# Algemene Verordening Bescherming Persoonsgegevens: uitkomst trialoog

## *Computerrecht* 2016/63

De Algemene Verordening Bescherming Persoonsgegevens (General Data Protection Regulation, of GDPR) komt er dan toch echt. Begin 2012 presenteerde de Europese Commissie een voorstel voor een Algemene Verordening Bescherming Persoonsgegevens die de Richtlijn Bescherming Persoonsgegevens uit 1995 moet vervangen. Over dit voorstel is bijna vier jaar gediscussieerd. In 2014 heeft het Europees Parlement een aangepaste versie van de Verordening aangenomen, op basis van de bijna 4000 amendementen die waren ingediend. In juni 2015 heeft de Raad van de Europese Unie haar voorstel gepubliceerd om op grond daarvan de trialoog-onderhandelingen te beginnen.

Op 15 december 2015 zijn de Commissie, de Raad, en het Europees Parlement het eens geworden over de tekst van de Verordening. Op het moment van schrijven moeten het Europees Parlement en de Raad deze definitieve tekst nog formeel aannemen. Nadat de Verordening formeel is aangenomen, duurt het twee jaar voor hij in werking treedt. De Verordening zal naar verwachting dus in de lente of de zomer van 2018 in werking treden.

De geconsolideerde tekst van de Verordening is hier te raadplegen: http://data.consilium.europa.eu/doc/document/ST-15039-2015-INIT/en/pdf

Later dit jaar verschijnt in dit tijdschrift een special over de nieuwe Verordening.

---

# Consultatie e-Privacyrichtlijn

## *Computerrecht* 2016/64

Nu de tekst van de Algemene Verordening Bescherming Persoonsgegevens is aangenomen, begint de Europe Commissie aan een ander groot privacy-project: de amendering van de e-Privacyrichtlijn (2002/58, voor het laatst geamendeerd in 2009). De e-Privacyrichtlijn bevat onder meer regels omtrent het communicatiegeheim, cookies, spam, en verkeers- en locatiegegevens.

Rosa Barcelo van DG CONNECT zei tijdens de Computers, Privacy & Data Protection conferentie in Brussel (eind januari), dat dit voorjaar een consultatieronde zal worden georganiseerd over de opvolger van de e-Privacyrichtlijn. Tijdens de conferentie zei Anna Buchta van de European Data Protection Supervisor dat de Supervisor liever zou zien dat de opvolger van de e-Privacyrichtlijn een Verordening wordt.

Een lastig punt zal de reikwijdte van de nieuwe regels zijn. Nu gelden de specifieke regels voor het verwerken van locatiegegevens bijvoorbeeld alleen voor aanbieders van elektronische communicatiediensten (zoals internet access providers en telefonie-aanbieders). Veel bedrijven die ook, en vaak meer, locatiegegevens verwerken, vallen nu nog buiten de reikwijdte van de e-Privacyrichtlijn.

---

# Privacy Shield moet Safe Harbor vervangen

## *Computerrecht* 2016/65

Zoals bekend heeft het Hof van Justitie van de Europese Unie op 6 oktober 2015 de 'Safe Harbor' beschikking ongeldig verklaard (Computerrecht 2016/6). De Artikel 29 Werkgroep suggereerde in oktober dat nationale privacytoezichthouders tot februari 2016 niet zouden overgaan tot handhavingsacties in verband met gegevensstromen naar de Verenigde Staten. Sinds oktober 2015 hebben de Europese Commissie en de Verenigde Staten onderhandeld om tot een oplossing te komen.

Op 2 februari 2016 maakte de Europese Commissie bekend dat zij en de Verenigde Staten het eens zijn geworden over een nieuw politiek akkoord voor trans-Atlantische gegevensstromen: het 'Privacy Shield'. Volgens de Commissie bevat de regeling de volgende elementen: (i) Nieuwe en zwaardere verplichtingen voor bedrijven die persoonsgegevens van Europeanen verwerken. (ii) Duidelijke waarborgen omtrent toegang tot persoonsgegevens door Amerikaanse veiligheidsdiensten. De Commissie zegt dat 'de VS heeft uitgesloten dat persoonsgegevens die in het kader van de nieuwe regeling naar de VS worden doorgegeven, willekeurig en op grote schaal worden gecontroleerd.' (iii) De rechten van Europeanen worden beter beschermd als hun persoonsgegevens worden opgeslagen in de Verenigde Staten.

Op het moment van schrijven is de tekst van de 'Privacy Shield'-regeling nog niet gepubliceerd. Max Schrems, en vele anderen in Europa, reageerden sceptisch op de berichten over het 'Privacy Shield'. De Artikel 29 Werkgroep heeft de Commissie opgeroepen de tekst met betrekking tot het Privacy Shield voor eind februari te verstrekken.

# Nieuws van de EDPS

*Computerrecht* 2016/66

De EDPS, de European Data Protection Supervisor, heeft een 'Ethics Advisory Group' ingesteld. In januari zijn de zes leden van de groep bekend gemaakt: J. Peter Burgess, filosoof en professor aan de Vrije Universiteit Brussels; Luciano Floridi, Professor of Philosophy and Ethics of Information, aan Oxford University; Jaron Lanier, auteur van onder meer 'Who Owns the Future' en 'You Are Not a Gadget'; Antoinette Rouvroy, onderzoeker bij de Universiteit van Namen; Aurélie Pols, verbonden aan de IE business school in Spanje; Jeroen Van den Hoven, Professor of Ethics and Technology, Technische Universiteit Delft. De bedoeling is dat de groep in januari 2017 een rapport publiceert, over de relatie tussen mensenrechten, technologie, en business modellen in de 21e eeuw, vanuit een ethisch perspectief.

# Nieuws van de Artikel 29 Werkgroep

*Computerrecht* 2016/67

De Artikel 29 Werkgroep heeft eind 2015 twee nieuwe opinies gepubliceerd. Ten eerste heeft de Artikel 29 Werkgroep een update van haar opinie uit 2010 over toepasselijk recht (WP179) gepubliceerd, naar aanleiding van het Google Spain arrest van het Hof van Justitie van de Europese Unie (Computerrecht 2014/115). Ten tweede heeft de Werkgroep in december richtsnoeren voor de lidstaten gepubliceerd, over de criteria om de naleving van het gegevensbeschermingsrecht te waarborgen in het kader van automatische uitwisseling van persoonsgegevens voor belastingdoeleinden (WP 234).

# Nieuws van de Autoriteit Persoonsgegevens (CBP)

*Computerrecht* 2016/68

Sinds 1 januari heeft het College Bescherming Persoonsgegevens (CBP) een nieuwe naam: de Autoriteit Persoonsgegevens. Ook is sinds 2016 de nieuwe meldplicht datalekken van kracht, en heeft de Autoriteit de bevoegdheid gekregen om boetes op te leggen.

Verder heeft de Autoriteit Persoonsgegevens beleidsregels gepubliceerd over cameratoezicht. De beleidsregels bevatten uitwerkingen van de relevante bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens. Ook publiceerde de Autoriteit Persoonsgegevens haar toezichtsagenda voor 2016. De Autoriteit zal zich voornamelijk richten op vijf onderwerpen: beveiliging van persoonsgegevens, big data en profiling, medische gegevens, persoonsgegevens bij de (digitale) overheid, en persoonsgegevens in de arbeidsrelatie.

De nieuwe website van de Autoriteit Persoonsgegevens is te vinden op: www.autoriteitpersoonsgegevens.nl.

## Europa

# Concepttekst 'Privacy Shield' openbaar

*Computerrecht* 2016/107

Op 29 februari heeft de Europese Commissie de concepttekst van het Privacy Shield-besluit, die het Safe Harbor-besluit zou moeten opvolgen, openbaar gemaakt. Sinds het Schremsarrest van het Hof van Justitie van de Europese Unie uit oktober 2016 (*Computerrecht* 2016/6) is het Safe Harbor-besluit ongeldig. Op grond van het Safe Harbor-besluit konden persoonsgegevens van Europeanen naar de VS doorgegeven worden onder bepaalde voorwaarden, maar na de Snowden-onthullingen was er veel kritiek op deze constructie.
De Commissie zegt het volgende over het Privacy Shield: De Commissie zegt het volgende over het Privacy Shield: "Het gaat onder meer om (...) schriftelijke verbintenissen van de regering van de VS over de handhaving van de regeling (...). Ook bieden deze verbintenissen zekerheid over de waarborgen en beperkingen met betrekking tot de gegevenstoegang van [Amerikaanse] overheidsdiensten."
Max Schrems, de aanjager achter de ongeldigverklaring van de oude Safe Harbor-regeling, zegt op de website van *Europe v Facebook* niet erg onder de indruk te zijn van het nieuwe Privacy Shield-besluit. Volgens hem bevat de nieuwe regeling slechts kleine verbeteringen, maar voldoet deze nog steeds niet aan de Europese wetgeving.

