25 jaar Privacy & Informatie

277

In dit laatste redactioneel van 2022 blik ik graag even terug en ook alvast vooruit naar het jaar 2023. Dat wordt een bijzonder jaar. Niet alleen omdat de AVG dan vijf jaar van toepassing is. Maar vooral omdat dit tijdschrift *Privacy & Informatie* dan 25 jaar bestaat. De redactie wil dat niet ongemerkt voorbij laten gaan. Maar daarover straks meer.

Het eerste nummer van *P&I* verscheen in april 1998. Als tijdschrift volgde *P&I* destijds een ander tijdschrift op: *Privacy & Registratie*, dat werd uitgegeven door de Stichting Privacy & Registratie. In het allereerste redactioneel schreef de redactie van toen[1] dat het als doelgroep voor ogen had: 'mensen die min of meer beroepsmatig bij het onderwerp bescherming van de persoonlijke levenssfeer betrokken zijn'. Die omschrijving is destijds voldoende ruim gekozen om ook vandaag nog de groep lezers te kunnen omvatten. De redactie had voor ogen om in het tijdschrift aandacht te besteden aan informationele privacy, maar ook aan de gevolgen van ICT-ontwikkelingen. De behoefte daaraan kwam voort uit de signalen van die tijd. Ten eerste de toenemende belangstelling voor het onderwerp. Privacy nam weer een belangrijke plaats in sinds de IRT-affaire. Ten tweede de talloze technologische ontwikkelingen. Bedenk dat internet nog maar in de kinderschoenen stond; de eerste website dateert van 1991. Ten derde de toegenomen mondigheid van de burger die steeds beter zijn weg wist te vinden naar de toenmalige toezichthouder, de Registratiekamer, en de rechter. Een vierde signaal was de wetgeving in ontwikkeling. Zo werd in februari 1998 het wetsvoorstel Wet bescherming persoonsgegevens bij de Tweede Kamer ingediend terwijl ook de Telecommunicatiewet een belangrijke plaats in het privacyrecht had ingenomen.[2]

Het tijdschrift is in de afgelopen jaren ook veranderd. Zo bestaat het uitneembare katern met Berichten van de Registratiekamer niet meer, maar bevat *P&I* wel een rubriek Actualiteiten uit België.

In de eerste aflevering van *P&I* waren vier artikelen opgenomen. Jan Holvast gaf een overzicht op hoofdlijnen van het wetsvoorstel Wet bescherming persoonsgegevens en presenteerde daarin ook een stappenplan.[3] Corien Prins stond in haar bijdrage stil bij de mate van betrokkenheid van burgers bij de bescherming van hun persoonsgegevens.[4] Ulco van der Pol gaf een kijkje in de keuken van de Registratiekamer en toonde welke middelen en methoden voor het toezicht en het sanctiebeleid ter beschikking stonden.[5] Eric Schreuders pleitte in zijn artikel o.a. voor een functionele benadering van privacy en de bescherming van het privéleven, waarbij de relatie van het individu met anderen centraal staat.[6] Het eerste katern Berichten van de Registratiekamer bevatte o.a. uitspraken en adviezen van de Registratiekamer over de Albert Heijn Bonus Kaart, direct mail door het ABP, het sofi-nummer op giro-afschriften, de persoonsgebonden Club Card, het personeelsinformatiesysteem bij de politie en het wetsvoorstel rekeningrijden dat de anonimiteit van de weggebruiker bedreigde.

Op de drempel van 2023, heeft de huidige redactie in overleg met de redactieraad besloten om ter gelegenheid van het 25-jarig jubileum een Privacyscriptieprijs uit te reiken. De Stichting Privacy & Registratie organiseerde deze eerder al in 2003, 2005 en 2007. Daarnaast denken we nog na over andere manieren om onze lezers bij ons jubileum te betrekken.

Over de 'Privacyscriptieprijs 2023' zullen wij in een van de volgende nummers van *P&I* meer informatie verstrekken. Dan zullen we bekendmaken onder welke voorwaarden men kan meedingen naar deze prijs. Ook zullen wij een aanmeldingsformulier beschikbaar stellen. Vooralsnog denken we aan masterscripties die zijn beoordeeld met een meer dan gemiddeld cijfer. De prijzen die we in het vooruitzicht willen stellen zijn op dit moment nog niet bekend, maar de drie prijswinnaars zullen in ieder geval worden uitgenodigd om een artikel over hun scriptie in ons tijdschrift te publiceren.

Dus: (ex-)studenten en docenten op het gebied van het privacyrecht, houd de komende afleveringen van *P&I* de informatie over de Privacyscriptieprijs 2023 in de gaten of neem contact op met de redactiesecretaris. Dan maken we er samen een mooi jubileumjaar van.

Sjaak Nouwt (hoofdredacteur P&I)

---

1 De redactieleden van het eerste uur waren: Jan Holvast, Hester de Vries, Eric Schreuders, Ellen Vunderink en ondergetekende.
2 Wie meer wil lezen over de privacyontwikkelingen uit de periode die daaraan voorafging, verwijs ik graag naar het boek van Jan Holvast, *Kroniek van de privacydiscussie. Nederland tot de jaren negentig,* Zutphen: Uitgeverij Paris 2020 (852 p).
3 Jan Holvast, 'Wet bescherming persoonsgegevens: overzicht en stappenplan', *P&I* 1998, afl. 1, p. 4-10.
4 Corien Prins, 'De bescherming van persoonsgegevens: de betrokkene betrokken', *P&I* 1998, afl. 1, p. 11-14.
5 Ulco van der Pol, 'De rol en het sanctiebeleid van de Registratiekamer: nu en straks', *P&I* 1998, afl. 1, p. 15-21.
6 Eric Schreuders, 'Waarden en regels: over privacy en de Wet bescherming persoonsgegevens', *P&I* 1998, afl. 1, p. 22-25.

F. Schuermans[*]

Het Belgische Controleorgaan op de politionele informatie: kennismaking met een gespecialiseerde politionele dataprotectieautoriteit

278

1 Inleiding

De Belgische geïntegreerde politie (GPI[1]) wordt door veel interne en externe instanties gecontroleerd. Denk maar aan de bestuurlijke (burgemeester, Minister van Binnenlandse Zaken en Justitie, …) en gerechtelijke overheden (OM, onderzoeksrechter en onderzoeksgerechten, vonnisrechter) en specifieke interne (Diensten Intern Toezicht en de AIG[2]) of externe controleorganen (Vast Comité van Toezicht op de Politiediensten of Comité P[3]). De meerderheid gaan over het functioneren van de politie in al haar opdrachten (bijstand/hulpverlening, bestuurlijke en/of gerechtelijke politie). Enkel het Controleorgaan op de politionele informatie (Controleorgaan dan wel COC[4]) – onderwerp van deze bijdrage – legt zich uitsluitend toe op de politionele informatiehuishouding. Zijn toezicht is dus bijzonder gespecialiseerd.

Het nieuwe Europese en Belgische privacy- en gegevensbeschermingskader (in hoofdorde de AVG, de LED,[5] de Belgische Wet gegevensbescherming[6] en de Wet op het politieambt[7]) dat in september 2018 werd afgerond betekende een hernieuwd begin voor het, n.a.v. de politiehervorming,[8] opgerichte Controleorgaan. Gestart als orgaan onder gezag van de politieminister (Binnenlandse Zaken en Justitie) werd het in 2014 overgeheveld naar de wetgevende macht als parlementaire onafhankelijke toezichthouder,[9] naar analogie met het Comité P (zelf opgericht in 1991). In 2018 kreeg het dan de belangrijke bevoegdheid van specifieke sectorale dataprotectieautoriteit (DPA) erbij.

2 Organisatie en bevoegdheden

Het COC bestaat uit drie directieleden: een voorzitter/magistraat, een lid-raadsheer/parketmagistraat en een lid-raadsheer/deskundige. Daarnaast beschikt het over een Dienst Onderzoeken van drie leden: twee leden afkomstig van de politie en een deskundige. Tot slot is er een Dienst Steun (secretariaat) bestaande uit twee juristen, een informaticus en een directie-assistent. Het is duidelijk dat het COC met zijn elf personeelsleden een eerder kleine toezichthouder is in verhouding tot het aantal te controleren instellingen en in vergelijking met gelijkaardige Belgische instellingen. Zo heeft het Comité P een kader

---

* Frank Schuermans is lid-raadsheer (lid directiecomité) in het Controleorgaan op de Politionele Informatie, advocaat-generaal bij het Hof van Beroep te Gent en Academisch Consulent Universiteit Gent, faculteit recht en criminologie, Institute for International Research on Criminal Policy (IRCP) & PIXLES, een Interdisciplinair kennis- en onderzoeksplatform van de Universiteit Gent; PIXLES staat voor *Privacy, Information Exchange, Law Enforcement and Surveillance.*

1 Acroniem voor Geïntegreerde Politie/Police Intégrée; de GPI bestaat uit de federale politie en de 185 lokale politiediensten. Het betreft dus uitsluitend de reguliere politie; het COC is *niet* bevoegd voor allerhande inspectiediesnsten (of in Nederland de zgn. bijzondere opsporingsambtenaren of BOA's).

2 Algemene Inspectie van de federale politie en van de lokale politie, aigpol.be.

3 comitep.be.

4 Acroniem voor Controleorgaan/Organe de Controle.

5 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming (AVG) of in het Engels afkorting 'GDPR' wat staat voor General Data Protection Regulation) enerzijds en Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (ook wel, ook in deze bijdrage, aangeduid als Richtlijn politie/justitie of in het Engels LED wat staat voor Law Enforcement Directive).

6 Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (Wet gegevensbescherming of WGB), *BS* 5 september 2018, 68616 (dit is de Belgische materiële privacywet).

7 Wet van 5 augustus 1992 op het politieambt (laatst gewijzigd door de wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten), *BS* 22 december 1992.

8 De toenmalige drie politiekorpsen (Rijkswacht, gemeentepolitie en de Gerechtelijke Politie bij de Parketten) werden in 1998 hervormd tot een geïntregreerde politiedienst op 2 niveaus (het federale en het zonale niveau), bestaande uit de federale politie en de (thans) 185 politiezones.

9 Wet van 18 maart 2014 betreffende het politionele informatiebeheer en tot wijziging van de wet van 5 augustus 1992 op het politieambt, de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en het Wetboek van Strafvordering, *BS* 28 maart 2014, 27465.

van 93 voltijds equivalenten.[10] Het COC is dus gedwongen prioriteiten te stellen. Als DPA specifiek bevoegd voor de controle en toepassing van de LED hoort het Belgische COC niettemin tot de eerder grotere spelers, wanneer de vergelijking wordt gemaakt met de andere EU-landen.[11]

3 Basisopdrachten

3.1 *Hoofdlijnen*

De opdrachten van het COC zijn:

1. Het toezicht op de toepassing van titel 2 Wet gegevensbescherming[12] ten aanzien van de politie,[13] de AIG en de passagiersinformatie-eenheid (BEL-PIU)[14] en omvat alle opdrachten verbonden met de bescherming van de persoonlijke levenssfeer door deze diensten in de uitvoering van *hun operationele opdrachten*.
2. Het toezicht op de toepassing van de AVG en van titel I WGB[15] door de politie en betreft alle opdrachten verbonden met de bescherming van de persoonlijke levenssfeer in de uitvoering van *de niet-operationele opdrachten* (vb. recrutering, selectie, tucht, arbeidsrechtelijke relaties, enz.).[16]
3. De controle van de verwerking van de informatie en de persoonsgegevens in alle politionele gegevensbanken (met ook focus op efficiëntie, effectiviteit en budgettaire aspecten).
4. Elke andere opdracht haar door of krachtens andere wetten verleend. Voorbeelden zijn:

– het zichtbaar en niet-zichtbaar (heimelijk) gebruik van camera's door de politie;
– de controle van de vorderingen van de douane gericht aan de Belgische passagiersinformatie-eenheid (BEL-PIU) in fiscale materies;[17]
– het valideren van de statistieken van de politie die de grondslag zijn voor de nieuwe Belgische Dataretentiewet[18] en de controle van de vorderingen van de Cel Vermiste Personen van de federale politie om verkeers- en locatiegegevens te bekomen van de telecomoperatoren (bijkomende opdracht sedert augustus 2022).

Bij clustering kunnen dus de volgende vier grote activiteitdomeinen worden onderscheiden:

– bevoegdheid/opdracht '*Data Protection Authority*' (DPA) ten aanzien van de politie, de AIG en de BEL-PIU;
– bevoegdheid/opdracht '*Controle en toezicht op de politionele informatiehuishouding en de gemeenschappelijke gegevensbanken terrorisme*'[19] t.a.v. de GPI;
– bevoegdheid/opdracht '*Bijzondere Administratieve Methoden*', meer bepaald alle vormen van politioneel cameragebruik;
– bijzondere controle- en/of valideringsbevoegdheden (*douane en dataretentie*).

In essentie gaat het toezicht van het COC over de volgende de kernelementen:

– effectiviteit, efficiëntie en economie van de politionele informatiehuishouding;
– wettigheid en regelmatigheid van het optreden;
– respect voor de privacy en de gegevensbeschermingsbeginselen.

3.2 *Strategische visie*

Het COC wil in de eerste plaats bijdragen aan een performante, democratisch en rechtstatelijke politionele werking – en informatiehuishouding. Daarbij is het bijbrengen van *awareness* de eerste opdracht en insteek. Pas als *ultimum remedium* is een sanctionering aan de orde via de uitoefening van de 'corrigerende bevoegdheden' en dat als enige politionele toezichthouder (het Comité P heeft deze bv. niet). Het bestaan van dergelijke dwangbevoegdheden is tegelijk een troef en een grote verantwoordelijkheid. Een voorbeeld is het door het COC opgelegde verbod

10 Zie comitep.be.
11 Zie o.a. COM(2022)364 def., 21, Mededeling van de commissie aan het Europees Parlement en de Raad, Eerste verslag over de toepassing en werking van Richtlijn (EU) 2016/680, de richtlijn gegevensbescherming bij rechtshandhaving ('Richtlijn rechtshandhaving'). Ongeveer de helft van de EU DPA voorzien tussen de 1 en 4 VTE voor de toepassing van de LED, 8 DPA voorzien tussen de 7 en 15 VTE.
12 Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (Wet gegevensbescherming of WGB), *BS* 5 september 2018, 68616 (De Belgische materiële privacywet). Titel 2 is de omzetting van de LED (Richtlijn 2016/680).
13 GPI staat voor 'Geintegreerde Politie – Police Intégrée'.
14 Zie de Wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, *BS* 25 januari 2017, 12905.
15 Titel 1 WGB behelst een reeks uitvoeringsbepalingen van de AVG.
16 Het moet gezegd dat de privacycommissie niet voor deze optie gewonnen was en dus zelf bevoegd wilde blijven voor de niet-operationele verwerkingen door de politie: 'De Commissie merkt op dat omwille van deze zware AVG-vereisten alleen al, het absurd is om het C.O.C. bevoegd te verklaren voor gegevensverwerkingen die onder de AVG vallen. Dit type van verwerkingen (het betreft bv. het HR-beheer bij politiediensten) vormt immers maar een fractie van alle verwerkingen bij de politie. De operationele verwerkingen van bv politiediensten vallen allen onder de Richtlijn en voor die verwerkingen is het daarentegen wel enigszins logisch dat het C.O.C. de bevoegde toezichthouder wordt.' (Advies CBPL 33/2018, randnummer 456, gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/advies_33_2018.pdf.) Vooral op vraag van de politie – die begrijpelijkerwijze slechts één dataprotectieautoriteit als gesprekspartners en toezichthouder wilde – en met instemming van het COC werd ervoor geopteerd om het COC bevoegd te maken voor alle verwerkingen van de politiediensten.
17 Art. 281 § 4 van de Algemene wet van 18 juli 1977 inzake douane en accijnzen, zoals ingevoegd door de Wet van 2 mei 2019 tot wijziging van diverse bepalingen betreffende de verwerking van passagiersgegevens, *BS* 24 mei 2019 (inwerkingtreding op 4 juni 2019).
18 Wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, *BS* 8 augustus 2022.
19 In de parlementaire werken bij de Wet Politioneel Informatiebeheer 2014 kunnen we daaromtrent het volgende lezen: 'Overigens, de wezenlijke opdrachten in termen van toezicht op het operationeel politioneel informatiebeheer die oorspronkelijk aan het controleorgaan toegekend waren, blijven ongewijzigd, met name het controleren van een efficiënte, maximale, beveiligde politionele gegevens- en informatieflux op basis van de behoefte om te kennen, alsook het verzekeren van de naleving van de procedures inzake de operationele politionele informatieverwerking', *Parl.St.* Kamer 2013-2014, nr. 3105/001, 63.

aan de federale politie/luchtvaartpolitie Brussels Airport om door te gaan met een systeem van cameratoezicht gecombineerd met gezichtsherkenning.[20]

4 Belangrijkste operationele activiteiten

Het is in het kader van deze bijdrage evident niet mogelijk in detail in te gaan op alle soorten dossiers, laat staan op alle aandachts- en knelpunten, na meer dan vier jaar vernieuwde operationele werking van het COC. Er wordt gefocust op enkele *capita selecta* m.b.t. de politionele informatiehuishouding.

4.1 *Verzoeken onrechtstreekse toegang*

Burgers kunnen in België hun rechten op inzage, rectificatie of wissing als datasubject *uitsluitend* uitoefenen op 'onrechtstreekse wijze', via het COC als toezichthouder. Het COC kan zijn onderzoek ook enkel eindigen met een zeer beperkte (en weinig verhelderende) communicatie aan de verzoeker, met namen, dat 'de nodige verificaties werden verricht'. Dit systeem, de uitzondering binnen de EU, is er vooral onder druk van de politie gekomen die kennelijk liever niet te maken krijgt met verzoeken tot rechtstreekse toegang. Het aantal verzoeken steeg inmiddels van 322 in 2018 naar 546 in 2021. Het aantal rectificaties dat moet worden doorgevoerd spreekt anderzijds tot de verbeelding vermits van de in 2021 behandelde ANG[21] dossiers zo'n 79% aanleiding hebben gegeven tot een gehele of gedeeltelijke archivering, wissing of rectificatie van de politionele registraties. In vergelijking met 2019 en 2020 is dat percentage in 2021 gestegen van respectievelijk 52% over 75,69% tot 79%.[22] Het grote voordeel van dit systeem is anderzijds dat het de toezichthouder een schat aan informatie oplevert over de politionele informatieverwerkingen, waardoor ze soms aanleiding zijn voor grotere proactieve toezichtonderzoeken (cf. verder).

4.2 *Vragen tot informatie en advies*

Daarnaast wordt het COC zowel door burgers als professionelen veelvuldig bevraagd omtrent privacy- en gegevensbeschermingsvraagstukken. Een belangrijk aantal gaat daarbij over de juridische geoorloofdheid van bepaalde gegevensstromen naar, maar vooral vanuit, de politie naar derden. Mag de politie operationele gegevens doorgeven aan gerechtsdeurwaarders, aan curatoren, aan partijen betrokken in een verkeersongeval, aan de brandweer, aan belastingdiensten, enz.? Andere vragen betreffen, bij wijze van voorbeeld, onderwerpen als *data breach*, gegevensbeschermingseffecten beoordeling (DPIA[23]), allerhande toepassingen van cameragebruik (bodycam, drones, …), gebruik van biometrische gegevens (zoals vingerafdrukken), enz. Jaarlijks ontvangt het COC zo'n 70 tot 80 vragen tot advies, in meerderheid afkomstig van de politie. Soms kan een specifieke vraag aanleiding zijn tot een toezichtonderzoek, zoals het geval is geweest bij het verbod om vingerafdrukken te gebruiken in een GDPR-context (voor toegangscontrole van het personeel bv.). Vooral ook cameragebruik leidt tot heel wat vragen. Sedert mei 2018 heeft het COC rond de 100 adviezen geformuleerd rond deze thematiek, meestal ten behoeve van de politie.[24] Nieuwe toepassing of thema's zoals 'slimme' camera's die ageren op bepaalde geluiden om interventieploegen gerichter te kunnen aansturen, vragen betreffende de geluidsopnames van bodycams, de problematiek van verzoeken tot toegang tot camerabeelden door een betrokkene of vragen rond het loggen van de raadpleging van de beelden zijn reeds de revue gepasseerd. Ook het hele ANPR[25] gebeuren is een thema waarop het COC regelmatig wordt aangesproken. Tot slot werden reeds om en bij de 80 DPIA's, voornamelijk inzake cameragebruik, voor advies voorgelegd aan het COC.

De beleidsmatig belangrijkste bevoegdheid blijft de adviesbevoegdheid op alle ontwerpen van federale of deelstatelijke regelgeving die geheel of slechts (zeer) gedeeltelijk raken aan de bevoegdheden van de onder het COC vallende instellingen, waaronder de politie. In 2021 werden 33 dergelijke adviesdossiers behandeld; sedert de start van het COC als DPA in september 2018 tot september 2022 tellen we 109 adviesdossiers. Het leven van beleidsmakers in het algemeen en politiechefs in het bijzonder is er met de komst van het COC als politionele DPA ongetwijfeld een stuk moeilijker op geworden. Zij komen thans te staan tegenover een DPA met kennis van zaken, expertise en ervaring in de materie. Dat heeft alles te maken met zijn samenstelling: (parket)magistraten, privacydeskundigen en politieofficieren stuurt men niet met een kluitje in het riet. In vergelijking met de vroegere privacycommissie (thans Gegevensbeschermingsautoriteit), die allerminst kon bogen op die inhoudelijke en vakgebonden expertise, is het COC derhalve, al naar gelang het sentiment, een te duchten 'tegenstrever' of 'zeer gewaardeerde stakeholder' voor de politie. De belangrijkste adviezen van het Controleorgaan kunnen teruggevonden worden op zijn website (controleorgaan.be), zodat ook het grote publiek en die stakeholders (bestuurlijke en gerechtelijk overheden, politiediensten, de academische wereld, middenveldorganisaties en

20 Tussentijds rapport DIO19005 van 16 september 2019 met corrigerende maatregel betreffende de visitatie bij de federale politie van de luchthaven Zaventem door het Controleorgaan op de politionele informatie met betrekking tot het gebruik van gezichtsherkenning op de nationale luchthaven van Zaventem, controleorgaan.be/publicaties/rapporten; Cf. ook 'Politie moet stoppen met test gezichtsherkenning', *De Standaard* 21 september 2019; 'Geen gezichtsherkenning meer op Zaventem', *Gazet van Antwerpen* 21 september 2019; 'La reconnaissance faciale toujours dans le flou', *Le Vif Express* 3 oktober 2019.

21 Dit is de Algemene Nationale Gegevensbank, met name de enige unieke nationale databank van en voor de GPI die door alle politiediensten moet gevoed worden en in beginsel uitsluitend 'gevalideerde' informatie bevat.

22 controleorgaan.be/Publicaties/Jaarverslagen.

23 Data Protection Impact Assesment.

24 Toestand op 15 december 2019.

25 Automatic Number Plate Recognition.

NGO's, enz.) zich kunnen vergewissen van de inhoud en kwaliteit ervan.

4.3 *Klachten en aangiften*

Het betreft dossiers ten laste van de politie of politieambtenaren waarbij effectief een klacht wordt neergelegd wegens een vermeende inbreuk op de privacy- of gegevensbeschermingsregels. In de praktijk gaat het veelal om burgers of collega's die vermoeden dat een politieambtenaar ten onrechte zijn of haar gegevens in de politionele databanken of de databanken die via het politieportaal PORTAL ter beschikking staan[26] van de politie heeft geraadpleegd. Van september 2018 tot 2022 werden 115 klachten ingediend. Het COC doet hier evenwel in meerderheid enkel een *prima facie*-onderzoek of zelfs enkel een onderzoek naar de identificatie van een mogelijke 'dader'. Bij concrete aanwijzingen van abusievelijke consultaties en bij een territoriaal aanknopingspunt wordt het dossier overgemaakt aan de korpschef (intern toezicht) en/of het bevoegde openbaar ministerie. Het gaat immers steeds ook om misdrijven. Daarnaast kan het COC ook klachten ontvangen die meer algemeen een onrechtmatige verwerking willen aanklagen door een politieambtenaar of politieorganisatie (vb. klacht door een politieambtenaar tegen de politieleiding wegens een onderzoek naar vermeend overmatig wifi-gebruik voor persoonlijke doeleinden op het werk).

4.4 *De toezichtonderzoeken*

Deze opdracht behoort sedert zijn ontstaan tot de *core-business* van het COC. Het aantal ambtshalve controleonderzoeken door het COC, toen het nog deel uitmaakte van de uitvoerende macht, was marginaal. Bij de overgang naar het parlement in 2014-2015 was het van meet af aan de bedoeling de controleonderzoeken op de politie prioritair te maken. Dat is maar gedeeltelijk gelukt, maar toch heeft het COC op twee jaar tijd enkele belangrijke ambtshalve controleonderzoeken uitgevoerd. In die 'predataprotectieperiode' lag de focus evenwel vooral op de aspecten legaliteit, efficiëntie en effectiviteit van de informatiehuishouding. Sedertdien is daar de zeer belangrijke en zelfs dominante privacy- en gegevensbeschermingscomponent bijgekomen.

Het COC onderscheidt de volgende toezichtonderzoeken:
- een **globaal toezicht** dat gepaard gaat met één of meerdere doorgedreven plaatsbezoeken en met een zeer ruime *scope* (de volledige informatiehuishouding van een politiedienst wordt bekeken);
- een **technisch toezicht** dat zich focust op de wettigheid, volledigheid en correctheid van de vattingen/verwerkingen in de politionele gegevensbanken en waarbij vooral de operationele efficiënte en correcte vattingen in de databanken aan de orde zijn;
- een **thematisch toezicht** waarbij onderzoek wordt gedaan naar één bepaald thema en zowel *deskresearch* als bezoeken ter plaatse mogelijk zijn (vb. gebruik van de bodycam);
- een **beperkt toezicht** behandelt één of slechts enkele (deel)aspecten van een politionele of niet-politionele gegevensverwerking (vb. een onderzoek naar onrechtmatig cameratoezicht op het vertrouwelijk 'Salduz' overleg tussen advocaat en verdachte);
- een **internationaal Toezicht** zijn de internationale onderzoeken waaraan het COC zijn medewerking verleent (vb. de SCHEVAL-evaluaties);
- een **bijzonder toezicht** in specifieke materies, zoals de jaarlijkse controles op de gemeenschappelijke gegevensbanken terrorisme en extremisme of de *BELPIU* onderzoeken.

Bij een globaal toezicht van een politie-entiteit worden bv. de volgende thema's onderzocht:
- nazicht van algemene aspecten van gegevensbescherming (heeft men überhaupt een beleid, is er een DPO en welke initiatieven neemt die, heeft men een register van de verwerkingen, enz.);
- de ANG (vooral kwaliteit van de voeding[27] en bewaartermijnen);
- toepassing van zichtbaar en heimelijk cameragebruik;
- bijzondere gegevensbanken: inhoud, beveiliging, koppelingen, enz.;
- gebruik van persoonlijke IT-apparatuur voor operationele doeleinden;
- verwerking van biometrische gegevens voor operationele en niet-operationele doeleinden;
- ICT en informatieveiligheid: beleid, architectuur, beveiliging, incidentenmanagement, logging,[28] enz.;
- enz.

Een fundamenteel onderscheid met de 'pre-DPA'-periode zijn de corrigerende maatregelen die het COC kan nemen en ook neemt ten aanzien van de politie. Het COC kan dus alle voorziene administratieve sancties/corrigerende maatregelen opleggen aan de GPI, behoudens de administratieve geldboete. De WGB heeft in artikel 222 § 2 immers voorzien dat 'het artikel 83 van de Verordening (de administratieve geldboetes dus) niet van toepassing (is) op de overheid en hun aangestelden of gemachtigden'. De ruimte ontbreekt om hier dieper op in te gaan, maar het moet benadrukt dat de meeste inbreuken op de GDPR en/of WGB ook een penaal misdrijf uitmaken dat bestraft wordt met strafrechtelijke geldboetes. Het

26 Het gaat dan om het Rijksregister (RRN), het repertorium der voertuigen (DIV) en het wapenregister.

27 Zoals bv. de vraag naar de systematische verplichte toepassing (bv. bij elke gerechtelijke arrestatie) door de politie van de zgn. 'drieledige tryptiek' (met name afnemen van vingerafdrukken, opstellen van een individuele beschrijving en het nemen van foto's). In de praktijk blijkt deze verplichting in belangrijke mate (vaak in meer dan 1 op de 3 gevallen) niet te worden nageleefd met alle nefaste operationele gevolgen vandien.

28 Hier kan verwezen worden naar de verplichting om een reden van raadpleging in te geven bij consultaties of verwerkingen in politionele databanken; ook hier zien we een zeer groot percentage raadplegingen door de leden van de politie waar geen dan wel volstrekt onbegrijpelijke motieven van raadpleging worden ingegeven (vaak tot boven de 90% van de raadplegingen).

niet respecteren van een door het COC opgelegde corrigerende maatregel (zoals een tijdelijke of definitieve verwerkingsbeperking of een verwerkingsverbod bijvoorbeeld) is evenzeer een misdrijf (art. 222 § 1, 1e lid juncto art. 222, 5° WGB).

Corrigerende maatregelen worden opgelegd in quasi alle toezichtonderzoeken (een 5 à 6 per jaar). Zo werden er bv. opgelegd in het kader van de onderzoeken/visitaties bij de politiezone Oostende (cameragebruik op het strand) en 'Federale Politie/luchtvaarpolitie te Brussel-Nationaal (cameragebruik met gezichtsherkenning). Deze bestonden respectievelijk in het opleggen van bepaalde publieke bekendmakingsverplichtingen van cameratoezicht op het strand en het bevel de verwerking stop te zetten. Het is voor het COC hoe dan ook telkens een belangrijke en delicate afweging. Het COC wenst de operationele werking van de politie zo min mogelijk te bemoeilijken, maar stelt wel vast dat zij haar dwingende bevoegdheden meer en meer moet hanteren en ook effectief hanteert.

Het COC voert om diezelfde reden van operationele werking ook een zeker 'gedoogbeleid' gedurende een bepaalde termijn. Een voorbeeld hiervan is de (niet-)toepassing van het Belgische systeem van (eerst) archiveren en (vervolgens) wissen van de persoonsgegevens en dus het respect voor de bewaartermijnen in alle politionele gegevensbanken. De vaststelling moet gemaakt worden dat politie reeds sedert april 2017 op dit punt niet meer conform aan de wettelijke regels handelt en een essentieel aspect van de politionele gegevensverwerking zich in de illegaliteit bevindt. De eerste correspondentie van het COC met de federale politie dateert van maart 2017 vermits het een thematisch onderzoek naar deze problematiek had geopend. Dit betekent m.a.w. dat het COC reeds meer dan vijf jaar een gedoogbeleid ter zake hanteert, zij het dat sedert april 2022 eerste aanzetten zijn gegeven tot een systeem van geautomatiseerde archivering. In de dagelijkse praktijk stelt het COC vooral bij de verzoeken tot onrechtstreekse toegang en bij klachten vast dat heel wat registraties (zowel processen-verbaal als informatierapporten) ten onrechte niet werden/worden gearchiveerd of gewist. De gevolgen hiervan zijn voor de burger in vele gevallen direct aanwijsbaar: geen toegang tot een bepaald beroep, tot een bepaalde plaats, negatief veiligheidsadvies, geen veiligheidsmachtiging (en dus niet de geambieerde job), ten onrechte (herhaaldelijke) fouilleringen of controles (al dan niet aan de grens), enz.

Een belangrijk aspect in deze toezichtonderzoeken is de controle op de cameraverwerkingen. Zo moeten niet-zichtbare (heimelijke) cameraverwerkingen voor doeleinden van bestuurlijke politie aan het COC genotificeerd worden, waarna het zo nodig al zijn controle- en dwangbevoegdheden kan uitoefenen. Daarnaast heeft het COC een algemene controleopdracht op elke vorm van cameragebruik: zichtbaar, niet-zichtbaar, op een niet besloten plaats, op een besloten plaats toegankelijk voor het publiek, op een besloten plaats niet toegankelijk voor het publiek, ANPR, met of zonder intelligente camera's, enz.

4.5 *Beleidsmatige activiteiten*

Uiteraard wordt het COC of zijn (personeels)leden regelmatig gevraagd voor meer beleidsmatige activiteiten. Het gaat dan om informeel of formeel overleg met de politieministers, hun kabinetten of administraties omtrent voorgenomen initiatieven, overleg met politie omtrent initiatieven die zij wensen te nemen, opleidingen of studiedagen waaraan het COC zijn deelneming toezegt, beleids- en operationele afspraken met andere dataprotectieautoriteiten of toezichthouders, overleg met DPO's van de politie, enz.

4.6 *Toekomstperspectieven*

'De politie legt verantwoording af over de manier waarop zij de voor haar beschikbare gegevens verwerkt. Zij heeft daarbij bijzondere aandacht voor de bescherming van de persoonlijke levenssfeer van de personen wiens gegevens deel uitmaken van de politionele informatie. Het daartoe bevoegde Controleorgaan op de Politionele Informatie (hierna benoemd "Controleorgaan") controleert de conforme uitvoering ervan. Een democratische controle op de werking van politie is noodzakelijk en aanvullend op het vertrouwen dat de politie geniet om op een democratische, wettelijke en correcte wijze om te gaan met de ingewonnen en verwerkte informatie', zo kan worden gelezen in een recent beleidsdocument van een subwerkgroep van het zgn. Coördinatiecomité GPI (intern politioneel beleidsorgaan samengesteld uit het directiecomité van de federale politie en de voorzitters van de Vaste Commissie van de Lokale politie).

Een eerste vaststelling is dat het COC, met zijn doorstart in september 2018, een volledig nieuw begin gemaakt heeft en er als kleine organisatie in geslaagd is op korte tijd zich als toezichthouder stevig te settelen in het dataprotectie- en politielandschap. Opvallend is ook dat het luik dataprotectie actueel rond de 60 à 70% van haar activiteiten omvat zodat het COC thans vooral een DPA is, hoewel het meer is, moet zijn en zal proberen te zijn in de toekomst.

Een tweede vaststelling is dat het COC bij de andere toezichtsorganen en de overheden een vrij groot vertrouwen geniet. Dat bewijst bijvoorbeeld het feit dat het Comité P zich in grote mate onthoudt van het behandelen van thema's die te maken hebben met de politionele in-

formatiehuishouding en haar vraag om alle onderzoeken betreffende onrechtmatige dataconsultaties of verwerkingen door leden van de GPI over te nemen. Dat bewijst ook de steeds nieuwe en bijkomende opdrachten en bevoegdheden die het COC er op een viertal jaar heeft bijgekregen, alsmede de politieke wil om de dwangbevoegdheden van het COC in de toekomst nog te versterken (bv. met het de mogelijkheid te geven een bestuurlijke dwangsom op te leggen[29]).

Een derde vaststelling is dat het COC niet aarzelt om zijn corrigerende bevoegdheden – en dus dwangbevoegdheden – uit te oefenen en op die manier probeert te verhelpen aan het klassieke grote gebrek in de materie van het privacy- en gegevensbeschermingsrecht, met name een tekort aan reële handhaving. Het COC tracht daaraan te verhelpen en waar nodig op proportionele wijze zijn dwangbevoegdheden uit te oefenen (uitgezonderd de administratieve geldboete die wettelijk niet mogelijk is). Proportioneel, omdat het COC evident de politiewerking niet onmogelijk wil maken door blind met zware corrigerende maatregelen uit te pakken. Het is op dat vlak vaak een moeilijke en delicate evenwichtsoefening.

