LOUWERS
IP|TECHNOLOGY ADVOCATEN

JAARUPDATE
DATA PRIVACY
2021

De Algemene Verordening Gegevensbescherming vierde in 2021 alweer haar derde verjaardag. Privacy is dan ook een onderwerp dat binnen de meeste organisaties niet meer is weg te denken. De ontwikkelingen binnen dit rechtsgebied gaan bovendien razendsnel. De Europese- en nationale wetgevers zitten niet stil en hetzelfde kan gezegd worden over de toezichthouders. Ook lijken steeds meer particulieren en bedrijven de gang naar de rechter te vinden als het gaat over privacy. Om uw geheugen op te frissen, treft u in deze jaarupdate een overzicht van interessante juridische ontwikkelingen die zich in 2021 binnen dit rechtsgebied hebben voorgedaan.

Wet- en regelgeving

Europees niveau

Internationale doorgifte

In 2020 werden de privacyregels inzake internationale doorgifte aangescherpt naar aanleiding van het Schrems II-arrest van het HvJ EU en de daaropvolgende richtsnoeren van de EDPB. Ook het afgelopen jaar gebeurde er veel op het gebied van internationale doorgifte. De Europese Commissie publiceerde op 4 juni 2021 nieuwe EU Standard Contractual Clauses ('SCCs') voor de doorgifte van persoonsgegevens naar landen buiten de Europese Economische Ruimte ('EER'). De oude SCCs mogen vanaf 27 september 2021 niet langer worden gebruikt voor nieuwe doorgiftes of doorgiftes waarbij de onderliggende verwerking wijzigt. Vanaf 27 december 2022 zullen ook bestaande doorgiften niet langer gelegitimeerd kunnen worden op basis van de oude SCCs en zal doorgifte dus alleen zijn toegestaan op basis van de nieuwe SSCs of een andere wettelijke legitimering. Hier kunt u meer lezen over de nieuwe SSCs.

Op 4 juni 2021 heeft de Europese Commissie ook een template verwerkersovereenkomst gepubliceerd, die een verwerkingsverantwoordelijke en verwerker binnen de EER met elkaar kunnen sluiten. De standaard sluit aan bij de nieuwe SSC's. In de verwerkersovereenkomst is onder andere opgenomen dat nieuwe partijen eenvoudig kunnen toetreden tot de verwerkersovereenkomst. Er wordt in de standaard niets geregeld over aansprakelijkheid.

ePrivacy

De invoering van de ePrivacy-verordening ('EPV') kan – nog steeds – met recht een hoofdpijndossier worden genoemd. De EPV heeft betrekking op elektronische communicatie en bevat onder meer regels over het gebruik van metadata, cookies en direct marketing. In februari 2021 is een definitief tekstvoorstel vastgesteld dat nu ter onderhandeling is ingebracht in de triloog; het overleg tussen Europese Commissie, Europees Parlement en de Raad van Ministers. Verwacht wordt dat de EPV niet voor 2023 in werking zal treden en, na een overgangsperiode van twee jaar, in 2025 van toepassing wordt.

AI-verordening

Op 21 april 2021 presenteerde de Europese Commissie het voorstel voor de Wet op de artificiële intelligentie, ook bekend als de AI-verordening. De AI-verordening kent een risico gebaseerde aanpak. Hoe meer risico een AI-systeem met zich meebrengt, hoe strikter de regels die ervoor gelden. AI-systemen die in strijd zijn met EU-waarden of die de fundamentele rechten en vrijheden van personen schenden zijn zelfs helemaal verboden. De AI-verordening kent specifieke bepalingen voor overheidsorganisaties en roept een *European Artificial Intelligence Board* in het leven.

eIDAS 2.0-verordening

De Europese Commissie presenteerde op 3 juni 2021 het voorstel tot aanpassing van de eIDAS-verordening. Het voorstel kent regels met betrekking tot de *European Digital Identity* en heeft als doel de doeltreffendheid van de huidige eIDAS-verordening te verbeteren, de voordelen ervan uit te breiden tot de private sector en betrouwbare digitale identiteiten

voor alle Europeanen te faciliteren. Daartoe wordt onder andere het concept om een *European Digital Identity Wallet* (digitale portemonnee) te gebruiken, geïntroduceerd. De *wallet* moet het mogelijk maken voor Europeanen om virtueel attributen op te slaan, zoals rijbewijs, diploma's en bankrekeningnummer, en naar keuze te delen met organisaties.