*Jan-Willem van der Ree & Frederik Zuiderveen Borgesius*

# Promotie Hielke Hijmans op zijn proefschrift 'The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU'

*Computerrecht* 2016/108

Op 5 februari 2016 is Hielke Hijmans gepromoveerd op het proefschrift 'The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU'. Het proefschrift gaat over privacy en gegevensbescherming als fundamentele waarden in de democratische rechtsstaat. De EU verdragen hebben de Europese Unie een breed geformuleerde opdracht gegeven om deze grondrechten effectief te beschermen, door middel van rechterlijk toezicht, wetgeving en toezicht door onafhankelijke autoriteiten. Hijmans analyseert in zijn proefschrift de bijdragen van deze actoren binnen het Europees rechtsbestel, en laat zien dat artikel 16 van het EU Werkingsverdrag de EU het vermogen geeft om op te treden als constitutionele waakhond van privacy en gegevensbescherming.

*Jan-Willem van der Ree & Frederik Zuiderveen Borgesius*

## Nederland

# Werkgevers mogen gezondheidsgegevens wearables niet verwerken als 'vrije' toestemming ontbreekt

*Computerrecht* 2016/109

Na onderzoek van de Autoriteit Persoonsgegevens hebben twee bedrijven de verwerking van persoonsgegevens van hun werknemers via wearables stopgezet. Door middel van wearables konden de bedrijven inzicht krijgen in de hoeveelheid beweging van hun werknemers. Eén bedrijf had ook inzicht in het slaappatroon van de werknemers.
Volgens de Autoriteit verwerkten de twee bedrijven de gegevens in strijd met de Wet bescherming persoonsgegevens. Persoonsgegevens over de hoeveelheid beweging en gegevens over slaappatronen zijn namelijk bijzondere (gevoelige) gegevens die iets zeggen over de gezondheid van de werknemers. Voor verwerking van dit soort bijzondere persoonsgegevens is vrije toestemming van de werknemer vereist en die ontbrak volgens de Autoriteit Persoonsgegevens. In een arbeidsverhouding is de werknemer namelijk financieel afhankelijk van de werkgever waardoor er over het algemeen geen sprake kan zijn van 'vrije' toestemming.

*Jan-Willem van der Ree & Frederik Zuiderveen Borgesius*

# Publicatie beleidsregels cameratoezicht door Autoriteit Persoonsgegevens

*Computerrecht* 2016/110

De Autoriteit Persoonsgegevens heeft in januari 2016 de beleidsregels cameratoezicht gepubliceerd. Doel van de beleidsregels is organisaties te helpen bij de privacyafweging die zij moeten maken als zij camera's willen inzetten. De beleidsregels zijn een uitwerking van de belangrijkste be-

palingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens die gelden voor de verwerking van persoonsgegevens door middel van een camera.
Uit de beleidsregels vloeit voort dat de inzet van een camera noodzakelijk moet zijn om de gestelde doelen te bereiken. Daarnaast moeten mensen worden geïnformeerd dat er cameratoezicht is vóórdat zij worden gefilmd en moeten de beelden adequaat worden beveiligd. Ook zijn er in de beleidsregels specifieke aandachtspunten opgenomen voor drones, slimme camera's en dashcams. Een drone kan bijvoorbeeld mensen volgen, waardoor een grotere inbreuk wordt gemaakt op de persoonlijke levenssfeer dan bij een statische camera. Voor dashcams geldt dat in beginsel de Wet bescherming persoonsgegevens van toepassing is als personen of kentekens herkenbaar worden gefilmd.
Tot slot stelt de Autoriteit Persoonsgegevens grenzen voor het gebruik van camera's bij sauna's en uitvaarten. Alleen wanneer de klant toestemming geeft, mag een ondernemer tijdens de uitvaartplechtigheid opnames maken. In saunacomplexen mag daarentegen helemaal geen cameratoezicht plaatsvinden in ruimtes waar bezoekers ontkleed kunnen zijn.

*Jan-Willem van der Ree & Frederik Zuiderveen Borgesius*

## Verouderd beveiligingsprotocol SSLv2 levert mogelijk schending Wet bescherming persoonsgegevens op

### *Computerrecht* 2016/111

Begin maart ontdekten beveiligingsonderzoekers een kwetsbaarheid die het mogelijk maakt om via het SSLv2 protocol binnen enkele uren verbindingen te ontsleutelen. Het SSLv2 protocol is een verouderd protocol dat als doel heeft beveiligde verbindingen met onder meer websites tot stand te brengen. RTL Nieuws maakte in navolging van dit nieuws bekend dat minstens 49 van 175 door RTL Nieuws onderzochte gemeentewebsites dit protocol nog gebruiken. Artikel 13 van de Wet bescherming persoonsgegevens vereist echter dat organisaties die persoonsgegevens verwerken adequate beveiligingsmaatregelen treffen. Nu de kwetsbaarheid van het SSLv2 protocol bekend is, kan niet meer volstaan worden met het SSLv2 protocol. De Autoriteit Persoonsgegevens raadt organisaties daarom aan de ICT-beveiligingsrichtlijnen voor Transport Layer Security van het NCSC in acht te nemen en indien gebruik wordt gemaakt van de programmeerbibliotheek OpenSSL, deze bij te werken naar de laatste versie.
Zie uitgebreid over het beveiligen van gegevens en communicatie: het proefschrift van A. Arnbak, 'Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives', 2015, http://dare.uva.nl/document/2/166342.

*Jan-Willem van der Ree & Frederik Zuiderveen Borgesius*

## Stichting verwerkt medische gegevens van werknemers in strijd met de Wet bescherming persoonsgegevens

### *Computerrecht* 2016/112

Uit onderzoek van de Autoriteit Persoonsgegevens blijkt dat Stichting Abrona bij ziekmelding van haar werknemers in strijd handelt met de Wet bescherming persoonsgegevens (z2014-00914). Abrona, een organisatie gespecialiseerd in dienstverlening aan mensen met een verstandelijke beperking in de provincie Utrecht (1300 werknemers en 800 vrijwilligers), registreerde bij ziekmelding de aard en oorzaak van de ziekte. Dit is in strijd met de wet, aangezien werkgevers bij ziekmelding aan zieke werknemers alleen gegevens mogen vragen die noodzakelijk zijn voor de vaststelling van de verplichting om loon door te betalen en hoe het verder moet met hun werkzaamheden. Medische gegevens zijn bijzondere (gevoelige) persoonsgegevens. Hiervoor gelden strenge wettelijke eisen. Het vaststellen of een werknemer arbeidsongeschikt is en de advisering daarover aan de werkgever zijn taken van de bedrijfsarts.
Abrona heeft na sluiting van het onderzoek medegedeeld dat ze maatregelen hebben getroffen. De Autoriteit Persoonsgegevens gaat nu onderzoeken in hoeverre deze maatregelen voldoende zijn.

*Jan-Willem van der Ree & Frederik Zuiderveen Borgesius*

## Filmen van chauffeurs door transportbedrijf in strijd met de Wet bescherming persoonsgegevens

### *Computerrecht* 2016/113

Na onderzoek van de Autoriteit Persoonsgegevens is gebleken dat het transportbedrijf De Rooy Transport BV zijn chauffeurs filmde tijdens hun ritten (z2015-00409). Het doel hiervan was om de chauffeurs aan te spreken op hun rijgedrag en zo het rijgedrag te verbeteren. De Autoriteit

Persoonsgegevens oordeelde echter dat het voor dit doel niet proportioneel is om de chauffeurs tijdens hun werktijd onafgebroken te filmen. Dit maakt een te grote inbreuk op de persoonlijke levenssfeer van de chauffeur, waardoor het transportbedrijf in strijd met de wet handelde.
Volgens de Autoriteit Persoonsgegevens moet altijd worden gekeken of hetzelfde doel ook met minder ingrijpende middelen kan worden bereikt. Dat bleek hier mogelijk. Zo wijst de Autoriteit Persoonsgegevens erop dat naast het trainen van de chauffeurs ook organisatorische en technische mogelijkheden denkbaar zijn om het rijgedrag van de chauffeurs te verbeteren, zonder de chauffeurs bloot te stellen aan continu cameratoezicht.
Het transportbedrijf heeft inmiddels aangegeven te zullen stoppen met filmen en dat het eerder opgenomen beeld- en geluidmateriaal is gewist. Hiermee is de geconstateerde overtreding beëindigd.