5 Besluit

Specifiek aan de Belgische situatie en zeldzaam binnen de EU is de creatie van een politiespecifieke dataprotectieautoriteit. De ervaringen ermee zijn, zeker vanuit het perspectief van de burger en overheden, zondermeer positief. De controle op, en dus ook de naleving, door de GPI van de (grond)regels inzake politionele informatiehuishouding in het algemeen en privacy en gegevensbescherming in het bijzonder hebben een kwantumsprong gemaakt sedert 2018. Uit onderzoek blijkt vaak dat, daar waar de reguliere dataprotectieautoriteit, er ook de politie (of andere handhavers) moet 'bijnemen', daarvoor in de regel amper tijd en geld wordt voor uitgetrokken.[30] Ook in België zagen we dat bij de oude privacycommissie (vóór 2018) en zien we actueel opnieuw dat het toezicht op andere handhavingsdiensten dan de politie, waarvoor niet het COC, maar de Gegevensbeschermingsautoriteit[31] bevoegd is, marginaal blijft en de focus dominant op de private sector ligt.

Of de politie eveneens onverdeeld gelukkig is met het Controleorgaan, sedert zijn vervelling naar ook een dataprotectieautoriteit, is moeilijk te zeggen. Het COC doet nu eenmaal voor de politie bij wijlen pijnlijke vaststellingen in zijn onderzoeken, zoals nog zeer recent in een West-Vlaamse politiezone – op vraag overigens van de procureur des Konings[32] aldaar – waar meerdere majeure pijnpunten werden blootgelegd zoals (1) het zo goed als nooit opgeven van een reden raadpleging (waardoor achteraf amper de rechtmatigheid van de consulatie of gegevensverwerking kan gecontroleerd worden), (2) collega's die elkaars burgerlijk en politioneel verleden geregeld opzoeken in de politionele databanken of zelf kennisnemen van politionele registraties hen betreffend als verdachte, of (3) het in grote mate in gebreke blijven bij de uitvoering van de zgn. 'tryptiek' (afname van vingerafdrukken, nemen van foto's en opmaak van individuele beschrijving van gearresteerden, met verplichte voeding naar de ANG).[33]

Zoals vaak zien we een variatie in leiders en leiderschapskwaliteiten bij de politie. Korpschefs die erin slagen het defensieve harnas af te leggen zien de onderzoeken en vaststellingen van het COC als een opportuniteit en (dikwijls) hefboom om interne weerstanden te overwinnen. Vaak zijn de ervaringen van het COC echter positief en maakt het betrokken politiekorps een ware omslag in zijn informatiehuishouding (waaronder bv. het informatieveiligheidsbeleid). Bovendien blijft de eerste insteek van het COC er één van bijstand, raadgeving en advies, waar men er niet omheen kan dat de politie overal te lande (soms te) vaak en gemakkelijk de weg naar het COC vindt. Geregeld zien we dat, omdat men er intern bij de politie, 'niet uit' geraakt, zowel politie als politieoverheden het COC als scheidsrechter zien. Het betekent alleszins dat het COC op slechts enkele jaren tijd het referentieorgaan is geworden in de brede materie van de politionele informatiehuishouding waaronder dominant privacy- en gegevensbescherming. Meer en meer besteedt het COC echter ook capaciteit aan efficiëntie en effectiviteit van de politiewerking door middel van adviezen en naar aanleiding van punctuele dossiers onrechtstreekse toegang (voorbeelden zijn de correcte werking en toepassing van het ANPR-camerageboeuren, de noodzaak aan meer geïntegreerde samenwerking tussen lokale en federale politie of tussen politiezones onderling, enz.). Ook dat wordt absoluut naar waarde geschat.

---

29 Op grond van een door de Wet gegevensbescherming voorgeschreven evaluatie is gebleken dat de bevoegdheden van het COC nog wat kunnen verfijnd worden; op dit ogenblik (september 2022) zijn er dan ook werkzaamheden bezig op beleids- en regeringsniveau om een reparatiewetgeving op te stellen waarin één en ander bijkomende voor het COC zou worden voorzien.

30 De verwerking van politiegegevens in vijf Europese landen, Verkennend Onderzoek, Groningen, 20 november 2020, Pro Facto, pro-facto.nl en pro-facto.nl/meer-actueel/832-internationale-input-voor-herziening-wet-politiegegevens. Aan deze door het Nederlandse WODC (Wetenschappelijk Onderzoek en Documentatiecentrum) bestelde studie nam het COC namens België deel. De vijf landen waarvan sprake is waren België, Denemarken, Duitsland (Noordrijn-Westfalen), Finland en Ierland (zie voor het rapport: repository.wodc.nl/bitstream/handle/20.500.12832/3025/3031-de-verwerking-van-politiegegevens-in-vijf-Europese-landen-volledige-tekst.pdf?sequence=7&isAllowed=y).

31 gegevensbeschermingsautoriteit.be.

32 De evenknie van de hoofdofficier van Justitie in Nederland.

33 Rapport CON21006 van 4 juli 2022, raadpleegbaar op controleorgaan.be (rubriek publicaties/rapporten).

*Mr. D.S. de Boer**

Brein/Ziggo-uitspraken: de invloed van het verbod op verwerking van strafrechtelijke persoonsgegevens op de medewerkingsplicht van Ziggo

279

1 Inleiding

Op 2 februari 2022 heeft de rechtbank Midden-Nederland vonnis gewezen in de zaak Stichting Brein tegen Ziggo B.V. (*Brein/Ziggo I*).[1] In deze zaak vordert Brein medewerking van Ziggo bij het doorsturen van waarschuwingsbrieven naar personen die vermeend inbreuk maken op intellectuele eigendomsrechten van derden (inbreukmakers). De rechtbank oordeelt dat Ziggo geen medewerking hoeft te verlenen. Kortgezegd constateert de rechtbank dat Ziggo bij het doorsturen strafrechtelijke persoonsgegevens van inbreukmakers verwerkt en dat op deze verwerking een verwerkingsverbod rust. Als gevolg van het verwerkingsverbod mag Ziggo geen medewerking verlenen bij het doorsturen van de waarschuwingsbrieven. In een nieuwe procedure tussen Brein en Ziggo wordt dit oordeel op 9 juni 2022 wederom door de rechtbank Midden-Nederland bevestigd (*Brein/Ziggo II*).[2] Vervolgens heeft het hof Arnhem-Leeuwarden op 11 oktober 2022 uitspraak gedaan in het hoger beroep op *Brein/Ziggo I* (*Brein/Ziggo III*).[3] Ook hier oordeelt het hof dat Ziggo (vooralsnog) geen strafrechtelijke persoonsgegevens mag verwerken. Vanwege de omstandigheid dat de uitspraak van het hof daags voor afronding van dit artikel is gepubliceerd, komt de uitspraak slechts zijdelings aan bod. Voor het vervolg duid ik de *Brein/Ziggo I-* en *II*-uitspraken gezamenlijk aan als de '*Brein/Ziggo*-zaken'.

In deze uitspraken wordt het verwerkingsverbod op strafrechtelijke persoonsgegevens voor het eerst als factor meegewogen bij de beoordeling of Ziggo medewerking moet verlenen aan Brein. Dit terwijl Brein in het verleden meermalen de medewerking van Ziggo heeft gevorderd. De medewerking bestond in die gevallen uit het verstrekken van NAW-gegevens van inbreukmakers aan Brein. Opvallend genoeg heeft het verwerkingsverbod in het verleden geen rol gespeeld bij het verstrekken van NAW-gegevens. In de uitspraken staan tal van interessante thema's, waaronder auteursrechthandhaving, rechten van betrokkenen en strafrechtelijke aspecten.

In dit artikel beperk ik mij tot de beoordeling van de invloed van het verwerkingsverbod op de medewerkingsplicht van Ziggo. Hierbij maak ik een onderscheid tussen de medewerkingsplicht die bestaat uit het verstrekken van NAW-gegevens en het doorsturen van waarschuwingsbrieven. Ten behoeve van de leesbaarheid kort ik deze verplichtingen af tot 'NAW-gegevens' en 'waarschuwingsbrieven'. De opbouw van mijn artikel ziet er als volgt uit. In paragraaf 2 geef ik een korte beschrijving van NAW-gegevens en waarschuwingsbrieven en geef ik aan op welke punten de medewerkingsverplichtingen van elkaar verschillen. Vervolgens bespreek ik in paragraaf 3 het wettelijk kader dat van toepassing is op NAW-gegevens en op waarschuwingsbrieven. Hierbij ligt de focus op de verwerking van strafrechtelijke persoonsgegevens. In paragraaf 4 en 5 beoordeel ik op welke wijze het wettelijk kader in de praktijk wordt toegepast op de medewerkingsverplichting. Hierbij maak ik een onderscheid tussen de situatie voor en na de toepassing van het verwerkingsverbod. Verder bespreek ik in paragraaf 6 wat de gevolgen zijn van het verwerkingsverbod voor de medewerkingsplicht van Ziggo bij het verstrekken van NAW-gegevens of het sturen van waarschuwingsbrieven. Tot slot sluit ik af met mijn conclusie in paragraaf 7.

2 Medewerkingsplicht: NAW-gegevens en waarschuwingsbrieven

2.1 *NAW-gegevens*

Brein houdt zich bezig met de bestrijding van inbreuken op intellectuele eigendomsrechten (IE-rechten). Als onderdeel van de werkzaamheden treft Brein handhavingsmaatregelen tegen inbreukmakers. De handhavingsmaatregelen hebben tot doel dat IE-inbreuken worden beëindigd. Tot op heden spreekt Brein vooral de grote inbreukmakers aan (en treft vervolgens vaak schikkingen).

Indien Brein niet beschikt over de persoonsgegevens van een inbreukmaker, heeft Brein geen mogelijkheid om tegen de inbreukmaker op te treden. Om toch handhavend te kunnen optreden is Brein genoodzaakt om de NAW-gegevens op te vragen bij tussenpersonen, zoals

* Dafne de Boer is advocaat bij Dirkzwager te Arnhem.

1 Rb. Midden-Nederland 2 februari 2022, ECLI:NL:RBMNE:2022:297, *JBP* 2022/82, m.nt. D.S. de Boer.
2 Rb. Midden-Nederland 9 juni 2022, ECLI:NL:RBMNE:2022:2198.
3 Hof Arnhem-Leeuwarden 11 oktober 2022, ECLI:NL:GHARL:2022:8676.

een internetaanbieder of websitehouder. Ziggo is zo'n tussenpersoon waar Brein weleens NAW-gegevens van inbreukmakers opvraagt. Brein verwacht bij een dergelijk verzoek dat Ziggo de NAW-gegevens van de inbreukmaker aan Brein verstrekt. Het doel van het verkrijgen van de NAW-gegevens is het kunnen treffen van maatregelen tegen de inbreukmaker.

2.2 *Waarschuwingsbrieven*

In aanvulling op de bestaande handhavingsmaatregelen is Brein in december 2020 de FLU-waarschuwingscampagne gestart. In het kader van de campagne maakt Brein gebruik van speciale software. Met deze software kunnen IP-adressen gedetecteerd worden waarmee illegaal aanbod ter beschikking wordt gesteld. De houders van de gedetecteerde IP-adressen worden door Brein als inbreukmakers aangemerkt. Brein wil vervolgens aan de inbreukmakers een waarschuwingsbrief sturen.

De procedure voor het versturen van de waarschuwingsbrieven bestaat uit de volgende stappen. Brein deelt de IP-adressen van inbreukmakers met Ziggo. Brein verzoekt Ziggo de IP-adressen aan de houders van de IP-adressen, oftewel de inbreukmakers, te koppelen. Vervolgens verwacht Brein dat Ziggo de waarschuwingsbrief doorstuurt aan de inbreukmakers. Het daadwerkelijk versturen van de brief verschuift hiermee naar Ziggo. In deze situatie heeft Brein dus geen belang meer bij het ontvangen van NAW-gegevens. Met het uitvoeren van deze procedure wordt ten opzichte van de oude handhavingsmaatregelen de rol van Brein kleiner en de rol van Ziggo groter.

In de waarschuwingsbrief wordt vermeld dat de inbreukmaker geen illegale content meer ter beschikking mag stellen. Ook wordt vermeld dat Brein bij nieuwe overtredingen zwaardere handhavingsmaatregelen zal treffen. Waar Brein tot op heden vooral reactief achter de grote vissen aangaat, gaat Brein nu proactief netwerken scannen en een breder publiek waarschuwen. Op deze wijze beperkt Brein zich tot waarschuwingen en blijft het weg van de 'normale' handhavingsmiddelen.

2.3 *Tussenconclusie*

De medewerking die bestaat uit het verstrekken van NAW-gegevens of het doorsturen van waarschuwingsbrieven komt grotendeels overeen. Bij NAW-gegevens en waarschuwingsbrieven begint de gegevensverwerking hetzelfde. Brein verstuurt IP-adressen naar Ziggo. Ziggo koppelt de IP-adressen aan inbreukmakers. Het verschil in de verwerking, en daarmee de medewerking, ontstaat in de volgende stap. Bij NAW-gegevens verstrekt Ziggo aan Brein NAW-gegevens. Bij waarschuwingsbrieven verstuurt Ziggo waarschuwingsbrieven naar inbreukmakers. In het tweede geval ontvangt Brein van Ziggo geen gegevens over inbreukmakers. Hierdoor is er voor Brein sprake van een minder vergaande verwerking dan wanneer Brein NAW-gegevens ontvangt.

3 Medewerkingsplicht: wettelijk kader

3.1 *Persoonsgegevens*

Bij het verlenen van medewerking verwerkt Ziggo NAW-gegevens en IP-adressen van inbreukmakers. NAW-gegevens bestaan uit gegevens over de naam, het adres en de woonplaats van een persoon. Deze gegevens kwalificeren als persoonsgegevens. Daarnaast is het de vraag of IP-adressen als persoonsgegevens kwalificeren. Uit het *Breyer*-arrest van het Europese Hof van Justitie (HvJ EU) volgt dat IP-adressen als persoonsgegevens kunnen kwalificeren.[4] De kwalificatie hangt af van de beoordeling of de partij die de gegevens verwerkt redelijkerwijs beschikt over de middelen die ingezet kunnen worden om een persoon aan de hand van die gegevens te identificeren. Hierbij wordt aangenomen dat wanneer bij de identificatie excessieve inspanningen worden gevergd, de gegevens niet kwalificeren als persoonsgegevens. Bij excessieve inspanningen kan worden gedacht aan situaties waarin het, gelet op de vereiste tijd, kosten en mankracht, ondoenlijk is om een persoon te identificeren of wanneer identificatie bij wet verboden is.[5] Er kan dus niet op voorhand worden vastgesteld dat een IP-adres als persoonsgegeven kwalificeert. Dit moet beoordeeld worden op basis van de middelen waarover een partij beschikt.

3.2 *Grondslag*

Ziggo heeft voor de verwerking van persoonsgegevens een grondslag nodig. In de Algemene Verordening Gegevensbescherming (AVG) is een limitatieve opsomming van zes grondslagen opgenomen.[6] Zonder de afzonderlijke grondslagen uitvoerig te bespreken, kan ik vaststellen dat Ziggo alleen in aanmerking komt voor de grondslagen 'toestemming'[7] en 'gerechtvaardigd belang'.[8] Toestemming is echter geen bruikbare grondslag. Een verwerking op basis van toestemming zou betekenen dat Ziggo aan de inbreukmaker expliciete toestemming moet vragen om de persoonsgegevens voor handhavingsdoeleinden van Brein te verwerken. Ik schat in dat de kans zeer klein is dat inbreukmakers vrijwillig meewerken en toestemming geven. Dat heeft tot gevolg dat de grondslag 'gerechtvaardigd belang' overblijft.

Op deze grondslag kan Ziggo een beroep doen indien de verwerking van persoonsgegevens noodzakelijk is voor de behartiging van het gerechtvaardigd belang van Ziggo of een derde, tenzij de belangen of rechten of vrijheden

4 HvJ EU 19 oktober 2016, ECLI:EU:C:2016:779 (*Breyer*).
5 HvJ EU 19 oktober 2016, ECLI:EU:C:2016:779, par. 46 (*Breyer*).
6 Art. 6 lid 1 AVG.
7 Art. 6 lid 1 onder a AVG.
8 Art. 6 lid 1 onder f AVG.

van de inbreukmaker zwaarder wegen. Hieruit kunnen drie voorwaarden worden afgeleid. De gegevensverwerking moet i) rechtmatig en ii) noodzakelijk zijn en iii) de belangen van de inbreukmaker mogen niet zwaarder wegen dan het belang van Brein of Ziggo bij de verwerking.

Bij de afgifte van NAW-gegevens wordt de grondslag gerechtvaardigd belang in veel gevallen gekoppeld aan de zorgplicht van de tussenpersoon. Met de zorgplicht wordt gedoeld op de plicht van de tussenpersoon om onwettige activiteiten, zoals IE-inbreuken, van klanten op te sporen en te voorkomen.[9] In het *Lycos/Pessers*-arrest[10] zijn criteria opgenomen voor de beoordeling van de zorgplicht. Wanneer aan de criteria wordt voldaan, kan de tussenpersoon onrechtmatig handelen door NAW-gegevens niet aan een belanghebbende te verstrekken. In het *Lycos/Pessers*-arrest zijn de volgende vier criteria neergelegd: a. de mogelijkheid dat de informatie, op zichzelf beschouwd, jegens de derde onrechtmatig en schadelijk is, is voldoende aannemelijk; b. de derde heeft een reëel belang bij de verkrijging van de NAW-gegevens; c. het is aannemelijk dat er in het concrete geval geen minder ingrijpende mogelijkheid bestaat om de NAW-gegevens te achterhalen; d. afweging van de betrokken belangen van de derde, de serviceprovider en de websitehouder (voor zover kenbaar) brengt mee dat het belang van de derde behoort te prevaleren. Het gevolg van het voldoen aan de *Lycos/Pessers*-criteria is dat er mede wordt voldaan aan de grondslag gerechtvaardigd belang.[11]

3.3 *Strafrechtelijke persoonsgegevens*

Vervolgens is het de vraag of de persoonsgegevens als strafrechtelijke persoonsgegevens kwalificeren. Strafrechtelijke persoonsgegevens zijn gegevens over 'strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen'.[12] In de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) is hieraan toegevoegd dat ook persoonsgegevens 'betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag' als zodanig aangemerkt moeten worden.[13]

Het schenden van IE-rechten kan als een strafbaar feit worden aangemerkt. In artikel 31 tot en met 33 Auteurswet zijn bijvoorbeeld bepalingen opgenomen over feiten waarbij sprake is van een schending van auteursrechten. Op grond van artikel 33 Auteurswet worden de betreffende feiten aangemerkt als misdrijf. Dat betekent dat een schending van auteursrechten als een strafbaar feit heeft te gelden. Deze vaststelling heeft tot gevolg dat gegevens over strafbare feiten in combinatie met gegevens over de persoon die de strafbare feiten pleegt, als strafrechtelijke persoonsgegevens aangemerkt moeten worden. Ik merk hierbij op dat het in de praktijk weinig tot niet voorkomt dat op basis van het strafrecht wordt opgetreden tegen IE-inbreuken. In de regel wordt dit op basis van het civiele recht gedaan.

Dat een schending van auteursrechten als een strafbaar feit aangemerkt moet worden, wordt ook door de Autoriteit Persoonsgegevens (AP) bevestigd. De AP deed dat in een besluit inzake de handhaving van intellectuele eigendomsrechten door Dutch FilmWorks B.V. (Besluit DFW).[14] In het kort speelde hier het volgende. Het Besluit DFW heeft betrekking op een voorgenomen verwerking van Dutch Film Works (DFW). DFW heeft aangegeven onderzoek te willen doen naar de betrokkenheid van bittorent-gebruikers bij handelingen die vermoedelijk inbreuk maken op de auteursrechten van DFW. Wanneer blijkt dat bittorrent-gebruikers inbreuk maken, wil DFW handhavend optreden.[15] In het Besluit DFW wordt het volgende vermeld: 'De AP stelt vast dat het verwerken van persoonsgegevens van personen waartegen een min of meer gegronde verdenking bestaat van handelingen die inbreuk maken op auteursrecht, aangemerkt moeten worden als strafrechtelijke persoonsgegevens'.[16] Gelet op het voorgaande constateer ik dat gegevens over inbreukmakers als strafrechtelijke persoonsgegevens kwalificeren.

3.4 *Verwerkingsverbod*

Op de verwerking van strafrechtelijke persoonsgegevens rust een verwerkingsverbod.[17] De gegevens mogen slechts verwerkt worden onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen bieden.[18] Voor Ziggo komt dit neer op een verwerkingsverbod van strafrechtelijke persoonsgegevens dat enkel bij wettelijke uitzondering opgeheven kan worden. De wettelijke uitzonderingen zijn in artikel 31, 32 en 33 UAVG neergelegd.[19] Dit betekent dat Ziggo bij de verwerking van strafrechtelijke persoonsgegevens naast een

9 Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt, *PbEG* 2000, L 178, overweging 48.
10 HR 25 november 2005, ECLI:NL:HR:2005:AU4019, *NJ* 2009/550, m.nt. P.B. Hugenholtz.
11 Strikt genomen volgt uit *Lycos/Pessers* dat wanneer aan de vier criteria wordt voldaan, art. 6 lid 1 onder f AVG zich niet verzet tegen de afgifte van NAW-gegevens.
12 Art. 10 AVG.
13 Art. 1 UAVG.
14 Autoriteit Persoonsgegevens, 'Definitief besluit inzake de verklaring omtrent de rechtmatigheid van online handhaving van intellectuele eigendomsrechten door Dutch FilmWorks B.V;z2017-02053', 5 december 2017.
15 Besluit DFM, p. 6-7.
16 Besluit DFW, p. 4.
17 Art. 10 AVG.
18 Art. 10 AVG.
19 De wettelijke uitzonderingen zijn in art. 31-33 UAVG neergelegd.

grondslag (gerechtvaardigd belang) ook een uitzonderingsgrond nodig heeft.

Ik beperk mij tot de bespreking van de meest relevante uitzonderingsgronden voor Ziggo. Dit zijn de volgende uitzonderingen: strafrechtelijke persoonsgegevens mogen verwerkt worden, indien i) de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering, of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid[20] en/of ii) de AP voor de verwerking een vergunning heeft verleend.[21] Voor het vervolg kort ik deze uitzonderingsgronden af tot 'uitzondering rechtsvordering' en uitzondering 'vergunning'.

In het kader van NAW-gegevens en waarschuwingsbrieven heeft de AP zich in het Besluit DFW uitgesproken over het verwerkingsverbod (zie ook par. 3.3). De AP stelt dat het verwerkingsverbod van toepassing is op de verwerking van strafrechtelijke persoonsgegevens door DFW. De AP stelt vervolgens ook dat DFW een beroep kan doen op de uitzondering rechtsvordering en de uitzondering belangenbescherming.[22] De AP spreekt zich niet uit over de bevoegdheden van eventuele derde partijen (zoals Ziggo) die bij de verwerking van strafrechtelijke persoonsgegevens worden betrokken. Op basis van het Besluit DFW blijft het dan ook onduidelijk of de AP van mening is dat Ziggo zich op een van de uitzonderingsgronden kan beroepen.

3.5 *Tussenconclusie: verwerkingsverbod van toepassing*

Bij het verlenen van medewerking in de zin van het verstrekken van NAW-gegevens of het doorsturen van waarschuwingsbrieven verwerkt Ziggo persoonsgegevens. Ziggo heeft voor de verwerking een grondslag nodig. Verder geldt dat de persoonsgegevens als strafrechtelijke persoonsgegevens kwalificeren. Op de verwerking van strafrechtelijke persoonsgegevens rust een verbod. Slechts bij wettelijke uitzondering mogen de strafrechtelijke persoonsgegevens worden verwerkt. Dit betekent dat Ziggo voor het verlenen van medewerking aan Brein een uitzonderingsgrond nodig heeft om strafrechtelijke persoonsgegevens te mogen verwerken.

4 Medewerkingsplicht: voor verwerkingsverbod

Anders dan in de *Brein/Ziggo*-uitspraken ligt het accent in oudere uitspraken niet zozeer op de voorwaarden voor gegevensverwerking, maar op de toetsing van de *Lycos/Pessers*-criteria. In verschillende uitspraken wordt weliswaar (indirect) gesproken over persoonsgegevens, maar vindt er geen kwalificatie van (strafrechtelijke) persoonsgegevens plaats.[23] Hetzelfde geldt voor de grondslag voor de gegevensverwerking.[24] Het lijkt erop dat op basis van de *Lycos/Pessers*-criteria wordt aangenomen dat de tussenpersoon al dan niet een gerechtvaardigd belang heeft bij de afgifte van NAW-gegevens.

Er zijn mij geen uitspraken van vóór *Brein/Ziggo I* bekend waarin NAW-gegevens van inbreukmakers als strafrechtelijke gegevens worden aangemerkt. Het lijkt er echter wel op dat Ziggo in het verleden een poging heeft gedaan om dit aspect tijdens een procedure aan te kaarten. Het betreft een geschil tussen DFW en Ziggo dat in 2019 voorlag bij het gerechtshof Arnhem-Leeuwarden.[25] In het geschil staat de vraag centraal of Ziggo NAW-gegevens van inbreukmakers aan DFW moet verstrekken. Het hof overweegt in deze zaak dat het relevant is dat de persoonsgegevens geen bijzondere persoonsgegevens betreffen maar (enkel) bestaan uit NAW-gegevens.[26] Omdat het onderwerp slechts een zeer klein onderdeel van de uitspraak beslaat, is het lastig om de overweging van het hof te kunnen duiden en in de juiste context te plaatsen. DFW gaat in cassatie en in de conclusie van de A-G komt het onderwerp opnieuw aan bod.[27] De A-G vermoedt dat Ziggo niet doelt op de verwerking van bijzondere persoonsgegevens, maar strafrechtelijke persoonsgegevens. In de ogen van de A-G heeft Ziggo dit in de processtukken echter onvoldoende gemotiveerd. Voor zover überhaupt sprake is van strafrechtelijke persoonsgegevens constateert de A-G dat Ziggo voor de verwerking van strafrechtelijke persoonsgegevens een beroep kan doen op de uitzonderingsgrond rechtsvordering.

Op basis van voorgaande constateer ik dat persoonsgegevens bij de afgifte van NAW-gegevens in het verleden niet zijn gekwalificeerd als strafrechtelijke persoonsgegevens. Als gevolg van het ontbreken van de kwalificatie wordt ook niet aan het verwerkingsverbod getoetst. De beoordeling of Ziggo NAW-gegevens moest verstrekken vond louter plaats op basis van de *Lycos/Pessers*-criteria.

5 Medewerkingsplicht: na verwerkingsverbod

5.1 *Brein/Ziggo I en II*

In het kort: wat speelt er in *Brein/Ziggo I* en *II*? Het verwerkingsverbod komt voor het eerst aan de orde in *Brein/Ziggo I*. In *Brein/Ziggo I* ligt de vraag voor of Ziggo verplicht is om op verzoek van Brein waarschuwingsbrie-

20 Art. 32 onder d UAVG.
21 Art. 33 lid 4 onder c UAVG.
22 Art. 33 lid 2 onder b UAVG: 'ter bescherming van zijn belangen, voor zover het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn.'
23 O.a. Rb. Noord-Holland 7 juni 2017, ECLI:NL:RBNHO:2017:4435 (*BREIN/Eweka Internet Services*); Hof Amsterdam 3 juli 2008, ECLI:NL:GHAMS:2008:BD6223 (*Leaseweb/BREIN*).
24 Zie vorige uitspraken en verder Rb. Den Haag 5 oktober 2015, ECLI:NL:RBDHA:2015:11408 (*BREIN/Google*).
25 Hof Arnhem-Leeuwarden 5 november 2019, ECLI:NL:GHARL:2019:9352.
26 Hof Arnhem-Leeuwarden 5 november 2019, ECLI:NL:GHARL:2019:9352, r.o. 5.17.
27 PHR 29 januari 2021, ECLI:NL:PHR:2021:83, par. 5.22-5.23.

ven door te sturen. De rechtbank stelt vast dat de verplichting een verwerking van strafrechtelijke persoonsgegevens inhoudt. De rechtbank oordeelt dat alleen Brein voor de verwerking over een wettelijke uitzonderingsgrond bezit. Door het ontbreken van een uitzonderingsgrond voor Ziggo, is het Ziggo niet toegestaan om de strafrechtelijke persoonsgegevens te verwerken. Dit leidt ertoe dat Ziggo geen grond heeft om de waarschuwingsbrieven door te sturen. Voorgaande verandert wanneer Ziggo voor de gegevensverwerking een vergunning bij de AP zou aanvragen. In dat geval heeft Ziggo wel een uitzonderingsgrond voor het doorsturen van de waarschuwingsbrieven.

In *Brein/Ziggo II* staat de vraag centraal of Ziggo aan Brein medewerking moet verlenen bij het handhavend optreden tegen een specifieke vermeende inbreukmaker. Volgens Brein heeft de inbreukmaker met één IP-adres meer dan 200 e-books toegankelijk gemaakt via een 'open directory'. Brein vordert primair medewerking van Ziggo bij het versturen van een waarschuwingsbrief en subsidiair verstrekking van NAW-gegevens van de inbreukmaker aan Brein. Brein voert vijf argumenten aan waarom Ziggo strafrechtelijke persoonsgegevens mag verwerken en dus medewerking zou moeten verlenen.[28] De rechtbank gaat niet mee met de redenering van Brein. De enige uitzonderingsgrond waar Ziggo (in de toekomst) een beroep op kan doen, is een vergunning van de AP. Dit geldt voor zowel de NAW-gegevens als de waarschuwingsbrieven.

5.2 *Persoonsgegevens*

In *Brein/Ziggo I* stelt de rechtbank dat partijen persoonsgegevens verwerken. De verwerking bestaat in het geval van Ziggo uit het koppelen van een IP-adres aan een inbreukmaker en het vervolgens versturen van de waarschuwingsbrief naar de inbreukmaker. Daarnaast stelt de rechtbank vast dat het versturen van IP-adressen door Brein aan Ziggo ook een verwerking van persoonsgegevens is. De rechtbank doet dit aan de hand van het *Breyer*-arrest (par. 3.1). Mede op basis van het arrest overweegt de rechtbank dat Brein (via de rechtbank) bij Ziggo de NAW-gegevens van houder van het IP-adres kan opvragen. De omstandigheid dat Brein nog niet voornemens is om van die mogelijkheid gebruik te maken, doet niet af aan het gegeven dat Brein over het wettelijk middel beschikt.[29] Voorgaande leidt ertoe dat de IP-adressen als persoonsgegevens worden gekwalificeerd. Dit is naar mijn mening een terechte conclusie.

5.3 *Grondslag*

In *Brein/Ziggo I* past de rechtbank de *Lycos/Pessers*-criteria toe op het doorsturen van waarschuwingsbrieven. Hiermee wordt het toepassingsbereik van *Lycos/Pessers* vergroot. De rechtbank overweegt dat Ziggo aan de criteria voldoet, met als gevolg dat Ziggo onrechtmatig handelt wanneer het de waarschuwingsbrieven niet doorstuurt. In het verlengde hiervan overweegt de rechtbank ook dat met het voldoen aan de *Lycos/Pessers*-criteria de grondslag gerechtvaardigd belang ook is gegeven. Ik signaleer dat het hof in *Brein/Ziggo III* op dit punt anders heeft geoordeeld. Het hof is de criteria opnieuw stap voor stap langs gegaan en is tot de slotsom gekomen dat Ziggo niet onrechtmatig handelt wanneer het de waarschuwingsbrieven niet doorstuurt.[30] Het hof komt dus niet eens toe aan de vraag of voor Ziggo een uitzondering op het verwerkingsverbod geldt. De medewerkingsplicht loopt al stuk bij het hebben van een algemene grondslag. Ik verwacht dat (ook) hier nog niet het laatste woord over is gezegd. Met het oog op de beoordeling van het verwerkingsverbod laat ik voor het vervolg van dit artikel de uitspraak van het hof buiten beschouwing. Ik ga er gemakshalve vanuit dat Ziggo wel een grondslag heeft voor de gegevensverwerking.

5.4 *Strafrechtelijke persoonsgegevens*

In *Brein/Ziggo I* stelt de rechtbank vast dat auteursrechtinbreuken op grond van artikel 31, 32 en 33 Auteurswet strafbaar zijn gesteld. Ook verwijst de rechtbank naar het Besluit DFW waarin de AP heeft vastgesteld dat gegevens over auteursrechtinbreuken kwalificeren als strafrechtelijke persoonsgegevens. De rechtbank constateert verder dat met de gedetecteerde IP-adressen auteursrechtelijk beschermde werken beschikbaar worden gesteld en dat er een gerechtvaardigd vermoeden is dat de houder van het IP-adres de werken beschikbaar heeft gesteld. Op basis van deze informatie komt de rechtbank tot de conclusie dat de gegevens als strafrechtelijke persoonsgegevens kwalificeren.

5.5 *Verwerkingsverbod*

Als gevolg van de kwalificatie van strafrechtelijke persoonsgegevens heeft Ziggo voor het doorsturen van waarschuwingsbrieven of het verstrekken van NAW-gegevens een uitzondering op het verwerkingsverbod nodig. De rechtbank ziet in *Brein/Ziggo I* vooralsnog geen uitzonderingsgrond op basis waarvan Ziggo strafrechtelijke persoonsgegevens mag verwerken. Naar mening van de rechtbank is de enige optie die in de toekomst voorhanden is, de uitzondering vergunning.[31] Dit betekent dat Ziggo bij de AP een vergunning moet aanvragen voor de verwerking van strafrechtelijke persoonsgegevens. De rechtbank overweegt voorts aan de hand van de *Lycos/Pessers*-criteria dat indien Ziggo over de vergunning beschikt, Ziggo onrechtmatig handelt wanneer het de waarschuwingsbrieven niet doorstuurt.[32] Hiermee lijkt

28 *Brein/Ziggo II*, r.o. 3.31-3.38.
29 *Brein/Ziggo I*, r.o. 3.4.
30 *Brein/Ziggo III*, r.o. 3.13.
31 *Brein/Ziggo I*, r.o. 3.15 en art. 33 lid 4 onder c UAVG.
32 *Brein/Ziggo I*, r.o. 3.42.

de rechtbank aan Ziggo impliciet een medewerkingsverplichting op te leggen vanaf het moment dat Ziggo over de vergunning beschikt.

In *Brein/Ziggo II* neemt Brein de stelling in dat de uitzonderingsgrond rechtsvordering op Ziggo van toepassing is omdat Brein middels *Brein/Ziggo II* een rechtsvordering instelt om de inbreuk tegen te gaan.[33] Volgens Brein is de uitzonderingsgrond rechtsvordering niet beperkt tot eigen rechtsvorderingen, maar kan het ook rechtsvorderingen van derde partijen betreffen.[34] De rechtbank beoordeelt in twee stappen of de uitzonderingsgrond rechtsvordering op Ziggo van toepassing is.

In de eerste stap wordt getoetst of de verwerking binnen de reikwijdte van de handelingen valt die verricht moeten worden in het kader van een rechtsvordering. Hierbij overweegt de rechtbank dat de reikwijdte van de uitzonderingsgrond niet beperkt is tot verwerkingen bij reeds ingestelde rechtsvorderingen, maar ook verwerkingen omvat die in de aanloop naar een gerechtelijke procedure plaatsvinden.[35] Voor wat betreft de waarschuwingsbrieven overweegt de rechtbank net als in *Brein/Ziggo I* dat de verwerking buiten de reikwijdte van uitzonderingsgrond rechtsvordering valt. De verwerking vindt plaats in het kader van een waarschuwingscampagne en de strafrechtelijke persoonsgegevens worden niet verder verwerkt voor het instellen van een rechtsvordering. Hiermee strandt de primaire vordering van Brein die bestaat uit het doorsturen van de waarschuwingsbrieven. Voor de afgifte van NAW-gegevens ligt het anders. Deze gegevens kunnen wel degelijk noodzakelijk zijn bij het instellen van een rechtsvordering.

