ICTRECHT adviesbureau

ICTRECHT IN DE PRAKTIJK

jaargang 9 nummer 2 april 2021

De online behandelings-overeenkomst

Vergeet uw wachtwoord-(beleid) niet

De geheimen van supermodellen: model-verwerkersovereenkomsten in de praktijk

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

De online behandelingsovereenkomst 4
Vergeet uw wachtwoord(beleid) niet 7
Wet- en regelgeving 10
Nieuwe regels in aankomst voor platformaanbieders 12
Microtargeting tijdens verkiezingscampagnes, macro in de politiek? 15
De geheimen van supermodellen: modelverwerkersovereenkomsten in de praktijk 18
Pas op! Likes kopen, kost geld! 21
Internetrechtspraak 24
Legal tech - Waarom moeilijk doen als het makkelijk kan? 30
Noot bij Gerechtshof Amsterdam 16 februari 2021 - ECLI:NL:GHAMS:2021:392 33
Van onze blog 35
ICTRecht Academy 38

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
Lisette Meij Directeur ICTRecht Privacy
l.meij@ictrecht.nl
Sten Demon Manager Legal & Technology
s.demon@ictrecht.nl
Steven Ras Algemeen directeur
s.ras@ictrecht.nl

Alisa Schurink Marketing adviseur
a.schurink@ictrecht.nl
Bram de Vos Juridisch adviseur
b.devos@ictrecht.nl
Britt Telleman Opleidingscoördinator
b.devos@ictrecht.nl
Dimmen Smolders Juridisch adviseur
d.smolders@ictrecht.nl
Esmée Kuyt Juridisch adviseur
e.kuyt@ictrecht.nl

Jonas van Ginkel Juridisch adviseur
j.vanginkel@ictrecht.nl
Laura Monhemius Juridisch adviseur
l.monhemius@ictrecht.nl
Max Rozendaal Security consultant
m.rozendaal@ictrecht.nl
Menno Konst Juridisch adviseur
m.konst@ictrecht.nl
Nicole Waaijer Marketing adviseur
n.waaijer@ictrecht.nl
Pramila Kramer Juridisch adviseur
p.kramer@ictrecht.nl
Sari Jansen Juridisch adviseur
s.jansen@ictrecht.nl
Eline Pellis Grafisch ontwerper
eline@elinepellis.com
Leonard Fäustle Stills & Motion
Foto's ICTRecht
info@leonardfaustle.nl

Sari Jansen
Juridisch adviseur

E-health

De online behandelings-overeenkomst

U bent tegenwoordig slechts één muisklik verwijderd van een online platform, waar een specialist u eenvoudig en snel kan voorzien van een antwoord op uw medische hulpvraag. De laagdrempeligheid van het op afstand en online verlenen van zorg, heeft echter niet geleid tot het ogenschijnlijk logische gevolg dat bepaalde verplichtingen niet of verminderd gelden. In dit artikel beantwoorden we de vraag of er bij het bieden van online (medische) hulp een behandelingsovereenkomst tot stand komt en zo ja, aan welke (wettelijke) verplichtingen de hulpverlener en diens ICT-leverancier vervolgens moeten voldoen.

De behandelingsovereenkomst

De Wet op de Geneeskundige Behandelingsovereenkomst (WGBO) regelt allerlei randvoorwaarden voor de samenwerking tussen de patiënt en een medisch specialist, in deze wet als 'hulpverlener' aangeduid. De hulpverlener moet bijvoorbeeld op grond van deze wet een medisch dossier inrichten en heeft een informatieplicht jegens zijn patiënt. Daarnaast heeft hij een medisch beroepsgeheim.
De wet is (in ieder geval) van toepassing zodra er sprake is van een behandelingsovereenkomst. Dit is een overeenkomst "waarbij een *hulpverlener* zich, in de uitoefening van een geneeskundig beroep of bedrijf, tegenover een ander verbindt tot het verrichten *van handelingen op het gebied van de geneeskunst,* die *rechtstreeks betrekking hebben op die ander"*.[1]
De relevante onderdelen uit deze definitie worden hierna nader toegelicht.

Hulpverlener

De hulpverlener is degene die een geneeskundig beroep of bedrijf uitoefent. Aanwijzingen voor de kwalificatie als hulpverlener zijn bijvoorbeeld het min of meer regelmatig verrichten van geneeskundige handelingen en het zich naar buiten kenbaar maken als geneeskundige beroepsbeoefenaar. Denk hierbij aan een psychotherapeut, een tandarts of een verpleegkundige. Ook een rechtspersoon, zoals een ziekenhuis, kan een hulpverlener zijn.

Handeling op gebied van geneeskunst

De hulpverlener moet zich verbinden tot het verrichten van een geneeskundige handeling. Dit is een breed begrip. Een geneeskundige handeling kan bijvoorbeeld het stellen van een diagnose, genezen, preventie en verplegen zijn. Ook het antwoord geven op een concrete medische (hulp)vraag is aan te merken als een dergelijke handeling. Onder een geneeskundige handeling wordt namelijk ook het beoordelen en het geven van raad over de gezondheidssituatie verstaan.

Rechtstreeks betrekking

Om te voldoen aan de kwalificatie van een behandelingsovereenkomst, moet er naast een 'hulpverlener' en een 'handeling op het gebied van geneeskunst' ook sprake zijn van individuele gerichtheid. Dit betekent dat de behandelovereenkomst 'rechtstreeks betrekking moet hebben op de persoon'. Rechtstreeks contact tussen hulpverlener en patiënt is hierbij niet nodig.[2]
Als de hulpverlener (een medisch specialist) ingaat op een concrete hulpvraag van een *specifieke* gebruiker van een online platform, dan is er sprake van individuele

1. Artikel 7:446 lid 1 van het Burgerlijk Wetboek.
2. KNMG-richtlijn, Niet-aangaan of beëindiging van de geneeskundige behandelingsovereenkomst, KNMG januari 2021, p.7.

gerichtheid. Er kunnen dus via een online platform behandelingsovereenkomsten tot stand komen. Dat betekent dat de hulpverlener (en ICT-leverancier) aan bepaalde wettelijke plichten moet voldoen.

Informatieplichten dienst van de informatiemaatschappij

Het aanbieden van online medische hulp via een platform is een vorm van online dienstverlening. Dit betekent dat de dienst gekwalificeerd wordt als een dienst van de informatiemaatschappij. Een leverancier van deze diensten, dat kan ook een hulpverlener of zorgaanbieder zijn, is dan verplicht om bepaalde informatie te verstrekken, zoals het KvK-nummer, vestigingsadres, telefoonnummer en btw-nummer. Alle informatie moet op een gemakkelijk vindbare plaats vermeld worden. Daarnaast gelden er aanvullende informatieverplichtingen als er online ook producten of diensten worden verkocht aan consumenten. Daarop geldt een uitzondering als er bepaalde gezondheidsdiensten worden verleend.[3] Hiervan is sprake als een zorgaanbieder in het kader van de geneeskundige behandelingsovereenkomst medische handelingen op afstand verricht. De ICT-leverancier zal doorgaans niet onder deze uitzondering vallen, maar de hulpverlener of zorgaanbieder wel. In plaats van de aanvullende informatieplichten die op grond van het consumentenrecht gelden, geldt het regime uit de WGBO.

Verplichtingen op grond van de WGBO

De behandelingsovereenkomst komt uitsluitend tot stand tussen de gebruiker van een platform en de hulpverlener: het platform zelf is geen partij bij deze overeenkomst. Dat betekent dat de plichten die voortvloeien uit de WGBO gelden voor de hulpverlener en niet voor (de leverancier van) het platform. De leverancier zal wel moeten faciliteren dat de hulpverlener aan haar verplichtingen uit de WGBO kan voldoen. Denk aan verplichtingen als het bieden van adequate hulp en zorg (de zorgplicht, art. 7:453 BW), het informeren van de patiënt op een heldere en adequate wijze (informatie- en overlegplicht, art. 7:448 BW), het bijhouden van een dossier (dossierplicht, art. 7:454 lid 1 en 2 BW), het bewaren van het dossier (bewaarplicht, art. 7:454 lid 3 BW) en het respecteren van de overige patiëntenrechten. Hieruit vloeit onder andere voort dat informatie die via online contact is verkregen van een patiënt in beginsel ook in diens dossier moet worden opgenomen.[4] Dit houdt overigens niet in dat de volledige online gesprekken opgeslagen moeten worden, wel moet de relevante informatie (ook) in het dossier van de patiënt opgenomen worden.

3. Artikel 6:230h lid 2 onder d van het Burgerlijk Wetboek.

Per januari 2020 is de WGBO gewijzigd. De belangrijkste wijzigingen zijn de aanpassing van de bewaar- en aanvangstermijn van het medisch dossier (20 jaar vanaf de laatste wijziging in het dossier); de aanvulling van de informatieplicht van de hulpverlener en het inzagerecht van nabestaanden. Dit geldt ook wanneer de behandelingsovereenkomst via een platform tot stand is gekomen.

Voor het verlenen van online zorg (op afstand) geldt dat indien er nog geen behandelingsrelatie bestaat het eerste consult tussen hulpverlener en patiënt face-to-face plaats dient te vinden. Om de kans op verspreiding van het coronavirus te verkleinen en de druk op zorgaanbieders te verlichten, heeft de Nederlandse Zorgautoriteit (NZa) vorig jaar op deze regel tijdelijk een uitzondering gemaakt. Hulpverleners kunnen het eerste consult met een patiënt nu ook digitaal of telefonisch doen.[5] Het is de bedoeling dat de versoepeling die is doorgevoerd tijdens de coronacrisis, in 2021 een definitieve plek krijgt in de regels.[6]

Gedragsregels

Naast de verplichtingen die voortvloeien uit de WGBO, bestaan er in het kader van de gezondheidszorg verscheidene richtlijnen, protocollen en gedragsregels. Een voorbeeld hiervan is de KNMG-richtlijn 'Omgaan met medische gegevens'.[7] Een dergelijke richtlijn heeft van zichzelf geen bindende kracht, wel is zij behulpzaam bij het interpreteren van wettelijke bepalingen (bijvoorbeeld het recht van de patiënt op informatie of zorg van een goed hulpverlener). Zo wordt in de eerder genoemde KNMG-richtlijn omschreven wanneer een online consult -waarbij de hulpverlener aan de patiënt een individueel medisch advies geeft- is geoorloofd.[8] Dit is ingevolge de richtlijn alleen geoorloofd als er aan een aantal cumulatieve voorwaarden is voldaan, zoals de voorwaarde dat de identiteit van de patiënt voldoende is vastgesteld en de hulpverlener de patiënt voldoende heeft geïnformeerd over de werkwijze bij online contact.

4. KNMG-richtlijn, Omgaan met medische gegevens, KNMG 2020, p.28.
5. Zie: https://www.nza.nl/actueel/nieuws/2020/03/13/nza-past-regelgeving-aan-vanwege-coronavirus
6. Zie: https://www.nza.nl/actueel/nieuws/2020/09/17/zorg-op-afstand-krijgt-structurele-plek-binnen-de-medisch-specialistische-zorg
7. Raadpleegbaar via: https://www.knmg.nl/advies-richtlijnen/dossiers/online-contact.htm
8. Raadpleegbaar via: https://www.knmg.nl/advies-richtlijnen/dossiers/online-contact.htm

Dit jaar zijn er een aantal nieuwe stukken uitgebracht. Zo heeft de KNMG afgelopen januari de vernieuwde richtlijn 'Niet-aangaan of beëindiging van de geneeskundige behandelingsovereenkomst' gepubliceerd, waarin duiding wordt gegeven wanneer de behandelingsovereenkomst kan worden beëindigd.[9] Op grond van de WGBO kan dat immers alleen eenzijdig door de hulpverlener als daar 'gewichtige redenen' voor zijn. In de richtlijn wordt een leidraad gegeven welke ook van toepassing is op behandelingsovereenkomsten die online tot stand zijn gekomen. De richtlijn gaat onder andere in op hoe een behandelingsovereenkomst tot stand komt; welke 'gewichtige redenen' bij eenzijdige opzegging van toepassing kunnen zijn en welke zorgvuldigheidseisen daarbij gelden.

Verder heeft de Patiëntenfederatie Nederland in samenwerking met KNMG, op verzoek van het ministerie van Volksgezondheid, Welzijn en Sport, handen en voeten gegeven aan het inzagerecht in het medisch dossier voor nabestaanden. De Patiëntenfederatie Nederland en KNMG hebben daartoe afgelopen januari een handreiking uitgebracht. Er is een uitgave voor hulpverleners en een uitgave voor patiënten en nabestaanden, met bijbehorende stroomschema's.[10]

Verplichtingen onder de AVG

Naast verplichtingen die gelden op grond van de WGBO en de gedragsregels die zijn neergelegd in richtlijnen voor de gezondheidszorg, dienen de hulpverlener en ICT-leverancier zich uiteraard ook te houden aan de privacywetgeving: de Algemene verordening gegevensbescherming (AVG). Zo is adequate beveiliging van de verwerkte gegevens noodzakelijk. Voor zorgaanbieders geldt dat zij met medische gegevens werken, welke worden aangemerkt als bijzondere persoonsgegevens. Dit brengt een zwaarder regime met zich mee. Ook voor het verwerken van bepaalde gegevens, zoals het Burgerservicenummer en het BIG-nummer, bestaat een apart regime. Niet alleen de leveranciers van de dienst moeten de zwaardere technische en organisatorische maatregelen in acht nemen, ook de zorgaanbieder zelf moet zich bewust zijn van zijn rol en verantwoordelijkheden.

Denk hierbij in ieder geval aan het gebruik van tweefactorauthenticatie bij de toegang tot het platform en daarnaast aan het bij het gebruik van het platform voldoen aan NEN 7510, NEN 7513 en indien relevant: NEN 7512. Verder kunt u denken aan het uitvoeren van een Data Protection Impact Assessment, indien verplicht, en het sluiten van de benodigde verwerkersovereenkomsten. Voorts moet er gebruik gemaakt worden van privacy-by-design en privacy-by-default. Richting de gebruikers van het platform zal een privacyverklaring gehanteerd moeten worden, waarin onder andere duidelijk is omschreven wat er met hun persoonsgegevens gebeurt.

Voor zowel hulpverleners als ICT-leveranciers is het dus van groot belang kritisch te kijken naar de diensten die feitelijk middels een online platform worden geleverd. Afhankelijk hiervan zullen partijen aan bepaalde verplichtingen moeten voldoen, in het bijzonder wanneer er een behandelingsovereenkomst tot stand komt.

9. Raadpleegbaar via: https://www.knmg.nl/actualiteit-opinie/nieuws/nieuwsbericht/vernieuwd-knmg-richtlijn-niet-aangaan-of-beeindiging-van-de-geneeskundige-behandelingsovereenkomst.htm

10. Raadpleegbaar via: https://www.patientenfederatie.nl/actueel/nieuws/handreiking-inzagerecht-nabestaanden

Max Rozendaal
Security consultant

Security

Vergeet uw wachtwoord-(beleid) niet

“Uw wachtwoord is verlopen en moet worden veranderd.” Wie heeft deze melding niet gezien op een maandagochtend net voor een belangrijke vergadering? Of de IT-helpdesk moeten bellen na een vakantie omdat een account geblokkeerd is omdat het wachtwoord niet tijdig is veranderd?

Wachtwoordbeleid, waarom doen we het zo?
Een van de hoekstenen van menig wachtwoordbeleid is het periodiek verplicht veranderen van het wachtwoord. Ook bevat wachtwoordbeleid vaak regels over cijfers en speciale tekens die een wachtwoord moet bevatten, en een maximumaantal foutieve inlogpogingen. Is een wachtwoordbeleid met deze regels in 2021 nog wel modern en opgewassen tegen de aanvallen van vandaag de dag? Of zijn er inmiddels betere regels voor een wachtwoordbeleid denkbaar?

In dit artikel wil ik graag een aanzet doen tot het heroverwegen van wachtwoordbeleid, en daarbij gebruiksgemak meewegen. Wachtwoordbeleid is lange tijd gebaseerd geweest op een aanbeveling van het Amerikaanse National Institute of Standards and Technology (NIST) uit 2004.[1] Daarin wordt aanbevolen om wachtwoorden willekeurige hoofdletters en speciale tekens te laten bevatten, en wachtwoorden ten minste iedere 90 dagen te wijzigen.

Moeilijke eisen aan wachtwoorden leiden niet tot sterkere wachtwoorden
Juist deze eisen maken dat mensen wachtwoorden zoals bijvoorbeeld “Wachtw00rd!” aanmaken. Binnen de eisen die gesteld worden aan een wachtwoord is heel eenvoudig een voorspelbaar wachtwoord te verzinnen. Vaak bevatten deze wachtwoord als eerste letter een hoofdletter, karakters zijn vervangen door een daarop lijkend cijfer, en het wachtwoord eindigt met een speciaal teken.

En als het wachtwoord periodiek gewijzigd moet worden? Dan wordt er door de gebruiker gewoon een volgnummer achteraan geplakt. Met de hoeveelheid wachtwoorden die vandaag de dag nodig zijn om werk uit te voeren is het heel begrijpelijk dat mensen zulke wachtwoorden verzinnen. Om de wachtwoorden te onthouden worden deze vaak ook nog eens opgeschreven op post-its en aan het computerscherm gehangen.