*Jan-Willem van der Ree & Frederik Zuiderveen Borgesius*

## Bij verwerking bijzondere persoonsgegevens moet contactformulier beveiligd zijn

*Computerrecht* 2016/114

In een brief aan de overkoepelende vereniging van fysiotherapeuten heeft de Autoriteit Persoonsgegevens uitgelegd hoe fysiotherapeuten het contactformulier op hun website moeten beveiligen. De Autoriteit Persoonsgegevens geeft hierbij aan dat de belangrijkste vraag is of de fysiotherapeuten via het contactformulier bijzondere persoonsgegevens verwerken, zoals gezondheidsgegevens en het burgerservicenummer van patiënten. Als dit het geval is, dan moet de fysiotherapeut de gehele webapplicatie via een beveiligde https-verbinding aanbieden. Wanneer geen bijzondere persoonsgegevens worden verwerkt, is het aan de fysiotherapeut om zelf op basis van een risicoanalyse en classificatieschema vast te stellen of het nodig is de webapplicatie via https aan te bieden.

*Jan-Willem van der Ree & Frederik Zuiderveen Borgesius*

## Europa

# Advocaat-generaal Hof van Justitie EU: dynamische IP-adressen zijn persoonsgegevens

*Computerrecht* 2016/150

Er is al lang discussie over de vraag onder welke omstandigheden IP-adressen moeten worden beschouwd als persoonsgegevens waarop de Richtlijn bescherming persoonsgegevens van toepassing is. In het arrest *Scarlet/Sabam* (C-70/10, ECLI:EU:C:2011:771) uit 2011 zei het HvJ EU over IP-adressen in de handen van een internet access provider dat die IP-adressen persoonsgegevens zijn. Een internet access provider kan doorgaans de naam van zijn klant koppelen aan het IP-adres dat de provider aan de klant heeft toegewezen. Voor partijen die geen internet access providers zijn, is het echter moeilijker om een IP-adres aan een naam te koppelen.

De zaak Breyer (C-582/14, ECLI:EU:C:2016:339) draait voornamelijk om de vraag of, kort gezegd, een dynamisch IP-adres een persoonsgegeven is in de handen van een websitehouder, als een derde partij (een internet access provider) een naam aan dat IP-adres kan koppelen.

Advocaat-generaal Campos Sánchez-Bordona beantwoordt die vraag bevestigend. Hij zegt "dat een IP-adres dat een aanbieder van diensten in verband met de toegang tot zijn internetsite opslaat, voor deze aanbieder een persoonsgegeven vormt, voor zover een internetprovider beschikt over de aanvullende gegevens die nodig zijn om de betrokken persoon te identificeren."

Aanbieders van internetdiensten kunnen wel een 'legitiem belang' (artikel 7(f) richtlijn) hebben om zulke persoonsgegevens ongevraagd te bewaren, bijvoorbeeld om DOS-aanvallen af te weren. Het is aan de nationale rechter om de oordelen welk belang in een specifieke zaak prevaleert.

*Jan-Willem van der Ree & Frederik Zuiderveen Borgesius*

## Nederland

# Afdeling bestuursrechtspraak Raad van State: vingerafdrukken verplicht bij aanvraag paspoort

*Computerrecht* 2016/151

Afgelopen mei heeft de Afdeling bestuursrechtspraak van de Raad van State in vier zaken geoordeeld dat wie een paspoort aanvraagt verplicht wordt daarbij twee vingerafdrukken af te staan. Voor een identiteitskaart geldt die verplichting niet, zo oordeelde de Afdeling in drie andere zaken.

De verplichting dat een paspoort slechts mag worden afgegeven als van de aanvrager een gezichtsopname en twee vingerafdrukken op de chip van de paspoort wordt opgenomen vloeit voort uit een Europese verordening. De Afdeling overwoog dat burgemeesters die de paspoorten afgeven niet van deze regel mogen afwijken nu een Europese verordening "verbindend is in al haar onderdelen en rechtstreeks toepasselijk is in elke lidstaat". Er mogen echter niet meer dan twee vingerafdrukken worden opgeslagen, en alleen voor zolang het nodig is om het paspoort te maken en te verstrekken. Gezichtsopnames mogen daarentegen wel langer bewaard worden. De vingerafdrukken en de gezichtsopnames mogen alleen decentraal worden opgeslagen. Op het moment worden die gegevens ook niet meer centraal opgeslagen.

De Europese verordening is niet van toepassing op de identiteitskaart (hoewel de Nederlandse wetgever eerst dacht van wel). Om deze reden werd in 2014 de Paspoortwet gewijzigd, waarmee de verplichting om vingerafdrukken af te geven bij het aanvragen van een identiteitskaart werd geschrapt. De Afdeling achtte de inbreuk die op het privéleven werd gemaakt vóór wijziging van de Paspoortwet daarom onrechtmatig.

De zeven uitspraken zijn te vinden op: www.raadvanstate.nl.

*Jan-Willem van der Ree & Frederik Zuiderveen Borgesius*

## Wetenschappelijke Raad voor het Regeringsbeleid: burgers onvoldoende beschermd in de context van big data

*Computerrecht* 2016/152

In april 2016 heeft de WRR (Nederlandse Wetenschappelijke Raad voor het Regeringsbeleid) een rapport gepubliceerd: *Big data in een vrije en veilige samenleving*. De WRR heeft in dit rapport geanalyseerd hoe de Nederlandse overheid big data kan gebruiken in het veiligheidsdomein. Conclusie is dat de huidige regels burgers onvoldoende beschermen en dat het gebruik van big data uitsluitend zijn vruchten kan afwerpen als de regelgeving versterkt wordt om zo fundamentele rechten en vrijheden te waarborgen. Volgens de WRR wordt in de huidige regelgeving vooral aandacht gegeven aan het verzamelen van big data. Maar voor burgers brengen ook de analyse en het gebruik van big data grote risico's met zich mee. "De WRR pleit ervoor dat die bestaande wetgeving wordt aangevuld met de regulering van en het toezicht op de fases van de *analyse* en het *gebruik* van Big Data."

Het rapport is hier te vinden: www.wrr.nl

*Jan-Willem van der Ree & Frederik Zuiderveen Borgesius*

## Rechter: geen verbod uitzending tv-programma Idols

*Computerrecht* 2016/153

Een deelnemer aan het tv-programma *Idols* heeft RTL Nederland en de producent van het programma voor de rechter gedaagd om te voorkomen dat beelden van zijn auditie op RTL 5 zouden worden uitgezonden. Volgens de eiser had Idols hem met opzet zo negatief mogelijk neergezet door de twee slechtste fragmenten uit te zenden. Hierdoor was hij naar zijn mening weggezet als clown, wat nadelig voor zijn carrière zou zijn.

De voorzieningenrechter ging hier echter niet in mee (ECLI:NL:RBAMS:2016:2228): "Op basis van deze beelden kan geen andere conclusie worden getrokken dan dat de auditie van [eiser] ronduit slecht was." Zelfs zo slecht dat het begrijpelijk was dat de juryleden eerst dachten dat het om een grap ging. Daarnaast overwoog de rechter dat de eiser had moeten weten dat niet alleen goede, maar ook slechte audities zouden worden uitgezonden. Tot slot had de eiser door het ondertekenen van de deelnemersverklaring op voorhand en onherroepelijk toestemming gegeven voor het uitzenden van de beelden. RTL 5 mocht de beelden dus uitzenden.

*Jan-Willem van der Ree & Frederik Zuiderveen Borgesius*

## Cijfers bemiddeling Autoriteit Persoonsgegevens bij 'right to be forgotten'-verzoeken

*Computerrecht* 2016/154

Sinds het *Google Spain-arrest* van het HvJ EU hebben mensen onder bepaalde omstandigheden het recht een zoekmachine een link niet te laten tonen in de zoekresultaten, bij zoekopdrachten op naam. Als de zoekmachine weigert, kan de betrokkene aan de Autoriteit Persoonsgegevens vragen om hierbij te bemiddelen. Uit cijfers blijkt dat dit 111 keer is gebeurd sinds juni 2014, waarbij de Autoriteit Persoonsgegevens 32 keer ook daadwerkelijk bemiddeld heeft. In alle gevallen werd om verwijdering uit Google gevraagd; in een aantal gevallen werd daarnaast ook om verwijdering uit Bing gevraagd. In 24 gevallen heeft Google de zoekresultaten verwijderd.

In 61 zaken werd niet bemiddeld, bijvoorbeeld omdat de beslissing van Google juist leek te zijn. Daarnaast werd er 16 keer een zaak niet in behandeling genomen, omdat bijvoorbeeld bleek dat het verzoek te laat was ingediend. In drie gevallen werd succesvol doorverwezen naar een overheidsorganisatie om de publicatie van persoonsgegevens bij de bron te laten verwijderen. Tot slot zijn nog twee zaken in behandeling bij de Autoriteit Persoonsgegevens.

Het overzicht is te vinden op: www.autoriteitpersoonsgegevens.nl.

*Jan-Willem van der Ree & Frederik Zuiderveen Borgesius*

# België

## Hof van Cassatie oordeelt over recht op vergetelheid

*Computerrecht* 2016/155

Het Hof van Cassatie in België heeft een vonnis geveld inzake het recht om vergeten te worden in het voordeel van de betrokkene (*Cass. 29 april 2016, AR C.15.0052.F.*). De Belgische krant Le Soir weigerde een online publicatie van een artikel uit 1994 over een dodelijk auto-ongeluk te anonimiseren, waarin de volledige naam van de bestuurder was vermeld.

