ICTRECHT
adviesbureau

ICTRECHT
IN DE PRAKTIJK

jaargang 8 nummer 3 juli 2020

Beeldmateriaal op scholen en de AVG: komt er ooit een klik?

De zorgplicht van ICT-dienstverleners

Geen privacy zonder security. En wat privacy van security kan leren

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

Alisa Schurink Opleidingscoördinator en Marketingmedewerker
a.schurink@ictrecht.nl
Bram de Vos Juridisch adviseur
b.devos@ictrecht.nl
Dimmen Smolders Juridisch adviseur
d.smolders@ictrecht.nl
Eline Hangelbroek Werkstudent
e.hangelbroek@ictrecht.nl
Iris de groot Juridisch adviseur ICTRecht Groningen
i.degroot@ictrecht.nl

Itte Overing Juridisch adviseur
i.overing@ictrecht.nl
Jasmine Benning Juridisch adviseur
j.benning@ictrecht.nl
Kors Monster Juridisch adviseur
k.monster@ictrecht.nl
Linde Mensink Juridisch adviseur
l.mensink@ictrecht.nl
Nicole Waaijer Marketing adviseur
n.waaijer@ictrecht.nl
Sari Jansen Juridisch adviseur
s.jansen@ictrecht.nl
Tim Wokke Juridisch adviseur
t.wokke@ictrecht.nl
Eline Pellis Grafisch ontwerper
eline@elinepellis.com
Leonard Fäustle Stills & Motion Foto's ICTRecht
info@leonardfaustle.nl

Dimmen Smolders
Juridisch adviseur

Jasmine Benning
Juridisch adviseur

Privacy

Beeldmateriaal op scholen en de AVG: komt er ooit een klik?

Het is steeds gebruikelijker voor volwassenen en kinderen om foto's of video's van elkaar te maken, ook op school. Wanneer dit beeldmateriaal voor eigen gebruik bedoeld is, is dit onder de Algemene verordening persoonsgegevens (AVG) in de regel geen probleem.[1]

Desondanks werken veel scholen aan mediawijsheid en stellen ze regels op voor het maken van foto's en video's op het schoolterrein, om het gebruik van beelden voor pesterijen of ander ongewenst gedrag te voorkomen. Tegenwoordig worden foto's en video's namelijk veelvuldig openbaar gemaakt via het Internet, met soms grote gevolgen.

Publiceert een school beeldmateriaal en zijn er personen herkenbaar in beeld, dan valt het gebruik van de foto of video niet meer onder persoonlijk gebruik, en daarmee is de AVG van toepassing. Denk hierbij niet alleen aan de jaarlijkse schoolfoto en klassenfoto, maar ook aan beelden die worden gemaakt tijdens schoolfeesten, schoolmusicals en sportdagen. De beelden van leerlingen, die bij zulke gelegenheden worden gemaakt, kunnen worden gedeeld, bijvoorbeeld met de ouders. Daarnaast plaatsen scholen vaak ook beeldmateriaal op hun website of op social media of laten zij foto's of video's zien tijdens open dagen en ouderavonden. In dit artikel wordt uitgelegd wat de eisen aan het gebruik van beeldmateriaal onder de AVG zijn en hoe scholen hieraan kunnen voldoen.

Is beeldmateriaal een persoonsgegeven?
Beeldmateriaal waarop iemand herkenbaar in beeld is, valt onder de definitie van een persoonsgegeven en geniet daarom de bescherming van de AVG. Onder die definitie valt een foto of video volgens de Autoriteit Persoonsgegevens (AP) al snel: alleen al iemands postuur kan ervoor zorgen dat de persoon identificeerbaar is.[2] De AVG maakt, zoals gezegd, wel een uitzondering voor persoonlijk en huishoudelijk gebruik. Wanneer je beeldmateriaal niet voor commerciële of professionele doeleinden verzamelt en het slechts in kleine kring deelt, hoef je niet te voldoen aan de vereisten onder de AVG. Hieronder kan bijvoorbeeld een ouder vallen die foto's maakt bij een schoolmusical, waar naast het eigen kind ook andere kinderen op staan.

Specifieke toestemming
Wanneer een school zelf beelden van leerlingen maakt en deze deelt, is dit echter een ander verhaal. Dan is er sprake van een verwerking van beeldmateriaal voor professioneel gebruik en daarmee is de AVG van toepassing. Er is dan een wettelijke grondslag nodig om de beelden te mogen maken en publiceren.

Wil een school foto's of video's van leerlingen maken en bijvoorbeeld gebruiken voor de website of de eigen Facebookpagina, dan moet hiervoor toestemming gevraagd worden. In het geval dat de leerling jonger dan 16 jaar is, dient de toestemming verkregen te worden van degene die de ouderlijke verantwoordelijkheid over

1. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/beeldmateriaal

2. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/beeldmateriaal#wanneer-is-een-persoon-op-een-foto-of-in-een-filmpje-te-identificeren-7295

het kind heeft.[3] Is het kind boven de 16 jaar, dan kan de toestemming bij de leerling zelf verkregen worden. Een mogelijke uitzondering is het gebruik van foto's ter identificatie. Voor het gebruik van een pasfoto op de leerlingenpas of in de leerlingenadministratie is bijvoorbeeld geen toestemming vereist. De school heeft namelijk een gerechtvaardigd belang hiervoor, omdat zij moet voldoen aan haar wettelijke identificatieplicht.

Scholen kunnen op verschillende manieren om toestemming vragen voor het gebruik van beeldmateriaal van leerlingen. De meeste scholen zullen ouders al bij de inschrijving om toestemming vragen, die dan geldt voor de gehele schooltijd. Het is dan echter noodzakelijk om jaarlijks onder de aandacht te brengen dat deze toestemming ingetrokken kan worden, bijvoorbeeld in de nieuwsbrief. De grootste ouderportalen bieden de mogelijkheid om via hun app een lijst met toestemmingsvragen aan ouders of leerlingen voor te leggen. Voor beeldmateriaal is die mogelijkheid een prima oplossing. Ouders kunnen dan aanvinken voor welke specifieke doeleinden zij toestemming geven.

Deze manieren van toestemming vragen, staan echter strikt genomen enigszins op gespannen voet met het vereiste dat de toestemmingsvraag onder de AVG specifiek dient te zijn. Wat voor foto's er in de schooltijd allemaal worden gemaakt en hoe je later tegen publicatie daarvan aankijkt is vooraf natuurlijk moeilijk in te schatten. Hoe waardevol is dus een toestemmingsverklaring van een aantal jaren oud? Dit wordt in de praktijk wel opgelost door ouders of leerlingen elk jaar opnieuw te vragen of hun toestemming nog geldig is. Streng bekeken is deze aanpak echter niet helemaal loepzuiver onder de AVG, maar een pragmatische oplossing is voor scholen in dit geval het beste.

Geen of ingetrokken toestemming

De noodzaak van toestemming voor het gebruik van foto's en video's van leerlingen door scholen heeft uiteraard als gevolg dat ouders of leerlingen toestemming kunnen weigeren of simpelweg kunnen vergeten toestemming te geven. Eenmaal gegeven toestemming kan bovendien altijd weer worden ingetrokken. Op basis van de AVG moet toestemming namelijk actief worden gegeven en te allen tijde ingetrokken kunnen worden.[4] Wat doe je als school, wanneer je geen toestemming hebt om beeldmateriaal van een leerling te gebruiken?

3. Zie artikel 8 lid 1 AVG.
4. Zie artikel 7 lid 3 AVG.

In sommige gevallen is dit makkelijk op te lossen. Wanneer je bijvoorbeeld een foto van leerlingen in de schoolgids wilt gebruiken, kies je simpelweg foto's van kinderen, waarvan toestemming is verkregen. Voor de klassenfoto ligt het iets ingewikkelder. Deze wordt ten slotte ook gedeeld met alle ouders van de kinderen die in de klas zitten. Kies je er dan voor om deze leerling buiten de klassenfoto te houden, ook al wil de leerling graag naast een klasgenoot zitten?

Tot slot

Het maken en delen van beeldmateriaal van leerlingen is een stuk lastiger geworden sinds de AVG van kracht is gegaan. Waar scholen voorheen vaker toestemming 'aannamen' dient deze nu expliciet en actief te worden gegeven. Als school zorg je er daarom ten eerste voor dat je altijd nagaat of het maken en delen van foto's of video's van de leerlingen in bepaalde gevallen wel echt nodig is. Vraag daarnaast de ouders of leerlingen kort voor de klassenfoto nog een keer om specifieke toestemming hiervoor en werk aan de bewustwording bij medewerkers met betrekking tot de AVG-eisen voor het maken en delen van beeldmateriaal van leerlingen. Dit vereist een compleet beleid over de omgang met beeldmateriaal. Door dergelijke maatregelen te treffen, speel je in ieder geval op veilig wat betreft de AVG. Bovendien laat je aan ouders en leerlingen zien dat je staat voor zorgvuldig gebruik van beeldmateriaal van kinderen. Ook dat ethische en opvoedkundige aspect is van belang, in deze tijd waarin beelden zo gemakkelijk ongecontroleerd blijven rondzwerven.

Bram de Vos
Juridisch adviseur

Wet- en regelgeving

Herziene Code Telemarketing
Per 1 maart 2020 is een herziene versie van de Code Telemarketing ingevoerd door de Reclame Code Commissie. Het document trad al op 1 januari 2020 in werking voor leden van DDMA, de branchevereniging die de code heeft opgesteld. Nu de Reclame Code Commissie de herziene versie heeft overgenomen, wordt deze ook relevant voor partijen die niet bij DDMA zijn aangesloten. Een belangrijke wijziging ten opzichte van de vorige versie, is dat intermediaire werving nu expliciet wordt geadresseerd. Bij deze vorm van werving bellen bedrijven iemand op voor eigen rekening en risico om hen een product of dienst (zoals een energiecontract) aan te bieden. Het gesloten contract verkopen zij vervolgens door aan de daadwerkelijke leverancier. Nieuw is ook dat telemarketeers in de toekomst moeten uitbellen met een herkenbaar nummer. Ook de regels omtrent het recht van verzet zijn aangepast. In de oude situatie moest bij ieder gesprek worden gewezen op het Bel-me-niet Register. Onder de herziene code is dit niet langer nodig als een persoon al in het register is opgenomen.

https://bit.ly/2XpeOw0

Wetsvoorstel Elektronische Gegevensuitwisseling in de Zorg
Op 10 maart 2020 is de internetconsultatie voor de Wet Elektronische Gegevensuitwisseling in de Zorg van start gegaan. Op dit moment wisselen zorgverleners informatie uit via verschillende kanalen en systemen. Er wordt nog regelmatig gewerkt met fax, papier of fysieke gegevensdragers, of in sommige gevallen vindt er helemaal geen uitwisseling plaats terwijl dit wel wenselijk is. Daardoor is informatie soms niet op tijd, op de juiste plek en in het juiste formaat beschikbaar. De wet moet zorgen voor een uniforme en gestandaardiseerde elektronische gegevensuitwisseling tussen zorgverleners. In het voorstel wordt allereerst de mogelijkheid gecreëerd om gegevensuitwisselingen verplicht elektronisch te laten plaatsvinden. Daarnaast kunnen er technische eisen worden gesteld aan de gegevensuitwisseling, om de interoperabiliteit te bevorderen. De nadere invulling zal worden vastgelegd bij Algemene Maatregel van Bestuur. De consultatie staat nog open tot 10 juni 2020.

https://bit.ly/3d3u8ov

Besluit verzekeringskeuringen ex-kankerpatiënten
Op 12 maart 2020 is een internetconsultatie gestart met betrekking tot het Besluit verzekeringskeuringen ex-kankerpatiënten. Het besluit regelt dat een verzekeraar bij het aangaan of wijzigen van een overlijdensrisicoverzekering slechts voor een beperkte termijn vragen mag stellen over iemands ziekteverleden als kankerpatiënt. Op dit moment geldt hiervoor geen maximale termijn en moeten ex-patiënten hierover lang nadat zij genezen zijn nog steeds informatie verstrekken aan de verzekeraar. Dit kan tot gevolg hebben dat zij door de verzekeraar geweigerd worden, of alleen tegen een aanzienlijk hogere premie worden geaccepteerd. Het niet kunnen afsluiten van de verzekering belemmert ex-patiënten om hun leven weer op te pakken. Zo wordt een overlijdensrisicoverzekering vaak verplicht gesteld bij het afsluiten van een hypotheek. Er wordt in het besluit een absoluut maximum van 5 jaar voor jongeren en 10 jaar voor volwassenen voorgeschreven. Bij vormen van kanker met een statistisch laag risico op terugkeer geldt een (niet gespecificeerde) kortere termijn.

https://bit.ly/2XqfrFA

Wijziging Telecommunicatiewet voor opt-in-systeem telemarketing
Op 25 maart 2020 werd een voorstel tot wijziging van de Telecommunicatiewet ingediend bij de Tweede Kamer. De wijziging ziet op het invoeren van een opt-in-systeem voor telemarketing, ter vervanging van het huidige opt-out-mechanisme. Op dit moment mogen personen ongevraagd worden benaderd voor commerciële, ideële of charitatieve doeleinden, tenzij zij zich hebben ingeschreven in het Bel-me-niet Register of anderszins hebben aangegeven niet te willen worden

benaderd. Als het wetsvoorstel wordt doorgevoerd mogen personen alleen nog worden benaderd indien zij daarvoor uitdrukkelijke toestemming hebben gegeven. Wel blijft er een uitzondering voor het benaderen van bestaande klanten.

https://bit.ly/3guviM2

Uitstel Verordening medische hulpmiddelen
Op 3 april 2020 heeft de Europese Commissie een voorstel aangenomen om de toepassing van de Verordening medische hulpmiddelen voor een jaar uit te stellen. Deze verordening stelt strengere eisen aan medische producten en aan fabrikanten die medische hulpmiddelen maken of verkopen. De Europese Commissie heeft tot uitstel besloten om de COVID-19 crisis zo goed mogelijk te kunnen bestrijden. Een tekort aan medische hulpmiddelen of een vertraagde certificering zou op dit moment onwenselijk zijn.

https://bit.ly/2TKu5Gu

Verzamelwet gegevensbescherming
Op 20 mei 2020 is de internetconsultatie voor de Verzamelwet gegevensbescherming gestart. Het voorstel bevat verschillende aanscherpingen van de Uitvoeringswet AVG ("UAVG") en gerelateerde wet- en regelgeving. Zo wordt het voor jongeren tussen de 12 en 16 jaar of personen die onder curatele of bewind staan mogelijk om onafhankelijk van hun vertegenwoordiger de toestemming voor het verwerken van persoonsgegevens in te trekken (zie artikel 5 UAVG). Ook een aantal uitzonderingen op het verbod op het verwerken van bijzondere persoonsgegevens worden aangepast of verduidelijkt. Daarnaast worden onder meer de uitzonderingen om rechten van betrokkenen in te perken (artikel 41 UAVG) aan banden gelegd. De consultatie staat nog open tot 14 juli 2020.

