel te bereiken?
3. Weegt het belang van uw organisatie (of een derde) zwaarder dan het privacybelang van de betrokkene?

De Autoriteit Persoonsgegevens heeft al bij de eerste stap een streep gezet door het standpunt van VoetbalTV. De Autoriteit Persoonsgegevens was immers van mening dat VoetbalTV een zuiver commercieel belang had bij de exploitatie van het platform. Zoals gezegd kan een zuiver commercieel volgens de Autoriteit Persoonsgegevens niet worden aangemerkt als gerechtvaardigd belang. En een belang kan pas gerechtvaardigd zijn als deze in (algemene) wetgeving of ergens anders in het recht is benoemd als rechtsbelang: een positieve toets.

4. https://bit.ly/2Vfyodi

De rechtbank overweegt echter in rechtsoverweging 16 dat de vraag of een organisatie een gerechtvaardigd belang heeft aan de hand van een negatieve toets moet worden beoordeeld. Dit brengt met zich mee dat ieder belang gerechtvaardigd kan zijn, zo lang deze maar niet in strijd is met het recht. Dit is een ruime interpretatie. De rechtbank vindt in overweging 47 van de AVG steun voor deze ruime interpretatie. Hierin staat namelijk expliciet genoemd dat "direct marketing" als voorbeeld kan dienen van een mogelijk gerechtvaardigd belang. Bij "direct marketing" kan ook geen rechtsbelang worden genoemd als basis.

Wat kunnen organisaties met de uitspraak?
Organisaties hebben op basis van onderhavige uitspraak meer ruimte gekregen om persoonsgegevens te verwerken op basis van de grondslag gerechtvaardigd belang. De Rechtbank geeft met haar negatieve toets namelijk een voorzet op maat aan organisaties die commerciële activiteiten willen ontplooien. Dit neemt niet weg dat je als organisatie nog steeds een goed verhaal moet hebben om de grondslag gerechtvaardigd belang rond te krijgen, waarmee de bal dus bij de organisaties zelf komt te liggen.

De Autoriteit Persoonsgegevens dient zicht bij haar beoordeling te laten leiden door de belangen die door de verwerkingsverantwoordelijke naar voren worden gebracht. Daarbij mag de Autoriteit Persoonsgegevens niet vooraf – bij stap 1 uit de driestappentoets – bepalen dat er geen gerechtvaardigd belang is, tenzij een belang in strijd is met het recht. De Autoriteit Persoonsgegevens zal dit moeten aantonen. Is het belang niet in strijd met het recht, dan moet de Autoriteit Persoonsgegeven een noodzakelijkheidstoets uitvoeren en een belangenafweging maken (stap 2 en stap 3 uit de driestappentoets). Commerciële activiteiten mogen dus niet al vooraf – bij stap 1 uit de driestappentoets – worden getackeld door de Autoriteit Persoonsgegevens. Of VoetbalTV gebruik kon maken van de grondslag gerechtvaardigd belang blijkt niet uit de uitspraak, omdat de Autoriteit Persoonsgegevens dit – stap 2 en stap 3 uit de driestappentoets – dus niet heeft getoetst.

Aan organisaties de taak om een gefundeerd verhaal te hebben bij de (voorgenomen) gegevensverwerking. In dit kader is het raadzaam om de driestappentoets op papier te zetten, zodat u kunt motiveren waarom gebruik kan worden gemaakt van de grondslag "gerechtvaardigd belang". Mocht er ooit discussie ontstaan over de grondslag, dan heeft u uw papieren motivering altijd achter de hand. Daarnaast kunnen maatregelen worden genomen om belangenafweging tussen de belangen van uw organisatie (of een derde) en het privacybelang van de betrokkene(n) in het voordeel te laten uitvallen van uw organisatie (of een derde). Denk aan maatregelen zoals (1) het op de juiste wijze informeren over de verwerking van persoonsgegevens; (2) de persoonsgegevens niet inzetten voor andere doeleinden; (3) de persoonsgegevens zo snel mogelijk en op een veilige manier verwijderen; (4) een onvoorwaardelijk recht van bezwaar aanbieden en duidelijk onder de aandacht brengen; en (5) het nemen van passende beveiligingsmaatregelen. Dergelijke maatregelen kunnen in de driestappentoets worden opgenomen. Vanzelfsprekend dienen de maatregelen ook in de praktijk ten uitvoer te worden gebracht.

Of de Autoriteit Persoonsgegevens in hoger beroep alsnog voor een *rematch* gaat tegen de uitspraak moeten we afwachten. We houden de zaak in ieder geval in de gaten.

Itte Overing
Juridisch adviseur

Tessa van Schijndel
Juridisch adviseur

E-health

Digitalisering in de zorg: 2020 en 2021

Dit is het een mooi moment om terug te blikken op wat 2020 ons allemaal heeft gebracht en vooruit te kijken naar 2021. De lijn die al jaren zichtbaar is, is het afgelopen jaar doorgetrokken: de zorg maakt een digitaliseringsslag. Komend jaar zal er met het wetsvoorstel Elektronische gegevensuitwisseling in de Zorg ("Wegiz")[1] nog een schepje bovenop worden gedaan. Sinds afgelopen jaar heeft de patiënt recht op elektronische afschrift en inzage van zijn medische gegevens. Als het wetsvoorstel wet wordt, dan moeten zorgaanbieders ook verplicht elektronisch gaan uitwisselen.

Zorg op afstand
Hoewel de hype rond digitalisering in de zorg al aardig op gang was, hoorde wij laatst dat dit in de zorg nog zo'n 15 jaar achterloopt ten opzichte van andere sectoren, zoals de financiële sector. Een bijzondere constatering, als je bedenkt welke ontwikkelingen de digitalisering in zorg het afgelopen jaar heeft doorgemaakt.

Als gevolg van de pandemie heeft de digitalisering onder de noemer zorg op afstand of beeldschermzorg een enorme vlucht genomen. Oplossingen voor zorg op afstand schieten als paddenstoelen uit de grond en ook ICTRecht heeft niet stilgezeten. We hebben afgelopen jaar factsheets geschreven met nuttige informatie over de juridische aandachtspunten bij zorg op afstand.[2] Ook hebben we een video podcast gepubliceerd die nog steeds gratis te bekijken is.[3] De wetgever heeft daarnaast wet- en regelgeving verruimd om mogelijkheden te creëren om meer zorg op afstand te verlenen. Zo is het eerste face-to-face contact tussen patiënt en zorgverlener niet langer meer een voorwaarde om de zorg vergoed te krijgen. De Nederlandse Zorgautoriteit ('NZa') heeft besloten om deze regel tijdelijk te verruimen. Daarnaast heeft het Ministerie van Volksgezondheid en Welzijn ('VWS') samen met de Vereniging van Zorgaanbieders voor Zorg communicatie ('VZVZ') een "corona-opt-in" ingesteld. Dit is een tijdelijke veronderstelde toestemming van de patiënt om zijn gegevens op te nemen in een elektronisch uitwisselingssysteem als de patient niet eerder zijn toestemming heeft verleend. Op de huisartsenpost en de spoedeisende hulp is het tijdelijk mogelijk om de gegevens te raadplegen van patiënten met een verdenking van een coronabesmetting.

Elektronisch uitwisselen van patiëntgegevens
Wanneer een patiënt bij een zorgverlener in behandeling is, legt deze zorgverlener medische gegevens van de patiënt vast. Deze medische gegevens kunnen relevant zijn voor andere zorgverleners. Hierbij is goede en tijdige gegevensuitwisseling tussen zorgverleners en met de patiënt onmisbaar voor goede zorg. Deze uitwisseling kan enerzijds plaatsvinden omdat de zorgverlener een behandelrelatie heeft met de patiënt of anderzijds via een elektronisch uitwisselingssysteem. ICTRecht heeft de ontwikkelingen van het laatste jaar op de voet gevolgd en hier uitgebreid over geschreven in diverse artikelen en blogs.

In het Wegiz zullen zorgverleners verplicht worden gesteld om onderling gegevens elektronisch en gestandaardiseerd met elkaar uit te wisselen. Minister Ark verwacht begin 2021 het wetsvoorstel naar de

1. Zie voor meer informatie: https://www.rijksoverheid.nl/documenten/brochures/2017/06/01/elektronische-gegevensuitwisseling-in-de-zorg
2. https://www.ictrecht.nl/juridisch-advies/zorg-ict-recht
3. https://www.ictrecht.nl/academy/webinars/webinar-zorg-op-afstand

Tweede Kamer te sturen. Het idee is om per gegevensuitwisseling een standaard te formuleren die in een Algemene Maatregel van Bestuur ('AMvB') verplicht wordt gesteld. De minister wil naar een model toe waar zo min mogelijk toestemming gevraagd hoeft te worden.

Via een elektronisch uitwisselingssysteem
In de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg ('Wabvpz') en het Besluit elektronische gegevensverwerking door zorgaanbieders zijn regels opgenomen rondom het elektronisch uitwisselingssysteem. Een deel van deze regels is op 1 juli 2017 al in werking getreden, terwijl het tweede deel afgelopen juli in werking trad. Voor het beschikbaar stellen van medische gegevens via een elektronisch uitwisselingssysteem geldt dat de patiënt vooraf uitdrukkelijke toestemming moet geven voor de opname van zijn gegevens in het systeem. Daar is sinds dit jaar bijgekomen dat de patiënt nu ook het recht heeft om kosteloos elektronische inzage en afschrift te krijgen van zijn medisch dossier en de logging daarvan. De eis van de gespecificeerde toestemming is wederom uitgesteld en wordt wellicht volledig geschrapt.

In het kader van een behandelrelatie
De uitwisseling van medische gegevens tussen zorgverleners in het kader van een behandelrelatie kenmerkt zich door de veronderstelde toestemming die wordt geacht aanwezig te zijn, omdat de patiënt toestemming heeft gegeven voor zijn behandeling.

Via een persoonlijke gezondheidsomgeving
Een ander pad dat de wetgever bewandelt is het stimuleren van de inzage in het medisch dossier door de patiënt. Middels een persoonlijke gezondheidsomgeving ('PGO') of een ander portaal waarmee patiënten hun gegevens kunnen inzien, kunnen ook gegevens met patiënten worden uitgewisseld. Op deze manier wordt voldaan aan de verplichting om de patiënt elektronisch inzage in zijn medisch dossier te geven. De Stichting MedMij is tot een afsprakenstelsel gekomen dat waarborgen biedt in de bescherming en beveiliging van de gegevensuitwisseling met patiënten.

Medische hulpmiddelen
De wetgeving rondom medische hulpmiddelen heeft ons het afgelopen jaar flink beziggehouden. Begin dit jaar schreven we over de druk die op de verschillende partijen komt te liggen die zich bezighouden met medische software. Fabrikanten en andere partijen, zoals ook zorgverleners, moeten zich voorbereiden op de nieuwe regels. Als een fabrikant een medisch hulpmiddel op de markt wil brengen, heeft hij een CE-markering nodig. Niet CE-gemarkeerde medische hulpmiddelen mogen niet door zorgverleners worden gebruikt. Die CE-markering geeft aan dat de software voldoet aan de wettelijke veiligheids- en kwaliteitseisen. De risicoklasse van de software bepaalt wie de CE-markering toekent.[4]

Kort daarna kwam de Europese Commissie met het bericht dat de Verordening Medische Hulpmiddelen ('MDR') met één jaar is uitgesteld. De Europese Commissie voorziet dat de implementatie van de MDR op dit moment een te grote belasting is voor de betrokken partijen.