Met al deze voorspelbaarheden maken we het een hacker wel erg makkelijk om in te breken in de organisatie. Voor een hacker is het namelijk niet heel moeilijk om met behulp van woordenlijsten deze veel voorkomende variaties te genereren, en geautomatiseerd te proberen. En wanneer een database waarin wachtwoorden zijn opgeslagen gelekt is, is deze aanval niet te verhinderen door een account na een aantal foutieve inlogpogingen te blokkeren.

Hoe langer het wachtwoord, des te meer tijd een hacker nodig heeft om alle mogelijke wachtwoordcombinaties die bestaan binnen die lengte te proberen. Voor een mens ziet een wachtwoord met speciale tekens, hoofdletters en cijfers er moeilijker uit. Maar een computer heeft daar geen boodschap aan. Een wachtwoord van 5 woorden dat aan de hand van een woordenlijst en dobbelstenen wordt verzonnen,[2] bevat ongeveer 4200 keer zoveel mogelijke combinaties als een ogenschijnlijk

1. NIST Special Publication 800-63, juni 2004, https://csrc.nist.gov/CSRC/media/Publications/sp/800-63/ver-10/archive/2004-06-30/documents/sp800-63-v1-0.pdf (laatst bezocht 23 februari 2021).

2. Zoals bijvoorbeeld beschreven op https://www.eff.org/nl/dice of https://theworld.com/~reinhold/diceware.html.

moeilijk wachtwoord van 8 karakters. En kies je voor 6 woorden? Dan zijn er ineens al 30 miljoen keer zoveel combinaties mogelijk. Terwijl zo'n wachtwoordzin veel eenvoudiger te onthouden is als er een ezelsbruggetje van gemaakt wordt.

Nieuwe NIST-aanbeveling voor wachtwoordbeleid
Inmiddels erkent NIST ook dat de oude aanbeveling die zij hebben gedaan voor het opstellen van wachtwoordbeleid achterhaald is geraakt. NIST heeft daarom een aangepaste versie van hun aanbevelingen voor wachtwoordbeleid gepubliceerd.[3] Daarin zijn een aantal zaken opvallend ten opzichte van de oude aanbeveling:

- Wachtwoorden moeten minimaal 8 posities lang zijn;
- Wachtwoorden moeten niet langer na een bepaalde periode verlopen;
- Er moeten niet langer eisen aan complexiteit gesteld worden, zoals minimaal één speciaal teken, één hoofdletter en één cijfer.

In plaats daarvan ligt de focus van deze aanbeveling op de volgende aspecten:

- Mogelijkheid voor gebruikers om langere wachtwoorden in te voeren;
- Het veilig opslaan van wachtwoorden door organisaties;
- Het invoeren van tweefactorauthenticatie;
- Het checken van wachtwoorden tegen lijsten van wachtwoorden die bij datalekken zijn betrokken, en dus openbaar zijn geworden;
- Het verbieden van woorden die te maken hebben met de context van het account waarvoor het wachtwoord wordt gekozen.[4]

Dit is een duidelijke trendbreuk met de eerdere aanbeveling die is gedaan. Naar aanleiding van deze wijziging, en het algemene beeld van cybersecurity experts dat de mogelijkheden van hackers verschuiven, is het aan te bevelen dat organisaties hun wachtwoordbeleid onder de loep nemen.

Aanvullende beveiligingsmaatregelen
Een wachtwoord dat veel tijd kost om te kraken beschermt goed tegen het uitlekken van wachtwoorden die op de juiste manier door een organisatie zijn opgeslagen. Wanneer een wachtwoordendatabase die niet goed ingesteld is bij een datalek betrokken is, dan kan het zomaar zijn dat de wachtwoorden niet eens gekraakt hoeven te worden, maar gewoon zo leesbaar zijn voor de hacker. Hierin schuilt het gevaar dat mensen wachtwoorden vaak hergebruiken. Een wachtwoord kan nog zo lang en sterk zijn, als het is uitgelekt maakt dat niet meer uit.

Om de organisatie beter te beschermen tegen het uitlekken van wachtwoorden die worden hergebruikt is het zeer raadzaam om tweefactorauthenticatie in te stellen. Naast de loginnaam en wachtwoord, iets dat de gebruiker weet, is dan ook iets dat de gebruiker in bezit heeft nodig om in te loggen. Een voorbeeld daarvan is een tijdelijke code gegenereerd door een authenticatie app. Het versturen van een code via SMS als tweede factor wordt in 2021 niet meer als veilig gezien.

Zelfs wanneer een hergebruikt wachtwoord uitlekt is het voor een aanvaller niet mogelijk om te loggen, omdat de vereiste tweede factor (bijvoorbeeld een code gegenereerd door een app) niet bekend is bij de aanvaller.

De meeste moderne applicaties bieden de mogelijkheid om tweefactorauthenticatie in te stellen, zoals cloudomgevingen voor kantoorapplicaties. Maar ook wanneer wordt gewerkt via een gevirtualiseerde werkplek bestaat vaak de mogelijkheid om het inloggen te beschermen met een tweede authenticatiefactor.

Door wachtwoordmanagers beschikbaar te stellen aan medewerkers in de organisatie wordt de kans op hergebruik van wachtwoorden al verkleind. Een wachtwoordmanager maakt het gebruikers eenvoudiger om voor iedere identiteit een uniek wachtwoord te genereren en op te slaan. Natuurlijk kennen wachtwoordmanagers ook risico's, een zorgvuldige afweging of dit een tool is die in de organisatie ingezet kan worden, moet dan ook worden gemaakt. Maar als een wachtwoordmanager gebruikt kan worden dan is het zeker een heel waardevolle toevoeging aan het wachtwoordbeleid van de organisatie.

Conclusie
Anno 2021 is het dus echt nodig om af te stappen van wachtwoordbeleid dat gebruikers aanzet tot slechte gewoontes. Door gebruikers beter voor te lichten over de sterkte van wachtwoorden, en hen de tools te geven om wachtwoorden eenvoudiger te managen worden organisaties veiliger. Wordt daarbij ook nog tweefactorauthenticatie ingezet, dan wordt het hackers al helemaal lastig gemaakt om geautomatiseerd wachtwoorden te kraken.

3. NIST Special Publication 800-63-3, juni 2017 (met updates in februari 2020), https://pages.nist.gov/800-63-3/sp800-63b.html (laatst bezocht 23 februari 2021).
4. Het wachtwoord voor het account dat bij ICTRecht gebruikt wordt zou bijvoorbeeld niet het woord 'ictrecht' mogen bevatten. Het wachtwoord van een e-mailaccount zou bijvoorbeeld niet de naam of het e-mailadres van de eigenaar mogen bevatten.

ICTRECHT
academy

"De opleiding wordt gegeven door deskundige docenten, die hun kennis van de praktijk combineren met nodige skills om de informatie aan de cursisten over te dragen. Het contact met andere juristen vind ik waardevol. Ik kan deze opleiding zeker aanbevelen in mijn netwerk."

Jan-Kees Karels
Jurist bij Wolleswinkel
Advocaten over opleiding
ICT-jurist 2019/20209

ICTRecht Academy biedt u een praktijkgerichte opleiding tot ICT-jurist op twee niveaus (start april 2021):

ICT-jurist en ICT-jurist: de verdieping

Vrijwel elk rechtsgebied krijgt tegenwoordig te maken met vraagstukken rondom het ICT-recht. Wilt u uitgebreide juridische én technische kennis opdoen over het ICT-vakgebied? Volg onze opleiding tot ICT-jurist. Of wordt een expert in uw vakgebied met onze verdiepende opleiding waarbij u kunt kiezen uit zes profielen. Beide niveaus duren één jaar en zijn in Amsterdam of online te volgen (via livestream dan wel video-opname).

Kijk voor meer informatie op:
ictrecht.nl/opleiding-ict-jurist

Enkel geïnteresseerd in het opdoen van alomvattende kennis en skills over privacy?
Volg onze opleiding tot allround privacy jurist.
Lees meer op: ictrecht.nl/opleiding-allround-privacy-jurist

Bram de Vos
Juridisch adviseur

Wet- en regelgeving

Europese resolutie inzake encryptie
Op 14 december 2020 heeft de Europese Raad een resolutie aangenomen waarin zij het belang onderstreept van veiligheid dankzij encryptie en veiligheid ondanks encryptie. Resoluties van de Europese Raad zijn juridisch niet bindend, maar hebben wel een belangrijke politieke betekenis. In de resolutie benoemt de Europese Raad allereerst het belang van sterke versleuteling voor de bewaking van fundamentele rechten en de algehele digitale veiligheid van burgers, overheden en bedrijven. Maar de Europese Raad wijst er tegelijkertijd op dat opsporingsautoriteiten hun wettelijke bevoegdheden effectief moeten kunnen uitoefenen. Toegang tot digitale informatie is essentieel in het kader van de rechtshandhaving en strafrechtpleging. Encryptie speelt hierbij volgens de Europese Raad een belangrijke belemmerende factor. Er moet een juiste balans worden gevonden tussen het belang bij encryptie enerzijds en het belang bij handhaving anderzijds. De Europese Raad stuurt aan op een actieve discussie met technologiebedrijven om zo naar passende oplossingen te zoeken.

https://bit.ly/37lc7Bc

Wijziging van de Wet toezicht
Op 15 december 2020 heeft de Eerste Kamer een wijziging van de Wet toezicht en geschillenbeslechting collectieve beheersorganisaties auteurs- en naburige rechten ("Wet toezicht") aangenomen. Doel van het wijzigingsvoorstel is om de slagvaardigheid van het College van Toezicht Auteurs- en naburige rechten ("College") te vergroten. Deze instantie houdt toezicht op zogeheten collectieve beheersorganisaties en openbare beheersorganisaties die zich inzetten voor auteursrechthebbenden, producenten en uitvoerende kunstenaars. Door de wetswijziging kan het College voortaan makkelijker boetes opleggen. Ook worden er een aantal nieuwe handhavingsbevoegdheden aan de toezichthouder toegekend.

https://bit.ly/2Zq1j0m

Goedkeurings- en uitvoeringswet Benelux-politieverdrag
Op 17 december 2020 heeft Minister Grapperhaus van Justitie en Veiligheid een wetsvoorstel aan de Tweede Kamer gestuurd met betrekking tot de goedkeuring en uitvoering van een nieuw Benelux-politieverdrag. Het verdrag is al in 2018 tot stand gekomen, maar moet (volgens de hiervoor geldende procedures) nog parlementair goedgekeurd worden. Het nieuwe verdrag moet tot een betere samenwerking met opsporingsautoriteiten uit België en Luxemburg leiden. Zo is het de bedoeling dat autoriteiten uit de verschillende landen (onder bepaalde voorwaarden) toegang krijgen tot elkaars databases. Ook maakt het nieuwe verdrag grensoverschrijdende achtervolgingen een stuk makkelijker.

https://bit.ly/37mZYvK

Tweede Kamer stemt tegen coronapaspoort
Op 5 januari 2021 heeft kamerlid Azarkan van DENK tijdens een debat over de ontwikkelingen rondom het coronavirus een motie ingediend tegen de invoering van een coronapaspoort. De motie houdt verband met een eerdere brief van het Ministerie van Volksgezondheid, Welzijn en Sport waarin de Gezondheidsraad wordt gevraagd om een advies uit te brengen over de ethische aspecten van het coronapaspoort. Het idee achter het coronapaspoort is om burgers die zich niet hebben ingeënt, de toegang tot bepaalde publieke voorzieningen te ontzeggen. Dat zou ook de deelname en/of het functioneren van deze burgers in de maatschappij negatief kunnen beïnvloeden. Volgens Azarkan wordt de invoering van een dergelijk paspoort door burgers ervaren als een verkapte manier om vaccinatie toch te verplichten. De motie werd (met een beperkte meerderheid) aangenomen.

https://bit.ly/3asWA4s

Brief aan Eerste Kamer tegen invoering 'Super SyRI'
Op 8 januari 2021 heeft een maatschappelijke coalitie een brief gestuurd aan de Eerste Kamer waarin zij haar zorgen uit over het voorstel voor de Wet gegevensverwerking door samenwerkingsverbanden. Hoewel er vanuit verschillende hoeken kritiek tegen de wet is geuit, heeft de Tweede Kamer het voorstel inmiddels aangenomen. De wet moet meer ruimte creëren voor zowel private als publieke organisaties om informatie (waaronder ook persoonsgegevens) met elkaar te delen, onder meer om fraude en georganiseerde criminaliteit op te sporen. De coalitie bestempelt het wetsvoorstel als 'Super SyRI', waarmee wordt verwezen naar het Systeem Risico Indicatie (SyRI) dat afgelopen jaar door de rechter onverbindend werd verklaard. Volgens de coalitie gaat deze nieuwe wet in verschillende opzichten verder dan SyRI. Daarnaast krijgt de minister volgens de coalitie te veel ruimte om (in lagere wetgeving) belangrijke details uit te werken. Zaken als de hoeveelheid en soorten gegevens, de partijen die erbij kunnen en de manier waarop ze worden verwerkt, worden bepaald zonder dat hier goedkeuring van de Eerste of Tweede Kamer voor nodig is. Ook doet het wetsvoorstel afbreuk aan het privacyrechtelijke doelbindingsbeginsel. De brief is ondertekend door onder meer het Platform Burgerrechten, het Nederlands Juristen Comité voor de Mensenrechten (NJCM), de FNV en Stichting Privacy First.

https://bit.ly/3dnxWUO

Richtsnoeren EDPB met voorbeelden datalekken
Op 14 januari 2021 heeft het European Data Protection Board (EDPB) nieuwe richtsnoeren vastgesteld over de omgang met datalekken. De richtsnoeren bevatten een aantal voorbeelden van veelvoorkomende soorten datalekken, zoals datalekken als gevolg van ransomware of menselijke fouten. Per categorie wordt aangegeven welke maatregelen er genomen moeten worden (zowel preventief als wanneer er daadwerkelijk een datalek heeft plaatsgevonden). De richtsnoeren gelden aanvullend op de algemene richtsnoeren over datalekken die al in 2016 door de Artikel 29 Werkgroep (de voorloper van het EDPB) werden aangenomen.

https://bit.ly/3pxnSuC, zie ook https://bit.ly/3auxEcw

Invoering opt-in-systeem voor telemarketing
Op 9 februari 2021 heeft de Eerste Kamer ingestemd met een wijziging van de Telecommunicatiewet in verband met de invoering van een opt-in-systeem voor telemarketing. Op dit moment geldt er een opt-out-systeem. Daarbij mogen mensen ongevraagd telefonisch benaderd worden, tenzij zich hebben ingeschreven in het Bel-me-niet-register. Na de doorvoering van de wetswijziging geldt juist als uitgangspunt dat mensen niet telefonisch benaderd mogen worden, tenzij ze hiervoor uitdrukkelijk toestemming hebben gegeven. Mensen die toestemming hebben gegeven, moeten steeds worden gewezen op de mogelijkheid om verzet aan te tekenen tegen het verdere gebruik van hun contactgegevens. Daarnaast mogen telemarketeers niet langer anoniem bellen door middel van nummerblokkering. Het opt-in-regime geldt overigens niet voor het benaderen van personen waar al een klantrelatie mee bestaat, mits de communicatie betrekking heeft op eigen gelijksoortige producten of diensten. Wel hebben de benaderde personen ook in dat geval een recht van verzet.

https://bit.ly/3pzUa8w

Onderhandelingsmandaat E-privacyverordening
Op 10 februari 2021 hebben de lidstaten van de Europese Unie overeenstemming bereikt over het onderhandelingsmandaat voor de E-privacyverordening. Nu er overeenstemming is, kan Portugal (als voorzitter van de Raad van de Europese Unie) in onderhandeling treden met het Europees Parlement om tot een definitieve tekst te komen. De verordening moet de bestaande E-privacyrichtlijn (Richtlijn 2002/58/EG) gaan vervangen. Deze richtlijn was aan vervanging toe, onder meer door technologische ontwikkelingen. Al in 2017 diende de Europese Commissie een voorstel voor de nieuwe E-privacyverordening in, maar tijdens het wetgevingstraject werd flinke vertraging opgelopen. Dankzij het mandaat kan men nu eindelijk gaan toewerken naar een definitieve versie.

https://bit.ly/2NfUQm3

Pramila Kramer
Juridisch adviseur

Cloud

Nieuwe regels in aankomst voor platformaanbieders

Wat zal de Digital Services Act en de Digital Markets Act voor hen betekenen?

Wegens de COVID-19 crisis zijn de digitale ontwikkelingen in een stroomversnelling gekomen. Zo is men nu genoodzaakt om op afstand te winkelen, zijn sociale media platforms dé manier om met elkaar te communiceren en is het aantal online platforms in een razend tempo toegenomen. Om deze diensten en digitale groei in goede banen te laten leiden is vanuit de Europese Commissie regulering op komst.