https://bit.ly/36tZWjY

Wetsvoorstel Zerodays Afwegingsproces
In de week van 8 juni zal er in de Tweede Kamer een plenair debat plaatsvinden over het voorstel voor de Wet Zerodays Afwegingsproces. Zerodays zijn fouten in software die nog niet bekend zijn bij de ontwikkelaar. Zerodays zijn een aantrekkelijk middel voor onder meer veiligheidsdiensten en opsporingsinstanties om bijvoorbeeld systemen van verdachten binnen te dringen. Echter, indien een zeroday niet gemeld wordt bij de ontwikkelaar van de software, kan deze kwetsbaarheid ook door anderen worden misbruikt. Het wetsvoorstel beoogt een afwegingskader te bieden voor zerodays die de overheid ontdekt, aankoopt of anderszins ter beschikking krijgt. Het doel daarvan is dat er een goede afweging kan plaatsvinden tussen de verschillende belangen die gemoeid zijn bij het geheimhouden of laten dichten ervan. De afdeling advisering van de Raad van State heeft zich eerder zeer kritisch uitgelaten over het voorstel. Volgens de Raad van State is het wetsvoorstel niet noodzakelijk gelet op al bestaande regelingen en het toezicht daarop.

https://bit.ly/2TzkYZl

Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
Op 1 juli 2020 treedt een aantal wijzigingen van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg ("Wabvpz") in werking. Nieuw is onder meer de verplichting voor de zorgaanbieder om een patiënt op diens verzoek kosteloos en elektronisch inzage te geven in zijn dossier. Op dit moment is alleen inzage in het papieren dossier wettelijk geregeld, en mag de hulpverlener hier nog een 'redelijke vergoeding' voor in rekening brengen (artikel 7:456 BW). Ook het toepassingsbereik van het inzagerecht wordt verruimd. Waar de huidige wettelijke regeling alleen betrekking heeft op de geneeskundige behandelovereenkomst, ziet de Wabvpz op alle zorgaanbieders die een patiëntendossier bijhouden. Daarnaast moet de zorgaanbieder bijhouden wie er in het dossier kijkt en werkt, omdat de patiënt recht heeft op een loggingsoverzicht.

https://bit.ly/2XvMhEQ

Tim Wokke
Juridisch adviseur

Contracteren | Cloud

De zorgplicht van ICT-dienstverleners

Over het belang van een passend ICT-contract is veel geschreven. Toch wordt er nog vaak geleverd op basis van een summiere offerte en algemene voorwaarden die niet, of niet geheel aansluiten op de diensten. Dit komt mogelijk doordat ICT-dienstverleners langer dan wenselijk vasthouden aan eenmaal opgestelde templates, terwijl de diensten die zij leveren met de tijd wel veranderen of worden uitgebreid. Maar ook de opdrachtgever speelt een rol bij onvolledige of onduidelijke ICT-contracten, omdat de focus veelal primair uitgaat naar de commerciële aspecten. Omdat ICT-projecten toch regelmatig anders uitpakken dan verwacht, zorgt dit er ook voor dat partijen soms moeten terugvallen op een gebrekkig ICT-contract. Bij klachten willen ICT-dienstverleners zich dan nog weleens op het standpunt stellen dat de klacht onterecht is omdat 'het niet (letterlijk) zo is afgesproken'.

De verplichtingen van de ICT-dienstverlener kunnen echter verder reiken dan wat op schrift is gesteld. Op basis van de wet moeten partijen namelijk rekening houden met wederzijdse belangen en heeft een dienstverlener een zekere zorgplicht. Die zorgplicht vult de overeenkomst als het ware aan tot een redelijk geheel, waarbij uiteraard rekening gehouden wordt met alle omstandigheden van het geval. In dit artikel wordt ingegaan op de aard en omvang van deze zorgplicht, mede aan de hand van voorbeelden uit de praktijk.

Zorgplicht bij een overeenkomst van opdracht

ICT-contracten zijn vrijwel altijd geheel of deels te kwalificeren als *overeenkomst van opdracht* (7:400 BW). Soms deels, als het contract mede ziet op andere typen overeenkomsten, zoals de huur of koop van apparatuur.

Het gevolg van de kwalificatie als overeenkomst van opdracht is dat de ICT-dienstverlener op grond van de wet bij zijn werkzaamheden allereerst de zorg van een goed opdrachtnemer in acht moet nemen (7:401 BW). Ook moet hij gevolg geven aan 'verantwoorde' aanwijzingen van de klant en moet hij de klant op de hoogte houden van de uitvoering van de opdracht (7:402 - 7:403 BW).

Hoe deze zorgplichten in een specifiek geval uitpakken is wel afhankelijk van alle omstandigheden van het geval. Zo zal van een eenpitter minder mogen worden verwacht dan van een doorgewinterde ICT-dienstverlener en zal de zorgplicht beperkter kunnen zijn als de klant zelf een professionele ICT-dienstverlener is, maar ook de prijs kan een rol spelen. Van een kennis die hobbymatig tegen kostprijs een website voor de bakker op de hoek levert, mag natuurlijk niet dezelfde zorg als van een professionele ICT-dienstverlener worden verwacht.

Naast de aard van partijen en de indruk die zij in de voorfase en tijdens de uitvoering van het ICT-contract wekken, speelt de tekst van het ICT-contract zelf ook een belangrijke rol bij de invulling van de zorgplicht. Dit komt doordat de voorgaande wettelijke zorgplichten van regelend recht zijn[1]. Dit betekent dat partijen onderling nadere invulling eraan kunnen geven, of zelfs kunnen besluiten deze zorgplichten buiten werking te stellen. Dit laatste geeft een ICT-dienstverlener overigens niet de vrijbrief zich als onzorgvuldig en onredelijk dienstverlener op te stellen. Zo kan een dienstverlener buiten het contract om alsnog onrechtmatig handelen en kan

1. De zorgplichten uit artikel 7:401 - 7:403 BW zijn van dwingend recht als de overeenkomst van opdracht tevens een agentuurovereenkomst is en de opdrachtnemer dus als handelsagent optreedt in de zin van artikel 7:428 BW.

binnen het contract het beginsel van redelijkheid en billijkheid alsnog een corrigerende rol spelen (6:248 BW).

Redelijkheid speelt dus onder Nederlands recht altijd wel een rol. Naar mate de verwachtingen van de klant beter zijn gemanaged en de ICT-dienstverlener bij de uitvoering van de opdracht de belangen van de klant naar beste weten en kunnen heeft behartigd, ligt wanprestatie van de zorgplicht dan ook minder voor de hand. Denk hierbij niet alleen aan het uitvragen van wensen en actief informeren van klanten over de voortgang van de opdracht, of aan het actief corrigeren van onjuiste verwachtingen van de klant, maar ook aan het waarschuwen van klanten als deze een instructie geven waarvan je weet dat het niet in diens belang is. Omdat hierbij alle omstandigheden van het geval een rol spelen - en dus niet alleen de bepalingen uit het ICT-contract - leidt dit in de praktijk tot interessante uitkomsten. Hierna volgen per onderwerp enkele voorbeelden uit de praktijk met bijbehorende rechtspraak.

Zorgplicht in de praktijk

Zorgplicht bij advisering

Voordat een ICT-contract gesloten wordt, zijn partijen al met elkaar in gesprek over de wensen en eisen van de klant en neemt de ICT-dienstverlener vaak een adviserende rol aan. In deze fase moet een goed ICT-dienstverlener al de belangen van de potentiële klant gaan behartigen. Het is daarbij verstandig niet zomaar uit te gaan van de correctheid van de informatie die de klant verschaft. Zelfs als de klant alles snel geregeld wil hebben, kan de ICT-dienstverlener het beste een kritische houding behouden. De klant schakelt de ICT-dienstverlener immers in als adviseur en het stellen van de kritische en verifiërende vragen past daar zeker bij. Ook het herhaaldelijk waarschuwen voor mogelijke nadelige gevolgen van een te snelle en niet doordachte aanpak, past daarbij.

Zo oordeelde het Hof Den Haag in 1984[2] dat een automatiseringsadviseur bij het geven van zijn advies zijn zorgplicht niet had nageleefd. De adviseur had te veel vertrouwd op de informatie van de klant en nagelaten zelf kritisch onderzoek te doen. Iets wat vanwege de grote belangen van de klant wel van een goed adviseur verwacht mocht worden. Het feit dat de klant aandrong op spoedadvies maakte dit niet anders. Dan had de adviseur maar duidelijker moeten aandringen op de noodzaak van uitgebreid onderzoek, of zijn uiteindelijke advies van uitgebreide kanttekeningen moeten voorzien (lees: vermelding dat alle risico's voor de klant zijn omdat adviseur niet in de gelegenheid werd gesteld volledig onderzoek te doen). De klant volledig volgen in diens wensen kan dus nadelige gevolgen hebben. Als je als adviseur beter weet, dan moet je dat kenbaar maken.

2. Hof Den Haag 8 maart 1984, Computerrecht 1984 nr. 2 (*RBC/ Brinkers*).

Zorgplicht bij projectbegeleiding en -bewaking
Bij het uitvoeren van projecten kan een ICT-dienstverlener verschillende rollen hebben. Als de dienstverlener de taak van projectbegeleiding heeft, brengt de zorgplicht bij een professioneel dienstverlener in ieder geval met zich mee dat algemeen bekende basisregels van projectmanagement moeten worden gevolgd.[3] Ook mag soms verwacht worden dat de voortgang van het project wordt bewaakt en de klant daarvan goed op de hoogte wordt gehouden. Mocht een dienstverlener bijvoorbeeld constateren dat een project uit de bocht schiet (al dan niet door toedoen van de klant) en dat de klant eigenlijk geen baat heeft bij verdere voortzetting, dan zou de dienstverlener moeten bijsturen in plaats van het project ongeremd laten doorlopen.[4]

Zorgplicht bij managen van verwachtingen
De zorgplicht speelt niet alleen een rol bij de uitvoering van het ICT-contract. In de voorfase tot aan het sluiten van de ICT-contract mag van een goed dienstverlener ook het een en ander worden verwacht. Zo kan een ICT-dienstverlener die redelijkerwijs moet weten dat een klant op zoek is naar bepaalde functionaliteiten, vervolgens niet wegkomen met het excuus dat die functionaliteiten niet expliciet in het ICT-contract zijn toegezegd. De zorgplicht brengt namelijk mee dat de dienstverlener in de voorfase de klant dan had moeten wijzen op de afwezigheid ervan.[5] Hetzelfde geldt voor het geval waarin een dienstverlener weet of moest vermoeden dat een klant een bepaalde softwarekoppeling inbegrepen acht, terwijl dat niet zo is. De dienstverlener moet in die gevallen actief informeren dat die koppeling niet mogelijk is, of indien wel realiseerbaar, dat het extra kosten en/of bepaalde risico's met zich meebrengt.[6]

3. Hof Amsterdam 22 november 2001 (ECLI:NL:GHAMS:2001:AD7868).
4. Rechtbank 18 januari 2017 (ECLI:NL:RBAMS:2017:228).
5. Hof Den Haag 31 maart 2015 (ECLI:NL:GHDHA:2015:1113).
6. Rechtbank Noord-Holland 4 juli 2019 (ECLI:NL:RBNHO:2018:5536).
7. Hof Amsterdam 28 april 2015 (ECLI:NL:GHAMS:2015:1635).
8. Rechtbank Limburg 21 juni 2017 (ECLI:NL:RBLIM:2017:6454) vervolg op tussenvonnis (ECLI:NL:RBLIM:2017:90).

Zorgplicht bij back-ups en klantdata
Het behoud van klantdata is voor afnemers van ICT-diensten uiteraard essentieel. Het maken van back-ups ter borging wordt dan ook vaak overeengekomen, maar niet altijd. In de gevallen dat dat niet tot de opdracht behoort is het de vraag of dit niet standaard uit de zorgplicht van een goed ICT-dienstverlener voortvloeit. Het Hof Amsterdam oordeelde eerder van niet.[7] De Rechtbank Limburg heeft daarentegen wel een keer geoordeeld dat van de dienstverlener mocht worden verwacht dat hij een back-up zou maken.[8] De dienstverlener had namelijk de opdracht een update uit te rollen op de systemen van de klant en was ervan op de hoogte dat dit risico's meebracht voor de klantdata. De klant had zelf een back-up, maar de dienstverlener had er niet op mogen vertrouwen dat deze back-up ook echt bruikbaar zou zijn. Hij had deze moeten testen, of als dat niet kon, toch zelf een back-up moeten maken. Zeker nu de dienstverlener ook wist van de risico's en het grote belang van klant bij behoud van de data. Op basis hiervan lijkt een standaard back-up verplichting niet voort te vloeien uit de zorgplicht, maar kunnen bijzondere omstandigheden toch deugdelijke voorzorgsmaatregelen vereisen.

Tot slot
Het is lastig een vinger te leggen op de aard en omvang van de wettelijke zorgplicht van ICT-dienstverleners. Omdat de besproken zorgplicht van regelend recht is, kan de ICT-dienstverlener het initiatief nemen om duidelijkheid te verschaffen over hoever deze zorgplicht reikt. Dit kan door in het ICT-contract helderheid te verschaffen over wat de klant mag verwachten, wat de rolverdeling is en wie welke verantwoordelijkheden draagt. Als er wordt gewerkt met voorwaarden die niet geheel aansluiten op de dienstverlening, loopt de ICT-dienstverlener het risico meer verantwoordelijkheden te dragen dan hem bekend is. In deze gevallen kan het geen kwaad om standaard al meer rekening te houden met de belangen van de klant.

Ook in de voorfase tot het sluiten van een ICT-contract moet rekening gehouden worden met de besproken zorgplicht. Er is namelijk al snel sprake van een overeenkomst van opdracht waarvoor deze zorgplicht geldt; zelfs als de voorafgaande advies- en inventarisatiewerkzaamheden kosteloos worden uitgevoerd. Alleen is de zorgplicht die dan geldt nog niet verder ingevuld of beperkt middels een passend ICT-contract.

ICTRECHT
adviesbureau

“Moet ik dit ICT-contract wel ondertekenen?”

Laat uw ICT-contract eerst checken voordat u de overeenkomst sluit!