Data Governance Act

Eind 2020 werd het tekstvoorstel van de *Data Governance Act* ('DGA') gepubliceerd en op 30 november 2021 werd duidelijk dat in de triloog overeenstemming was bereikt over een definitieve tekst. De DGA beoogt het delen van data uit verschillende sectoren en lidstaten te vergemakkelijken en betrouwbaarder te maken, onder andere door de introductie van "gegevensbemiddelingsdiensten" als de data persoonsgegevens zijn en door bij te dragen aan de ontwikkeling van *European data spaces* waarbinnen data vrijelijk kan worden uitgewisseld tussen private en publieke partijen met als doel het stimuleren van innovatie door hergebruik van data. De DGA zorgt er ook voor dat de mogelijkheden van hergebruik van beschermde data uit de publieke sector (zoals persoonsgegevens en data beschermd door intellectuele eigendomsrechten) ruimer worden. Tot slot moet de DGA het beschikbaar stellen van gegevens in het algemeen belang (data-altruïsme) bevorderen.

Digital Services Act & Digital Markets Act

Zoals we in ons vorige jaaroverzicht schreven, zijn eind 2020 de tekstvoorstellen voor de *Digital Services Act* ('DSA') en de *Digital Markets Act* ('DMA') bekendgemaakt. Op 25 november 2021 bereikten de EU-ministers een akkoord over de tekstvoorstellen. De DSA en DMA hebben tot doel een veiliger digitale ruimte te creëren waarin de grondrechten van alle gebruikers van digitale diensten worden beschermd en gelijke spelregels tot stand te brengen om innovatie, groei en concurrentievermogen te stimuleren, zowel op de Europese interne markt als wereldwijd. Er wordt gestreefd naar een definitief akkoord in 2022. Na inwerkingtreding wordt een deel van de bepalingen uit de DSA direct toepasselijk en een ander deel na zes maanden. Voor de DMA bedraagt deze laatste termijn drie maanden.

Data Act

Op 6 december 2021 publiceerde de Europese Commissie de resultaten van de openbare raadpleging over de nog vast te stellen *Data Act* ('DA') waarin onder andere de toegang tot en het delen van data tussen bedrijven en de overheid in het openbaar belang en het delen van data tussen bedrijven onderling gereguleerd gaan worden. Daarnaast moet de DA onderwerpen gaan reguleren als het gebruik van *smart contracts* in het kader van gegevensdeling, de rechten op niet-persoonsgegevens die worden gegenereerd bij professioneel gebruik van *Internet-of-Things*-toepassingen, de verbetering van portabiliteit van data voor zakelijke gebruikers van clouddiensten en de waarborgen die moeten gelden bij het gebruik van niet-persoonsgegevens in een internationale context. Tot slot zal de DA de regels inzake de rechtsbescherming van databanken gaan wijzigen. Het tekstvoorstel van de Europese Commissie wordt in 2022 verwacht.

Minimumeisen aan digitale veiligheid slimme apparaten

Op 29 oktober 2021 zijn regels gepubliceerd die de cyberveiligheid van alle draadloze apparaten die met het internet zijn verbonden moet vergroten. Deze *Internet-of-Things*-apparaten, zoals routers, beveiligingscamera's, slimme thermostaten, koelkasten, verlichting en deurbellen, moeten vanaf 2024 aan minimumeisen voldoen. Zo moet de consument voor ingebruikname van het slimme apparaat eerst zelf een sterk wachtwoord instellen in plaats van dat een zwak standaardwachtwoord volstaat, moeten de slimme apparaten regelmatig en gemakkelijk geüpdatet kunnen worden, moeten persoonlijke en financiële gegevens van de consument afgeschermd worden en moet de consument de mogelijkheid krijgen de gegenereerde data te beheren en te verwijderen.