De Europese Commissie heeft in december 2020 twee wetgevingsinitiatieven voorgesteld om de huidige e-Commerce richtlijn te vervangen: de Digital Services Act ("DSA") en de Digital Markets Act ("DMA"). De Commissie heeft hierin regels neergelegd die de verantwoordelijkheden en verplichtingen van aanbieders van digitale diensten vastleggen, en dan met name die van online platforms, zoals sociale media en marktplaatsen.[1] In dit artikel gaan we in op de doelen van beide wetsvoorstellen en een aantal gevolgen die deze voorstellen met zich meebrengen voor grote online platformaanbieders.

Doelen van de Digital Services Act

Het doel van dit voorstel is om verschillende verplichtingen en verantwoordelijkheden op te leggen aan aanbieders van intermediaire diensten en online platforms. Dergelijke platforms worden verplicht gesteld om bepaalde maatregelen te nemen ter bescherming van consumenten en om, onder andere, de verspreiding van illegale of oneerlijke praktijken op platforms tegen te gaan. Strengere eisen worden gesteld aan transparantie en verantwoording voor de manier waarop inhoud gemodereerd wordt of hoe advertenties getoond worden. Daarbovenop zal het gebruik van algoritmische processen meer worden gereguleerd.[2] De automatische verspreiding van (des)informatie valt hieronder, zoals in het geval van 'clickbait' of het aanschaffen van 'neplikes' en 'nepvolgers' op sociale media accounts.[3]

Doelen van de Digital Markets Act

De DMA introduceert, onder andere, regels voor platforms die met name optreden als poortwachters (welke

1. http://bit.do/fN4xy
2. http://bit.do/fN4xv, Overweging 58.
3. http://bit.do/fN4xs

platforms hieronder vallen komt in de volgende alinea aan de orde). Dit voorstel heeft als doel om te voorkomen dat poortwachters oneerlijke voorwaarden opleggen aan zakelijke gebruikers en consumenten. Voorbeelden van oneerlijke voorwaarden zijn onder meer het gunstiger behandelen van eigen diensten op zoekmachines of situaties waarin gebruikers vastzitten aan een bepaalde dienst en als gevolg van een sterke 'vendor lock-in' beperkte mogelijkheden hebben om over te schakelen naar alternatieve diensten. Met deze verordening wil de Commissie gelijke concurrentievoorwaarden tot stand brengen om op deze manier meer ruimte te creëren voor kleinere ondernemingen zoals mkb'ers, scale-ups en start-ups.[4]

Gevolgen voor platforms die gekenmerkt worden als poortwachters

Allereerst is het van belang om vast te stellen wanneer men van een poortwachter kan spreken. Ingevolge artikel 3 DMA wordt een platformaanbieder als poortwachter aangemerkt indien deze: (1) een aanzienlijke impact heeft op de interne markt, (2) een kernplatformdienst, zoals een onlinezoekmachine of cloudcomputerdienst, aanbiedt die voor zakelijke gebruikers essentieel is om eindgebruikers te bereiken, en (3) die met betrekking tot haar activiteiten een duurzame positie inneemt (of waarvan verwacht wordt dat dit in de nabije toekomst zal gebeuren). Een aanbieder van een kernplatformdienst kan door de Commissie tot poortwachter benoemd worden.[5] Zulke aanbieders worden geacht te voldoen aan een jaaromzet van tenminste € 6,5 miljard en om meer dan 10% van de Europese bevolking te bereiken (dat is momenteel een bereik van 45 miljoen gebruikers). Beide wetsvoorstellen zetten een aantal verplichtingen voor poortwachters uiteen. Hieronder gaan we in op een drietal neergelegde verplichtingen.

Niet langer aan de zijlijn toekijken

Poortwachters mogen niet langer aan de zijlijn toekijken hoe hun platformdiensten door bepaalde gebruikers gebruikt worden, of beter gezegd, misbruikt worden. Overeenkomstig artikel 25 DSA zijn deze platforms verplicht om de risico's die voortvloeien uit de werking van het gebruik van hun diensten te identificeren, analyseren en beoordelen. Deze risicobeoordeling dient niet enkel de verspreiding van illegale content tegen te gaan, maar ook om eventuele negatieve gevolgen voor de uitoefening van grondrechten zoals de vrijheid van meningsuiting en informatie of het

4. http://bit.do/fN4v3

5. http://bit.do/fN4xk, artikel 3 lid 6.

verbod op discriminatie tegen te gaan. Alsook de verspreiding van (des)informatie die een negatief effect kan hebben op de volksgezondheid of op verkiezingsprocessen.[6] Poortwachters zijn verplicht om hierbij een actief content moderatiebeleid te implementeren en deze risico's te mitigeren.[7]

Niet langer persoonsgegevens combineren
Tot op heden mogen poortwachters, die meerdere kernplatformdiensten aanbieden, persoonsgegevens combineren voor eigen doeleinden. In artikel 5 (a) DMA is neergelegd dat poortwachters niet langer persoonsgegevens mogen combineren die afkomstig zijn van kernplatformdiensten met persoonsgegevens van andere eigen aangeboden diensten of met persoonsgegevens van de diensten van derden. Het is voor de poortwachter dus ook niet meer toegestaan om eindgebruikers op andere diensten van zichzelf automatisch aan te melden, tenzij daar specifiek toestemming voor is verleend conform de AVG. Poortwachters dienen vooral d.m.v. transparantie gebruikers meer inzicht te bieden omtrent de manier waarop hun persoonsgegevens gecombineerd worden.

Niet langer data voor zichzelf houden
Poortwachters hebben toegang tot grote hoeveelheden gegevens die zij verzamelen bij de verlening van hun kernplatformdiensten. Poortwachters worden verplicht gesteld om zakelijke gebruikers de gelegenheid te bieden om hun gegevens over te kunnen dragen. Zowel zakelijke gebruikers als eindgebruikers krijgen het recht om onder artikel 6 (h) DMA toegang te verkrijgen tot de gegevens die zij hebben verstrekt of gegenereerd op de diensten van de poortwachter, deze toegang dient gratis te worden verleend.[8] Het is de bedoeling dat deze gegevens in real-time kunnen worden ingezien om gegevensportabiliteit te vergemakkelijken en dat hier de technische mogelijkheid voor gecreëerd wordt. In de praktijk heeft dit betrekking op informatie over bijvoorbeeld zoekopdrachten of informatie over clicks.[9]

Indien deze poortwachters niet voldoen aan de opgelegde verplichtingen, kan de Commissie significante sancties opleggen zoals een boete die kan oplopen tot 10% van de wereldwijde jaarlijkse omzet.[10] Als laatste maatregel krijgt de Commissie de bevoegdheid om dergelijke platforms te forceren om (onderdelen van) het bedrijf af te stoten.

Slotsom
Kortom, de DSA en de DMA dienen ter ondersteuning van de digitale wereld. Echter moeten deze wetsvoorstellen nog door het Europese Parlement en de Raad goedgekeurd worden voordat ze van kracht kunnen gaan. Niettemin dienen enkele onbeantwoorde vragen te worden beantwoord. Krijgen platforms die gekenmerkt worden als poortwachters bijvoorbeeld een recht van bezwaar op deze benaming en zijn de verschillende verplichtingen die opgelegd worden wel technisch haalbaar in de praktijk? Poortwachters lijken geschikt om meer verantwoordelijkheden te dragen en zijn in ieder geval verplicht om niet langer aan de zijlijn toe te kijken qua informatieverspreiding, mogen persoonsgegevens niet langer zomaar combineren en niet langer data voor zichzelf houden. Deze maatregelen zullen niet alleen gunstig zijn voor consumenten maar ook voor zakelijke gebruikers, aldus de Commissie. De EU heeft er tenslotte baat bij om te blijven innoveren op digitaal vlak, door maatregelen aan poortwachters op te leggen blijven ook nog kansen over voor de kleinere spelers op de markt.

6. http://bit.do/fN7PJ
7. http://bit.do/fN4sz, artikel 26.
8. http://bit.do/fN4vT, overweging 54 en 55.
9. http://bit.do/fN4sk, overweging 56.
10. http://bit.do/fN4sa

Esmée Kuyt
Juridisch adviseur

Privacy | Overheid | Marketing

Microtargeting tijdens verkiezingscampagnes, macro in de politiek?

De Tweede Kamerverkiezingen hebben op 15, 16 en 17 maart jl. plaatsgevonden. Ditmaal op een andere manier dan wij gewend waren, namelijk driedaags, stemmen per post was voor ouderen mogelijk en je mocht drie in plaats van twee volmachten aannemen. In de maand daarvoor, op 16 februari, heeft de Autoriteit Persoonsgegevens (hierna: AP) de Handleiding privacy verkiezingscampagnes gepubliceerd.[1] In de handleiding van de AP wordt een stappenplan beschreven. Bij gebruik van persoonsgegevens voor een campagne geldt dat politieke partijen zich aan de Europese privacywetgeving moeten houden (de AVG). Daarbij benoemt de AP specifiek microtargeting als veelgebruikt middel. In dit artikel kijken we naar microtargeting en gaan we in op de handleiding van de AP.

Microtargeting, wat is dat precies?
Door de huidige maatregelen van de overheid, bestond campagne voeren voor politieke partijen niet meer uit ouderwets handjes schudden en goodies uitdelen op de plaatselijke markt. Politieke partijen voerden digitaal campagne. Met microtargeting kunnen specifieke groepen worden beïnvloed. Zo kunnen mensen die in het leger werken bijvoorbeeld boodschappen te zien krijgen van politieke partijen die hierop inzetten. Microtargeting kan door politieke partijen ingezet worden met gebruik van diensten van derde partijen. Beïnvloeding gebeurt, maar het is wel van groot belang dat dit op een rechtmatige, transparante wijze verloopt en er sprake is van een gelijk speelveld voor vrije verkiezingen. Microtargeting is een aandachtsgebied van de AP uit de Focus AP 2020-2023.[2]

Beïnvloeding van verkiezingen en schending van privacy zijn met elkaar verbonden. Een bekend voorbeeld daarvan is het Cambridge Analytica schandaal.[3] In juli 2020 werd al onderzoek gedaan naar de rol en effecten van politieke microtargeting in Nederland door UvA communicatiewetenschapper Tom Dobber.[4] Zijn aanleiding voor het onderzoek waren het gebruik van microtargeting voor de verkiezing van Donald Trump en de 'leave' campagne waardoor de Brexit in gang is gezet. In zijn onderzoek kwam naar voren dat politieke partijen in Nederland microtargeting gebruiken, weliswaar in aangepaste vorm door onder andere (privacy-)wetgeving. De conclusie van Dobber met betrekking tot het bedreigende karakter van microtargeting is in dat kader van belang: "Maar beïnvloeding door PMT wordt onacceptabel wanneer het overgaat in

1. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleiding_privacy_verkiezingscampagnes.pdf
2. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/focus_ap_202-2023_groot.pdf
3. https://www.ictrecht.nl/blog/wie-trackt-er-aan-de-touwtjes-gepersonaliseer-de-advertenties-onder-vuur
4. https://www.uva.nl/shared-content/faculteiten/nl/faculteit-der-maatschappij-en-gedragswetenschappen/nieuws/2020/07/is-politieke-microtargeting-een-bedreiging-voor-democratie.html

manipulatie, wanneer het misbruik maakt van de kwetsbaarheden van mensen door vooral in te spelen op hun angsten, wanneer gebruik wordt gemaakt van leugens of onrechtmatig verkregen persoonlijke data en wanneer het uitgevoerd wordt door niet-legitieme actoren".

Als persoonsgegevens niet op een rechtmatige manier zijn verkregen, is sprake van onrechtmatige verwerking van persoonsgegevens. Dat is niet toegestaan volgens de AVG en kan resulteren in hoge boetes. Bij politieke microtargeting ligt een inbreuk op privacy dus op de loer. Alleen al om die reden is het goed dat de AP hier aandacht aan besteed via haar handleiding.

De handleiding van de AP

De Tweede Kamerverkiezingen hebben onlangs plaatsgevonden. Desalniettemin kan de handleiding handvatten bieden voor toekomstige verkiezingscampagnes. Als eerste stap noemt de AP dat gecheckt moet worden of het noodzakelijk is om persoonsgegevens te verwerken voor de campagne activiteit en of er geen minder ingrijpende campagne methode mogelijk is. Dit vloeit voort uit de beginselen van de AVG (art. 5 AVG). De AP geeft verder (stap 2) aan dat microtargeting ingewikkeld is en raad daarom deskundigheid aan in de vorm van een Functionaris Gegevensbescherming of externe.

Vervolgens geeft de AP (stap 3) aan dat lidmaatschap van een politieke partij een bijzonder persoonsgegeven is, omdat het gaat over de politieke opvatting van een natuurlijk persoon. Voor bijzondere persoonsgegevens geldt een verwerkingsverbod tenzij er -naast een van de AVG-gronden om te mogen verwerken - een uitzondering van toepassing is uit de AVG. In art. 9 van de AVG is een uitzondering opgenomen, waarin staat dat het verbod niet geldt voor het onderhouden van regelmatig contact met bestaande leden van een politieke partij. Dat onderscheid is dus belangrijk. Bij niet-leden kunnen politieke partijen namelijk geen beroep doen op deze uitzondering als het gaat om gegevens over politieke opvattingen. Dan moet de politieke partij nagaan of een andere uitzondering van toepassing is. Uitdrukkelijke toestemming van betrokkenen wordt door de AP genoemd. Deze vorm van toestemming is een zwaardere variant dan 'reguliere' toestemming. Naast de normale vereisten van toestemming (vrijelijk, ondubbelzinnig, specifiek en geïnformeerd). Het zwaartepunt ligt hier bij de wilsuiting. Deze moet expliciet zijn gericht op het geven van toestemming.

Daarnaast is een belangrijk punt (stap 4) of de politieke partij derde partijen inschakelt en zo ja, welke privacyrol deze partijen innemen. Is het bedrijf dat wordt ingeschakeld een verwerker of zijn de politieke partij en het bedrijf beide verwerkingsverantwoordelijken? De European Data Protection Board heeft *'guidelines on the targeting of sociale media users'*[5] opgesteld. Hoewel deze nog niet definitief is, wordt hierin uitleg gegeven over de ingewikkelde privacy rolverdelingen in dat kader.

Als stap 5 geeft de AP aan dat openbare informatie niet zomaar gebruikt mag worden. Denk hierbij bijvoorbeeld aan mensen met openbare profielen op Facebook die duidelijk hun steun uitspreken voor een politieke partij. Op het moment dat politieke partijen deze gegevens gaan verwerken (bijvoorbeeld verzamelen of ordenen om politieke berichten naar deze mensen ofwel betrokkenen te sturen), is sprake van verwerking van deze persoonsgegevens. Als het gaat om politieke opvattingen van mensen geldt dan dus wederom dat sprake is van bijzondere persoonsgegevens en de regels hieromtrent uit de AVG. Een goede tip van de AP (stap 6) is om te controleren of datasets met persoonsgegevens op een rechtmatige manier zijn verzameld door in te schakelen bedrijven en of de bedrijven genoeg garanties met betrekking tot AVG-compliancy kunnen bieden. De AP geeft ook aan dat het kan helpen een DPIA (Data Protection Impact Assessment) uit te voeren om goed te kunnen documenteren wat de exacte afwegingen zijn geweest. Naleving van de AVG en *awareness* zijn daarbij noodzakelijk. Dat betekent bijvoorbeeld dat niet alleen een campagneteam goed moet worden geïnformeerd, maar ook de personen op de kandidatenlijst. Daarnaast moeten de rechten van betrokkenen – zoals het recht op vergetelheid - gewaarborgd en gefaciliteerd worden (stap 7).

Conclusie

Hoewel de verkiezingen tijdens publicatie van dit artikel al voorbij zijn, is het goed om bewust te zijn van de privacyregels rondom verkiezingscampagnes. In een digitaliserende wereld en een steeds verder digitaliserende overheid, zal de AVG een rol blijven spelen. Naar mijn mening zou de DPIA (stap 6) de eerste moeten zijn. Een DPIA bij elke voorgenomen digitale verkiezingscampagne met persoonsgegevens uitvoeren is namelijk een mooie manier om te toetsen (en je kan beargumenteren dat het verplicht zou moeten zijn bij dit soort verwerkingen). De vraag is wel of gebruik van politieke microtargeting door deze toets komt.

5. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-082020-targeting-social-media-users_nl

PRIVACY VERIFIED

Maak privacy aantoonbaar

Met ons certificeringsprogramma ‘Privacy Verified’ helpen wij organisaties op een praktische wijze te voldoen aan de wet. Daarnaast biedt het de mogelijkheid om bij klanten aantoonbaar te maken op welke wijze privacy wordt gewaarborgd. Een privacyaudit of DPIA laten uitvoeren? Dat kan middels Privacy Verified.

Actie: het Privacy Verified Basic traject nu eenmalig **voor € 1.590 excl. btw** (i.p.v. € 1.850). Deze prijs betreft de audit, verificatie, certificaat en gebruik van ons Privacy Verified portaal. Actie geldt t/m 30 juni 2021.

Gebruik maken van deze actie? Mail naar info@privacyverified.nl.