Met betrekking tot de gevolgde procedure, oordeelt het Hof dat geen sprake is van een 'persdelict' aangezien geen misdrijf werd gepleegd. De niet-communicatie van de zaak aan het Openbaar Ministerie resulteert daarom niet in nietigheid. Daarnaast oordeelt het Hof dat cascade-aansprakelijkheid niet van toepassing is, aangezien onderhavige zaak geen problematiek inzake het opstellen van het artikel betreft, maar het gevolg is van een redactionele keuze (de online beschikbaarstelling van het artikel).

Het Hof oordeelt dat een balans gemaakt moet worden tussen het recht op privacy (waar het recht om vergeten te worden deel van uitmaakt) en de vrijheid van meningsuiting, en dit temporeel gezien in 2010, bij aanvraag tot anonimisering. Het Hof verwijst naar het arrest *Google Spain* van het HvJ EU en oordeelt (onder andere gezien het significant tijdsverloop) in het voordeel van het recht om vergeten te worden. Le Soir moet bijgevolg de naam van de bestuurder verwijderen uit het online beschikbare artikel.

*Kaat Van Delm*

## Europa

# Privacy Shield is aangenomen

*Computerrecht* 2016/195

De Europese Commissie heeft op 12 juli 2016 het Privacy Shield-besluit, een zogeheten adequaatheidsbesluit, aangenomen. Het Privacy Shield maakt onder bepaalde voorwaarden de doorgifte van persoonsgegevens naar de Verenigde Staten mogelijk. Het Privacy Shield zal jaarlijks worden geëvalueerd.
Het Privacy Shield is de opvolger van het Safe Harbor-besluit. Sinds het Schrems-arrest van het Hof van Justitie van de Europese Unie uit oktober 2015 (*Computerrecht* 2016/6) is het Safe Harbor-besluit ongeldig. Vooral sinds de Snowden-onthullingen over de geheime diensten in de VS was er veel kritiek op de Safe Harbor-constructie.
De Europese Commissie zegt over de VS:

> "Het Office of the Director of National Intelligence (bureau van de directeur van het nationale inlichtingenwerk) heeft (...) verduidelijkt dat het bulksgewijs verzamelen van gegevens alleen onder specifieke voorwaarden mogelijk is en zo gericht mogelijk moet zijn."

Volgens de Europese Commissie voldoet het Privacy Shield aan de vereisten die het Europees Hof van Justitie heeft vastgesteld in het Schrems-arrest. Critici, waaronder Max Schrems, betwijfelen dat.

Meer informatie: www.privacyshield.gov.

# Hof van Justitie van de Europese Unie over toepasselijk recht en Richtlijn bescherming persoonsgegevens (Amazon EU Sàrl)

*Computerrecht* 2016/196

Het Hof van Justitie van de Europese Unie heeft beslist in de zaak Amazon EU Sàrl (C-191/15). Dit arrest betreft een Oostenrijkse zaak, terwijl Amazon EU in Luxemburg gevestigd is. De Oostenrijkse rechter vroeg aan het Hof of de Richtlijn bescherming persoonsgegevens zo moet worden uitgelegd dat de verwerking van persoonsgegevens door een e-commercebedrijf wordt beheerst door het recht van de lidstaat waarop dit bedrijf zijn activiteiten richt.
Het Hof antwoordt:

> "De verwerking van persoonsgegevens door een e-commercebedrijf wordt beheerst door het recht van de lidstaat waarop dit bedrijf zijn activiteiten richt, indien blijkt dat dit bedrijf de betrokken gegevensverwerking verricht in het kader van de activiteiten van een vestiging die zich in die lidstaat bevindt. Het is aan de nationale rechter om te beoordelen of dit het geval is."

Het Hof beantwoordt ook vragen over de Rome I Verordening (betreffende het recht dat van toepassing is op verbintenissen uit overeenkomst), de Rome II Verordening (betreffende het recht dat van toepassing is op niet-contractuele verbintenissen), en de Richtlijn oneerlijke bedingen in consumentenovereenkomsten.

In een andere zaak, over dataretentie (Tele2 Sverige AB, C-203/15) heeft de advocaat-generaal van het Hof van Justitie van de Europese Unie zijn opinie uitgebracht; zie daarover de rubriek Telecommunicatie in dit tijdschrift.

# Europees Hof voor de Rechten van de Mens: arresten artikel 8 (recht op privacy)

*Computerrecht* 2016/197

Onder artikel 8 van het Europees Verdrag voor de Rechten van de Mens heeft eenieder het recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Het Europees Hof voor de Rechten van de Mens (EHRM) heeft een aantal arresten gewezen over artikel 8 EVRM. Hier een selectie.

De zaak Karabeyoğlu/Turkije (7 juni 2016, nr. 30083/10) betreft het onderscheppen van telefoon-communicatie van de heer Karabeyoğlu, een officier van justitie, in het kader van een strafrechtelijk onderzoek naar een illegale organisatie, en het gebruik van de verkregen informatie voor een aparte tuchtprocedure. Het EHRM beslist dat in de tuchtrechtprocedure artikel 8 EVRM is geschonden, om twee redenen. De informatie was gebruikt voor andere doeleinden dan waarvoor deze was verzameld, en de informatie was, anders dan de nationale wet voorschrijft, niet vernietigd binnen 15 dagen nadat het strafrechtelijk onderzoek was afgelopen. Ook in een andere Turkse zaak waarin de telefoon van een advocaat getapt werd, besliste het EHRM dat artikel 8 EVRM geschonden was (Özel/Turkije, 19602/06, 7 juni 2016).

Versini-Campinchien Crasnianski/Frankrijk (nr. 49176/11, 16 juni 2016) betreft de onderschepping, de transcriptie en het gebruik in een tuchtprocedure van gesprekken die een advocaat met een van haar cliënten had. Het enkele feit dat het om een advocaat gaat, is niet voldoende om een schending van artikel 8 EVRM aan te nemen.

De zaak Popovi/Bulgarije (nr. 39651/11, 9 juni 2016) betreft de arrestatie van de heer Popovi, voormalig secretaris-generaal van het Ministerie van Financiën, tijdens een politieoperatie die gepaard ging met veel media-aandacht. Popovi is uiteindelijk vrijgesproken. Het Ministerie van Binnenlandse Zaken had filmbeelden van de arrestatie gemaakt, en die naar buiten gebracht. Onder meer daarom besliste het EHRM dat artikel 8 EVRM was geschonden.

De zaak Bărbulescu/Roemenië (nr. 61496/08) is op 6 juni 2016 verwezen naar de grote kamer. De zaak betreft het ontslag van een werknemer door een particuliere onderneming, omdat de werknemer, in strijd met de bedrijfsregels, het internet gebruikte voor privédoeleinden. In een arrest van 12 januari 2016 besliste het EHRM dat artikel 8 EVRM niet geschonden was. Nu moet de grote kamer zich over de zaak buigen.

## Nederland

# Wijziging Gemeentewet: verruiming van de bevoegdheid van de burgemeester tot de inzet van toezicht met camera's, inclusief drones

*Computerrecht* 2016/198

Sinds 1 juli is de Gemeentewet aangepast (zie J-J. Oerlemans, *Computerrecht* 2016/115). De oude regeling van cameratoezicht in de Gemeentewet was beperkt tot de inzet van statisch cameratoezicht met behulp van vaste camera's. Nu kan de burgemeester mobiele camera's, inclusief *drones*, inzetten. Overigens zette de politie al mobiele camera's in.
De burgemeester mag mobiele camera's inzetten ter handhaving van de openbare orde. Daarbij hoeft geen sprake te zijn van een verstoring van de openbare orde of van een concrete dreiging daarvan. Onder handhaving van de openbare orde door de burgemeester valt ook de algemene voorkoming van strafbare feiten die invloed hebben op de orde en rust.
De burgemeester kan, als de gemeenteraad hem deze bevoegdheid bij verordening heeft verleend, een gebied aanwijzen waarbinnen camera's kunnen worden ingezet. De bevoegdheid tot de inzet van cameratoezicht wordt niet beperkt tot een wettelijk verankerde maximale tijdsduur. De burgemeester bepaalt dus, met inachtneming van de verordening, de tijdsduur van de gebiedsaanwijzing.