Nationaal niveau

Corona

De Wet publieke gezondheid is in 2021 verschillende keren gewijzigd vanwege de maatregelen om verspreiding van het Coronavirus tegen te gaan. Zo werd op 22 november 2021 het wetsvoorstel Tijdelijke wet verbreding inzet corona-toegangsbewijzen ingediend. Met het wetsvoorstel wordt beoogd het coronatoegangsbewijs verplicht te stellen voor werknemers in sectoren waar het coronatoegangsbewijs ook aan bezoekers wordt gevraagd, zoals horeca, cultuur en niet essentiële detailhandel. Daarnaast wil het kabinet ook dat er een toegangsbewijsplicht voor werknemers komt op werkplekken waar het risico op besmettingen hoog is. Als een werkgever zorgdraagt voor een beschermingsniveau dat vergelijkbaar is met het beschikken over een coronatoegangsbewijs, geldt de verplichting tot het tonen van een coronatoegangsbewijs niet.

Wetvoorstel Wet gegevensverwerking door samenwerkingsverbanden

Het wetsvoorstel Wet gegevensverwerking door samenwerkingsverbanden ('WGS') beoogt een juridische grondslag te creëren voor het systematisch delen en verwerken van persoonsgegevens, waaronder door profilering, door samenwerkingsverbanden die bestaan uit bestuursorganen en private partijen die persoonsgegevens verwerken voor zwaarwegende algemene belangen, zoals de bestrijding van fraude en georganiseerde criminaliteit. Het wetsvoorstel is in behandeling bij de Eerste Kamer en heeft daar aanleiding gegeven tot het inwinnen van nader advies van de Autoriteit Persoonsgegevens, Raad van State en het College voor de Rechten van de Mens. Het is nog niet bekend wanneer de Eerste Kamer over het wetsvoorstel stemt.

Zorg

Op 3 mei 2021 is het wetsvoorstel Wet elektronische gegevensuitwisseling in de zorg ('Wegiz') ingediend bij de Tweede Kamer. Voor specifieke gegevensuitwisselingen gaat gelden dat deze elektronisch moeten plaatsvinden. Bovendien kunnen er eisen aan taal en techniek worden gesteld en kan worden bepaald dat verplicht gebruikgemaakt moet worden van gecertificeerde ICT-producten of -diensten.

Op 1 juni 2021 werd de consultatieversie van de Wet kwaliteitsregistraties zorg ('Wkz') gepubliceerd. De Wkz gaat het onder strikte omstandigheden mogelijk maken uitsluitend gepseudonimiseerde persoonsgegevens van patiënten zonder hun toestemming te verwerken ten behoeve van kwaliteitsregistraties die een algemeen belang dienen en zijn opgenomen in een register dat het Zorginstituut gaat bijhouden.

De Wet digitale overheid ('Wdo') legt de basis voor verdere digitalisering van de overheid en regelt onder andere de manier waarop burgers en bedrijven kunnen inloggen bij de overheid, bij zorgverleners en zorgverzekeraars en bij pensioenfondsen. Het wetsvoorstel werd op 18 februari 2020 door de Tweede Kamer aangenomen en is na van vragen van de Eerste Kamer aangepast door middel van een novelle. De novelle is op dit moment in behandeling bij de Tweede Kamer en zodra die erover heeft gestemd zal de Eerste Kamer het wetvoorstel en de novelle behandelen.

Toezichthouders

European Data Protection Board

Internationale doorgifte

Zoals eerder aangegeven, is er in 2021 weer veel gebeurd op het gebied van internationale doorgifte. Zo zijn de EDPB aanbevelingen 01/2020 definitief aangenomen op 18 juni 2021. Hierin wordt ingegaan op de mechanismes en maatregelen die organisaties kunnen treffen om ervoor te zorgen dat de doorgifte van persoonsgegevens aan derde landen rechtsgeldig plaatsvindt. Duidelijk wordt dat organisaties een zogenaamde *data transfer impact assessment* ('DTIA') moeten uitvoeren, voordat zij persoonsgegevens aan derde landen - niet EER-landen - mogen doorgeven. Een DTIA is zowel verplicht wanneer de doorgifte wordt gebaseerd op SSCs als wanneer *Binding Corporate Rules* ('BCRs') als doorgiftemechanisme worden gebruikt. Een DTIA is niet verplicht wanneer de doorgifte gebaseerd kan worden op een adequaatheidsbesluit van de Europese Commissie. Verder gaat de EDPB in op eventuele aanvullende technische, organisatorische en contractuele maatregelen die getroffen kunnen worden wanneer uit de DTIA zou blijken dat het beschermingsniveau in het derde land niet voldoende adequaat is. Bekijk hier het volledige stappenplan van de EDPB.