Lisette Meij
Directeur Privacy Verified

020 6631941
info@privacyverified.nl

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

Dimmen Smolders
Juridisch adviseur

Laura Monhemius
Juridisch adviseur

Privacy

De geheimen van supermodellen: modelverwerkersovereen-komsten in de praktijk

De verwerkersovereenkomst is inmiddels niet meer weg te denken uit de gemiddelde (ICT-)contractenset. Zo krijgen wij bijvoorbeeld met enige regelmaat de volgende situatie (in verschillende variaties) voorgelegd in onze praktijk: "Beste ICTRecht, hierbij een verwerkersovereenkomst die wij van een klant ontvingen. De dienstverlening is trouwens vorige week al begonnen, dus we verwerken al persoonsgegevens. Kan deze verwerkersovereenkomst zo getekend worden? Dan is dat ook maar geregeld." Stuur dan als jurist maar eens terug dat je zelf even nodig hebt om de onrechtmatige en onredelijke punten eruit te halen en dat dan pas de onderhandelingen kunnen beginnen.

Om het proces van het sluiten van verwerkersovereen-komsten eenvoudiger te laten verlopen, zijn er in bepaalde sectoren modelverwerkersovereenkomsten opgesteld. Verwerkingsverantwoordelijken of verwer-kers (afhankelijk van de verwerkersovereenkomst) in de sector kunnen, of moeten zelfs, kiezen om dit model te hanteren. De vraag is: welke modellen worden er door Nederlandse organisaties zoal gehanteerd? Waarom kies je er wel of niet voor om een model van de sector te hanteren en kan er over de inhoud nog worden onderhandeld?

Wel of geen model in de sector?

Organisaties in dezelfde sector kennen vaak dezelfde belangen en verwerken vaak dezelfde soorten persoonsgegevens. Zo worden bijvoorbeeld in het primair en voortgezet onderwijs veel persoonsgege-vens van minderjarigen verwerkt en in de zorg veel gezondheidsgegevens. Daarvoor worden hoge eisen gesteld aan de beveiliging van de persoonsgegevens. In zulke situaties kan het sluiten van een verwerkers-overeenkomst worden bespoedigd door een vast model te gebruiken, waarin de belangen voldoende worden beschermd. Van leveranciers aan partijen in deze sectoren wordt dan vereist dat ze aan de standaard eisen voldoen.

Voor een succesvolle modelverwerkersovereenkomst is daarom een belangrijk vereiste dat de sector in staat is om het gebruik van het model tot op zekere hoogte 'af te dwingen'. Een model wat maar weinig wordt gebruikt, heeft weinig toegevoegde waarde. Er moet daarom enerzijds veel draagvlak zijn onder partijen in de sector, om een model te hanteren. Het verplicht stellen van het gebruik, zoals bij de VNG-verwerkers-overeenkomst het geval is, kan natuurlijk ook. Ander-zijds moet het model ook redelijk genoeg zijn voor de wederpartijen. Een modelverwerkersovereenkomst heeft weinig voordelen, als er alsnog langdurige onder-handelingen uit voortkomen. Dit levert vooral bij het BoZ-model nog wel eens discussie op: vooral de ICT-dienstverleners, die geen tot weinig gezondheids-gegevens verwerken voor een zorgpartij, kunnen vaak niet aan de zware beveiligingseisen voldoen. Het gebruik van een model heeft wel weer als voordeel dat, als eenmaal een standaardreactie is geformuleerd,

deze ook aan andere klanten in dezelfde sector kan worden voorgelegd.

Veel modelverwerkersovereenkomsten horen dan ook bij een standaard set algemene voorwaarden. Zo hoort de verwerkersovereenkomst voor rijksoverheidsorganisaties bij één van de sets inkoopvoorwaarden van het Rijk (Arvodi, Arbit of Ariv). Ook de NLdigital verwerkersovereenkomst hoort bij de algemene voorwaarden die door de branchevereniging voor IT-leveranciers wordt aangeboden. Omdat de verwerkersovereenkomsten op veel plaatsen naar de toepasselijke voorwaarden verwijzen, is het niet goed mogelijk om deze documenten los van elkaar te zien.

Welke modellen worden veel gehanteerd?
De hierboven genoemde voordelen gelden in het bijzonder voor een aantal sectoren. De meest gebruikte modelverwerkersovereenkomsten worden hieronder toegelicht.

Arvodi/Arbit/Ariv (rijksoverheidsorganisaties)
Allereerst zijn rijksoverheidsorganisaties als verwerkingsverantwoordelijken logische gebruikers van een model. Rijksoverheidsorganisaties kunnen hoge eisen stellen in contracten met leveranciers. Zoals eerder genoemd, hanteren zij dan ook standaard inkoopvoorwaarden, en in het verlengde daarvan, de bijbehorende modelverwerkersovereenkomst.

VNG (gemeenten)
Net als rijksoverheidsdiensten, stellen gemeenten hoge eisen aan leveranciers. Dit komt tot uiting in de verwerkersovereenkomst van de Vereniging van Nederlandse Gemeenten (VNG). In tegenstelling tot de andere modellen die hier besproken worden, is het gebruik ervan verplicht voor gemeenten. Het is nog maar de vraag of er sancties kunnen worden opgelegd voor het schenden van deze plicht, maar het laat wel zien dat er veel waarde wordt gehecht aan het gebruik van het model. Goed om te weten: deze verwerkersovereenkomst is een redelijke middenweg voor zowel de verwerkingsverantwoordelijke als de verwerker. Geen van de verplichte onderwerpen stelt zeer strenge eisen aan de leverancier. De bijlagen bevatten de vertalingsslag naar de praktijk, waarin de dienstverlening en de beveiligingsmaatregelen nog eens duidelijk worden toegelicht.

Privacyconvenant 3.0 (primair en voortgezet onderwijs)
Voor scholen is het uiteraard belangrijk dat de vele persoonsgegevens die ze verwerken, grotendeels van minderjarigen, veilig zijn bij leveranciers. Het Privacyconvenant 3.0 voor primair en voortgezet onderwijs, waarvan een modelverwerkersovereenkomst onderdeel uitmaakt, legt daar de basis voor. Hierin zijn bijvoorbeeld specifieke afspraken opgenomen voor uitwisseling van het onderwijskundig rapport en voor leermiddelenleveranciers. Deze overeenkomst is erg evenwichtig en algemeen en daarmee redelijk voor beide partijen.

Brancheorganisaties Zorg (zorginstellingen)
Als er in één sector grootschalig met gevoelige persoonsgegevens wordt gewerkt, is het de zorgsector. Een aantal brancheorganisaties in de zorg, kortweg BoZ genoemd, heeft daarom een modelverwerkersovereenkomst opgesteld, waarin hoge eisen aan leveranciers worden gesteld.

Het is voor leveranciers onder meer verplicht om aantoonbaar te voldoen aan de ISO27001 en/of NEN7510, maar ook aan de NEN7512 en -7513, en aan 'andere NEN-normen die voor de gezondheidszorg van toepassing zijn verklaard'. Ook op de bekende discussiepunten, zoals het auditrecht, de meldplicht en ondersteuningsverplichtingen, dient de leverancier het een en ander te kunnen waarborgen. Voor essentiële zorginfrastructuren, zoals een elektronisch patiëntendossier, is dat, gezien de gevoeligheid van de persoonsgegevens, gewenst en zelfs vanzelfsprekend. Ook de Autoriteit Persoonsgegevens heeft in 2013 namelijk al aangegeven dat het NEN7510-normenkader in de zorgsector als standaard van informatiebeveiliging dient te worden gezien. Op grond van sommige wettelijke regelingen is het zelfs al verplicht om aantoonbaar hieraan te kunnen voldoen. Zoals hierboven ook al aangestipt, is dit wat lastiger voor leveranciers die niet tot kerntaak hebben om gezondheidsgegevens te verwerken. Hun dienstverlening is daar niet op ingericht, maar zij worden wel verwacht de verwerkersovereenkomst te ondertekenen. In dat geval komt de discussie vaak tot leven en wordt Bijlage 4 ten volle ingezet. Zoals ook bij de andere overeenkomsten, zullen partijen er uiteindelijk toch samen uit moeten komen.

Andere modellen
Naast de bovenstaande, veelgebruikte modellen bestaan er een aantal verwerkersovereenkomsten die standaard in kleinere kring worden gebruikt.

Zo biedt Coöperatie SURF een aantal modelovereenkomsten aan voor met name onderwijs- en onderzoeksinstellingen, in het SURF Juridisch Normenkader (Cloud)services. Naast een verwerkersovereenkomst, is een modelovereenkomst voor gezamenlijke verwerkingsverantwoordelijken gepubliceerd. Inmiddels wordt gewerkt met de derde versie van de verwerkersovereenkomst. Gezien de gevoeligheid van de persoonsgegevens van bijvoorbeeld studenten en onderzoekers, wordt ook hier meer dan het wettelijk

vereiste gevraagd van de leverancier. Wel zijn er in de laatste versie wat tegemoetkomingen gedaan ten opzichte van de leverancier. De bijlagen bieden wederom de mogelijkheid om de dienstverlening en beveiligingsmaatregelen praktisch in te vullen en om aanpassingen te doen op de standaardtekst.

Ook de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA) hanteert een model voor haar leden. Deze ziet vanzelfsprekend op de verwerking van persoonsgegevens bij de activiteiten die accountants als verwerker uitvoeren bij hun klanten, zoals in het geval van loonverwerking.

Als laatste voorbeeld biedt ook de Nederlandse Orde van Advocaten een modelverwerkersovereenkomst aan. Deze is, in tegenstelling tot het model voor accountants, bedoeld voor advocatenkantoren in de rol van verwerkingsverantwoordelijke.

Welke kenmerken hebben modelverwerkersovereenkomsten met elkaar gemeen?
Zoals hierboven al benoemd, is het allereerst nodig dat zowel de sector zelf als de wederpartijen het belang inziet van het gekozen model. Een heel eenzijdige verwerkersovereenkomst zal ertoe leiden dat wederpartijen hun hakken in het zand zetten en op hun beurt standaard aanpassingen eisen. Een aantal modellen is daarom vrij algemeen van aard en sluit waar mogelijk aan op de tekst van de AVG. Zo is de kans beperkt dat wederpartijen in discussie gaan over de voorgestelde afspraken. Gezien de waarborgen die dienen te worden geboden in de zorgsector, is daar in die branche logischerwijs minder sprake van.

Een ander kenmerk van modelverwerkersovereenkomsten is dat ze bestaan uit een hoofdtekst, waarin alle juridische afspraken staan, en één of meerdere lege bijlage(n) waarin alle specifieke details van de verwerking beschreven dienen te worden. Ook vereiste of geboden beveiligingsmaatregelen worden vaak in een bijlage beschreven. Daarnaast wordt vaak een overzicht opgenomen van de ingeschakelde subverwerkers en verwerkingslocaties. Vooral aan dat laatste wordt extra aandacht besteed sinds de Schrems II-uitspraak van afgelopen zomer van het Europese Hof.

Leveranciers die een generiek product of generieke dienstverlening aanbieden, kunnen de bijlagen standaard invullen. Het is dus aan te bevelen voor partijen, die diensten of producten aan scholen of gemeenten aanbieden, om hun eigen template van het toepasselijke model vast compleet te maken. Uiteraard kan dit niet wanneer de keuze voor de te verwerken persoonsgegevens door de klant wordt gemaakt. Wanneer de dienstverlening per klant verschilt zal per geval, in onderling overleg, bekeken moeten worden welke verwerking van persoonsgegevens zal plaatsvinden bij de levering van het product of de dienst.

Holland's next top model of extreme makeover?
Standaard verwerkersovereenkomsten zijn in veel sectoren gangbaar. Waar dat helpt om goede, passende afspraken te maken die de risico's van de verwerking van persoonsgegevens daadwerkelijk verkleinen, is dat een goede ontwikkeling. In sectoren waar geen model wordt gehanteerd, is vaak veel tijd nodig om het initiële voorstel van één partij tot een aanvaardbare verwerkersovereenkomst voor beide partijen te maken.

Verwerkingsverantwoordelijken en verwerkers moeten echter altijd voorzichtig zijn bij het gebruiken van een modelverwerkersovereenkomst. Het kan verleidelijk zijn om te denken dat een model one-size-fits-all betekent en daarom geen specifieke aanpak vereist. Wanneer de verwerkersovereenkomst niet in verhouding staat tot de risico's kan dat voor één van de partijen, of allebei, vervelende gevolgen hebben.

Menno Konst
Juridisch adviseur
Noord-Nederland

Jonas van Ginkel
Juridisch adviseur
Noord-Nederland

Marketing | Cloud

Pas op! Likes kopen, kost geld!

Sociale media worden steeds meer en steeds vaker door bedrijven gebruikt om producten en/of diensten op de markt te zetten. Bedrijven proberen daarbij zo goed als mogelijk voor de dag te komen waarbij de belangrijkste bron de beschikbare informatie op het internet is. Factoren als likes, reviews en volgers worden daarbij steeds belangrijker. Consumenten baseren immers hun aankoopgedrag op basis van deze factoren. Hierdoor is een ware handel ontstaan in 'nep'-likes, 'nep'-reviews en zelfs 'nep'-volgers. Volgens de Autoriteit Consument en Markt (hierna: de ACM) kan de consument hierdoor worden misleid en heeft dit effect op de concurrentie tussen bedrijven.[1] De ACM heeft in de zomer van 2020 aangekondigd om tegen deze misleidende praktijken op te treden. Recentelijk is hiervoor de eerste handelaar op de vingers getikt.[2]

Werkwijze ACM

De toezichthoudende autoriteit heeft onderzoek gedaan naar partijen die handelen in nep-likes, nep-reviews en nep-volgers. Ook Nederlandse partijen bieden dergelijke diensten aan. De ACM spoort deze aanbieders op, verstuurt waarschuwingsbrieven en draagt hen op om te stoppen met de dienstverlening. Verder wordt van deze partijen inzage gevorderd in het klantenbestand. Hiermee krijgt de ACM inzicht in welke bedrijven, influencers en anderen partijen gebruikmaken van nep-likes, nep-reviews en nep-volgers.

1. CM, 'ACM pakt handel in nepreviews en nep-likes aan', 25 juni 2020, via: https://www.acm.nl/nl/publicaties/acm-pakt-handel-nepreviews-en-neplikes-aan.
2. ACM, 'Besluit van de Autoriteit Consument en Markt op grond van artikel 2.9 van Wet handhaving consumentenbescherming tot het opleggen van een last onder dwangsom aan Bicep Papa B.V. wegens overtreding van artikel 8.8 van de Wet handhaving consumentenbescherming', 24 november 2020, via: https://www.acm.nl/sites/default/files/documents/last-onder-dwangsom-bicep-papa-voor-gebruik-nepvolgers-en-neplikes.pdf.

Op de radar

In juni 2020 wordt de ACM op de hoogte gesteld dat het bedrijf Bicep Papa B.V. (hierna: Bicep Papa) likes ingekocht zou hebben. Het vormt de aanleiding voor een onderzoek naar de online-activiteiten van het bedrijf. Deze activiteiten bestaan voornamelijk uit het verkopen van voedingsmiddelen en drogisterijwaren via een webshop. Door onder meer drie Instagram-accounts worden deze producten gepromoot. Uit opgevraagde informatie door de ACM blijkt dat Bicep Papa diensten heeft afgenomen van een aanbieder van nep-likes en nep-volgers. Vanaf 2018 zijn een grote hoeveelheid transacties verricht om dit te bekostigen. De aangekochte likes en volgers worden automatisch gegenereerd met behulp van robots waardoor nep-accounts zorgen voor de interactie.

Op basis van het uitgevoerde onderzoek heeft de ACM de handelswijze van Bicep Papa juridisch gezien beoordeeld. In het vervolg van het stuk zal allereerst worden stil gestaan bij wat een oneerlijke handelspraktijk is. Verder kijken wij inhoudelijk naar het besluit van de ACM en de eventuele verdere consequenties. Wij sluiten af met het aangeven wat de (juridische) ontwikkelingen zijn omtrent nep-likes en nep-volgers.

Oneerlijke handelspraktijken
Een oneerlijke handelspraktijk bestaat uit twee elementen. Allereest moet sprake zijn van een handelspraktijk. Het begrip handelspraktijk wordt in de wet ruim omschreven. Bijna iedere gedraging en/of handeling van een handelaar kan als handelspraktijk worden aangemerkt. Dit is zeker het geval bij reclame- en marketinguitingen. De handelspraktijk moet verband houden met de verkoop van een product of dienst. Van belang is dat de handelspraktijk wordt verricht tegenover een consument.

Vervolgens moet deze handelspraktijk als oneerlijk worden bestempeld. Hiervoor geeft de wet drie vereisten. Het eerste is dat de handelaar in strijd handelt met de vereisten van zijn professionele toewijding. De handelaar moet ten aanzien van de consument een bepaald niveau van vakkundigheid en zorgvuldigheid in acht nemen. Hij moet zich dus gedragen als een 'normale handelaar' die werkt volgens de professionele standaard. Ten tweede moet de consument de mogelijkheid hebben om een geïnformeerd besluit te nemen. Hierin mag hij niet worden beperkt door de handelaar. Tot slot moet de consument op basis van die informatie een keuze hebben genomen die hij anders niet had gemaakt. Deze consument is door het Hof van Justitie omschreven als een persoon die gemiddeld geïnformeerd, omzichtig en oplettend is.[3] Het is echter niet zo dat de consument daadwerkelijk moet zijn misleid. Het is voldoende als hij had kunnen worden misleid.