De deskundige juridisch adviseurs van ICTRecht staan voor u klaar om uw ICT-contract binnen slechts 2 werkdagen te checken met de quickscan. Zo ontvangt u snel een praktisch advies waarop u kunt vertrouwen. Voor zowel afnemers als leveranciers van ICT-contracten!

Neem de quickscan nu af op
ictrecht.nl/ict-contracten-check

Kors Monster
Manager privacy
& security

Privacy Security

Geen privacy zonder security

En wat privacy van security kan leren

Privacy en security worden vaak in één adem genoemd. Dat is niet verwonderlijk, aangezien één van de kernbegrippen binnen het securitydomein 'vertrouwelijkheid' is en de privacywetgeving vereist dat organisaties 'passende technische en organisatorische beveiligingsmaatregelen' treffen om een 'op het risico afgestemd beveiligingsniveau' te waarborgen. Nu privacytoezichthouders zich expliciet uitspreken over beveiliging en er ook boetes zijn uitgedeeld vanwege een te laag beveiligingsniveau kunnen we er niet langer omheen: om privacy goed geregeld te hebben, moet ook je informatiebeveiliging op orde zijn.

Hoe het niet moet #1: Haga ziekenhuis
Veel mensen, en zeker privacy professionals, zullen zich het incident bij het Haga ziekenhuis nog kunnen herinneren. Tv-persoonlijkheid 'Barbie' werd na een overdosis drugs met spoed opgenomen in het ziekenhuis. Bij een interne controle bleek dat tientallen medewerkers haar medisch dossier hadden ingekeken, terwijl die medewerkers geenszins bij de behandeling van Barbie betrokken waren.

Na een onderzoek van de Autoriteit Persoonsgegevens (AP) had het Haga ziekenhuis de discutabele 'eer' om de eerste te zijn, die op grond van de Algemene verordening gegevensbescherming (AVG) werd beboet. De rekening: € 460.000,-. Het verwijt: het ziekenhuis deed te weinig om te controleren of enkel geautoriseerde personen toegang zochten tot medische dossiers en daarnaast werd geen tweefactorauthenticatie toegepast, hetgeen voor de AP aanleiding was om te concluderen dat de beveiliging onvoldoende was.

Hoe het niet moet #2: 1&1 Telecom
Een recenter voorbeeld betreft de Duitse telecomprovider 1&1 Telecom. De 'Bundesbeauftragte für den Datenschutz und die Informationsfreiheit' (BfDI) legde de Telecomprovider een boete van ruim 9,5 miljoen euro op. Wat was er aan de hand? Door telefonisch contact op te nemen met de helpdesk van 1&1 Telecom kon eenvoudig informatie van klanten van 1&1 worden opgevraagd. De identiteit van de beller werd gecontroleerd door naam en geboortedatum te vragen. Deze controle vond de BfDI onvoldoende, en dus een boete van 9,5 miljoen euro waard.

Wat eist de AVG op securitygebied?
Artikel 32 AVG vereist dat organisaties 'passende technische en organisatorische maatregelen' treft om een 'op het risico afgestemd beveiligingsniveau' te waarborgen, waaarbij rekening moet worden gehouden met:

- De stand van de techniek;
- De uitvoeringskosten;
- De aard, omvang, context en verwerkingsdoeleinden;
- De qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen.

Dat is een flinke mond vol. In de praktijk is dit een AVG-bepaling waarbij wij veel juristen zien afhaken.

Weinig wettelijke bepalingen zijn zo open en vaag geformuleerd als deze.

Dat heeft de wetgever echter bewust gedaan: enerzijds gaan technische ontwikkelingen razendsnel, waardoor wetgeving een te traag instrument is om voor te schrijven welke concrete beveiligingsmaatregelen zouden moeten worden getroffen. Anderzijds zijn er dusdanig veel factoren relevant voor het bepalen van wat een passende beveiliging is, dat de wetgever dat niet centraal voor alle organisaties die aan de AVG dienen te voldoen, kan bepalen. Vandaar dat organisaties dit zelf moeten afwegen en invullen.

De AVG geeft, in vergelijking met haar voorganger[1], wel richting voor het bepalen van passende beveiligingsmaatregelen. Zo worden pseudonimisering en versleuteling als specifieke maatregelen getipt, evenals:

- Het permanent kunnen garanderen van de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht;
- Het vermogen om bij een incident de beschikbaarheid van persoonsgegevens tijdig te herstellen;
- Het regelmatig testen, beoordelen en evalueren van de doeltreffendheid van de getroffen beveiligingsmaatregelen.

Raakvlakken met informatiebeveiliging
De wetgever lijkt in de AVG enigszins te willen pronken met andermans veren, met dien verstande dat de beveiligingsvoorschriften sterk hinten op principes en werkwijzen die in het domein van de informatiebeveiliging al geruime tijd worden gehanteerd. Dat gaat verder dan de referentie aan de kernbegrippen uit de informatiebeveiliging (vertrouwelijkheid, integriteit en beschikbaarheid).

Om te beginnen met de frase 'een op het risico afgestemd beveiligingsniveau'. Binnen het domein van informatiebeveiliging is de 'risk based approach' eveneens gebruikelijk. Zo speelt binnen de ISO27001-standaard[2] de risicoanalyse een centrale rol. Door op gestructureerde wijze kwetsbaarheden en bedreigingen te identificeren en te wegen ontstaat een integraal beeld van de risico's voor informatiebeveiliging (en de bedrijfsvoering). De risicoanalyse vormt het startpunt voor het beslissen over te nemen maatregelen en de implementatie daarvan.

Anderzijds hint de AVG op het implementeren van een 'plan-do-check-act-cyclus' (PDCA-cyclus)[3]. Dat is een manier om een cyclisch proces in te richten, die erop gericht is om over tijd het proces te verbeteren. In de plan-fase wordt, o.a. op basis van de geïnventariseerde risico's, bepaald welke maatregelen zullen worden ingesteld. In de do-fase worden de maatregelen geïmplementeerd of ten uitvoer gebracht. Vervolgens wordt in de check-fase beoordeeld of de maatregelen conform het plan zijn uitgevoerd en of zij het gewenste effect sorteren. Op basis van deze controle kan in de act-fase worden bijgestuurd.

1. Voor Nederland: de Wet bescherming persoonsgegevens.
2. ISO27001 is een internationaal erkende standaard voor het procesmatig inrichten van informatiebeveiliging.
3. O.a. door in art. 32 de risk based approach voor te schrijven en in art. 32 lid 1 sub d een procedure voor regelmatig testen, beoordelen en evalueren verplicht te stellen.

Vervolgens begint de cyclus opnieuw bij het valideren van de risico's en het maken van nieuwe plannen.

De PDCA-cyclus wordt ook binnen het informatiebeveiligingsdomein toegepast en neemt een centrale rol in bij het inrichten van een information security management system (ISMS)[4]. Het is een goede werkwijze om doorlopend het beveiligingsniveau te controleren en waar nodig te verbeteren.

Wat privacy van security kan leren
De PDCA-cyclus, die in de vorige paragraaf werd toegelicht, is een goed middel om er procesmatig voor te zorgen dat het beveiligingsniveau van informatie (waaronder persoonsgegevens) afgestemd is én blijft op de specifieke context en risico's. Maar de PDCA-cyclus is niet alleen voor de beveiliging van persoonsgegevens relevant. Binnen het privacydomein kan de PDCA-cyclus worden toegepast om ook de andere facetten van de privacyhuishouding continu te verbeteren. Denk bijvoorbeeld aan de wijze waarop betrokkenen hun rechten kunnen uitoefenen, de gepubliceerde privacyverklaring en het verwerkingsregister.

4. Het ISMS is het geheel aan afspraken, maatregelen, processen en procedures waarmee informatiebeveiliging wordt geborgd binnen een organisatie.

Conclusie
Privacy wil je om verschillende redenen goed geregeld hebben: niet alleen omdat toezichthouders grote boetes kunnen opleggen, maar zeker ook om het vertrouwen van uw stakeholders (zoals klanten) te behouden en daarmee de continuïteit van uw organisatie te borgen. Om privacy goed geregeld te hebben, zult u ook de beveiliging van persoonsgegevens op orde moeten hebben.

Informatiebeveiliging is niet technisch en eng. Vanzelfsprekend komt er techniek bij kijken, maar om informatiebeveiliging goed geregeld te hebben, zijn technische beveiligingsmaatregelen niet genoeg. Het begint met het identificeren van risico's en het maken van een weloverwogen plan om de beveiliging naar het gewenste niveau te tillen. Dat hoeft niet meteen 100% perfect te zijn: dankzij de PDCA-cyclus worden de maatregelen doorlopend geëvalueerd en bijgesteld. Dankzij deze werkwijze wordt de beveiliging van informatie (zoals persoonsgegevens) continu verbeterd. En dat is een werkwijze die ook op andere gebieden binnen het privacydomein uitkomst kan bieden.

Itte Overing
Juridisch adviseur

E-health Privacy

Wetsvoorstel Elektronische Gegevensuitwisseling in de Zorg

Voor goede zorg is het noodzakelijk dat patiëntgegevens digitaal worden uitgewisseld. Gebrek aan eenduidigheid in taal in de zorg en in de techniek en een gebrek aan integrale aanpak door uiteenlopende belangen van zorgaanbieders[1], zorgverleners[2] en IT-leveranciers, staan hieraan echter in de weg.

Daar zorgverleners moeten kunnen beschikken over adequate, actuele en uniforme informatie op de juiste plek op het juiste moment om goede zorg te kunnen verlenen, heeft de Tweede Kamer de Minister voor Medische Zorg ("de Minister") herhaaldelijk gevraagd om meer de regie te nemen op het gebied van gegevensuitwisseling tussen zorgverleners. Met het wetvoorstel Elektronische Gegevensuitwisseling in de Zorg ("het wetsvoorstel") neemt de Minister die regie.

Om te bepalen of dit de gewenste vorm van regie is, liggen het wetsvoorstel en bijbehorende Memorie van Toelichting ("de MvT") nu ter internetconsultatie. Eenieder kan reageren.

Eerder, in 2008 en 2011, probeerde de overheid de regie ook naar zich toe te trekken met de ontwikkeling van een landelijk EPD en bijbehorende technologie: het Landelijk Schakelpunt. Hierop kwam veel kritiek, onder andere dat veldpartijen zelf verantwoordelijk zijn voor het leveren van goede zorg en dus ook voor de inrichting en totstandbrenging van elektronische gegevensuitwisseling. Verder is er flink gediscussieerd over of een opt-in of opt-out noodzakelijk was, oftewel of een patiënt vooraf toestemming moest geven of dat het voldoende is als er achteraf bezwaar kan worden gemaakt.

Daarna heeft de overheid zich terughoudend opgesteld, desalniettemin heeft zij wel verschillende programma's gestart om de veldpartijen te ondersteunen. In de MvT wordt aangegeven dat er klaarblijkelijk toch wel behoefte is aan overheidsbetrokkenheid, en is er noodzaak tot een inhaalslag. Want al zijn er zeker stappen de goede richting in gezet, de veldpartijen hebben de overheid nodig om het gebrek aan eenduidigheid en het gebrek aan integrale aanpak op te lossen.

Scope

Binnen de scope van het wetsvoorstel valt het elektronisch uitwisselen van informatie over een cliënt, een natuurlijke persoon die zorg vraagt of aan wie zorg

1. Zoals gedefinieerd in lid 1, 6 en 8 van artikel 1 van de Wkkgz: "een instelling dan wel een solistisch werkende zorgverlener". In de concept MvT wordt nog expliciet aangegeven dat hiermee gedoeld wordt op 'de bestuurders'.
2. Zoals gedefinieerd in lid 1 van artikel 1 van de Wet kwaliteit klachten en geschillen zorg ("Wkkgz"): *"een natuurlijke persoon die beroepsmatig zorg verleent."*
3. Zoals gedefinieerd in lid 1 van artikel 1 van de Wkkgz.

wordt verleend,[3] tussen zorgverleners. Het voorstel richt zich tot zorgaanbieders[4], niet de zorgverleners. Zij moeten erop toezien dat de gegevens op de juiste elektronische manier worden uitgewisseld door zorgverleners en dat daarbij gebruik wordt gemaakt van IT-producten of diensten die de verplichte certificaten hebben.[5]

Binnen de scope van het wetsvoorstel valt de zorg of dienst zoals omschreven bij of krachtens de Zorgverzekeringswet of de Wet langdurige zorg en handelingen zoals bedoeld in artikel 1 van de Wet op beroepen in de individuele gezondheidszorg. Jeugdhulp en maatschappelijke ondersteuning vallen er nu nog buiten, het is wel de bedoeling de reikwijdte van de wet later te verbreden.[6]

In het wetsvoorstel wordt gesproken over elektronisch uitwisselen. Het gaat dan uitdrukkelijk niet om het verplicht uitwisselen middels een elektronisch uitwisselingssysteem zoals gedefinieerd in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Dan is altijd vooraf toestemming van de cliënt nodig voor de opname in het uitwisselingssysteem, dat zou het verplicht stellen van het elektronisch uitwisselen onmogelijk maken. Verder kunnen misschien eindelijk ook alle faxapparaten met pensioen, want die vallen niet onder "elektronisch uitwisselen".

Wel wordt er met elektronisch uitwisselen van gegevens bedoeld: het delen en benaderen van gegevens middels een computersysteem via een elektronische weg, waarbij het delen rechtstreeks tussen zorgverleners gebeurt, al dan niet op een gestandaardiseerde wijze.

Stap voor stap

Met dit wetsvoorstel worden zorgaanbieders "stap voor stap", "gegevensuitwisseling na gegevensuitwisseling", verplicht om erop toe te zien dat zorgverleners onderling in ieder geval gegevens elektronisch en gestandaardiseerd met elkaar uitwisselen.

De Minister geeft in de MvT wel aan dat: *"De baten van het elektronisch uitwisselen van gegevens bij een aangewezen gegevensuitwisseling moeten in beginsel uiteindelijk hoger zijn dan de lasten."* Voorgaande zal onder andere moeten blijken uit een te maken maatschappelijke kosten-batenanalyse. Daarnaast moeten de gegevensuitwisselingen bijdragen aan het verlenen van goede zorg en realiseerbaar en uitvoerbaar zijn. Dat betekent niet alleen dat duidelijk moet zijn welke gegevens nodig zijn voor goede zorg, maar ook dat de uitwisseling technisch uitvoerbaar moet zijn.