Gelet op het voorgaande is de tweede stap beperkt tot NAW-gegevens. In deze stap beoordeelt de rechtbank of de uitzonderingsgrond beperkt is tot eigen rechtsvorderingen (van Ziggo) of dat het ook rechtsvorderingen van derde partijen (van Brein) mag betreffen. De rechtbank komt tot het oordeel dat de uitzondering is beperkt tot eigen rechtsvorderingen.[36] Deze lezing zou blijken uit de memorie van toelichting bij de UAVG waarin het volgende wordt vermeld: 'Particulieren kunnen onder omstandigheden hun rechten in een rechterlijke procedure niet effectueren zonder dat zij beschikken over bepaalde gegevens van hun wederpartij'.[37] Hierbij wordt extra waarde gehecht aan de zinssnede 'hun rechten' waaruit zou blijken dat de rechtsvordering moet zien op de rechten van de eisende of verwerende partij. In dit geval hebben de strafrechtelijke persoonsgegevens betrekking op een rechtsvordering van Brein. Brein heeft belang bij het uitoefenen van haar rechten en kan een beroep doen op de uitzonderingsgrondslag. Gelet op de omstandigheid dat Ziggo geen eigen belang heeft bij de rechtsvordering, overweegt de rechtbank dat Ziggo geen beroep kan doen op de uitzonderingsgrond.

Dit leidt ertoe dat voor Ziggo wederom enkel de uitzonderingsgrond vergunning van toepassing is. In dat kader voert Brein nog aan dat Ziggo zich naar beste vermogen moet inspannen om de vergunning te krijgen. De rechtbank gaat hier niet in mee. Het beperkt zich (opnieuw) tot de vaststelling dat Ziggo onrechtmatig handelt wanneer het ondanks een vergunning geen waarschuwingsbrieven doorstuurt. Daarbij geeft de rechtbank aan dat Brein geen medewerking of inspanning van Ziggo heeft gevorderd. Bij gebreke van een vordering geeft de rechtbank geen oordeel over de vraag wat Ziggo moet doen om de vergunning te verkrijgen.[38]

6 Medewerkingsplicht: gevolgen verwerkingsverbod

6.1 *Algemeen*

Zowel bij NAW-gegevens als bij waarschuwingsbrieven moeten de persoonsgegevens gekwalificeerd worden als strafrechtelijke persoonsgegevens. Voorheen vond deze kwalificatie niet plaats bij NAW-gegevens. In *Brein/Ziggo II* wordt dit rechtgetrokken en worden de persoonsgegevens zowel bij NAW-gegevens als bij waarschuwingsbrieven als strafrechtelijke persoonsgegevens aangemerkt. Als gevolg van de kwalificatie is het verwerkingsverbod van toepassing en heeft Ziggo een uitzonderingsgrond nodig om medewerking te kunnen/mogen verlenen. Uit de *Brein/Ziggo*-uitspraken is gebleken dat Ziggo slechts in aanmerking komt voor de uitzonderingsgrond vergunning. Ik plaats hier twee opmerkingen bij.

6.2 *Uitzonderingsgrond rechtsvordering*

Uit *Brein/Ziggo II* volgt dat zelfs wanneer sprake is van een (nog in te stellen) rechtsvordering van Brein, Ziggo niet ten behoeve van Brein strafrechtelijke persoonsgegevens mag verwerken. Ik vraag mij af of de uitzonderingsgrond zo beperkt moet worden uitgelegd. Deze uitleg lijkt niet in lijn te zijn met de uitleg van het Hof van Justitie (HvJ EU) in het *Rigas*-arrest.[39] In dit arrest overweegt het HvJ EU juist dat het geen twijfel lijdt dat het belang van een derde bij het verkrijgen van persoonsgegevens om schade in rechte te kunnen verhalen, een gerechtvaardigd belang is.[40]

Ook ben ik van mening dat artikel 32 lid d UAVG breder uitgelegd moet worden. In het artikel is opgenomen dat strafrechtelijke persoonsgegevens verwerkt mogen

33 *Brein/Ziggo II*, r.o. 3.33.
34 *Brein/Ziggo II*, r.o. 3.33.
35 *Brein/Ziggo II*, r.o. 3.35.
36 *Brein/Ziggo II*, r.o. 3.35.
37 MvT UAVG, p. 103.
38 *Brein/Ziggo II*, r.o. 3.43.
39 HvJ EU 4 mei 2017, ECLI:EU:C:2017:336.
40 HvJ EU 4 mei 2017, ECLI:EU:C:2017:336, par. 29.

worden, indien het noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering. Deze uitzonderingsgrond heeft dus betrekking op een noodzakelijke verwerking van strafrechtelijke persoonsgegevens. Het artikel vermeldt niets over welke partijen de noodzakelijke verwerking mogen verrichten. In *Brein/Ziggo II* is de afgifte van NAW-gegevens noodzakelijk voor het instellen van een rechtsvordering. Zonder de NAW-gegevens van de wederpartij kan Brein immers geen rechtsvordering instellen. Voor Brein is het noodzakelijk dat Ziggo de strafrechtelijke persoonsgegevens verwerkt zodat Brein een rechtsvordering kan instellen. De in *Brein/Ziggo II* geciteerde tekst uit de memorie van toelichting maakt voorgaande niet anders (par. 5.5). Uit de memorie van toelichting volgt slechts dat een partij onder omstandigheden over de persoonsgegevens van de wederpartij moet kunnen beschikken. Uit de memorie van toelichting volgt daarentegen geenszins dat het derde partijen niet is toegestaan om ten behoeve van (bijvoorbeeld) de eisende partij strafrechtelijke persoonsgegevens te verwerken. Naar mijn mening zou de uitzonderingsgrond rechtsvordering daarom wel van toepassing moeten zijn op Ziggo. Verder merk ik op dat de (zeer) beperkte uitleg van de uitzonderingsgrond rechtsvordering niet alleen voor Brein, maar ook voor andere partijen grote gevolgen heeft. Partijen die bijvoorbeeld in het kader van smaad gegevens bij een websitehouder of internetaanbieder willen opvragen, lopen op basis van deze uitspraken ook tegen de lamp.

6.3 *Uitzonderingsgrond vergunning*

De beperkte uitleg van de uitzonderingsgrond rechtsvordering zal in veel gevallen tot gevolg hebben dat tussenpersonen alleen nog op basis van een vergunning strafrechtelijke persoonsgegevens mogen verwerken. Het aanvragen van een vergunning heeft nogal wat voeten in de aarde. De tussenpersoon moet onder andere een Data Protection Impact Assessment (DPIA) uitvoeren, eventueel voorafgaand aan de vergunningaanvraag de AP raadplegen, een protocol opstellen en de daadwerkelijke vergunning aanvragen. Het is de vraag of een tussenpersoon hier vrijwillig en ten behoeve van een derde tijd, geld en moeite in gaat steken. Ziggo heeft duidelijk laten merken dat niet vrijwillig te doen.[41] Uit de omstandigheid dát een vergunning noodzakelijk is, volgt nog niet dat Ziggo verplicht is om de vergunning aan te vragen. Deze medewerkingsverplichting moet Brein moet expliciet vorderen. Tot op heden is dat nog niet gebeurd. Mijn verwachting is dat een dergelijke procedure nog wel in het verschiet ligt. Brein heeft immers in het kader van de waarschuwingscampagne ook op de lange termijn baat bij medewerking van Ziggo. Daarentegen vraag ik mij wel af in hoeverre het voor andere partijen nog loont om een heel proces te starten zodat van tussenpersonen medewerking in de vorm van een vergunningsaanvraag gevorderd kan worden.

7 Conclusie

Het verwerkingsverbod is van toepassing op de verwerking van strafrechtelijke persoonsgegevens door Ziggo ten behoeve van Brein. Het verbod heeft niet alleen gevolgen voor het doorsturen van waarschuwingsbrieven, maar ook voor het verstrekken van NAW-gegevens. Door de (zeer) beperkte uitleg van de uitzonderingsgrond rechtsvordering komen derde partijen, zoals Ziggo, niet in aanmerking voor deze uitzonderingsgrond. Dat leidt naar mijn mening tot een onwenselijke situatie. Ten eerste wordt Brein de mogelijkheid ontnomen om snel en eenvoudig een beroep te doen op derde partijen bij het optreden tegen inbreukmakers. Daarnaast moet Brein een procedure starten om Ziggo te kunnen verplichten tot het aanvragen van een vergunning bij de AP. Het is nu de vraag of Brein deze koers doorzet en er een *Brein/Ziggo IV* komt waarin de medewerking van Ziggo wordt gevorderd in de vorm van het aanvragen van een vergunning.

41 *Brein/Ziggo III*, r.o. 3.21.

De rechtbank Amsterdam stelt prejudiciële vragen aan het Hof over de uitleg van gerechtvaardigd belang

Rb. Amsterdam 22 september 2022, ECLI:NL:RBAMS:2022:5565

Mr. S.E.A. Vermeer-de Jongh en Mr. E.W.S. Peperkamp*

280

1 Inleiding

De rechtbank Amsterdam besliste op 22 september jl. als eerste Nederlandse rechter om prejudiciële vragen te stellen aan het Hof van Justitie van de Europese Unie (Hof) over de uitleg van gerechtvaardigd belang zoals vervat in artikel 6, lid 1 onder f van de Algemene verordening gegevensbescherming (AVG).[1]

Het is niet geheel onverwachts dat de uitleg van gerechtvaardigd belang centraal staat in de Nederlandse rechtspraak gezien de normuitleg grondslag 'gerechtvaardigd belang'[2] van de Autoriteit Persoonsgegevens (AP) die met veel kritiek is ontvangen. Kort gezegd, stelt de AP sinds 2019 dat gerechtvaardigde belangen in wetgeving of elders in het recht moeten zijn benoemd als een rechtsbelang en dat 'het enkel dienen van winstmaximalisatie' en 'zuiver commerciële belangen' niet als gerechtvaardigde belangen kwalificeren.

De AP legt op basis van deze uitleg zowel een boete van € 525 000 aan de Koninklijke Nederlandse Lawn Tennis Bond (KNLTB)[3] als en een boete van € 575 000 aan VoetbalTV op,[4] met Nederlandse rechtspraak over de uitleg van gerechtvaardigd belang[5] tot gevolg. Ondanks deze relevante rechtspraak, volgt uit een recente tussenuitspraak dat de rechtbank Amsterdam zich genoodzaakt houdt om de *KNLTB*-beroepsprocedure aan te houden totdat het Hof prejudiciële vragen over de uitleg van gerechtvaardigd belang heeft beantwoord. Hierdoor hangt de prangende vraag of een gerechtvaardigd belang in het recht moet zijn benoemd als rechtsbelang nog steeds boven de markt.

2 Het boetebesluit van de AP

In de *KNLTB*-zaak staat de verstrekking van persoonsgegevens van een deel van de KNLTB-leden in juni en juli 2018 aan twee sponsoren centraal. Zoals gebruikelijk in de sportbranche, heeft ook de KNLTB verschillende sponsoren met wie zij samenwerkt. De AP concludeert in het Boetebesluit dat sprake is van een onverenigbare verdere verwerking[6] en dat de KNLTB geen rechtmatige grondslag[7] heeft.

De KNLTB baseert de verstrekking op de grondslag gerechtvaardigd belang.[8] Uit het Boetebesluit volgt dat de KNLTB en de AP verdeeld zijn over de vraag hoe het gerechtvaardigde belang van de KNLTB luidt. Voorafgaand aan de verstrekking informeert de KNLTB haar leden over onder meer het belang van het creëren van meerwaarde voor het KNLTB-lidmaatschap door tennisgerelateerde en andere relevante aanbiedingen van sponsoren te kunnen ontvangen.[9] De AP duidt het belang van de KNLTB daarentegen als 'het belang zo veel mogelijk geld te verdienen' en 'het enkele belang persoonsgegevens te gelde te kunnen maken c.q. daar winst mee te kunnen maken'.[10] NB, in het Boetebesluit wordt door de AP nog niet nader ingegaan op de stelling van de KNLTB dat het aan de verwerkingsverantwoordelijke (lees: de KNLTB) is om het gerechtvaardigd belang te stellen.

---

* Saskia Vermeer- de Jongh en Lisa Peperkamp zijn als advocaten IT- en privacyrecht verbonden aan HVG Law en staan de KNLTB bij in de bezwaar- en beroepsprocedure volgend op het boetebesluit van de AP.

1 Rb. Amsterdam 22 september 2022, ECLI:NL:RBAMS:2022:5565, r.o. 6. Overal waar wij verder alleen een rechtsoverweging vermelden, verwijzen wij naar deze uitspraak.
2 AP, Normuitleg grondslag 'gerechtvaardigd belang', te raadplegen via: autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf.
3 AP, besluit tot het opleggen van een bestuurlijke boete aan de KNLTB, 20 december 2019 (Boetebesluit).
4 Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111, procesverloop.
5 Idem en ABRvS 27 juli 2022, ECLI:NL:RVS:2022:2173.
6 Art. 5 lid 1 onder b AVG.
7 Art. 5 lid 1 onder a AVG jo. art. 6 lid 1 AVG.
8 Uit Boetebesluit, overweging 145 e.v. volgt dat de KNLTB meent op het Informatieblad 'Verstrekken gegevens uit ledenadministratie' gepubliceerd door het College bescherming persoonsgegevens (de rechtsvoorganger van de AP) te kunnen vertrouwen dat gerechtvaardigd belang een passende grondslag kan zijn.
9 Boetebesluit, overwegingen 35-41.
10 Idem, overwegingen 134-136.

Uit vaste rechtspraak volgt dat voor een geldig beroep op deze grondslag vereist is dat de driestappentoets wordt doorlopen: (1) er moet sprake zijn van een gerechtvaardigd belang, (2) de verwerking moet noodzakelijk zijn om dat belang te behartigen en (3) er moet een afweging plaatsvinden tussen de belangen van een verwerkingsverantwoordelijke of derde en de belangen van de betrokkene waarbij de belangen van de betrokkene niet zwaarder mogen wegen.[11]

Uit het Boetebesluit volgt dat de KNLTB en de AP verdeeld zijn over de wijze waarop gerechtvaardigd belang zoals bedoeld in stap (1) van de driestappentoets moet worden uitgelegd. De AP hanteert een zogeheten *positieve toets* en stelt dat uit het systeem van de AVG volgt dat een gerechtvaardigd belang terug te voeren moet zijn op een grondrecht of rechtsbeginsel: 'Immers, een verwerking van persoonsgegevens is altijd een inmenging op het fundamentele recht op bescherming van persoonsgegevens. Daardoor is iedere verwerking in beginsel onrechtmatig.'[12] Dat houdt volgens de AP in dat die belangen in wetgeving of elders in het recht dienen te zijn benoemd als een rechtsbelang.[13] Zuiver commerciële belangen en het belang van winstmaximalisatie ontberen voldoende specificiteit en missen een dringend 'wettelijk' karakter zodat zij niet kunnen kwalificeren als gerechtvaardigde belangen, aldus de AP.[14] In het Boetebesluit gaat de AP niet in op de stelling van de KNLTB dat deze uitleg geen steun vindt in bijvoorbeeld de wettekst van de AVG,[15] eerdere jurisprudentie van het Hof[16] en de uitleg zoals wordt gehanteerd door andere toezichthouders.[17, 18]

3 De *VoetbalTV*-uitspraken

In de twee uitspraken[19] die volgen op de boete aan VoetbalTV staat ook de uitleg van gerechtvaardigd belang centraal. De rechtbank Midden-Nederland concludeert dat gerechtvaardigd belang op een open en flexibele manier moet worden uitgelegd en dat een gerechtvaardigd belang niet terug te voeren hoeft te zijn op een grondrecht of rechtsbeginsel (de *negatieve toets*). De rechtbank Midden-Nederland concludeert dat uit een opinie van de Artikel 29-werkgroep[20] en rechtspraak van het Hof[21] volgt dat het lidstaten niet vrijstaat om een beroep op het gerechtvaardigd belang voor bepaalde categorieën op voorhand of categorisch uit te sluiten zonder ruimte voor een concrete belangenafweging.[22] De rechtbank concludeert verder dat het aan een verwerkingsverantwoordelijke zelf is om het gerechtvaardigd belang te stellen en daar ook feitelijk naar te handelen.[23]

In de door de AP ingestelde hogerberoepsprocedure oordeelt de Afdeling bestuursrechtspraak van de Raad van State (Afdeling) op 27 juli 2022 dat de AP op onjuiste gronden een boete aan VoetbalTV heeft opgelegd en dat de uitspraak van de rechtbank Midden-Nederland in stand moet worden gehouden.[24] Deze uitspraak van de Afdeling geeft helaas geen antwoord op de vraag of de AP terecht of onterecht meent dat een gerechtvaardigd belang in het recht moet zijn benoemd als rechtsbelang (en dat 'winstmaximalisatie' en 'zuiver commerciële belangen' niet als gerechtvaardigde belangen kwalificeren). Relevant is wel dat de Afdeling oordeelt dat het door VoetbalTV aangevoerde belang niet slechts een zuiver commercieel belang is en dat de AP ten onrechte de door VoetbalTV gestelde belangen niet heeft meegewogen: 'Het is aan de verwerkingsverantwoordelijke om te stellen wat het belang bij de verwerking is, waarom die verwerking noodzakelijk is en dat hij hiernaar moet handelen.'[25]

---

11 HvJ EU 4 mei 2017, ECLI:EU:C:2017:336, r.o. 28 (*Rīgas satiksme*) en HvJ EU 29 juli 2019, ECLI:EU:C:2019:629, r.o. 95 (*Fashion ID*).
12 Idem, overweging 128.
13 Idem, overweging 131.
14 Idem, overweging 138. Zie ook AP, Normuitleg grondslag 'gerechtvaardigd belang', waarin de AP deze normuitleg voor het eerst verkondigt, te raadplegen via: autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf.
15 Onder meer gezien het bepaalde in overweging 47, AVG: 'De verwerking van persoonsgegevens ten behoeve van direct marketing kan worden beschouwd als uitgevoerd met het oog op een gerechtvaardigd belang'.
16 HvJ EU 24 november 2011, ECLI:EU:C:2011:277 (*ASNEF*), HvJ EU 13 mei 2014, ECLI:EU:C:2014:317 (*Google Spain*), HvJ EU 19 oktober 2016, ECLI:EU:C:2016:779 (*Breyer*), HvJ EU 11 december 2019, ECLI:EU:C:2019:1064 (*M5A-SCaraA*) en HvJ EU 29 juli 2019, ECLI:EU:C:2019:629 (*Fashion ID*).
17 Zie onder meer Information Commissioner's Office, 'When can we rely on legitimate interests', te raadplegen via: ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests, Gegevensbeschermingsautoriteit België, Gerechtvaardigd belang: 'Een belang wordt als gerechtvaardigd beschouwd zolang dit je dit nastreeft op een wijze die in overeenstemming is zowel met de regelgeving inzake gegevensbescherming als andere relevante regelgeving', te raadplegen via: gegevensbeschermingsautoriteit.be/gerechtvaardigd-belang en Commission Nationale de l'Informatique et des Libertés, 'L'intérêt légitime: comment fonder un traitement sur cette base légale?', te raadplegen via: cnil.fr/fr/les-bases-legales/interet-legitime.
18 Boetebesluit, overweging 127.
19 Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111 en ABRvS 27 juli 2022, ECLI:NL:RVS:2022:2173.
20 Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 april 2014, p. 24.
21 HvJ EU 24 november 2011, ECLI:EU:C:2011:277, r.o. 34 (*ASNEF*), HvJ EU 11 december 2019, ECLI:EU:C:2019:1064, r.o. 53 (*M5A-SCaraA*) en HvJ EU 19 oktober 2016, ECLI:EU:C:2016:779, r.o. 62 (*Breyer*).
22 Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111, r.o. 15.
23 Idem, r.o. 17.
24 Zie voor meer uitleg over deze uitspraak van de Afdeling de noot van mr. A. Holtland, 'Uitspraak Raad van State over VoetbalTV', zoals ook opgenomen in deze editie van *P&I*.
25 ABRvS 27 juli 2022, ECLI:NL:RVS:2022:2173, r.o. 8.

4 De *KNLTB*-tussenuitspraak rechtbank Amsterdam

Anders dan de rechtbank Midden-Nederland en de Afdeling, laat de rechtbank Amsterdam zich in de tussenuitspraak van 22 september jl. niet uit over de wijze waarop gerechtvaardigd belang wordt uitgelegd. De rechtbank Amsterdam licht summier toe waarom verschillende interpretaties van gerechtvaardigd belang mogelijk kunnen zijn.

De rechtbank Amsterdam stelt enerzijds dat de uitspraak van de rechtbank Midden-Nederland en de daarin aangehaalde bronnen inderdaad het standpunt van de KNLTB lijken te ondersteunen dat elk belang, dus ook een zuiver commercieel belang, een gerechtvaardigd belang kan zijn.[26] In aanvulling hierop, stelt de rechtbank dat de AVG duidelijk voorschrijft wanneer een verwerking zijn rechtsgrondslag in een lidstatelijke of Unierechtelijke bepaling moet vinden. De KNLTB voert namelijk aan dat indien de Uniewetgever met de term 'gerechtvaardigd' inderdaad 'wettelijk' heeft bedoeld dan daadwerkelijk de term 'wettelijk' in plaats van 'gerechtvaardigd' was toegepast in artikel 6, lid 1, onder f van de AVG (zoals bijvoorbeeld wel is gedaan in artikel 6, lid 1, onder c van de AVG).[27]

Tegenover bovenstaande argumenten stelt de rechtbank Amsterdam dat: 'het niet te rijmen (lijkt) met de hoge mate van bescherming die de AVG betoogt te bieden wanneer de wens om zonder toestemming van betrokkene geld te verdienen met andermans persoonsgegevens wordt aangemerkt als gerechtvaardigd belang.'[28] Onduidelijk is op welke bronnen de rechtbank Amsterdam deze mogelijke uitleg baseert. Onduidelijk is eveneens waarom de rechtbank Amsterdam hier voorbijgaat aan de door de KNLTB gestelde belangen (lees: het creëren van meerwaarde voor het KNLTB-lidmaatschap door tennisgerelateerde en andere relevante aanbiedingen van sponsoren te kunnen ontvangen).

De rechtbank Amsterdam gaat in de tussenuitspraak voorbij aan een door *NRC* eerder op 3 juli 2022 gepubliceerde brief waaruit volgt dat de Europese Commissie (EC) de AP al in maart 2020 duidelijk maakt dat zij verontrust is over de naar haar oordeel onjuiste uitleg die de AP aan het begrip gerechtvaardigd belang geeft: 'we are concerned by the strict interpretation in the explanation note stating that interests such as a pure commercial interest does not qualify as a "legitimate" interest as regards Article 6(1)(f) GDPR (...) it is difficult to reconcile the strict interpretation of the Dutch DPA of what can constitute a legitimate interest with the intended effect that the EU legislators wanted to attribute to Article 6(1)(f) GDPR.'[29] Uit deze brief volgt dat ook de EC pleit voor een meer open uitleg van gerechtvaardigd belang: 'The strict interpretation laid down by the Dutch DPA severely limits businesses' possibilities of processing personal data for commercial interests, as they would have to collect consent from the data subject in every case where an economic interest in pursued, since the other relevant legal grounds in Article 6(1) GDPR have, effectively, be rendered inapplicable'.

Het is verder opvallend dat de rechtbank Amsterdam oordeelt dat niet is gebleken van een *acte clair* of *acte éclairé*. Er zijn immers genoeg steekhoudende argumenten te bedenken waaruit volgt dat wel sprake is van een *acte clair* of *acte éclairé* en dat aldus een prejudiciële procedure niet voor de hand ligt.[30]

De rechtbank Amsterdam oordeelt dat niet gebleken zou zijn van een *acte clair* aangezien de wettekst geen uitsluitsel zou geven over de definitie en de reikwijdte van het begrip gerechtvaardigd belang.[31] Anders dan de rechtbank Amsterdam, lijkt de rechtbank Midden-Nederland in de *VoetbalTV*-uitspraak op basis van relevante criteria zoals de verschillende taalversies, de eigen terminologie en de context van de bepaling[32] te concluderen dat wel degelijk sprake is van een *acte clair*: 'Dat het gerechtvaardigd belang (…) niet moet worden gezien als een min of meer wettelijk belang, zoals verweerder meent, maar veel meer als een legitiem belang, sluit ook aan bij de **buitenlandse vertalingen van dit begrip**, te weten "legitimate interests"(Eng.), "berechtigten Interessen"(Du.) en "des intérêts légitimes" (Fr.). Er is daarmee een **duidelijk onderscheid gemaakt met de wettelijke verplichting die is genoemd in artikel 6, eerste lid, aanhef en onder c**, van AVG, "legal obligation" (Eng.), "rechtlichen Verpflichtung"(Du.) en "une obligation légale" (Fr.). Dat het gerechtvaardigd belang moet worden bekeken aan de hand van een negatieve toets, **komt ook overeen met overweging 47 van de AVG** waarin als voorbeeld van een mogelijk gerechtvaardigd belang "direct marketing" wordt genoemd.'[33]

Of daadwerkelijk geen sprake is van een *acte éclairé* valt eveneens te betwisten. Bij de beoordeling of sprake is van *acte éclairé* volstaat het als de vraag in een gelijksoortig geval voorwerp van een prejudiciële beschikking is geweest, maar de aan de orde zijnde vraagstukken hoeven niet volledig gelijk te zijn.[34] De *Google Spain*[35] en

26 R.o. 5.3.
27 R.o. 5.5.
28 R.o. 5.4.
29 'Brussel vindt Nederlandse privacywaakhond te strikt', *NRC* 3 juli 2022 en Brief van EC aan AP, 6 maart 2020, te raadplegen via: static.nrc.nl/2022/pdf/letter-dutch-dpa-legitimate-interest.pdf.
30 Art. 267 Verdrag betreffende de werking van de Europese Unie.
31 R.o. 5.2.
32 HvJ EU 28 februari 2019, ECLI:EU:C:2019:576, concl. A-G G. Pitruzzella, r.o. 64 (*Amazon EU*).
33 Rb. Midden-Nederland 23 november 2020, ECLi:NL:RBMNE:2020:5111, r.o. 16.
34 HvJ EU 6 oktober 2021, ECLI:EU:C:2021:799, r.o. 36 (*Consorzio Italian Management e.a.*).
35 HvJ EU 13 mei 2014, ECLI:EU:C:2014:317 (*Google Spain*).

Fashion ID-arresten[36] waarin sprake was van verwerkingen van persoonsgegevens die allebei een commercieel belang dienden lijken aan die maatstaf te voldoen.

5 Vooruitblik

Wat ons betreft is het op basis van de grammaticale, wetshistorische en wetsystematische interpretatie van artikel 6, lid 1, onder f van de AVG denkbaar dat ook het Hof zal oordelen dat het aan een verwerkingsverantwoordelijke zelf is om het gerechtvaardigd belang te stellen én dat een gerechtvaardigd belang niet terug te voeren hoeft te zijn op een grondrecht of rechtsbeginsel.

Voor nu is het afwachten of het Hof de uitleg van de AP onderschrijft of juist zal oordelen dat het de AP gezien de strekking van een verordening (lees: harmonisatie en uniformiteit) niet vrij staat om een afwijkende uitleg aan een norm met een autonome betekenis onder het Europees (privacy) recht te geven.[37] Mogelijk dat de European Data Protection Board (EDPB) in de tussentijd een nieuwe opinie over de uitleg van gerechtvaardigd belang zal publiceren die meer duidelijkheid biedt, al kunnen wij ons voorstellen dat de EDPB de uitspraak van het Hof afwacht. Hoewel de markt dringend behoefte heeft aan meer duidelijkheid over de reikwijdte van gerechtvaardigd belang, is de kous voorlopig dus nog niet af…

36 HvJ EU 29 juli 2019, ECLI:EU:C:2019:629 (*Fashion ID*).

37 Zie ook art. 51 lid 2 AVG: 'Elke toezichthoudende autoriteit draagt bij tot de consequente toepassing van deze verordening in de hele Unie. Daartoe werken de toezichthoudende autoriteiten onderling en met de Commissie samen overeenkomstig hoofdstuk VII' en HvJ EU 28 februari 2019, ECLI:EU:C:2019:576, A-G G. Pitruzzella, r.o. 64 (*Amazon EU*): 'Wanneer voorts een bepaling van Unierecht voor een bepaald begrip niet naar het recht van de lidstaten verwijst, wordt dat begrip in de gehele Unie autonoom en uniform uitgelegd, waarbij niet alleen rekening wordt gehouden met de bewoordingen van de betrokken bepaling, maar ook met de context ervan en met het doel van de regeling waarvan zij deel uitmaakt.'

Uitspraak Raad van State over *VoetbalTV*

Mr. A. Holtland*

281

Samenvatting

VoetbalTV is een videoplatform voor amateurvoetbal dat in opdracht van voetbalclubs videobeelden maakt van amateurvoetbalwedstrijden (waaronder van minderjarigen). De Autoriteit Persoonsgegevens legde een bestuurlijke boete op van € 575 000, vanwege het vermeende onrechtmatig verwerken van persoonsgegevens omdat VoetbalTV geen grondslag zou hebben voor de gegevensverwerking in het kader van haar bedrijfsactiviteiten. De Afdeling Bestuursrechtspraak van de Raad van State oordeelt in de uitspraak van 27 juli 2022 (ECLI:NL:RVS:2022:2173) over de wijze waarop de AP de grondslag 'gerechtvaardigd belang' in dit geval moet toetsen en oordeelt dat de toets van de AP in dit geval niet volstaat. In die toets zijn niet alle door VoetbalTV gestelde belangen meegewogen en zijn niet alle stappen uit de 3-stappentoets – die bij de toets of sprake is van een gerechtvaardigd belang moet worden uitgevoerd – doorlopen. De Afdeling oordeelt dan ook dat de opgelegde bestuurlijke boete niet in stand kan blijven. In deze annotatie wordt kort de uitspraak van de rechtbank Amsterdam van 22 september 2022[1] aangestipt die ook zeer relevant is voor de uitleg van de grondslag 'gerechtvaardigd belang'. Voor een nadere analyse over die uitspraak verwijs ik graag naar de annotatie van mr. S.E.A. Vermeer-de Jongh en mr. E.W.S. Peperkamp elders in dit nummer.

Noot

In de onderhavige uitspraak oordeelt de Afdeling Bestuursrechtspraak van de Raad van State (Afdeling) over de rechtmatigheid van de bestuurlijke boete die de Autoriteit Persoonsgegevens (AP) op 16 juli 2020 oplegde aan VoetbalTV vanwege het (vermeende) onrechtmatig verwerken van persoonsgegevens. In dit hoger beroep was de vraag aan de orde of VoetbalTV persoonsgegevens mocht verwerken voor haar bedrijfsactiviteiten op basis van de grondslag 'gerechtvaardigd belang' (art. 6 lid 1 onder f AVG).

Het andere 'hete hangijzer' dat in de *VoetbalTV-boete*zaak speelde in eerste aanleg,[2] was de vraag of de activiteiten van VoetbalTV onder de 'journalistieke exceptie' uit de Algemene Verordening Gegevensbescherming (AVG) vallen. Dat zou betekenen dat de AVG niet op die verwerking van persoonsgegevens van toepassing zou zijn en de AP ook niet bevoegd was om handhavend op te treden. Die vraag beantwoordt de rechtbank in eerste aanleg ontkennend, volgens de rechtbank omdat de verwerking niet uitsluitend een journalistiek doel dient (r.o. 4).

In de literatuur werd een aantal vraagtekens geplaatst bij (voornamelijk) het oordeel van de rechtbank over de journalistieke exceptie.[3] Helaas voor de praktijk komt deze vraag in het hoger beroep bij de Afdeling niet meer aan de orde omdat het hoger beroep van de AP sneuvelt op het punt van de onderbouwing van het 'gerechtvaardigd belang' en het voorwaardelijke incidenteel hoger beroep van VoetbalTV dus niet aan bod komt. Gelet op ontwikkelingen rondom het begrip 'gerechtvaardigd belang' gaf deze uitspraak van de Afdeling (los van de vraag over de journalistieke exceptie) aanleiding voor een nadere analyse.

Achtergrond

VoetbalTV is een videoplatform voor amateurvoetbal. Dit platform maakt in opdracht van voetbalclubs videobeelden van amateurvoetbalwedstrijden. Er worden onder meer minderjarigen in beeld gebracht. Via VoetbalTV kunnen voetbalmomenten worden teruggekeken, wedstrijden worden geanalyseerd en gegevens worden verzameld en gedeeld met anderen. VoetbalTV is daarmee ook een sociaal platform.

De AP legde in juli 2020 aan VoetbalTV een bestuurlijke boete op van € 575 000, vanwege de vermeende onrechtmatige verwerking van persoonsgegevens bij deze activiteiten.

Wat was er in geschil?

De AP stelde zich op het standpunt dat deze verwerking van persoonsgegevens door VoetbalTV niet was toegestaan, omdat die niet 'rechtmatig, behoorlijk en transparant' zou zijn (art. 5 lid 1 onder a AVG) en niet kon

* Anke Holtland is advocaat bij NautaDutilh.

1 Rb. Amsterdam 22 september 2022, ECLI:NL:RBAMS:2022:5565.
2 Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111.
3 Zie onder meer: *P&I* 2021/7, afl. 1, m.nt. M.D. Reijneveld & T.F. Walree; *Computerrecht* 2021, afl. 6, m.nt. M. Jansen; *JBP* 2021, afl. 1, m.nt. K. Konings en *Mediaforum* 2021, afl. 7, m.nt. Q.J. Tjeenk Willink & C. Plaizier.

worden gebaseerd op een van de grondslagen genoemd in artikel 6, eerste lid van de AVG. VoetbalTV stelde zich op het standpunt dat de genoemde verwerking van persoonsgegevens wel kon worden gebaseerd op zo'n grondslag, namelijk artikel 6, eerste lid onder f van de AVG: *'de verwerking van persoonsgegevens is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.'*

De kernvraag is: hoe moet worden bepaald (lees: wie de bewijslast draagt voor de stelling) of een verwerkingsverantwoordelijke zich op die grondslag kan baseren. Die kernvraag vloeit voort uit de wijze waarop het juridisch kader is geformuleerd, waaruit drie cumulatieve voorwaarden voortvloeien, maar waaruit nog niet rechtstreeks duidelijk is op welke wijze wordt beoordeeld óf aan die cumulatieve voorwaarden wordt voldaan.

Volgens vaste rechtspraak van het Hof van justitie van de Europese Unie (HvJ EU) luiden die drie cumulatieve voorwaarden waaraan moet worden voldaan om persoonsgegevens op basis van die grondslag persoonsgegevens te mogen verwerken als volgt:[4]

1. Er moet sprake zijn van de behartiging van een gerechtvaardigd belang van de verwerkingsverantwoordelijke.
2. De verwerking moet voor dat gerechtvaardigde belang noodzakelijk zijn.
3. Het gerechtvaardigd belang van de verwerkingsverantwoordelijke moet zwaarder wegen dan de belangen of de grondrechten en fundamentele vrijheden van diegene wiens persoonsgegevens worden verwerkt.

Deze drie cumulatieve voorwaarden worden de '3-stappentoets' genoemd. In het boetebesluit voerde de AP deze toets uit en kwam bij de eerste stap al tot de conclusie dat VoetbalTV voor haar bedrijfsactiviteiten geen persoonsgegevens mag verwerken op basis van de grondslag 'gerechtvaardigd belang'. De AP oordeelt zelf inhoudelijk over de grondslag 'gerechtvaardigd belang', en stelt dat het belang van VoetbalTV geen 'gerechtvaardigd belang' betreft, omdat dit een 'zuiver commercieel belang' betreft en geen 'rechtsbelang'. Waarbij een 'rechtsbelang' volgens de AP een belang is dat volgt uit een wet. Deze wijze van beoordelen van de AP volgt uit haar eigen beleidsregel 'Normuitleg grondslag "gerechtvaardigd belang"' (Normuitleg) die de AP op haar website heeft gepubliceerd. Op basis van deze analyse legt de AP dan ook een bestuurlijke boete op aan VoetbalTV.