Misleidende handelspraktijken
De wet bepaalt dat een misleidende handelspraktijk als oneerlijk wordt gezien. Dat betekent dat als sprake is van een misleidende handelspraktijk, ook sprake is van een oneerlijke handelspraktijk. Men spreekt van een misleidende handelspraktijk wanneer de handelaar informatie verstrekt die feitelijk onjuist of misleidend is. Deze informatie moet worden gegeven ten aanzien van één van de genoemde gevallen in de wet. Bijvoorbeeld ten aanzien van het bestaan van het product; de hoedanigheid van de handelaar; de prijs etc. Daarnaast kan ook het weglaten van essentiële informatie worden gezien als een misleidende handelspraktijk.[4]

Naast de bovengenoemde voorbeelden benoemt de wet ook bepaalde handelspraktijken die altijd misleidend zijn.[5] Dit wordt ook wel de 'zwarte lijst' genoemd. Deze handelspraktijken worden onder alle omstandigheden als misleidend beschouwd. Het gevolg is dat als een handelaar zich schuldig maakt aan één van de genoemde handelingen, hij altijd een oneerlijke handelspraktijk verricht. Een voorbeeld hiervan is dat een handelaar beweert of de indruk wekt dat een product legaal kan worden verkocht terwijl dit niet het geval is.

Nep-likes en nep-volgers
Terug naar Bicep Papa. Bicep Papa promoot via Instagram producten aan consumenten en wordt aangemerkt als handelaar. Deze promotie houdt rechtstreeks verband met de (bevordering van) verkoop van producten. Dit wordt dan ook aangemerkt als een handelspraktijk. Beoordeeld moet worden of het gebruikmaken van nep-likes en nep-volgers in het kader van deze handelspraktijk aangemerkt kan worden als een oneerlijke handelspraktijk.

Het krijgen van veel likes en het hebben van veel volgers zegt iets over de kwaliteit of de populariteit van een handelaar en de aangeboden producten en diensten. Het schetst een beeld dat veel consumenten een product of dienst aanraden en ervaring hebben met de handelaar. Meer likes en meer volgers geven een positiever beeld en wekken de indruk dat een bepaalde handelaar als 'goed en betrouwbaar' kan worden aangemerkt. Hierdoor wordt de consument op het verkeerde been gezet en dus misleid. Als de gemiddelde consument had geweten dat de Instagram-accounts van Bicep Papa minder volgers en likes zouden hebben, dan had een consument wellicht het gepromote product niet gekocht. Daarnaast is de ACM van mening dat als een handelaar nep-likes of nep-volgers plaatst of laat plaatsen, dat de handelaar zich dan op bedrieglijke wijze voordoet als consument. Dit is onder alle omstandigheden misleidend, aangezien deze handelspraktijk op de 'zwarte lijst' staat.[6] De ACM concludeert dat de handelspraktijken van Bicep Papa op meerdere vlakken als misleidend moet worden beschouwd en het daarom een oneerlijke handelspraktijk betreft.

Het vormt de aanleiding voor de ACM om handhavend op te treden tegen nep-likes en nep-volgers. De toezichthouder legt Bicep Papa een last onder dwangsom op met een maximum van € 100.000. De last onder dwangsom heeft als doel om een bepaalde onrechtmatige handeling te beëindigen voor een vastgestelde datum. Bicep Papa moet ervoor zorgen dat voor die datum de nep-likes en nep-volgers ongedaan zijn gemaakt. Als Bicep Papa deze onrechtmatige situatie niet tijdig herstelt, is het bedrijf gehouden om per week een dwangsom te betalen van € 12.500.

3. HvJ EU 16 juli 1998, C-210/96, ECLI:EU:C:1998:369, r.o. 31.
4. Artikel 6:193b; artikel 6:193c; artikel 6:193d Burgerlijk Wetboek.
5. Artikel 6:193g Burgerlijk Wetboek.
6. Artikel 6:193g sub v Burgerlijk Wetboek.

Mogelijke consequenties
De zaak van Bicep Papa laat zien dat de inzet van nep-likes en/of nep-volgers vergaande financiële risico's met zich mee kunnen brengen. Naast de last onder dwangsom heeft de ACM nog een ander instrument om ervoor te zorgen dat een verboden handeling wordt bestraft: de bestuurlijke boete.[7] Met een bestuurlijke boete kan een handelaar bestraft worden voor het verrichten van de oneerlijke handelspraktijk. In tegenstelling tot de last onder dwangsom betreft dit niet een herstelsanctie, maar ligt de nadruk op het straffen van de handelaar.

De last onder dwangsom en de bestuurlijke boete kunnen afzonderlijk worden opgelegd. De ACM heeft echter de mogelijkheid om ook beide instrumenten gelijktijdig op te leggen als een handelaar zich schuldig maakt aan een oneerlijke handelspraktijk.

Ook de consument heeft bepaalde rechten als een overeenkomst tot stand komt als gevolg van een oneerlijke handelspraktijk. De consument kan deze overeenkomst laten vernietigen. Als dat gebeurt bestaat de overeenkomst op dat moment niet meer. Een consument die misleid wordt, heeft dus de mogelijkheid om de overeenkomst te vernietigen.[8]

Daarnaast kan een handelaar ook aansprakelijk worden gesteld voor de ontstane schade aan de kant van de consument. In dat geval dient de handelaar te bewijzen dat de schade niet door zijn praktijk is ontstaan. De bewijslast ligt daardoor bij de handelaar.[9]

En hoe nu verder...
Op dit moment is er een ontwikkeling gaande dat het plaatsen van nep-likes en nep-volgers harder aangepakt moet worden. De ACM heeft de eerste stap gezet door een last onder dwangsom op te leggen. Wij verwachten dat de ACM in de toekomst meer handhavend gaat optreden tegen deze handelspraktijken.

Op basis van de huidige regelgeving moeten vele stappen genomen worden om aan te tonen dat een consument wordt misleid. Dit gaat veranderen nu de Europese wetgever de richtlijn modernisering consumentenrechten heeft opgesteld. Deze richtlijn brengt een aantal veranderingen met zich mee ten aanzien van de oneerlijke handelspraktijken.

Zo wordt de zwarte lijst uitgebreid met een aantal handelspraktijken die onder alle omstandigheden misleidend zijn. Toegevoegd gaat onder meer worden:

"Het plaatsen of een andere rechts- of natuurlijke persoon de opdracht geven tot het plaatsen van valse beoordelingen of aanbevelingen van consumenten of het op misleidende wijze voorstellen van consumenten-beoordelingen of aanbevelingen op sociale media, teneinde producten te promoten."[10]

De richtlijn moet door de Nederlandse wetgever omgezet worden naar nationale wetgeving. De eerste stappen zijn hiervoor gezet en een voorstel van wet ligt op tafel. In de Memorie van Toelichting van dit voorstel geeft de wetgever daarbij expliciet aan dat onder dit artikel ook nep-likes vallen. Wij verwachten dat ook nep-volgers onder dit artikel geschaard kunnen worden.[11]

Deze ontwikkeling betekent dat de ACM alleen maar hoeft na te gaan of een handelaar nep-likes of nep-volgers heeft geplaatst of laten plaatsen. De reden hiervoor is dat een dergelijke praktijk onder alle omstandigheden misleidend is. Het wordt daarmee voor de toezichthouder makkelijker om aan te tonen dat sprake is van een oneerlijke handelspraktijk. Mede gezien het feit dat de ACM handhavend optreedt, zal het voor een handelaar op sociale media niet meer lonen om nep-likes dan wel nep-volgers te kopen. Het moge duidelijk zijn, likes kopen gaat uiteindelijk meer geld kosten.

7. Artikel 2.9 Wet handhaving consumentenrechten.
8. Artikel 6:193j lid 3 Burgerlijk Wetboek.
9. Artikel 6:193j lid 2 Burgerlijk Wetboek.
10. Richtlijn (EU) 2019/2161 betreft beter handhaving en modernisering van de regels voor consumentenbescherming.
11. Implementatie wet richtlijn modernisering consumentenbescherming van 23 oktober 2020 p. 5 MvT www.internetconsultatie.nl.

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Internetrechtspraak

Meerdere AVG-verwijderingsverzoeken in korte tijd
(Rechtbank Den Haag, 27 november 2020)
In deze zaak gaat het om de verwijdering van zoekresultaten die in Google verschijnen. De twee verzoekers in deze zaak hadden bij Google een verzoek ingediend om zoekresultaten over hun betrokkenheid bij een vermeende fraudezaak te laten verwijderen. Google heeft vervolgens enkele URL's verwijderd, maar niet alle. Vervolgens kwam er vanuit de twee verzoekers nog twee keer een verwijderingsverzoek binnen bij Google. Een deel van de URL's in die latere verzoeken waren URL's waarvan Google al had laten weten dat het die niet zou verwijderen. Google wilde de al behandelde URL's dan ook niet nog een keer behandelen. De vraag die in deze zaak speelt is: mag dat? In artikel 21 AVG staat dat een betrokkene te allen tijde bezwaar mag maken. Maar geldt dit ook nadat een verwijderingsverzoek is afgewezen? Of mag Google weigeren gevolg te geven aan het verzoek vanwege het repetitieve karakter? Maakt het dan nog uit binnen welk tijdsbestek soortgelijke verwijderverzoeken zijn ingediend? De rechtbank is voornemens deze prejudiciële vragen voor te leggen aan het Hof van Justitie van de Europese Unie.

https://bit.ly/3q5M8V9

Langskomen gemeentehuis niet vereist voor identificatie
(Raad van State, 9 december 2020)
Op grond van de AVG moet bij het honoreren van rechten van betrokkenen door de verwerkingsverantwoordelijke gecontroleerd worden of het verzoek ook daadwerkelijk van de juiste persoon komt. De verzoeker in deze zaak verzocht de gemeente Uithoorn om zijn persoonsgegevens te wissen. Bij dit verzoek heeft hij een kopie van een gewaarmerkte kopie van zijn paspoort gevoegd. De gemeente vond echter dat hiermee de identiteit niet deugdelijk vastgesteld kon worden en verzocht hem om langs te komen op het gemeentehuis. De verzoeker kwam niet langs, maar overhandigde nogmaals de kopie én verzocht om een DigiD-link zodat hij zichzelf daarmee kon identificeren. Het college besloot om het verzoek niet te behandelen. Hier maakte verzoeker bezwaar tegen, maar het bezwaar werd ongegrond verklaard. Waar de rechtbank het met het college eens was, vond de Raad van State dat dit anders lag. Er waren in dit geval namelijk ook andere mogelijkheden om de identiteit vast te stellen, naast langskomen op het gemeentehuis. Het overleggen van een kopie van een paspoort wordt daarnaast in beginsel als een redelijke maatregel aangemerkt om de identiteit te controleren. Ook heeft het college aangegeven niet te twijfelen aan de identiteit. De eis van het college was in dit geval daarom geen redelijke maatregel. De rechtbank heeft ten onrechte geoordeeld dat het college in redelijkheid van verzoeker heeft mogen eisen om langs te komen op het gemeentehuis.

https://bit.ly/3b1Kaki

***Printing on demand* houdt boek beschikbaar voor publiek**
(Gerechtshof Amsterdam, 15 december 2020)
Appellante is auteur. Zij heeft een exploitatieovereenkomst gesloten met uitgever Overamstel voor de uitgave van een door haar geschreven boek. Appellante komt in 2017 te weten dat haar boek uitverkocht is en de uitgever van plan is exemplaren alleen nog te leveren via *'printing on demand'.* Dit is een nieuwe productiewijze waarbij een boek slechts geprint wordt wanneer een boekhandelaar of koper daarom vraagt. Appellante is het oneens dat haar boek middels deze wijze wordt uitgegeven en geeft dit aan bij de uitgever. De uitgever wil echter niet akkoord gaan met een herdruk van het boek. Appellante besluit daarom de exploitatieovereenkomst te beëindigen, primair op grond van artikel 16 van de overeenkomst, subsidiair op grond van artikel 25e Auteurswet. De rechter oordeelt dat er geen grond is voor toewijzing van de vordering van appellante. Bij artikel 16 van de overeenkomst is het van belang dat het boek 'beschikbaar is voor het publiek'. Dat betekent dat het boek binnen een maand in boekvorm verkrijgbaar moet zijn. Middels *printing on demand* kan het boek ruim binnen die termijn verkregen worden. Uitgever Overamstel wordt daarom gevolgd in de stelling dat zij met het beschikbaar stellen van *printing on demand*

de titel ‘in boekvorm voor het publiek’ beschikbaar heeft gehouden.

https://bit.ly/2PbRpgT

BKR-registratie
(Gerechtshof Arnhem-Leeuwarden, 17 december 2020)
Het hof ‘s-Hertogenbosch heeft in augustus 2020 geoordeeld dat kredietregistratie door financiële instellingen (banken) wel als wettelijke verplichting valt aan te merken en dat de verzoeker daarom geen recht heeft op bezwaar uit artikel 21 AVG. In september 2020 oordeelde het hof Den Haag echter dat er geen sprake is van een wettelijke verplichting in deze vorm van gegevensverwerking. Het hof Arnhem-Leeuwarden heeft vervolgens op 17 december 2020 uitspraak gedaan in een zaak die betrekking heeft op BKR-registratie. Het hof Arnhem-Leeuwarden verwijst in deze uitspraak naar de twee eerdere beschikkingen van augustus en september en sluit zich aan bij de uitspraak van het hof ‘s-Hertogenbosch van augustus. Volgens het hof Arnhem-Leeuwarden wordt in de beschikking van hof Den haag geen (kenbare) aandacht besteed aan de (naar het oordeel van het hof overtuigende) argumenten waarop het hof ‘s-Hertogenbosch in zijn beschikking van augustus concludeerde dat de registratie van kredietgegevens in het Centraal Krediet Informatiesysteem juist wel plaatsvindt op grond van een wettelijke plicht als bedoeld in artikel 6 lid 1 onder c AVG. Banken mogen volgens hoven Arnhem-Leeuwarden en ‘s-Hertogenbosch dus voor de uitoefening van hun wettelijke plicht tot deelname aan een kredietregistratiesysteem rechtmatig persoonsgegevens laten verwerken door BKR. Wanneer de verwerking van persoonsgegevens gebaseerd is op een wettelijke plicht zoals hier, kan de betrokkene geen beroep doen op het in artikel 17 AVG neergelegde recht op gegevenswissing. De betrokkene heeft in dat geval ook niet het recht van bezwaar als bedoeld in artikel 21 AVG, omdat dat recht is verbonden aan gegevensverwerking op grond van artikel 6 lid 1 onder e en f AVG.

https://bit.ly/3b2bjTZ

Artikelen 149 en 151a van de Gemeentewet geven geen bevoegdheid om bijzondere persoonsgegevens te verwerken
(Raad van State, 23 december 2020)
Op grond van artikel 151a van de Gemeentewet heeft de gemeenteraad van Utrecht een vergunningstelsel voor seksinrichtingen en escortbedrijven in de Algemene plaatselijke verordening (hierna: APV) opgenomen. Een voorwaarde om te mogen werken als raamprostituee is dat voldaan wordt aan de registratieplicht. In het gemeentelijk systeem wil de burgemeester NAW-gegevens, het telefoonnummer, e-mailadres, bankrekeningnummer, geboortedatum, nationaliteit, geboorteplaats en -land, verblijfsstatus, IP-adres, signalen van mensenhandel, spreektaal, KvK-nummer, eerdere registratie en politiegegevens gaan verwerken. Als grondslag voor het verwerken van deze (bijzondere) persoonsgegevens van de sekswerkers koos de gemeente voor de uitzonderingsgrond ‘het zwaarwegend algemeen belang’, waarbij als belang het tegengaan van ernstige misstanden als uitbuiting en mensenhandel wordt aangedragen. De Autoriteit Persoonsgegevens (AP) heeft zich echter op het standpunt gesteld dat voor een dergelijke registratieplicht in een APV het zwaarwegend algemeen belang geen toereikende grondslag is, op grond waarvan het verbod van gegevensverwerking kan worden doorbroken. De gegevensverwerking wordt daarom onrechtmatig geacht. De gemeente was het hier niet mee eens, maar de Raad van State wel. De bepalingen waarop de gemeente een beroep doet geven geen uitdrukkelijke bevoegdheid om een uitzondering te maken op het verbod om bijzondere persoonsgegevens te verwerken.

https://bit.ly/3b5L5jA

Werknemer heeft geen recht op inkomsten auteursrechten
(Rechtbank Noord-Holland, 24 december 2020)
Onderneming SI Music houdt zich bezig met het commercieel produceren en exploiteren van muziek voor opdrachtgevers. X is in 2011 in dienst getreden en maakt muziekwerken die vervaardigd worden voor relaties van SI Music. Deze muziekwerken zijn vanaf de aanvang van het dienstverband niet onder de naam van SI Music aangemeld bij Buma/Stemra, maar onder de naam van X. De reden hiervoor is dat Buma/Stemra alleen natuurlijke personen kent als deelnemers, geen rechtspersonen. Over de jaren 2013 tot en met 2018 heeft Buma/Stemra in totaal € 193.785,09 betaald aan X in verband met ROA, de zogenoemde Regeling Oudedagsvoorziening Auteurs. SI Music heeft X gesommeerd dit bedrag aan haar door te betalen. X weigert en beargumenteert dat de ROA een oudedagsvoorziening is die volgens de verstrekker Buma/Stemra geen exploitatie-inkomst is. De ROA is volgens hem in het leven geroepen met een sociaal-cultureel doel en mag alleen besteed worden als oudedagsvoorziening. X voert tevens aan dat SI Music niet heeft voldaan aan haar informatie- en zorgplicht en dat uit de arbeidsovereenkomst niet volgt dat X verplicht is om het betaalde bedrag te betalen. De kantonrechter oordeelt dat uit de arbeidsovereenkomst duidelijk volgt dat X geen recht heeft op het door Buma/Stemra betaalde bedrag, omdat dit rechtstreeks voortvloeit uit inkomsten van muziekauteursrechten.