Er zijn door de Minister vooralsnog, na consultatie van het Informatieberaad Zorg, dertien gegevensuitwisselingen op de "Roadmap" gezet waarmee gestart kan worden:

1. Ambulance-overdracht;
2. Medicatie-Digitaal receptenverkeer;
3. Medicatie–Verstrekken & Toedienen;
4. Ziekenhuizen BgZ;
5. Verpleegkundige overdracht;
6. Ketenzorg Diabetes;
7. GGZ-overdracht BgZ;
8. Verloskunde- Gynaecologie;
9. Beeld-Ziekenhuizen;
10. Beeld-Pathologie;
11. MDO Oncologie;
12. Triageverwijzing;
13. Geboortezorg/JGZ.

Welke gegevens en hoe

Bij Algemene Maatregel van Bestuur ("AMvB")[7] wordt per gegevensuitwisseling vastgesteld welke gegevens moeten worden uitgewisseld. Denk hierbij aan:

- Gegevens zoals onderdeel van goede zorg en bepaald in sectoroverstijgende kwaliteitstandaarden[8] of zoals vastgesteld bij wet;
- Administratieve gegevens;
- Gegevens over cliëntcontext.

De uitdaging hierbij wordt dat de bestaande praktijk snel kan wijzigen omdat bijvoorbeeld andere gegevens nodig blijken voor het verlenen van goede zorg. De verplichte gegevensuitwisseling moet dan mee kunnen bewegen.

4. Let op, artikel 1 lid 7 Wkkgz is hier van toepassing: *"Indien een instelling wordt gevormd door een organisatorisch verband van natuurlijke personen, richten de uit deze wet voortvloeiende verplichtingen zich tot ieder van die personen."*
5. Artikel 2.1 van het wetsvoorstel.
6. Verder is het wetsvoorstel niet van toepassing in gevallen zoals beschreven in artikel 1.2 onder 2 van het wetsvoorstel.
7. Alvorens de AMvB's zoals onderdeel van het wetsvoorstel te kunnen vaststellen, moeten zij ter goedkeuring worden voorgelegd middels een voorhangprocedure als waarborg voor parlementaire betrokkenheid.
8. https://www.zorginzicht.nl/kwaliteitsinstrumenten?sortering=status

Zodra een bepaalde gegevensuitwisseling verplicht elektronisch moet, en daarbij bepaalde eisen gelden op grond van een AMvB, dan is het aan de zorgaanbieder om hiervoor zorg te dragen. Hierbij kiest de Minister ervoor om de interoperabiliteit in eerste instantie over te laten aan het veld ("spoor 1"). Interoperabiliteit moet bereikt worden door taal en techniek te standaardiseren. Wel kunnen er ook dan bij of krachtens AMvB bepaalde standaarden verplicht worden.[9] Het gaat dan om bijvoorbeeld NEN 7510, de norm voor informatiebeveiliging in de zorg, een standaard die breder geldt dan voor een specifieke gegevensuitwisseling. Daarnaast moet natuurlijk gewoon worden voldaan aan geldende wet- en regelgeving.

Mocht het veld niet tot een voldoende niveau van standaardisatie komen voor interoperabiliteit, dan kan er middels een AMvB (verdere) standaardisatie afgedwongen worden ("spoor 2"). Middels de AMvB wordt een bepaalde certificering opgelegd aan de IT-leverancier. De zorgaanbieder mag dan enkel nog gebruik maken van IT-producten of diensten die de juiste certificering hebben.

Hiermee lijkt de Minister de IT-leveranciers ook tegemoet te komen. Implementatie van standaarden en dus het laten certificeren van een product of dienst, kan alleen rendabel worden indien die standaarden landelijk worden gehanteerd.

Certificerende instellingen en handhaving
Zodra een certificering nodig is, moet de IT-leverancier het desbetreffende certificaat verkrijgen voor zijn dienst of product. Er wordt een voorbeeld gegeven: vaak bestaat er al een (langdurige) relatie tussen een IT-leverancier en zorgaanbieder. Er wordt dan een softwarepakket met bijbehorende dienstverlening afgenomen en in bepaalde gevallen tevens bijbehorende hardware. Ook in die gevallen is en blijft de leverancier verantwoordelijk voor een juiste certificering van zijn product en/of dienst.

Het certificaat moet aangevraagd worden bij een geaccrediteerde certificerende instelling die daartoe ook nog eens is aangewezen door de Minister middels publicatie in de Staatscourant. De accreditatie kan verkregen worden van de Raad van Accreditatie.[10]

De Minister kan, bij of krachtens AMvB, de mogelijkheid hebben toe te zien op de certificerende instellingen en zo nodig de toewijzing schorsen of zelfs intrekken. Voorgaande is belangrijk daar een certificerende instelling niet alleen het certificaat verleend maar ook moet blijven toezien op het voldoen aan de eisen die gelden voor de dienst of het product. In de MvT staat dat zij hiertoe "steekproefsgewijs controles en administratieve audit uitvoeren".[11] Vervolgens kan een certificaat geschorst of ingetrokken worden. Als de IT-leverancier het daar niet mee eens is, kan hij naar de bestuursrechter. De certificerende instelling wordt namelijk aangemerkt als bestuursorgaan.

Indien er geen certificaat geldt of wordt aangevraagd, dan kan de instelling niet handhaven. De door de Minister aangewezen ambtenaren houden dan toezicht op de aanwezigheid van een certificaat. Door hen kan een bestuursrechtelijke punitieve sanctie worden opgelegd van maximaal € 900.000,-.

Als de zorgaanbieder niet aan de gestelde verplichtingen voldoet, kan door de Minister, of de instantie waaraan de handhaving is gemandateerd, de schriftelijke aanwijzing worden ingezet. De zorgaanbieder krijgt dan voorgeschreven binnen welke termijn hij wat voor elkaar moet hebben. Voorgaande wordt al dan niet kracht bijgezet door een herstelsanctie in de vorm van een last onder bestuursdwang of dwangsom.[12]

Ontwikkelingen
Op de nieuwe website www.gegevensuitwisselingindezorg.nl kunnen alle ontwikkelingen gevolgd worden rondom het programma Elektronische Gegevensuitwisseling in de Zorg en het tot 10 juni ter internetconsultatie gelegde wetsvoorstel.
De website opent met: "*De zorg maakt een digitaliseringsslag.*" Of dit gaat gebeuren onder de regie zoals voorgesteld in het wetsvoorstel, de bal ligt nu bij het veld.

9. Artikel 1.3 lid 2 onder a van het wetsvoorstel.
10. https://www.rva.nl
11. Zie paragraaf 7.3 van de concept MvT.
12. Artikel 2.1 van het wetsvoorstel

Iris de Groot
Juridisch adviseur
ICTRecht Groningen

Software Contracteren

Onderhoud van standaardsoftware

Bij de ontwikkeling van software wordt vaak gebruikgemaakt van standaardsoftware. Het gebruik van standaardsoftware biedt namelijk veel voordelen. Het is goedkoper en vaak sneller in gebruik te nemen. En waarom het wiel twee keer uitvinden, als het al is uitgevonden? Toch zitten er ook nadelen aan het gebruik van standaardsoftware. In de praktijk ontstaan er namelijk vaak discussies en interpretatieverschillen over het onderhoud. Want wat gebeurt er als de ontwikkelaar ermee stopt, wie verricht dan het onderhoud van de standaardsoftware?

Noodzakelijkheid van onderhoud

Zonder onderhoud is software na verloop van tijd onbruikbaar. Het is dus noodzakelijk dat er om de zoveel tijd fouten ('bugs') worden verwijderd en dat er verbeteringen worden doorgevoerd zoals 'updates'. Bij het onderhoud van software is de afnemer veelal afhankelijk van de ontwikkelaar. De ontwikkelaar heeft de broncode in zijn bezit en de afnemer kan zelf, zonder deze broncode, niet met het onderhoud van de software aan de slag. Een problematisch punt wanneer de ontwikkelaar er besluit mee te stoppen, failliet gaat of als de relatie met de ontwikkelaar stukloopt.

De broncode

De broncode is simpel gezegd de originele tekst waar de betreffende software uit voortkomt. Het is leesbare tekst die wordt 'vertaald' naar een code (de objectcode) die een systeem vervolgens kan lezen. Deze code bevat vervolgens aantekeningen over de werking en de functionaliteiten van de software. Op het moment dat je de broncode aanpast zal de software ook worden gewijzigd. Veelal zal de afnemer voor het aanbrengen van aanpassingen in de software en het verbeteren van fouten dus over de broncode moeten beschikken.

Auteursrechtelijke bescherming

De broncode wordt doorgaans beschermd door het auteursrecht. Over de omvang van de bescherming is bepaald dat de bescherming wordt verleend aan de uitdrukkingswijze van het programma, in welke vorm dan ook. Hetgeen betekent dat software zowel in de vorm van objectcode als in de vorm van broncode beschermd is.

De auteursrechtelijke bescherming van de broncode betekent dat software niet zonder toestemming mag worden gewijzigd. De rechthebbende – of met andere woorden, de softwareontwikkelaar – dient toestemming te verlenen voor wijzigingen die aan de software worden aangebracht. Zonder toestemming is het aanbrengen van wijzigingen aan software niet toegestaan en levert het een inbreuk op de auteursrechten van de rechthebbende op.

Uitzondering Auteurswet

Software mag dus niet zomaar worden aangepast, ook niet voor onderhoud. Onderhoud kan echter binnen bepaalde grenzen worden toegestaan.[1] In de Auteurswet is namelijk een uitzondering opgenomen, wat maakt dat verbodshandeling binnen kaders worden toegelaten.[2]

Deze uitzondering geldt alleen voor de 'rechtmatige verkrijger' van de software. Een licentienemer (de afnemer van de software) is een rechtmatige verkrijger en zou dus het onderhoud van de software zelf of door een derde kunnen laten verrichten. Echter is het daarnaast ook vereist dat het aanbrengen van wijzigingen in de software "noodzakelijk is voor het met dat werk

1. Artikel 45j Auteurswet.
2. Artikel 45i Auteurswet.

beoogde gebruik". Alleen dan valt het onder de uitzondering. De vervolgvraag is dan ook; wat valt er precies onder 'noodzakelijk' en 'beoogd gebruik'? Dit zijn immers termen die op verschillende manieren kunnen worden uitgelegd.

Noodzakelijk voor het met het werk beoogde gebruik
De afnemer van de software heeft een aantal minimumrechten die ervoor zorgen dat de afnemer de software mag (blijven) gebruiken. In de eerste plaats gaat het erom dat de handelingen noodzakelijk dienen te zijn voor het gebruik van het programma. In de tweede plaats moet het gaan om gebruik dat met het programma wordt beoogd. In die gevallen is er geen toestemming van de rechthebbende (lees: softwareontwikkelaar) nodig. Er kunnen contractueel uitzonderingen op deze wettelijke licentie worden gemaakt, maar bij overeenkomst kunnen niet alle handelingen worden verboden. Handelingen in het kader van het laden, in beeld brengen of het verbeteren van fouten zijn toegestaan. "Met andere woorden, verveelvoudigingshandelingen die noodzakelijk zijn voor het onderhoud van het programma in de zin dat het programma overeenkomstig het daarmee beoogde doel kan (blijven) functioneren, zijn zonder toestemming van de rechthebbende toegestaan aan degene die rechtmatig beschikt over [een] exemplaar van het programma."[3]

Met het woord 'noodzakelijk' wordt dus tot uitdrukking gebracht dat de desbetreffende handelingen technisch absoluut vereist zijn om het programma te kunnen gebruiken overeenkomstig het beoogde doel. Het beoogde doel kan contractueel zijn vastgelegd of voortvloeien uit de aard van de programmatuur in combinatie met de andere omstandigheden van het geval. Maar ook deze definiëring blijft enigszins vaag, dit is terug te zien in de rechtspraak.

De Rechtbank Midden-Nederland kwam in april 2019 tot de conclusie dat de interpretatie van de zinsnede "noodzakelijk is voor het met dat werk beoogde gebruik" lastig is en op verschillende manieren kan worden uitgelegd.[4] Dit was een zaak die was aangespannen door een softwareleverancier tegen een licentienemer die het onderhoud van de software had uitbesteed aan een derde. De softwareleverancier meende dat er sprake was van een inbreuk op het auteursrecht, waarbij de licentienemer een beroep op de hierboven besproken uitzondering uit de Auteurswet deed. De rechtbank gaf de licentienemer de opdracht om het 'noodzakelijkheids-

3. *Kamerstukken II 1991/92, 22531, 3, p. 12-13.*
4. Rb. Midden-Nederland 10 april 2019, ECLI:NL:RBMNE:2019:1478.

vereiste' en het 'beoogde gebruik' nader te duiden, omdat dit nergens op schrift was vastgelegd.

Bijna een jaar later, op 5 maart 2020, volgt er een nieuw tussenvonnis.[5] De rechtbank concludeert dat de door de derde verrichte onderhoudswerkzaamheden onvoldoende noodzakelijk waren voor het beoogde gebruik. Naar het oordeel van de rechtbank had de licentienemer het beoogde gebruik te ruim geformuleerd en de onderhoudswerkzaamheden onvoldoende beschreven. Daarnaast was onvoldoende onderbouwd dat die handelingen technisch 'absoluut vereist' waren om de software te gebruiken overeenkomstig het beoogde doel. De licentienemer pleegt daarmee inbreuk op het auteursrecht van de softwareontwikkelaar/leverancier.

Standaard- en maatwerksoftware

Software is dus auteursrechtelijk beschermd, ongeacht of het gaat om standaardsoftware of om maatwerksoftware. Toch is het onderscheid tussen standaard- en maatwerksoftware relevant. Dit onderscheid kan namelijk van belang zijn voor de invulling van het 'beoogde gebruik' van de software. Zo zal het gebruik van software dat in opdracht van een onderneming is ontwikkeld, niet snel buiten de grenzen van het 'beoogde gebruik' vallen. De verhouding tussen de partijen is immers gestoeld op het feit dat het gaat om maatwerk, waarbij de software speciaal voor deze onderneming is gemaakt. Al snel brengt de aard van de software in combinatie met de omstandigheid dat het gaat om maatwerk mee, dat het verrichten van onderhoud noodzakelijk is voor het beoogde doel. Dat ligt echter anders bij standaardsoftware. Dit is software die doorgaans op niet-exclusieve basis en tegen een fractie van de ontwikkelkosten ter beschikking wordt gesteld. Vandaar dat hierbij meer terughoudendheid op zijn plaats is. Het belang van dit onderscheid wordt ook duidelijk uit de twee tussenvonnissen. De (standaard) software die centraal staat in de zaak wordt door verschillende transportbedrijven en logistieke bedrijven gebruikt als backoffice-systeem voor hun bedrijfsprocessen. Dit maakt dat er striktere grenzen voor toegelaten handelingen worden gehanteerd en er minder snel sprake zal zijn van 'beoogd gebruik.'