VoetbalTV daarentegen stelt dat als 'gerechtvaardigd belang' moet worden aangemerkt: 'ieder belang dat niet in strijd is met de wet' (de zogenaamde 'negatieve toets'). VoetbalTV stelt te voldoen aan die 'negatieve toets' (stap 1) en voert ter onderbouwing aan de volgende belangen te hebben bij het verwerken van persoonsgegevens:

i. vergroting van de betrokkenheid en het spelplezier van voetballiefhebbers, inclusief dat van spelers die in beeld worden gebracht;
ii. het kunnen uitvoeren van technische analyses voor/door trainers en/of analisten van de voetbalclubs en derde partijen;
iii. het bieden van de mogelijkheid aan onder andere spelers, vrienden en familieleden om wedstrijden op afstand (terug) te kunnen kijken, bijvoorbeeld als zij daarbij niet fysiek aanwezig kunnen zijn; en
iv. VoetbalTV heeft een kanalisatiefunctie, omdat zij bijdraagt aan een hoger niveau van privacybescherming onder andere doordat zij het opnemen van wedstrijden via andere kanalen tegengaat.

Het oordeel van de Afdeling

De Afdeling neemt in deze uitspraak een duidelijk standpunt in over de rolverdeling tussen de AP als toezichthouder en VoetbalTV als partij die aan dat toezicht is onderworpen. De Afdeling oordeelt hierover dat het aan VoetbalTV is om te stellen (1) welk belang VoetbalTV bij de verwerking van persoonsgegevens in het kader van haar bedrijfsactiviteiten heeft, (2) waarom die verwerking noodzakelijk is en (3) dat VoetbalTV hiernaar moet handelen. De rol van de AP is om (a) te beoordelen wat de verwerkingsverantwoordelijke werkelijk doet, (b) te bezien of gestelde belangen daarmee overeenkomen en (c) ook werkelijk worden behartigd door de verwerking en (d) of deze gerechtvaardigd zijn. Het primaat voor het afwegen of voor een gegevensverwerking een gerechtvaardigd belang bestaat ligt dus bij de verwerkingsverantwoordelijke. Zonder dat in de uitspraak van de Afdeling letterlijk wordt gesproken over bewijslast, legt dat oordeel in essentie de bewijslast voor de stelling dat géén sprake is van een gerechtvaardigd belang bij de AP. Hoewel dit op zichzelf een logische uitkomst is, is het een verhelderend en belangrijk punt in deze uitspraak (nu de bewijslast dus niet was af te leiden uit de 3-stappentoets). Dit is de eerste keer dat in de rechtspraak zo duidelijk een standpunt wordt ingenomen over de rol van de AP bij de beoordeling van de vraag of een gerechtvaardigd belang aanwezig is.

Ondanks dit duidelijke standpunt, blijven er nog wel een aantal belangrijke vragen openstaan. Onduidelijk is bijvoorbeeld waarom VoetbalTV zou moeten stellen dat zij naar de door haar genoemde belangen bij de verwerking van persoonsgegevens moet handelen (stelling 3 die VoetbalTV naar voren zou moeten brengen). Daarnaast komen de drie onderwerpen die VoetbalTV zou moeten

4 Zie hierover onder meer HvJ EU 29 juli 2019, C-40/17, ECLI:EU:C:2019:629 (*Fashion ID*); recent hanteerde ook de rechtbank Amsterdam deze toets: Rb. Amsterdam 22 september 2022, ECLI:NL:RBAMS:2022:5565.

stellen niet (volledig) overeen met de vier onderwerpen die de AP vervolgens moet beoordelen volgens het oordeel van de Afdeling. Wat VoetbalTV daadwerkelijk doet hoeft VoetbalTV bijvoorbeeld niet te stellen, maar dient de AP wel te beoordelen. Voor de vraag of de verwerking noodzakelijk is geldt weer dat VoetbalTV dit moet stellen, maar dat de AP dit niet hoeft te beoordelen. Hoe dit in de praktijk zou moeten werken, wordt met het oordeel van de Afdeling dus nog niet helemaal duidelijk.

Voor de inhoudelijke toets voert VoetbalTV – zoals hiervoor toegelicht – een aantal belangen aan die niet uitsluitend commerciële belangen zijn (vergroten van het spelplezier etc.). Die belangen heeft de AP niet meegewogen in de besluitvorming. Uit de uitspraak volgt niet dat de AP betwistte dat de andere door VoetbalTV genoemde belangen niet zouden zijn meegewogen in de besluitvorming of überhaupt dat die belangen meegewogen zouden moeten worden, bijvoorbeeld door te stellen dat VoetbalTV niet naar die andere door VoetbalTV genoemde belangen handelt. Het niet betwisten van de AP van deze punten, leidt ertoe dat in dit geschil vaststaat dat VoetbalTV ook andere belangen had bij de verwerking van persoonsgegevens op basis van de grondslag gerechtvaardigd belang en dat de AP die belangen niet heeft meegewogen bij haar besluitvorming. Het niet meenemen van die belangen in de besluitvorming is een onzorgvuldigheid, gelet op het oordeel van de Afdeling over de verdeling van verantwoordelijkheden tussen AP en verwerkingsverantwoordelijke. De Afdeling komt dan ook tot de conclusie dat de AP bij de eerste stap van de 3-stappentoets op onjuiste gronden heeft vastgesteld dat VoetbalTV in strijd met artikel 6, eerste lid, onderdeel f van de AVG heeft gehandeld. De andere twee stappen van de 3-stappentoets zijn niet uitgevoerd. De bestuurlijke boete die de AP had opgelegd, kan dan ook niet in stand blijven.

Gelet op het voorgaande, komt de Afdeling aan het beantwoorden van de grote vraag in deze procedure – namelijk wanneer sprake is van een zuiver commercieel belang en of een zuiver commercieel belang als 'gerechtvaardigd belang' kan worden aangemerkt – niet toe. Kennelijk ziet de Afdeling ook geen aanleiding om volledigheidshalve deze vraag toch nog te beantwoorden voor de praktijk (hetgeen de Afdeling in sommige andere gevallen wel doet, in een zogenaamd *obiter dictum*). Dat is jammer, omdat er veel behoefte bestaat aan duidelijkheid op dit punt, maar het is niet onlogisch dat de Afdeling deze vraag niet beantwoordt: de door VoetbalTV aangedragen belangen zijn volgens de Afdeling niet louter commercieel van aard (r.o. 8).

De Afdeling ziet aanleiding om de uitspraak van de rechtbank in stand te laten, maar legt aan de uitkomst van die uitspraak wel een andere motivering ten grondslag. De rechtbank in eerste aanleg oordeelde wel inhoudelijk over de standpunten van beide partijen. Voor de praktijk is die inhoudelijke discussie nog steeds relevant en daarom zal ik aan die discussie ook aandacht besteden.

Voor het standpunt van VoetbalTV, namelijk dat de zogenaamde 'negatieve toets' moet worden uitgevoerd, waarbij wordt bekeken of het belang niet in strijd is met een wettelijke norm, zag de rechtbank een aantal aanknopingspunten. Dit standpunt is onder meer terug te vinden in de opinie van de 'Groep Gegevensbescherming Art. 29' (WP29, de voorloper van de *European Data Protection Board*), waarin afgevaardigden zitten van de nationale autoriteiten, over de grondslag 'gerechtvaardigd belang'.

Uit die WP29-opinie volgt dat de grondslag 'gerechtvaardigd belang' een breed scala aan belangen kan omvatten. Deze opinie is opgesteld om de 'gerechtvaardigd belang'-grondslag in de Privacyrichtlijn (95/46/EG) te duiden. Die richtlijn geldt niet meer, maar met de inwerkingtreding van de AVG (die de Privacyrichtlijn op 25 mei 2016 verving) heeft dit advies zijn relevantie niet verloren, omdat de grondslag 'gerechtvaardigd belang' inhoudelijk gelijk in de AVG is opgenomen.

Daarnaast verwijst de rechtbank naar de conclusie van advocaat-generaal M. Bobek bij het *Fashion ID*-arrest.[5] In die conclusie stelt Bobek onder meer dat het verzamelen en het doorzenden van persoonsgegevens om zo goed mogelijk reclame te kunnen maken (zoals in het *Fashion ID*-arrest onderwerp van geschil was), een gerechtvaardigd belang zou kunnen zijn. In het *Fashion ID*-arrest zelf wordt geen aandacht besteed aan welke belangen er als 'gerechtvaardigd belang' kunnen worden aangemerkt.

Naast deze twee aanknopingspunten die de rechtbank aanhaalt, stelt ook de Europese Commissie (EC) zich op het standpunt dat het gerechtvaardigd belang niet zo beperkt moet worden uitgelegd als de AP doet in de brief die de EC op 6 maart 2020 aan de AP stuurde. De EC stelt daarin zich zorgen te maken over de strikte interpretatie van 'gerechtvaardigd belang', die de AP hanteert in de Normuitleg grondslag 'gerechtvaardigd belang'. De EC acht deze interpretatie niet in lijn met de AVG en verzoekt de AP de Normuitleg aan te passen. Deze brief van de EC en het antwoord van de AP op die brief bieden een nuttig inzicht in de argumenten in deze discussie.

De EC wijst op het *Rigas satiksme*-arrest van het HvJ EU[6] – waarnaar A-G Bobek in zijn eerder aangehaalde conclusie overigens ook verwijst – waarin het HvJ EU oordeelde dat het belang van een derde bij het verkrijgen van persoonsgegevens van een persoon die schade aan de eigendommen van de derde had veroorzaakt als gerechtvaardigd belang kon worden gezien, terwijl die derde een puur economisch belang had: namelijk het aansprakelijk stellen van de betreffende persoon. Dit arrest ziet

5 Concl. A-G M. Bobek 19 december 2018, C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*).
6 HvJ EU 4 mei 2017, C-13/16, ECLI:EU:C:2017:336 (*Rigas satiksme*).

op de interpretatie van het 'gerechtvaardigd belang' onder de Privacyrichtlijn (Richtlijn 95/46/EG), die op 25 mei 2018 door de AVG is vervangen.

Ook wijst de EC in de brief aan de AP op de 'vrijheid van ondernemerschap' zoals vastgelegd in artikel 16 van het Handvest van de Grondrechten van de Europese Unie (EU-Handvest). De EC stelt dat een zuiver commercieel belang, zoals winstmaximalisatie, onder dit recht valt. De EC benoemt overweging 4 en 47 bij de AVG, waaruit volgt dat het recht op bescherming van persoonsgegevens geen absoluut recht is en de verwerking van persoonsgegevens ten behoeve van *direct marketing* kan worden beschouwd als uitgevoerd met het oog op een gerechtvaardigd belang. Aan het eind van de brief merkt de EC nog op dat de strikte interpretatie van de AP de mogelijkheden voor ondernemers om persoonsgegevens te verwerken voor commerciële doeleinden ernstig beperkt en dat met die strikte interpretatie naar de mening van de EC geen gerechtvaardigde belangenafweging wordt gemaakt tussen het recht op bescherming van persoonsgegevens aan de ene kant en de vrijheid van ondernemerschap aan de andere kant.

De AP heeft hierop gereageerd bij brief d.d. 31 augustus 2022, waarin de AP de EC verzoekt om een gesprek en vooruitlopend op dat gesprek vast een aantal argumenten ter onderbouwing van zijn standpunt benoemt. De AP stelt dat de grondslag gerechtvaardigd belang in het licht van artikel 8 en 52 van het EU-Handvest zo moet worden geïnterpreteerd dat op het recht op bescherming van persoonsgegevens slechts inbreuk mag worden gemaakt als daarin is voorzien bij wet (en ook aan de overige waarborgen uit artikel 52 van het EU-Handvest wordt voldaan). Daarbij stelt de AP het oneens te zijn met de interpretatie van de HvJ EU-rechtspraak door de EC. De AP stelt onder meer dat in het *Rigas stiksme*-arrest niet slechts een economisch belang aan de orde was, maar ook het recht om schade te verhalen, die de veroorzaker van de schade verplicht is te vergoeden. Ook merkt de AP op het niet eens te zijn met het standpunt van de EC dat 'winstmaximalisatie' onder het recht op vrijheid van onderneming uit artikel 16 EU-Handvest zou moeten worden gevat.

Deze antwoordbrief geeft een duidelijker beeld van de onderbouwing van het standpunt van de AP dan in de uitspraak van de Afdeling naar voren komt. De AP vindt dus dat artikel 6, eerste lid, onderdeel f van de AVG onvoldoende wettelijke basis vormt om een inbreuk op de bescherming van persoonsgegevens te rechtvaardigen. Het ligt voor de hand dat de AP deze onderbouwing ook in de *VoetbalTV*-procedure naar voren heeft gebracht, maar dit komt in de uitspraken (in eerste aanleg en in hoger beroep) niet terug. Het is natuurlijk praktisch dat bestuursrechtelijke uitspraken kort en bondig zijn, maar in dit geval lijkt het er toch op dat een relevant gedeelte van de onderbouwing van het standpunt van de AP in de uitspraken niet wordt gereflecteerd.

Zowel de brief van de EC als het antwoord daarop van de AP zijn door *NRC* gepubliceerd (op de website van *NRC*).

De juridische discussie over het gerechtvaardigd belang wordt ondertussen vervolgd in de bestuursrechtelijke procedure die de Koninklijke Nederlandse Lawn Tennis Bond (KNLTB) is gestart tegen een boetebesluit van de AP, waarin de AP een vergelijkbaar standpunt in heeft genomen over de reikwijdte van het 'gerechtvaardigd belang'. In die situatie had de AP de 'volledige drie stappentoets' wel uitgevoerd. Na de uitspraak in hoger beroep in de *VoetbalTV*-zaak, werd door de rechtbank Amsterdam de tussenuitspraak van 22 september 2022 gepubliceerd in de *KNLTB*-zaak. Uit die tussenuitspraak blijkt dat de rechtbank Amsterdam prejudiciële vragen heeft gesteld aan het HvJ EU, waaronder de vraag hoe de term 'gerechtvaardigd belang moet worden uitgelegd en specifiek of een 'zuiver commercieel belang' onder omstandigheden kan worden aangemerkt als een gerechtvaardigd belang. Voor een nadere toelichting hierop verwijs ik graag naar de eerder genoemde bijdrage van mr. S.E.A. Vermeer-de Jongh en mr. E.W.S. Peperkamp in dit nummer.

De antwoorden op die vragen zullen ongetwijfeld nog een tijd op zich laten wachten, maar met het stellen van deze prejudiciële vragen, zal voor de praktijk dan toch duidelijkheid worden geschept.

Gevolgen voor VoetbalTV

Voor VoetbalTV had deze (naar nu blijkt onrechtmatige) bestuurlijke boete vergaande consequenties. Deze vormde namelijk een belangrijke aanleiding voor het faillissement van VoetbalTV dat op 11 september 2020 is uitgesproken. Inmiddels is dit faillissement weer opgeheven na een schuldeisersakkoord.

Of VoetbalTV haar bedrijfsactiviteiten zal hervatten is nog niet bekend. Daarvoor is ook relevant dat met de onderhavige uitspraak niet vaststaat dat de verwerking van persoonsgegevens door VoetbalTV rechtmatig is. In de onderhavige situatie kwam de AP al bij de eerste stap van de 3-stappentoets tot de conclusie dat geen persoonsgegevens zouden mogen worden verwerkt op grond van de grondslag 'gerechtvaardigd belang', waarbij de AP niet alle door VoetbalTV genoemde belangen meewoog, terwijl alle door de verwerkingsverantwoordelijke gestelde belangen in die stap moeten worden betrokken en de toets of persoonsgegevens mogen worden verwerkt op basis van de grondslag 'gerechtvaardigd belang' nog twee stappen kent. Mogelijk leidt die toets er alsnog toe dat VoetbalTV geen persoonsgegevens mag verwerken op basis van de grondslag 'gerechtvaardigd belang'.

Evenmin is bekend of er van de zijde van VoetbalTV nog een vervolg zal worden gegeven aan deze uitspraak, nu hiermee de onrechtmatigheid van het boetebesluit (dat de basis vormde voor het faillissement van VoetbalTV) is gegeven, is niet uitgesloten dat VoetbalTV bijvoorbeeld

een schadevergoedingsvordering bij de AP indient. Dit zal mogelijk ook afhangen van VoetbalTV's eigen analyse over de vraag of zij onrechtmatig persoonsgegevens heeft verwerkt (hetgeen ook afhankelijk is van de laatste twee stappen uit de niet-uitgevoerde 3-stappentoets).

Boekbespreking

Privacy in de zorg

Mr. dr. J. Nouwt[*]

282

Bespreking van: Sophie Hendriks, Ivette Janssen, Barbara Krol, Jurriaan Dane, Martin Hemmer, René Huigen & Ruben Tienhooven, *Privacy in de zorg. Een praktische gids voor zorgverleners, managers en juristen.* Amsterdam: Berghauser Pont Publishing 2022, 232 p., ISBN: 9789492952622, € 59,50.

In de zomer van 2022 verscheen het boek *Privacy in de zorg* bij uitgeverij Berghauser Pont. Het boek is geschreven door zeven auteurs met verschillende achtergronden. Een aantal van hen is advocaat, een aantal is werkzaam als jurist bij een ziekenhuis en een aantal van hen is consultant op het terrein van privacy en informatiebeveiliging. Hieronder schets ik wat de lezer kan verwachten aan inhoudelijke informatie en plaats ik enkele positieve en kritische kanttekeningen daarbij.

Na een algemene inleiding in hoofdstuk 1, worden in hoofdstuk 2 de Algemene verordening gegevensbescherming (AVG) en Uitvoeringswet AVG (UAVG) besproken. Daarin wordt het algemene kader over de toepasselijkheid van de AVG uitgelegd, inclusief de belangrijkste vereisten en definities, zoals die van persoonsgegevens, pseudonimisering en bijzondere persoonsgegevens. Maar ook kernbegrippen als de verwerkingsverantwoordelijke en verwerker en het datalek. Daarnaast schetst dit hoofdstuk de beginselen waar iedere verwerking van persoonsgegevens aan moet voldoen, verplichtingen van de verwerkingsverantwoordelijke, de rechten van betrokkenen uit AVG en UAVG, de grondslagen voor gegevensverwerkingen en de uitzonderingen op het verwerkingsverbod voor bijzondere persoonsgegevens.

In hoofdstuk 3 komen het medisch beroepsgeheim en de mogelijke uitzonderingen daarop aan bod. Het bevat een uiteenzetting van de reikwijdte en inhoud van het medisch beroepsgeheim. Maar ook worden verschillende situaties besproken die zich voor kunnen doen in de praktijk van een zorgaanbieder en waarbij persoonsgegevens over iemands gezondheid kunnen worden gedeeld met anderen, zoals in de samenwerking met andere zorgaanbieders. Een overzicht van gronden om het beroepsgeheim te mogen doorbreken en grondslagen en uitzonderingsgronden voor verwerking van (bijzondere) persoonsgegevens uit de AVG is te vinden in Bijlage 1 van het boek. Ook de rechten van betrokkenen ten aanzien van de verwerking van hun persoonsgegevens in medische dossiers worden in dit hoofdstuk besproken.

Vervolgens wordt in hoofdstuk 4 speciale aandacht besteed aan de elektronische uitwisseling van gezondheidsgegevens bij samenwerking tussen zorgaanbieders. Dit vindt plaats in een ingewikkeld en complex juridisch terrein van civielrechtelijke relaties tussen samenwerkende zorgaanbieders en cliënten. De complexiteit wordt mede veroorzaakt door het feit dat de Wet geneeskundige behandelingsovereenkomst (Wgbo) dateert uit 1995 en een onderdeel is van het Burgerlijk Wetboek (BW), dat er van uitgaat dat een geneeskundige behandelingsovereenkomst tot stand komt tussen een hulpverlener en een patiënt. De Wgbo is niet afgestemd op de groeiende variëteit aan samenwerkingsverbanden in de zorg en sluit ook niet goed meer aan bij nieuwere wet- en regelgeving, zoals de Wet kwaliteit, klachten en geschillen in de zorg (Wkkgz), de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) en het wetsvoorstel Wet elektronische gegevensuitwisseling in de zorg (Wegiz). In combinatie met de AVG en UAVG mag daarom met recht worden gesproken van een ingewikkeld stelsel van wet- en regelgeving.

Het hoofdstuk bespreekt de verschillende manieren waarop gegevens kunnen worden uitgewisseld tussen zorgaanbieders onderling en tussen zorgverleners en cliënten. Ook de landelijke ontwikkelingen, zoals de onlinetoestemmingsvoorziening Mitz,[1] voor de registratie van toestemming voor gegevensuitwisseling, komen aan bod, evenals de ervaringen die zijn opgedaan met specifieke regelgeving voor elektronische gegevensuitwisseling, zoals de Wabvpz. Die wet bevat een aantal digitale patiëntenrechten, die ook in dit hoofdstuk worden besproken. Voorts wordt kort ingegaan op het wetsvoorstel Wegiz die verplichtingen voor elektronische uitwisselingen van gezondheidsgegevens bevat. Bijlage 3 van het boek bevat een checklist waarmee kan worden nagegaan welke privacyaspecten spelen bij samenwerkingsvormen tussen zorgaanbieders.

Hoofdstuk 5 bespreekt de mogelijkheden die het wettelijk kader biedt om medische gegevens te gebruiken voor wetenschappelijk onderzoek. Daarbij komen achtereenvolgens aan bod: de AVG, UAVG, de Wet medisch-wetenschappelijk onderzoek met mensen (WMO), de Wgbo en de Gedragscode Gezondheidsonderzoek. Het

---

* Sjaak Nouwt is werkzaam als zelfstandig privacy-adviseur en als beleidsadviseur gezondheidsrecht bij de artsenfederatie KNMG, gespecialiseerd in privacy- en gezondheidsrecht. Hij is tevens hoofdredacteur van *Privacy & Informatie*. Deze bijdrage is op persoonlijke titel geschreven.

1 vzvz.nl/diensten/gemeenschappelijke-diensten/mitz.

hoofdstuk sluit af met een stappenplan waarmee kan worden bepaald welke wetgeving van toepassing is en of een medisch-ethische toetsing verplicht is.

In hoofdstuk 6 wordt ingegaan op eHealth. Dat is een onderwerp dat een grote diversiteit kent aan ICT-toepassingen in de zorg. In navolging van de indeling die de Inspectie voor Gezondheidszorg en Jeugd (IGJ) hanteert, bespreken de auteurs de privacyrechtelijke aspecten van toepassingen voor cliënten, ter ondersteuning van zorgverleners en systemen die helpen bij medische beslissingen, waaronder medische apps. Toepassingen voor cliënten zijn bijvoorbeeld persoonlijke gezondheidsomgevingen (PGO's), online communicatie tussen cliënten en zorgverleners en gezondheidsapps. Tevens wordt aandacht besteed aan medische hulpmiddelen, kunstmatige intelligentie (AI) en big data. Besproken wordt waar een gebruiker van eHealth-toepassingen bij stil moet staan alvorens een toepassing in gebruik te nemen. Toepassingen ter ondersteuning van zorgverleners worden ook in hoofdstuk 4 behandeld.

Daarna wordt in hoofdstuk 7 stilgestaan bij het onderwerp informatiebeveiliging. De AVG stelt algemene beveiligingseisen aan de verwerking van persoonsgegevens. Bij informatiebeveiliging draait het om het treffen van maatregelen die ervoor moeten zorgen dat persoonsgegevens vertrouwelijk, integer en beschikbaar blijven (de 'CIA' van Confidentiality, Integrity, en Availability). In wetgeving op het gebied van informatiebeveiliging in de zorg worden specifieke aanvullende eisen gesteld die in ons land nader uitgewerkt zijn in een aantal NEN-normen. Besproken wordt hoe daaraan voldaan kan worden en dat naast technische maatregelen ook organisatorische maatregelen van belang zijn om gegevens adequaat te beschermen, maar tevens de informatiesystemen en applicaties. Ook wordt in dit hoofdstuk uitgebreider dan in hoofdstuk 4 ingegaan op het wetsvoorstel Wegiz, dat zich op het moment van publicatie van dit boek in de voorbereidende fase bevindt.

Hoofdstuk 8 bespreekt de handhaving van de naleving van de AVG, waar zorgaanbieders mee kunnen worden geconfronteerd. Een verwerkingsverantwoordelijke moet kunnen aantonen dat hij de AVG naleeft. De handhaving daarvan en controle daarop vindt plaats door de Autoriteit Persoonsgegevens (AP). Maar ook de Nederlandse Zorgautoriteit (NZa), de Inspectie Gezondheidszorg en Jeugd (IGJ) en de Autoriteit Consument en Markt (ACM) houden toezicht op de naleving van wetgeving in de zorgsector. De verhouding tussen deze toezichthouders komt in dit hoofdstuk aan bod. Ook worden boetes behandeld die de AP in 2019 en 2020 oplegde aan het HagaZiekenhuis en aan het OLVG. In beide gevallen werd de tweefactorauthenticatie voor de toegang tot het ziekenhuisinformatiesysteem niet goed toegepast en werden de logbestanden onvoldoende gecontroleerd door de ziekenhuizen.

In het afsluitende hoofdstuk 9 wordt ten slotte kort stilgestaan bij verwachte toekomstige ontwikkelingen. Terecht wijzen de auteurs in de inleiding bij dit hoofdstuk op de snel veranderende wereld, in het bijzonder de veranderingen van technische en juridische realiteit. Daarmee geven de auteurs aan dat de inhoud van hun boek al snel kan worden ingehaald door de voortgaande ontwikkelingen op dit terrein. Zij wijzen daarvoor zelf al naar een aantal ontwikkelingen vanuit de EU, zoals het voorstel voor een verordening voor een Europese ruimte voor gezondheidsgegevens (EHDS), de digitale diensteninfrastructuur voor e-Gezondheidszorg (eHDSI) en Europese Referentienetwerken (ERN's) oftewel virtuele adviespanels van medisch specialisten. Ook noemen de auteurs (opnieuw) de Wegiz die momenteel aanhangig is in de Eerste Kamer. Tot slot wijzen zij op de digitalisering als oplossing om de zorg in de toekomst werkbaar en betaalbaar te kunnen houden. Zij verwachten daarbij veel van AI-toepassingen in de zorg en van zelflerende zorgrobots.

De auteurs hebben geprobeerd om het boek te laten aansluiten bij de praktijk door regelmatig voorbeelden en tips te vermelden. Daarnaast gebruiken zij een centrale casus in de vorm van een cliënt met een zorgvraag waar meerdere deelonderwerpen van dit boek op van toepassing zijn. Bij ieder relevant deelonderwerp staan de auteurs stil bij de vraag: wat betekent dit voor Robin? Gedurende het boek komt Robin, die last heeft van fors overgewicht en hartkloppingen, in verschillende situaties terecht waarbij sprake is van verwerking van zijn gezondheidsgegevens. Samen met de tips en voorbeelden, geeft deze casus als rode draad handvatten voor de toepassing van de regels voor gegevensbescherming in de praktijk.

Er zijn ook enkele kritische inhoudelijke kanttekeningen te maken bij het boek. Zo wordt er in een aantal voetnoten in hoofdstuk 2 verwezen naar oude adviezen van de WP29-werkgroep (1/2010 en WP259). Deze zijn inmiddels vervangen door nieuwe richtsnoeren van de EDPB (07/2020 resp. 05/2020).

In hoofdstuk 3 stellen de auteurs dat huisartsen op een huisartsenpost (HAP) als vervangers van de eigen huisarts worden beschouwd, waardoor zij via het Landelijk Schakelpunt (LSP) toegang hebben tot een deel van het dossier van een cliënt bij de eigen huisarts, tenzij de cliënt daar bezwaar tegen heeft gemaakt. Mijns inziens gaan de auteurs daarbij voorbij aan de bijzondere eis van uitdrukkelijke toestemming die artikel 15a Wabvpz voorschrijft, voordat de eigen huisarts dat dossier digitaal toegankelijk mag maken voor raadpleging door de HAP. Dit is een bijzondere toestemming, los van AVG of Wgbo, die zorgaanbieders van hun patiënten moeten hebben gekregen, voordat zij andere zorgaanbieders toegang mogen verlenen tot hun patiëntendossiers of tot onderdelen daarvan.

In hetzelfde hoofdstuk bespreken de auteurs de verstrekking van gegevens aan vertegenwoordigers van meerderjarige wilsonbekwame patiënten. Daarbij stellen zij dat een wettelijke vertegenwoordiger niet per definitie recht op inzage en afschrift van informatie uit het dossier van wilsonbekwame patiënt heeft, maar alleen als dit nodig is om toestemming te geven. Hoewel het onderscheid subtiel is, lijken de auteurs daar het recht op inzage en afschrift (art. 7:456 BW) ten onrechte niet te onderscheiden van het recht op informatie om op basis

daarvan toestemming te kunnen geven voor een medische verrichting (art. 7:448 en 450 BW). Een zorgaanbieder moet aan wettelijke vertegenwoordigers wel de informatie verschaffen die nodig is om toestemming voor een medische verrichting te kunnen geven, maar dat is iets anders dan het tegemoetkomen aan het recht op inzage of afschrift van persoonsgegevens.

In hoofdstuk 5 staat dat patiënten en cliënten via toestemmingsformulieren toestemming kunnen geven, zoals bedoeld in artikel 6 en 9 AVG, voor het verwerken van hun persoonsgegevens voor medisch-wetenschappelijk onderzoek. En dat dit in de toekomst wellicht ook mogelijk is via persoonlijke gezondheidsomgevingen (PGO's). In een voetnoot wordt uitgelegd dat een PGO een website of een app is waar patiënten toegang hebben tot hun eigen gezondheidsgegevens. Een PGO is echter iets anders dan een patiëntenportaal. Een patiëntenportaal kan ook bestaan uit een website of app, aangeboden door een zorgaanbieder, waarmee patiënten toegang hebben tot hun eigen gezondheidsgegevens die de zorgaanbieder (ziekenhuis, huisarts, e.d.) in elektronische patiëntendossiers over die patiënten hebben vastgelegd. Een PGO wordt daarentegen beheerd door een patiënt, die zelf bepaalt welke informatie hij daarin vastlegt en wie hij daar toegang toe verleent. De uitleg in de voetnoot kan daardoor verwarring wekken.

Tot slot viel mij op dat de auteurs in hun conclusie de verwachting uitspreken dat de komende decennia de privacyrechtelijke kaders in de kern overeind zullen blijven. Dat is dan echter wel buiten de plannen gerekend van minister Kuipers van Volksgezondheid, Welzijn en Sport, om de grondslagen voor gegevensuitwisseling in de zorg grondig te herzien.[2] De minister wil daar vanaf 2023 een begin mee maken. Dat toont aan dat het boek mogelijk al op korte termijn een inhoudelijke actualisering behoeft. Dat past dan weer wel in de technische en juridische veranderingen waar de auteurs zichzelf ook van bewust zijn (zie hierboven). Desondanks is een compliment op zijn plaats voor de auteurs, gelet op de positieve waarde die dit boek volgens mij kan hebben als praktische gids in het juridisch complexe gebied van privacybescherming in de zorg.

2 Kamerbrief minister Kuipers, 9 mei 2022 over de herijking van grondslagen voor gegevensuitwisseling in de zorg: *Kamerstukken II, 2021/22, 27 529, nr. 276* (Informatie- en Communicatietechnologie (ICT) in de zorg).

Privacy Algemeen

283

Europese toezichthouders vragen om aanvulling AVG

De Europese privacytoezichthouders willen dat de Europese Commissie nieuwe regels maakt in aanvulling op de Algemene verordening gegevensbescherming (AVG), om de samenwerking tussen toezichthouders in internationale zaken te verbeteren. Dat schrijven zij in een brief aan de Europese Commissie. De Autoriteit Persoonsgegevens (AP) en de rest van de Europese privacytoezichthouders, verenigd in de European Data Protection Board (EDPB), vragen de Europese Commissie om nieuwe regels, om verduidelijking van bestaande regels of om het gelijktrekken van regels over procedures die nu nog verschillen per Europese lidstaat. Het gaat om aanvullende regels op veertien punten. Waaronder duidelijkheid over de rechten van mensen die een klacht indienen, criteria voor het in behandeling nemen van klachten, deadlines voor het behandelen van zaken, de manier waarop zaken kunnen worden afgesloten, onderzoeksbevoegdheden en het publiceren van besluiten.

Wanneer de regels in verschillende Europese landen beter op elkaar worden afgestemd, kunnen de Europese toezichthouders efficiënter samenwerken.

Aanleiding voor de brief zijn onder andere bijeenkomsten van de toezichthouders in Wenen en Brussel dit voorjaar. Daar werd gesproken over het versterken van handhaving van de AVG in internationale zaken en de noodzaak om samenwerking te verbeteren.

Het vaststellen van de procedurele obstakels was een van de concrete actiepunten uit het statement dat in Wenen is aangenomen.

In het huidige systeem werken EU-toezichthouders samen in internationale zaken. Dat zijn zaken die burgers in meerdere lidstaten van de Europese Unie raken. De samenwerking is geregeld in het een-loket-mechanisme in de AVG.