De MDR zal nu naar alle waarschijnlijkheid vanaf mei 2021 van toepassing worden. Dit betekent dat er voor onder andere software veel gaat veranderen. De definitie van een medisch hulpmiddel wordt aangescherpt, waardoor een breder scala aan software als medisch hulpmiddel wordt aangemerkt. Bovendien wordt een nieuwe risicoclassificatie toegevoegd, waardoor medische software in een hogere risicoklasse valt en beoordeling door een externe partij, een zogenaamde *notified body*, noodzakelijk is.

Al met al een aantal nieuwe ontwikkelingen die we ook komend jaar op de voet zullen blijven volgen. Op deze manier blijven we u ondersteunen bij het vertalen van de wet- en regelgeving naar de praktijk, het opstellen of beoordelen van documenten, het voeren van onderhandelingen (al dan niet op de achtergrond) en het leveren van continue ondersteuning op afstand of locatie. Wilt u zelf meer kennis in huis halen? Lees onze (blog)artikelen en/of volg een van onze trainingen of webinars.

4. https://www.ictrecht.nl/blog/kunnen-notified-bodies-de-werkdruk-door-de-verordening-over-medische-hulpmiddelen-aan

Gratis webinar Leveranciers-management

ICTRECHT

Binnen de zorg is men hard op weg om zelfs de primaire processen - het verlenen van zorg - te digitaliseren. Deze digitalisering wordt meestal ingekocht. Een belangrijk onderwerp hierbij is informatieveiligheid.

Verplichte kost in dat kader is de implementatie van NEN 7510. Een onderwerp uit de NEN 7510 dat in het oog springt is: leveranciers-management.

In deze webinar van 1 uur neemt ICTRecht u mee in het onderwerp leveranciers-management. Aan de hand van praktijk-voorbeelden en met gebruik van de drie expertises: security, privacy & ICT- en gezondheidsrecht, geven wij u meer inzicht in wat NEN 7510 precies vereist als het aankomt op leveranciersmanagement.

Schrijf u gratis in en ontvang de webinar direct in uw mailbox!

Inschrijven kan via:
ictrecht.nl/zorg-webinar

Niek Bakker
Juridisch adviseur
Noord-Nederland

Milan van der Spoel
Juridisch adviseur
Noord-Nederland

E-commerce

Consumentenrecht van update voorzien

Wat verandert er voor de verkoper?

Momenteel zijn het voor webshops ongekende tijden. Waar vele bedrijven vechten om het hoofd boven water te houden, zien internetwinkels in ons land sinds de uitbraak van het coronavirus hun omzet explosief stijgen. Er is al lange tijd een digitalisering van onze maatschappij gaande, maar tegenwoordig zit deze in een hogesnelheidstrein. Nu de consument meer online aankopen doet dan ooit, komen vernieuwingen in het Nederlandse kooprecht als geroepen.

Per 1 januari 2022 wordt het Nederlandse consumentenrecht aangevuld en gemoderniseerd door de implementatie van twee nieuwe richtlijnen: Richtlijn EU 2019/771 (hierna: Richtlijn verkoop goederen) en Richtlijn EU 2019/770 (hierna: Richtlijn digitale inhoud en diensten). Omdat consumenten in plaats van tastbare objecten tegenwoordig steeds meer computerspellen, e-books, streamingdiensten en andere digitale diensten kopen, dient het consumentenkooprecht hierop aangepast te worden. De richtlijnen vervangen de verouderde Richtlijn consumentenkoop uit 1999 en zullen in Nederland spoedig hun toepassing vinden door middel van de Implementatiewet richtlijnen verkoop goederen en levering digitale inhoud. In dit artikel zullen de grootste veranderingen ten gevolge van deze update van het consumentenrecht besproken worden.

Rijkweidte

Beide richtlijnen gaan uit van maximumharmonisatie en zijn alleen van toepassing op overeenkomsten tussen een professionele verkoper of leverancier en een consument (B2C). Onder de Richtlijn verkoop goederen valt naast de koop van 'gewone' zaken tevens de koop van zaken met digitale elementen. Dit betreffen zaken waarin digitale inhoud of een digitale dienst is verwerkt of die daarmee op zodanige wijze onderling verbonden is, dat het ontbreken daarvan ertoe zou leiden dat de zaak zijn functies niet meer kan vervullen (*embedded software)*. Er valt hierbij bijvoorbeeld te denken aan slimme huishoudelijke apparaten of een smartwatch.

Onder de Richtlijn digitale inhoud en diensten vallen overeenkomsten voor de levering van louter digitale inhoud en digitale diensten. Met andere woorden bevinden deze inhoud en diensten zich niet op een fysieke drager. Bij digitale inhoud kan gedacht worden aan computerprogramma's en e-books. Digitale diensten zijn bijvoorbeeld video- en muziekstreamingsdiensten.

Noodzakelijke updates

De implementatie van de richtlijnen brengt verschillende veranderingen met zich mee waar nieuwe overeenkomsten vanaf 1 januari 2022 aan moeten voldoen.[1] Met name de verplichting voor de verkoper om de consument te voorzien van noodzakelijke updates die nodig zijn om ervoor te zorgen dat software (en bijbehorende beveiliging) in overeenstemming met de overeenkomst blijft, zal merkbaar zijn in de praktijk. Deze eis geldt echter enkel voor meegeleverde software en niet voor alle goederen. Als men bijvoorbeeld een digitaal leerboek aanschaft, heeft men logischerwijs

bij het verschijnen van de nieuwe editie niet automatisch recht op een 'update'.

Hoe lang dient een verkoper aan deze eis te voldoen? Een voor de praktijk belangrijke vraag, waar nog geen duidelijk antwoord op is. Dit zal moeten blijken uit rechtspraak. De richtlijnen stellen immers dat de consument zo lang van updates dient te worden voorzien, als hij redelijkerwijs mag verwachten.[2] Door geen termijn aan de updateverplichting te stellen, worden de huidige conformiteitsregels in stand gehouden. Het is aan de koper om de updates op tijd en correct te installeren, mits de verkoper hiertoe correcte instructies geeft. Wanneer de koper dit nalaat, kan hij de verkoper wat updates betreft niet aanspreken op (non-)conformiteit.

Conformiteit
De kern van beide richtlijnen ziet op het conformiteitsbegrip, ook wel de wettelijke garantie genoemd. Delen van deze nieuwe regelgeving zijn gelijk gebleven aan de oude regelgeving of vormen een codificatie van rechtspraak van de Europese Unie. Er zullen uitgebreidere subjectieve en objectieve conformiteitseisen worden gesteld. De subjectieve eis is dat een zaak, digitale inhoud of digitale dienst moet voldoen aan de vereisten die in de koopovereenkomst zijn overeengekomen, zoals de hoeveelheid en kwaliteit.[3] Daarnaast zijn ook de verwachtingen van de consument op basis van de precontractuele informatie relevant. De objectieve eis is dat een goed geschikt moet zijn voor de doeleinden waarvoor goederen van hetzelfde type gewoonlijk worden gebruikt.

De verkoper is aansprakelijk voor een conformiteitsgebrek dat binnen twee jaar na levering kenbaar wordt, of wanneer de overeenkomst een duurovereenkomst betreft, voor de periode waarin de digitale inhoud of digitale dienst moet worden geleverd. De consument dient de verkoper binnen bekwame tijd op de hoogte te stellen van het gebrek. In Nederland gaat een termijn van twee maanden na ontdekking gelden. Voor de levering van digitale inhoud en digitale diensten geldt een dergelijke kennisgevingsverplichting niet.

Omkering bewijslast bij gebreken
Aangrenzend aan conformiteit, brengen de richtlijnen een belangrijke wijziging mee ten aanzien van de duur voor de omkering van de bewijslast. Oorspronkelijk was deze termijn slechts zes maanden. In de Nederlandse wetgeving wordt deze termijn na implementatie verdubbeld. Indien een gebrek zich binnen één jaar na aflevering manifesteert, vindt een omkering van de bewijslast plaats.[4] Er geldt een vermoeden dat het gebrek al aanwezig was ten tijde van de koop. Vervolgens is aan de verkoper om het tegendeel te bewijzen. Deze termijn geldt zowel voor zaken als digitale inhoud en digitale diensten. In het geval van een voortdurende levering van digitale inhoud geldt een termijn van de gehele contractsperiode.

Remedies bij non-conformiteit
Ten slotte staan de consument volgens de nieuwe richtlijnen verschillende remedies ter beschikking bij non-conformiteit. De consument kan zich slechts op non-conformiteit beroepen en de overeenkomst ontbinden indien het gebrek niet gering is. In tegenstelling tot bij betaling met een prijs, is ontbinding bij slechts een gering gebrek van een digitale dienst of digitale inhoud wel mogelijk indien de consument met persoonsgegevens heeft betaald. De bewijslast van conformiteit ligt bij de verkoper.

De consument heeft onder de Richtlijn verkoop goederen recht op kosteloos herstel van het gebrekkige of levering van het ontbrekende, prijsvermindering of ontbinding. Ook volgens de Richtlijn digitale inhoud en diensten dient de handelaar eerst te trachten het gebrek weg te nemen. Enkel indien uit een verklaring van een handelaar blijkt dat hij niet zal of kan nakomen, het geschonden leveringsmoment essentieel is, het gebrek zich opnieuw manifesteert, het gebrek van grote ernst is of het wegnemen van de non-conformiteit ernstige overlast zou opleveren, is prijsvermindering mogelijk en eventueel ontbinding.

Conclusie
Om te blijven voldoen aan de meest recente wetgeving voor consumentenrecht, is het dus belangrijk dat leveranciers hun website en algemene voorwaarden up-to-date houden en zelf ook bewust blijven van alle wettelijke verplichtingen. Heeft u hulp nodig bij het vernieuwen van uw algemene voorwaarden of website om te blijven voldoen aan de meest recente consumentenrecht-wetgeving? ICTRecht helpt u hier graag bij.

1. De nieuwe wetgeving is tevens van toepassing op reeds bestaande overeenkomsten omtrent digitale inhoud en digitale diensten, waarvan de levering nog plaats dient te vinden na 1 januari 2022.
2. Er moet worden gekeken naar de levensduur van de zaak, vgl. art. 7:17 lid 2 en 7:18 BW.
3. Een goed moet wat betreft de beschrijving, het type, de hoeveelheid en kwaliteit, functionaliteit, compatibiliteit, interoperabiliteit en andere kenmerken voldoen aan de koopovereenkomst, overweging 26 Richtlijn EU 2019/771.
4. Er is hier sprake van minimumharmonisatie, lidstaten mogen de termijn zelfs verlengen tot twee jaar, art. 11 Richtlijn EU 2019/771 en art. 12 Richtlijn EU 2019/770.

Eline Streefkerk
Juridisch adviseur

Privacy

Is het vergeetrecht in de vergetelheid geraakt?

Het zwart maken van mensen, producten of bedrijven op internet is een trend die nog steeds in ontwikkeling is. Het Ministerie van Justitie definieert *naming & shaming* als: "Het publiek bekendmaken van negatieve informatie over eigenschappen van producten en productieprocessen. Het doel is de reputatie van de aanbieder van het product of de dienst te beïnvloeden en het gedrag van de consumenten te sturen."[1] Daarnaast worden er regelmatig pikante video's gedeeld op internet en wordt er *fake news* de wereld in geholpen. Er worden zelfs zelfmoordpogingen gepleegd n.a.v. negatieve reacties op social media. Maar als een schadelijke boodschap eenmaal gepubliceerd is op internet en is gekoppeld aan uw naam, is er dan nog een weg terug?