X heeft zich wel terecht op het standpunt gesteld dat hij nog aanspraak heeft op een betaling van een bonus, waardoor deze aanspraak verrekend wordt met de vordering van SI Music. Daarnaast vindt de kantonrechter de opgelegde boete van € 257.000 bovenmatig en matigt hij deze daarom tot een bedrag van € 5.000.

https://bit.ly/3ulja16

Verwijzen naar merk om compatibiliteit aan te tonen mag alleen als de verwijzing juist is in de ogen van het relevante publiek
(Hoge Raad, 8 januari 2021)
Verwijzen naar een merk om compatibiliteit aan te tonen mag op grond van het Benelux-verdrag inzake de intellectuele eigendom (BVIE). Deze verwijzing is alleen toegestaan als de verwijzing juist is. In deze zaak ging het om een chipfabrikant, Infineon, die chips maakt voor chipkaarten. Bij de verkoop van deze chips vermeldt Infineon dat deze chips 'Mifare compatibel' zijn. Dit is om aan te geven dat de chips uitgelezen kunnen worden door MIFARE-kaartlezers. Volgens NXP, houder van het woordmerk MIFARE, is deze verwijzing niet toegestaan omdat de verwijzing niet juist is. Er is namelijk een *add-on* nodig om de compatibiliteit te bewerkstelligen. De Hoge Raad stelt dat de juistheid van een verwijzing naar een merk om compatibiliteit aan te tonen volgens 'de eerlijke gebruiken in nijverheid en handel' beoordeeld moet worden. Het doel van verwijzend merkgebruik is het informeren van de koper over de compatibiliteit.
De Hoge Raad stelt daarom dat bij het beoordelen van de juistheid van de verwijzing gekeken moet worden hoe het relevante publiek de verwijzing zal opvatten. Het gaat hier om een product dat verkocht wordt aan bedrijven met een hoge graad van deskundigheid. Daarbij stelt Infineon dat er nog nooit geklaagd is door haar klanten over (ontbrekende) compatibiliteit van de chips met MIFARE-kaartlezers. Het enkele feit dat er een *add-on* nodig is, betekent dus niet dat de verwijzing onjuist is.

https://bit.ly/3q5OtPV

Zwarte lijst met namen artsen verboden in kort geding
(Rechtbank Midden-Nederland, 8 januari 2021)
In dit kort geding voor de rechtbank Midden-Nederland vorderde de Stichting Stop Online Shaming (Stichting SOS) van een andere stichting genaamd Stichting Slachtoffers Iatrogene Nalatigheid-Nederland (SIN.nl), dat SIN-NL de domeinnamen zwartelijstartsen.nl en zwartelijstartsen.com binnen twee werkdagen zou overdragen aan eiseres en daarnaast een verzoek bij Google zou indienen om verwijzingen naar de site te verwijderen. Dit alles onder last van een dwangsom. Een van de redenen voor deze eisen was dat volgens Stichting SOS de inhoud van de website in strijd zou zijn met diverse artikelen van de AVG. Alles tegen elkaar afwegend oordeelde de kortgedingrechter dat het door Stichting SOS vertegenwoordigde belang dat individuele zorgverleners door publicaties niet behoren te worden blootgesteld aan lichtvaardige verdachtmakingen, naar zijn oordeel zwaarder woog dan het belang van SIN.nl om aandacht te vragen voor (het verzwijgen van) medische fouten. In het kort kwam het erop neer dat de rechter in deze zaak het recht op eerbiediging van de goede naam zwaarder vond wegen dan het recht op vrijheid van meningsuiting. De zwarte lijst met namen van artsen is dan ook niet toegestaan.

https://bit.ly/3b5ITtK

Schadevergoeding wegens aantasting in persoon
(Rechtbank Noord-Nederland, 12 januari 2021)
Gemeente Oldambt heeft in 2016 een perceel waarop zich een niet meer in gebruik zijnde schietbaan bevond te koop gezet voor een symbolisch bedrag van € 1. Eiser heeft belangstelling voor de aankoop van de schietbaan. Hij vraagt daarom een omgevingsvergunning aan en vult zijn gegevens in. Zijn gegevens zijn vervolgens onterecht openbaar gemaakt. In deze procedure gaat het om de vraag of eiser in verband met een aantal datalekken op de gemeentelijke website tegenover de gemeente aanspraak kan maken op betaling van een schadevergoeding voor de door hem gestelde materiele en immateriële schade. Eiser claimt dat hij zowel materiële als immateriële schade heeft geleden doordat zijn openbaargemaakte vergunningsaanvraag bijna twee jaar lang ten onrechte voor iedereen zichtbaar op de website van de gemeente heeft gestaan.
Zo waren zijn BSN-nummer, e-mailadres en mobiele telefoonnummer openbaar gemaakt. Eiser stelt materiële schade te hebben geleden, omdat hij ten gevolge van de datalekken zich niet veilig voelde en daardoor bepaalde veiligheidsmaatregelen heeft genomen. Zo heeft hij rolluiken, alarm- en camerasystemen aangeschaft. Deze schade was begroot op € 11.000. De immateriële schade bestond uit sterke angstgevoelens. Eiser stelt zich lange tijd niet veilig te hebben gevoeld in zijn eigen huis als gevolg van het voor lange tijd openbaar zijn van zijn persoonsgegevens. De kantonrechter concludeert dat de gemeente met het ontstaan van genoemde datalekken de AVG heeft geschonden en daarom schadeplichtig is jegens eiser. Hij oordeelt dat geen aanleiding bestaat voor toewijzing van een bedrag aan materiële schadevergoeding, omdat de door eiser getroffen beveiligingsmaatregelen aan zijn

woning niet als redelijke kosten ter voorkoming of beperking van schade als gevolg van de datalekken aangemerkt konden worden. De vordering van immateriële schade wordt wel toegewezen. De persoonlijke levenssfeer van eiser was geschonden en nadelige gevolgen zoals identiteitsfraude lagen voor de hand. Omdat de datalekken niet tot concrete negatieve gevolgen hebben geleid, stelt de kantonrechter de schadevergoeding vast op een bedrag van € 500.

https://bit.ly/3b2Xgxr

Verhouding leidende toezichthouder tot andere betrokken nationale toezichthouders
(Conclusie AG Bobek, 13 januari 2021)
Het hof van beroep te Brussel had het Hof van Justitie van de Europese Unie de vraag voorgelegd of de AVG zich ertegen verzet dat een andere nationale gegevensbeschermingsautoriteit dan de leidende gegevensbeschermingsautoriteit in haar lidstaat een gerechtelijke procedure instelt in verband met schendingen van de AVG bij grensoverschrijdende gegevensverwerking. Volgens advocaat-generaal (AG) Bobek is de gegevensbeschermingsautoriteit van de staat waar een verwerkingsverantwoordelijke of verwerker zijn hoofdvestiging in de Europese Unie heeft, algemeen bevoegd om gerechtelijke procedures in te stellen als de AVG is geschonden bij grensoverschrijdende gegevensverwerking. Bobek beperkt het recht om juridische procedures te starten met betrekking tot overtredingen van de AVG hiermee niet tot enkel de zogenoemde *'lead authority'.* Volgens Bobek zijn overige betrokken gegevensbeschermingsautoriteiten ook bevoegd om op dit gebied op te treden, maar beperkter. Het is nog afwachten of het Hof de conclusie van de AG volgt.

https://bit.ly/3uSnWsW

Belgische privacy-activisten verliezen beroep tegen vingerafdruk op ID-kaart
(Grondwettelijk Hof, België, 14 januari 2021)
België mag vingerafdrukken opslaan op de elektronische identiteitskaart (eID) van burgers. De Belgische overheid doet dit om identiteitsfraude tegen te gaan. Het Grondwettelijk Hof vond dat dit de inbreuk op de privacy rechtvaardigt. De betreffende wet voorziet in voldoende waarborgen om onevenredige gevolgen te voorkomen. Er is namelijk geen permanent centraal register waarin alle vingerafdrukken van burgers worden verwerkt en de autoriteiten die gemachtigd zijn om de gegevens te lezen worden limitatief opgesomd. De privacy voorvechters die de zaak hebben aangespannen gaan kijken of ze naar het Europees Hof voor de Rechten van de Mens kunnen stappen.

https://bit.ly/3dVwxVs

Twitterbericht burgemeester niet onrechtmatig
(Rechtbank Rotterdam, 15 januari 2021)
Een burgemeester (gedaagde), lid van het CDA, heeft op Twitter een bericht geplaatst waarin hij verwijst naar een speech van Thierry Baudet van Forum voor Democratie na de Provinciale Statenverkiezing. De tweet luidde: *"Iemand zei tegen me dat de elite geen boeken leest. Ofzo. Dus heb ik wat boeken die ik voor m'n studie doornam maar weer op de leesstapel gelegd. Kijken of ik er nog wat van kan op steken",* met daarbij afbeeldingen van boeken over fascisme en nationaalsocialisme. Twee dagen later was het bericht verwijderd.
De kantonrechter oordeelt dat gedaagde met zijn tweet een verband legde tussen Baudet en het Forum enerzijds en het fascisme en nationaalsocialisme anderzijds. De kantonrechter oordeelde dat het mogelijk is dat leden en aanhangers van het Forum, waaronder eiser, het niet eens zijn met de inhoud van de tweet of zich erdoor beledigd voelen. Het feit dat een uitlating beledigend is of zo kan worden ervaren is echter niet op zichzelf onrechtmatig. Daarnaast is de uitlating gedaan in het kader van een politiek debat. Zo'n uitlating zal niet snel onrechtmatig zijn, omdat het politieke debat 'scherp' gevoerd moet kunnen worden. Er is geen sprake van schending van artikel 20 van het Internationaal verdrag inzake burgerrechten en politieke rechten, welke bepaling het propageren van op nationale afkomst, ras of godsdienst gebaseerde haatgevoelens die aanzetten tot discriminatie, veiligheid of geweld verbiedt. Het bericht heeft namelijk geen betrekking op afkomst, ras of godsdienst. Daarnaast zet het bericht volgens de kantonrechter niet aan tot discriminatie, vijandigheid of geweld. Gedaagde heeft weliswaar met zijn bericht het gedachtegoed van Baudet en het Forum in verband gebracht met het fascisme en nationaalsocialisme, maar deze uitlating valt binnen de grenzen van de vrijheid van meningsuiting, omdat het om een waardeoordeel gaat dat is geuit in het kader van het publieke debat. Daarom heeft de burgemeester niet onrechtmatig gehandeld. Eiser voert nog aan dat het bericht niet binnen de grenzen van meningsuiting valt, omdat gedaagde heeft verklaard dat het bericht zijn eigen mening niet juist weergeeft. Eiser stelt dat de vrijheid van meningsuiting geen uitlatingen bevat die iemand doet terwijl diegene in werkelijkheid een andere mening heeft, maar dat standpunt is niet juist. Ook deze uitlatingen vallen onder de vrijheid van meningsuiting.

https://bit.ly/2O8JWPe

Aanbieder "The Tasting Games" mag deze naam blijven gebruiken
(Rechtbank Amsterdam, 28 januari 2021)
X heeft een eenmanszaak welke actief is op het gebied van smaak en smaakbeleving. Onder andere worden proeverijen van dranken en voedingsmiddelen met veelal een spelelement aangeboden. X maakt gebruik van domeinnaam tastinggame.nl en is actief op Facebook en Instagram onder de accountnaam 'tastinggame' met als titel "The Tasting Game". Op 17 september 2020 zijn twee vennootschappen onder de statutaire- en handelsnamen The Tasting Games Nederland B.V. en The Tasting Games International geregistreerd in het handelsregister. Daarnaast maakt The Tasting Games c.s. gebruik van verschillende domeinnamen, waaronder thetastinggames.nl. PlayToTV B.V. heeft deze vennootschappen opgericht met als doel het exploiteren van haar online gaming technologie in een nieuw product: 'tasting games', een proeverij spel. Dit spel wordt aangeboden middels een app genaamd 'The Tasting Games'. X heeft The Tasting Games c.s. gesommeerd om elk gebruik als handelsnaam, domeinnaam en e-mailadres van de benaming Tasting Games of The Tasting Games (met 'Nederland' en 'International' als toevoeging) te staken. X vindt dat The Tasting Games c.s. in strijd handelt met artikel 5 Handelsnaamwet. The Tasting Games c.s. handelt volgens haar onrechtmatig door de nodeloze verwarring van het gebruik 'Tasting Games' ter aanduiding van de app, als ook het gebruik van de domeinnamen 'thetastinggames.nl' en 'thetastinggamesshop.nl'. The Tasting Games c.s. heeft hiertegen aangevoerd dat X geen feitelijke uitvoering geeft aan de naam 'Tasting Game' en dat 'Tasting Game' als louter beschrijvende naam geen onderscheidend vermogen heeft. Volgens The Tasting Games c.s. maakt zij ook geen gebruik meer van de 'the tasting games' als handelsnaam, maar uitsluitend als merk en domeinnaam. De rechter oordeelt dat eisers wel degelijk gebruik maakt van de handelsnaam 'Tasting Game', maar dat deze als louter beschrijvend dient te worden aangemerkt. Door de beperkte bescherming van de handelsnaam is het niet aannemelijk dat het gebruik van 'the tasting games' als merk tot verwarring zal leiden. Omdat er geen sprake is van verwarringsgevaar, is het gebruik van de naam 'the tasting games' als merk door The Tasting Games c.s. niet onrechtmatig.

https://bit.ly/3029KPG

Parkeerwekker zit rechtbank niet zo lekker
(Rechtbank Amsterdam, 1 februari 2021)
Parkeerwekker is een systeem dat scanauto's van de gemeente herkent. Als het systeem een scanauto waarneemt krijgt de gebruiker daarover een melding. De gebruiker kan dan snel de parkeerkosten betalen om zo een boete te ontlopen. Volgens Parkeerwekker is het alleen een middel om vergeetachtige gebruikers te helpen. De rechter kon zich daar niet in vinden en was van mening dat Parkeerwekker aanzet tot onrechtmatige gedragingen, te weten het niet betalen van de (volledige) verschuldigde parkeerbelasting. Dit levert een onrechtmatige gedraging op tegen de gemeente. Het gebruik en aanbieden van Parkeerwekker is in Amsterdam nu verboden.

https://bit.ly/3uGp96v

Concurrenten kunnen geen beroep doen op de AVG
(Rechtbank Zeeland-West-Brabant, 3 februari 2021)
In deze zaak ging het om aanbieders van GPS-horloges voor ouderen. De GPS-horloges van de partijen hebben speciale functies om ouderen te helpen in het geval van nood. Zo is er een GPS-functie voor wanneer ze de weg kwijt zijn en kunnen ze noodoproepen maken als er iets aan de hand is. LCT en LifeWatcher vinden dat Avium zich schuldig maakt aan oneerlijke concurrentie. LCT en LifeWatcher maken namelijk gebruik van dure software terwijl Avium gratis software gebruikt. Ze baseren hun vordering op onrechtmatige daad en stellen dat Avium in strijd handelt met een wettelijke plicht. Ze zijn van mening dat Avium in strijd handelt met zowel de Wet oneerlijke handelspraktijken als de AVG. Met betrekking tot de schending van de AVG oordeelt de rechtbank dat concurrenten geen beroep op de AVG toekomt. Alleen de toezichthouder en de betrokkenen kunnen actie ondernemen op grond van de AVG. LCT en LifeWatcher hebben ook gesteld dat Avium door het gebruik van gratis software aan oneerlijke concurrentie doet. De rechtbank stelt vast dat gratis software niets nieuws onder de zon is en dat het gebruik ervan niet leidt tot oneerlijke concurrentie. Avium heeft haar gebruikers er ook voldoende over geïnformeerd.