Die samenwerking kan beter, omdat elke toezichthouder zijn zaken behandelt volgens zijn nationale procedurele recht, dat per lidstaat verschilt. Dat zorgt soms voor vertraging of zorgt ervoor dat klachten in de ene lidstaat anders worden behandeld dan in de andere lidstaat. (CE)

Bronnen: edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-eu-commission-procedural-aspects-could-be_en

Nieuwsbericht Autoriteit Persoonsgegevens 12 oktober 2022, autoriteitpersoonsgegevens.nl

284

EDPB publiceert aangepaste versie richtsnoeren datalekken

De EDPB heeft een aangepaste versie van de richtsnoeren over datalekken ter consultatie voorgelegd. De belangrijkste wijziging ten opzichte van de vorige versie betreft de meldplicht voor bedrijven die geen vestiging in de EU hebben, maar wel onder de AVG vallen. Deze bedrijven dienen voortaan datalekken te melden bij alle toezichthouders van de landen waar betrokkenen door het lek zijn geraakt. De vorige versie van de richtsnoeren bepaalde nog dat deze bedrijven een datalek alleen moeten melden bij de toezichthouder van de lidstaat waar hun EU-vertegenwoordiger zit. De EDPB licht toe dat deze wijziging is aangebracht om de meldingsplicht voor datalekken onder de AVG in lijn te brengen met het one-stop-shopprincipe waarbij organisaties die grensoverschrijdende verwerkingen uitvoeren, maar met één privacytoezichthouder zaken hoeven te doen. Dat one-stop-shopprincipe geldt immers ook niet voor bedrijven die geen EU-vestiging hebben. De consultatieperiode van de nieuwe versie van de richtsnoeren loopt tot 29 november 2022. (NW)

Bron: edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf

285

EDPB publiceert concept-Richtsnoeren over de leidende autoriteit

Op 10 oktober 2022 heeft de EDPB richtsnoeren over hoe de leidende autoriteit te bepalen voor verwerkingsverantwoordelijke en verwerker ter consultatie voorgelegd (08/2022). Met deze richtsnoeren wordt de eerdere publicatie van de Artikel 29-werkgroep over dit onderwerp (WP244 rev.01) goedgekeurd. De EDPB heeft, naast wat tekstuele wijzigingen, een paragraaf over gezamenlijk verantwoordelijken toegevoegd. Gezamenlijke verantwoordelijken kunnen niet zelf een hoofdvestiging kiezen die voor beide gezamenlijke verantwoordelijken geldt voor de verwerkingen die zij gezamenlijk uitvoeren. Dit volgt uit het begrip 'hoofdvestiging' dat immers uit hoofde van de AVG voor een enkele verwerkingsverantwoordelijke geldt. Dit kan niet vervolgens worden uitgebreid voor een situatie van gezamenlijke verwerkingsverantwoordelijkheid. De consultatie is open tot 2 december 2022. (NW)

Bron: edpb.europa.eu/system/files/2022-10/edpb_guidelines_202208_identifyinglsa_targetedupdate_en.pdf

286

EDPS-informatiepagina over machinelearning

In het licht van het toenemende gebruik van machinelearning in alledaagse apparaten en diensten, publiceerde de EDPS samen met de Spaanse autoriteit (AEPD) een kort document getiteld: '10 misunderstandings about machine learning'. Machinelearning is een bijzondere vorm van kunstmatige intelligentie die wordt gebruikt om specifieke problemen op te lossen, zoals classificeren en voorspellen, bijvoorbeeld in sociale media, virtuele personal assistants en zelfrijdende auto's. Hiertoe worden modellen voor ma-

chinelearning getraind met behulp van relatief grote hoeveelheden gegevens. De resultaten van machinelearning zijn sterk afhankelijk van de nauwkeurigheid en representativiteit van de gebruikte gegevens. In de publicatie trachten de EDPS en AEPD enkele misverstanden uit de weg te ruimen en veelvoorkomende vragen te beantwoorden. Met name dan dat machinelearningsystemen zogenaamd minder onderhevig zouden zijn aan menselijke vooroordelen (dat zijn ze wel) en hoe nauwkeurig en kwalitatief de gegevens moeten zijn die gebruikt worden om machinelearningsystemen te trainen. (JA)

Bron: edps.europa.eu/system/files/2022-09/22-09-20_10-misunderstandings-on-machine-learning_en.pdf

287

EDPS en EDPB in open brief: 'Gebrek aan middelen brengt handhaving van individuele rechten op gegevensbescherming in gevaar'

De voorzitters van de EDPB (Andrea Jelinek) en EDPS (Wojciech Wiewiórowski) stellen in een open brief gericht aan het Europees Parlement en de Raad, dat ze zich bijzonder zorgen maken over de begroting van 2023. Indien deze niet aanzienlijk verhoogd wordt, aldus de voorzitters, kunnen hun respectievelijke organisaties hun taken niet naar behoren uitvoeren. Tijdens de voorbereiding van de algemene begroting van de EU 2023 heeft de EDPS twee opeenvolgende begrotingsvoorstellen bij de Europese Commissie ingediend met het verzoek om meer personeel en financiële middelen, zodat de EDPB en de EDPS hun groeiende takenpakket en toenemende werklast kunnen beheren. De gevraagde verhoging werd door de Europese Commissie afgewezen. (JA)

Bron: edps.europa.eu/press-publications/press-news/press-releases/2022/edpb-edps-lack-resources-puts-enforcement-individuals-data-protection-rights-risk_en

288

Hof van Justitie specificeert recht op vergetelheid

In een arrest van 17 oktober werpt het Hof licht op de verdeling van verantwoordelijkheden betreffende het recht op gegevenswissing ('recht op vergetelheid') in artikel 17 van de AVG. De onderliggende zaak betrof de Belgische telecomprovider Proximus, die niet voldoende maatregelen had genomen om persoonsgegevens uit een publieke telefoongids te halen. Het Hof oordeelde dat voor het opnemen van persoonsgegevens in publiek beschikbare telefoongidsen, de operator van telefoondiensten de toestemming van de abonnee moet bekomen. Wanneer die toestemming wordt ingetrokken, kan de verwerkingsverantwoordelijke verplicht worden om passende technische en organisatorische maatregelen te nemen om derde verwerkingsverantwoordelijken te informeren over die intrekking. Het gaat hier dan in het bijzonder om de operator van telefoondiensten die de persoonsgegevens van haar abonnees verstrekte en andere aanbieders van publiek beschikbare telefoongidsen en telefooninlichtingendiensten aan wie de gegevens werden verstrekt. Daarenboven kan artikel 17(2) van de AVG ook worden gebruikt om de respectievelijke aanbieder van publieke telefoongidsen verantwoordelijk te stellen 'redelijke maatregelen' te nemen om zoekmachines in te lichten over het verzoek tot gegevenswissing. (JA)

Bron: eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0129

289

Smart meters vallen onder ePrivacyrichtlijn

In het kader van energiebesparingen en klimaatbescherming werd in 2019 reeds Richtlijn 2019/944 aangenomen betreffende onder andere de uitrol van slimme meters. Een slim metersysteem is een elektronisch apparaat dat energieverbruik meet en verbruiksgegevens uitwisselt met energieleveranciers en -diensten om het gebruik van elektriciteit te monitoren. Hoewel het een nuttig energiebesparingsinstrument kan zijn, houdt het uiteraard ook risico's in voor de bescherming van de persoonsgegevens, aangezien het patronen en precieze details over iemands privéleven kan onthullen (bv. wanneer iemand op vakantie is, of zelfs welke apparaten op welke momenten gebruikt worden).

De EDPB heeft formeel opmerkingen gemaakt bij de Commissie over de uitvoeringsverordening betreffende de toegang tot meet- en elektriciteitsverbruiksgegevens door energieleveranciers en aanverwante diensten. Zo wordt bijvoorbeeld gewezen op het feit dat slimme meters krachtens de e-privacyrichtlijn kunnen worden beschouwd als 'eindapparatuur'. Als zodanig vereist toegang tot informatie die is opgeslagen in een 'eindapparaat' volgens de e-privacyrichtlijn in beginsel de toestemming van de gebruiker, tenzij toegang tot dergelijke informatie strikt noodzakelijk is voor de aanbieder van een dienst van de informatiemaatschappij om de uitdrukkelijk door de gebruiker gevraagde dienst te leveren. (JA)

Bron: edps.europa.eu/system/files/2022-09/22-08-24_access-metering-and-consumption-data_en.pdf

Internationaal

290

De EDPS beveelt Europol om gegevens te wissen

De EDPS beveelt Europol om gegevens over personen zonder bewezen verband met een criminele activiteit te wissen. De EDPS heeft het Hof van Justitie van de Europese Unie (HvJ EU) verzocht twee bepalingen van de onlangs gewijzigde Europolverordening, die op 28 juni 2022 in werking is getreden, nietig te verklaren. De twee bepalingen hebben gevolgen voor reeds door Europol verrichte verwerkingen van persoonsgegevens. Volgens de EDPS ondermijnen deze bepalingen daar-

door de rechtszekerheid voor de persoonsgegevens van personen en bedreigen zij de onafhankelijkheid van de EDPS – de toezichthoudende autoriteit voor gegevensbescherming van de instellingen, organen en instanties van de EU. Kortom worden met de artikelen 74 bis en 74 ter, Europols verwerkingen van grote hoeveelheden persoonsgegevens van personen zonder bewezen verband met criminele activiteiten te verwerken, retroactief gelegaliseerd. Dit soort verwerking van persoonsgegevens is volgens de EDPS in strijd met de Europol-verordening, eerder al duidelijk gemaakt in een besluit van 3 januari 2022, waarin Europol wordt verzocht de betrokken gegevens te wissen. In plaats daarvan werd nu dus door de wetgever beslist dat dit soort gegevensverwerkingen met terugwerkende kracht legaal is, aldus de EDPS. (JA)

Bron: edps.europa.eu/system/files/2022-09/EDPS-2022-23-EDPS-request%20to%20annul%20two%20new%20Europol%20provisions_EN.pdf

291

TikTok geeft toe dat personeel in China data van Europese gebruikers monitort

De Chinese sociale-video-app TikTok heeft zijn privacybeleid aangepast, waarbij nu bevestigd wordt dat medewerkers in landen waaronder China toegang krijgen tot gebruikersgegevens om ervoor te zorgen dat hun ervaring met het platform ‘consistent, plezierig en veilig’ is. De aankondiging zorgt voor heel wat opschudding. In het Nederlandse programma Jinek roept technologie-expert Alexander Klöpping op tot een verbod op TikTok. (JA)

Bron: thebestsocial.media/nl/tiktok-china-verbod-jinek/

292

TikTok past beleid aan: data Nederlanders binnenkort wél naar China

Na jaren van beloftes dat gegevens van Europeanen niet naar China zouden gaan, verandert dat volgende maand alsnog. Vanaf 2 december 2022 krijgt het personeel van TikTok toegang tot de data van Europese gebruikers. De gegevens die worden doorgestuurd gaan onder andere over het kijkgedrag van gebruikers.

De nieuwe voorwaarden komen na jaren van geruchten dat TikTok data zou doorsturen. TikTok ontkende dat in eerste instantie, maar gaf deze zomer al toe dat Chinese medewerkers toegang hebben tot data van in ieder geval Amerikaanse gebruikers. Of de Chinese overheid ook toegang heeft tot die data, wilde een topvrouw in de VS tegenover Amerikaanse senatoren niet zeggen.

Een dataroute naar China is een heikel punt, omdat Europa met China geen data-overeenkomst heeft. China staat niet op de lijst met landen die volgens de EU hun data-bescherming op orde hebben. Men is bang dat data van onder meer minderjarige Europeanen terechtkomen bij de Chinese overheid via het Chinese TikTok-moederbedrijf ByteDance. Wat er vervolgens met die data gebeurt, is niet duidelijk. TikTok ligt vanwege zijn Chinese moederbedrijf en enorme populariteit al langer onder een vergrootglas. De app heeft ruim 1 miljard gebruikers wereldwijd, in Nederland zeker 3 miljoen gebruikers. Daarom startte de Ierse gegevensbeschermingsautoriteit DPC vorig jaar al een onderzoek naar TikTok, en of de gegevens van gebruikers wel op een juiste manier worden verwerkt volgens de AVG. Ierland leidt dat onderzoek omdat het Europese datacenter van TikTok in Ierland staat. Ook de VS doet onderzoek naar TikTok. Onder de vorige president Trump kwam het bijna tot een gedwongen verkoop van TikTok aan een Amerikaans bedrijf. Dat kwam uiteindelijk niet zo ver, maar ook de huidige Amerikaanse president Biden vergroot de afstand tot China. Zijn regering vindt dat het westen te afhankelijk is van China, zeker op technologisch gebied. Nieuwe, verregaande sancties moeten dat veranderen. (TW)

Bron: rtlnieuws.nl/tech/artikel/5344365/tiktok-privacybeleid-data-nederlanders-naar-china

293

Lek schijnt licht op problematische verwerking persoonsgegevens door Frontex

Op 4 november publiceerde Statewatch een reeks documenten over Frontex (het Europees agentschap voor de grens- en kustwacht), betreffende de verwerking van persoonsgegevens voor bestrijding van grensoverschrijdende criminaliteit. Uit de documenten blijkt, aldus Statewatch, hoe Frontex-management het advies van zijn functionaris voor gegevensbescherming (DPO) heeft willen negeren, in navolging van eerdere pogingen om de functionaris voor de grondrechten (FRO) van het agentschap buitenspel te zetten in het schandaal over pushbacks aan de Grieks-Turkse grens en operaties aan de Hongaars-Servische grens. (JA)

Bron: statewatch.org/observatories/frontex/document-collection-frontex-and-operational-personal-data/

294

Belgische overheid lanceert nationale AI-strategie

De federale overheid in België heeft een Nationaal convergentieplan voor de ontwikkeling van artificiële intelligentie voorgesteld. Sinds 2016 zijn er al meer dan 60 landen die een nationale AI-strategie hebben opgesteld. Het Belgische plan telt negen doelstellingen, waarbij iedere doelstelling gericht is op het bevorderen van een ethisch model, met een evenwicht tussen innovatie en bescherming van de grondrechten, en op het ontwikkelen van een ecosys-

teem van talent. Bekijk de strategie in de link hieronder. (JA)

Bron: data-en-maatschappij.ai/beleidsmonitor/belgi%C3%AB-nationaal-convergentieplan-voor-de-ontwikkeling-van-artificiële-intelligentie

295

Rechtbank verplicht Zweedse autoriteit tot het behandelen van klachten

Een administratieve rechtbank in Stockholm heeft geoordeeld dat de Zweedse gegevensbeschermingsautoriteit (IMY) AVG-klachten moet onderzoeken en de gebruiker of klager bij het proces moet betrekken. Het gaat hier om een zaak waarin een gebruiker in januari 2019 een klacht indiende bij de Oostenrijkse DSB naar aanleiding van een ontoereikend antwoord van Spotify op zijn inzageverzoek. De klacht werd doorgestuurd naar de Zweedse IMY, die verantwoordelijk is voor Spotify. Maar na zes maanden had de klager nog steeds geen bericht over een beslissing.

De IMY was van mening dat het niet bij de oorspronkelijke klager hoefde terug te komen omdat het ambtshalve een breder onderzoek naar Spotify had ingesteld. Maar dat onderzoek heeft meer dan drie jaar geduurd. De termijn om te reageren op een verzoek om toegang krachtens de AVG is één maand en volgens de Zweedse wet moet een autoriteit binnen zes maanden reageren, anders kan de klager binnen vier weken een beslissing eisen. Na meer dan drie jaar wachten heeft de oorspronkelijke klager precies dat gedaan op grond van artikel 12 van de Zweedse administratieve wetgeving. (JA)

Bron: noyb.eu/en/sweden-users-are-not-party-their-own-privacy-rights

296

Duitse bedrijven herinnerd aan termijn vervangen modelcontracten

De Duitse dataprotectieautoriteit van Nedersachsen heeft op 2 november jl. een persverklaring uitgebracht om organisaties er aan te herinneren de 'oude' door de Europese Commissie goedgekeurde modelcontracten te vervangen door de nieuwe. De periode gedurende welke organisaties zich voor de doorgifte naar derde landen nog op de oude modelcontracten kunnen verlaten, loopt af op 27 december a.s. De autoriteit herinnert de organisaties er daarbij tevens aan dat doorgiften zonder adequate beschermingsmaatregelen opgeschort kunnen worden en dat ook een geldboete kan worden opgelegd. (NW)

Bron: dataguidance.com/news/eu-lfd-niedersachsen-reminds-deadline-conversion-old

297

Boete van 20 miljoen voor Clearview AI in Frankrijk

De Franse toezichthouder heeft Clearview AI een boete van € 20 miljoen opgelegd. Clearview is een bedrijf dat is gespecialiseerd in gezichtsherkenningstechnologie, met name voor de verkoop aan opsporings- en handhavingsinstanties. Ondertussen heeft Clearview een database van zo'n twintig miljard afbeeldingen opgebouwd, onder andere door deze van internet te 'scrapen'. In mei 2022 start de CNIL na ontvangst van verschillende klachten een onderzoek, in samenwerking met andere Europese toezichtshouders. Clearview zou zonder grondslag biometrische gegevens verwerken en hebben nagelaten betrokkenen te informeren dat ze hun gegevens kunnen laten verwijderen uit de database. De CNIL geeft Clearview de opdracht alle gegevens over Franse mannen en vrouwen te verwijderen en verwijderingsverzoeken te honoreren. Omdat Clearview weigert gehoor te geven aan de opdracht van de CNIL, gaat de CNIL over tot het opleggen van de boete van € 20 miljoen. Clearview heeft twee maanden de tijd om alsnog te voldoen aan de opdracht van de CNIL op straffe van een boete van € 100 000 per dag.

Clearview kreeg in maart 2022 al een boete van € 20 miljoen opgelegd door de Italiaanse toezichthouder vanwege onrechtmatige verwerking van biometrische gegevens en locatiegegevens. In mei 2022 kreeg Clearview een boete van de toezichthouder uit het Verenigd Koninkrijk, omgerekend € 8,9 miljoen. Ook in Griekenland kreeg Clearview een boete van € 20 miljoen opgelegd. Het onderzoek door de toezichthouder in Oostenrijk loopt nog. De toezichthouders uit België, Zweden, Duitsland, Canada en Australië hebben eerder al bevolen dat Clearview niet langer foto's van burgers mocht verzamelen en dat foto's uit de database moesten worden verwijderd. (NW)

Bron: privacy-web.nl/nieuws/cnil-legt-clearview-ai-boete-van-20-miljoen-euro-op/

298

Verwerken van persoonsgegevens in Deense archieven

De Deense toezichthouder, Datatilsynet, heeft op 7 november 2022 richtsnoeren gepubliceerd over het verwerken van persoonsgegevens in lokale archieven. Datatilsynet heeft met vertegenwoordigers van het archiefwezen gesproken om meer inzicht te krijgen in eventuele beperkingen van de privacywet op het werk van het archiefwezen. De bedoeling is met name dat de privacywet niet in de weg staat aan dat werk. De richtsnoeren bevatten vier specifieke aanbevelingen voor de archieven. (NW)

Bron: dataguidance.com/news/denmark%C2%A0datatilsynet-publishes-guidelines-local

299

Richtsnoeren certificering van internationale doorgiften van persoonsgegevens in China

De technische commissie voor de nationale informatiebeveiligingsstandaard in China, de TC260, heeft een aangepaste versie gepubliceerd van de technische specificaties voor de certificering van internationale doorgifte van persoonsgegevens. Deze specificaties vormen onderdeel van de 'Practice Guidelines for Cybersecurity Standards'. De richtsnoeren bevatten de basisvereisten die worden gesteld aan de betrokken partijen, zoals het aanstellen van een verantwoordelijke persoon voor de verwerking van persoonsgegevens, de regels voor internationale doorgifte en de vereisten voor het uitvoeren van een DPIA. Meer specifiek moeten betrokkenen geïnformeerd worden over de doorgifte (per e-mail, tekstbericht, brief of fax) en over de doeleinden, soort en duur van de verwerking en moet toestemming van de betrokkenen worden verkregen.

Verwerkers en certificeringsinstanties in de landen of regio's waar de derde-ontvanger is gevestigd moeten geïnformeerd worden over wijzigingen in wet- en regelgeving. Ontvangers moeten tevens verplicht worden om onmiddellijk maatregelen te treffen en de betrokken partijen te informeren in geval van een datalek, van fraude of verlies van data. Tot 15 november 2022 konden partijen feedback geven op de nieuwe versie van de richtsnoeren. (NW)

Bron: dataguidance.com/news/china-tc260-releases-draft-revised-specification-cross

Bedrijfsleven

300

Vordering tot afgifte back-up bedrijfstelefoon afgewezen wegens gebrek aan belang

Multimax (werkgever) verzocht een arbeidsongeschikte werknemer zijn werktelefoon in te leveren. Deze telefoon bevatte zowel zakelijke als privégegevens van de werknemer. De werknemer gaf de telefoon terug nadat hij alle gegevens had gewist. Hij bewaarde wel een back-up op zijn privélaptop. Multimax vorderde de integrale back-up, inclusief privégegevens, op grond van een zwaarwegend bedrijfsbelang. De werkgever voerde aan dat de gegevens software en beveiligingscodes kunnen bevatten die cruciaal zijn voor de continuïteit van de bedrijfsvoering. De werknemer weigerde integrale afgifte van de back-up omdat deze privégegevens bevat. Het gerechtshof Arnhem-Leeuwarden oordeelt dat Multimax haar belang bij afgifte van de integrale back-up onvoldoende heeft onderbouwd. Multimax heeft onvoldoende concreet gemaakt om welke gegevens het gaat en zo overweegt het hof '*als Multimax echt af hankelijk is van één telefoon om over haar software en beveiligingscodes te beschikken, dit niet voor rekening en risico van [geïntimeerde] komt, maar dat Multimax haar bedrijfsvoering anders had moeten inrichten.*' Daarnaast weegt het hof mee dat Multimax weinig bereidheid heeft getoond om dit geschil op te lossen, door voorstellen van werknemer om de back-up te vernietigen of de zakelijke en privégegevens te laten scheiden door een neutrale derde partij te weigeren. (ETh)

Bron: Hof Arnhem-Leeuwarden 6 september 2022, ECLI:NL:GHARL:2022:7672, deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHARL:2022:7672

301

Geen privacyinbreuk bij het filmen van een 'zieke' werknemer door een recherchebureau

Een werknemer van een installatiebedrijf zat inmiddels een jaar thuis na ziekmelding. De werknemer gaf aan dat hij door ziekte niet meer kon autorijden, lopen, trekken, tillen, knielen etc. Het installatiebedrijf werd getipt dat de werknemer ondanks zijn ziekmelding intensieve kluswerkzaamheden in zijn nieuwe huis verrichtte. De werkgever vermoedde dat de werknemer had gelogen over zijn beperkingen, en schakelde een recherchebureau in dat de werknemer gedurende drie dagen observeerde en beelden van de klussende werknemer vastlegde. Hierop werd de werknemer op staande voet ontslagen. Volgens de werknemer is zijn recht op privacy geschonden. De kantonrechter oordeelt dat het belang van de werkgever om de waarheid te achterhalen over de verklaringen van de werknemer over zijn beperkingen zwaarder weegt dan het recht op privacy van de werknemer. De ernst van de inbreuk is beperkt omdat het recherchebureau uitsluitend de werknemer heeft gefilmd op het moment dat hij kluswerkzaamheden uitvoerde en het onderzoek maar drie dagen heeft geduurd. Er was geen minder zwaar middel voorhanden om de waarheid te achterhalen omdat werkgever het vermoeden had dat werknemer zou hebben gelogen, het aangaan van een gesprek was bijvoorbeeld niet een geschikter middel geweest. (ETh)

Bron: Rb. Midden-Nederland 20 juli 2022, ECLI:NL:RBNME:2022:2960, deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2022:2960

302

Ontslag op staande voet wegens het niet voldoen aan de instructie om de camera aan te laten staan, is niet rechtsgeldig

Een werknemer van een Amerikaans telemarketingbedrijf voldeed niet aan de instructie van de werkgever om gedurende de hele dag de camera van de computer aan te zetten. Het ontslag op staande voet wegens 'refusal to work' en 'insubordination' is niet rechtsgeldig. Het verplichten tot het aan laten staan van de camera van de werknemer is in strijd met diens recht op respect op het privéleven, zonder dat hiervoor een gerechtvaardigde grondslag bestaat. Daarom is geen sprake van het weigeren om te voldoen aan een redelijk bevel of opdracht van de werkgever en daarmee geen reden voor ontslag op staande voet. (ETh)

Bron: Rb. Zeeland-West-Brabant 28 september 2022, ECLI:NL:RBZWB:2022:5656, deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBZWB:2022:5656

Overheid

303

Nederland krijgt algoritmetoezichthouder in 2023

Een nieuwe autoriteit gaat toezien op het gebruik van algoritmen. Deze algoritmetoezichthouder zal in de loop van 2023 worden opgericht. De regering heeft dit recentelijk bekendgemaakt. (CE)

Bron: rijksoverheid.nl/actueel/nieuws/2022/10/07/overheid-gaat-meer-doen-om-problemen-algoritmen-te-voorkomen

304

Overheid overtreedt wet met verzamelen tweets

Overheden tappen op grote schaal tweets om te achterhalen hoe burgers tegen hun beleid aankijken. Toestemming van twitteraars ontbreekt.

Zonder dat twitteraars het weten, verzamelt de overheid hun berichten om reacties op beleid in de samenleving te peilen. Onder meer het Ministerie van Sociale Zaken, de Belastingdienst en de Nederlandse Voedsel- en Warenautoriteit (NVWA) gaan op die manier te werk, blijkt uit een rondvraag van *AG Connect*, *iBestuur en Binnenlands Bestuur* in samenwerking met dagblad *Trouw*. Volgens deskundigen is deze werkwijze problematisch, omdat gebruikers ten onrechte niet worden geïnformeerd.

Overheden gebruiken voor het verzamelen en analyseren van (kritische) tweets tools van commerciële bedrijven als Coosto, OB14Wan en Twittertap. Deze tools 'tappen' Twitter, verzamelen op grote schaal (anonieme) berichten en maken deze geschikt voor data-analyse. Het gaat om vragen van twitteraars, berichten waar de betreffende overheid in wordt genoemd door bijvoorbeeld opiniemakers, of nieuwsartikelen en reacties daarop. Ook meten overheden soms het sentiment in de samenleving aan de hand van een groot aantal tweets. Ook het Sociaal Cultureel Planbureau verzamelde afgelopen jaren duizenden tweets over klimaatverandering en 'nationale identiteit' voor twee onderzoeken naar deze thema's. Daarbij werden ook bijzondere persoonsgegevens van twitteraars verzameld zoals religieuze overtuiging, etnische afkomst, iemands seksuele gedrag of politieke opvattingen, blijkt uit een uittreksel van het verwerkingsregister. De tweets werden overigens geanonimiseerd verzameld. Voor het SCP geldt volgens een woordvoerder echter een uitzondering. Toestemming en informeren van twitteraars is volgens de wet hier niet verplicht omdat het gaat om onderzoek voor statistische doeleinden.

Uit eerder onderzoek van *Binnenlands Bestuur*, *AG Connect* en *iBestuur* werd duidelijk dat overheden vaak geen benul hebben van welke persoonsgegevens ze doorgeven aan Amerikaanse techreuzen. De verwerkingsregisters waarin dit wordt bijgehouden zijn bij geen van de onderzochte organisaties compleet. (CE)

Bron: binnenlandsbestuur.nl/digitaal/hoe-de-overheid-duizenden-tweets-verzamelt-en-daarbij-de-wet-overtreedt?tid=TIDP2973010X3674108ABA8F4D78B8A567AB72B022EDYI5&utm_campaign=BB_NB_Wekelijks&utm_medium=email&utm_source=binnenlandsbestuur

305

Werkagenda Digitalisering van het kabinet

Een gemeente die dienstverlening aanbiedt via WhatsApp, of een wethouder die communiceert via TikTok, moet in de toekomst wellicht op zoek naar een ander platform om het contact met inwoners te onderhouden. In de Werkagenda Digitalisering van het kabinet, ligt de nadruk op het borgen van publieke waarden, zoals transparantie, privacy en inclusiviteit. Dat houdt onder meer in dat online platforms en diensten in de komende jaren kritisch tegen het licht worden gehouden. Voldoen ze aan de Europese Digital Services Act (DSA) en aan de eisen die de Nederlandse overheid stelt? 'Als een platform niet voldoet aan onze voorwaarden, zullen we ze daarop aanspreken,' zegt staatssecretaris Alexandra van Huffelen van D66 tegen *Binnenlands Bestuur*. 'In eerste instantie geven we ze de gelegenheid om zich te verbeteren. Maar als dat niet gebeurt, moeten we er afscheid van nemen.'

In Europees verband wordt gewerkt aan alternatieven voor communicatie, social media en clouddiensten. Het kabinet wil publieke instellingen stimuleren om dergelijke platforms in te zetten. Toch betekent dit nog niet dat gemeenten hun Facebookgroepen dan maar

moeten opdoeken. ‘Ik heb liever dat Facebook, Google of Microsoft zich verbeteren dan dat we ze ‘cancelen,’ om het in de terminologie van de digitale wereld te zeggen,’ stelt Van Huffelen. ‘Het effect van een verbetering is breder dan de overheid, en raakt ook gebruikers thuis.’ Ze wijst erop dat het de rijksoverheid al een aantal keer eerder is gelukt om betere voorwaarden te bedingen, bijvoorbeeld over het gebruik van Google in het onderwijs.

Zou het verbeteren van de ICT-systemen van de overheden de sleutel kunnen zijn om het vertrouwen van de burger terug te winnen? ‘Vertrouwen begint met echt contact maken, met mensen spreken en goed luisteren naar wat ze nodig hebben. Maar als het gaat over digitaal, dan zijn twee zaken uit de werkagenda belangrijk, namelijk dat zakendoen met de overheid makkelijk en begrijpelijk moet zijn, en ook altijd live kan, met een mens van vlees en bloed tegenover je. Ten tweede die transparantie: inzichtelijkheid in hoe we beslissingen nemen. Weten dat de overheid secuur met jouw gegevens omgaat, is een groot onderdeel van dat vertrouwen.’ (CE)

Bron: Binnenlands Bestuur 4 november 2022

306

Platform Open Overheid vernieuwd

Op 20 september 2022 is de website open-overheid.nl vernieuwd. Deze website voorziet in het volledige aanbod van instrumenten, diensten en kaders waarmee rijksorganisaties aan de slag kunnen om opener en transparanter te zijn. De site moet de basis zijn voor het werken aan een open overheid.

Het programma Open Overheid heeft tot doel om de openheid van de rijksoverheid te vergroten en haar informatiehuishouding en -voorziening te verbeteren. Transparantie rondom beleidskeuzes moet toenemen, door ruimer en actiever overheidsinformatie te delen. Een goede informatiehuishouding moet de rijksoverheid in staat stellen om op een betrouwbare en transparante wijze haar taken uit te voeren. Journalisten, burgers en onderzoekers moeten zo beter en sneller geholpen worden. De website is bedoeld voor professionals die binnen het rijk werken aan een open overheid, zoals programmamanagers, projectmanagers, informatiespecialisten, communicatieadviseurs en juristen. Onderwerpen die van toepassing zijn op het verbeteren van de informatiehuishouding en het streven naar een open overheid, zoals openbaarmaking en e-mailarchivering, staan centraal en leiden de bezoeker naar bijbehorend aanbod. De site wordt nog verder aangevuld, maar je vindt er nu al tools, kaders, diensten en handreikingen van verschillende organisaties bij elkaar. Documenten van overheidsorganisaties zoals gemeenten, provincies, waterschappen en de rijksoverheid die in het platform te vinden zijn: beleidsnota’s van departementen waarin beleid wordt beschreven; Woo-verzoeken; beslisnota’s, documenten waarin ambtenaren alle afwegingen onder elkaar zetten om tot een beleidskeuze te komen; agenda’s en verslagen vergaderingen zoals de ministerraad; contactgegevens van overheidsinstanties en Kamerstukken. (WA & CE)

Bron: informatiehuishouding.nl/actueel/nieuws/2022/09/20/nieuw-platform-open-overheid-voor-professionals-gelanceerd en open-overheid.nl/

307

Raad van State uit kritiek op wet voor delen data door overheid

De Raad van State (RvS) is bezorgd dat het wetsvoorstel dat als doel heeft om overheden meer gegevens te laten delen, de persoonsgegevens onvoldoende beschermt. Het adviesorgaan raadt het kabinet aan om het wetsvoorstel nog niet in te dienen bij de Tweede Kamer, maar deze eerst op een aantal punten aan te passen of nader toe te lichten.

Het doel van de Wet hergebruik van overheidsinformatie (Who) is om data die zijn verzameld door overheden zo veel mogelijk te delen, zodat deze makkelijk kunnen worden hergebruikt. Dat kan voor onderzoek, maar ook voor commercieel gebruik. Dat gebeurt bijvoorbeeld momenteel al met filemeldingen. Die worden bijgehouden door Rijkswaterstaat, maar worden gedeeld en kunnen daardoor ook worden gebruikt in apps.

De RvS vreest dat onder de nieuwe wet per ongeluk persoonlijke gegevens kunnen worden gedeeld. Data mogen alleen worden gedeeld als ze niet herleidbaar zijn tot personen. Dat kan bijvoorbeeld door alleen iemands woonplaats en opleidingsniveau bekend te maken, maar niet diens naam. ‘Alleen, het is voorstelbaar dat anonieme gegevens later, met snellere en slimmere computers, alsnog teruggerekend kunnen worden tot de oorspronkelijke persoonsgegevens’, aldus het adviesorgaan.

De Autoriteit Persoonsgegevens (AP) was in augustus ook al kritisch over het wetsvoorstel. De AP wil dat het in principe verboden wordt om data uit openbare registers, zoals die van de Kamer van Koophandel en het kadaster, te hergebruiken. Ook vindt de toezichthouder dat duidelijk moet worden vastgelegd wanneer hier een uitzondering op mag worden gemaakt. (TW)

Bron: rtlnieuws.nl/tech/artikel/5342028/wet-open-data-privacy-overheid

308

Datalek bij kadaster: geheime adressen waren bijna een maand lang gewoon toegankelijk

Door een datalek bij het kadaster zijn geheime woonadressen tijdelijk zichtbaar geweest. Dat blijkt uit correspondentie van het kadaster met getroffen personen die de *Volkskrant* heeft ingezien. Volgens het kadaster is de oorzaak een recente update van het systeem en waren de gegevens alleen tussen 18 september en 11 oktober te raadplegen.

Het kadaster heeft melding gedaan bij de Autoriteit Persoonsgegevens (AP). Om hoeveel getroffenen het gaat, is niet duidelijk. Van deze personen wordt overigens wél een objectlijst weergegeven, waarin te zien is welke percelen of appartementsrechten een persoon of organisatie op naam heeft staan, zegt een woordvoerder van het kadaster. 'Een woonadres is iets anders dan een objectadres. Het objectadres mogen wij wettelijk gezien niet afschermen.' (TW)

Bron: volkskrant.nl/nieuws-achtergrond/datalek-bij-kadaster-geheime-adressen-waren-bijna-een-maand-lang-gewoon-toegankelijk~b0bb6836

309

Toezichthouder Agentschap Telecom wordt Rijksinspectie Digitale Infrastructuur

De toezichthouder Agentschap Telecom gaat vanaf 1 januari 2023 verder onder de naam Rijksinspectie Digitale Infrastructuur. Dat heeft de overheidsinstantie aan *AG Connect* laten weten. De toezichthouder behoudt zijn huidige taken, maar gaat ook nadrukkelijk investeren in de digitale veiligheid van Nederland.

Het Agentschap Telecom (AT) is de toezichthouder op het gebied van telecommunicatie- en IT-netwerken in Nederland. Als gevolg van de toenemende digitalisering wordt dat een steeds groter domein en neemt ook het aantal opdrachtgevers toe. 'Telecom' verdwijnt dus uit de nieuwe naam, aangezien dat de lading volgens de toezichthouder niet meer dekt.

De benaming 'Agentschap' past volgens de organisatie ook niet helemaal meer, aangezien er meer geïnvesteerd wordt in de toezichtstaken en deze intensiever worden. Met digitalisering komen immers ook nieuwe kwetsbaarheden en risico's mee, die maken dat 'maatschappelijke belangen en publieke waarden onder druk staan'. Daarnaast is het volgens de organisatie belangrijk dat de overheid vat krijgt op de gehele digitale infrastructuur. 'Daarvoor is een sterke Rijksinspectie nodig die het geheel overziet, kansen en risico's tijdig signaleert en in kan grijpen als dat nodig is.' (TW)

Bron: computable.nl/artikel/nieuws/overheid/7425281/250449/ap-nieuwe-witwas-wet-zorgt-voor-bancair-sleepnet.html

310

Gemeente handelt onzorgvuldig bij doorsturen van vertrouwelijke informatie

Een man vernam dat zijn buurman van de gemeente Amersfoort een vergunning had gekregen voor de bouw van een veranda. Hij was het daar niet mee eens en diende een bezwaarschrift in bij de gemeente. Tijdens de bezwaarprocedure stuurde de man de gemeente een e-mail met extra informatie. Hij wilde niet dat deze informatie bij zijn buurman terechtkwam. Daarom schreef hij erbij dat de informatie vertrouwelijk was. Maar de gemeente stuurde de vertrouwelijke informatie toch door naar zijn buurman. De man klaagt erover dat de gemeente de vertrouwelijke informatie heeft verstrekt aan zijn buurman. Zonder hem vooraf te waarschuwen of hem de gelegenheid te bieden om de informatie terug te nemen. Als gevolg van het doorsturen van de vertrouwelijke informatie is de verhouding tussen de buurman en de man extra geëscaleerd. De ombudsman vindt dat de gemeente meer rekening had moeten houden met de situatie dat er sprake was van een burenconflict. En daarom de man eerst in de gelegenheid had moeten stellen om de vertrouwelijke informatie terug te nemen. De gemeente had de man vervolgens moeten betrekken bij de beoordeling van zijn verzoek om de informatie vertrouwelijk te behandelen. De gemeente heeft onvoldoende onderzocht of er mogelijkheden waren om aan de bezwaren van de man tegen inzage door zijn buurman tegemoet te komen. (CE)

Bron: nationaleombudsman.nl/nieuws/rapporten/2022149

311

Rijksoverheid mag voortaan commerciële clouddiensten gebruiken

De rijksoverheid mag voortaan van commerciële clouddiensten gebruikmaken, zo heeft staatssecretaris Van Huffelen van Digitalisering op 29 augustus in een brief aan de Tweede Kamer laten weten. Tot nu toe mochten overheidsinstanties alleen eigen clouddiensten gebruiken. Het nieuwe cloudbeleid geldt niet voor het Ministerie van Defensie en is ook niet toegestaan voor als staatsgeheim gerubriceerde informatie. Voor gegevens uit de basisregistratiepersoonsgegevens en bijzondere persoonsgegevens geldt het principe 'nee tenzij'. (TW)

Bron: security.nl/posting/766127/Rijksoverheid+mag+voortaan+commerci%C3%ABle+clouddiensten+gebruiken

312

Reactie AP op Rijksbreed cloudbeleid

Het kabinet wil overheidsdata voortaan kunnen opslaan bij commerciële clouddiensten. Dit brengt grote privacyrisico's met zich mee en daar moet het kabinet mee aan de slag in de verdere uitwerking van het beleid. Dat schrijft de Autoriteit Persoonsgegevens (AP) in een brief van 11 november aan staatssecretaris Van Huffelen van Digitalisering.