Een duidelijke licentie van groot belang

De conclusie van de twee tussenvonnissen verduidelijkt de grenzen die aan de uitzondering worden gesteld. Daarnaast geeft het des te meer aan dat het van groot belang is om goed te kijken naar de softwarelicentieovereenkomst, zoals de omschrijving van waar de licentie toe strekt en wat het beoogde gebruik is. Zo is het bijvoorbeeld raadzaam om expliciet in de overeenkomst op te nemen of het is toegestaan het onderhoud aan een derde uit te besteden. Indien je het als softwareleverancier onwenselijk acht dat een derde onderhoud aan de software verricht, is het goed om te bepalen wat er gaat gebeuren indien de relatie met uw klant ophoudt te bestaan. Dit kan bijvoorbeeld aan de hand van een exit-bepaling. Met een duidelijke omschrijving kan partijen de weg naar de rechter (mogelijk) worden bespaard.

5. Rv. Midden-Nederland 5 maart 2020, zaaknummer NL18.5132.

Linde Mensink
Juridisch adviseur

Privacy

Het nut en de noodzaak van een Functionaris Gegevensbescherming

Uw organisatie verwerkt waarschijnlijk op veel verschillende manieren persoonsgegevens. Sollicitatieprocedures, marketingactiviteiten, maar ook een ogenschijnlijk simpel contactformulier: dit alles brengt allerlei persoonsgegevens met zich mee die op een zorgvuldige manier moeten worden beveiligd, opgeslagen én anderszins 'netjes' verwerkt moeten worden. In elke organisatie spelen daarnaast ook verschillende belangen, die bij de verschillende functies en afdelingen komen kijken. De marketeer, die graag zo veel mogelijk data wil verzamelen en deze met elkaar combineren om zeer gericht te kunnen adverteren. De HR-medewerker, die graag werkt met ouderwetse lijstjes in Excel om bij te houden wanneer zij haar collega's attenties verstuurt bij bijzondere privégebeurtenissen. Maar ook de eventplanner die graag wil registreren welke gasten wellicht een allergie hebben, of andere dieetwensen. Kortom: nagenoeg elke organisatie heeft te maken met persoonsgegevens en elke afdeling heeft weer bepaalde visies over de omgang met deze persoonsgegevens. Het is een feit dat voor alle organisaties, en daarmee ook alle afdelingen, geldt dat zij zich moeten houden aan de toepasselijke privacyregels. Niet altijd even gemakkelijk! Gelukkig hoeft een organisatie dit niet altijd geheel zelf uit te zoeken.

De Functionaris Gegevensbescherming (FG) en in het Engels: Data Protection Officer (DPO) is de persoon binnen een organisatie die toezicht houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG). Dit klinkt wellicht nog wat abstract. Hoe werkt dat precies? De FG heeft een breed takenpakket, waaronder het creëren van privacybewustzijn in de organisatie en het actief betrokken zijn bij de wijze waarop de organisatie omgaat met persoonsgegevens.

De FG fungeert tevens als eerste aanspreekpunt voor de Autoriteit Persoonsgegevens (AP). Kenmerkend voor de FG is dat deze een onafhankelijke rol dient te behouden binnen de organisatie, maar tegelijk rechtstreekse lijnen heeft met het bestuur. De FG heeft kennis van privacywetten en -regelgeving, maar ook voldoende inzicht in en kennis van security of 'korte lijntjes' met die afdelingen, én de processen binnen de organisatie. De FG kan een personeelslid van de organisatie zijn, of kan de taken op grond van een dienstverleningsovereenkomst verrichten. De FG wordt wel eens gekscherend een 'schaap met vijf poten' genoemd. Niet zo gek, gezien de competenties en kennis waarover hij of zij moet beschikken. Maar wat betekent dit nu in de praktijk? Wat moet (of mag) een FG doen in de dagelijkse praktijk?

Hieronder leest u een aantal praktische voorbeelden:

- Elke organisatie dient haar betrokkenen te informeren over hoe het bedrijf omgaat met persoonsgegevens. De FG kan helpen bij het opstellen van de benodigde privacyverklaringen. Ook voor nieuwe plannen in de organisatie, zoals tracking via de website, geldt dat hierover moet worden geïnformeerd en dat de nodige toestemmingen moeten worden uitgevraagd. Dit is een aangewezen situatie waarover de FG kan adviseren.
- Met alle verwerkers, zoals leveranciers, dient een verwerkersovereenkomst gesloten te worden. De FG kan het sluiten van, maar ook het onderhandelen over, deze verwerkersovereenkomsten uit handen nemen.
- De werkwijze van (nieuwe) processen waarbij gegevens worden verwerkt, dient gecontroleerd te worden om ervoor te zorgen dat niet meer gegevens worden verwerkt dan nodig zijn.
- De verschillende programma's en systemen waarmee een organisatie werkt, dienen te worden beveiligd. Het moet mogelijk zijn om te achterhalen wie welke gegevens kan inzien en kan wijzigen. Niet alleen beveiliging tegen onbevoegde toegang is noodzakelijk. Ook beveiliging tegen verlies is belangrijk.
- Een organisatie moet een beleid hebben over hoe de werknemers moeten handelen in het geval van een datalek. Daarnaast is het belangrijk dat de awareness onder het personeel wordt bevorderd.
- Betrokkenen hebben verschillende privacy rechten, en worden zich hier ook steeds meer bewust van! Eventuele lastige vragen kan een organisatie gemakkelijk doorsturen naar de FG. De FG kan de vragen van de betrokkenen beantwoorden en kan verzoeken beoordelen voor het inzien van de gegevens of het aanpassen ervan.
- Bewaartermijnen moeten gehanteerd worden. De FG zal ervoor zorgen dat de gegevens die de organisatie verwerkt periodiek worden opgeschoond.

In bepaalde situaties zijn organisaties wettelijk verplicht om een FG aan te stellen.[1] Dit geldt voor publieke organisaties en overheidsinstanties, organisaties die doen aan profilering, hun personeel 'tracken' of anderszins vanuit hun kernactiviteiten op grote schaal individuen volgen of diens activiteiten in kaart brengen. Maar ook organisaties die vanuit hun kerntaak op grote schaal bijzondere persoonsgegevens verwerken, zoals gegevens over iemands gezondheid of religie zijn verplicht tot het aanstellen van een FG, denk hierbij aan een ziekenhuis. Voor deze laatste categorie heeft de AP duiding gegeven over de richtlijn voor grootschaligheid[2], waaruit blijkt wanneer een zorginstelling verplicht is om een FG aan te stellen. Deze verplichting tot aanstelling geldt ook wanneer een organisatie strafrechtelijke persoonsgegevens verwerkt. Daarnaast kunnen EU-lidstaten andere situaties benoemen waarin een FG verplicht is.

Veel meer duiding is nog niet gegeven over de verplichting tot aanstelling van een FG en het komt dan ook vaak voor dat een organisatie hierover twijfelt. De AP beveelt in gevallen van twijfel over een aastelling, aan om wél een FG aan te stellen en het zekere voor het onzekere te nemen. Belangrijk bij een keuze is dat er een goede onderbouwing is waarom er wél of juist niet voor is gekozen. Natuurlijk is het in veel gevallen gewoonweg ontzettend handig om een FG aan te (laten) stellen, zelfs wanneer dit niet wettelijk verplicht is.

De FG schiet te hulp

Een FG heeft kennis van de AVG en heeft als taak om de organisatie te adviseren (gevraagd en ongevraagd) op het gebied van privacy. Een FG zal niet alleen melden welke persoonsgegevens onder de AVG níét mogen worden verwerkt, maar zal juist ook ondersteunen bij het ontwikkelen van plannen en beleid om persoonsgegevens op de juiste wijze en op een nette manier te verwerken. Waar dat niet duidelijk is, kan er simpelweg een vraag naar de FG worden gestuurd die daar een duidelijk antwoord op kan geven.

Waar vindt u zo'n FG? Voor hoeveel uur per week moet u deze in dienst nemen? Is extern inhuren voor uw organisatie een uitkomst? Als deze administratieve hordes zijn genomen, dan resten nog vragen als: wat kunt u nu eigenlijk verwachten van een FG? En waar zit de meerwaarde van het aanstellen van de FG voor uw organisatie?

Wij snappen dat er tal van dit soort vragen op uw pad kunnen komen. Benieuwd wat een FG voor uw organisatie kan betekenen? Neem contact op via privacy@ictrecht.nl en profiteer van korting op een FG-abonnement!

1. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/functionaris-gegevensbescherming-fg
2. https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-uitleg-over-grootschalige-gegevensverwerking-de-zorg

PRIVACY VERIFIED

Verander privacywetgeving in een strategisch wapen

Het vastleggen en managen van uw privacy (AVG/GDPR) is een verplichting die steeds belangrijker is voor uw klanten en partners. Met ons certificeringsprogramma wordt privacy in 3 heldere stappen een onderscheidende propositie van uw organisatie.

Lisette Meij
Directeur ICTRecht Privacy

Demi Grandiek
Juridisch Adviseur

020 6631941
info@privacyverified.nl

Wilt u meer weten over Privacy Verified?
Bezoek onze website:
privacyverified.nl

Zo werken wij thuis!

“Blijf zo veel mogelijk thuis” is het advies dat we heel wat weken nageleefd hebben. Of we nu aan het werk waren, naar een serie keken of gingen sporten; alles vond plaats op dezelfde vertrouwde vierkante meters. Zo gold dit ook voor onze collega's Simone, Viola en Martijn. We hebben aan hun gevraagd: hoe creëer je een fijne thuiswerkplek? En wat mis je nu eigenlijk van het kantoorleven? We laten u graag zien hoe de medewerkers van ICTRecht thuiswerken.

Werkplek Simone

Simone Wessels – Office manager
Als Office manager was het thuiswerken in het begin wel even een omschakeling voor Simone. Zo moest de telefoon worden omgezet en verhuisde haar tweede computerbeeldscherm van kantoor naar huis. Sinds dit alles geregeld is, kan Simone prima vanuit huis werken. Wel zijn haar werkzaamheden nu anders: “Op kantoor zet ik onder meer iedere dag de lunch klaar, maar dat is natuurlijk nu niet nodig. Dit geeft mij ruimte om andere taken op te pakken die anders bleven liggen. Zo ben ik momenteel bezig met het updaten van het handboek voor ons team, wat ook erg leuk is om mee bezig te zijn.”

Simone heeft thuis een vaste werkplek ingericht: “Ik had nog een bureautafel en -stoel staan van mijn studie, dus die kwamen nu weer goed van pas. Ik heb alles neergezet in de woonkamer wat ik toch wel de fijnste plek vind om te werken. Hier heb ik lekker de ruimte en het is daarnaast een lichte kamer, dat vind ik belangrijk. Als de zon schijnt, vind ik het dan ook heerlijk als die deels op mij schijnt tijdens het werken.”

Ondanks dat we niet meer op kantoor aan het werk zijn, hoeft het contact met collega’s niet te verwateren: “Doordat ik binnenkomende telefoontjes vaak doorverbind spreek ik eigenlijk nog alle collega’s, wat prettig is. Zo blijf ik toch nog een beetje met iedereen in contact. Maar ik mis de gezellige momenten die ik anders met collega’s op kantoor heb wel hoor! Daarnaast beweeg ik een stuk minder sinds ik thuiswerk dus ga ik vaak even drinken halen om zo toch even te kunnen lopen. In de lunchpauze fiets ik (bijna) iedere dag naar het werk van mijn man om daar mee te lunchen. Zo ben ik er echt even uit en kan ik even lekker buiten zijn. Wat mij betreft een echte aanrader!”

Viola de Boer – Juridisch adviseur
Het thuiswerken bevalt Viola goed, want geen reistijd meer en efficiëntere werkuren: “Ik win zo twee uur per dag doordat ik nu niet hoef te reizen. Voorheen reisde ik altijd met het openbaar vervoer en dat kan best stressvol zijn. Dit is natuurlijk nu volledig weggevallen. Wel probeer ik gedurende deze periode om mijn routine er goed in te houden door dagelijks op hetzelfde tijdstip op te staan. Verder heb ik tijdens het thuiswerken weinig afleiding waardoor ik mijn werkuren erg doeltreffend kan benutten.”

Viola maakt onderdeel uit van ICTRecht Detachering en werkt een groot deel van haar week voor een opdrachtgever. De opdracht loopt gelukkig nog steeds door, maar dan vanuit huis: “Ik werk al een lange tijd

Werkplek Viola

voor deze opdrachtgever, dus ik weet precies hoe de organisatie in elkaar zit en zij weten wat ze aan mij hebben, hierdoor kan de samenwerking ook op afstand prima doorgang vinden. In het begin merkte je dat iedereen moest wennen aan het videobellen en waren er wat technische uitdagingen. Het is leuk om te zien dat het op dit moment best soepel verloopt en mensen eraan gewend raken. Eerder liep ik bij iemand binnen als ik een vraag had, maar inmiddels ervaar ik het als net zo makkelijk om even iemand te videobellen. We weten elkaar goed te vinden."

Naast voordelen neemt het thuiswerken natuurlijk ook nadelen met zich mee zoals minder sociaal contact met collega's. Vooral haar collega's van ICTRecht Detachering spreekt Viola nu minder dan normaal en dat mist ze wel. De opdrachtgever van Viola organiseert twee keer per week een vast momentje waarin ze even kan bijpraten met haar team en er is een online pubquiz georganiseerd: "Zowel ICTRecht als mijn opdrachtgever doen hun best om iedereen zoveel mogelijk te faciliteren, helpen en steunen. Zo heeft ICTRecht mijn bureaustoel bij mij thuis laten afleveren waardoor ik nu een prima thuiswerkplek heb om ongestoord aan het werk te kunnen gaan!"

Martijn Michael – Juridisch adviseur
Onze Martijn omschrijft het thuiswerken als erg wennen, maar natuurlijk ziet ook hij de voordelen ervan in: "Op den duur went natuurlijk alles. Ik kan nu langer in mijn bed blijven liggen, ik werk flexibeler en krijg veel meer gedaan door thuis te werken, maar het gevaar is direct ook dat ik vaak langer doorwerk en ik zit continu op dezelfde plaats. De grens tussen werk en privé is totaal verdwenen door het thuiswerken en dat heeft twee kanten."

"Het samen lunchen met collega's of het even bij een collega kunnen binnenlopen mis ik het meest", aldus Martijn. Martijn maakt onderdeel uit van het Cloud-team binnen ICTRecht, onderling organiseren zij momenteel online sociale momentjes. Toch merkt hij nu dat het moeilijk is om even tijd vrij te maken voor andere dingen als hij eenmaal aan het werk is op zijn kamer: "Op kantoor hadden we altijd een vast moment waarop we gingen lunchen, nu ik vanuit huis werk, vergeet ik regelmatig om te lunchen. Dat is wel lastig. Daarnaast schieten de sociale momenten er bij mij vaak in doordat ik toch wel merk dat de drempel nu hoger ligt om gewoon even bij te kletsen."