https://bit.ly/3r51iLD

Gedwongen ontgrendelen van een smartphone toegestaan
(Hoge Raad, 9 februari 2021)
Cassatie in belang der wet. In deze zaak werd de telefoon van een verdachte ontgrendeld door de verdachte te boeien en zijn duim op de vingerafdrukscanner te plaatsen. De vraag in cassatie was of artikel 61a van het Wetboek van Strafvordering voldoende wettelijke grondslag biedt voor het op deze wijze toegang verkrijgen tot de smartphone. De advocaat van de verdachte droeg aan dat het handelen van de politie in strijd was met artikel 6 EVRM en het daaruit voortvloeiende nemo tenetur-beginsel. Dit beginsel houdt (kort gezegd) in dat een verdachte niet verplicht is om bewijs tegen zichzelf

te leveren. Het is aan de opsporingsautoriteiten om dit bewijs te verzamelen. Uitgaande van het nemo tenetur-beginsel, kan een verdachte niet worden gehouden om belastende informatie vrij te geven, of om bijvoorbeeld de wachtwoorden van zijn of haar telefoon of computer aan de opsporingsautoriteiten te overhandigen. De politie heeft overigens wel bevoegdheden om zelf te proberen zo'n computer of telefoon te kraken, al is dat in de praktijk niet altijd eenvoudig. De belangrijkste overweging van de rechtbank (en nu ook van de Hoge Raad) is dat het nemo tenetur-beginsel niet onbegrensd is. Waar het nemo tenetur-beginsel géén bescherming tegen biedt, is het passief ondergaan van bepaalde onderzoeksmaatregelen. Als er onderzoeksmateriaal is dat onafhankelijk van de wil van de verdachte bestaat, dan mogen opsporingsautoriteiten dat desnoods onder (gepaste) dwang van de verdachte verkrijgen. Een vingerafdruk van de verdachte bestaat namelijk onafhankelijk van zijn of haar wil. En daar biedt het nemo tenetur-beginsel dus géén bescherming tegen. Daarmee is er volgens de Hoge Raad grondrechtelijk geen bezwaar om die vingerafdruk onder (lichte) dwang van de verdachte af te nemen. Zie de blog op pagina 35.

https://bit.ly/3uFrVc1

Deliveroo bezorgers hebben een arbeidsovereenkomst
(Gerechtshof Amsterdam, 16 februari 2021)
Bezorgers van Deliveroo werken op basis van een opdrachtovereenkomst in plaats van een arbeidsovereenkomst. Op die manier is Deliveroo niet gebonden aan de strenge regels die op een arbeidsovereenkomst van toepassing zijn. FNV is het niet eens met deze praktijken en is van mening dat de overeenkomst tussen de bezorgers en Deliveroo eigenlijk wel een arbeidsovereenkomst is. Deliveroo zal zich daarom aan de regels moeten houden die gelden voor een arbeidsovereenkomst. Deliveroo is het hier niet mee eens en stelt dat zij een IT-onderneming zijn die opdrachtgevers (restaurants) en opdrachtnemers (bezorgers) bij elkaar brengt. Het hof heeft alle omstandigheden van de werkzaamheden beoordeeld en is van mening dat slechts de aan de bezorgers gegeven vrijheid ten aanzien van het verrichten van de arbeid, een omstandigheid is die wijst op de afwezigheid van een arbeidsovereenkomst. Alle andere omstandigheden, zoals de wijze van loonbetaling, het uitgeoefende gezag en de zekere werktijden wijzen meer op de aanwezigheid van een arbeidsovereenkomst. De vrijheid die bezorgers hebben is overigens niet onverenigbaar met het kwalificeren van de overeenkomst als een arbeidsovereenkomst. Het hof oordeelt dus, in lijn met de kantonrechter, dat er sprake is van een arbeidsovereenkomst tussen de bezorgers en Deliveroo. Zie de noot op pagina 33.

https://bit.ly/3e4K7pw

Sten Demon
Manager Legal & Technology

Innovatie

Legal tech

Waarom moeilijk doen als het makkelijk kan?

Inderdaad, met legal tech kunnen juridische processen een stuk efficiënter verlopen. Maar met dit artikel gooien we het over een hele andere boeg. Dit artikel gaat namelijk over verandermanagement: Hoe krijg je jouw organisatie nu mee in de overstap naar legal tech? Normaal gesproken wordt het maar lastig gevonden en leidt verandering tot weerstand. De inzet van nieuwe technologieën vereist behoorlijk wat overtuigingskracht. De pandemie heeft echter bewezen dat zelfs de meest conservatieve ondernemingen makkelijk veranderen als het écht moet.

Gereedschap of proces?
Legal tech is een *hypewoord* dat al jaren zeer breed wordt gebruikt. Stap voor stap verandert legal tech de dagelijkse werkzaamheden van juristen en dat zal voorlopig zo doorgaan. Ik verwacht bijvoorbeeld niet dat we over vijf jaar nog handmatig een geheimhoudingsovereenkomst *van a tot z* controleren.

In de meeste gevallen kan legal tech gezien worden als het gereedschap dat wordt ingezet binnen een bepaald proces om een specifiek doel te bereiken. Net als bij echt gereedschap bestaat echter het gevaar dat je je blind staart op een mooi product en iets aanschaft zonder goed na te denken over wat dit product precies betekent voor jouw organisatie en processen. Past het product bijvoorbeeld binnen de huidige processen, of moet je deze processen juist aanpassen op het product? Ofwel, is dit nu echt de juiste *tool* voor mij?

Het is belangrijk om altijd breder te kijken dan alleen het specifieke product en je te focussen op het transformeren van een bepaald werkproces met behulp van technologie. Het aanschaffen van een product in de hoop dat daarmee de processen veranderen werkt niet. Mensen houden namelijk niet van verandering. Hieronder ga ik verder in op een aantal belangrijke aspecten en valkuilen bij de overstap naar legal tech. Waar moet je nu rekening mee houden?

Inventariseren
De overstap naar legal tech start bij een goede inventarisatie. Is het doel bijvoorbeeld om een inefficiënt proces te verbeteren en daar de juiste technologie voor te zoeken? Of ben je reeds bekend met een technologie en wil je deze inzetten om adequate processen te verbeteren? Het is natuurlijk makkelijker om een proces te veranderen waar iedereen zich aan ergert, dan om de processen te veranderen waar mensen zich niet echt aan storen. Door knelpunten te beschrijven ontstaan er duidelijke eisen aan de technologie. Hierbij kun je tevens de wensen van medewerkers uitvragen. Op deze manier betrek je relevante personen bij het bereiken van jouw doel. Deze betrokkenheid en transparantie is essentieel bij de overstap naar een nieuwe technologie.

Een valkuil bij deze eerste stap is het beperken van de inventarisatie tot één afdeling, terwijl werkprocessen van verschillende afdelingen vaak samenhangen. Een glanzend nieuwe tool voor de juridische afdeling moet bijvoorbeeld niet betekenen dat de salesafdeling ineens drie extra stappen moet nemen om een contract getekend te krijgen. In dat geval zal de salesafdeling gewoon de oude werkwijze aanhouden.

Plannen
Na de inventarisatie kun je bepalen welke technologie het beste aansluit bij de behoefte van de organisatie. Om de organisatie en met name de directie mee te krijgen in deze verandering, is het aan te raden om een overtuigend plan te maken. In dit plan ga je natuurlijk in op de huidige knelpunten en de oplossingen die de legal tech met zich meebrengt. Hierbij kun je ook het belang van innovatie benadrukken, want stilstaan is achteruitgaan. Voor je het weet moet de organisatie halsoverkop een inhaalslag maken op de concurrentie. Zoals gezegd is iedere onderneming tot verandering in staat, mits de juiste motivering gevonden kan worden.

Een ander belangrijk aspect om te benadrukken in het plan zijn de kosten. Wat zijn de (licentie)kosten van de legal tech en welke besparingen levert het op? Bepaalde technologie verdient zich duidelijk terug vanwege bijvoorbeeld de tijdsbesparing die het oplevert. Soms is dit echter niet het geval, maar is het voordeel dat de *compliance* van de organisatie verbetert en dat hiermee de kans op hoge boetes van toezichthouders wordt gemitigeerd.

In jouw plan kun je ook een planning opnemen. Welke interne en externe middelen heb je op welk moment nodig? Bij het maken van een planning is sneller niet altijd beter. Wellicht voelt het goed als je de gewenste overstap dit jaar nog kan afronden, maar het maakt meestal weinig uit of de overstap nu in december wordt afgerond of in januari. Het forceren van een overstap tijdens de drukste periode van het jaar is bijvoorbeeld geen goed idee. Medewerkers houden dan vast aan de bekende werkwijze omdat zij niet het gevoel hebben dat ze tijd kunnen besteden aan het leren van iets nieuws.

Implementatie, trainen en nazorg
Met implementatie bedoel ik hier het daadwerkelijk in gebruik nemen van de gekozen legal tech. Hoe dit precies verloopt is natuurlijk mede afhankelijk van de gekozen technologie. Ik kan echter wel benoemen dat betrokkenheid een van de belangrijkste aspecten is voor een succesvolle implementatie. Het is daarom aan te raden om medewerkers op de hoogte te houden van de voortgang en enthousiast te maken voor de nieuwe technologie. Betrek de relevante medewerkers ook bij de keuzes die gemaakt moeten worden in het kader van de implementatie. Als de medewerkers de mogelijkheid hebben gehad om mee te beslissen over optie a of b, dan zullen de gevolgen van deze keuze makkelijker worden geaccepteerd.

Bij veel nieuwe technologieën kan niet verwacht worden dat medewerkers dit *out of the box* kunnen gebruiken. Het is daarom belangrijk om medewerkers te trainen in het gebruik van de nieuwe technologie. De training is ook een mooi moment om de medewerkers enthousiast te maken over de nieuwe technologie en om eventueel alvast wat feedback te ontvangen. Wees bereid om meerdere trainingen te organiseren door het jaar heen, zodat de medewerkers regelmatig herinnerd worden aan alle functionaliteiten en *best practices*. Een mooi voorbeeld hiervan is Microsoft Word. Sommige juristen werken als sinds de basisschool met Word, maar zijn niet bekend met 90% van de functionaliteiten en gebruiken het daarom zeer inefficiënt.

Naast betrokkenheid en training is nazorg zeer belangrijk. Als gebruikers in de eerste weken na ingebruikname vastlopen en niet snel genoeg geholpen worden, dan kan de overstap naar legal tech alsnog mislukken. Vragen en klachten van medewerkers moeten in het begin daarom snel opgevolgd worden. Dit wordt ook wel een *hypercare* fase genoemd. Hiermee kan voorkomen worden dan medewerkers weer terugvallen in de oude bekende processen.

Vragen?
De legal tech consultants van ICTRecht kunnen u bij uitstek adviseren over technologie die specifiek aansluit bij uw organisatie en processen. Indien gewenst helpen wij ook bij het implementeren van de gekozen oplossingen, het managen van de nodige veranderingen en het creëren van draagvlak binnen de organisatie. Bovendien kunnen wij jou én jouw collega's trainen in het gebruik van de gekozen legal tech oplossing.

ICTRECHT
adviesbureau

Werk efficiënter door legal tech

Ervaren wat de juiste technologie kan betekenen voor uw juridische processen?

Laat legal tech voor uw organisatie werken.

Bent u klaar met zoeken naar hoe juridische processen beter en efficiënter kunnen? De legal tech consultants van ICTRecht bieden uitkomst en geven deskundig advies op maat. ICTRecht helpt met het implementeren van de gewenste legal tech oplossing, helpt uw medewerkers efficiënt te werken met de technologie en kan uw organisatie ondersteunen op het gebied van verandermanagement.

Meer weten? Bekijk:
ictrecht.nl/legal-tech-advies

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Noot bij Gerechtshof Amsterdam, 16 februari 2021 ECLI:NL:GHAMS:2021:392

Op basis van alle omstandigheden van het geval kwalificeert de overeenkomst van de maaltijdbezorgers met Deliveroo als arbeidsovereenkomst. Met deze droge omschrijving zet het hof Amsterdam een stevige streep door het bedrijfsmodel van maaltijdbezorger Deliveroo en haar concullega's – alle bezorgbedrijven en andere platforms die met "flexibele zzp'ers" goedkoop vraag en aanbod bij elkaar brengen. Geen werknemers, aldus jarenlang het standpunt. Maar langzaam maar zeker wordt dit beeld scherp bijgesteld.

In twee zaken bij dezelfde rechtbank kwam FNV als vakbond op voor de algemene kwestie of voedselfietsbezorgbedrijf Deliveroo haar bezorgers als zzp'er mocht aanmerken. Dit was een collectieve procedure, waar Deliveroo bezwaar tegen maakte met het argument dat ieder arbeidscontract anders is en de beoordeling of iemand werknemer is ook. Maar de rechter bepaalde meteen dat FNV wél mag procederen over zoiets principieels als dit.

Tegen de uitspraak – ja, ze zijn werknemer – kwam Deliveroo met zo ongeveer alle mogelijke argumenten in het verweer. Onder meer dat ieder contract toch anders is, wat de rechter terzijde schuift: je kunt best een algemene uitspraak doen over mensen die bepaald werk verrichten, en dan eventueel in uitzonderingsgevallen daar weer van afwijken.

Kern van de uitspraak is een arrest uit november[1], waarin de Hoge Raad bepaalde dat de bedoelingen van partijen er niet toe doet bij de vraag of een contract een arbeidsovereenkomst is. Je kijkt er objectief naar: werkt iemand 'in dienst', krijgt hij of zij 'loon' om 'gedurende zekere tijd' bepaalde 'arbeid' te verrichten. Zo ja, dan is het een arbeidscontract. En dan doet het er niet toe wat er bovenaan het contract staat of zelfs wat je allebei verklaard te hebben gewild.

Dit is ter bescherming van de werknemer, die anders maar al te vaak plechtig zal verklaren zzp'er wilde te zijn. Wat precies is dat er gebeurde bij Deliveroo, dat in februari 2018 al haar werknemers uitnodigde voor zichzelf te beginnen en tot haar grote vreugde van ontzettend veel zzp'ers een aanbod kreeg om pakketjes te bezorgen. Ja, zo generiek reageert men:

> Deliveroo heeft verder betwist dat het bezorgen van maaltijden voor haar een kernactiviteit betreft. Zij stelt dat zij een IT-bedrijf is, en het bezorgen van maaltijden daarbij slechts van ondergeschikte betekenis is.

Droogjes constateert het gerechtshof dat zij "Deliveroo hierin niet kan volgen." Ik denk dat we dit standpunt voor marktplaatspartijen maar eens naar de giechelafvalbak gaan verwijzen.

Dat de bezorgers een vergoeding krijgen, staat buiten kijf. Maar is dat loon? Dat is natuurlijk lastig te zeggen. Het hof vindt belangrijk dat wat je aan het eind van de maand overhoudt, niet véél meer is dan het minimumloon uit de wet. Daar schemert doorheen dat zzp'ers meestal toch voor meer dan dat willen werken. Wat niet meehelpt is dat Deliveroo de vergoeding eenzijdig kan aanpassen, wat niet logisch is bij zzp'ers, en dat

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

haar standaardcontract de aanname bevat dat de bezorger "hobbymatig" de werkzaamheden verricht in de zin van de belastingwetgeving.

Belangrijker is de vraag of zij 'in dienst' zijn, oftewel of Deliveroo gezag kan uitoefenen over de bezorgers. Dat lijkt het geval: Deliveroo zegt waar je moet zijn en hoe laat je moet leveren om geld te verdienen. Daarbij komt dat wat de bezorgers doen, eigenlijk gewoon de "kernarbeid" van het bedrijf is. Een zzp'er haal je er eerder bij om iets incidenteels te doen. De ICT van een juristenkantoor, bijvoorbeeld, of de website van een bakker. Wie brood komt bakken bij die bakker, zal wel werknemer zijn en geen gedetacheerde zzp'er dus.

Maar ook de techniek kan gezag uitoefenen:

> Het GPS-systeem geeft Deliveroo daarmee een vergaande controlemogelijkheid op de werkwijze van de bezorger. FNV heeft erop gewezen, en zulks komt het hof ook aannemelijk voor, dat deze GPS-bekendheid ook een druk op de bezorger uitoefent. De klant rekent op bezorging van een maaltijd op een bepaald tijdstip; wanneer een bezorger bijvoorbeeld langzamer gaat fietsen, dan zal de klant (en daarmee Deliveroo) hierover teleurgesteld zijn, hetgeen een bezorger menselijkerwijs zal willen proberen te voorkomen. Het GPS-systeem geeft Deliveroo (al dan niet via haar klanten) dus een vergaande controlemogelijkheid, die eveneens als een vorm van gezag is aan te merken.

Deze overweging is bij mijn weten nog niet eerder in de rechtspraak toegepast. Het GPS-systeem is de kern van het bedrijf van Deliveroo: zo brengt zij vraag (bestellingen van maaltijden) bij aanbod (restaurants die deze kunnen bereiden). Doel van Deliveroo is deze grofweg binnen 30 minuten bezorgd te krijgen, en door middel van GPS kan men de bezorgers lokaliseren die in de buurt zijn en die ook nog eens binnen dit tijdsvak van hun startpunt naar het restaurant naar de klant kunnen gaan.