De AP zegt dat in het cloudbeleid de privacyrisico's onvoldoende in kaart zijn gebracht en vraagt de staatssecretaris met name oog te hebben voor de risico's van het opslaan van persoonsgegevens in landen buiten Europa, waar de privacywet Algemene verordening gegevensbescherming (AVG) niet geldt. Zo kunnen bijvoorbeeld Amerikaanse inlichtingendiensten persoonsgegevens van Nederlanders opvragen bij Amerikaanse bedrijven. Zelfs als de servers van die bedrijven in Europa staan. 'Daardoor kunnen die diensten jou bijvoorbeeld onterecht in verband brengen met terrorisme of fraude, waardoor je de VS

en andere landen niet meer binnenkomt', zegt Wolfsen. Omdat het overgrote deel van de veelgebruikte cloudaanbieders op dit moment Amerikaans is, zou de staatssecretaris ook Europese alternatieven moeten stimuleren, stelt de AP in de brief.

Tot slot is het beleid nu te vrijblijvend, stelt de AP. Zo zijn zelfstandige bestuursorganen niet verplicht het beleid te volgen. 'Terwijl instellingen als het UWV, het CBS en de Sociale Verzekeringsbank gevoelige persoonsgegevens van ons allemaal in hun systemen hebben staan', aldus Wolfsen. De AP heeft haar adviezen daarover ook in een gesprek met Van Huffelen overgebracht. Zij heeft aangegeven de adviezen van de AP ter harte te nemen. (CE)

Bron: Persbericht Autoriteit Persoonsgegevens 14 november 2022, autoriteitpersoonsgegevens.nl

313

AP helpt raadsleden bij controleren inzet technologie en samenwerkingsverbanden

De Autoriteit persoonsgegevens (AP) publiceert tips voor gemeenteraadsleden voor het controleren van de inzet van technologie en het deelnemen aan samenwerkingsverbanden.

Het gaat om aanvullingen op de bestaande handreiking 'Gemeenten en privacy: wat kunt u als raadslid doen?' die raadsleden helpt de juiste vragen te stellen over privacy binnen hun gemeente. Gemeenten verwerken veel persoonsgegevens van burgers. Dat doen zij steeds vaker met innovatieve technologie en in samenwerkingsverbanden met andere partijen. Met als doel om taken sneller of beter uit te voeren en de burger beter van dienst te zijn. Maar het brengt ook privacyrisico's met zich mee. Door het gemeentebestuur kritisch te bevragen, komen raadsleden op voor de privacy van de inwoners.

Bron: Nieuwsbericht Autoriteit Persoonsgegevens 7 november 2022, autoriteitpersoonsgegevens.nl

Zorg

314

Geen meldplicht voor artsen over rijgeschiktheid patiënten

Het Ministerie van Infrastructuur en Waterstaat (IenW) wil geen meldplicht voor artsen over rijgeschiktheid van patiënten. De KNMG, FMS, LHV en NHG zijn tevreden met deze uitkomst, die onderdeel vormt van het project ter verbetering van het stelsel medische rijgeschiktheid. Eén van de doelen van dit optimalisatietraject is te bezien of er alternatieven mogelijk zijn, die het huidige stelsel kunnen verbeteren. Een meldplicht voor artsen om betreffende patiënten te melden bij het CBR, was één van de opties die breed werd verkend. In goed overleg met IenW wordt nu een informatierol voor artsen uitgewerkt.

In een Kamerbrief worden verbeteringen voorgesteld van het stelsel medische rijgeschiktheid. Deze Kamerbrief wordt besproken in het commissiedebat van IenW over verkeersveiligheid en wegen op 6 december 2022.

Uit de Kamerbrief blijkt onder meer dat de verantwoordelijkheid voor iemands rijgeschiktheid blijft liggen bij de rijbewijshouder. Zij zijn zelf verplicht om een melding te doen bij het CBR om hun rijgeschiktheid te laten testen als zij twijfelen over hun gezondheid en het effect hiervan op hun rijgeschiktheid. In de toekomst worden rijbewijshouders wettelijk verplicht zich bij het CBR te melden middels een gezondheidsverklaring na de diagnose van één van de meest risicovolle aandoeningen voor de verkeersveiligheid. Deze wettelijke bepaling en voor welke aandoeningen deze gaat gelden, wordt de komende tijd door het IenW nog nader uitgewerkt. Zij zullen daar ook medisch-inhoudelijke deskundigen bij betrekken.

Artsen krijgen geen meldplicht en ook geen uitlegplicht over de relatie tussen aandoeningen en rijgeschiktheid, maar hebben daarin wel een informatierol. De arts kent de medische situatie van de patiënt het beste en kan de patiënt informeren over de wettelijke meldplicht die op hem rust. (SNO)

Bron: Nieuwsbericht KNMG 3 november 2022, knmg.nl/actualiteit-opinie/nieuws/nieuwsbericht/geen-meldplicht-voor-artsen-over-rijgeschiktheid-patienten.htm

315

Zorgverzekeraars hebben meer zicht op fraude door samenwerking

Zorgverzekeraars hebben in 2021 ruim duizend fraudeonderzoeken afgerond. In 649 gevallen bleek daadwerkelijk sprake van fraude, in totaal is daarmee een bedrag van ruim € 17 miljoen gemoeid. Zorgverzekeraars werken steeds meer samen met de Nederlandse arbeidsinspectie en toezichthouders NZA en IGJ omdat zij zien dat fraudeonderzoeken steeds complexer worden. Zij zetten daarnaast extra in op het voorkomen van fraude. Dit staat in de jaarrapportage fraudebeheersing 2021 van alle zorgverzekeraars.

Zorgverzekeraars zien dat fraudeonderzoeken steeds complexer worden. Bij het onderzoeken van fraudesignalen werken zorgverzekeraars daarom steeds intensiever samen met het Informatie Knooppunt Zorgfraude, waar de signalen gedeeld kunnen worden met ketenpartners zoals de Nederlandse Zorgautoriteit (NZa), Inspectie Gezondheidszorg en Jeugd (IGJ) en Nederlandse Arbeidsinspectie (NLA). Op die manier kunnen belemmeringen, zoals onvoldoende onderzoeksbevoegdheid, gebrek aan medewerking of bewijsstukken, ondervangen worden.

Vorig jaar zijn 1053 fraudeonderzoeken afgerond, ruim 200 meer dan in 2020. Bij zo'n 60% van de onderzochte zaken werd fraude vastgesteld, waaronder in de sectoren wijkverpleging (54%) en paramedische zorg (16%). Daarnaast werd relatief vaak fraude vastgesteld met persoonsgebonden budgetten voor langdurige zorg (13%). Na het vaststellen van fraude, treffen zorgver-

zekeraars maatregelen tegen de betreffende zorgaanbieder.

In Nederland hechten we veel waarde aan een goede gezondheidszorg. Het is belangrijk dat geld dat bestemd is voor zorg, ook aan zorg besteed wordt. Zorgfraude ondermijnt het zorgstelsel. Daarom treden ook zorgverzekeraars daartegen op, onder andere door signalen van fraude te onderzoeken. Fraudebeheersing heeft een gepaste plek in alle processen van de zorgverzekeraar, zoals het zorginkoopbeleid en het verwerken van declaraties. Zorgverzekeraars zoeken bij het beheersen van fraude altijd naar een goede balans tussen vertrouwen en controle. Zij richten zich zo veel mogelijk op preventie: voorkomen waar het kan, alleen onderzoeken en bestraffen waar het moet. Op die manier gaat er minder zorggeld verloren en is er minder onderzoek nodig. (SNO)

Bron: Nieuwsbericht Zorgverzekeraars Nederland 13 oktober 2022, zn.nl/actueel/nieuws/nieuwsbericht?newsitemid=8145666048

316

Start implementatie medicatieoverdracht in de keten

Regio-organisaties GERRIT (regio Friesland) en Stichting RijnmondNet (regio Rijnmond) starten met zorgaanbieders en hun leveranciers als eerste met de implementatie van medicatieoverdracht. Zij implementeren de nieuwe informatiestandaard Medicatieproces 9 in combinatie met de richtlijn 'Overdracht van medicatiegegevens in de keten' in een tweejarige Kickstart. Hiermee start de landelijke uitrol van medicatieoverdracht in de keten. Ook GGZ Friesland doet mee in de regio Friesland.

Veilige en efficiënte medicatieoverdracht is van groot belang. Zorgverleners rondom een patiënt of cliënt hebben niet altijd een actueel en volledig medicatieoverzicht. Daardoor wordt niet altijd de juiste medicatie voorgeschreven of toegediend. Jaarlijks zijn er zelfs duizenden (her)opnames in het ziekenhuis vanwege het ontbreken van de juiste medicatiegegevens. Wekelijks worden in Nederland meer dan 1200 mensen in het ziekenhuis opgenomen door medicatie-incidenten. Bijna de helft hiervan is vermijdbaar door een juiste medicatieoverdracht.

Elektronische gegevens beter uitwisselen waardoor wél een actueel en volledig medicatieoverzicht beschikbaar is. Dat is van belang voor heel de zorgketen. De patiëntveiligheid verbetert en het bespaart zorgverleners veel tijd na implementatie in de keten. Daarom werken negen zorgsectoren, waaronder de Nederlandse ggz, en hun IT-leveranciers, het Ministerie van Volksgezondheid, Welzijn en Sport, de Patiëntenfederatie Nederland, MIND, RSO Nederland, Zorgverzekeraars Nederland, Nictiz en VZVZ hier samen aan.

De Kickstart Medicatieoverdracht omvat: het aanpassen van informatiesystemen, het testen ervan en een eerste begeleide uitrol van de systemen en de werkprocessen van de deelnemers aan het samenwerkingsverband. En het ontsluiten van informatie naar patiënten middels een PGO. Om de landelijke implementatie zorgvuldig te laten verlopen delen de regio-organisaties hun praktijkervaring en wordt de informatiestandaard bijgesteld als nodig. Op basis van deze testen in de praktijk, worden de puntjes op de i gezet en wordt voorbereid op de landelijke implementatie van medicatieoverdracht in de keten.

In de regio Friesland werkt GERRIT met de deelnemende zorgorganisaties: Stichting Antonius Zorggroep (Sneek), Gezondheidscentrum Makkum, Apotheek De Dokkumer Wâlden, Stichting Alliade, Stichting Geestelijke Gezondheidszorg Friesland, Stichting Patyna.

In de regio Rijnmond werkt Stichting RijnmondNet met de deelnemende zorgorganisaties: Erasmus Universitair Medisch Centrum Rotterdam, Huisartsenpraktijk Emmapark, Huisartspraktijk Overschie, Apotheek Pijnacker Centrum, Poli-apotheek Sint Franciscus Gasthuis, Stichting Laurens, Stichting Star-shl.

Meer informatie over de implementatie (Kickstart) is beschikbaar op: samenvoormedicatieoverdracht.nl. (SNO)

Bron: Nieuwsbericht De Nederlandse ggz 7 oktober 2022, denederlandseggz.nl/nieuws/2022/regio-friesland-en-rijnmond-implementeren-medicatieoverdracht-in-de-keten

317

Merendeel ziekenhuizen en klinieken kan gegevens aan patiënten beschikbaar stellen via PGO

Na de huisartsen en ggz-instellingen is 70% van de ziekenhuizen, categorale instellingen en klinieken nu ook klaar om gegevens aan patiënten beschikbaar te stellen via een Persoonlijke Gezondheidsomgeving (PGO). Het betreft 70% van de 198 instellingen die deelnemen aan VIPP 5, het implementatieprogramma om de uitwisseling van medische gegevens tussen instellingen en patiënten te versnellen. Deze instellingen zijn voor patiënten vindbaar vanuit PGO's. Hiermee is een belangrijke eerste deadline behaald van VIPP 5.

Een PGO biedt een dossier waarin alle zorgverleners, uiteenlopend van ziekenhuizen en zelfstandige klinieken tot huisartsen en apotheken, medische gegevens met patiënten kunnen uitwisselen. Voor patiënten ontstaat hiermee één omgeving waar zij hun gezondheidsgegevens van verschillende zorgverleners kunnen verzamelen. In het onlangs afgesloten Integraal Zorg Akkoord is opgenomen dat alle inwoners van Nederland in 2025 digitaal toegang moeten hebben tot hun eigen zorggegevens via een Persoonlijke Gezondheidsomgeving.

Afgelopen vrijdag 30 september was de eerste deadline voor VIPP 5. Deze eerste stap is het technisch gereed maken van de informatiesystemen om medische gegevens beschikbaar te stellen via een PGO. Instellingen zijn hier actief mee aan de slag gegaan. Inmiddels heeft 70% van de deelnemende instellingen een positieve audit behaald. Instellingen kunnen tot dertien weken na

de deadline een audit laten afnemen.

De volgende stap is patiënten te stimuleren om een PGO te gaan gebruiken. Uiterlijk 30 juni 2023 dienen zorginstellingen aan te kunnen tonen dat in een periode van 30 dagen minimaal 5% van hun patiënten gegevens heeft opgehaald via een PGO.

Het gebruik van een PGO vraagt om zowel scholing van medewerkers als patiënten, merken de zorginstellingen die actief met VIPP 5 aan de slag zijn. Dialysecentrum Ravenstein heeft de audit behaald. Meer dan 5% van hun patiënten maakt inmiddels ook gebruik van een PGO. 'Om patiënten kennis te laten maken met een PGO, hebben we de patiënten hierin persoonlijk begeleid. Afhankelijk van de behoefte van de patiënt. De ene patiënt vond het fijn om dit persoonlijk in de kliniek te doen, de ander op afstand bijvoorbeeld telefonisch', vertelt Daan Hollander, directeur van het dialysecentrum. 'Er zit veel verschil in de digitale vaardigheid van de patiënten. Het vergt toch wel enige vaardigheid om een PGO te kunnen gebruiken'.

Govert Tukker is projectleider bij het LangeLand Ziekenhuis. Het LangeLand heeft de audit behaald en is nu op weg naar 5% PGO-gebruik. 'We zijn vorig jaar al gestart met het informeren en scholen van onze medewerkers. Om patiënten te informeren hebben we onlangs in de centrale hal van het ziekenhuis een digitaal loket geopend. Hier kunnen patiënten vijf dagen per week worden geholpen met het gebruiken van de digitale middelen die ons ziekenhuis inzet, zoals het patiëntenportaal van het LangeLand Ziekenhuis en PGO's. De afgelopen weken zien we het PGO-gebruik toenemen. We blijven ons inzetten om de 5% gebruikseis snel te halen.'

Over VIPP 5

VIPP is het Versnellingsprogramma Informatie-uitwisseling Patiënt en Professional. Het programma VIPP 5 focust op de gestandaardiseerde uitwisseling van medische gegevens met de patiënt via een persoonlijke gezondheidsomgeving (PGO) en tussen instellingen onderling. Om deze ambitie kracht bij te zetten, werken de branchevereniging NFU, NVZ en ZKN binnen het programma VIPP 5 samen om medisch-specialistische zorginstellingen te ondersteunen bij de implementatie van de doelstellingen. Een unieke, zorgbrede samenwerking. (SNO)

Bron: Nieuwsbericht Nederlandse Vereniging van Ziekenhuizen 6 oktober 2022, nvz-ziekenhuizen.nl/nieuws/merendeel-ziekenhuizen-en-klinieken-klaar-om-gegevens-aan-patienten-beschikbaar-te-stellen

318

Tweede Kamer stemt unaniem vóór Wegiz

De Tweede Kamer heeft op 27 september 2022 het wetsvoorstel voor de Wet elektronische gegevensuitwisseling in de zorg (Wegiz) unaniem aangenomen.

Volgens VWS-minister Ernst Kuipers zorgt deze wet ervoor dat verschillende systemen met elkaar kunnen communiceren, zodat zorgverleners eenvoudig gegevens met elkaar kunnen delen en zo beter en sneller hun patiënt kunnen helpen. Het belooft meer digitale verbondenheid in de zorg.

Volgens programmamanager Ans van den Bosch bevestigt deze uitslag dat we op de goede weg zitten. Volgens haar is dit een belangrijk moment. Het ministerie is erg blij dat de Tweede Kamer de wet heeft aangenomen. Het wetsvoorstel moet natuurlijk nog worden behandeld in de Eerste Kamer, maar deze uitslag bevestigt dat we op de goede weg zitten.

Er verandert nog niet meteen iets in het zorgveld. Het ministerie gaat door met de uitwerking van de onderliggende regelgeving. Dat zijn de algemene maatregelen van bestuur (AMvB's). Van die besluiten zullen zorginstellingen wel iets gaan merken. De eerste AMvB treedt in 2023 in werking en gaat over het digitaal versturen van het recept van de huisarts naar de apotheek. Dit is via een spoor 1-aanwijzing. Dit gaat nog niet via een bepaalde standaard, maar het wordt wel een gegevensuitwisseling die verplicht elektronisch moet plaatsvinden. Andere gegevensuitwisselingen volgen vanaf 2024.

Op de achtergrond is men al bezig alsof de wet erdoorheen is. Dat gaat vaak zo want je moet veel voorbereidingen treffen. Het feit dat de Wegiz nu door de Tweede Kamer is aangenomen, geeft wel een sterk signaal af. Dat geeft Van den Bosch en haar collega's vernieuwde energie en zij ziet de behandeling in de Eerste Kamer met vertrouwen tegemoet.

Er zijn ook uitdagingen voor de toekomst. Een deel van de afspraken over de implementatie van de gegevensuitwisseling in de zorg is nu ook geland in het Integraal Zorgakkoord (IZA). Dat geeft extra richting. In de uitvoering komt men zeker nog zaken tegen die nadere uitwerking behoeven. Er worden veel dingen voor het eerst gedaan en dat is altijd spannend, maar Van den Bosch gelooft dat het met gezamenlijke inzet gaat lukken.

Ondanks het uitstel van de wetsbehandeling (die stond een jaar geleden al op de agenda van de Tweede Kamer) is Van den Bosch er trots op dat ze als team de energie hebben weten vast te houden. Zij is erg trots op de inzet van alle betrokken collega's en hoopt dat ze dit gevoel samen met alle partijen kunnen vasthouden. (SNO)

Bron: Nieuwsbericht Ministerie van Volksgezondheid, Welzijn en Sport 27 september 2022, gegevens uitwisselingindezorg.nl/gegevensuitwisseling/nieuws/2022/09/27/tweede-kamer-stemt-voor-wegiz

319

ICT-storingen in ziekenhuizen: lessen en aanbevelingen

Ziekenhuizen kunnen meer doen om bij een ICT-storing de impact voor patiënten te verkleinen. En ze kunnen ook meer doen om te voorkomen dat er ICT-storingen ontstaan. Die conclusie trekt de Inspectie Gezondheidszorg en Jeugd na vragen aan veertien ziekenhuizen

waar een grote ICT-storing was geweest. Uit de eigen onderzoeken van de ziekenhuizen komen vijf lessen naar voren. De inspectie doet daar zelf nog een aantal aanbevelingen bij.

De ziekenhuizen onderzochten de storingen zelf. Door naar de uitkomsten te vragen, kan de inspectie de rode draden zien. Een van de lessen gaat over het oefenen voor verschillende soorten crises. Alle ziekenhuizen waren het erover eens dat dat belangrijk is. De ziekenhuizen die dat hadden gedaan gaven aan daarvan te hebben geprofiteerd. En die het niet of te weinig hadden gedaan ervoeren er de negatieve gevolgen van.

Bij twaalf van de veertien storingen hadden de technische problemen flinke gevolgen voor de zorg. Volgens de rapportages van de ziekenhuizen liep geen enkele patiënt aantoonbaar gezondheidsschade op door de storing. De inspectie heeft daar ook geen aanwijzingen voor.

Maar dat neemt niet weg dat de gevolgen voor de patiënten groot waren. Zo konden de zorgverleners niet meer bij het elektronisch patiëntendossier. En bij tien storingen moest de spoedeisende hulp dicht. Ook stelden tien ziekenhuizen operaties uit. De ziekenhuizen betrokken de patiënten zelf niet bij de evaluatie van de storing. Dat kan wat betreft de inspectie beter, omdat de ziekenhuizen ook van hen kunnen leren.

Voor informatiebeveiliging bestaat voor ziekenhuizen (en andere zorgorganisaties) een wettelijke norm, de NEN 7510. Die gaat deels over de continuïteit van informatiesystemen, dus wat je doet om ICT-storingen te voorkomen. Nog lang niet alle ziekenhuizen voldoen aan deze norm. De inspectie stelt daar nu een deadline voor. Uiterlijk eind 2023 moeten alle ziekenhuizen aan de norm NEN 7510 voldoen.

De ziekenhuizen kunnen een aantal dingen van elkaar leren als het gaat om ICT-storingen. In een factsheet heeft de inspectie de lessen en eigen aanbevelingen op een rij gezet. Ook is daarin meer informatie te vinden over de oorzaak en gevolgen van de storingen. (SNO)

Bron: Nieuwsbericht Inspectie Gezondheidszorg en Jeugd 27 september 2022, igj.nl/actueel/nieuws/2022/09/27/ict-storing-probleem-voor-ziekenhuis-en-patient

320

Betere elektronische cliëntendossiers nodig voor verpleegkundige zorg

Verpleegkundige verslaglegging is essentieel voor kwalitatief goede en veilige zorg. Om de kwaliteit van de verslaglegging te verbeteren moeten elektronische cliëntendossiers, waarin verpleegkundigen documenteren, beter aansluiten bij het werk van verpleegkundigen en bovendien gebruiksvriendelijk zijn. Het is daarom cruciaal dat verpleegkundigen een prominente stem hebben bij de (door)ontwikkeling van elektronische cliëntendossiers. Dit komt naar voren uit het onderzoek waarop wijkverpleegkundige en Nivel-onderzoeker Kim de Groot op 19 september promoveerde aan de Vrije Universiteit Amsterdam.

Verslaglegging over zorgverlening aan cliënten is geen doel op zich, maar vormt een belangrijke bron van informatie voor verpleegkundigen en verzorgenden. Voor de patiëntveiligheid en de kwaliteit van zorg is goede verslaglegging essentieel. Er zijn indicaties dat de kwaliteit van de verslaglegging niet goed genoeg is, maar hoe dit verbeterd kan worden is tot nu toe onduidelijk.

Verpleegkundigen en verzorgenden noteren in de elektronische cliëntendossiers de informatie over de zorg die een cliënt krijgt. Zij zijn over het algemeen niet erg positief over de volledigheid en nauwkeurigheid van de gegevens die in deze dossiers staan, noch over de gebruiksvriendelijkheid van de elektronische dossiers. Dit terwijl juist ook dit laatste een belangrijk voorwaarde is voor kwalitatief goede verslaglegging.

De beperkte gebruiksvriendelijkheid van de dossiers is volgens wijkverpleegkundigen tevens een oorzaak van de hoge werkdruk die zij ervaren. Hoewel ze verslaglegging nuttig en noodzakelijk vinden voor goede zorgverlening, levert het veel werk op. Dit zit hem met name in het continu moeten switchen tussen verschillende onderdelen van een elektronisch cliëntendossier en het vaak moeten overtypen van informatie op verschillende plekken in één dossier.

De Groot laat met haar onderzoek zien hoe belangrijk het is om in de toekomst verpleegkundigen te betrekken in de verdere ontwikkeling van de elektronische dossiers. De stem van de eindgebruiker – de zorgprofessional – ontbreekt tot nu toe vaak, wat een gemiste kans is voor het optimaliseren van het gebruik van de dossiers. (SNO)

Bron: Nieuwsbericht Nivel 19 september 2022, nivel.nl/nl/nieuws/betere-elektronische-clientendossiers-nodig-voor-goede-en-veilige-verpleegkundige-zorg

Sociaal domein

321

Wmo-voorspelmodel

Met het Wmo-voorspelmodel kunnen gemeenten op wijk- en gemeenteniveau zien hoeveel mensen de komende vijf jaar gebruik zullen maken van Wmo-voorzieningen. Het Wmo-voorspelmodel gebruikt een algoritme, gebaseerd op open data. De voorspellingen worden getoond in een dashboard. Het model is ontwikkeld door datawetenschappers van VNG en gemeenten, in samenwerking met eindgebruikers. Het model is vanaf 20 januari 2022 openbaar toegankelijk, net als de achterliggende code en het algoritme.

Het Wmo-voorspelmodel voorspelt op basis van historische data het aantal Wmo-gebruikers per categorie. Deze informatie geeft ambtenaren meer inzicht in de ontwikkeling van het gebruik van de Wmo, en genereert stuurinformatie voor beleidsvraagstukken, inkoop en financiën. (CE)

Bron: vng.nl/projecten/wmo-voorspelmodel

322

Decentralisaties vanuit burgerperspectief

De Nationale ombudsman opent een onderzoek naar de invloed van burgers binnen de Wet maatschappelijke ondersteuning (Wmo). Hij wil weten of burgers wel voldoende betrokken worden bij het oplossen van hun hulpvraag of probleem. En of zij invloed hebben op de totstandkoming van het beleid en de uitvoering.

Verder onderzoekt de ombudsman in hoeverre gemeenten binnen de Wmo de regie houden, wanneer zij hun publieke taken overdragen aan private partijen.

De afgelopen vijftien jaar zijn meerdere taken van de Rijksoverheid overgedragen aan gemeenten. Met als belangrijkste redenen om burgers beter en sneller te kunnen helpen, menselijk contact te bevorderen en kosten te besparen. Gemeenten staan immers dichter bij de burger dan het Rijk. In de praktijk blijkt dit niet altijd te lukken. De ombudsman ontvangt regelmatig klachten van burgers over gebrek aan inspraak en participatie. Hij vindt dat burgers invloed moeten kunnen uitoefenen op beslissingen en ontwikkelingen die hen rechtstreeks raken. De Nationale ombudsman onderzoekt daarom de decentralisaties vanuit burgerperspectief. Het gaat daarbij specifiek over de Wmo, de Participatiewet en de Jeugdwet. Het onderzoek naar de Wmo is het eerste van de drie onderzoeken en wordt naar verwachting eind 2022 afgerond. (CE)

Bron: nationaleombudsman.nl/nieuws/2022/opening-onderzoek-naar-invloed-van-burgers-in-de-wmo

323

Jeugdwet en Wmo ook onder bereik Wet Bibob

Door een wijziging van de Wet Bibob (art. 1 lid 4 onder b) kunnen gemeenten vanaf 1 oktober 2022 deze wet inzetten om te beoordelen of zorgaanbieders binnen de Jeugdwet en de Wet maatschappelijke ondersteuning 2015 (Wmo 2015) al dan niet bonafide zijn. Dit biedt gemeenten een stevig handvat om te voorkomen dat publiek geld bij criminele organisaties of personen terechtkomt. Gemeenten voeren de Jeugdwet en de Wmo 2015 uit door het sluiten van contracten met aanbieders van jeugdzorg en maatschappelijke ondersteuning. Gemeenten moesten in de aanbestedingsprocedures van deze contracten nog kiezen voor de aanbieder met de 'economisch meest voordelige inschrijving' (het emvi-criterium). In de praktijk betekent dit dat gemeenten offertes moeten opvragen en beoordelen. Met deze wet is het emvi-criterium geschrapt. Dit maakt aanbestedingsprocedures zonder offertefase mogelijk. (WA)

Bron: binnenlandsbestuur.nl/juridisch/wet-bibob-nu-ook-toepasbaar-voor-open-house-inkoop

Politie en justitie

324

Gebruik risicomodellen door politie verankert discriminatie

Fair Trails heeft een rapport uitgebracht waarin ze analyseren hoe de Amsterdamse politie omgaat met profilering risicomodellen (een vorm van predictive policing) genaamd 'Top600' (voor volwassenen) en 'Top400' voor mensen van 12 tot 23 jaar). Hun grootste zorg is dat discriminerende politiepraktijken (bijvoorbeeld bepaalde groepen mensen vaker arresteren dan andere) worden verankerd in systemen die dit soort arrestaties vervolgens doen toenemen. Een duidelijk voorbeeld van wat een risico blijft: algoritmische feedback loops. (JA)

Bron: racismandtechnology.center/2022/10/28/the-devastating-consequences-of-risk-based-profiling-by-the-dutch-police/

325

Het openbaar ministerie en politie informeren burger onvoldoende over tipgeversprocedure

De Nationale ombudsman (No) heeft onderzoek gedaan naar de informatieverstrekking aan burgers als het openbaar ministerie (OM) in strafzaken een financiële beloning uitlooft aan tipgevers. Hierbij gaat het om de situatie waarin het OM aan de burger een financiële beloning in het vooruitzicht heeft gesteld voor informatie die leidt tot de opheldering van zeer ernstige misdrijven of de opsporing en aanhouding van (voortvluchtige) verdachten of veroordeelden. De No vindt het van belang dat de informatieverstrekking aan burgers over de tipgeversprocedure goed geregeld is. Dit betekent dat het OM en de politie aan de burger algemene informatie, uitleg moeten geven over de inrichting van de tipgeversprocedure, over de rol van de betrokken instanties en over welke informatie zij wel of niet kunnen delen en waarom dit zo is. Burgers moeten weten waar ze aan toe zijn als ze met het oog op een financiële beloning in een strafzaak een tip (willen) geven. De No begrijpt dat opsporingsonderzoeken een afgeschermd karakter hebben en heeft er begrip voor dat het OM en de politie daarom geen informatie kunnen delen met burgers over de inhoud van lopende opsporingsonderzoeken. Maar het gaat om informatie over hoe de tipgeversprocedure is vormgegeven en wat er binnen dat proces in zijn algemeenheid met een ingediende tip gebeurt. Zij moeten ook weten dat zij procedurele mogelijkheden hebben als zij vinden dat zij in aanmerking komen voor een beloning. De No vindt dat zowel burgers als het OM en de politie er bij gebaat zouden zijn als aan de voorkant (bijvoorbeeld bij de bekendmaking van de beloning of het indienen van een tip) meer informatie aan burgers wordt verstrekt over de procedurele aspecten van de tipgeversprocedure. Dit gebeurt volgens de ombudsman nu nog onvoldoende. De ombuds-

man roept het OM en de politie daarom op om de informatieverstrekking aan burgers te verbeteren. (WA)

Bron: nationaleombudsman.nl/nieuws/rapporten/2022189

326

Onderzoek naar mededeling aan CBR door politie-eenheid Rotterdam

De politie kan het rijbewijs innemen als er aan getwijfeld wordt of betrokkene nog geschikt is om te rijden. Bijvoorbeeld door gebruik van alcohol of drugs, gevaarlijk rijgedrag of gezondheidsredenen. De politie stuurt dan een bericht naar het CBR waarin ze uitlegt wat er is gebeurd en waaraan wordt getwijfeld (grondslag: artikel 130 Wegenverkeerswet 1994 en artikel 4:2, lid 1, e. van Besluit politiegegevens). Het CBR besluit vervolgens of betrokkene geen of wel een cursus of onderzoek moet volgen/ondergaan. Aldus kan sprake zijn van een stevige inbreuk op de privacy van betrokkene.

Op 4 oktober 2022 publiceerde de Nationale ombudsman (No) hierover een voorbeeld op de website; een klacht hierover is door de No verworpen. (WA)

Bron: nationaleombudsman.nl/nieuws/rapporten/2022163

327

Openbaar ministerie niet-ontvankelijk in zaken mondkapjesplicht in ov

Het openbaar ministerie (OM) heeft drie personen ten onrechte vervolgd, die in de zomer van 2020 geen mondkapje droegen in het openbaar vervoer (OV). Het gerechtshof Amsterdam heeft dit op 27 oktober 2022 beslist.* De kantonrechter zag eerder af van het opleggen van een straf, omdat de verdachten niet eerst waren gewaarschuwd door de buitengewoon opsporingsambtenaar (boa) maar direct waren bekeurd. Daartegen kwam de officier van justitie in hoger beroep. Het hof heeft nu het OM niet-ontvankelijk verklaard in de vervolging. Het hof stelt vast dat in verband met de coronapandemie onder verantwoordelijkheid van de Staatssecretaris van Infrastructuur en Waterstaat het Protocol verantwoord blijven reizen in het Openbaar Vervoer is vastgesteld. In het protocol is verduidelijkt hoe de mondkapjesplicht in het ov moest worden gehandhaafd. Volgens het hof blijkt uit het protocol dat boa's reizigers eerst zouden aanspreken op de plicht tot het dragen van een mondkapje. Als de aangesproken reiziger de aanwijzing tot het dragen van een mondkapje niet alsnog opvolgde, kon in het uiterste geval een boete worden gegeven. Reizigers mochten er dus op vertrouwen dat zij niet bekeurd zouden worden, zonder dat zij eerst werden aangesproken en in de gelegenheid waren gesteld alsnog een mondkapje op te doen of het ov te verlaten. Het OM mocht daarom niet tot strafvervolging overgaan in deze zaken, waarin de reiziger niet eerst was gewaarschuwd. (WA)

ECLI:NL:GHAMS:2022:3041
ECLI:NL:GHAMS:2022:3040
ECLI:NL:GHAMS:2022:3039)

Bron: rechtspraak.nl/Organisatie-en-contact/Organisatie/Gerechtshoven/Gerechtshof-Amsterdam/Nieuws/Paginas/Openbaar-Ministerie-niet-ontvankelijk-in-zaken-mondkapjesplicht-in-OV.aspx

328

Nationale Samenwerking tegen Ondermijnende Criminaliteit (NSOC)

In de maanden oktober en november 2022 heeft de Minister van Justitie en Veiligheid de Tweede Kamer geïnformeerd over de bestrijding van georganiseerde ondermijnende criminaliteit. Een afzonderlijk onderwerp daarbij betreft de Nationale Samenwerking tegen Ondermijnende Criminaliteit (NSOC). De NSOC is (als vervanger van het Multidisciplinaire Interventieteam MIT) opgericht voor het delen van informatie en het bedenken van nieuwe methoden om criminele structuren en hun verdienmodellen te verstoren. Het betreft de Politie, het openbaar ministerie, de Douane, de Belastingdienst, de FIOD, de Koninklijke Marechaussee en andere onderdelen van het Ministerie van Defensie. De focus van de NSOC ligt op de aanpak van criminele geldstromen en de achterliggende bedrijfsstructuren, zoals witwaspraktijken via handelsstromen en financiële dienstverleners die criminelen bij bedrijven helpen, corruptie en geweld. Ook wordt gericht gekeken naar logistieke dienstverleners van criminelen. De NSOC en de FIU-Nederland (Financial Intelligence Unit – Nederland) werken samen bij de aanpak van criminele geldstromen op alle voorkomende onderwerpen, waaronder Trade Based Money Laundering (TBML, het opzetten van handelsstructuren om crimineel geld wit te wassen). In de NSOC-labs, wordt in een experimentele omgeving gewerkt aan oplossingen voor specifieke problemen. Op 4 november jl. meldt de minister dat binnenkort de directeur van de NSOC het actieplan bespreekt met enkele burgemeesters en andere lokale partners om te verkennen hoe de NSOC en de lokaal bestuurlijke aanpak elkaar kunnen versterken. In deze verkenning wordt ook de motie van leden Michon-Derkzen (VVD) en Mutluer (PvdA) betrokken waarin wordt verzocht om een gezamenlijke agenda van de NSOC en de RIEC's (Regionale Informatie- en Expertise Centra). Er wordt uitgegaan van een totaalbudget van € 50 miljoen, inclusief beheerskosten, met een maximale formatie van 244 fte. (WA)

Bronnen: Kamerstukken II 2022/23, 24077, nr. 504, Kamerstukken II 2022/23, 29911, nr. 379 en Aanhangsel Handelingen II 2022/23, nr. 606

329

Kabinet presenteert nieuwe cybersecuritystrategie

Namens het kabinet presenteerde minister Yeşilgöz-Zegerius (Justitie en Veiligheid en coördinerend bewindspersoon cybersecurity), samen

met minister Adriaansens (Economische Zaken en Klimaat) en staatssecretaris Van Huffelen (Koninkrijksrelaties en Digitalisering), op 10 oktober 2022 de nieuwe Nederlandse cybersecuritystrategie 2022-2028. Bij de strategie hoort ook een actieplan met concrete acties om Nederland digitaal veiliger te maken. Minister Yeşilgöz-Zegerius: 'De digitale dreiging neemt fors toe waarbij criminelen en vijandige staten onze belangen bedreigen zoals de Nationaal Coördinator Terrorismebestrijding en Veiligheid concludeert. Daarom is nu actie nodig om onze digitale weerbaarheid te verhogen, het stelsel te versterken en de dreiging aan te pakken. Alleen dan zijn we als Nederland in staat om op een veilige manier de economische en maatschappelijke kansen van digitalisering te verzilveren, en tegelijkertijd onze veiligheid en publieke waarden te beschermen. Digitale systemen vormen het 'zenuwstelsel' van onze maatschappij Daarom moeten we deze systemen beschermen en zorgen dat we voorbereid zijn als er toch iets mis gaat. De hele overheid moet hierin voorop lopen en samenwerken met een netwerk van publiek en private partners'.