Martijn werkt vanuit zijn kamer. Zijn werkplek ziet er ongeveer net zo uit als op kantoor, maar wel heeft hij geprobeerd om met meubels zijn werkplek te scheiden van de rest van zijn kamer, waardoor hij beide werelden toch een beetje van elkaar kan afsluiten. Het creëren van een fijne thuiswerkplek is belangrijk want het thuiswerken blijft een rol spelen in de toekomst verwacht Martijn: "De coronacrisis heeft de ogen van vele bedrijven geopend omtrent de mogelijkheden voor thuiswerken en de efficiëntie die het met zich meebrengt. Fysiek contact zal altijd belangrijk blijven, maar er zou meer gewerkt kunnen worden met flexwerk systemen. We hebben immers aangetoond dat het bedrijf op afstand succesvol functioneert en dat kan een nieuwe stap zijn. De situatie waar we momenteel in verkeren vormt daarvan een begin denk ik."

Werkplek Martijn

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Internetrechtspraak

Gerechtshof Amsterdam 3 maart 2020
(Online nieuwsarchief)
In 1999 verscheen in de Volkskrant een artikel met de kop "Piramidespel Eurobizz Diamond is failliet". Het artikel noemt ook de naam van de voorzitter, en blijkt zonder belemmering te vinden in het online archief van de krant. Ook een Google search op deze naam levert een directe link. De oud-voorzitter stapt naar de rechter omdat hij zichzelf aldus nog steeds geassocieerd ziet met dit piramidespel. Hij eist verwijdering uit het archief wegens onrechtmatige perspublicatie, en doet ook een beroep op de Wbp. Beide eisen worden afgewezen nu er voldoende steun was in het feitenmateriaal en de beschuldigingen de organisatie betreffen, niet hem als persoon. Het online houden van een oud artikel met naam en toenaam is niet op zich onrechtmatig.

https://bit.ly/3eOigY2

Rechtbank Amsterdam 9 maart 2020
(Airbnb dient twee heren)
Een Nederlandse huurder had ruim € 500,- aan servicekosten betaald aan Airbnb. In de Nederlandse wet staat dat een bemiddelaar tussen twee partijen niet zomaar van beiden een vergoeding mag vragen (art. 7:417 BW, het "verbod op dienen van twee heren"). Doel hiervan is belangenverstrengeling te voorkomen: namens de verhuurder wil je bijvoorbeeld zo veel mogelijk huur vragen, en namens de huurder de goedkoopste deal. En dan ook nog eens van beiden een courtage vangen, dat werkt niet. Airbnb vraagt van beide partijen een vergoeding, weliswaar noemt men dit servicekosten maar de rechter prikt daar doorheen. De e-commercerichtlijn staat niet aan dit verbod in de weg. Vanwege het te lage procesbelang is hoger beroep of cassatie niet mogelijk; diverse organisaties hebben al massaclaims tegen Airbnb aangekondigd.

https://bit.ly/376ngV5

Rechtbank Amsterdam 12 maart 2020 (Foto-inbreuk)
Een receptensite publiceert een foto van gevulde eieren in tableau, waarna de fotograaf een factuur voor € 371,- stuurt. Dit bedrag is opgebouwd als licentie-inkomsten plus verlies van exclusiviteit en buitengerechtelijke kosten, plus een vordering voor proceskosten (1019 Rv). Gedaagde stelt dat de foto geëmbed is, wat toch volgens Europese jurisprudentie (Svensson) legaal is. De rechtbank ziet dat anders: omdat de foto zichtbaar is als deel van de website van gedaagde, heeft zij deze opnieuw openbaar gemaakt en moet zij dus betalen. De rechtbank wijst de licentie-inkomsten toe plus de buitengerechtelijke kosten.

https://bit.ly/3h2FlYG

Rechtbank Amsterdam 17 maart 2020
(Vuurwapens op filmpjes)
Verdachte werd aangehouden in het kader van onderzoek naar een liquidatie. Op zijn telefoon werden diverse filmpjes aangetroffen waarin hij vuurwapens voorhanden had. De filmpjes tonen ook dure merkschoenen en -tassen die op andere foto's door verdachte gedragen werden. DNA op de bij een huiszoeking aangetroffen vuurwapens in combinatie met de filmpjes levert genoeg bewijs op van bezit van vuurwapens.

https://bit.ly/2Y9uvYm

Hoge Raad 17 maart 2020 (Internetoplichting)
Internetoplichting door op Facebook goederen op het gebied van licht- en geluidtechniek aan te bieden maar niet te leveren, art. 326.1 Sr. Bewijsklachten daderschap en pleegplaats. Uit bewijsvoering kan - zonder nadere motivering - die ontbreekt, nog niet met voldoende mate van nauwkeurigheid worden afgeleid dat het verdachte is geweest die aangevers heeft bewogen tot betaling van geldbedragen door gebruik te maken van bewezenverklaarde oplichtingsmiddelen en dat Renkum daarvan pleegplaats was. Volgt vernietiging en terugwijzing.

https://bit.ly/2XCYEQV

Rechtbank Amsterdam 23 maart 2020
(Afsluitkosten internetaansluiting)
Eisende partij heeft gesteld dat zij, althans haar rechtsvoorganger UPC, met gedaagde partij per 1 oktober 1999 een overeenkomst heeft gesloten, die per 5 maart 2018 is gewijzigd in die zin dat gedaagde partij toen is overgestapt op een ander pakket te weten het Connect Complete en Play Max Pakket. Deze wijziging is aan gedaagde partij bevestigd bij e-mail. De overeenkomst is per 15 augustus 2018 beëindigd wegens wanbetaling. Eisende partij heeft verder gesteld dat de overeenkomst online is gesloten. Eiser kan echter niet aantonen dat aan haar informatieplichten is voldaan, met name dat meer is gedaan dan naar algemene voorwaarden te verwijzen. Onder meer ontbreekt de ingangsdatum, de gebruikskosten en de afsluit- en retourkosten van de mediabox. De rechtbank staat incasso van de helft van de kosten toe.

https://bit.ly/3gXIpp7

Hoge Raad 24 maart 2020
(ACAB nu wel algemeen bekend)
Belediging van politieambtenaar door voorafgaand aan voetbalwedstrijd in Amsterdam lettercombinatie 'ACAB' te zingen, art. 266.1 jo. 267.2 Sr. Discussiepunt is al geruime tijd of algemeen bekend is dat dit "All cops are bastards" betekent. In eerdere zaak (2011) bepaalde Hoge Raad van niet, onder meer omdat het Hof destijds zelf was gaan googelen en daarbij resultaten van ná het feit had betrokken in haar oordeel. Nieuws over deze zaak maakte, aldus de HR, deze betekenis ondertussen van algemene bekendheid. Het oordeel dat de verdachte 'opzettelijk' politieambtenaar [verbalisant 1] heeft beledigd door het zingen van de leus 'ACAB', is aldus niet onbegrijpelijk en toereikend gemotiveerd. (Vgl. HR 11 juni 2019, ECLI:NL:HR:2019:899.)

https://bit.ly/3dFh1dA

Rechtbank Den Haag 25 maart 2020
(Merkgebruik op internetaankopen)
Easycosmetic is verkoper van parfum- en cosmeticaproducten van ruim 250 verschillende merken. Voor de verzending van via internet verkochte producten aan haar klanten maakte de organisatie gebruik van verpakkingsdozen waarin in totaal 80 tekens gelijk aan verschillende merken worden afgebeeld. Coty (actief in de markt van parfumproducten, cosmetica en huidverzorging en verantwoordelijk voor de handhaving van intellectuele eigendomsrechten) sommeerde Easycosmetic het gebruik van de merken op de verpakkingsdozen te staken. Het Hof oordeelt de reden van Coty als gegrond en beveelt Easycosmetic iedere inbreuk op de merken te staken en gestaakt te houden.

https://bit.ly/3dCmrpK

Rechtbank Midden-Nederland 26 maart 2020
(MijnDUO als bekendmaking)
Plaatsen van een besluit op MIJNDUO is een andere geschikte wijze van bekendmaken zoals bedoeld in artikel 3:41, 2e lid, van de Awb. Verweerder heeft besluit daarom op de juiste wijze bekendgemaakt. Het bezwaar van eiser is daarom te laat ingediend.

https://bit.ly/2UgxE7P

Rechtbank Noord-Holland 30 maart 2020
(YouTube-uitlatingen)
Eiseres (autohandelaar) vordert staking uitlatingen van gedaagde (klant) op reviewsites en in YouTube-filmpjes dat eiseres zou 'spelen met de kilometerstanden' en op andere wijze fraude zou bedrijven. Voorzieningenrechter acht een deel van de uitlatingen onrechtmatig, wegens gebrek aan steun in beschikbare feitenmateriaal. Andere video's mogen blijven staan.

https://bit.ly/2XCyOw9

Rechtbank Rotterdam 3 april 2020
(Bewijsopdracht internetovereenkomst)
Op naam van gedaagde is online een overeenkomst met Tele2 gesloten voor een 24-maanden telefonie abonnement plus een iPhone 7 ter waarde van € 768,-. Nadat niet wordt betaald, start Tele2 een incassoprocedure. Gedaagde stelt nooit de overeenkomst te hebben gesloten en dat een ander (mogelijk de ex-partner) zijn gegevens heeft gebruikt. De rechtbank legt de bewijslast bij Tele2 dat het wel degelijk gedaagde was. De kopie identiteitsbewijs + bankpas levert niets op, want er is geen controle uitgevoerd wie deze heeft aangeleverd. Bij de handtekening onder het contract staat "i.o." en een betaling van 1 cent bewijst ook niet dat het gedaagde was. Tele2 mag nader bewijs leveren; ik ben zeer benieuwd.

https://bit.ly/30htfFg

Gerechtshof 's-Hertogenbosch 7 april 2020
(Colportage bij bakkerij)
Een bakkerij kreeg in de winkel het aanbod een website en app te laten bouwen. Na een geschil over de kwaliteit wil de bakkerij van de overeenkomst af, maar faalt in haar beroep op de Colportagewet. Het Hof toetst wel de algemene voorwaarden met reflexwerking naar de

kleine ondernemer in het achterhoofd, maar ziet geen onredelijke bezwarendheid in de duur van de overeenkomst. Ook een beroep op art. 7:408 mag niet slagen omdat expliciet een niet-reduceerbare termijn is overeengekomen.

https://bit.ly/3ha7VaW

Gerechtshof Amsterdam 7 april 2020
(Idee toesturen)
Eiser in de zaak heeft in 2012 de Rabobank benaderd met een idee: *"Om de gevolgen van skimmen (…) drastisch te beperken zo niet geheel te voorkomen".* Hij stuurt tevens een e-mail met nadere beschrijving van het idee, en verlangt provisie van vijf jaar lang een redelijk percentage van de besparingen. De Rabobank gaat na een eerste discussie niet in op zijn voorstel. In 2012 verschijnen media-berichten van een nieuwe beveiliging van de Rabobank, die behoorlijk lijkt op het voorgelegde idee. Allereerst blijkt geen geheimhouding overeengekomen, en heeft de Rabobank aangetoond al sinds 2011 bezig te zijn met haar nieuwe techniek. De vorderingen worden afgewezen.

https://bit.ly/2Y5nXtL

Centrale Raad van Beroep 14 april 2020
(Handel via Marktplaats versus bijstand)
Een burger ontvangt bijstand. De gemeente stelt onderzoek in naar aanleiding van een melding dat hij zijn oude bedrijf (export van tweedehands artikelen) nog voortzet. Het onderzoek laat 742 advertenties op Marktplaats zien, de inkomsten hieruit zijn niet gemeld, net zo min als de handel zelf. De burger stelt dat nog geen sprake was van handel, omdat er niets verkocht was en volgens de rechtspraak pas melding verplicht is als er wezenlijke verdiensten worden gemaakt (ECLI:NL:CRVB:2010:BM9097). De CRB merkt de advertenties aan als handelsactiviteiten, en constateert dat melding wel degelijk moet wanneer men begint bij de handel, ook al wordt er nog geen omzet gemaakt.

https://bit.ly/30eapyR

Rechtbank Den Haag 22 april 2020
(Licentie medische software)
Een praktijk voor gynaecologische en verloskundige diagnoses en behandelingen neemt een licentie af op een medisch softwarepakket voor praktijkondersteuning. In de implementatie blijkt een verschil van inzicht tussen partijen over de benodigde hardware en wie de kosten daarvan moet dragen. De rechtbank constateert dat de grootste risico's hiervan bij de praktijk moeten liggen gezien de voorlichting en afspraken in het contract. De praktijk doet vervolgens een beroep op dwaling, omdat zij nooit akkoord zou zijn gegaan als zij inderdaad al die implementatie (en kosten) zelf had moeten dragen nog bovenop het geoffreerde. De rechtbank wijst dit af; er is genoeg over de kosten en randvoorwaarden gesproken. Wel wordt het aantal concurrent users waarvoor gefactureerd wordt beperkt, omdat dit niet duidelijk genoeg nader overeengekomen is.

https://bit.ly/3cDMont

Rechtbank Rotterdam 24 april 2020
(Bewijs internetcontract)
Ziggo eist van een consument betaling van een abonnementsom. Gedaagde stelt dat hij geen contract heeft afgesloten omdat hij al een contract met KPN heeft en zijn coaxkabel slechts één levering van internet aankan. KPN weerlegt desgevraagd deze technische stelling. Bovendien blijkt dat het installatiepakket is aangenomen (met handtekening), en dat facturen van Ziggo zijn betaald. Dat [gedaagde] kampte met gezondheidsproblemen waardoor hij niet goed wist wat hij deed en daardoor ook de bevestigingsmail niet heeft gelezen komt, hoe vervelend ook, voor rekening en risico van [gedaagde] en kan niet aan Ziggo worden tegengeworpen.