De oplossing
Op 13 mei 2014 was er een baanbrekend arrest van het Europese Hof van Justitie met betrekking tot het vergeetrecht.[2] Vanaf dit moment werd de mogelijkheid geschapen voor betrokkenen om aan zoekmachines een verzoek te doen om bepaalde zoekresultaten, die gelinkt worden aan hun naam, te verwijderen. Voor het effectief inroepen van het vergeetrecht tegen zoekmachines dient er een afweging gemaakt te worden. Hierbij spelen drie verschillende belangen een rol:
1. Het commerciële belang van een zoekmachine om de zoekresultaten te tonen;
2. Het belang van informatievergaring voor het publiek;
3. Het privacybelang van de betrokkene die een beroep doet op het vergeetrecht.

Hoe werkt dat dan bij Google?
Op een speciaal ingerichte website van Google kan een betrokkene een verzoek doen om bepaalde zoekresultaten te verwijderen.[3] Vervolgens komt dit verzoek binnen bij Google, die het verzoek beoordeeld. Hierbij moet een afweging gemaakt worden tussen de drie verschillende belangen. Deze afweging wordt in eerste instantie door Google zelf gemaakt.[4]

Mocht het verzoek worden afgewezen, kan de betrokkene een klacht indienen bij de Autoriteit Persoonsgegevens. Zij kunnen opnieuw een inhoudelijke afweging maken en kunnen Google alsnog verzoeken de zoekresultaten te verwijderen. Indien betrokkene het niet eens is met de beslissing van Google of de Autoriteit Persoonsgegevens, kan deze nog de weg naar de rechter bewandelen.

Of toch niet?
Maar hoe effectief is het inroepen van het vergeetrecht eigenlijk? Wordt er weleens een verzoek gehonoreerd door Google of de rechter? Of is het arrest toch niet zo baanbrekend als we in eerste instantie dachten?

Zoals hierboven uiteengezet dient er voor de honorering van een verwijderingsverzoek van bepaalde zoekresultaten een afweging te worden gemaakt. Als eerste uitgangspunt geldt daarbij dat privacyrechten in beginsel voorrang hebben. Dit uitgangspunt is echter afhankelijk van "de aard van de informatie en de gevoeligheid ervan voor het privéleven van de betrokkene om over deze informatie te beschikken, wat met name wordt bepaald door de rol die deze persoon in het openbare leven speelt."[5] In dit kader gaat het er

1. https://bit.ly/39S9PMb
2. https://bit.ly/37IckxT
3. https://bit.ly/3IX9qdN
4. https://bit.ly/3qLCPLF
5. HvJ EU 13 mei 2014, zaak C-131/12, overweging 81.

met name om wie de persoon is die het verzoek indient en welke (maatschappelijke) functie hij of zij uitoefent.[6] De minister-president moet bijvoorbeeld meer negativiteit dulden dan een gemiddeld persoon, gezien zijn publieke functie. Naast de rol die de betrokkene in het openbare leven speelt, speelt ook een rol of de zoekresultaten onnauwkeurig, ontoereikend, niet ter zake dienend of bovenmatig zijn voor de doeleinden van de verwerking. Bijvoorbeeld omdat zij niet zijn bijgewerkt of omdat zij langer worden bewaard dan noodzakelijk is, tenzij de bewaring ervan is vereist wegens historische, statistische of wetenschappelijke doeleinden.[7]

Er zijn regelmatig betrokkenen geweest die hun heil zochten bij de burgerlijke rechter. Uit de eerste uitspraken die volgden na de uitspraak van het Europese Hof van Justitie kan worden afgeleid dat er een bepaalde terughoudendheid was in de beoordeling van de verwijderingsverzoeken.[8] Zo werd door de Nederlandse rechter bepaald dat het vergeetrecht moet worden gekwalificeerd als een 'uitzondering op het algemene uitgangspunt op het recht van Google Inc. op informatievrijheid, waaraan strenge eisen worden gesteld.[9]

In een uitspraak die daarop volgt oordeelt de rechter dat het verboden is voor Google om strafrechtelijke persoonsgegevens te verwerken, tenzij er sprake was van een uitzonderingsgrond in de destijds geldende Wet bescherming persoonsgegevens (Wbp).[10] De rechter lijkt in de uitspraken die hierop volgen een andere weg in te slaan. De definitie van strafrechtelijke gegevens wordt beperkt uitgelegd, waardoor het verwerkingsverbod niet op Google van toepassing is. Er hoeft geen sprake te zijn 'van een strafrechtelijke veroordeling, maar wel van zodanige concrete feiten en omstandigheden dat zij een als een strafbaar feit te kwalificeren bewezenverklaring kunnen dragen.[11] Een link naar een artikel werd niet aangemerkt als een strafrechtelijk gegeven en de beschuldiging ervan ook niet, waardoor de zoekresultaten zichtbaar mochten blijven in Google.[12] Ook werd bepaald dat tuchtrechtelijke persoonsgegevens niet onder de definitie van bijzondere of strafrechtelijke persoonsgegevens zouden vallen, en dat de verwijzing naar het strafrecht impliceert dat het tenminste moet gaan om maatregelen met een punitief karakter.[13]

Daarna volgt er een uitspraak van het Europese Hof van Justitie, waarin voor opheldering gezorgd wordt met betrekking tot het verwerkingsverbod voor Google. Uit deze uitspraak volgt dat Google bijzondere persoonsgegevens kunnen beroepen, indien zij zich onder bepaalde omstandigheden kan beroepen op 'redenen van zwaarwegend algemeen belang'. Daarnaast volgt uit deze uitspraak dat Google hierbij moet nagaan of de opname van deze zoekresultaten strikt noodzakelijk blijkt ter bescherming van het recht op vrijheid van informatie van het publiek die mogelijk geïnteresseerd is in toegang tot deze webpagina via een dergelijke zoekopdracht. Ook wordt bepaald dat indien een verwijderingsverzoek moet worden uitgevoerd, Google niet gehouden is deze links te verwijderen voor alle versies van zijn zoekmachine doch enkel voor alle lidstaat specifieke versies van die zoekmachine.[14]

Opmerkelijk aan deze uitspraak van het Europese Hof van Justitie is daarnaast dat Google in ieder geval uiterlijk bij het verwijderingsverzoek de resultatenlijst dusdanig dient te ordenen dat het algehele beeld dat hiermee voor de internetgebruiker wordt geschetst een afspiegeling vormt voor de actuele gerechtelijke situatie, hetgeen onder meer vereist dat links naar webpagina's die daarover informatie bevatten als eerste op deze lijst verschijnen.[15]

Conclusie

Het vergeetrecht is absoluut niet in de vergetelheid geraakt. Er zijn veelvuldig rechtszaken aangespannen die ons meer inzicht zouden moeten verschaffen in de wijze waarop het commerciële belang van Google, de informatievergaring voor de internetgebruikers en het privacyrecht van betrokkene tegen elkaar zouden moeten worden afgewogen. Door de laatste uitspraak van het Europese Hof van Justitie heeft Google echter niet alleen de verplichting om deze belangen zelf tegen elkaar af te wegen, maar zou zij er ook nog voor moeten zorgen dat de zoekresultaten worden gemanipuleerd. Heel bijzonder, als je het mij vraagt.

6. Zie bijvoorbeeld Rb. Den Haag 19 april 2018 of Rb. Midden Nederland 14 november 2018.
7. HvJ EU 13 mei 2014, zaak C-131/12, overweging 92.
8. Rb. Amsterdam 18 september 2014, Rb. Amsterdam 12 februari 2015, Rb. Amsterdam 24 december 2015.
9. Rb. Amsterdam 12 februari 2015, r.o. 4.7.
10. Rb. Rotterdam 29 maart 2016.
11. Rb. Rotterdam 29 maart 2016, r.o. 4.8.
12. Rb. Den Haag 12 januari 2017 en Rb. Midden Nederland 20 februari 2017.
13. Rb. Amsterdam 19 juli 2018, r.o. 4.4 en Gerechtshof Den Haag 24 december 2019.
14. Hof van Justitie EU 24 september 2019, zaak C-136/17, r.o. 78.
15. Hof van Justitie EU 24 september 2019, zaak C-136/17, r.o. 78.

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Internetrechtspraak

Afwijzing verzoek op grond van artikel 17 AVG
(Rechtbank Amsterdam, 2 april 2020)
De rechtbank Amsterdam wijst een verzoek op grond van artikel 17 AVG (recht op vergetelheid van een geanonimiseerde uitspraak die betrekking heeft op verzoekster, gepubliceerd op www.rechtspraak.nl) af omdat een juridische analyse van een rechtszaak niet aan te merken valt als een 'persoonsgegeven' in de zin van de AVG.

https://bit.ly/3m0WDqL

Inbreuk op Uniemerkrecht
(Gerechtshof Den Haag, 21 april 2020)
Het gerechtshof Den Haag oordeelt, na terugverwijzing door de Hoge Raad, dat een houdster van een Uniewoordmerk met succes een inbreukprocedure kan starten tegen een domeinnaamhouder die de naam (Uniewoordmerk) in de domeinnaam verwerkt. Hierdoor kan de indruk gewekt worden dat de twee partijen een commerciële band zijn aangegaan, die feitelijk gezien niet bestaat. De domeinnaamhouder heeft inbreuk gemaakt op het Uniemerkrecht van de Uniemerkhoudster.

https://bit.ly/3guQXny

Blue Ocean tegen X
(Gerechtshof Amsterdam, 14 juli 2020)
Er bestaat een overeenkomst (PSA) tussen twee partijen ter ontwikkeling en exploitatie van een applicatie op het gebied van Human Resource Management. Partij X zou de architectuur en de ontwikkeling van de applicatie verzorgen, terwijl Blue Ocean de applicatie zou testen, verkopen en implementeren bij eindgebruikers. Vervolgens is er een geschil ontstaan over de inspanningsverbintenis van X, de partij die de ontwikkeling van de applicatie zou verzorgen. De implementatie van de door X geleverde software is bij twee partijen niet goed verlopen en afnemers van de software geven aan dat zij problemen ondervinden met de gedemonstreerde software. Ter verdediging stelt X dat er een verschil is tussen het design en het gebruik van de applicatie, waardoor het mogelijk niet aansluit bij de wensen en ideeën van Blue Ocean. Ook voert zij aan dat Blue Ocean heeft gefaald om acceptatietesten uit te voeren en hierdoor zelf ook een goede werking van de applicatie heeft gehinderd. Blue Ocean maakt een verwijt dat de applicatie op alle browsers zou moeten kunnen draaien, maar gezien dit nooit specifiek overeengekomen is (en IE10 door Microsoft niet meer ondersteunt wordt) kan dit X niet verweten worden. X mocht ervan uitgaan dat Blue Ocean deskundig genoeg was om eventuele problemen op te merken en te ondervangen. Zij kan de schuld niet neerleggen bij X, omdat ze zelf tekort is geschoten. Volgens het Hof kan er niet worden vastgesteld dat X haar inspanningsverplichting, informatie- of waarschuwingsplicht heeft geschonden en bekrachtigt het vonnis van de rechtbank Amsterdam.