In de Nederlandse cybersecuritystrategie beschrijft het kabinet haar visie op de digitale samenleving en de rol van overheid, bedrijven en burgers daarin.

Om de gestelde doelen te bereiken wordt het stelsel rondom digitale veiligheid versterkt. Hiertoe worden bijvoorbeeld het Nationaal Cybersecurity Centrum, Digital Trust Center en het Cyber Security Incident Response Team for Digital Service Providers samengevoegd tot één nationale cybersecurity autoriteit. Daarnaast komt er wet- en regelgeving die helder en toetsbaar is waardoor vrijblijvendheid voor het treffen van maatregelen verleden tijd wordt. Eisen voor veilige hard- en software worden in Europees verband gesteld. Voor de totstandkoming en implementatie van de strategie werken alle ministeries samen, ook met publieke en private partners. (WA)

Bron: rijksoverheid.nl/actueel/nieuws/2022/10/10/kabinet-presenteert-nieuwe-cybersecuritystrategie

330

Duidelijker kader nodig voor verwerking persoonsgegevens strafrechtelijke onderzoeken

Het huidige juridische kader is nog onvoldoende aangepast aan de nieuwe realiteit van opsporingsonderzoeken waarbij de politie grote hoeveelheden persoonsgegevens verzamelt. Om de privacy van personen beter te beschermen, moet het Wetboek van Strafvordering een duidelijker kader bieden voor het verwerken van persoonsgegevens tijdens digitaal opsporingsonderzoek, concluderen onderzoekers van de Radboud Universiteit. Ook zou er beter toezicht moeten komen op de manier waarop politie en OM met deze gegevens omgaan in strafrechtelijke onderzoeken. Door inbeslagname of hacks van grote gegevensdragers heeft de politie steeds vaker toegang tot enorme hoeveelheden persoonsgegevens. Dit biedt kansen voor het digitale opsporingswerk en de vervolging van verdachten van zware misdrijven. Denk aan de miljoenen recent gekraakte (criminele) berichten van Ennetcom, EncroChat of Sky ECC. Ook biedt het kansen om actief strafbare feiten aan het licht te brengen door gegevens met elkaar te combineren via geavanceerde technologieën. Maar niet is duidelijk hoever de politie hierin mag gaan en hoe dit wettelijk geregeld moet worden. Uit het onderzoek, uitgevoerd in opdracht van het WODC, blijkt dat in het Wetboek van Strafvordering (Sv) vooral aandacht is voor de inzet van digitale opsporingsbevoegdheden: in welke gevallen, voor welke doelen en met toestemming van welke autoriteit mogen persoonsgegevens worden verzameld? Dat geldt zowel voor het huidige Sv als voor (de plannen voor de) modernisering van het Sv. Aan het verdere gebruik van die gegevens wordt veel minder aandacht besteed. Terwijl de politie juist door het verdere gebruik een (nieuwe) inbreuk op de privacy van burgers kan maken. Bijvoorbeeld door het uitvoeren van data-analyses met gegevens die zijn overgenomen uit een inbeslaggenomen server of computer. Het is niet duidelijk hoe de regels die daarover in de Wet politiegegevens (Wpg) staan zich verhouden tot het Sv. De onderzoekers bevelen aan om sommige regels uit de Wpg over te brengen naar het Sv. Zodat daarin een duidelijk kader wordt geboden voor het onderzoeken van gegevens tijdens de uitoefening van digitale opsporingsbevoegdheden. Ook pleiten ze voor meer specifieke regels voor strafvorderlijk onderzoek aan bulkgegevens. Daarnaast bevelen de onderzoekers aan om een commissie van toezicht op te richten die toezicht houdt op de politie en het OM wat betreft het verwerken van gegevens. Vergelijkbaar met de commissie die toezicht houdt op de inlichtingendiensten AIVD en MIVD. (WA)

Bron: wodc.nl/actueel/nieuws/2022/10/25/wet-moet-duidelijker-kader-bieden-voor-verwerking-persoonsgegevens-tijdens-strafrechtelijke-onderzoeken

331

Voorruiten ANPR-foto's automatisch geblindeerd

Inzittenden van auto's komen niet langer op de zogeheten ANPR-foto's te staan. Voorruiten worden voortaan automatisch geblurd op de foto's. Voorheen gebeurde dit blinderen handmatig, wat een erg arbeidsintensieve klus was. ANPR staat voor Automatic Number Plate Recognition. Het is gericht op het maken van foto's van kentekenplaten, niet op het fotograferen van inzittenden. Met ANPR-camera's werden sporadisch foto's gemaakt waarop onbedoeld personen herkenbaar voorkwamen. Dit is sinds 13 oktober 2022 verleden tijd. Foto's die worden gemaakt van alle kentekens die een politiecamera passeren, mogen 28 dagen worden bewaard op basis van artikel 126jj Wetboek van Strafvordering. Door het automatisch blinderen van voorruiten

wordt nog beter aan deze voorwaarde voldaan. (WA)

Bronnen: politie.nl/nieuws/2022/oktober/24/voorruiten-anpr-fotos-automatisch-geblindeerd.html

Kamerstukken I 2021/22, 33542, nr. j, k, l en m

332

Grote zorgen strafrechtadvocaten over te weinig transparantie hacken en aftappen

Het openbaar ministerie (OM) en de politie gebruiken de laatste jaren steeds vaker berichten die via versleutelde communicatiediensten als EncroChat zijn verstuurd als bewijsmateriaal. Strafrechtadvocaten vragen zich hardop af of deze berichten rechtmatig zijn verkregen, en of ze een betrouwbaar en volledig beeld opleveren in een rechtszaak, zo niet dan neemt de kans op een eerlijk proces af. Daarnaast staat de privacy voor alle burgers onder druk. Ruim honderd strafrechtadvocaten hebben in oktober een brandbrief naar de Minister van Justitie en Veiligheid, Tweede Kamer, Raad voor de rechtspraak en het openbaar ministerie gestuurd. Zij stuurden de brief omdat zij zich 'grote zorgen over de strafrechtspleging in Nederland' maken. (WA)

Bronnen: privacy-web.nl/artikelen/strafrechtadvocaten-slaan-alarm-over-opsporingmethoden-grens-is-bereikt/?

vanboomadvocaten.nu/brandbrief-strafrechtadvocatuur/

333

Helios, een politietool voor het creëren van één intelligencepositie op thema's

Op 10 november 2022 is het verslag vastgesteld van de vaste commissie voor Digitale Zaken van de Tweede Kamer, inhoudende een lijst van vragen en antwoorden, onder meer over de tool 'Helios'. Helios is een tool waarmee men op basis van een datamodel informatiebeelden ten behoeve van veiligheidsvraagstukken genereert die rechtmatig, juridisch en ethisch verantwoord zijn. Helios is geen enkelvoudige ICT-toepassing maar een applicatie waarin primair geregistreerde broninformatie verrijkt kan worden. Helios maakt voor wat betreft de softwareontwikkeling gebruik van een mix van producten die binnen de politie aanwezig zijn, producten die worden aangekocht en door de politie zelf ontwikkelde componenten. De ontwikkeling van de datatoepassingen en algoritmes geschiedt door datawetenschappers die binnen de politie werkzaam zijn. Het doel van Helios is om bij te dragen aan het binnen de politie creëren van één intelligencepositie op thema's. Vanuit deze centrale intelligencepositie worden, met behulp van gevalideerde datamodellen, inzichten gegenereerd die het politiewerk op strategisch, tactisch en operationeel niveau ondersteunen. Denk hierbij aan inzicht in ontwikkelingen op de cocaïnemarkt en de invloed die dit heeft op criminele samenwerkingsverbanden die zich op die markt begeven. Voor de toepassing van Helios wordt gebruikgemaakt van gegevens die zich al in de informatiesystemen van de politie bevinden en waarvan het mogelijk is om deze voor het doel van het verkrijgen van inzichten verder te verwerken. Daartoe kwalificeren verscheidene categorieën gegevens. Er is geen uniforme opvatting over de drempelwaarde wanneer er sprake is van 'big data', maar het ligt voor de hand om in het geval van Helios te spreken over een 'big data'-toepassing. De toepassing van algoritmen hierbij bevindt zich momenteel in een voorbereidende fase. Op dit moment is er nog geen sprake van de operationele inzet van zelflerende systemen, algoritmes of (semi)geautomatiseerde risicoprofielen. Het Wetboek van strafvordering en de Wet politiegegevens, alsook het geldende normenkader, bepalen de mogelijkheden voor het verder verwerken van gegevens binnen de politie. Het programma Helios wordt uitgevoerd in opdracht van de portefeuille intelligence. (WA)

Bron: Kamerstukken II 2022/23, 36200 VI, nr. 2 en VII, nr. 58, zoek.officielebekendmakingen.nl/kst-1058730.pdf

334

Handelingsperspectief leidinggevenden politie Wet screening

De politie heeft als werkgever de bevoegdheid om ambtenaren van politie aan een betrouwbaarheidsonderzoek te onderwerpen, zowel voorafgaand aan als tijdens het dienstverband. Door diverse ontwikkelingen, zoals de georganiseerde criminaliteit die dichter op rechtshandhavingsinstanties gaat zitten en de wens om meer informatie bij het onderzoek te betrekken, is aanscherping en verruiming van het betrouwbaarheidsonderzoek noodzakelijk. Deze aanscherping en verruiming hebben geleid tot de Wet screening ambtenaren van politie en politie-externen (hierna: de wet), die op 1 januari 2023 in werking zal treden. De wet bepaalt dat iedereen die bij (of voor) de politie werkt gescreend moet zijn. De uitkomst van de screening resulteert in een besluit, de Verklaring van betrouwbaarheid (hierna: Vvb). Indien deze Vvb wordt geweigerd, kan de medewerker zijn functie niet (meer) uitoefenen. Ontheffing uit de functie is hiervan het gevolg. Daarnaast voorziet de wet ook in continue controle op de betrouwbaarheid van de medewerker en de meldplicht, waardoor ook betrouwbaarheidsrisico's vroegtijdig kunnen worden gesignaleerd en aangepakt.

Zie voor het 'Besluit screening ambtenaren van politie en politie-externen' *Staatsblad* 2022, nr. 380. (WA)

Bron: Staatscourant 2022, 29728

335

Coalitie Europese landen in de strijd tegen georganiseerde misdaad

De coalitie van Europese landen in strijd tegen zware en georganiseerde misdaad wordt versterkt. Dat heb-

ben België, Duitsland, Frankrijk, Italië, Spanje en Nederland op 7 oktober 2022 in Amsterdam afgesproken. De opsporingsdiensten van de zes landen werken in onderzoeken veel samen, bijvoorbeeld dankzij het kraken van versleuteld berichtenverkeer van criminelen met EncroChat en Sky ECC. De samenwerking wordt opgevoerd en verbreed, bijvoorbeeld in verbinding met andere landen zoals in Latijns-Amerika. Minister Yeşilgöz-Zegerius van Justitie en Veiligheid heeft met ministers en vertegenwoordigers van justitie en van Binnenlandse Zaken uit België, Duitsland, Frankrijk, Italië en Spanje een meerjarig actieplan afgesproken om meer als één front samen te werken in de strijd tegen georganiseerde misdaad. Ook vertegenwoordigers van de Europese Commissie, Europol en Eurojust namen deel aan de bespreking. Het doel is om criminele netwerken en hun bedrijven te verstoren, te doorbreken en neer te halen door elkaars krachten meer te bundelen: middelen, expertise en interventies meer op elkaar afstemmen en gezamenlijk inzetten. De EU-wetgeving wordt hiervoor versterkt en samenwerkingsafspraken met landen van waaruit de betaling en handel in crypto's worden ondersteund. Innovaties worden ondersteund om de detectie van illegale goederen te vergroten en om informatievergaring en -deling tussen opsporingsautoriteiten te vergroten terwijl de bescherming van gegevens wordt behouden. (WA)

Bron: rijksoverheid.nl/actueel/nieuws/2022/10/07/coalitie-europese-landen-in-de-strijd-tegen-georganiseerde-misdaad

336

Pilots nieuwe Wetboek van Strafvordering

Vanaf 1 oktober 2022 wordt in vijf pilots praktijkervaring opgedaan met regelingen uit het Wetboek van Strafvordering (Sv), dat gemoderniseerd wordt. Het gaat over prejudiciële vragen, mediation, extra bevoegdheden voor de hulpofficier van justitie, audiovisuele registratie en gegevens na inbeslagname. Deze laatste pilot biedt een nieuwe opsporingsbevoegdheid inhoudend dat de politie nadat een apparaat, zoals een telefoon, tablet, computer of server in beslag is genomen, ook kennis mag nemen van informatie die na inbeslagname binnenkomt op het apparaat, deze informatie mag vastleggen en meenemen als bewijs. Ook wordt het toegestaan om een netwerkzoeking te verrichten (onderzoek aan een net inbeslaggenomen apparaat, en data die zich ergens anders bevinden). Ook wordt in de pilot bijgehouden hoe vaak gebruik wordt gemaakt van het doorbreken van een biometrische beveiliging (irisscan, gezichtsherkenning of vingerafdruk) tegen de wil van de gebruiker. Van deze bevoegdheid wordt al gebruikgemaakt op basis van een uitspraak van de Hoge Raad van 9 februari 2021. Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) evalueert de pilots en inzichten in bijvoorbeeld de werklasteffecten en financiële gevolgen van de nieuwe regelingen. Dit kan leiden tot hervorming of aanvulling van de regelingen, het beleid en de werkwijzen. (WA)

Bron: rechtspraak.nl/Voor-advocaten-en-juristen/Reglementen-procedures-en-formulieren/Strafrecht/Paginas/pilots-nieuwe-wetboek-van-strafvordering

337

Brief regering; wetsevaluatie Wet computercriminaliteit III en hackbevoegdheid politie

Op 16 september 2022 heeft de Minister van Justitie en Veiligheid het WODC-rapport 'De hackbevoegdheid in de praktijk, een empirisch onderzoek naar de uitvoering van de bevoegdheid tot het heimelijk en op afstand binnendringen in geautomatiseerd werk (artikelen 126nba, 126uba, 126zpa Sv)' aangeboden aan de Voorzitter van de Tweede Kamer. In dit rapport komt een aantal knelpunten naar voren die de uitvoering van de bevoegdheid bemoeilijken. Het betreft de manier waarop kan worden binnengedrongen, de inzet van commerciële middelen, de meldplicht voor onbekende kwetsbaarheden, het toezicht door de Inspectie Justitie en Veiligheid en de keuring van technische hulpmiddelen. De minister verwijst verder naar het rapport zelf. In 2020, 2021 en in 2022 heeft de Inspectie Justitie en Veiligheid rapporten uitgebracht over het toezicht dat zij uitoefent op de bevoegdheid politie. Gelet op het voorgaande verwacht de minister voor haar inhoudelijke reactie op de rapporten geruime tijd nodig te hebben. Zij verwacht deze in het voorjaar van 2023 naar de Tweede Kamer te kunnen toesturen. In 2024 is het tweede deel van de evaluatie voorzien, waarin de overige delen van de wet worden behandeld. (WA)

Bron: Kamerstukken II 2022/23, 34372, nr. 30

338

'Politiewerk op het web', onduidelijkheid over online gegevensvergaring

Er moet meer duidelijkheid komen over de bevoegdheden waarbinnen de politie informatie mag verzamelen op internet. Dat staat in het rapport 'Politiewerk op het web'. Internet heeft het politiewerk op uiteenlopende manieren veranderd. Een van de veranderingen is dat er voor de politie een bron van gegevens bij is gekomen. In dit verkennende onderzoek wordt in kaart gebracht op welke wijze de politie online gegevens vergaart ten behoeve van zowel intelligence als opsporing (internet rechercheren). De uitkomsten zijn gebaseerd op interviews met 41 respondenten die werkzaam zijn in de informatieorganisatie, basisteams en rechercheonderdelen. Uit het onderzoek komt naar voren dat het online vergaren van gegevens in steeds meer organisatieonderdelen binnen de politie plaatsvindt. Dit maakt dat er behoefte is aan afstemming binnen en ook tussen eenheden: wie doet wat? Daarnaast blijkt dat het gebruik van

online vergaarde gegevens ten behoeve van intelligence gebruikelijker is dan in het kader van opsporing. In beide domeinen wordt zowel handmatig gewerkt als gebruikgemaakt van software. Met name bij de online intelligencevergaring worden door de politie onduidelijkheden met betrekking tot bevoegdheden ervaren. Deze gaan vooral over de reikwijdte van artikel 3 van de Politiewet en over het gezag op het gebied van online gegevensvergaring ten behoeve van de openbare orde. In de opsporing speelt vooral de vraag wanneer het online vergaren van gegevens een 'stelselmatig' karakter krijgt, wat wil zeggen dat het een meer dan geringe inbreuk maakt op de persoonlijke levenssfeer van burgers. Het online vergaren van gegevens is een vakgebied binnen digitaal politiewerk. Het bijhouden van dit vakgebied kost tijd en is voor politiemensen die incidenteel actief zijn met het online vergaren van gegevens niet goed mogelijk. Op basis van het onderzoek worden verschillende aandachtspunten voor de doorontwikkeling van online gegevensvergaring binnen de politie meegegeven. Deze hebben vooral betrekking op de digitale 'fitheid' van leidinggevenden, een betere verankering van het vakgebied binnen de recherche, het verduidelijken van het juridisch kader en het waarderen en faciliteren van de professionals die dit relatief nieuwe politiewerk uitvoeren. (WA)

Bronnen: politieenwetenschap.nl/persberichten/politie-vergaart-steeds-vaker-gegevens-online-122
politie.nl/nieuws/2022/september/27/00-onduidelijkheid-over-online-gegevensvergaring.html

Internet en technologie

339

OESO publiceert rapport over het gebruik van Dark Patterns door bedrijven

De OESO bracht onlangs een rapport uit over 'Dark Commercial Patterns'. Het OESO-directoraat voor Wetenschap, Technologie en Innovatie (STI) onderneemt een breed scala aan activiteiten om beter te begrijpen hoe informatie- en communicatietechnologieën (ICT's) bijdragen aan duurzame economische groei en sociaal welzijn.

Het rapport 'Dark Commercial Patterns' gaat in op 'de groeiende behoefte om dark commercial patterns uitgebreid aan te pakken' en bouwt verder op eerdere discussies over dit onderwerp. Het rapport bespreekt onder meer de definitie en aard van dark patterns, hun prevalentie en impact op consumenten, alsook regelgevings-, handhavings-, educatieve en technische maatregelen.

De term dark patterns (donkere (commerciële) patronen) verwijst naar een grote verscheidenheid aan praktijken die vaak worden aangetroffen in online gebruikersinterfaces en die ertoe leiden dat consumenten keuzes maken die mogelijk niet in hun belang zijn, onder meer door gebruik te maken van vooroordelen van consumenten. Ze proberen consumenten er meestal toe te brengen meer geld, persoonlijke gegevens of aandacht te geven dan gewenst. Zo zijn ze onlosmakelijk verbonden met een onderliggend businessmodel, ook al hebben ontwerpers van gebruikersinterfaces vaak geen kwaad in de zin.

Daarnaast bevat het rapport ook verschillende bijlagen die dieper ingaan op concrete instanties van dark patterns en de gevolgen ervan, met voorbeelden van handhavingsacties. (JA)

Bron: oecd-ilibrary.org/science-and-technology/dark-commercial-patterns_44f5e846-en

340

Privacy en gegevensbescherming bij sportapps vaak ondermaats

Sport- en fitnessapps, zoals Strava, winnen jaar na jaar aan populariteit. Het zijn ook vaak echte sociale netwerken geworden. Je deelt er zeer persoonlijke gegevens, en soms onbewust ook je woon- of werklocatie als startpunt van je sportactiviteiten. De apps laten je meestal toe die locaties te verbergen, maar onderzoekers van de KU Leuven ontdekten dat die optie in vele gevallen een vals gevoel van veiligheid geeft. In het verleden is al vaker gebleken dat Strava kampt met privacyproblemen. In 2018 bijvoorbeeld werden geheime militaire bases in conflictgebieden Syrië en Irak ontdekt door de app. Om gebruikers te beschermen verbergt Strava tegenwoordig automatisch de eerste en laatste tweehonderd meter van een route.

De Leuvense onderzoekers ontwikkelden een zogenaamde inference attack en pasten die toe op geanonimiseerde activiteiten die werden gedeeld op sportapps. 'Zo konden we bij de 1,4 miljoen Strava-activiteiten die we analyseerden tot 85 procent van de verborgen locaties toch blootleggen, puur op basis van de extra gegevens die publiek werden prijsgegeven', zegt één van de onderzoekers. De onderzoekers hebben hun bevindingen met Strava gedeeld en zitten binnenkort met de makers aan tafel om hun voorstellen voor verbeteringen te bespreken. (TW & JA)

Bronnen: nieuws.kuleuven.be/nl/2022/je-loopt-meer-in-de-kijker-dan-je-denkt-privacy-bij-sportapps-vaak-ondermaats
security.nl/posting/773015/Onderzoekers%3A+privacyzones+Strava+geven+vals+gevoel+van+veiligheid

341

De onzichtbare uitbuiting die kunstmatige intelligentie mogelijk maakt

Een recent artikel legt de problematische arbeidsomstandigheden en supply chains van kunstmatige intelligentiesystemen bloot. De manier waarop dergelijke systemen vaak worden getraind, vergt enorme hoeveelheden tijdrovend werk, zoals het labelen, sorteren en categoriseren van gegevens, en wordt opgesplitst in kleinere taken om dan uitbesteed te worden aan 'datawerkers' over de hele wereld. Deze 'datawerkers' hebben een verschrikkelijk laag loon en werken vaak in

erbarmelijke omstandigheden. Dit werk is cruciaal om kunstmatige intelligentiesystemen mogelijk te maken, maar wordt vaak genegeerd in verkooppraatjes van bedrijven, overheden en internationale organisaties die stellen dat KI en automatisering innovatief en onvermijdelijk zijn. Evenmin wordt er vaak over gesproken als men het over AI-ethics heeft. Dit roept vragen op betreffende de bredere impact van KI-systemen en wie deze systemen eigenlijk ten goede komen. Het werk dat bijvoorbeeld moet gebeuren om ongewenste inhoud van sociale media te houden, is bijzonder traumatiserend. Het artikel gaat verder in op hoe de ontwikkeling van KI-systemen berust op de uitbuiting van goedkope arbeid door rechteloze en gemarginaliseerde werknemers in hedendaagse sweatshops. De auteurs van dit artikel stellen dat als we AI-ethics serieus willen nemen, we de uitbuiting in de KI-industrie een halt toe moeten roepen, door transnationale organisaties te steunen en solidariteit tussen de werknemers op te bouwen. Verder moeten we misleidende beelden en verhalen over de 'superintelligentie' van KI in het publieke debat verwerpen. (JA)

Bron: noemamag.com/the-exploited-labor-behind-artificial-intelligence/

342

Inzet van intelligente technologie in het onderwijs

De Nederlandse Onderwijsraad heeft een rapport gepubliceerd over de impact van het gebruik van 'intelligente technologieën' in het onderwijs. Technologie zoals AI kan volgens het rapport een toegevoegde waarde hebben als het slim en verantwoord wordt ingezet, maar het kan ook leiden tot verschraling van het onderwijs. (JA)

Bron: onderwijsraad.nl/publicaties/adviezen/2022/09/28/inzet-van-intelligente-technologie

343

Wetenschappers zijn te slordig met kunstmatige intelligentie

Onderzoekers gebruiken vaak kunstmatige intelligentie in hun studies om voorspellingen te doen op basis van data en slimme algoritmes. Twee Amerikaanse wetenschappers waarschuwen in een artikel dat kunstmatige intelligentie vaak onjuist wordt toegepast wat ten koste gaat van de betrouwbaarheid en reproduceerbaarheid van wetenschappelijk onderzoek.

Twee onderzoekers van de universiteit van Princeton deden een literatuurstudie in zeventien disciplines, van geneeskunde tot politicologie. In twintig reviews, de meeste recente maar ook een aantal oudere, telden ze 329 publicaties waarvan de resultaten niet of maar deels herhaalbaar waren, door manco's in het gebruik van AI-modellen. Dat kan leiden tot 'bizar overoptimistische conclusies'. De onderzoekers gebruiken een ruime definitie van 'reproduceerbaar': niet alleen moeten de data en algoritmische codes traceerbaar zijn, de data moeten ook correct zijn geanalyseerd. Belangrijkste valkuil bij het gebruik van machinelearning is het lekken van data, waardoor de uitkomsten van een onderzoek vervuild kunnen raken. De onderzoekers identificeren acht soorten data leaking, zoals het onbedoeld opnemen van niet-relevante data of verschillende datasets niet goed uit elkaar houden. Als testdata vermengd raken met data uit de evaluatieset, leidt dat tot 'betere' maar bij nader inzien ondeugdelijke voorspellingen. De computer heeft de uitkomst dan al verwerkt in zijn voorspellingen. Het onderzoek van de Princeton-wetenschappers is een preprint: nog niet getoetst voor publicatie in een wetenschappelijk tijdschrift. Niettemin heeft hun waarschuwing veel losgemaakt bij wetenschappers die zich zorgen maken over AI-methodes voor kwantitatief voorspellend onderzoek. Aan een online workshop van Kapoor over het onderwerp namen meer dan 1600 academici deel. (TW)

Bron: nrc.nl/nieuws/2022/08/10/wetenschappers-zijn-te-slordig-met-machine-learning-a4138587

344

Cyber Security Raad: chatberichten kunnen op korte termijn niet afgetapt worden

Berichten via diensten zoals WhatsApp zijn sterk beveiligd, tot frustratie van opsporingsdiensten die digitale criminele communicatie willen aftappen. De Cyber Security Raad (CSR) adviseert het kabinet zich te focussen op 'reële alternatieven'.

De CSR ziet op 'korte en middellange termijn' geen mogelijkheden om Nederlandse opsporingsdiensten op een veilige manier mee te laten lezen met versleutelde digitale berichten. Het Ministerie van Justitie en Veiligheid wordt geadviseerd op zoek te gaan naar 'reële alternatieve mogelijkheden' om criminelen op te sporen, zoals hacken en het opvragen van bedrijfsgegevens.

Berichten via chatdiensten zoals WhatsApp, Instagram en Signal zijn steeds vaker sterk beveiligd met zogenaamde end-to-end-encryptie. De berichten zijn daardoor goed beschermd, maar criminelen óók door die strengere beveiliging. Het Ministerie van Justitie en Veiligheid zoekt daarom al jarenlang naar manieren om 'achterdeurtjes' te bouwen in de versleuteling van die berichtenapps, zodat aftappen mogelijk wordt. Ook in de Europese Unie lopen zulke onderzoeken. In afwachting van de uitkomsten van die bredere zoektochten naar veilige aftapmogelijkheden, adviseert de CSR het kabinet nu alternatieven te verkennen. De raad spreekt zich overigens nadrukkelijk niet uit 'over de (on-)wenselijkheid van functionele of technische inperkingen van encryptie'.

CSR-lid Bart Jacobs, hoogleraar aan de Radboud Universiteit Nijmegen, noemt het advies niettemin

'een doorbraakje'. In de Cyber Security Raad zitten naast academici en experts uit het bedrijfsleven ook vertegenwoordigers vanuit de opsporings- en inlichtingendiensten. 'Op dat punt – of nu wel of niet verder gezocht moet worden naar mogelijkheden om een decryptiebevel te geven – daar is de raad niet eensgezind over. Encryptie wordt nog niet door iedereen zonder meer geaccepteerd en dus wordt een oordeel zorgvuldig vermeden. Maar dat die diensten bereid zijn na te denken over alternatieven, dáár ligt vooral de meerwaarde van dit advies.' (TW)

Bron: nrc.nl/nieuws/2022/08/25/cyber-security-raad-chatberichten-kunnen-op-korte-termijn-niet-afgetapt-worden-a4139839

345

Verenigd Koninkrijk stopt met immigratie-algoritme dat volgens critici racistisch is

Het Britse Ministerie van Binnenlandse Zaken heeft toegezegd niet langer een algoritme te gebruiken voor het verwerken van visumaanvragen. Op dit algoritme is kritiek omdat het raciaal vooringenomen zou zijn. Critici stellen dat het onjuist is dat het algoritme de nationaliteit van de aanvrager meeneemt in de beslissing omdat dit er voor zorgt dat 'mensen uit rijke blanke landen "Speedy Boarding" krijgen; armere mensen van kleur worden naar de achterkant van de rij geduwd'.

Het ministerie ontkent dat zijn systeem racistisch bevooroordeeld is en er lopen hierover nog steeds rechtszaken. Toch heeft het ministerie ermee ingestemd het algoritme niet langer te gebruiken en is het van plan om later dit jaar een nieuwe versie te lanceren. In de tussentijd zal het VK een tijdelijk systeem invoeren dat geen nationaliteit gebruikt om aanvragen te sorteren. (TW)

Bron: technologyreview.com/2020/08/05/1006034/the-uk-is-dropping-an-immigration-algorithm-that-critics-say-is-racist

346

Onderzoek naar hybride mens-AI-aanpak

Onderzoekers van MIT's Computer Science and AI Laboratory (CSAIL) hebben een methode ontwikkeld die kan helpen bij een betere samenwerking tussen mensen en AI-systemen bij het nemen van beslissingen. De methode maakt gebruik van twee afzonderlijke machinelearningmodellen; één neemt de daadwerkelijke beslissing, of dat nu het diagnosticeren van een patiënt is of het verwijderen van een bericht op sociale media, en één voorspelt of de AI of de mens de betere beslisser is.

De onderzoekers testten de hybride mens-AI-aanpak in verschillende scenario's, waaronder beeldherkenning en het detecteren van haatspraak. Het AI-systeem kon zich aanpassen aan het gedrag van de expert en indien nodig de beslissing aan hem overlaten, waardoor de twee besluitvormers samen snel een nauwkeurigheidsniveau bereikten dat hoger was dan bij een eerdere hybride mens-AI-aanpak. Hoewel de experimenten in dit onderzoek nog relatief eenvoudig waren, denken de onderzoekers dat een dergelijke aanpak uiteindelijk kan worden toegepast op complexe beslissingen, zoals in de gezondheidszorg. (TW)

Bron: technologyreview.com/2020/08/05/1006003/ai-machine-learning-defer-to-human-expert

347

'Geigerteller' die piept als computer data naar Google stuurt

Een ontwikkelaar heeft een app voor besturingssysteem Linux gemaakt die piepjes laat horen op het moment dat een website, programma of dienst data naar Google verstuurt. Op Twitter heeft de ontwikkelaar een korte demo geplaatst. Hierin bezoekt hij een vacaturesite van de Nederlandse overheid en krijgt daarbij regelmatig een buzz te horen, zelfs als hij alleen maar het webadres intypt of een menu uitklapt. Dat gebeurt volgens hem niet alleen in Google-browser Chrome, maar ook in Firefox. (TW)

Bronnen: tweakers.net/geek/200208/ontwikkelaar-maakt-geigerteller-die-piept-als-os-data-naar-google-stuurt.html
twitter.com/bert_hu_bert/status/1561466204602220544

348

Mozilla wil fonds opzetten voor 'verantwoorde technologie'

Mozilla, de organisatie achter de browser Firefox, wil volgend jaar een investeringsfonds opzetten voor startups 'die werken aan technologie die het internet beter moet maken'. Daarmee doelt het onder meer op techologie die 'privacyvriendelijk, transparant en inclusief is'.

In het aankondigingsbericht over het zogenoemde Mozilla Venturesfonds beweert Mozilla's executive director Mark Surman dat veel startups en kleine ontwikkelaars 'obstakels tegenkomen wanneer ze producten willen maken die mensen op de eerste plaats zetten', zoals het vinden van investeerders. Het fonds is bedoeld voor startende bedrijven in een vroeg stadium waarvan de producten of technologieën 'een of meer van de waarden in het Mozilla Manifest bevorderen, namelijk privacy, inclusiviteit, transparantie, toegankelijkheid en menselijke waardigheid'.

Het investeringsfonds moet nog worden opgericht. Dat gebeurt volgend jaar. Toch heeft Mozilla al investeringen gedaan in drie startups: wachtwoordmanager HeyLogin, Block Party, een app met blokkeertools voor Twitter-gebruikers en Secure AI Labs, een ontwikkelaar die software maakt voor ziekenhuizen. Volgens Surman onderschrijven deze drie bedrijven 'het idee dat de digitale wereld privé, veilig en respectvol kan zijn'. Geïnteresseerden die denken dat ze aan de eisen voor het fonds voldoen of investeerders die willen meewerken aan het fonds

kunnen contact opnemen met Mozilla. (TW)

Bron: tweakers.net/nieuws/203036/mozilla-wil-fonds-van-35-miljoen-dollar-opzetten-voor-verantwoorde-technologie.html

349

Instagram introduceert leeftijdsverificatie met video of ID-bewijs

Instagram-gebruikers die hun leeftijd willen veranderen van jonger dan 18 jaar naar ouder dan 18 jaar moeten voortaan ook in Europa hun leeftijd verifiëren. Dergelijke gebruikers kunnen hiervoor een foto van een identiteitsbewijs uploaden of een 'videoselfie' opnemen en versturen.

Het verificatieproces werd al eerder in de Verenigde Staten uitgerold en is nu ook van toepassing in Europa. Vooralsnog geldt de vereiste alleen voor gebruikers die hun leeftijd willen veranderen van jonger dan 18 jaar naar ouder dan 18 jaar. Bij het aanmaken van een nieuw account kan een gebruiker simpelweg een geboortedatum naar keuze opgeven.