Op 28 juni 2021 is een adequaatheidsbesluit voor het VK aangenomen. Daarmee oordeelt de Europese Commissie dat het niveau van bescherming van persoonsgegevens in het VK gelijkwaardig is aan dat in de EU. Van 1 januari 2021 tot 28 juni 2021 gold een overgangsperiode. In die periode konden organisaties persoonsgegevens aan het VK blijven doorgeven zonder dat aanvullende maatregelen voor de doorgifte nodig waren. Dat blijft nu zo. Andersom kunnen organisaties in de VK ook vrij persoonsgegevens versturen naar organisaties in de EU.

Op 7 juli 2021 zijn er ter consultatie richtsnoeren gepubliceerd inzake gedragscodes als instrument voor doorgiftes. Hierin worden onder meer praktische richtsnoeren gegeven over de inhoud van gedragscodes, het proces voor de aanneming ervan en de betrokken actoren, alsmede de eisen waaraan een gedragscode voor internationale doorgiften moet voldoen en welke garanties erin moeten worden geboden.

Verder zijn er op 18 november 2021 richtsnoeren over de wisselwerking tussen de toepassing van artikel 3 AVG (territoriale reikwijdte van de AVG) en de bepalingen inzake internationale doorgifte als bedoeld in hoofdstuk V van de AVG gepubliceerd. De richtsnoeren staan nog open voor consultatie tot 31 januari 2022. Aangezien in hoofdstuk V het begrip "doorgifte" niet wordt gedefinieerd, is de vraag gerezen of organisaties in derde landen die rechtstreeks onder het bereik van de AVG vallen op grond van artikel 3, ook een beroep moeten doen op een van de in hoofdstuk V opgesomde doorgiftemechanismen en deze moeten toepassen wanneer zij persoonsgegevens vanuit de

EER ontvangen. Daar moeten deze richtsnoeren duidelijkheid over geven.

Overig

In het begin van 2021 publiceerde de EDPB concept richtsnoeren met voorbeelden van datalekken. De richtsnoeren zijn op 14 december 2021 definitief vastgesteld. Zij vormen een aanvulling op de eerdere richtsnoeren betreffende datalekken en zijn bedoeld om organisaties te helpen bij het nemen van beslissingen over datalekken en inzicht te geven in de factoren die in aanmerking moeten worden genomen bij verschillende risicobeoordelingen.

Op 2 februari 2021 publiceerde de EDPB een document naar aanleiding van het verzoek van de Europese Commissie om verduidelijking over de consequente toepassing van de AVG toegespitst op gezondheidsonderzoek. De EDPB kondigt daarin aan dat er richtsnoeren over de verwerking van persoonsgegevens voor wetenschappelijke onderzoeksdoeleinden in voorbereiding zijn. Deze richtsnoeren zijn nog niet verschenen.

Verder stelde de EDPB de eerdere gepubliceerde richtsnoeren inzake de verwerking van persoonsgegevens in het kader van verbonden voertuigen en mobiliteitsgerelateerde toepassingen, virtuele spraakassistenten, de beperkingen op grond van artikel 23 AVG en de richtsnoeren betreffende de targeting van gebruikers van sociale media het afgelopen jaar definitief vast. In deze laatste richtsnoeren wordt onder meer aandacht besteed aan de verantwoordelijkheden van *targeters* en aanbieders van sociale media. Het belangrijkste doel van de richtsnoeren is om de verdeling van de rollen en verantwoordelijkheden tussen de aanbieder van sociale media en de *targeter* te verduidelijken.