# Twee rapporten Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

*Computerrecht* 2016/199

De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) bekijkt of de Wet op de Inlichtingen- en Veiligheidsdiensten 2002 en de Wet veiligheidsonderzoeken goed worden uitgevoerd. Daarbij toetst ze het handelen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD).
De CTIVD heeft twee nieuwe rapporten gepubliceerd.
In 2014 is er in de Tweede Kamer gedebatteerd over praktijken van de Amerikaanse National Security Agency en de rol van Nederland daarin. Er werden verschillende moties ingediend. Naar aanleiding van die moties heeft de CTIVD een rapport gepubliceerd over de invulling van samenwerkingscriteria door de AIVD en de MIVD (Rapport 48) en over het uitwisselen van gegevens met buitenlandse inlichtingen- en veiligheidsdiensten (Rapport 49).

De rapporten zijn te vinden op www.ctivd.nl.

# Rechtbank: Instagram moet naam vrijgeven van anonieme accounthouder vanwege pesten

*Computerrecht* 2016/200

Op Instagram is door een onbekende een account aangemaakt; daarop plaatste de onbekende pornografische dan wel seksueel getinte foto's en video's. Daarbij werd door het vermelden van een bijnaam, "Varkensneus", gesuggereerd dat de foto's en video's een bepaald minderjarig meisje betroffen. De moeder van het meisje heeft aangifte gedaan tegen de onbekende accounthouder bij de politie. Instagram heeft de account verwijderd. Toen de moeder daarom verzocht, weigerde Instagram echter de naam- en adresgegevens van de accounthouder te verstrekken. Tijdens de zitting vertelde de moeder dat het meisje erg wordt gepest.
De rechtbank besliste dat Instagram de naam- en adresgegevens van de accounthouder moet verstrekken (Rechtbank Noord-Holland 5 juli 2016, ECLI:NL:RBNHO:2016:5535). Onder verwijzing naar *Lycos/Pessers* (Hoge Raad 25 november 2005, ECLI:NL:HR:2005:AU4019, *Computerrecht* 2006/11) zei de rechtbank:

> "Een rechtsplicht tot het verstrekken van NAW-gegevens zoals in deze zaak gevorderd, kan voor een provider bestaan als aannemelijk is dat anoniem, althans door een door de benadeelde niet te traceren persoon, onrechtma-

tige uitlatingen via deze provider openbaar zijn gemaakt en de benadeelde alleen door tussenkomst van de provider, door middel van het verstrekken van NAW-gegevens, dergelijk onrechtmatig handelen zou kunnen bestrijden."

De rechtbank legde ook de gevorderde dwangsom van € 500 per dag op, als prikkel ter nakoming van het vonnis.

## Hof: Google Blogger hoeft blogpost over veroordeelde crimineel niet te verwijderen

### *Computerrecht* 2016/201

Een man die tot zes jaar gevangenisstraf was veroordeeld wegens poging tot uitlokking van een huurmoord, wilde dat Google Blogger een blogpost over hem verwijderde. Het gaat hier om een verwijderingsverzoek aan Google als aanbieder van een *blogdienst*. Het gaat hier dus niet om een verzoek aan Google als aanbieder van een *zoekmachine* om niet meer naar een blogpost te verwijzen.
Het Hof bevestigt een kort geding-vonnis uit 2015 (ECLI:NL:RBDHA:2015:11276): Google hoeft de blogpost niet te verwijderen. Het Hof noemt zeven redenen waarom in dit geval de vrijheid van meningsuiting van de (anonieme) blogger zwaarder weegt dan de privacy van de man. De blogpost is niet onrechtmatig volgens het Hof.
De man noemde onder andere als argument voor verwijdering dat de blogpost over hem de verwerking van bijzondere persoonsgegevens (strafrechtelijke gegevens) met zich brengt. De man betoogde dat het verwerken van zulke persoonsgegevens verboden is, en dat daarom de blogpost onrechtmatig is. Het Hof zegt echter dat de verwerking onder de journalistieke exceptie van de Wet bescherming persoonsgegevens valt. (Google als zoekmachine-exploitant zou zich overigens niet op die uitzondering kunnen beroepen. Zie *Computerrecht* 2016/126.)
Dezelfde man had overigens al in twee instanties een zaak verloren waarin hij Google verzocht om bepaalde resultaten te verwijderen uit de zoekmachine (Rb. Amsterdam 18 september 2014, ECLI:NL:RBAMS:2014:6118; Gerechtshof Amsterdam 31 maart 2015, ECLI:NL:GHAMS:2015:1123). In die zaak is cassatie ingesteld. De Hoge Raad zal zich dus buigen over een 'right to be forgotten' zaak.

## Autoriteit Persoonsgegevens, nieuwsoverzicht

### *Computerrecht* 2016/202

Aleid Wolfsen is de nieuwe voorzitter van de Autoriteit Persoonsgegevens (AP). Eerder was Wolfsen onder meer rechter, Tweede Kamer-lid, en burgemeester van Utrecht. De oude voorzitter, Jacob Kohnstamm, is benoemd tot Officier in de Orde van Oranje-Nassau vanwege zijn verdiensten voor de privacybescherming. Hieronder een overzicht van ander nieuws met betrekking tot de AP.

De AP heeft, naar aanleiding van een wijziging van de Telecommunicatiewet per 1 juli 2016, haar boetebeleidsregels aangepast. In de gewijzigde Telecommunicatiewet is het boetemaximum verhoogd van € 450.000 tot € 900.000 (zie ook de rubriek Telecommunicatie in dit tijdschrift).

De AP heeft winkels en gemeenten gewezen op de wettelijke eisen die gelden wanneer zij gebruikmaken van wifi-tracking (16 juni 2016). Verder concludeert de AP na onderzoek dat bij bijna de helft van de Nederlandse ziekenhuizen informatie van bezoekers van de ziekenhuiswebsites wordt doorgegeven aan derden via tracking cookies. De AP heeft 39 ziekenhuizen en de brancheorganisaties van de ziekenhuizen gewezen op de overtredingen (23 juni 2016).

De AP heeft de Belastingdienst aangeschreven over onrechtmatig verstrekte inkomensgegevens van huurders aan hun verhuurders. Daarbij heeft de AP de Belastingdienst verzocht verhuurders van sociale huurwoningen die onrechtmatig verstrekte inkomensgegevens onder zich hebben, te vragen om deze gegevens te vernietigen. De Belastingdienst heeft aan de AP laten weten dat zij verhuurders van sociale huurwoningen heeft gevraagd om de inkomensgegevens over de jaren 2013-2015 te vernietigen (13 juni 2016).

Een aantal verantwoordelijken heeft overtredingen beëindigd, waaronder Google. Eerder had de AP maatregelen geëist onder dreiging van een dwangsom. "Inmiddels heeft de Autoriteit vastgesteld dat Google ondubbelzinnige toestemming vraagt van ál zijn gebruikers voor het gebruik van hun persoonsgegevens. Hierdoor is de resterende overtreding beëindigd en hoeft het bedrijf geen dwangsom te betalen" (14 juni 2016).

De Gemeente Renkum heeft eerder op de gemeentesite gepubliceerde adressen van opgerolde wietkwekerijen van de site verwijderd (6 juni 2016). Elf gemeenten hebben de eerder door de AP geconstateerde overtredingen met betrekking tot de beveiliging van persoonsgegevens die met Suwinet worden uitgewisseld beëindigd (22 juli 2016). Na onderzoek van de AP hebben uitzendbureaus Adecco (5 juli 2016) en Randstad (19 juli 2016), in verschillende zaken, overtredingen beëindigd.

Ook bedrijfsrecherchebureau Hoffmann BV heeft zijn werkwijze aangepast zodat het niet langer in strijd met de wet handelt. Hoffmann verzamelde onder meer sociale mediaprofielen van sollicitanten en werknemers. De AP zegt over toestemming als grondslag voor het screenen van sollicitanten:

> "Toestemming kan geen grondslag zijn voor de screening van sollicitanten omdat de sollicitant afhankelijk is van de (potentiele) werkgever en de toestemming daarom niet vrij is. Ondanks dat de Autoriteit Persoonsgegevens hierover heeft gepubliceerd lijkt een aantal screeningsbedrijven toestemming nog steeds als grondslag aan te merken."

De AP heeft geadviseerd over een ontwerpbesluit dat screening van woningzoekenden door gemeenten regelt (18 juli 2016).

Meer informatie: www.autoriteitpersoonsgegevens.nl.

## Proefschrift Axel Arnbak: hoe zou de EU-wetgever de beveiliging van privé-communicatie moeten beschermen?

### *Computerrecht* 2016/203

Het proefschrift van Axel Arnbak (Instituut voor Informatierecht, Universiteit van Amsterdam) is verschenen bij Kluwer Law International: "Securing private communications, Protecting private communications security in EU law – Fundamental rights, functional value chains and market incentives".
Het proefschrift, dat economische en juridische inzichten combineert, biedt vijf aanbevelingen voor de EU-wetgever om privé-communicatiebeveiliging te beschermen: "(i) De EU-wetgever moet de uit de fundamentele rechten voortvloeiende positieve verplichtingen rondom privé-communicatiebeveiliging steviger veiligstellen in EU-wetgeving; (ii) De impliciete en verborgen gijzeling van EU-wetgeving door nationale veiligheidsbelangen van de lidstaten moet in de toekomst geëxpliciteerd en genuanceerd worden; (iii) De EU-wetgever dient bescherming te bieden in de gehele functionele waardeketen van elektronische communicatie, in plaats van alleen aan 'persoonsgegevens' of ten aanzien van conventionele telecom-aanbieders, zoals internet access providers; (iv) De EU-wetgever zou hardnekkig marktfalen in communicatiebeveiliging moeten aanpakken". (v) Arnbak presenteert verder een analytisch model als vertrekpunt voor de bescherming van privé-communicatiebeveiliging in EU-wetgeving.