Het algoritme hiervoor heet 'Frank', volgens Deliveroo cruciaal voor haar organisatie. Zij zegt heel veel tijd en kosten te hebben besteed en te blijven besteden aan de ontwikkeling van dit systeem. De criteria op basis waarvan wordt vastgesteld welke bezorger de rit het meest efficiënt kan uitvoeren, zijn door Deliveroo als volgt omschreven:

"Om deze vaststelling (het aanbieden van een bepaalde bestelling aan de bezorger die dat zo effectief mogelijk kan voltooien, hof) te kunnen maken, verwerkt Frank gegevens over de locatie van de bezorger ten opzichte van het restaurant, het voertuigtype, een schatting van wanneer de bestelling gereed is voor bezorging en de geschatte bezorgtijd. Het algoritme maakt daarin geen onderscheid in de persoon of de wijze waarop een bezorger zijn diensten aanbiedt en kan dat ook niet. Deze data zijn voor Frank niet beschikbaar noch van belang."

Dit klinkt mooi, maar zegt niet zo veel. Dat betekent dat Deliveroo, die het algoritme 'Frank' heeft ontworpen en voortdurend aanpast, een grote bemoeienis heeft met de wijze waarop werkzaamheden worden verricht. De bezorger heeft zich er maar naar te schikken. Of Deliveroo via 'Frank' de bestelling aanbiedt aan de bezorger uitsluitend op basis van afstand ('de bezorger met fiets die zich het dichtst bij het restaurant bevindt krijgt de bestelling aangeboden') of dat ook andere criteria worden gehanteerd (zoals de snelheid waarmee een bepaalde bezorger doorgaans zijn bestellingen afhandelt, of zijn beoordeling door klanten) is niet duidelijk geworden.

In een dergelijke situatie is het gebruik van dit systeem eenvoudigweg een controlemogelijkheid te noemen. Deliveroo kan hiermee sturen hoe haar bezorgers zich moeten gedragen. En juist omdat dit impliciet is – het zijn geen harde instructies – is het extra venijnig: wie niet precies weet waar hij op aangesproken wordt, gaat op alle punten juist harder werken en voelt zich meer gedwongen.

Daar komt bij dat de bezorgers zich naar buiten toe moeten profileren als "iemand van Deliveroo", zodat restaurants weten wie hun maaltijden bezorgt en passanten eventuele overlast kunnen melden bij Deliveroo. Alles bij elkaar (en dat is de juridische standaard) zijn de Deliveroo-bezorgers dus gewoon werknemers. De criteria zijn redelijk op het bedrijf gericht maar ik denk dat je dit vrij eenvoudig ook kunt toepassen op andere fietsbezorgdiensten en andere door platforms gecoördineerde individuen.

Van onze blog

Cloud Overheid

18 februari 2021

Hoge Raad: politie mag dwang gebruiken om telefoon met vingerafdruk te ontgrendelen

Steeds meer telefoons maken gebruik van biometrische beveiliging, zoals vingerafdrukken of gezichtsscans. Dat is een stuk veiliger dan een standaard toegangscode à la '0000' of '1234'. Volgens Apple[1] is de kans slechts één op 50.000 dat Touch ID het laat afweten. Het nieuwere Face ID is nog een stuk veiliger zegt Apple[2], met een inbraakkans van ongeveer één op 1.000.000. Maar hoe moet met dergelijke toegangsbeveiliging worden omgegaan in een strafproces? Is een verdachte verplicht om zijn of haar vingerafdruk af te staan, of om bijvoorbeeld een scan te laten maken van zijn of haar gezicht als de politie daar om vraagt? Dankzij een arrest van de Hoge Raad[3] van vorige week hebben we hier inmiddels meer duidelijkheid over. Het lijkt erop dat opsporingsautoriteiten een verdachte inderdaad kunnen vragen om een telefoon te ontgrendelen met zijn of haar vingerafdruk. Wil een verdachte niet meewerken, dan mag er (lichte) dwang worden uitgeoefend om toch toegang te krijgen tot het apparaat.

1. https://apple.co/3racDtF
2. https://apple.co/3811Ydq
3. https://bit.ly/3sH4fCg

Achtergrond

Aanleiding voor het arrest was een politieonderzoek naar *phising* uit 2015. Op basis van het onderzoek werd in 2016 een verdachte aangehouden; ook zijn iPhone werd door de politie in beslag genomen. De telefoon bleek beveiligd met een vingerafdruk. De politie heeft de verdachte eerst gevraagd om zelf zijn telefoon te ontgrendelen. Toen de verdachte dat weigerde, is hij geboeid en heeft de politie (onder dwang) zijn duim op de vingerafdrukscanner gelegd. Op de telefoon werd belastend bewijsmateriaal gevonden, maar volgens zijn advocaat had hij nooit gedwongen mogen worden om zijn telefoon te ontgrendelen. De Rechtbank Noord-Holland was het niet met de advocaat eens. Uiteindelijk besloot de procureur-generaal van de Hoge Raad cassatie in belang der wet in te stellen om definitief uitsluitsel te krijgen.

Nemo tenetur-beginsel

Volgens artikel 6 van het Europees Verdrag voor de Rechten van de Mens (EVRM) heeft iedere verdachte recht op een eerlijk proces. Dit brengt onder meer met zich mee dat rechtszaken binnen een redelijke termijn behandeld moeten worden en dat een rechtszaak beslist moet worden door een onpartijdige en onafhankelijke rechter. Uit artikel 6 EVRM vloeit óók het zogeheten 'nemo tenetur-beginsel' voort. Dit beginsel houdt (kort gezegd) in dat een verdachte niet verplicht is om bewijs tegen zichzelf te leveren. Het is aan de opsporingsautoriteiten om dit bewijs te verzamelen. De verdachte bepaalt zelf hoe hij of zij zich verdedigt in de procedure en of hij of zij wel of niet medewerking wil verlenen.

Uitgaande van het nemo tenetur-beginsel, kan een verdachte niet worden gehouden om belastende informatie vrij te geven, of om bijvoorbeeld de wachtwoorden van zijn of haar telefoon of computer aan de opsporingsautoriteiten te overhandigen. De politie heeft overigens wel bevoegdheden om zelf te proberen zo'n computer of telefoon te kraken, al is dat in de praktijk niet altijd eenvoudig. Ook in de onderhavige zaak heeft de politie dit overwogen, maar volgens de Officier van Justitie was er (in ieder geval in 2016) nog geen techniek om de iPhone van de verdachte te kraken.

Dat de politie de telefoon niet kon kraken, was volgens de advocaat van de verdachte géén reden om hem te dwingen *zelf* de telefoon te ontgrendelen. Volgens de advocaat werd daarmee onder meer het recht op een eerlijk proces (artikel 6 EVRM) aangetast. De rechtbank was het daar eerder echter mee oneens[4]. De Hoge Raad bevestigt nu dat de politie inderdaad een vingerafdruk van de verdachte mocht afnemen om de telefoon te ontgrendelen, ook als de verdachte zelf niet bereid was om deze af te staan.

Afhankelijk versus onafhankelijk van de wil
De belangrijkste overweging van de rechtbank (en nu ook van de Hoge Raad) is dat het nemo tenetur-beginsel niet onbegrensd is. Het Europese Hof voor de Rechten van de Mens (EHRM) heeft in het verleden al verschillende arresten gewezen over het toepassingsbereik daarvan. Uit die arresten volgt dat het nemo tenetur-beginsel vooral bescherming biedt tegen het actief afleggen van verklaringen. Je hoeft dus als verdachte niet *uit eigen wil* informatie te verstrekken die gedurende het strafproces tegen jou gebruikt kan worden (zie onder meer deze zaak[5] voor de liefhebbers).

Waar het nemo tenetur-beginsel géén bescherming tegen biedt, is het passief ondergaan van bepaalde onderzoeksmaatregelen. Als er onderzoeksmateriaal is dat *onafhankelijk van de wil* van de verdachte bestaat, dan mogen opsporingsautoriteiten dat desnoods onder (gepaste) dwang van de verdachte verkrijgen. Opsporingsautoriteiten kunnen een verdachte dus bijvoorbeeld dwingen om bloed- en urinemonsters af te geven (zie ook dit arrest[6] van het EHRM).

Volgens de Hoge Raad moet het afnemen van een vingerafdruk min of meer gelijkgesteld worden aan het afnemen van bijvoorbeeld een bloedmonster. Die unieke print op de vinger van de verdachte bestaat namelijk *onafhankelijk van zijn of haar wil*. En daar biedt het nemo tenetur-beginsel dus géén bescherming tegen. Daarmee is er volgens de Hoge Raad grondrechtelijk geen bezwaar om die vinger afdruk onder (lichte) dwang van de verdachte af te nemen.

In het licht van de eerdere rechtspraak van het EHRM is de beoordeling van de Hoge Raad goed te begrijpen, al is de uitwerking daarvan in de praktijk wel enigszins merkwaardig. Een vingerafdruk of gezichtsscan dient natuurlijk hetzelfde doel als een 'traditioneel' wachtwoord of een cijfercode, namelijk voorkomen dat derden toegang kunnen krijgen tot bepaalde informatie. Toch wordt het wachtwoord 'beschermd' door artikel 6 EVRM en een vingerafdruk of gezichtsscan niet. Je kunt je afvragen hoe logisch dat is.

Niet in alle gevallen
Opmerking verdient dat de opsporingsautoriteiten een verdachte niet zómaar kunnen dwingen om zijn of haar vingerafdruk af te staan. De bevoegdheid waar de politie zich in dit geval op baseerde was artikel 61a van het Wetboek van Strafvordering. Die bevoegdheid geldt alleen bij (verdenking van) misdrijven waarbij voorlopige hechtenis open staat, en dat zijn serieuze vergrijpen. Je moet dan bijvoorbeeld denken aan misdrijven waar een (maximum) gevangenisstraf van vier jaar voor staat, computervredebreuk, et cetera.

4. https://bit.ly/3qbbiS2
5. https://bit.ly/3sGyDgd
6. https://bit.ly/3uLA5jm

Auteur
Bram de Vos
Juridisch adviseur

23 februari 2021

Autoriteit Persoonsgegevens legt (weer) boete op voor onvoldoende beveiliging

Begin deze maand heeft de Autoriteit Persoonsgegevens (AP) een boete van € 440.000 opgelegd aan het Amsterdamse ziekenhuis OLVG, voor het onvoldoende beveiligen van medische dossiers. De kans bestaat dat u een déjà vu-moment ervoer bij het lezen van dat nieuwsbericht: dat was toch al een keer gebeurd? Dat klopt: in 2019 heeft de toezichthouder de eerste echte boete[1] onder de AVG opgelegd aan een ander ziekenhuis, voor – in grote lijnen – dezelfde overtreding. Wat ging er precies fout bij het OLVG?

Onbevoegde toegang

Zoals gezegd kreeg in 2019 een Haags ziekenhuis een boete voor onbevoegde inzage door zo'n 100 medewerkers in het medisch dossier van een bekende Nederlander. Dat werd allemaal gelogd, maar die logbestanden werden alleen niet voldoende gemonitord en gecontroleerd. Daarnaast was er geen tweefactorauthenticatie geïmplementeerd voor relevante systemen. Dit leidde uiteindelijk tot een boete van € 460.000.

Begin deze maand bleek het ook bij het Amsterdamse ziekenhuis niet goed te gaan. Iedere handeling in het ziekeninformatiesysteem werd wel gelogd. De controle daarop kon alleen niet gezien worden als een 'passende beveiliging'.

Ondanks dat het geschreven beleid een maandelijkse controle bevatte, werden in werkelijkheid slechts twee proactieve en acht incidentele controles uitgevoerd in bijna anderhalf jaar tijd. Dat was niet voldoende om onbevoegde toegang tot medische dossiers te signaleren en eventuele maatregelen te nemen, ook gezien het feit dat het ziekenhuis medische dossiers houdt van zo'n 500.000 patiënten. De AP herhaalt het uitgangspunt dat logging 'systematisch en consequent' moet plaatsvinden. Steekproefsgewijze controle en/of op basis van klachten is niet voldoende.

Tweefactorauthenticatie

Het Haagse ziekenhuis maakte in 2019 geen gebruik van tweefactorauthenticatie. Ook dit ging bij het OLVG niet goed: het ziekenhuisinformatiesysteem was op computers binnen het netwerk toegankelijk via gebruikersnaam en wachtwoord. Medewerkers die op de digitale werkplek zijn ingelogd, krijgen via single sign-on (SSO) ook meteen toegang tot patiëntdossiers. Toegang buiten het netwerk is wel alleen mogelijk met tweefactorauthenticatie. Ook dit was echter niet genoeg: o.a. het NEN7510-normenkader, waaraan het OLVG zich committeert, schrijft voor dat toegang tot medische gegevens dient te gebeuren op basis van tweefactorauthenticatie. De AP stelde hier aldus een overtreding op vast.

Hoe nu verder?

Het OLVG gaat in ieder geval niet in beroep. De visie van de AP is duidelijk met deze tweede uitspraak over passende beveiliging in de zorg: er wordt veel waarde gehecht aan tweefactorauthenticatie, logging en de controle daarvan. Vragen over hoe u dit het beste in kunt richten binnen uw organisatie? Neem dan contact op met ons, wij helpen u graag verder.

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

Auteur
Laura Monhemius
Juridisch adviseur

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

iapp CPE credits approved

Trainingsoverzicht april - juni 2021

Dinsdag 20 april 2021
Privacy en persoonsgegevens: de basis voor niet-juristen
Heeft u in uw werk (als niet-jurist) te maken met persoonsgegevens en wilt u meer over de AVG weten? Of heeft u in uw werk (nog) niet te maken met persoonsgegevens, maar heeft u hier wel interesse in? Volg dan deze praktijkgerichte training waarin de AVG uitgebreid aan bod komt en u praktische handvatten krijgt aangereikt. Voorkennis over privacy is niet nodig.

http://bit.ly/3jUjZP5

Donderdag 22 april 2021
Beschikbaarheid en continuïteit in de cloud (2 PO)
Outsourcing naar de cloud brengt enorme afhankelijkheid mee. Gebruikers van clouddiensten moeten daarom altijd afspraken maken over beschikbaarheid. Verlies van data of dienst kan immers leiden tot bedrijfsdiscontinuïteit. Daarbij wordt onderscheid gemaakt tussen tijdelijke onbeschikbaarheid en definitieve onbeschikbaarheid. De eerste situatie kan met een goede SLA worden opgevangen, de tweede vereist exit- of continuïteitsafspraken.

http://bit.ly/3u6xlXK

Dinsdag 11 mei 2021
Ondernemen: SaaS-diensten (4 PO)
Alles gaat naar de cloud, en digitale dienstverlening is daarmee alomtegenwoordig. Een ICT-jurist dient bekend te zijn met impact van Software as a Service en te weten hoe om te gaan met de juridische randvoorwaarden van dit type dienstverlening.

http://bit.ly/3djd0y3

Donderdag 17 juni 2021
Open source software (4 PO)
Open source is de verzamelnaam voor alle soorten software die gratis wordt aangeboden onder voorwaarden die vrij gebruik toestaan. Dit model blijkt in de praktijk zeer succesvol; er is vrijwel geen softwarepakket of -dienst op de markt dat geen gebruik maakt van open source. Tegelijk roepen die unieke randvoorwaarden unieke risico's op, met name vanuit dag-tot-dag compliance oogpunt.

http://bit.ly/3djddRR

Deze trainingen vindt u misschien ook interessant:

Maandag 19 april 2021
FG Newsflash | Live webinar

Dinsdag 20 april 2021
Cloud en software: basisbeginselen ICT en recht (2 PO)

Dinsdag 20 april 2021
Cloud en software: platforms en tussenpersonen (2 PO)

Donderdag 22 april 2021
Innovatie, ICT en recht (2 PO)

Maandag 3 mei 2021
AVG rechtspraak update | Live webinar (1 PO)

Dinsdag 18 mei 2021
Privacy en persoonsgegevens: verwerkersovereenkomst (4 PO)

Dinsdag 1 juni 2021
Technologie: werking internet (2 PO)

Dinsdag 1 juni 2021
Ondernemen: fiscale aspecten (2 PO)

Donderdag 3 juni 2021
Agile software ontwikkelen (4 PO)

Dinsdag 15 juni 2021
Privacy: AVG op hoofdlijnen (6 PO)

Bekijk ons volledige trainingsoverzicht op:
ictrecht.nl/trainingen

Praktische kennis opdoen over AVG? Wellicht zijn de themadagen binnen onze opleiding tot FG/DPO dan iets voor u!

Op een themadag wordt één specifiek thema behandeld. De trainingen zijn los afneembaar en ook een op maat gemaakt pakket van losse trainingen is mogelijk. Bestemd voor beginnende FG's/DPO's en iedere andere (juridische/niet-juridische) privacy professional.

15 april 2021
Themadag verantwoordelijke en verwerker deel I*

22 april 2021
Themadag verantwoordelijke en verwerker deel II*

29 april 2021
Themadag security

12 mei 2021
Themadag inventariseren en registreren

20 mei 2021
Themadag rechten van betrokkenen

27 mei 2021
Themadag datalekken

3 juni 2021
Themadag online marketing en cookies

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

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

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

Heeft u vragen of wilt u meer weten?

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

Britt Telleman
Opleidingscoördinator


ICTRECHT
adviesbureau