Ook de richtsnoeren over de begrippen verwerkingsverantwoordelijke en verwerker zijn in 2021 definitief vastgesteld. In de richtsnoeren wordt onder meer ingegaan op gezamenlijke verantwoordelijkheid en de verplichtingen die conform de AVG rechtstreeks op verwerkers rusten. De richtsnoeren bevatten een aantal handige flowcharts voor organisaties.

In oktober 2021 liet de EDPB weten dat zij een eerste gecoördineerde actie gaat lanceren gericht op cloud-gebaseerde diensten door de publieke sector. In zo een actie geeft de EDPB prioriteit aan een bepaald onderwerp waar toezichthoudende autoriteiten op nationaal niveau aan gaan werken. De nationale resultaten worden vervolgens gebundeld en geanalyseerd.

Op 18 november 2021 uitte de EDPB in een verklaring gericht aan de Europese Commissie enkele zorgen over de voorgestelde *Digital Services Act*, *Digital Markets Act*, *Data Governance Act* en de AI-verordening. In deze verklaring herhaalt de EDPB haar eerdere oproep tot een verbod op het gebruik van AI voor de automatische herkenning van menselijke kenmerken in voor het publiek toegankelijke ruimten. Ook dringt zij er bij de Europese Commissie op aan om een geleidelijke afschaffing te overwegen op de inzet van *tracking cookies* voor online reclame. Het opstellen van profielen van kinderen zou volgens de EDPB helemaal verboden moeten worden.

Autoriteit Persoonsgegevens

Budget en focus

De AP krijgt vanaf 2025 structureel 8 miljoen euro meer budget, zo volgt uit het regeerakkoord en de bijbehorende budgettaire bijlage. In de jaren daarvoor krijgt de toezichthouder geleidelijk ook al meer budget. Dit komt bovenop de 3,6 miljoen euro die wordt uitgetrokken voor een nieuwe algoritme-toezichthouder die blijkens het regeerakkoord bij de AP wordt ondergebracht. Het budget is een stuk lager dan de 100 miljoen euro waar de AP zelf om had gevraagd.

Het verhoogde budget lijkt hard nodig te zijn; zo blijkt uit het uiterst kritische rapport over de AP van de Nationale ombudsman dat nog op de valreep van 2021 verscheen. In dit rapport bespreekt de Nationale ombudsman de problemen bij de AP aan de hand van twee exemplarische klachten van burgers, waarvan er in 2020 klaarblijkelijk maar liefst 9800 op de plank lagen. Daarnaast doet de ombudsman een aantal algemene aanbevelingen aan de AP.

In het document AP Focus 2020-2023: 'Dataprotectie in een digitale samenleving' worden drie focusgebieden genoemd waaraan de AP de komende jaren extra aandacht gaat besteden. Dat zijn datahandel, digitale overheid en artificiële intelligentie & algoritmes. Die focus zal er het aankomende jaar dus ook nog zijn.

Handhaving

Het voorgaande jaar werden weer talloze boetebesluiten gepubliceerd. Niet al deze boetes zijn in 2021 opgelegd. Sommigen dateren al van eerdere jaren.

Zo werd er een boete van 440.000 euro aan het OLVG opgelegd, omdat het ziekenhuis te weinig maatregelen had genomen om toegang door onbevoegde medewerkers tot medische dossiers te voorkomen. Ook bij een orthodontiepraktijk waren de privacyrechten van patiënten in het geding. Omdat patiënten zich via een onbeveiligde website konden aanmelden, werd een boete van 12.000 euro opgelegd. De 25 GGD'en ontvingen weliswaar (nog) geen boete, maar de AP droeg hen wel op om op korte termijn meer maatregelen te nemen om persoonsgegevens beter te beschermen. Toen begin

2021 bleek dat er gegevens uit de systemen van de GGD werden verhandeld, intensiveerde de AP het toezicht en startte zij een onderzoek.
Het UWV ontving eveneens een boete vanwege een slechte beveiliging. Omdat het UWV het versturen van groepsberichten via de zogenoemde 'Mijn Werkmap'-omgeving niet goed had beveiligd, ontstonden er verschillende datalekken van persoonsgegevens van in totaal ruim 15.000 mensen. De boete bedroeg 450.000 euro.