https://bit.ly/3lZMs5E

Undercover in Nederland' niet verboden
(Rechtbank Amsterdam, 23 juli 2020)
De rechtbank Amsterdam beslist dat de televisieuitzending 'Undercover in Nederland' niet verboden hoeft te worden, eiseres moet wel volledig onherkenbaar in beeld verschijnen.

https://bit.ly/39Vrhz6

Inbreuk auteursrechten op foto
(Rechtbank Midden-Nederland, 5 augustus 2020)
Eiser is een fotograaf die zijn foto's op verschillende websites plaatst. Een van die websites wordt geëxploiteerd en beheerd door gedaagde. Hij heeft de foto in bewerkte vorm op meerdere plaatsen op zijn website en de bijbehorende Facebookpagina geplaatst, waarbij de naam van de fotograaf is verwijderd en het logo van de website over de foto heen is geplaatst. Hiervoor heeft eiser geen toestemming gegeven en geen vergoeding ontvangen. Dat gedaagde de afbeelding zonder naamsvermelding op Google had gevonden en niet wist dat hij deze niet zomaar mocht gebruiken, doet niet af aan

de inbreuk van het auteursrecht door gedaagde. De inbreuk hoeft niet bewust plaats te vinden. Eiser krijgt het gevorderde bedrag van € 360 per jaar toegewezen.

https://bit.ly/3mZwfP6

Rectificatieverzoek uitlating op Facebook
(Rechtbank Limburg, 18 augustus 2020)
Gedaagde heeft in januari 2020 een puppy aangeschaft bij eisers. Vijf maanden later moet het dier vanwege ernstige gezondheidsklachten worden ingeslapen. Gedaagde plaatst na het overlijden van de hond een negatief bericht over de 'broodfokker' waar de hond is aangeschaft en roept onder andere mensen op om geen hond aan te schaffen bij deze 'malafide' fokker. Het bericht heeft 10 dagen op Facebook gestaan en is zo'n 21.000 keer gedeeld, waarna gedaagde het bericht heeft verwijderd. De kern van dit geschil ziet op de uitlatingen die gedaagde openbaar op social media heeft gedaan en of deze onrechtmatig jegens de eisers zijn. De eisers zijn niet gediend van dit bericht over hun handelspraktijken en eisen dat gedaagde de term 'broodfokker' niet langer zal noemen en dat gedaagde het bericht van social media afhaalt. Daarnaast vorderen zij dat gedaagde een rectificatie van het bericht openbaar op Facebook plaatst, zodat de naam van de fokker niet langer negatief wordt benoemd. De rechtbank oordeelt dat het gebruik van de term 'broodfokker' onder de vrijheid van meningsuiting valt en het verbieden van dit soort uitlatingen in strijd met het recht uit artikel 10 lid 2 EVRM zou zijn. Verder ziet de rechtbank geen risico dat gedaagde, na verwijdering van het eerste bericht, nogmaals dit soort berichten zal plaatsen over de situatie rondom de pup. Tot slot oordeelt de rechtbank over de gevorderde rectificatie (over het inmiddels verwijderde, maar vaak gedeelde bericht): "temeer nu niet gezegd is dat dezelfde personen een rectificatie zullen delen waardoor het bereik en daarmee het effect van een eventuele rectificatie zodanig gering is dat geen passende oplossing biedt." De vorderingen van eisers worden afgewezen.

https://bit.ly/39TP96k

Akte van overdracht IE-recht voldoende bepaalbaar
(Rechtbank Amsterdam, 4 september 2020)
In deze zaak heeft eiser voor gedaagde (bedrijf voor online verbetering van levensstijl) software ontwikkeld. In de samenwerkingsovereenkomst die partijen zijn aangegaan is een bijlage (akte van inbreng) opgenomen waarin de IE-rechten van eiser op gedaagde worden overgedragen. Eiser stelt dat dit een tijdelijke overdracht zou inhouden en de definitieve overdracht nooit heeft plaatsgevonden, omdat de rechten uit de bepaling van de overeenkomt onvoldoende nauwkeurig zijn beschreven en eist een verbod voor gedaagde op het gebruik van de IE-rechten. Duidelijk wordt dat het de intentie was om de IE-rechten op de software over te dragen en dat deze in de akte van overdracht voldoende bepaalbaar omschreven zijn. De IE-rechten zijn rechtsgeldig aan de gedaagde overgedragen.

https://bit.ly/37IhcmA

Recensies Google (Maps) onrechtmatig
(Rechtbank Amsterdam, 8 september 2020)
De voorzieningenrechter oordeelt dat recensies die geplaatst zijn op Google (Maps) onrechtmatig zijn, wanneer deze niet zijn gebaseerd op daadwerkelijke ervaringen met het bedrijf waar de recensie over wordt geschreven.

https://bit.ly/2K1mHVg

Verzoek tot verwijdering registratie bij Bureau Kredietregistratie
(Gerechtshof Den Haag, 8 september 2020)
Uitspraak gerechtshof Den Haag. Verzoekster dient een verzoek in bij de ING bank waarmee zij de bank verzoekt om de betalingsachterstand - die zij eerder heeft opgebouwd - te verwijderen uit het registratiesysteem van het Bureau Kredietregistratie. Verzoekster stelt dat er een belangenafweging gemaakt dient te worden o.g.v. artikel 21 lid 2 AVG, omdat de registratie o.g.v. artikel 6 lid 1 sub e of f AVG heeft plaatsgevonden. De ING betwist dit en stelt dat de registratie op grond van een wettelijke verplichting heeft plaatsgevonden (art. 6 lid 1 sub c AVG); de ING heeft de kredietregistratie uitgevoerd o.g.v. de wettelijke plicht die voortvloeit uit de Wet financieel toezicht. Het Hof gaat hier niet in mee en stelt dat er geen sprake is van een wettelijke verplichting voor deze vorm van gegevensverwerking. De overige grieven van verzoekster houden overigens geen stand en ING wordt in het gelijk gesteld. Een maand geleden oordeelde het gerechtshof 's-Hertogenbosch nog dat deze kredietregistratie door financiële instellingen (banken) wel onder artikel 6 lid 1 sub c AVG vallen en dat de verzoeker daarom geen recht op bezwaar uit artikel 21 AVG toekomt.

https://bit.ly/2K6UCf4

Eisers tegen YouTube
(Rechtbank Amsterdam, 9 september 2020)
Eisers (een programmamaker en huisarts) plaatsen op YouTube een tweetal interviews op het YouTube-kanaal Cafe Weltschmerz (burgerjournalistiek platform). In deze interviews spreekt de huisarts zich uit als voorstan-

der van het geneesmiddel Hydroxychloroquine, dat volgens hem ingezet kan worden tegen de bestrijding van COVID-19. De video's worden door YouTube verwijderd, omdat zij in strijd zijn met de Servicevoorwaarden van het platform. YouTube heeft deze voorwaarden in mei 2020 aangevuld met het 'Beleid tegen misleidende medische informatie over COVID-19'. Eisers zijn het niet eens met de verwijdering van hun video's van het platform. Zij stellen dat het beleid van YouTube in strijd is met de visie van de Wereldgezondheidsorganisatie (WHO) en het Nederlandse RIVM en dat het beleid niet vaststaat. Daarnaast zou de verwijdering van de video's een onaanvaardbare beperking van hun recht op vrijheid van meningsuiting zijn en zou YouTube censuur plegen. Nu er nog geen duidelijkheid is over de werking van het geneesmiddel, is het niet de taak van YouTube om daarover te oordelen, aldus de eisers. YouTube geeft aan dat zij verantwoording afdragen voor de content die op het platform wordt geplaatst en stelt dat de verwijdering van de video's gerechtvaardigd kan worden met een beroep op de huidige Servicevoorwaarden. De rechtbank oordeelt dat de interviews van eisers als desinformatie kunnen worden aangemerkt, nu de werking van het betreffende geneesmiddel niet is bewezen en er aan de toelating van geneesmiddelen strikte eisen gesteld worden. De visie van de huisarts over het geneesmiddel vormt geen onderdeel van het debat en informeert de kijker onjuist. YouTube had het recht om de video's te verwijderen, mede vanwege de bekendheid van het platform. De vordering van de eisers worden afgewezen. Zie ook de noot op pagina 33.

https://bit.ly/36ZeJVF

Inbreuk privacy werknemer bij verwijtbaar handelen
(Gerechtshof 's-Hertogenbosch, 10 september 2020)
Het gerechtshof 's-Hertogenbosch ontbindt arbeidsovereenkomst op verzoek werkgever, nadat werknemer verwijtbaar heeft gehandeld. Dat de werkgever, om tot deze conclusie te komen, een inbreuk op de privacy van de werknemer heeft gemaakt weegt niet op tegen de handelswijze van de werknemer.

https://bit.ly/2VSoCy2

HvJEU doet uitspraak over netneutraliteit
(Hof van Justitie van de EU, 15 september 2020)
In deze uitspraak legt het Hof van Justitie voor het eerst de verordening van de Unie uit waarin de "neutraliteit van het internet" is verankerd. Het Hongaarse telecombedrijf Telenor rekende een 'nultarief' voor bepaalde diensten. Zelfs nadat de databundel op is, kan door abonnementhouders van deze diensten gebruik worden gemaakt. Alle overige diensten worden vertraagd of zelfs geblokkeerd. De Hongaarse media-autoriteit oordeelde eerder al dat deze handelswijze in strijd is met de verordening. Nu vindt ook het Hof dat dit soort abonnementen het recht van gebruikers op een vrij en open internet in gevaar brengen en dat een internettoegangsdienst geen beperking van de uitoefening van de rechten van eindgebruikers zoals in Verordening 2015/2120, mag opleveren.

https://bit.ly/2VXvOZK

Auteursrecht op database
(Rechtbank Den Haag, 16 september 2020)
Scientia is een Engelse leverancier van software om roosters te generen voor hogescholen en universiteiten. Voor de software maakt zij gebruik van twee databases (ESDB en RDB). Eveoh is een Nederlandse onderneming en ontwikkelt, implementeert, integreert en host software ten behoeve van onderwijsinstellingen. Bij klanten van Eveoh die de software van Scientia afnemen, leest de software van Eveoh de data van de databases ESDB en RDB uit. De software van Eveoh is complementair aan die van Scientia, Eveoh stelt dat Scientia op de hoogte is van deze werkwijze en kan op basis van een specialistenrapport aantonen dat zij de *instances* slechts host en niet kopieert. Maar Scientia is van mening dat Eveoh door een koppeling te maken naar de databases inbreuk maakt op haar auteursrechten. Scientia kan onvoldoende onderbouwen waarom het gebruiken van de bij een afnemer opgedane kennis over de tabellen auteursrechtinbreuk oplevert. De stelling van Eveoh dat de databases niet auteursrechtelijk zijn beschermd en als dat al zo zou zijn, zij een beroep kunnen doen op artikel 45m uit de Auteurswet kan Scientia ook niet direct weerleggen. De vordering van Scientia wordt afgewezen.

https://bit.ly/374u1st

Apollo maakt inbreuk op auteursrecht softwareontwikkelaar Jelurida
(Rechtbank Amsterdam, 22 september 2020)
De rechtbank Amsterdam oordeelt dat Apollo Fintech inbreuk maakt op het auteursrecht van softwareontwikkelaar Jelurida (ontwikkelaar van Nxt Software) door een cryptomunt aan te bieden die is gebaseerd op de Nxt software, omdat een deel van de broncode is gekopieerd. Jelurida stelt de software enkel beschikbaar onder voorwaarden. Apollo heeft deze voorwaarden niet in acht genomen door de software zonder inachtneming van de licentie van Jerurida te verstrekken. Apollo wordt bevolen een brief te sturen

naar haar zakelijke afnemers waarin zij hen verzoekt om de Apollo Software opnieuw te installeren, waarbij zij de voorwaarden van Jerudia actief moeten accepteren.