Zie voor meer informatie en de academische versie van het proefschrift: www.axelarnbak.nl.

## Proefschrift Rob van den Hoven van Genderen: privacyschending overheid op grond van nationale veiligheid

### *Computerrecht* 2016/204

Op 10 juni 2016 is Rob van den Hoven van Genderen bij de Vrije Universiteit Amsterdam (VU) gepromoveerd op zijn proefschrift "Privacy Limitation Clauses: Trojan Horses under the Disguise of Democracy. On the Reduction of Privacy by National Authorities in Cases of National Security and Justice Matters".
Op de site van de VU ligt Van den Hoven van Genderen toe: "Ik heb in mijn onderzoek vastgesteld dat privacy en bescherming van persoonsgegevens onderhevig zijn aan de dynamiek van de politieke situatie. Hierin is een golfbeweging te zien: na 9/11 kwam er een golf van nieuwe regels die de mogelijkheden voor inlichtingendiensten en justitie vergroten, en na de ontboezemingen van Snowden kwam er weer een rem op die activiteiten. En nu, na de aanslagen in Parijs en Brussel, worden het toezicht en interceptie-bevoegdheden, bijvoorbeeld om af te luisteren, opnieuw versterkt."
Van den Hoven van Genderen pleit voor een actievere en meer controlerende rol van het parlement, en voor een onafhankelijke autoriteit die de uitvoering van privacybeperkende maatregelen controleert. "Er dient steeds een onafhankelijke belangenafweging bij de invoering en uitvoering van zulke maatregelen te zijn, waarbij alle belangen van een democratische rechtsorde in ogenschouw worden genomen."

Zie voor meer informatie: www.rechten.vu.nl.

## België

## Hof beslist ten nadele van Privacycommissie in Facebook-zaak

### *Computerrecht* 2016/205

Het Hof van Beroep heeft op 29 juli 2016 het vonnis van de rechtbank in de Facebook-zaak geannuleerd. De zaak betrof

het gebruik van cookies en sociale plug-ins voor het volgen van online gedrag van internetgebruikers zonder Facebook-account. Omdat Facebook een aanbeveling van de Privacycommissie niet opvolgde, dagvaardde de Privacycommissie Facebook. In kort geding werd beslist dat Facebook het registreren van deze gegevens moest stopzetten, gezien het feit dat Facebook op geen enkele wijze toestemming verwierf om gegevens te verwerken van personen die niet over een Facebook-account beschikken.
Facebook ging tegen deze beslissing in beroep, en maakte als reactie op de uitspraak alle openbare Facebook pagina's ontoegankelijk voor Belgische internetgebruikers zonder Facebook-account.
In juli 2016 annuleerde het Hof van Beroep de beslissing in kort geding. Volgens het Hof van Beroep zijn de Belgische hoven en rechtbanken niet bevoegd ten aanzien van Facebook Inc (de Amerikaanse moedermaatschappij) en Facebook Ireland, waar de gegevens voor Europa verwerkt worden. Het Hof zegt dat Belgische hoven en rechtbanken wel bevoegd zijn ten aanzien van Facebook België. Maar volgens het Hof is er geen urgentievereiste (spoedeisend belang).
De Privacycommissie overweegt in cassatie te gaan in deze kort geding-procedure. De procedure ten gronde wordt behandeld in 2017.

Meer informatie: www.privacycommission.be.

*Patrick Van Eecke, Kaat Van Delm & Frederik Zuiderveen Borgesius*

## Jaarverslag Belgische Privacycommissie

### *Computerrecht* 2016/206

De Belgische Privacycommissie heeft haar jaarverslag voor 2015 gepubliceerd. Uit het jaarverslag blijkt duidelijk dat de Privacycommissie meer bemiddelingsdossiers te verwerken heeft gekregen (met vaststelling van inbreuken in 64% van de gevallen), assertiever voor de dag gekomen is (de Facebook-zaak) en standpunt heeft ingenomen op enkele belangrijke nieuwe technologische ontwikkelingen (drones, geo-locatie).
Het jaarverslag bevat statistieken inzake de activiteiten van 2015: Vijf aanbevelingsdossiers werden geopend, met name aanbevelingen aan wetgevende instellingen of verantwoordelijken voor de verwerking, waarvan het bekendste dossier de Facebook aanbeveling is, die uitmondde in een rechtszaak (zie verder), en 64 adviesdossiers, voornamelijk opgestart via adviesaanvragen van wetgevende instellingen. Er werden 6240 aangiftes voor camerabewaking geteld (een stijging van 886 aangiftes in vergelijking met 2014). 4192 informatie-, bemiddeling- en controledossiers werden behandeld (een stijging van 336 dossiers in vergelijking met 2014): 3561 informatieaanvragen, 347 bemiddelingsaanvragen (i.e. klachtenprocedures, waarbij de Privacycommissie als bemiddelaar optreedt) en 284 controledossiers (i.e. dossiers met betrekking tot de autorisatie voor bijvoorbeeld onrechtstreekse toegang tot gegevens, waarvoor de Privacycommissie een controle of onderzoek uitvoert). Er werd een inbreuk op de privacy vastgesteld in 64% van de bemiddelingsaanvragen en 26% werd ongegrond verklaard. De onderwerpen waar het vaakst een informatieaanvraag voor werd ingediend zijn privacyaspecten op het werk, beveiligingscamera's, direct marketing, het recht op afbeelding en internet.
Het jaarverslag geeft ook een overzicht van projecten van de Privacycommissie. De Privacycommissie heeft een aanbeveling uitgevaardigd inzake cookies (Aanbeveling 01/2015). De Aanbeveling introduceert een lijst aanbevelingen, die de problemen samenvatten en praktische antwoorden bieden op vragen van juristen, technici en website ontwikkelaars met betrekking tot informatieverstrekking en direct marketing praktijken. Er werd advies verleend bij een ontwerp van Koninklijk besluit met betrekking tot het gebruik van op afstand bestuurde luchtvaartuigen. De Privacycommissie verleende een positief advies, aangezien het ontwerp de Privacywet toepasselijk maakt op alle soorten drones. Het Koninklijk besluit trad in werking op 25 april 2016. In navolging van de terroristische aanslagen in Parijs, werden wetgevende initiatieven genomen die een impact konden hebben op privacy. Er werd de Privacycommissie gevraagd om advies uit te brengen inzake bepaalde anti-terreurmaatregelen. De Privacycommissie heeft een paper gepubliceerd met betrekking tot het thema 'Privacy op de werkvloer'. Deze paper bepaalt hoe persoonsgegevens op een correcte en privacy vriendelijke wijze moeten behandeld worden op de werkvloer. Thema's behandeld in deze paper zijn onder andere geo-lokalisatie in bedrijfswagens, toezicht op elektronische communicatie en camerabewaking.

Meer informatie: www.privacycommission.be.

*Patrick Van Eecke & Kaat Van Delm*

## Europa

# Advocaat-generaal: geen 'right to be forgotten' ten aanzien van vennootschapsregister

*Computerrecht* 2016/239

De advocaat-generaal van het Hof van Justitie van de Europese Unie heeft zijn opinie gepubliceerd in de zaak *Manni/Italië* (C-398/15). Manni vroeg De Kamer van Koophandel een bestand te anonimiseren met betrekking tot een onderneming die in 1992 failliet ging, waarvan hij de enige directeur was.

De advocaat-generaal zegt, samengevat, dat persoonsgegevens in een handelsregister relevant blijven, en niet verwijderd moeten worden. De advocaat-generaal vindt 'dat openbare registers als de vennootschapsregisters hun wezenlijke doel, te weten het bieden van rechtszekerheid door middel van de transparante beschikbaarheid van juridisch betrouwbare informatie, slechts dan kunnen waarmaken, indien zij voor eenieder en voor onbepaalde tijd toegankelijk zijn'.

# Advocaat-generaal: ontwerpovereenkomst EU/Canada inzake doorgifte van persoonsgegevens van passagiers in strijd met grondrechten

*Computerrecht* 2016/240

De EU en Canada hebben in 2010 onderhandelingen gestart over een overeenkomst over de doorgifte en de verwerking van persoonsgegevens van passagiers: *pasenger name records*. Deze PNR-overeenkomst moet het mogelijk maken dat PNR-gegevens aan de Canadese autoriteiten worden doorgegeven met het oog op het gebruik, de bewaring en eventueel de latere doorgifte van gegevens, om terrorisme en andere grensoverschrijdende criminaliteit te bestrijden.