https://bit.ly/2BEZNik

Rechtbank Amsterdam 24 april 2020
(Holyboot vs The Holy Boat)
Eenmanszaak Holyboot (een woordspeling op de plaatsnaam Holysloot) verhuurt fluisterboten voor tot zes personen, en gebruikt de naam 'holyboot' en 'Holyboat' op internet. Gedaagde is Holy Boat bv en handelt onder "The Holy Boat" in de verhuur van boten tot 40 personen, waarbij deel van de formule is dat men cannabis mag roken aan boord. Eiser ziet dit als verwarringwekkend gebruik van haar handelsnaam, zeker omdat op internet bij zoeken op "holy boat/boot" beide partijen snel boven water komen. De rechtbank is het daarmee eens; beide partijen bieden recreatie op het water aan met verhuurboten. Dat de doelgroepen niet exact hetzelfde zijn (The Holy Boat richt zich meer op jongeren in de binnenstad van Amsterdam) doet daaraan niet af. De rechtbank verbiedt het verder gebruik van de handelsnaam maar legt geen dwangsommen op, omdat het bedrijf van gedaagde vanwege de coronacrisis toch al stilligt.

https://bit.ly/3eVxBWF

Rechtbank Noord-Nederland 28 april 2020
(Niet-anoniem vonnis)
Eiser heeft een huurcontract voor een woning met verhuurder Nijestee. Bij vonnis van de voorzieningenrechter van de rechtbank Noord-Nederland van 23 juni 2017 is eiser veroordeeld om haar woning te ontruimen en ter vrije beschikking te stellen van Nijestee gedurende de periode dat Nijestee aan de woning de geplande werkzaamheden verricht en de woning gedurende de uitvoering van de geplande werkzaamheden niet te betreden. Het vonnis wordt door Nijestee aan andere partijen gegeven, kennelijk om druk te zetten op deze anderen om wél mee te werken aan deze werkzaamheden. De rechtbank verklaart dit in strijd met de AVG omdat het vonnis niet geanonimiseerd is.

https://bit.ly/2AGv1oT

Rechtbank Den Haag 30 april 2020
(IP adressen identificeren)
Stichting Brein vordert het verstrekken van identificerende gegevens door gedaagde als serverprovider van klanten die via IP-adressen inbreuk maken op auteursrechten van eiseres. Aan de vereisten van artikel 843a Rv is ten dele voldaan, alleen zijn de gevorderde gegevens te onbepaald in omvang en tijd. Slechts de NAW-gegevens plus e-mailadressen en KVK-nummers (m.b.t. ondernemingen) hoeven te worden verstrekt en alleen voor de tijdspanne waarin (vooralsnog) vaststaat dat via de IP-adressen van gedaagde inbreuk is gemaakt op de (naar voorlopig oordeel aangenomen) auteursrechten van eiseres. Aan de vereisten onder de AVG is eveneens voldaan.

https://bit.ly/3gXgN3n

Rechtbank Rotterdam 1 mei 2020
(Bruidsfoto's op Pinterest)
Een bruidsfotograaf overlegt met het stel na afloop over publicatie van enkele foto's op zijn website van de 'romantische fotoshoot met een sexy randje'. Per mail wordt over drie foto's gesproken, waarna blijkt dat er zeven foto's worden gepubliceerd op zowel de site als op Facebook, Instagram en Pinterest. Het stel spreekt de fotograaf aan op schending portretrecht. Het gaat hier om foto's in opdracht, dus geldt het sterke portretrecht (toestemming) van artikel 19 Auteurswet. De rechtbank oordeelt dat de vrouw voldoende herkenbaar in beeld was, ondanks dat haar gezicht een aantal malen is weggelaten. De publicatie is derhalve onrechtmatig nu toestemming ontbreekt. De schade wordt begroot op € 1.500,-, mede gezien het zeer intieme karakter van de shoot en de duidelijke belofte dat de foto's privé zullen blijven.

https://bit.ly/2XE0Zed

Hoge Raad 12 mei 2020
(Skydrive geen gegevensdrager)
Bij een kinderporno-zaak wordt in de tenlastenlegging bewezen verklaard dat verdachte "een gegevensdrager, (...) te weten een digitale opslagruimte (Skydrive)" in zijn bezit heeft gehad. Echter, in geval van digitale opslag door gebruik van een clouddienst moet onderscheid worden gemaakt tussen de aldus voor de gebruiker beschikbare digitale opslagruimte en de gegevensdrager waarop die opslagruimte zich bevindt. Mede in aanmerking genomen dat het Hof heeft miskend dat de term 'bezit' a.b.i. art. 240b Sr volgens de wetsgeschiedenis een fysieke connotatie heeft. Nu tevens is bewezenverklaard het in bezit hebben van een laptop, behoeft dit evenwel niet tot cassatie te leiden. Hierbij in aanmerking genomen dat, indien het gewraakte onderdeel uit de bewezenverklaring vervalt, de aard en de ernst van hetgeen is bewezenverklaard in zijn geheel beschouwd niet worden aangetast, terwijl ook de kwalificatie van het bewezenverklaarde ongewijzigd blijft.

https://bit.ly/2Bx6Nh0

Hoge Raad 12 mei 2020
(Verbeurdverklaarde bitcoins)
Verdachte is eerder veroordeeld voor onder meer diefstal van elektriciteit, dit in verband met illegale hennepkweek. Bij de aanhouding is een computer voor het minen van bitcoins in beslag genomen, alsook diverse bitcoins zelf. In cassatie wordt geklaagd dat deze apparatuur geen "voorwerp waarmee het feit begaan is", omdat de diefstal van elektriciteit niet door deze comptuers gebeurde. De HR doet de zaak op artikel 81 RO af en bevestigt daarmee het oordeel van het Hof.

https://bit.ly/2XDlE2j

Rechtbank Gelderland 13 mei 2020
(Foto's kleinkinderen)
Eiseres is de dochter van gedaagde. Vanwege een ruzie hebben partijen al ruim een jaar geen contact meer met elkaar. De oma publiceert desondanks foto's van kleinkinderen, en wordt door de dochter aangesproken wegens schending van de AVG. De rechtbank acht de AVG inderdaad van toepassing; dit is geen huishoudelijke

of particuliere publicatie meer omdat de foto's publiek zijn. Daarnaast is bij Facebook niet uit te sluiten dat geplaatste foto's verspreid kunnen worden en in handen van derden kunnen komen. In strijd met de wet verklaart de rechtbank vervolgens dat altijd ouderlijke toestemming nodig is bij foto's van personen onder de 16 (het is namelijk: áls toestemming de grondslag is, dán is toestemming ouders nodig). De oma mag de foto's niet meer publiceren.

https://bit.ly/3f0uUTF

Rechtbank Amsterdam 15 mei 2020
(Facebook advertenties)
Internetplatform Facebook treft vooralsnog voldoende maatregelen om nep-bitcoin advertenties met bekende Nederlanders te weren. Alleen vordering tot het verstrekken van identificerende gegevens van adverteerders is toegewezen.

https://bit.ly/30qPGYX

Rechtbank Oost-Brabant 18 mei 2020
(Reviews op Google Maps)
Eiser wordt geconfronteerd met reviews op Google Maps, die hij kan herleiden tot betrokkenen in een geschil waarvoor hij als deskundige eerder een deskundigenbericht heeft opgesteld. Gedaagden ontkennen dat zij achter een deel van de reviews schuilgaan en stellen dat zij door het plaatsen van de reviews het publiek belang dienen. Geoordeeld wordt dat uit de inhoud en timing van publicatie van de reviews blijkt dat gedaagden de reviews hebben geplaatst. Hoewel men zich kritisch en opiniërend mag uitlaten in een recensie of review, zijn bepaalde in de betrokken reviews vermelde feiten onjuist en bedienen gedaagden zich van kwalificaties met een sterk feitelijk karakter, die gedaagden niet of onvoldoende onderbouwen. Bovendien hebben gedaagden er bewust voor gekozen om de reviews op het medium Google Maps te plaatsen, waardoor zij een groot publiek zouden (kunnen) bereiken. Het gevorderde bevel tot verwijdering en het verbod worden toegewezen.

https://bit.ly/30e4Z75

Hoge Raad 26 mei 2020
(YouTube geen algemene bekendheid)
In een helingszaak had het Gerechtshof geoordeeld dat "een contactslot van een scooter/bromfiets met bouten is vastgemaakt en eerst kan worden verwijderd en/of vervangen door de plastic kap van het voertuig los te schroeven" kan worden aangemerkt als een feit van algemene bekendheid. Dit op basis van aan YouTube (opmerkelijk genoeg als "you tube" geschreven) ontleende video's. Dit deel van de motivatie is volgens de HR onbegrijpelijk, omdat het gaat om één bron en er geen gelegenheid tot reageren is geweest (vgl. ECLI:NL:HR:2011:BP0291). Een en ander leidt wegens gebrek aan belang niet tot cassatie, nu de bewezenverklaring ook met weglating van het onderdeel in de nadere bewijsoverweging over de wijze waarop een contactslot van een scooter is vastgemaakt en kan worden verwijderd, toereikend is gemotiveerd. Zie de noot op pagina 32.

https://bit.ly/3dCopGE

Hoge Raad 26 mei 2020 (Phishing-fraude)
Medeplegen van computervredebreuk (art. 138ab Sr), medeplegen (poging tot) diefstal d.m.v. valse sleutel (art. 311.1.5 Sr), medeplegen (poging tot) oplichting (art. 326 Sr), deelname aan criminele organisatie die zich richt op het plegen van phishing, oplichting en diefstal. (art. 140.1.Sr).

https://bit.ly/3cBBa2U

ICTRECHT
academy

Online IT Law Summer School

Duik mee in de toekomst van het ICT-recht!

Start 28 juli 2020.

Wilt u deze zomer écht iets nieuws leren op het snijvlak van recht en techniek? De ICTRecht Academy daagt u uit om deel te nemen aan de IT Law Summer School. Onze algemeen directeur en ICT-jurist Arnoud Engelfriet neemt u op unieke wijze mee in de toekomst van het ICT-recht. Voor zowel juristen als IT'ers.

Schrijf u nu in via
ictrecht.nl/it-law-summer-school

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Noot bij Hoge Raad 26 mei 2020 (YouTube geen algemene bekendheid)

Wanneer kan men internetbronnen gebruiken als rechtbank, en maakt het daarbij uit of men zoekt naar feiten van algemene bekendheid? Die vraag speelt al enige tijd, en in twee recente rechtszaken kwam de vraag weer langs. Daarom even de gelegenheid om een en ander weer op te frissen.

De recentste zaak is ECLI:NL:HR:2020:916, waarin de Hoge Raad ingaat op de overweging van het Hof dat "een contactslot van een scooter/bromfiets met bouten is vastgemaakt en eerst kan worden verwijderd en/of vervangen door de plastic kap van het voertuig los te schroeven" kan worden aangemerkt als een feit van algemene bekendheid. Het Hof was daarbij uitgegaan van YouTube-video's (opmerkelijk genoeg als "you tube" geschreven). Dit in het kader van een discussie of het contactslot door een val kon zijn afgebroken, wat als deel van een verweer tegen heling was gebruikt (een bromfiets zonder contactslot voelt meer evident dan een gestolen bromfiets immers).

Op grond van artikel 339 lid 2 van het Wetboek van Strafvordering (hierna: Sv) behoeven feiten of omstandigheden van algemene bekendheid geen bewijs. Kort gezegd gaat het om gegevens die ieder van de rechtstreeks bij het geding betrokkenen, geacht moet worden te kennen of die zonder noemenswaardige moeite uit algemeen toegankelijke bronnen te achterhalen zijn. De achterliggende gedachte is dat processen eindeloos zouden worden in omvang en tijd indien alle relevante feitelijkheden in de volste zin van het woord zouden moeten worden bewezen.

In de regel (ECLI:NL:HR:2016:522) is een gegeven dat aan een internetbron is ontleend van algemene bekendheid indien dat gegeven geen specialistische kennis veronderstelt en de juistheid daarvan redelijkerwijs niet voor betwisting vatbaar is. In die zaak had het Hof geoordeeld dat Aloë capensis niet hetzelfde is al Aloë vera en dus niet mag worden ingevoerd. Het Hof had gebaseerd op gegevens die het had ontleend aan: "Bronnen op het internet die uit dien hoofde als algemeen bekend worden verondersteld althans in elk geval in de onderhavige procedure".

Een voorbeeld is ECLI:NL:HR:2018:1125. In deze zaak had het Hof via Google Maps de plaatselijke gesteldheid op of aan de openbare weg rondom een voor de zaak relevante plaats vastgesteld. Dit was een feit van algemene bekendheid (in casu: dat de woning van de getuige recht tegenover een schuifhek was gelegen waar een verdachte overheen geklommen was). Voor deze constatering was dus geen nader bewijs nodig. Logisch ook, de situatie op de weg is wat deze is, daar is verder geen discussie over mogelijk.

Echter, de enkele omstandigheid dat een bepaald gegeven aan openbare bronnen op het internet kan worden ontleend, brengt op zichzelf nog niet mee dat zo een gegeven daarom een feit of omstandigheid van algemene bekendheid is in de hier bedoelde zin. Gezien deze uitspraak is het logisch dat ook het Hof in de helingzaak de fout in is gegaan. Dat een YouTube-video laat zien dat een contactslot van een bromfiets goed vastzit, is op zich een feit. Het voelt logisch om te concluderen dat het slot er dan niet zomaar af zal breken bij een val, maar dat is bij lange na nog niet hetzelfde als dat het een feit van algemene bekendheid is.

Geen rechtsregel dwingt de rechter ertoe een algemeen bekend gegeven bij het onderzoek op de terechtzitting

ter sprake te brengen. Indien echter niet zonder meer duidelijk is of het gaat om een algemeen bekend gegeven, behoort de rechter dat gegeven aan de orde te stellen bij de behandeling van de zaak op de terechtzitting. Op die manier wordt voorkomen dat de rechtbank haar beslissing doet steunen op mededelingen of waarnemingen die hem buiten het geding ter kennis zijn gekomen en waarvan de overige bij het geding betrokkenen onkundig zijn gebleven, zodat zij niet in staat zijn geweest zich daarover uit te laten. Indien bij dat onderzoek op de terechtzitting vervolgens het uitdrukkelijk onderbouwde standpunt wordt ingenomen dat en waarom het gegeven niet van algemene bekendheid is, zal de rechter in geval van afwijking van dat standpunt in zijn uitspraak op de voet van art. 359.2 Sv de redenen dienen op te geven die daartoe hebben geleid.

Deze rechtsregel werd geformuleerd in de "ACAB"-zaak uit 2011 (ECLI:NL:HR:2011:BP0291). In die zaak oordeelde het Hof dat de betekenis van de afkorting A.C.A.B. als "All Cops Are Bastards" als een feit van algemene bekendheid heeft te gelden. Dit had het Hof vastgesteld met een zoekopdracht in Google, maar niet vooraf met partijen besproken. Gezien het feit plaatsvond in 2007 en het Hof in 2009 had gegoogeld, ontstond daarbij ook nog eens de complicatie dat het aantal treffers niet doorslaggevend kon zijn: wat was immers de situatie ten tijde van het feit? Nieuws over deze zaak werd zo wijdverbreid opgepakt dat in een latere zaak (ECLI:NL:HR:2019:899, zie ook ECLI:NL:HR:2020:501) de HR oordeelde dat ondertussen de betekenis van deze term wél algemeen bekend was.