https://bit.ly/36ZGoWE

Microsoft blokkeert (voorlopig) terecht toegang tot OneDrive
(Rechtbank Midden-Nederland, 8 oktober 2020)
Kort geding. Eiser wordt op verdenking van het bezit van kinderpornografie door Microsoft de toegang ontzegd tot zijn OneDrive-account. Microsoft geeft in eerste instantie niet prijs waarom de toegang is geblokkeerd, maar tijdens het kort geding wordt duidelijk dat hij met een opgeslagen foto in zijn OneDrive de servicevoorwaarden van Microsoft zou hebben geschonden. Microsoft mag de bestanden uit de drive niet verwijderen; in de bodemprocedure moet worden beslist of de man weer toegang krijgt tot zijn OneDrive.

https://bit.ly/2VSQNNv

Stichting Viruswaarheid vs. Facebook
(Rechtbank Amsterdam, 13 oktober 2020)
Stichting Smart Exit (belangenbehartiger van onder andere horeca in coronatijd) en Stichting Viruswaarheid (strijdend voor een democratische rechtstaat in coronatijd) starten een rechtszaak tegen Facebook die hun Facebookpagina's 'Nee tegen 1,5 meter' en 'Viruswaanzin' heeft verwijderd. Facebook zou hiermee inbreuk maken op de vrijheid van meningsuiting, vereniging en betoging van de eisers. Vanwege de horizontale werking van vrijheid van meningsuiting gaat die vlieger niet meteen op en daarnaast heeft Facebook een maatschappelijke plicht om zich te houden aan overheidsrichtlijnen. Het debat over wat wel en niet passend is in coronatijd is nog gaande.

https://bit.ly/3gtNWUt

Duurovereenkomst mag niet zomaar worden beëindigd
(Rechtbank Amsterdam, 26 oktober 2018)
Kort geding. NPS levert software en diensten op het gebied van outsourcing en heeft een Value Added Reseller overeenkomst gesloten met gedaagde: ontwikkelaar en leverancier van software. Gedaagde zegt de overeenkomst, na onduidelijkheden over en weer, met NPS op. NPS stelt dat dit onrechtmatig is en stelt dat voor het opzeggen van een duurovereenkomst een zwaarwegende grond nodig is. De rechter oordeelt dat gedaagde te snel heeft opgezegd, mede vanwege de tussentijdse rechtsovergang die heeft plaatsgevonden bij NPS. Daarbij oordeelt de rechtbank dat de gevolgen van de fouten van de rechtsvoorganger van NPS niet bij NPS kunnen worden neergelegd.

https://bit.ly/37TR0FQ

Celstraf en tbs voor bedreiger prinses Amalia
(Rechtbank Overijssel, 3 november 2020)
Een 32-jarige oud-militair is dinsdag veroordeeld voor het bedreigen van prinses Amalia. De man bedreigde prinses Amalia en een vriend van haar via Instagram. Hij dreigde onder meer seksuele handelingen te plegen en over te gaan tot (dodelijk) geweld. De verklaring van verdachte dat hij niet wist dat hij de berichten naar het echte account van Amalia stuurde, acht de rechtbank ongeloofwaardig. De verdachte verklaart immers dat hij op het internet gezocht heeft naar het echte account van Amalia. De rechtbank is van oordeel dat verdachte een ongezonde obsessie heeft voor het Koningshuis en in het bijzonder voor prinses Amalia. De rechtbank vindt dit zorgelijk, kwalijk en onacceptabel en veroordeelt de 32-jarige tot een gevangenisstraf van drie maanden en tbs met dwangverpleging van maximaal vier jaar.

https://bit.ly/3qFiqaQ

Rectificatie dekenstandpunt
(Raad van State, 4 november 2020)
Als reactie op een tuchtklacht uit 2017 heeft de deken een zogenoemd dekenstandpunt uitgebracht. Appellant heeft op grond van artikel 16 AVG verzocht om rectificatie van het dekenstandpunt, omdat volgens hem het volgende daarin ontbreekt: "op vervolging aangiftes "2009" was reeds in raadkamer Rechtbank-Breda 13 januari 2010 ter verdediging aangevoerd "advocaat met fiscaal adviseur des cliënte"; in diens cassatieschriftuur door [advocaat] domweg weggelaten, hetgeen in executiegeding [advocaat] deed schorsen als raadsman." Dit verzoek van appellant is door de deken afgewezen. "Advocaat met fiscaal adviseur des cliënte" betreft volgens de deken geen persoonsgegeven, waardoor hij op grond van artikel 16 van de AVG niet kan rectificeren. De rechtbank oordeelde dat de deken het verzoek om rectificatie terecht heeft afgewezen, maar dat dit op onjuiste gronden is gedaan. De Raad van State verklaart het hoger beroep van appellant niet-ontvankelijk, verklaart het hoger beroep van de deken gegrond en vernietigt de uitspraak van de rechtbank.

https://bit.ly/2VVSBoP

Eisers tegen GOOGLE LLC
(Rechtbank Noord-Nederland, 5 november 2020)
Eisers (ondernemers die actief zijn (geweest) op de vastgoedmarkt in Groningen) verzoeken de rechter om verwijdering van URL's die verwijzen naar web- en bronpagina's. Als in de zoekmachine van Google gezocht wordt naar de namen van eisers, worden zoekresultaten zichtbaar die verwijzingen bevatten naar publicaties op web- of bronpagina's betreffende onder meer artikelen op de website www.sikkom.nl en www.wikipedia.org en verwijzingen naar een aflevering van het programma "Foute Boel" op SBS en een aflevering van het programma #BOOS op BNNVARA. Eén van de eisers is namelijk samen met 'Spot In' op 2 maart 2018 door ROOD (jongerenorganisatie van de SP) verkozen tot "Huisjesmelker van het Jaar 2018". Eisers hebben beiden via een advocaat met behulp van een online formulier van Google verzocht om URL's te verwijderen van de zoekresultatenpagina die getoond worden bij een zoekopdracht op de namen van eisers. Google heeft deze verzoeken afgewezen. De rechtbank is van oordeel dat niet is gebleken dat de publicaties waarnaar de zoekresultaten verwijzen, vol onjuistheden staan. Daarnaast oordeelt de rechtbank dat berichtgeving door Sikkom, BNNVARA en SBS een waarschuwingsfunctie heeft en deze berichtgeving deel uitmaakt van een (lokaal) maatschappelijk debat over onder meer de huursector en dat eisers publieke figuren zijn op de Groningse vastgoedmarkt. Volgens de rechtbank dienen eisers om deze reden te dulden dat hun handelen in de media ter discussie kan worden gesteld. Volgens de rechtbank is daarnaast door eisers niet voldoende gemotiveerd waarom de URL's onvindbaar gemaakt of verwijderd moeten worden. Ook is volgens de rechter onvoldoende uiteengezet waarom het belang van eisers bij verwijdering zou prevaleren boven het economisch belang van de exploitant van de zoekmachine en het gerechtvaardigde belang van de internetgebruikers. De verzoeken tot verwijdering van de URL's worden door de rechtbank afgewezen.

https://bit.ly/3gtSpXf

Orange România tegen de Roemeense gegevensbeschermingsautoriteit
(Arrest van het Hof (Tweede kamer), 11 november 2020)
Orange România is een aanbieder van mobiele telecommunicatiediensten op de Roemeense markt. Aangezien de activiteit van de vennootschap de verwerking van persoonsgegevens omvat, is Orange România ingeschreven in het Register inzake de verwerking van persoonsgegevens van de nationale autoriteit voor het toezicht op de verwerking van persoonsgegevens (de ANSPDCP). Op 28 maart 2018 heeft de ANSPDCP aan Orange România een boete opgelegd voor het verzamelen en opslaan van kopieën van identiteitsdocumenten van haar klanten zonder dat zij hiervoor uitdrukkelijke toestemming hadden gegeven. Het Tribunalul București (de rechter in eerste aanleg, Boekarest, Roemenië) heeft het Hof van Justitie verzocht om de voorwaarden te specificeren waaronder de toestemming van de klanten voor de verwerking van persoonsgegevens als geldig kan worden beschouwd. Het Hof concludeert dat het contract voor het leveren van een telecommunicatiedienst die een clausule bevat waarin staat dat de klant heeft ingestemd met het verzamelen en opslaan van zijn identiteitsbewijs, niet kan aantonen dat deze klant op geldige wijze toestemming heeft gegeven als het vakje met betrekking tot deze clausule door de verwerkingsverantwoordelijke is aangevinkt voordat het contract werd ondertekend. De toestemming moet volgens het Hof vrij gegeven, ondubbelzinnig, geïnformeerd en specifiek zijn. Indien deze toestemming in een schriftelijke verklaring wordt gegeven die ook betrekking heeft op andere zaken, moet deze verklaring in een begrijpelijke en gemakkelijk toegankelijke vorm en in een heldere en duidelijke taal worden omschreven.

https://bit.ly/2VVUh1B

Appellante tegen minister van Onderwijs, Cultuur en Wetenschap
(Raad van State, 18 november 2020)
In verband met een geschil op de voormalige school van de minderjarige zoon van appellante, verzocht zij de minister van Onderwijs, Cultuur en Wetenschap om inzage in het dossier van haar zoon. Dit verzoek is door de minister gedeeltelijk toegewezen. Tegen deze gedeeltelijke toewijzing is appellante in bezwaar gegaan. Dit bezwaar is door de minister ongegrond verklaard. Vervolgens heeft de Afdeling bestuursrechtspraak van de Raad van State op 5 februari 2020 geoordeeld dat de minister ten onrechte geen inzage heeft gegeven in de persoonlijke beleidsopvattingen van ambtenaren. Dit heeft ertoe geleidt dat de minister op grond van artikel 15 lid 1 en lid 3 AVG onder weglakking van persoonsgegevens van derden alsnog inzage heeft gegeven in het dossier. Appellante is opnieuw in beroep gegaan bij de Afdeling bestuursrechtspraak van de Raad van State en betoogt dat de minister onvoldoende gevolg heeft gegeven aan de uitspraak van de Afdeling van 5 februari 2020. Appellante stelt dat er meer notities zouden moeten zijn dan de minister heeft overgelegd en dat de minister in de overgelegde stukken meer weggelakt heeft dan alleen persoonsgegevens.
De Afdeling is van oordeel dat het betoog van appellante dat de minister niet alle persoonsgegevens heeft verstrekt, faalt. Volgens de Afdeling heeft appellante niet aannemelijk gemaakt dat de minister niet alle stukken heeft

verstrekt en had zij dit eerder in de procedure kunnen aanvoeren. Over het standpunt van appellante dat de minister onterecht passages heeft weggelakt, zegt de Afdeling dat het gaat om persoonsgegevens van derden en dat appellante gelet op artikel 15 lid 1 AVG hier geen recht op heeft. Op grond van artikel 4, aanhef en onder 1, van de AVG valt hieronder ook informatie waarmee een derde direct of indirect kan worden geïdentificeerd. Om deze reden is de Afdeling van oordeel dat de minister deze passages terecht heeft weggelakt. De Afdeling verklaart het beroep ongegrond.