De overeenkomst is ondertekend in 2014. Daarna heeft de Raad van de Europese Unie de goedkeuring gevraagd van het Europees Parlement. Het Parlement heeft zich tot het Hof gewend met de vraag of de ontwerpovereenkomst verenigbaar is met het EU-recht, en in het bijzonder met het recht op privacy en het recht op gegevensbescherming (artikel 7 en 8 van het Handvest van de grondrechten van de EU).

De advocaat-generaal zegt dat meerdere bepalingen van de ontwerpovereenkomst in strijd zijn met de grondrechten van de EU.

# Oostenrijkse prejudiciële vragen in zaak Schrems tegen Facebook

*Computerrecht* 2016/241

De hoogste Oostenrijkse rechter heeft op 12 september prejudiciële vragen gesteld aan het Hof van Justitie van de Europese Unie (C-498/16), in een door Max Schrems aangespannen rechtszaak tegen Facebook.

Schrems wil samen met 25.000 anderen een vordering instellen tegen Facebook. De Oostenrijkse rechter vraagt zich af of dit mogelijk is, nu een deel van die anderen in verschillende EU-lidstaten of zelfs buiten de EU wonen. Daarnaast zegt Facebook dat Schrems niet als consument moet worden aangemerkt, nu hij publiekelijk opkomt voor zijn rechten, door bijvoorbeeld boeken te publiceren en lezingen te houden.

Het gaat, samengevat, om twee prejudiciële vragen:

(1) Wordt onder het begrip 'consument' verstaan: de eigenaar van een privé-Facebook-account die de vorderingen van een groot aantal consumenten verkrijgt onder de toezegging dat hen ieder een deel van de winst toekomt bij een eventuele toewijzing van de vorderingen, en in het kader daarvan boeken publiceert, lezingen geeft, websites beheert en donaties verzamelt?

(2) Moet artikel 16 van de Brussel I Verordening (EG 44/2001) zo worden uitgelegd dat een consument in een lidstaat gezamenlijk met het uitoefenen van zijn eigen rechten, ook gelijksoortige rechten tegen hetzelfde bedrijf kan uitoefenen van andere consumenten die woonachtig zijn in: i) dezelfde lidstaat; ii) een andere lidstaat; of iii) een derde land?

Er spelen nu dus drie zaken rond Facebook in Luxemburg. Er zijn prejudiciële vragen gesteld in een Duitse zaak naar aanleiding van een onderzoek van de privacytoezichthouder van Schleswig-Holstein (C-210/16). Max Schrems meldt dat er mogelijk prejudiciële vragen worden gesteld in een Ierse procedure, over modelcontracten voor de doorgifte van persoonsgegevens naar niet-EU landen (zie www.europe-v-facebook.org). In 2015 leidde een procedure tussen Schrems en Facebook tot de ongeldigverklaring van het Safe Harbor besluit (C-362/14).

Meer informatie: www.fbclaim.com.

*Chelsea Bruijn & Frederik Zuiderveen Borgesius*

# Ierse prejudiciële vragen: zijn geschreven examenantwoorden persoonsgegevens?

## *Computerrecht* 2016/242

Nowak zakte, tot vier keer toe, voor een examen van de organisatie Chartered Accountants Ireland. Nowak deed een inzageverzoek op grond van de Ierse Wet bescherming persoonsgegevens, om zijn handgeschreven examenantwoorden in te zien. Chartered Accountants Ireland verstrekte een aantal gegevens, maar weigerde Nowak's examenantwoorden te verstrekken, omdat dat geen persoonsgegevens zouden zijn.

Nowak klaagde bij de Ierse privacytoezichthouder, de Data Protection Commissioner. De Data Protection Commissioner zei dat de examenantwoorden geen persoonsgegevens zijn, en weigerde de klacht te onderzoeken. Nowak zegt dat zijn antwoorden in het examenformulier wel persoonsgegevens zijn. Hij stelt bijvoorbeeld dat het formulier biometrische gegevens bevat, omdat de antwoorden met de hand zijn geschreven, en zijn antwoorden een weergave vormen van zijn intellect, denkprocessen en mening.

Nowak stapte naar de rechter; die gaf de Data Protection Commissioner gelijk. Nowak ging twee keer in hoger beroep. Het Ierse Supreme Court heeft uiteindelijk twee prejudiciële vragen gesteld aan het Hof van Justitie van de Europese Unie (C-434/16):

1. Kunnen gegevens die in of als antwoorden door een kandidaat tijdens een beroepsexamen worden opgeschreven, persoonsgegevens zijn in de zin van [De Richtlijn bescherming persoonsgegevens]?
2. Indien het antwoord op vraag 1 luidt dat alle of sommige van dergelijke gegevens persoonsgegevens kunnen zijn in de zin van de richtlijn, welke factoren zijn dan relevant voor de vaststelling of het in een bepaald geval bij dergelijk schriftelijk examenwerk om persoonsgegevens gaat, en hoe zwaar dienen dergelijke factoren te wegen?

# Nederland

# Rechter: school hoeft niet mee te werken met onderzoek naar plaatser wraakporno

## *Computerrecht* 2016/243

In de zogenoemde 'wraakpornozaak' heeft de voorzieningenrechter op 21 september een vonnis gewezen. Eiseres, het slachtoffer, heeft in juni 2015 een kort geding gevoerd tegen Facebook nadat een haar onbekende derde een account heeft aangemaakt op Facebook met een profielfoto van eiseres (*Computerrecht* 2015/163). Deze derde heeft daarop een opname geplaatst waarin eiseres seksuele handelingen verricht bij een jongen die ten tijde van maken van de opname haar vriend was. Eiseres is op de opname duidelijk herkenbaar in beeld. Eiseres had haar (inmiddels) ex-vriend geen toestemming gegeven om de opname te openbaren.

In 2016 heeft (na procedures in kort geding) een onderzoek plaatsgevonden bij Facebook naar het account. Uit dit onderzoek is gebleken dat de maker van het account voor het uploaden van de opname hoogstwaarschijnlijk gebruik heeft gemaakt van een IP-adres dat werd gebruikt door het ROC West-Brabant, een organisatie met 20 scholen.

Eiseres vorderde in kort geding dat het ROC West-Brabant een intern onderzoek start naar de uploader van een wraakpornofilmpje.

De rechter wijst het verzoek van eisers af. Het onderzoek zou de verwerking van persoonsgegevens met zich mee brengen. Artikel 8(f) van de Wet bescherming persoonsgegevens, de legitiem-belang-bepaling, staat verwerking toe als de belangen van de verantwoordelijke zwaarder wegen dan de belangen van de betrokkene. Er moet daarom een afweging gemaakt worden tussen het algemene privacybelang van de leerlingen en medewerkers van het ROC enerzijds, en het individuele belang van het slachtoffer anderzijds.

> "De voorzieningenrechter overweegt dat [eiseres] niet aannemelijk heeft gemaakt dat zij de identiteit van de maker van het Nep-Account niet of op minder bezwaarlijke wijze dan middels verwerking van persoonsgegevens op de computer- en netwerksystemen van het ROC kan achterhalen. Het ROC heeft in dit verband gesteld dat een strafrechtelijk onderzoek gaande is, welk onderzoek strafvorderlijke mogelijkheden biedt tot waarheidsvinding die nog niet zijn aangewend."

> "Ten slotte neemt de voorzieningenrechter in aanmerking dat de vordering van [eiseres] er op gericht is om een schadeclaim te kunnen ontwikkelen tegen de thans nog anonieme derde en dat de vordering niet tot doel heeft een einde te maken aan een onrechtmatige situatie die nog steeds voortduurt. Het onrechtmatig handelen, hoe verwerpelijk ook, is al geruime tijd voorbij."

De rechter concludeert dat het ROC niet onrechtmatig heeft gehandeld door het privacybelang van haar leerlingen en medewerkers te laten prevaleren boven het individuele belang van de eiseres.

ECLI:NL:RBZWB:2016:5832

*Chelsea Bruijn & Frederik Zuiderveen Borgesius*

# Autoriteit Persoonsgegevens, nieuws

## *Computerrecht* 2016/244

De Autoriteit Persoonsgegevens (AP) heeft vastgesteld dat Stichting Voor Mijn Kleinkind in strijd handelt met de Wet bescherming persoonsgegevens (Wbp). De stichting publiceert op internet gegevens van kinderen met wie grootouders contact zoeken. Hiermee schendt de stichting de privacyrechten van de betreffende kinderen en hun ouders. Op de site van de stichting, voormijnkleinkind.nl, kunnen grootouders die tegen hun wil geen contact hebben met hun kleinkind een pagina voor dit kind aanmaken en daarop berichten plaatsen. Wie in een zoekmachine de voor- en achternaam van een kind intypt, kan bij deze pagina terechtkomen. Als de stichting haar werkwijze niet in overeenstemming brengt met de wet, kan de AP handhavende maatregelen nemen (11 oktober 2016).