De videoverificatie gebeurt in samenwerking met het bedrijf Yoti, dat op basis van ingezonden beelden inschat hoe oud een gebruiker is. Andere websites waaronder YouTube en Airbnb gebruiken ook leeftijdsverificatie middels beeldherkenning. (TW)

Bron: tweakers.net/nieuws/203146/instagram-brengt-leeftijdsverificatie-met-video-of-id-bewijs-uit-in-europa.html

350

Vlaanderen krijgt camera's die herkennen of automobilist smartphone vasthoudt

De Vlaamse regering start volgend jaar een proef waarbij camera's worden ingezet die herkennen of automobilisten een smartphone vasthouden. Er wordt onder andere naar Nederland als voorbeeld gewezen, waar dergelijke camera's al langer worden gebruikt. Privacyexperts en ook de Belgische politiek hebben hun bedenkingen en waarschuwen voor risico's zoals gezichtsherkenning. Drie jaar geleden organiseerde de Vlaamse regering ook al een proef met het gebruik van cameratoezicht. Betrapte automobilisten werden destijds echter niet beboet, omdat het gebruik van de 'slimme camera's' om overtredingen op te sporen onwettig is. Dit keer heeft de regering een achterdeur gevonden om de pilot toch te laten plaatsvinden, zo meldt *De Tijd*. Een agent controleert de gemaakte camerabeelden en stelt dan vast of er sprake is van een overtreding. (TW)

Bron: security.nl/posting/773603/Vlaanderen+krijgt+camera%27s+die+herkennen+of+automobilist+smartphone+vasthoudt

Curiositeit

351

Gemeente Stadskanaal mocht het identiteitsbewijs los van voorwaarden klant inzien

De gemeente Stadskanaal wil het recht op de lopende uitkering van een vrouw vaststellen en nodigt haar uit voor een gesprek. De sociaal-rechercheur vraagt haar voor het gesprek om haar identiteitsbewijs te tonen. De vrouw wil dit alleen doen onder de voorwaarde dat de sociaal-rechercheur een overeenkomst tekent die inhoudt dat de gemeente met haar afspreekt de persoonsgegevens niet aan derden te verkopen. Dat doet de sociaal-rechercheur niet en daarna komt het niet meer tot een inhoudelijk gesprek. De vrouw vindt het niet tekenen niet juist en schrijft de Nationale ombudsman. De Nationale ombudsman vindt dat de gemeente Stadskanaal om het identiteitsbewijs van de vrouw mocht vragen. In de wet staat dat voor de uitvoering van de Participatiewet om het identiteitsbewijs kan worden gevraagd. (CE)

Bron: nationaleombudsman.nl/nieuws/brieven/2022153

Werkten mee aan 'Actualiteiten België': Yung Shin Van Der Sype (YV), counsel Crowell & Moring, vrijwillig medewerker KU Leuven Centre for IT & IP Law – imec; Christopher Dumont, associate Crowell & Moring.
Coördinatie en editing: Yung Shin Van Der Sype, counsel, Crowell & Moring, vrijwillig medewerker KU Leuven Centre for IT & IP Law – imec.

Privacy algemeen

352

Marktenhof stelt prejudiciële vragen in de *IAB Europe*-zaak

Op 2 februari 2022 had de Geschillenkamer van de Gegevensbeschermingsautoriteit (GBA) een administratieve geldboete opgelegd aan Interactive Advertising Bureau Europe (IAB Europe). Bovendien had de GBA IAB Europe twee maanden de tijd gegeven om een actieplan op te stellen om haar activiteiten in overeenstemming te brengen met de AVG. Tegen deze beslissing ging IAB Europe in beroep bij het Brusselse Marktenhof.

De feiten in het kort: De GBA had een resem klachten ontvangen die gericht waren tegen IAB Europe die betrekking hadden op de overeenstemming van het zogenaamde Transparency & Consent Framework (TCF) met de AVG. Het TCF, dat door IAB Europe werd ontwikkeld, heeft tot doel bij te dragen tot de naleving van de AVG door organisaties die gebruikmaken van het OpenRTB-protocol. Dit protocol is een van de meest gebruikte protocollen voor Real Time Bidding, d.w.z. de ogenblikkelijke, geautomatiseerde veiling van gebruikersprofielen voor het verkopen en het aankopen van advertentieruimte op internet. Wanneer gebruikers voor het eerst een website of applicatie bezoeken wordt hen om hun toestemming gevraagd voor het verzamelen en delen van hun persoonsgegevens. De gebruikers kunnen op deze interface ook bezwaar maken tegen verschillende soorten van verwerking op basis van de gerechtvaardigde belangen van adtech-verkopers. Het TCF vergemakkelijkt het vastleggen van de voorkeuren van de gebruikers. De voorkeuren van de gebruikers worden gecodeerd en opgeslagen in een TC-string, die wordt gedeeld met de organisaties die deelnemen aan het OpenRTB-systeem zodat zij weten waarvoor de gebruikers hun toestemming hebben gegeven. In haar beslissing van 2 februari 2022, oordeelde de GBA dat IAB Europe als verwerkingsverantwoordelijke optreedt met betrekking tot de registratie van het toestemmingssignaal, en het bijhouden van de bezwaren en de voorkeuren van individuele gebruikers door middel van een unieke TC-string. IAB Europe betwist dit.

Het Marktenhof buigt zich over het beroep van IAB Europe in een tussenarrest van 7 september 2022. Alvorens recht te doen, besluit het de volgende prejudiciële vragen te stellen aan het Hof van Justitie:

1. a) Moet artikel 4, 1 AVG, gelezen in samenhang met de artikelen 7 en 8 EU-Handvest, in die zin worden uitgelegd dat een tekenreeks die de voorkeuren van een internetgebruiker in verband met de verwerking van zijn persoonsgegevens op gestructureerde en machineleesbare manier capteert, een persoonsgegeven uitmaakt ten aanzien van (1) een sectororganisatie die aan haar leden een standaard ter beschikking stelt waarbij zij hen voorschrijft op welke wijze die tekenreeks praktisch en technische gegenereerd, opgeslagen en/of verspreid moet worden, en (2) de partijen die op hun websites of in hun apps die standaard geïmplementeerd hebben en op die manier dus toegang hebben tot die tekenreeks?
   b) Maakt het daarbij een verschil uit als de implementatie van de standaard inhoudt dat deze tekenreeks samen met een IP-adres beschikbaar is?
   c) Leidt het antwoord op vraag a) + b) tot een andere conclusie indien deze normerende sectororganisatie zelf geen wettelijke toegang heeft tot de persoonsgegevens die binnen deze standaard door haar leden worden verwerkt?
2. a) Moeten de artikelen 4, 7 en 24, 1 AVG, gelezen in samenhang met de artikelen 7 en 8 EU-Handvest, aldus worden uitgelegd dat een normerende sectororganisatie als verwerkingsverantwoordelijke moet worden gekwalificeerd, wanneer zij aan haar leden een standaard voor het beheer van toestemming aanbiedt die naast een bindend technisch kader voorschriften bevat waarin gedetailleerd wordt bepaald hoe deze toestemmingsgegevens, die persoonsgegevens uitmaken, opgeslagen en verspreid moeten worden?
   b) Leidt het antwoord op vraag a) tot een andere conclusie indien deze sectororganisatie zelf geen wettelijke toegang heeft tot de persoonsgegevens die binnen deze standaard door haar leden worden verwerkt?
   c) Indien de normerende sectororganisatie als verwerkingsverantwoordelijke of gezamenlijke verwerkingsverantwoordelijke voor de verwerking van de voorkeuren van internetgebruikers moeten worden aangeduid, strekt die (gezamenlijke) verantwoordelijkheid van de normerende sectororganisatie zich dan ook automatisch uit naar de daaropvolgende verwerkingen door derden waarvoor de voorkeuren van de internetgebruikers werd bekomen, zoals gerichte online reclame door uitgevers en vendors?

Het Marktenhof schorst de behandeling van de zaak en zendt de zaak naar de rol in afwachting van het antwoord op de prejudiciële vragen. (YV)

Bron: Hof van Beroep Brussel, Sectie Marktenhof, 19e kamer A, Kamer voor marktzaken 7 september 2022, 2022/AR/292; Gegevensbeschermingsautoriteit, Geschillenkamer 2 februari 2022, Beslissing ten gronde nr. 21/2022,

gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-21-2022.pdf

353

Foto en graad van verwantschap voor een digitale membershipkaart

De Geschillenkamer van de Gegevensbeschermingsautoriteit (GBA) heeft in een beslissing van 17 oktober 2022 nogmaals uiteengezet en verder verduidelijkt wat wel en niet kan bij digitale membershipkaarten.

In deze zaak konden eigenaars van een vakantiehuis en hun familieleden enkel aan een voordelig tarief toegang krijgen tot het zwembad van een vakantiepark indien zij een digitale membershipkaart aanmaakten. Hiervoor moesten de aanvragers van de kaart hun naam en foto verstrekken, alsook die van andere gebruikers van de kaart met vermelding van de graad van verwantschap ten aanzien van de aanvrager. Deze gegevens werden opgeslagen in een databank.

De klager wou genieten van de voordelen van de digitale membershipkaart zonder foto's en zonder de graad van verwantschap van de andere gebruikers mee te delen. Toen dit hem geweigerd werd diende hij klacht in bij de GBA.

De Geschillenkamer stelt vooreerst vast dat de verwerking steunde op een rechtmatigheidsgrond die de verwerking van persoonsgegevens in de context van een digitale membershipkaart kan rechtvaardigen, namelijk de uitvoering van een overeenkomst. De verwerkingsverantwoordelijke had daarnaast haar gerechtvaardigd belang ingeroepen, maar deze rechtsgrond werd nooit gecommuniceerd aan de kaarthouders. De Geschillenkamer herinnert eraan dat de AVG vereist dat de verwerkingsverantwoordelijke voorafgaand de verwerking over de rechtsgrond moet beslissen en dat *post factum* een rechtsgrond toevoegen in strijd is met deze bepaling.

Een verwerkingsgrond op zich volstaat evenwel niet. De andere beginselen inzake de verwerking van persoonsgegevens, waaronder de minimale gegevensverwerking, moeten ook gerespecteerd worden. Dit houdt in dat de persoonsgegevens toereikend, ter zake dienend en beperkt moeten zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. De verwerkingsverantwoordelijke rechtvaardigde de verwerking van de foto en de graad van verwantschap van andere gebruikers om misbruik van de membershipkaart te vermijden. De Geschillenkamer erkent dit doeleinde als rechtmatig, maar stelt evenwel een inbreuk vast nu dit doeleinde evenzeer kon gerealiseerd worden zonder verwerking van de foto's van de gebruikers van de membershipkaart en hun graad van verwantschap. Het volstaat om bij de ingang van het zwembad een louter visuele controle van de identiteitskaart uit te voeren, waarop zowel de naam als de foto van de betrokkene zichtbaar staan vermeld. De graad van verwantschap kan op geen enkele wijze gecontroleerd worden aan de hand van enig document zodat dit in elk geval niet noodzakelijk is. Deze loutere visuele controle valt trouwens volgens de GBA niet onder het toepassingsgebied van de AVG, vermits dergelijke controle niet gepaard gaat met enige vorm van verwerking. Deze werkwijze is bijgevolg minder intrusief.

De gegevensverwerkingsverantwoordelijke werd bevolen om de verwerking binnen een termijn van twee maanden in overeenstemming te brengen met de AVG, zonder bijkomende sanctie. (CD)

Bron: Gegevensbeschermingsautoriteit, Geschillenkamer 17 oktober 2022, Beslissing ten gronde 147/2022, gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-147-2022.pdf

354

Onduidelijk geformuleerd verzoek tot inzage

De Geschillenkamer van de Gegevensbeschermingsautoriteit (GBA) heeft in een beslissing van 11 oktober 2022 uitspraak gedaan over het dwingend karakter van een verzoek tot inzage.

In deze zaak had een verzekeringsmaatschappij nagelaten te antwoorden op een vraag van een betrokkene die vroeg of de verzekeringsmaatschappij gegevens over hem verwerkte en indien dit het geval zou zijn om hiervan een kopie te ontvangen, alsook om ingelicht te worden over de wettelijk voorgeschreven informatie van de AVG waaronder de verwerkingsdoeleinden, de categorieën van persoonsgegevens, de bestemmingen van de persoonsgegevens, de bewaartijd van de persoonsgegevens, de rechten van de betrokkene, de bron vanwaar de persoonsgegevens werden verzameld en of de persoonsgegevens buiten de Europese Unie werden doorgegeven.

De verzekeringsmaatschappij antwoordde binnen de twee weken bij monde van haar functionaris voor gegevensbescherming dat de informatie zou worden opgevraagd, maar dat het advies van de adviserende arts vertrouwelijk is en niet kon worden overgemaakt. De medische rapporten zouden worden overgemaakt aan de arts aangewezen door de betrokkene.

De betrokkene antwoordde dat medische rapporten rechtstreeks aan hem of haar moesten worden overgemaakt. De verzekeringsmaatschappij heeft hier nooit op geantwoord waarop de betrokkene een klacht indiende bij de GBA.

De Geschillenkamer herinnert eraan dat een verzoek tot toegang van persoonsgegevens niet zonder gevolg kan blijven louter omdat het onvolledig is, gebaseerd is op een verkeerde wetsbepaling of blijk geeft van een verkeerd begrip van het ingeroepen recht. Als een verwerkingsverantwoordelijke zich op een uitzondering wil beroepen om niet in te gaan op een verzoek, of om niet binnen de wettelijke termijn te reageren, dan dient hij die keuze eveneens binnen een maand mee te delen aan de betrokkene. Zonder het standpunt van de verzekeringsmaatschappij te hebben gehoord, is de Geschillenkamer *prima facie* van oordeel dat er sprake kan zijn van een inbreuk.

Om de verzekeringsmaatschappij te informeren over het feit dat het mogelijk een inbreuk pleegt op de AVG, beveelt de Geschillenkamer in een beslissing voorafgaand aan een beslissing ten gronde, om binnen een maand gevolg te geven aan het verzoek tot toegang of om argumenten kenbaar te maken, waarna de zaak hervat zal worden. Dit geeft de verzekeringsmaatschappij nog een kans om zich te conformeren en mogelijks een lichtere sanctie opgelegd te krijgen. (CD)

Bron: Gegevensbeschermingsautoriteit, Geschillenkamer 11 oktober 2022, Beslissing ten gronde 144/2022, autoriteprotectiondonnees.be/publications/ordonnance-n-144-2022.pdf

355

Gegevensuitwisseling in het kader van een buitenlands vermogensonderzoek

De Geschillenkamer van de Gegevensbeschermingsautoriteit (GBA) heeft in een beslissing van 11 oktober 2022 uitspraak gedaan over het uitwisselen van gegevens in het kader van een buitenlands vermogensonderzoek.

In deze zaak deelde een sociale huisvestigingsmaatschappij persoonsgegevens van huurders van een sociale woning met derden in het kader van een buitenlands vermogensonderzoek.

De Geschillenkamer stelt vooreerst vast dat de verwerking steunt op een wettelijke verplichting. Sociale huisvestigingsmaatschappijen moeten met name nagaan of hun (kandidaat-)huurders aan de toepasselijke voorwaarden voldoen, zowel bij de aanvang als tijdens de volledige duurtijd van de huurovereenkomst. Sociale woninghuur is immers voorbehouden aan kwetsbare personen die zelf niet kunnen voorzien in hun huisvestigingsbehoeften zonder hulp. Om als verwerkingsgrond te kunnen worden aangewend, dient de wettelijke bepaling voldoende duidelijk, precies en voorspelbaar te zijn. Na een analyse van de desbetreffende bepaling stelt de Geschillenkamer vast dat dit het geval is en de wettelijke bepaling bijgevolg kan dienen als grondslag voor de controle en naleving van de inschrijvingsvoorwaarden en dit tijdens de gehele duur van de sociale huurovereenkomst. Daarbij merkt de Geschillenkamer op dat voor de vervulling van een taak van algemeen belang of openbaar gezag, de verwerking vaak niet steunt op een nauwkeurig omschreven wettelijke bepaling, maar wel op een algemene machtiging. In dit geval moet de instantie belast met de vervulling van de taak van algemeen belang of openbaar gezag zelf een afweging maken over de noodzakelijkheid van de verwerking.

Ook de noodzakelijkheid van het buitenlands vermogensonderzoek wordt in deze zaak bevestigd aangezien de betrokkene al meerdere keren was uitgenodigd om eventueel bezit in het buitenland te melden, eerst bij de ondertekening van een verklaring op eer en vervolgens wanneer de sociale huisvestigingsmaatschappij de betrokkene via een waarschuwingsbrief op de hoogte bracht van haar voornemen om een buitenlands vermogensonderzoek door te voeren wegens ernstige aanwijzingen of vermoedens van een buitenlands onroerend bezit.

In het kader van het buitenlands vermogensonderzoek werden persoonsgegevens doorgegeven naar Turkije. De Geschillenkamer stelt vast dat hiervoor eveneens een wettelijk grond voorhanden was, namelijk de noodzakelijkheid voor de behartiging van een zwaarwegend algemeen belang dat is erkend in het recht van de Unie. De doorgifte wordt noodzakelijk geacht voor dezelfde redenen als hierboven uiteengezet.

De GBA stelt wel een inbreuk vast op artikel 28, lid 2 en 3 van de AVG omdat de volgende elementen ontbraken in de overeenkomst met de verwerker:

- de handtekening van de directeur die de sociale huisvestigingsmaatschappij vertegenwoordigt;
- de datum waarop de verwerkingsovereenkomst aanvangt;
- een omschrijving van de duur van de verwerking;
- een omschrijving van het soort persoonsgegevens en de categorieën van betrokkenen en van de aard van de verwerking en
- een voorafgaande specifieke of algemene schriftelijke toestemming van de sociale huisvestigingsmaatschappij aan de verwerker om andere verwerkers in dienst te nemen.

Aangezien de sociale huisvestigingsmaatschappij onmiddellijk de verwerkingsovereenkomst in lijn heeft gebracht met de AVG, besluit de Geschillenkamer enkel een berisping te formuleren.

Bijkomend kan worden opgemerkt dat de Geschillenkamer in haar beslissing stelt dat het onderzoek door de Inspectiedienst van de Gegevensbeschermingsautoriteit op een loyale wijze dient te gebeuren. Indien het antwoord van de verwerkingsverantwoordelijke voor de Inspectiedienst niet volstaat, komt het aan de Inspectiedienst toe om te verduidelijken op welke punten meer informatie nodig is door bijvoorbeeld specifiekere vragen te stellen over een bepaald onderwerp of document. De Inspectiedienst kan niet louterweg uit een gebrekkig antwoord een inbreuk op de verantwoordingsplicht vaststellen. Het is immers voor de verwerkingsverantwoordelijke niet altijd gemakkelijk om een omvattend antwoord te formuleren op de algemene en ruime vragen van de Inspectiedienst. (CD)

Bron: Gegevensbeschermingsautoriteit, Geschillenkamer 18 oktober 2022, Beslissing ten gronde 149/2022, gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-149-2022.pdf

356

Berisping voor het niet rechtmatig plaatsen van een bewakingscamera in een privétuin

Een buur had een bewakingscamera geplaatst die toelaat om ook de tuin en de leefruimte van twee van zijn achterburen te capteren.

De Geschillenkamer van de Gegevensbeschermingsautoriteit (GBA) sprak zich in een beslissing van 17 oktober 2022 uit in deze zaak. Vooreerst bevestigt de GBA haar bevoegdheid. De beelden van personen die worden vastgelegd met bewakingscamera's vallen immers onder het begrip *persoonsgegeven* en de registratie en opslag van die beelden is een geautomatiseerde verwerking van persoonsgegevens. Vervolgens benadrukt de Geschillenkamer dat wanneer het bewakingssysteem het privédomein van anderen of de openbare ruimte bestrijkt, er geen sprake kan zijn van een uitsluitend *zuiver persoonlijke of huishoudelijke activiteit*.

Persoonsgegevens mogen enkel op rechtmatige wijze worden verwerkt. Daarnaast moet de verwerking ook behoorlijk en transparant gebeuren. Artikel 8 van de Camerawet verbiedt elk geheim gebruik van camera's, en artikel 7 § 2, zesde lid van de Camerawet wijst op de informerende rol van een pictogram (en de verplichte plaatsing hiervan). Uit de vaststellingen van de lokale politiedienst en de Inspectiedienst volgt dat er aanvankelijk geen pictogram werd voorzien, omdat de verweerder namelijk niet op de hoogte was van het bestaan van een verplichting in die zin. Uit een latere vaststelling bleek dat er een – weliswaar foutief – pictogram was voorzien dat niet aan de wettelijke vereisten voldeed. Dit maakt een inbreuk uit op artikel 5, lid 1, a) van de AVG.

Persoonsgegevens mogen enkel worden verzameld voor een welbepaald en uitdrukkelijk omschreven doeleinde. Ook de Camerawet vereist een mededeling aan de politie voor een bewakingscamera in een niet publiek toegankelijke plaats. *In casu* werd de doelstelling van de camerabewaking laattijdig geregistreerd, wat een inbreuk uitmaakt op artikel 5, lid 1, b) van de AVG.

Verder stelt de Geschillenkamer ook een inbreuk vast op artikel 5, lid 1, c) van de AVG, aangezien er meer beelden werden verwerkt dan noodzakelijk. De camera had namelijk een bewegingsfunctie waarvan de verantwoordelijke initieel geen gebruikmaakte.

De verwerking van persoonsgegevens kan slechts rechtmatig zijn wanneer ze is gesteund op één van de rechtsgronden uit artikel 6, lid 1 AVG. De verantwoordelijke die een verwerking steunt op haar gerechtvaardigd belang, dient hiertoe de *doeltoets*, de *noodzakelijkheidstoets*, en de *afwegingstoets* te kunnen doorstaan.

Diefstal kan de doeltoets rechtvaardigen. Het plaatsen van een bewakingscamera aan een garage/carport voor het beschermen van motorvoertuigen van hoge waarde is een gerechtvaardigd doel.

Voor de noodzakelijkheidstoets dient rekening gehouden te worden met het beginsel van minimale gegevensverwerking. Volgens de Geschillenkamer kan het continu filmen van een deel van de tuin en een deel van het huis van de klagers niet aanzien worden als *ter zake dienend*, noch als *noodzakelijk*, om het gerechtvaardigde belang van de verantwoordelijke te waarborgen. Bijgevolg is er sprake van een inbreuk op artikel 6, lid 1, f) van de AVG.

Alles in acht genomen, kiest de Geschillenkamer ervoor om enkel een berisping te formuleren aangezien de ernst van de inbreuk geen administratieve geldboete vereist. (FN)

Bronnen: Wet van 21/03/2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, BS 31 mei 2007; Koninklijk besluit van 10 februari 2008 tot vaststelling van de wijze waarop wordt aangegeven dat er camerabewaking plaatsvindt, BS 21 februari 2008; Koninklijk besluit van 8 mei 2018 betreffende de aangiften van de plaatsing en het gebruik van bewakingscamera's en betreffende het register van de beeldverwerkingsactiviteiten van bewakingscamera's, BS 15 april 2019; Gegevensbeschermingsautoriteit, Geschillenkamer 17 oktober 2022, Beslissing ten gronde 138/2022, gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-138-2022.pdf

357

Verstrekking van identiteitskaart als voorwaarde tot gegevenswissing

Een verwerkingsverantwoordelijke kan weigeren gevolg te geven aan het verzoek van een betrokkene om diens rechten uit te oefenen, wanneer hij aantoont dat hij niet in staat is de betrokkene te identificeren.

De Geschillenkamer van de Gegevensbeschermingsautoriteit herinnert er evenwel aan dat de verantwoordelijke er zich voor moet behoeden om niet meer gegevens te verwerken dan nodig met het oog op de identificatie van de betrokkene.

Door in de privacyverklaring de uitoefening van rechten te onderwerpen aan de voorafgaande verstrekking van een identiteitsbewijs miskent de verantwoordelijke het beginsel van minimale gegevensverwerking. Wanneer de verwerkingsverantwoordelijke gebruikmaakt van het e-mailadres van een betrokkene om deze direct marketing berichten toe te sturen, en de betrokkene zich wenst uit te schrijven voor de ontvangst van die berichten, dan is het voldoende dat de betrokkene zich aan de hand van hetzelfde e-mailadres tot de verwerkingsverantwoordelijke richt om zijn rechten uit te oefenen. (FN & YV)

Bron: Gegevensbeschermingsautoriteit, Geschillenkamer 29 september 2022, Beslissing 145/2022, gegevensbeschermingsautoriteit.be/publications/waarschuwing-en-berisping-nr.-145-2022.pdf

Agenda

Agenda

358

Dag van de FG uitgesteld

De Autoriteit Persoonsgegevens laat weten dat de 'Dag van de FG' op 12 oktober helaas niet door kon gaan. Door capaciteitsproblemen bij de Autoriteit Persoonsgegevens (AP) kon men deze dag niet organiseren zoals u van de AP mag verwachten. De Dag van de FG wordt verplaatst naar het voorjaar van 2023.

Via de FG-nieuwsbrief worden FG's op de hoogte gehouden over de Dag van de FG en de ontwikkelingen in het vakgebied. Meld u aan voor de FG-nieuwsbrief.

Meer informatie: autoriteitpersoonsgegevens.nl – Info voor FG's

Opleiding Data Science en Gegevensbescherming

Deze opleiding biedt deelnemers een afwisselend en praktijkgericht programma van computerwetenschappen en juridische verdieping in onder meer de privacywetgeving. Mr. Friederike van der Jagt (advocaat Hunter Legal, fellow Onderzoekcentrum Onderneming & Recht Radboud Universiteiten) en dr. Jaap-Henk Hoepman (universitair hoofddocent Radboud Universiteit) zijn als (hoofd)docenten verbonden aan deze opleiding.

Datum: 15 december 2022, 17 januari, 9 februari, 7 en 30 maart en 4 april 2023

Locatie: La Vie Meeting Center Utrecht

Meer informatie: ru.nl/cpo/cursus/cursussen/ie-informatie-privacyrecht/opleiding-data-science-gegevensbescherming-0/

Doe mee aan de Nederlandse Privacy Awards!

Op 28 januari 2023 (Europese Dag van de Privacy) worden door Stichting Privacy First weer de jaarlijkse Nederlandse Privacy Awards uitgereikt!

Er zijn 4 categorieën waarvoor inschrijvingen genomineerd konden worden:

1. categorie Consumentenoplossingen (van bedrijven voor consumenten);
2. categorie Bedrijfsoplossingen (binnen een bedrijf of business-to-business);
3. categorie Non-profit (overheid, zorg en onderwijs);
4. Aanmoedigingsprijs voor een baanbrekend(e) technologie, initiatief of persoon.

Datum: 28 januari

Meer informatie: privacyawards.nl

Openbare surveillance 'The Follower'

Het nieuwe project van de Vlaamse digitale kunstenaar Dries Depoorter laat aan de hand van AI-technologie zien hoe Instagramfoto's werkelijk tot stand komen.

Openbare camera's die gericht zijn op toeristische trekpleisters waar je kunt zwaaien naar het thuisfront. Het klinkt onschuldig, maar het nieuwe kunstproject van Depoorter, 'The Follower', laat zien dat je ongemerkt meer wordt gefilmd dan je denkt.

Aan de hand van de geo-tag op Instagram kan de kunstenaar via open-source camera's het moment vinden waarop de Instagramfoto wordt gemaakt. Met zijn project wil Depoorter laten zien wat een persoon met beperkte toegang tot data en camera's al kan bereiken en maken. 'Wat zou een overheid dan kunnen, die veel meer toegang heeft tot data?' Depoorter wil de gevaren van nieuwe technologieën aantonen. Want daar zijn mensen niet altijd bewust van vindt de kunstenaar.

Meer informatie: driesdepoorter.be

Call for Panels CPDP2023 – Ideas That Drive Our Digital World

This call for panels is aimed at academic consortia, research projects, think tanks and other research organisations and welcomes proposals that address the ideas that drive our digital world. Welcome are cutting edge panels in all areas related to technology, privacy and data protection, and particularly invite proposals that fit the general conference theme.

Another call, to individuals for academic research papers, will go out in October 2022.

For-profit organisations interested in organising a panel at CPDP or otherwise wishing to support the conference, are kindly asked to refer to the Sponsorship page or reach out to info@cpdpconferences.org for further information.

Dates of the CPDP-conference 2023 are 24, 25 and 26 May 2023.

More information: cpdpconferences.org/call-for-panels#form

Cameratoezicht & Privacy

Tijdens de cursus Cameratoezicht & Privacy besteden we aandacht aan de privacyregels die gelden voor de inzet van camera's. Met behulp van de casuïstiek leert u hoe u een camerabeleid inricht.

Datum: 2 februari 2023

Locatie: Utrecht

Meer informatie: berghauserpontacademy.nl/cursussen/

Privacybeleid bij DPIA's en cameratoezicht

Met dit cursuspakket, bestaande uit de e-learning DPIA en de fysieke workshop Cameratoezicht & Privacy til je jouw privacybeleid naar een (nog) hoger niveau. Een combinatie van online leren in eigen tempo over DPIA's, plus in groepsverband aan de slag met het inrichten van een rechtmatig camerabeleid.

Datum: 2 februari 2023

Locatie: Utrecht

Meer informatie: berghauserpontacademy.nl/cursussen/

DPIA-praktijkdag

Tijdens deze cursus ga je samen met de docenten het volledige DPIA-proces doorlopen en worden diverse praktische DPIA-modellen behandeld. Je kunt vragen inbrengen en gaat oefenen met een volledig en goede uitvoering van een DPIA. Na afloop kun je aan de slag met het uitvoeren van een DPIA binnen jouw organisatie.

Datum: 15 februari 2023
Locatie: Utrecht

Meer informatie: berghauserpontacademy.nl/cursussen/

Privacywetgeving in de opsporing

Tijdens deze cursus wordt u op de hoogte gebracht van de wetgeving die op de gegevensverwerkingen door BOA's van toepassing is. U leert wanneer uw BOA's zich aan de Wpg moet houden, wanneer aan de AVG en wat de belangrijkste verschillen zijn tussen deze wetten. Ook leert u welke stappen er moeten worden gezet om aan de Wpg te voldoen, hoe gegevens gedeeld kunnen worden en hoe gegevens uit opsporingsactiviteiten kunnen worden gebruikt in het toezichtwerk.

Datum: 16 februari 2023
Locatie: Utrecht

Meer informatie: berghauserpontacademy.nl/cursussen/

Privacy Officer 2.0

Voor veel organisaties is het verplicht om een interne privacy toezichthouder (privacy officer) aan te wijzen. Maar ook zonder die plicht is steeds vaker een hoofdrol weggelegd voor interne privacyadviseurs. Als Privacy Officer 2.0 bent u in staat een eigen strategie te ontwikkelen m.b.t. privacybeleid die u in de praktijk kunt brengen of waarmee u uw management adviseert en overtuigt. Haal de benodigde kennis in huis om de impact van de AVG op uw organisatie praktisch in kaart te brengen. Al 6 jaar dé basisopleiding voor Privacy Officers! Met nieuwe experts (o.a. Udo Oelen, NS), checklists en digitale handreiking AVG compliance.

Datum: meerdere startdata in het jaar, eerstvolgende: 15, 16, 20 en 30 maart en 1, 2 , 15 en 16 juni 2023
Locatie: Amsterdam en online

Meer informatie: outvie.nl/privacyofficer

Gegevensverwerking en Privacy in het sociaal domein

Met deze vierdaagse cursus Privacy in het sociaal domein wordt u opgeleid tot privacyprofessional in het sociaal domein. U verwerft kennis van de wet, kunt adviseren over de werkprocessen en weet op welke manier gegevens uitgewisseld kunnen worden.

Datum: 21 en 28 maart en 4 en 11 april 2023
Locatie: Utrecht

Meer informatie: berghauserpontacademy.nl/cursussen/

Leergang Senior Privacy Professional

In de Leergang Senior Privacy Professional krijgt u verdiepende kennis over leiderschapscompetenties, vergroot u uw eigen effectiviteit en geeft u invulling aan uw (seniore) rol. Aan de hand van casuïstiek en opdrachten met complexe situaties gaat u de diepte in en krijgt u competenties waarmee u als senior professional kunt optreden en hoe u invloed en sturing in de organisatie krijgt en houdt.

De opleiding is ontwikkeld voor de moderne privacyprofessional die complexe vraagstukken niet uit de weg gaat en binnen de organisatie het verschil weet te maken.

Datum: meerdere startdata in het jaar, eerstvolgende: 20 en 27 maart en 3, 13 en 20 april 2023
Locatie: Amsterdam

Meer informatie: outvie.nl/senior-privacy-professional

Privacy en arbeidsrecht

In deze halfdaagse cursus 'Privacy en arbeidsrecht' leert u over de belangrijkste privacythema's en privacygerelateerde vragen op de werkvloer, en krijgt u handvatten voor uw dagelijkse praktijk.

Datum: 6 april 2023
Locatie: Utrecht

Meer informatie: berghauserpontacademy.nl/cursussen/

De AVG en de basisregistraties van de publieke sector

De cursus AVG en de basisregistraties van de publieke sector geeft inzicht in het stelsel van de basisregistraties en de verhouding met de AVG.

Datum: 13 april 2023
Locatie: Utrecht

Meer informatie: berghauserpontacademy.nl/cursussen/

Auditing Privacy

Met de inwerkingtreding van de AVG zijn er nieuwe normenkaders. De focus ligt primair op het compliant zijn van gegevensbescherming. Het auditen van privacy onder de AVG zal nog een uitdaging worden.

Zorg dat u goed op de hoogte bent van alle aspecten die komen kijken bij een privacyaudit en voorkom dat u (privacy)risico's over het hoofd ziet. Deze masterclass geeft u concrete handvatten voor een adequate aanpak en uitvoering van privacy-audits. Hierdoor maakt u de organisatie privacycompliant en in control.

Datum: meerdere start data in het jaar, eerstvolgende: 6 en 12 oktober en 3 november 2023
Locatie: Amsterdam en online

Meer informatie: outvie.nl/privacyaudit

Implementatie Data-ethiek

Deze praktijkgerichte, hybride training leert u omgaan met de ethische vraagstukken van data en persoonsgegevens. Ook leert u de morele verantwoordelijkheid van uw functie en de praktische implementatie van data-ethiek binnen uw organisatie.

U gaat aan de slag met ethische casussen en maakt een plan van aanpak voor het implementeren van data-ethiek. Op de laatste trainingsdag gaat u uw plannen presenteren aan experts uit het bedrijfsleven. Deze experts geven u feedback op de plannen en tips en tricks om ethiek onderdeel van de bedrijfsvoering te maken.

Datum: ga naar outvie.nl/data-ethiek voor updates omtrent data 2023

Locatie: Amsterdam en online

Meer informatie: outvie.nl/data-ethiek

Actualiteitenreeks Next Step Privacy Compliance

Als dataprivacyprofessional moet u juist nu op de hoogte zijn van actualiteiten. Zo kunt u uw privacycompliancebeleid hierop aanpassen. De explosieve toename en beschikbaarheid van data en persoonsgegevens door connected devices, platforms en algoritmes zet privacy en dataprotectie onder druk. Om grip op de gevolgen voor dataprotectie en het continu naleven van wetgeving te krijgen (en houden) is de actualiteitenreeks ontwikkeld, bestaande uit zes keuzemodules.

In deze reeks komen actuele issues en oplossingen aan bod rond datadoorgiftes, onafhankelijk toezicht en het continu voldoen aan privacy wet- en regelgeving.

Datum: ga naar outvie.nl/privacy-compliance voor updates omtrent data 2023

Locatie: online

Meer informatie: outvie.nl/privacy-compliance

Privacy by Design

Privacy by Design (PbD) is een zware vereiste uit de AVG en stelt de privacybescherming van betrokkenen centraal. Dit vraagt om een overall strategie en een integrale aanpak. Het niet of onvoldoende meenemen van privacy in producten of werkwijzen kan resulteren in risico's die moeilijk beheersbaar zijn, met al dan niet desastreuze gevolgen. Denk aan de SyRi- en Toeslagenaffaire, waarbij gegevens onverantwoord en niet AVG-compliant gebruik zijn.

Deze training geeft u concrete handvatten om Privacy by Design praktisch te maken en structureel te verankeren in uw organisatie. Hierdoor maakt u de organisatie AVG-proof en in control en verkleint u de kans op maatregelen van toezichthouder(s) en boetes.

Datum: ga naar outvie.nl/privacy-compliance voor updates omtrent data 2023

Locatie: Amsterdam en online

Meer informatie: outvie.nl/privacybydesign

Inhoudsopgave 2022