https://bit.ly/39Vspmo

VoeltbalTV hoeft boete Autoriteit Persoonsgegevens niet te betalen
(Rechtbank Midden-Nederland, 23 november 2020)
VoetbalTV is een (inmiddels failliet) videoplatform voor het amateurvoetbal. Op het platform kan men amateurvoetbalwedstrijden terugkijken, wedstrijden analyseren, gegevens verzamelen en deze delen met anderen. De Autoriteit Persoonsgegevens (AP) is een onderzoek gestart naar de mogelijke inbreuk op de privacy van (minderjarige) spelers en toeschouwers die te zien zijn op het platform. De AP concludeerde dat VoetbalTV voor het maken van opnames en het uitzenden van voetbalwedstrijden op grond van artikel 6, eerste lid, van de AVG geen geldige grondslag heeft en dus de persoonsgegevens onrechtmatig verwerkte. Na het door VoetbalTV ingestelde beroep niet tijdig beslissen, heeft de AP aan VoetbalTV een boete opgelegd van € 575.000. VoetbalTV is van mening dat het opnemen en uitzenden van de wedstrijden valt onder de journalistieke exceptie en dat zij een gerechtvaardigd belang heeft om persoonsgegevens te verwerken. De rechtbank oordeelt dat de journalistieke exceptie niet opgaat. De beelden hebben volgens de rechtbank te weinig nieuwswaarde, omdat het gaat om het uitzenden van amateursport en- spel. Daarnaast is de rechtbank van oordeel dat de AP uitgaat van een verkeerde interpretatie van het gerechtvaardigd belang. De AP heeft volgens de rechter bij het onderzoek niet gelet op de noodzakelijkheid, proportionaliteit en subsidiariteit en evenmin een belangenafweging gedaan. Volgens de AP had VoetbalTV een zuiver commercieel belang bij de exploitatie van het platform. Dit commerciële belang kan volgens de AP niet worden aangemerkt als gerechtvaardigd belang. De AP heeft vastgesteld dat er geen sprake is van een gerechtvaardigd belang en heeft vervolgens de verwerking van de persoonsgegevens niet volledig onderzocht. Het HvJ heeft herhaaldelijk bevestigd dat het lidstaten niet vrijstaat om een beroep op het gerechtvaardigd belang op voorhand uit te sluiten. De rechtbank komt tot de conclusie dat het besluit van de AP niet voldoende zorgvuldig is genomen en vernietigt het boetebesluit van de AP. Hierdoor hoeft VoetbalTV de boete niet te betalen. Zie ook het artikel op pagina 14.

https://bit.ly/37J324C

Sten Demon
Manager ICTRecht
Detachering

Innovatie

Legal tech voor iedereen?

“Legal tech, dat is toch iets met smart contracts en blockchain?” Klopt, maar het is ook veel meer dan dat. Er zijn inmiddels veel verschillende legal tech oplossingen waarmee vrijwel iedere jurist of ondernemer zijn voordeel kan doen. Of het nu gaat om efficiënter werken of juist om het verbeteren van de kwaliteit en continuïteit van juridische bedrijfsprocessen, legal tech kan erbij helpen. Hoe dan? Dat leest u hier!

In vrijwel iedere sector zorgen nieuwe technologieën voor talloze voordelen. Hetzelfde geldt voor de juridische sector. Velen hebben een mening over wat het begrip ‘legal tech’ nu precies betekent, maar voorlopig wordt het in de praktijk gebruikt als een containerbegrip voor alle technologie en software waarmee juridische processen verbeterd kunnen worden. Het is belangrijk om te begrijpen dat legal tech niet alleen is bedoeld voor advocaten of grote ondernemingen. Ook startups kunnen er veel voordeel uit halen, helemaal nu vrijwel iedereen vanuit huis werkt.

Maar waar moeten we dan aan denken? Hieronder leest u hoe legal tech kan ondersteunen bij een proces waar iedere onderneming mee te maken heeft, namelijk: contracteren.

Opzoek naar die ene bepaling in die oude overeenkomst?
Het kopje van deze paragraaf is vast herkenbaar. In plaats van het opstellen van een nieuwe overeenkomst of bepaling, gaat u opzoek naar een voorbeeld van jaren terug. In de tijd die het u kost om te achterhalen waar u het voorbeeld ook alweer had opgeslagen, had u makkelijk de nieuwe overeenkomst of bepaling kunnen opstellen. Dit probleem komt niet alleen voor bij juristen, maar bijvoorbeeld ook bij medewerkers van HR- en Salesafdelingen die regelmatig met overeenkomsten werken.

Met de juiste legal tech kunt u contracteren standaardiseren. Met software als JuriBlox kunnen de laatste templates en contractsbepalingen teruggevonden worden in één systeem. Dit levert uiteraard tijdswinst op en voorkomt fouten zoals oude klantnamen die nog ergens rondslingeren in het document. Tevens helpt het gebruik van legal tech bij het waarborgen van continuïteit. Bijvoorbeeld wanneer tijdelijke vervanging nodig is gedurende een zwangerschapsverlof. Een collega of tijdelijke inhuurkracht heeft dan direct alle informatie binnen handbereik en zo hoeven processen niet stil te liggen.

Hoe vaak heeft u die overeenkomst al gecontroleerd?
Niet alleen juristen, maar ook veel ondernemers zien dagelijks standaardcontracten langskomen. Denk in dit kader bijvoorbeeld aan geheimhoudingsovereenkomsten (NDA’s) en verwerkersovereenkomsten.
De inhoud van dit soort overeenkomsten zijn zeker niet uniek. De meeste geheimhoudingsovereenkomsten kennen dezelfde opzet en dezelfde afspraken. Toch neemt u elke keer de hele overeenkomst door om eventuele grote risico’s te mitigeren. Zou het niet ideaal zijn als zo’n controle geautomatiseerd kan worden?

Dit is precies waar bepaalde legal tech ondernemingen, zoals NDA Lynn, zich nu mee bezig houden. Door middel van machine learning is software goed in staat om standaardovereenkomsten te controleren. Zo hoeft u geen aandacht te besteden aan alle standaardbepalingen, maar kunt u focussen op de afwijkende afspraken die daadwerkelijk risico’s kunnen opleveren. Conclusies die dit soort *review-bots* opleveren, kunt u zelfs gebruiken om te beslissen of de betreffende overeenkomst afgehandeld moet worden door een ervaren of startende medewerker.

Klaar met term sheets en documenten vergelijken?
Zodra u een overeenkomst heeft opgesteld of gecontroleerd, is de volgende stap meestal het onderhandelen. Zelfs wanneer de commerciële aspecten van een overeenkomst al helemaal zijn afgerond, moet er regelmatig nog onderhandeld worden over de juridische aspecten van de overeenkomst. Dit spelletje zal niet zomaar veranderen. Gelukkig kan het wel efficiënter dan het bijhouden van alle wijzigingen in Microsoft

Word, waarna u alsnog een complete document-vergelijking uitvoert omdat u de jurist van de wederpartij niet vertrouwt. Met software voor online onderhandelen ontstaat er nooit meer twijfel over welke versie nu de laatste is en of de wederpartij alle wijzigingen wel goed heeft bijgehouden. Daarnaast kunt u real-time onderhandelen over iedere bepaling zonder dat u de complete review en e-mail van de wederpartij hoeft af te wachten.

Hoe regelt u die handtekening nu vrijwel iedereen thuiswerkt?
Wanneer de onderhandelingen zijn afgerond, kan de overeenkomst ondertekend worden. In deze tijd voelt het behoorlijk knullig als je de CEO moet vragen om thuis de overeenkomst te printen, deze te ondertekenen, vervolgens te scannen en deze weer terug te sturen. Dit kan natuurlijk makkelijker door gebruik te maken van oplossingen voor digitaal onderteken, zoals Signhost.

U kunt nog meer voordeel halen uit oplossingen voor digitaal onderteken, wanneer je deze koppelt aan een contractmanagementsysteem. Zo kunt u de getekende overeenkomst altijd terugvinden en kunt u grip houden op bijvoorbeeld de looptijd van de overeenkomst.

Waar te starten?
Zoals aangegeven zijn er veel oplossingen om uit te kiezen. Maar waar kunt u het beste starten? Het laatste wat u wilt, is medewerkers die klagen over een gekozen oplossing, waardoor deze vervolgens nooit gebruikt wordt. Wilt u weten welke processen u kunt verbeteren of welke legal tech het beste bij uw organisatie past? ICTRecht helpt u graag met de volgende werkzaamheden:

- Het inventariseren van de wensen en het analyseren van de huidige processen binnen uw onderneming of afdeling. Op basis van onze inventarisatie en analyse kunnen wij adviseren over welke legal tech oplossingen het beste bij u past.
- Indien gewenst helpen wij ook bij het implementeren van de gekozen oplossingen, het managen van de nodige veranderingen en het creëren van draagvlak binnen de organisatie of afdeling. Weerstand vanuit de medewerkers kan voorkomen worden door niet te veel veranderingen en oplossingen tegelijkertijd te introduceren en medewerkers te betrekken bij de verschillende stappen in het proces.
- Bovendien kunnen wij u én uw collega's trainen in het gebruik van de gekozen legal tech oplossing.

ICTRecht
Werving & Selectie

ICTRECHT
werving & selectie

De perfecte match tussen uw organisatie en onze kandidaten

Als organisatie op zoek naar juridisch talent?

ICTRecht Werving & Selectie fungeert als intermediair tussen het bedrijfsleven en werkzoekenden. Wij matchen juristen op het gebied van privacy, ICT en security aan de juiste organisaties.

Werving & Selectie via ICTRecht betekent:

1. **Meer efficiëntie**: direct in contact met een geschikte kandidaat.
2. **Vakkundige kandidaten**: getest op juridische inhoud en vaardigheden.
3. **Deskundigheid voorop**: met onze ervaring in de juridische branche is uw kandidaat snel gevonden.

Meer weten? Neem contact met ons op of bezoek onze website: **ictrecht.nl/werving**

Fleur Biegstraaten
f.biegstraaten@ictrecht.nl

Ardine Siepman
a.siepman@ictrecht.nl

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Noot bij ECLI:NL: RBAMS:2020:4435[1]

Hoever mag YouTube gaan in zijn strijd tegen misinformatie over corona? En staat het verwijderen van video's die niet aan de huisregels voldoen een open maatschappelijk debat over het coronabeleid van de overheid en het RIVM in de weg? Interviewer Ab Gietelink en huisarts Rob Elens hebben een kort geding tegen YouTube aangespannen omdat de videoreus video's van de twee had verwijderd omdat ze in strijd zijn met de huisregels omtrent coronamisinformatie. De video's prijzen het niet-werkende hydroxychloroquine aan als COVID-19-medicijn.

De term censuur valt veel in dat verband. Formeel kan dat niet. De term censuur betekent in het juridisch jargon dat de overheid voorafgaand toezicht uitoefent op uitingen, oftewel je mag pas iets publiceren na goedkeuring. Ingrijpen achteraf (bijvoorbeeld strafrechtelijk vervolgen voor smaad) is dus geen censuur.

Een private partij kan in die definitie geen censuur plegen, om de simpele regel dat ze geen overheid is. En dat is ook wel logisch: hoezo kan een private partij eisen dat ik mijn uitingen voorafgaand aan hem voorleg? Ja, als we dat zo afgesproken hebben – denk aan werkgevers of opdrachtgevers die zoiets eisen. Maar als je dat zelf afspreekt, dan is het wat raar om vervolgens te klagen dat je privaat gecensureerd wordt.