De AP heeft de gedragscode slimme meters overige dienstenaanbieders rechtmatig verklaard. De volledige titel luidt: 'Gedragscode Verwerking door Overige Diensten Aanbieders (ODA's) van op Kleinverbruikers betrekking hebbende Persoonlijke Meetgegevens afkomstig uit Slimme Meters'. Overige Diensten Aanbieders zijn bedrijven die energiebesparingsdiensten leveren, zoals apps waarmee mensen hun energieverbruik kunnen monitoren. Overige Diensten Aanbieders verwerken persoonlijke meetgegevens. Deze gegevens geven inzicht in het elektriciteits- en gasverbruik van mensen. Dit zijn persoonsgegevens (21 september 2016).

De aanbieders van interactieve digitale televisie XS4ALL en KPN hebben na onderzoek van de AP diverse overtredingen van de Wbp beëindigd. De bedrijven informeerden hun klanten onvoldoende over het verzamelen en gebruiken van persoonsgegevens over het tv-kijkgedrag. De bedrijven stelden zonder toestemming van klanten kijkcijfers op over het tv-kijkgedrag voor onder meer marktonderzoek. Ook bewaarden de bedrijven de persoonsgegevens te lang (12 augustus 2016).

De AP heeft een last onder dwangsom opgelegd aan Bluetrace. Dit bedrijf levert wifi-tracking-technologie waarmee in en rondom winkels de wifisignalen van mobiele apparaten worden opgevangen (zie *Computerrecht* 2016/125). Uit onderzoek van de AP blijkt dat Bluetrace via wifi-tracking locatiegegevens van winkelbezoekers en voorbijgangers verzamelt zonder hen hier goed over te informeren. Bovendien verzamelt en bewaart Bluetrace meer gegevens dan noodzakelijk is voor het in kaart brengen van bezoekersaantallen. Bluetrace heeft na het onderzoek maatregelen getroffen, maar deze zijn onvoldoende om de overtredingen te beëindigen. In de last onder dwangsom wordt Bluetrace gesommeerd de overtredingen binnen zes maanden te beëindigen (1 september 2016).

De AP heeft geadviseerd over het register onderwijsdeelnemers, in de voorgestelde Algemene wet onderwijs (11 augustus 2016). Ook heeft de AP geadviseerd over de aanpassing van de Regeling Jeugdwet. Op grond van deze regeling mogen jeugdhulpverleners hun geheimhoudingsplicht doorbreken voor de financiële afwikkeling van en controle op de jeugdhulp (3 oktober 2016).

In een brief aan de Minister van Binnenlandse Zaken uit de AP haar bezorgdheid met betrekking tot het eID-stelsel. Dit stelsel wordt gezamenlijk ontwikkeld door de overheid en het bedrijfsleven en vormt een standaard voor identificatie bij online dienstverlening. Volgens de AP is er onvoldoende aandacht besteed aan de beveiliging (27 september 2016).

De AP heeft vragen en antwoorden gepubliceerd over gezondheidsprojecten voor kinderen en jongeren. Gemeenten monitoren daarbij, met hulp van scholen, de gezondheid van leerlingen, bijvoorbeeld om overgewicht tegen te gaan (22 augustus 2016). Ook heeft de AP vragen en antwoorden gepubliceerd over datalekken waarbij ransomware is aangetroffen. Ransomware is malware die een computer of bestanden gijzelt (3 oktober 2016).

De bestuursrechter heeft beslist dat de AP een onderzoek had moeten uitvoeren naar de Nederlandse Spoorwegen (ECLI:NL:RBGEL:2016:4553). Een reiziger had bij de AP een verzoek tot handhaving ingediend, omdat een voordeelurenabonnement bij de Nederlandse Spoorwegen alleen te combineren is met een persoonlijke OV-chipkaart, waardoor zijn reisgegevens verwerkt worden. Reizigers die veel om hun privacy geven, kunnen dus niet met korting reizen. De AP had het verzoek van de man afgewezen. Kortom, volgens de rechter moet de AP meer onderzoek moet doen naar de manier waarop de Nederlandse Spoorwegen persoonsgegevens verwerkt.

# Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten: rapport over Militaire Inlichtingen- en Veiligheidsdienst en targeting

## *Computerrecht* 2016/245

De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) heeft een toezichtsrapport gepubliceerd over de over de bijdrage van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) aan targeting. In het rapport wordt met de term targeting gedoeld op 'het proces dat kan leiden tot (dodelijk) geweldgebruik door strijdkrachten om een strategische doelstelling te bereiken in de context van een

(militaire) operatie'. De CTIVD gaat in op de rol van de MIVD bij targeting in lopende en recent afgeronde missies en de op dit punt relevante samenwerking met buitenlandse diensten.

De CTIVD heeft onder meer het volgende vastgesteld:

1. Het juridisch kader dat de MIVD in zijn huidige beleid voor verstrekking hanteert, is onvoldoende toegespitst op het risico dat hiermee kan worden bijgedragen aan onrechtmatig geweldgebruik.
2. De MIVD heeft in het kader van twee militaire missies (waar Nederland zelf onderdeel van was) doelbewust een bijdrage aan targeting geleverd. Deze verstrekkingen waren in overeenstemming met de wet.
3. De MIVD heeft, buiten militaire missies waar Nederland zelf onderdeel van was, geen inlichtingen verstrekt aan buitenlandse diensten met het uitdrukkelijke doel hiermee bij te dragen aan targeting.
4. Ondanks dat de MIVD niet de bedoeling had bij te dragen aan targeting, konden sommige aan buitenlandse diensten verstrekte inlichtingen daar in beginsel wel voor worden gebruikt. De CTIVD heeft geen concrete aanwijzingen gevonden dat de MIVD hierbij een onaanvaardbaar risico heeft geaccepteerd op een bijdrage aan onrechtmatig geweldgebruik.

Het toezichtsrapport 50 is te vinden op www.ctivd.nl.

*Chelsea Bruijn & Frederik Zuiderveen Borgesius*

## België

# Privacycommissie, nieuws

## *Computerrecht* 2016/246

De Privacycommissie heeft een stappenplan gepubliceerd voor bedrijven en organisaties ter voorbereiding van de implementatie van de Algemene Verordening Gegevensbescherming. Met behulp van het stappenplan kunnen verantwoordelijken en verwerkers de verschillen tussen de huidige Privacywet en de nieuwe Verordening opsporen en hun beleid hierop afstemmen (16 september 2016).

De Privacycommissie heeft geadviseerd over een ontwerp van koninklijk besluit houdende uitvoering van verschillende artikelen van de wet houdende internering en diverse bepalingen inzake justitie (Advies nr. 46/2016, 31 augustus 2016). Ook heeft de Privacycommissie geadviseerd over het wetsvoorstel tot wijziging van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, wat betreft de werking van het Controleorgaan op de politionele informatie (Advies nr. 45/2016, 31 augustus 2016).

Meer informatie: www.privacycommission.be.

# Proefschrift Brendan Van Alsenoy, over verantwoordelijken en verwerkers

## *Computerrecht* 2016/247

Op 30 augustus 2016 heeft Brendan Van Alsenoy (KU Leuven) met succes zijn proefschrift verdedigd: Regulating data protection: the allocation of responsibility and risk among actors involved in personal data processing. Prof. dr. Peggy Valcke is de promotor; dr. Els Kindt is co-promotor. Hier een samenvatting:

> "De Europese wetgeving voorziet een aantal voorwaarden en verplichtingen om ervoor te zorgen dat de persoonlijke levenssfeer van het individu beschermd blijft wanneer zijn of haar persoonsgegevens worden verwerkt. De wetgeving maakt daarbij een onderscheid naargelang de hoedanigheid van de partij die bij de verwerking van persoonsgegevens betrokken is. Het belangrijkste onderscheid is het onderscheid tussen de 'verantwoordelijke voor de verwerking' en de 'verwerker'. Samen vormen deze begrippen de verdeelsleutel waarmee verantwoordelijkheid en aansprakelijkheid wordt toegewezen. Bepaalde technologische en maatschappelijke ontwikkelingen hebben er echter voor gezorgd dat het steeds moeilijker wordt om deze begrippen toe te passen in de praktijk. Het proefschrift wenst te vernemen of (en zo ja, hoe) de verdeling van verantwoordelijkheid en aansprakelijkheid ten aanzien van partijen die betrokken zijn bij de verwerking van persoonsgegevens kan worden herzien op een wijze die de rechtszekerheid vergroot met behoud van ten minste een gelijkwaardig niveau van bescherming van persoonsgegevens."