Wanneer een rechtbank zelf uitgaat van bronnen van derden, en het betreft géén feiten van algemene bekendheid, dan schendt zij het beginsel van hoor en wederhoor wanneer zij dit pas in het vonnis voor het eerst meldt. In ECLI:NL:HR:2011:BR1654 ontbrak het Hof het aan feiten over een softwarepakket, waarop zij zelf het internet betrad om deze te verwerven ("De bewindvoerder heeft geen informatie overgelegd over de werking van het Smart FMS systeem, maar het internet (www.smartfms.nl) biedt wel enige informatie."). Aldus had de bewindvoerder geen enkele kans gehad te protesteren tegen deze conclusie of te proberen te bewijzen dat dit wél een nuttig systeem voor zijn cliënt was. Al eerder (ECLI:NL:HR:2011:BP5612) had de HR in gelijke zin geoordeeld; het Hof had toen gehandeld in strijd met het beginsel van hoor en wederhoor door eigener beweging verkregen feitelijke gegevens aan zijn beslissing ten grondslag te leggen zonder partijen in de gelegenheid te stellen daarvan kennis te nemen en zich daarover desgewenst uit te laten.

In de praktijk lijkt mij het verstandigste om bij op internet gevonden informatie standaard deze aan partijen voor te leggen, tenzij het gaat om echt zuiver feitelijke informatie waarover geen discussie kan zijn.

Van onze blog

Cloud Contracteren

18 mei 2020

Garanties en vrijwaringen in ICT-contracten

In een ICT-contract leggen leverancier en afnemer de verplichtingen over en weer bij de levering van bepaalde ICT-diensten, vast. Regelmatig wordt gevraagd om de garantie dat de geleverde software vrij van gebreken is. Ook een bepaling waarin de leverancier de afnemer vrijwaart voor claims van derden in verband met inbreuken op intellectuele eigendomsrechten, komt veelvuldig voor.

Garanties en vrijwaringen vormen vaak onderwerp van discussie bij de onderhandelingen over de inhoud van een ICT-contract. Beiden hebben tot gevolg dat de wederpartij zich zeker kan voelen over een bepaalde toezegging of situatie. Maar wat zijn de juridische gevolgen van een dergelijke clausule? Wat is het verschil tussen een garantie en vrijwaring?

Garantie
Een garantie wordt in principe gezien als een versterkte verplichting om een bepaald resultaat te behalen. Wanneer dit resultaat uitblijft, is de leverancier automatisch tekortgeschoten. Een beroep op overmacht is dan niet mogelijk. Dat betekent dat zelfs wanneer er zich een natuurramp heeft voorgedaan waardoor je niet de ICT-diensten kon leveren, je hierachter niet kan verschuilen.

De impact van een garantieclaim kun je wel beperken door een aansprakelijkheidsclausule op te nemen in het ICT-contract. Als je een bepaalde aansprakelijkheidsbeperking overeenkomt (bijvoorbeeld tot een bepaald bedrag of de som van de betaalde vergoedingen over een bepaalde periode), dan geldt die in principe ook bij een garantieclaim. Of men bij een geschonden garantie ook een beroep kan doen op een aansprakelijkheidsbeperking, is echter wel discutabel en hangt af van de bewoordingen in het aansprakelijkheidsartikel en de garantieclausule. Wanneer expliciet wordt opgeschreven dat de aansprakelijkheidsbeperking ook voor de garantie geldt, is er juridisch weinig mis mee.

Vrijwaring
Een vrijwaring houdt kortgezegd in dat je de wederpartij afschermt tegen een claim die een derde bij de wederpartij neerlegt. Dat betekent dat jij de discussie voert met de betreffende derde en –als het zo ver komt- de procedure moet voeren bij de rechter en de kosten moet dragen. Belangrijk om te vermelden is dat een beperking van aansprakelijkheid niet geldt voor een vrijwaring. Daarin verschilt de vrijwaring dus van de garantie. Bij een vrijwaring zal je alle kosten moeten dragen, zoals de schadevergoeding en de advocaatkosten.

Als je bent verzekerd voor aansprakelijkheid, is het maar de vraag of de verzekeraar bij een vrijwaring tot uitkering zal overgaan. Een plicht tot vrijwaring is immers geen verplichting tot het vergoeden van schade. Bij een vrijwaring ga je verder: je betaalt ook de kosten en dergelijke die niet als schade bij jou zouden zijn gekomen.

Opnemen in het contract?
In alle gevallen geldt: het geven (of niet) van een garantie of vrijwaring is een vrije keuze, waar wel iets tegenover moet staan. Je kan ervoor kiezen om de garantie of vrijwaring niet te geven of te beperken, omdat een dergelijke vergaande toezegging bijvoorbeeld niet in verhouding staat tot het bedrag dat de afnemer voor de diensten betaalt. Hoe dan ook blijven garanties en vrijwaringen onderwerpen in een ICT-contract die de nodige aandacht verdienen.

Auteur
Sari Jansen
Juridisch adviseur

25 mei 2020

25 mei: 2 jaar AVG!

Vandaag is het alweer twee jaar geleden dat de Algemene verordening gegevensbescherming (AVG) van toepassing werd. Een mooie kans om terug te blikken op wat er gebeurd is de afgelopen twee jaar, waarin de toezichthouder en de rechter niet hebben stilgezeten. In deze blog vertellen we u over het werk (en de werklast van de Autoriteit Persoonsgegevens (AP), de manier waarop rechters hebben besloten over betaling van schadevergoeding aan personen voor privacy-schendingen en de toekomst van data-uitwisseling met de Verenigde Staten (mag dat straks nog wel?).

Meer privacy-bewustzijn
Zeker vanaf de intrede, maar eigenlijk al sinds de aankondiging van de AVG is het privacy-bewustzijn in Nederland in ieder geval sterk gegroeid. Burgers worden duidelijk mondiger en zijn zich meer bewust van hun rechten. Dat blijkt in ieder geval al uit het nog immer stijgende aantal klachten dat de AP ontvangt.[1] Hoewel de toezichthouder blij is dat burgers haar weten te vinden, wordt er zo veel beroep op haar gedaan dat zij de drukte niet aan kan.[2]

Ondanks de drukte, heeft de AP wel van zich laten horen. Eind vorig jaar heeft bijvoorbeeld een omvangrijk onderzoek plaatsgevonden naar het gebruik van cookies op websites.[3] Belangrijk om te weten is dat een onderzoek niet per definitie in een boete hoeft te eindigen. Uiteindelijk ligt het belang van de AP bij het juist naleven van de privacywetgeving, en kúnnen organisaties er met de schrik vanaf komen indien zij alle medewerking verlenen en de inbreukmakende processen binnen gegeven korte tijd aanpassen en verbeteren. Uiteraard kost het nog altijd meer moeite en tijd om te genezen dan om te voorkomen.

1. https://autoriteitpersoonsgegevens.nl/nl/nieuws/forse-stijging-privacyklachten-2019
2. https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2020D11306&did=2020D11306
3. https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-veel-websites-vragen-op-onjuiste-wijze-toestemming-voor-plaatsen-tracking-cookies

Boetes in Nederland
Mocht een organisatie toch niet voldoen aan de eisen, dan komen de boetes wel de kop op steken. Dat is in Nederland onder de AVG tot nu toe drie keer gebeurd.

Een boete werd bijvoorbeeld uitgedeeld aan het Haga Ziekenhuis, die de interne beveiliging van patiëntendossiers niet goed op orde had. Er kon daardoor onder andere door een groot aantal ziekenhuismedewerkers in het dossier van de BN'er Barbie worden gekeken. In maart dit jaar werd een tweede AVG-boete opgelegd aan tennisbond KNLTB voor het verkopen van ledenlijsten aan sponsors. De laatste en hoogste boete tot nu toe werd uitgedeeld aan een onbekend bedrijf, die bij de rechter anonimiteit heeft bedongen. Deze mysterieuze organisatie heeft € 725.000,- moeten betalen omdat ze de vingerafdrukken van haar werknemers scande (bijzondere persoonsgegevens), zonder de noodzaak hiervan voldoende te kunnen beargumenteren.

De boetes die in 2018 werden uitgedeeld aan Uber en Theodoor Gilissen Bankiers werden nog onder de Wet bescherming persoonsgegevens (Wbp) gewezen. Het grootste verschil met deze oude wet is de hoogte van de boetes: de maximumboete onder de AVG ligt aanzienlijk hoger.

Schadevergoeding voor privacy-schending
De boetes zijn niet het enige handhavingsmechanisme onder de AVG. Onder bepaalde omstandigheden kunnen mensen ook zelf schadevergoeding claimen voor een schending van hun privacy door een bedrijf of de overheid.

In Nederland werd een toekenning van schadevergoeding vanwege schending van de AVG door de gemeente Deventer vernietigd in hoger beroep, omdat niet voldoende was aangetoond dat er nadelige gevolgen waren voor het slachtoffer vanwege de schending. Het UWV moest aan de andere kant wel € 250,- uitkeren wegens de schade die een werkneemster had opgelopen vanwege de privacyschending door het UWV, die bij haar angst- en stressklachten had veroorzaakt. De hoogste schadevergoeding die tot nu toe is toegewezen was voor

een man wiens psychologische en psychiatrische gegevens zonder zijn toestemming aan een medisch tuchtcollege waren verstuurd[4]: hij krijgt € 500,- als immateriële schadevergoeding.

Duidelijk mag zijn dat een schending van privacy niet direct een recht op schadevergoeding doet ontstaan. Wanneer rechters ook bij aangetoonde nadelige gevolgen van de privacyschending slechts zeer magere schadevergoedingen toewijzen, zullen burgers naar verwachting niet snel meer naar de rechter stappen voor schendingen van de AVG vanwege de grote geld- en tijdinvestering die met een gang naar de rechter gemoeid is.

***Privacy Shield* ter discussie**

Dan uiteindelijk nog een zeer interessante zaak waar menig privacy jurist naar uitkijkt: Schrems II. Men hoopt dat het Hof van Justitie van de Europese Unie uitspraak zal doen over zowel de standaardcontractbepalingen van de Europese Commissie en het Privacy Shield. Beide zijn constructies die ervoor zorgen dat persoonsgegevens alsnog kunnen worden verzonden naar landen die geen “passend beschermingsniveau” bieden, dat wil zeggen niet dezelfde privacywaarborgen aanhouden zoals wij die onder de AVG nu kennen in Europa. Mochten beide constructies wegvallen, dan zou het bijvoorbeeld ook ‘illegaal’ worden om persoonsgegevens op te slaan in de Verenigde Staten. Vanwege het grote aantal Amerikaanse clouddiensten in gebruik in Nederland zou dat ook hier mogelijk grote gevolgen hebben. Op 16 juli staat de beoordeling van Schrems II op de agenda!

4. https://www.raadvanstate.nl/actueel/nieuws/@120666/bestuursrechter-kan-vaker/

Auteur
Linde Mensink
Juridisch adviseur

Deze blog is geschreven in samenwerking met Eline Hangelbroek.

1 PUNTEN PO ADVOCATUUR NEDERLANDSE ORDE VAN ADVOCATEN
4 PUNTEN PO ADVOCATUUR NEDERLANDSE ORDE VAN ADVOCATEN
6 PUNTEN PO ADVOCATUUR NEDERLANDSE ORDE VAN ADVOCATEN

Trainingsoverzicht september – december 2020

iapp CPE credits approved

Dinsdag 14 juli
FG Newsflash | Live webinar
Word op de hoogte gebracht van de belangrijkste actualiteiten die voor u als FG in de praktijk relevant zijn. Tijdens de één uur durende live webinar komt onder mee de belangrijkste rechtspraak, berichtgeving van de AP en best practices aan bod. De FG Newsflash wordt verzorgd door twee privacy adviseurs, tevens zelf werkzaam als FG.

https://bit.ly/3htBUuF

Dinsdag 14 juli
AVG rechtspraak update | Live webinar (1 PO)
Op de hoogte blijven van actuele privacy rechtspraak en benieuwd welke lessen hieruit kunnen worden getrokken voor de praktijk? Onder leiding van twee privacy adviseurs wordt tijdens deze één durende live webinar de belangrijkste uitspraken én de essenties hiervan besproken. Daarbij maken we meteen een vertaalslag naar de praktijk.

https://bit.ly/30Phoyu

Dinsdag 29 september
ICT en gezondheidsrecht (6 PO)
Werkt u bij een zorginstelling of bent u een ICT-dienstverlener in de zorg? Vraagt u zich af wat de regels zijn voor het uitwisselen van medische gegevens online en hoe men moet werken in de cloud? U leert het tijdens deze eendaagse training over ICT, beveiliging & privacy in de zorg. De training is geaccrediteerd door ABAN, KNMG-GAIA.

https://bit.ly/37KVuO0

Dinsdag 27 oktober
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/2L1JM86

Dinsdag 3 november
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/3gowsse

Dinsdag 17 november
Update Algemene verordening gegevensbescherming (AVG) (4 PO)
Wij praten u in een middag bij over de belangrijkste recente ontwikkelingen op het gebied van de Algemene verordening gegevensbescherming (AVG). Er worden praktijkvoorbeelden behandeld, onder meer over datalekken en boetes.

https://bit.ly/2OpHt0q

Dinsdag 1 december
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/35LBVU1

Specialiseer u tot FG/DPO

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 als FG/DPO.

Start oktober 2020.

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

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.

Tristan Duchenne
Kwaliteitscoördinator en FG
bij Trubendorffer
Deelnemer opleiding FG/DPO
september 2019

Direct vanuit huis juridische kennis opdoen over ICT, privacy en recht?

Bekijk onze webinars.

Met de webinars van ICTRecht Academy bent u snel op de hoogte van de nieuwste ontwikkelingen. Onze webinars zijn bestemd voor onder meer advocaten, bedrijfsjuristen en technische professionals.

Bekijk ons webinar aanbod op
ictrecht.nl/webinars

Heeft u vragen of wilt u meer weten?

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

Alisa Schurink
Opleidingscoördinator
en Marketingmedewerker

Onze maatregelen tegen Covid-19
Wij houden rekening met alle normen rondom Covid-19. Onze opleidingslocaties nemen maatregelen in acht door onder meer de schoonmaak standaarden uit te breiden en de locaties aan te passen volgens de 1,5 meter afstand regel.


ICTRECHT
adviesbureau