Bij partijen als YouTube wreekt zich het feit dat zij wel private partijen zijn, maar zo machtig dat ze eigenlijk als een soort van overheid te zien zijn. Je kunt nauwelijks om ze heen. Ja, in theorie heb je andere sites, maar noem er eens twee waar jij regelmatig kijkt? Dailymotion, inderdaad. Op Vimeo staan ook films, maar hoe vaak kijkt men daar nou echt?

Ik begrijp dus wel dat mensen zeggen dat het voelt als censuur, zo'n grote partij die eigenlijk overkomt als overheid en die dan zegt "deze onderwerpen mag je niet meer bespreken". Ik ben ooit afgestudeerd op de stelling dat als een partij zó groot is dat er effectief geen alternatieve platforms zijn (zeg maar, het marktplein versus het industrieterrein als enige twee opties voor demonstraties) dat die grote partij dan onder dezelfde regels als de overheid moet vallen. Zoals het EHRM dat formuleerde:

> "Where, however, the bar on access to property has the effect of preventing any effective exercise of freedom of expression or it can be said that the essence of the right has been destroyed, the Court would not exclude that a positive obligation could arise for the State to protect the enjoyment of the Convention rights by regulating property rights."

Dat zou betekenen dat deze partij geen inhoudelijk beleid meer mag voeren over wat zij toelaat. Ik twijfel of YouTube zó groot is – het gaat niet per se om het publiceren van een video, en er zijn ook grote platforms zoals Facebook of Instagram waar je terecht kunt om een minstens zo grote doelgroep te bereiken.

YouTube had eerder dat jaar regels aangenomen die stelden dat er geen content geplaatst mag worden die tegen de voorschriften van de WHO of lokale gezondheidsinstanties (zoals ons RIVM) in mag gaan. Een van die regels stelt specifiek dat je niet mag claimen dat er een bewezen geneesmiddel is. De video's van deze interviews werden verwijderd onder een standaardmededeling, kennelijk vanwege overtreding van die regel.

1. https://bit.ly/36ZeJVF

De kortgedingrechter oordeelt dat YouTube, als een van de belangrijkste online videoplatforms ter wereld, niet zomaar mag besluiten om "wel de content die overeenstemt met de visie van de WHO en het RIVM toe te laten en niet andersluidende, kritische content. Daarmee zou de YouTube gebruiker die brede content mag verwachten, slechts kennis kunnen nemen van de mening van de groep experts die de WHO en het RIVM adviseren, terwijl de wijze van bestrijding en behandeling van COVID-19 wereldwijd nog volop in onderzoek is en nog allerminst vaststaat".

Dit mede omdat "ook de WHO en het RIVM hun adviezen nog steeds [bijstellen]". Dat is een wat ergerlijke samenvatting van wetenschappelijk onderzoek – helemaal omdat de rechter ook spreekt van "de visie van de WHO". Wetenschap is geen mening. Maar goed, we hadden dus haast. En uiteindelijk ging het niet over of je kritiek op de WHO of het RIVM mocht hebben maar of je in strijd met hun wetenschappelijke bevindingen mag vinden dat iets wél werkt.

De vervolgvraag is dan ook of de specifieke video's van de interviews weggehaald hadden mogen worden, als je net hebt gezegd dat in brede zin ook andersluidende, kritische meningen geuit mogen worden. YouTube wijst daartoe op onder meer de Europese afspraken tegen desinformatie en op het feit dat deze video's onjuiste, schadelijke en gevaarlijke informatie bevatten.

De rechtbank besluit uiteindelijk dat de video's weg moeten omdat de informatie wordt gegeven door een (huis-)arts en niet slechts een mening is maar pretendeert een feit te zijn:

> "Een arts die zonder sluitend bewijs en wetenschappelijk onderbouwde tests claimt dat HCQ of een alternatief middel – dat zonder recept te verkrijgen is – werkt, licht het publiek onjuist voor. Daarnaast kan het schadelijk en gevaarlijk zijn. (…) Zoals het in de interviews door hem is verwoord, vormt het geen onderdeel van het debat, hetgeen YouTube wel zou hebben toegelaten, maar bevatten zijn uitlatingen onjuiste informatie die mogelijk schadelijk en gevaarlijk is. Juist als arts dient hij zich dit te realiseren."

De uitkomst is dus dat YouTube wel degelijk de video's weg mocht halen, zij het om een andere reden dan in hun beleid stond.

In een vergelijkbare zaak (ECLI:NL:RBAMS:2020:4966[2]) bevestigt de kortgedingrechter dat Facebook ook berichten mag verwijderen als dat in strijd is met hun huisregels. In die zaak wijst de rechter er fijntjes op dat het hierboven aangehaalde arrest geen verbodsregels voor platforms met zich meebrengt, maar alleen een mogelijke plicht voor de Staat om nadere regels te maken wanneer blijkt dat plaforms zoals YouTube en Facebook het maatschappelijk debat al te zeer smoren door hun machtspositie.

Indirect heeft de vrijheid van meningsuiting wel effect op relaties tussen burgers onderling. In juridische taal, deze werkt door in bijvoorbeeld de redelijkheid en billijkheid of de maatschappelijke betamelijkheid. Ook dan is het geen automatisme dat je dus alles moet mogen zeggen, een toetsing blijft vereist. En in dit geval valt die uit in het voordeel van Facebook:

> "In het licht hiervan wordt wel het volgende overwogen. Facebook handelt door haar COVID-19 beleid te hanteren voorshands niet in algemene zin in strijd met hetgeen – naar huidige opvattingen – maatschappelijk betamelijk is. Zij heeft een maatschappelijke plicht om zich te houden aan overheidsrichtlijnen, tenzij die evident onjuist zijn. Dat is voorshands niet het geval. Het wetenschappelijk en maatschappelijk debat over COVID-19 en wat passende en doeltreffende maatregelen zijn, is nog gaande."

En dan gaat de rechtbank nog een stapje verder. Want Facebook volgt de Europese aanbevelingen van de overheid, en die aanbevelingen moet je dan juist zien als een (softe) regulering van het spanningsveld tussen de uitingsvrijheid, de volksgezondheid en de belangen van Facebook en haar gebruikers. Daarmee doet Facebook dus eigenlijk al precies wat ze moet doen.

En wat is nu het verschil met YouTube? Daar werd vooral gezegd dat in het algemeen kritische uitingen op overheidsbeleid en wetenschappelijke bevindingen niet zomaar tegengehouden mag worden, maar wel gevaarlijke uitingen afkomstig van een huisarts: die nemen mensen eerder serieus. Dus dat voelt als een specifieker geval dan deze uitspraak.

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

Van onze blog

Privacy

4 november 2020

Mag een werkgever locatiegegevens en urenstaten van een werknemer controleren?

Op 14 september 2020 heeft gerechtshof 's-Hertogenbosch uitspraak gedaan in een ontslagzaak waarin privacy een belangrijke rol speelde. Een interessante zaak, omdat deze laat zien hoe het Hof omgaat met privacy in de werkgever-werknemers sfeer. Mag de werkgever de locatiegegevens en urenstaten controleren om ontslag rond te krijgen?

Aan het werk op de woonboulevard?
Wat was er aan de hand? De werknemer werkte als servicetechnicus. Als servicetechnicus was hij verantwoordelijk voor het onderhouden, storingsvrij houden en aanpassen van sprinklerinstallaties. Wekelijks moest de werknemer het aantal gewerkte uren invullen op een urenoverzicht. De uren worden bijgehouden in de 'Nemo-app'. De servicetechnicus moet op start drukken als hij begint met werken bij de klant. Bij voltooiing dient de klant een handtekening te zetten. De app registreert dan de gewerkte tijd. Daarnaast zit er in elke bedrijfsbus een zogeheten black box met een GPS-tracker. Hiermee kan de locatie van de werknemer worden bijgehouden. In geval van een storing bij een opdrachtgever kan de afdeling planning de locatiegegevens gebruiken om de dichtstbijzijnde servicetechnicus naar de storing te sturen.

De werkgever ontdekte dat er een verschil was tussen de werktijden van de Nemo-app en de gegevens afkomstig van de GPS-tracker uit de bedrijfsbus. Zo was de werknemer onder werktijd te vinden op plaatsen waar geen klanten zijn gevestigd. Bijvoorbeeld op de woonboulevard.

Informeren: werknemer wist van de black box
Als je als werkgever de locatiegegevens registreert van de bedrijfsbus van een werknemer, dan verzamel je persoonsgegevens. En wanneer je persoonsgegevens verzamelt, moet je hierover volgens artikel 13 van de AVG informeren. Hoe je aan deze wettelijke verplichting voldoet is vormvrij. Dit kun je bijvoorbeeld doen via een interne privacyverklaring.[1] Maar ook via een personeelshandboek, arbeidsvoorwaardenreglement of intern privacybeleid.

In dit geval maakte de werkgever gebruik van een privacybeleid, waar de werknemer van op de hoogte is gesteld. Het protocol volgsystemen waarin het gebruik van de black box is geregeld maakt weer onderdeel uit van het privacybeleid. Daarnaast heeft de werknemer bij ingebruikname van de bedrijfsbus, de autoregeling ondertekend. In artikel 6.4 van deze autoregeling staat:

"6.4 GPS-systemen - In veel gevallen is de bedrijfsauto voorzien van een GPS-systeem (black box). Teneinde een evenwichtig beleid te voeren met betrekking tot het gebruik van de GPS-systemen, waarbij zowel een verantwoord gebruik van de GPS-systemen wordt nagestreefd, alsmede de privacy van personeelslid wordt beschermd heeft werkgever een protocol met betrekking tot het gebruik van GPS-systemen opgesteld. Ieder personeelslid is gehouden zich te gedragen conform dit protocol. Dit protocol maakt onlosmakelijk onderdeel uit van deze autoregeling en wordt bij bestelling van de bedrijfsauto aan personeelslid ter hand gesteld. Het protocol is tevens na te lezen op het intranet."

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

Het Hof overwoog dat de werknemer bekend moet worden verondersteld met het bestaan van de inhoud van het protocol volgsystemen. De overweging van het Hof laat zien dat het belangrijk is om werknemers op de hoogte te stellen van de persoonsgegevens die van hen worden verwerkt.

Of het Hof het gebruik van de locatiegegevens als onrechtmatig had bestempeld als de werkgever de werknemer niet had geïnformeerd is lastig te zeggen. Maar dat het invloed kan hebben op de rechtmatigheid, dat staat als een paal boven water. Het verwerken van persoonsgegevens mag niet uit de lucht komen vallen. Zorg er daarom als werkgever voor dat je op de juiste wijze de werknemers informeert.

Proportionaliteit

Een andere belangrijke overweging van het Hof ziet op de gefaseerde uitvoering van het onderzoek naar de locatiegegevens afkomstig van de black box en de urenstaat. In eerste instantie heeft de werkgever alleen de locatiegegevens en de urenstaat van week 9 onderzocht, in verband met de onregelmatigheden die waren aangetroffen in een werkbon van dezelfde week. Toen uit dat onderzoek bleek dat de uren op de urenstaat niet overeenkwamen met de locatiegegevens van de black box, heeft Trigion het onderzoek uitgebreid naar de periode vanaf 1 januari 2019. Pas toen ook uit dat onderzoek bleek dat de werknemer stelselmatig meer uren schreef dan hij werkte, is de werkgever, om er zeker van te zijn dat het ging om bestendig gedrag, in haar onderzoek teruggegaan tot april 2017.

De overwegingen van het Hof laten zien dat waarde kan worden gehecht aan proportionaliteit. Oftewel, gaat de inbreuk op de privacy van de werknemer niet verder dan noodzakelijk en kan het niet een onsje minder. In dit geval wilde de werkgever uitsluiten dat het ging om incidenten. Een gefaseerde uitvoering van het onderzoek zorgt ervoor dat rekening is gehouden met proportionaliteit.

2. https://bit.ly/2LfldHr
3. https://bit.ly/2VSdVM5
4. https://bit.ly/3qJw1y6

Controle locatiegegevens in combinatie met urenstaten in lijn met AVG

Het Hof oordeelt uiteindelijk dat de inbreuk op privacy niet zodanig is geschonden dat dit onrechtmatig is geweest. Wat in de uitspraak niet naar voren komt, is of de werkgever een Data Protection Impact Assessment (DPIA)[2] heeft (laten) uitvoeren, en welke grondslag is gebruikt voor de gegevensverwerking.

Een DPIA is onder andere verplicht bij grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens om activiteiten van werknemers te monitoren. Een DPIA is ook verplicht bij een grootschalige verwerkingen en/of stelselmatige monitoring van locatiegegevens. Een DPIA was hier op zijn plaats geweest. Een DPIA is een uitstekend middel om de risico's van een gegevensverwerking in kaart te brengen, en maatregelen aan te dragen om de risico's zoveel mogelijk weg te nemen. In een DPIA kan bijvoorbeeld worden bekeken welke grondslag voor de gegevensverwerking in aanmerking komt. Komt de grondslag gerechtvaardigd belang[3] in beeld? Dan kan in de DPIA een gedegen afweging plaatsvinden. Maar denk bijvoorbeeld ook aan onderwerpen als bewaartermijnen en beveiligingsmaatregelen die in een DPIA kunnen worden belicht.

Onrechtmatig bewijs weegt mee

Het Hof overwoog ook nog dat onrechtmatig verkregen bewijs 'in beginsel' meeweegt in de ontslagzaak. Het algemene maatschappelijk belang dat de waarheid aan het licht komt, weegt in principe zwaarder dan het belang van uitsluiting van bewijs. Slechts indien sprake is van bijkomende omstandigheden, kan bewijs worden uitgesloten. Hoewel dit staande rechtspraak is van de Hoge Raad[4], is het goed om deze overweging ook in deze zaak terug te zien. Het gevaar ligt op de loer dat werkgevers de afweging gaan maken om een onrechtmatige inbreuk op de privacy van werknemers te maken, omdat dit ertoe kan bijdragen dat een werkgever een ontslag bij de rechter rond kan krijgen. Een boete van de Autoriteit Persoonsgegevens of een bijkomende immateriële schadevergoeding voor de werknemer wegens een inbreuk op de privacy zal dit mogelijke gevaar recht moeten trekken.

Auteur
Jay Remmelzwaal
Juridisch adviseur

17 november 2020

Kansspelautoriteit deelt terecht last onder dwangsom uit voor verboden 'lootboxes' in FIFA-game

De Nederlandse Kansspelautoriteit heeft terecht een last onder dwangsom opgelegd aan de bekende gameontwikkelaars Electronic Arts Inc. en Electronic Arts Swiss Sàrl voor het spel FIFA. Zo heeft de rechtbank in Den Haag recentelijk bepaald. In 2019 legde de Kansspelautoriteit de last onder dwangsom op aan de makers van het populaire voetbalspel omdat het spel verboden 'lootboxes' bevat. In een rechtszaak tussen partijen werd de Kansspelautoriteit door de rechter in haar gelijk gesteld.[1]

Illegaal kansspel

De lootboxes in FIFA, de 'Packages', zijn in strijd met de wet omdat zij aangemerkt kunnen worden als illegaal kansspel. Spelers hebben geen invloed op de inhoud van de lootbox en het is een verrassing wat de inhoud en waarde van de lootbox is. In de lootboxes van FIFA zitten bijvoorbeeld voetbalspelers die het elftal waarmee het spel wordt gespeeld, beter kunnen maken. De inhoud kan een hoge waarde hebben en deze is door spelers te verhandelen. Hierdoor is er sprake van een overtreding van de Wet op de kansspelen. Volgens de Nederlandse wet mag een kansspel waarmee een prijs of premie te winnen is, alleen worden aangeboden als daar een vergunning voor is verleend.

Ondertussen houdt de Kansspelautoriteit zich alweer een aantal jaar bezig met lootboxes in games. Een paar jaar geleden schreven we er ook al over[2]: de Kansspelautoriteit begon in 2018 met het controleren van verboden lootboxes in games. In een eerder onderzoek had zij al vastgesteld dat dergelijke lootboxes in sommige games in strijd zijn met de Wet op de Kansspelen (Wok). Na haar eerdere onderzoek had de Kansspelautoriteit al contact opgenomen met de gameontwikkelaars die de verboden kansspelen in hun games geïntegreerd hadden. Die partijen kregen een waarschuwing en het gebod om de lootboxes uit hun games te verwijderen, of op dusdanige wijze aan te passen dat deze niet langer in strijd zijn met de Wok.

Geen gehoor aan de Kansspelautoriteit

Verschillende ontwikkelaars gaven gehoor aan de oproep van de Kansspelautoriteit. De makers van het spel FIFA deden dit niet. De Kansspelautoritiet geeft daarom de last onder dwangsom op aan het bedrijf, om af te dwingen dat de overtreding van de Wok wordt gestopt. De Kansspelautoriteit geeft aan dat zij de overtreding van de wet door dit bedrijf extra ernstig vindt omdat veel minderjarigen en jongvolwassenen toegang hebben tot Packs in FIFA. Zij zijn extra vatbaar voor het ontwikkelen van een gokverslaving.

Mogelijk zullen er in de nabije toekomst nog meer lasten onder dwangsom worden uitgedeeld door de Kansspelautoriteit, aan de gameontwikkelaars die momenteel nog geen gehoor hebben gegeven aan de oproep om de illegale lootboxes uit hun games te verwijderen.

1. https://bit.ly/37lVSgK
2. https://bit.ly/2W2Kl6l

Auteur
Kim Groot
Juridisch adviseur

Trainingsoverzicht januari - april 2021

Dinsdag 12 januari & 23 maart 2021

Contracteren: de verdieping (6 PO)

Contracteren in de ICT vereist bijzondere aandacht, met name waar het gaat om software. Van ontwikkeling tot licentie en distributie en omgang met open source: software ligt immers aan de basis van vrijwel alle ICT-dienstverlening. Voortbouwend op de basistraining worden de algemene aandachtspunten uitgewerkt en nieuwe aspecten, zoals Agile ontwikkeling van software, geïntroduceerd. U gaat niet weg tot u al onze praktijktrucs kent!

https://bit.ly/30SjKfv

Dinsdag 26 januari 2021

Contracteren: de basis (6 PO)

Contracteren ligt aan de wortel van een groot deel van het ICT-recht. ICT-contracten kennen verschillende types, van softwarelicentie tot resellerovereenkomst en van algemene voorwaarden tot mantelcontract. Elk contract vereist algemene aandachtspunten (onder meer kwaliteit, aansprakelijkheid, intellectueel eigendom, datatoegang, continuïteit en persoonsgegevens) en daarnaast specifieke aspecten.

https://bit.ly/38zlrTB

Donderdag 28 januari 2021

FG Newsflash | Live webinar

De ontwikkelingen op het gebied van privacy volgen elkaar in rap tempo op. Duizelt het u als FG ook wel eens en vindt u het lastig om in alle drukte zelf op de hoogte te blijven? Of wilt u juist graag bevestiging dat u op de hoogte bent van de belangrijkste ontwikkelingen? Volg dan onze FG Newsflash en word op de hoogte gebracht van de belangrijkste actualiteiten die voor u als FG in de praktijk relevant zijn.

https://bit.ly/38C57Bh

Donderdag 28 januari 2021

AVG rechtspraak update | Live webinar (1 PO)

Laat u gedurende een uur bijpraten over de belangrijkste privacy uitspraken, de essenties hiervan én de vertaalslag naar de praktijk. Deze live webinar wordt verzorgd door twee van onze privacy adviseurs. De insteek is praktijkgericht en wij bieden ruimte voor u om vragen te stellen.

https://bit.ly/36wxw9c

Dinsdag 9 maart 2021

Privacy en persoonsgegevens: de basis (6 PO)

Wanneer is de AVG van toepassing, wat is een persoonsgegeven en waar moet u rekening mee houden op privacygebied? In deze dagtraining wordt de AVG op hoofdlijnen uitgewerkt om zo het kader voor een zorgvuldige omgang met persoonsgegevens te kunnen realiseren.

https://bit.ly/36qauRG

Dinsdag 16 maart 2021

Privacy en persoonsgegevens: de verwerkersovereenkomst (4 PO)

De verwerkersovereenkomst is de juridische borging in de relatie tussen een verantwoordelijke en een verwerker in de omgang met persoonsgegevens. Vaak wordt hierbij een standaarddocument gebruikt. De uitdaging is dit te laten aansluiten bij de werkelijke situatie en de daarnaast bestaande documenten.

https://bit.ly/2GXGZxQ

Dinsdag 6 april 2021

Privacy en persoonsgegevens: de verdieping (6 PO)

Privacywetgeving kent open normen en grijze gebieden. Als jurist moet u deze kunnen identificeren en op een deskundige en begrijpelijke wijze naar de praktijk kunnen vertalen. Hierbij is diepgravende kennis over de relevante technologie van groot belang. Tijdens de training leert u onder meer over binding corporate rules, de verwerkersovereenkomst, registers en de Functionaris Gegevensbescherming (FG).

https://bit.ly/3nfVXOZ

Praktische kennis opdoen over de Europese privacy-wetgeving (AVG)? Wellicht zijn de themadagen binnen onze opleiding tot FG/DPO dan iets voor u!

Op een themadag wordt één specifiek thema behandeld. De trainingen zijn los afneembaar en ook een op maat gemaakt pakket van losse trainingen is mogelijk.

Bestemd voor FG's/DPO's en iedere andere (juridische/niet-juridische) privacy professional.

25 maart 2021
Themadag FG en privacywetgeving

8 april 2021
Themadag soft skills

15 april 2021
Themadag verantwoordelijke en verwerker deel I*

22 april 2021
Themadag verantwoordelijke en verwerker deel II*

29 april 2021
Themadag security

12 mei 2021
Themadag inventariseren en registreren

20 mei 2021
Themadag rechten van betrokkenen

27 mei 2021
Themadag datalekken

3 juni 2021
Themadag online marketing en cookies

*Deze themadag beslaat twee dagen. Om aan deel II te mogen deelnemen, dient deel I gevolgd te zijn.

Kijk voor meer informatie op
ictrecht.nl/fg-opleiding

Onze maatregelen tegen Covid-19
Wij volgen de berichtgeving rondom Covid-19 nauwgezet. Indien trainingen niet op locatie kunnen plaatsvinden, stappen wij over op online.

Heeft u vragen of wilt u meer weten?

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

Britt Telleman
Opleidingscoördinator


ICTRECHT
adviesbureau