Verder legde de AP onderhoudsbedrijf CP&A een boete van 15.000 euro op vanwege overtredingen bij het verwerken van gezondheidsgegevens van zieke werknemers. Het CP&A hield onterecht bij wat de oorzaak was van het ziekteverzuim en de verzuimregistratie was bovendien onvoldoende beveiligd.

Transavia ontving een boete van 400.000 euro in verband met een slechte beveiliging, waardoor een hacker toegang kreeg tot de systemen en persoonsgegevens van 25 miljoen personen kon inzien. Dit was niet het enige datalek dat tot een boete leidde binnen de reisbranche. Ook Booking.com werd beboet, omdat zij een datalek te laat bij de AP meldde. Bij dit datalek werden onder andere creditcardgegevens buitgemaakt. Dit resulteerde in een boete van 475.000 euro.

De PVV Overijssel ontving een boete van 7.500 euro wegens het uitblijven van een melding van een datalek bij de AP. Het datalek kwam in beeld omdat iemand een klacht bij de AP had ingediend naar aanleiding van een e-mail met een uitnodiging voor een achterbanbijeenkomst, waarin de e-mailadressen van alle 101 geadresseerden zichtbaar waren. Lees hier meer over de boetes opgelegd aan Booking.com en PVV Overijssel.

De eerste boete van de AP aan een overheidsinstantie, betrof de boete van 600.000 euro die aan de Gemeente Enschede werd opgelegd. De gemeente kon personen gedurende langere tijd via hun telefoon volgen vanwege *WiFi-tracking* in de binnenstad. Er is bezwaar aangetekend tegen de boete.

TikTok moet een boete van 750.000 euro betalen. Door de privacyverklaring niet in het Nederlands aan te bieden, legde TikTok volgens de AP onvoldoende uit hoe de app persoonsgegevens verzamelt, verwerkt en verder gebruikt. Dit levert een overtreding van de AVG op, mede omdat de doelgroep voornamelijk bestaat uit jonge kinderen die extra kwetsbaar zijn.

Verder werd aan Locatefamily.com een boete van 525.000 euro opgelegd, omdat zij geen vertegenwoordiger in de EU had aangesteld. Organisaties die onder de reikwijdte van de AVG vallen, zijn daar wel toe verplicht. Locatefamily.com is een platform waar mensen contactgegevens kunnen zoeken van familie die zij uit het oog zijn verloren of van mensen met wie zij graag in contact willen komen. Op het platform staan persoonsgegevens van mensen over de hele wereld, waaronder van 700.000 Nederlanders. Verschillende Europese toezichthouders ontvingen klachten over het bedrijf. Daarom werkte de AP in het onderzoek samen met de Canadese- en negen andere Europese privacytoezichthouders.

De boete van 2,75 miljoen euro die aan de Belastingdienst werd opgelegd is de hoogste boete in Nederland onder de AVG tot nu toe. Daarmee kreeg de kinderopvangtoeslagenaffaire ook een privacyrechtelijk staartje. De boete werd opgelegd omdat de dubbele nationaliteit van aanvragers van kinderopvangtoeslag zonder rechtsgeldige grondslag werd verwerkt. Door gegevens over nationaliteit onnodig op te nemen, handelde de Belastingdienst bovendien discriminerend.

Overig

Naast handhaving heeft de AP ook nog andere taken, zoals voorlichting en advisering. In het kader van dat takenpakket luidde de AP het afgelopen jaar de noodklok over de explosieve toename van het aantal *hacks* en datadiefstal. Het aantal datalekmeldingen steeg in 2020 met maar liefst 30% ten opzichte van 2019. Ook lanceerde de AP het afgelopen jaar een nieuw meldformulier voor datalekken. Hier kunt u meer lezen over de wijzigingen in het formulier.

De AP liet zich het voorgaande jaar kritisch uit over een aantal wetsvoorstellen, waaronder het Wetsvoorstel transparantieregister zorg en het Wetsvoorstel elektronische gegevensuitwisseling in de zorg. Op grond van laatstgenoemd wetsvoorstel zouden zorgaanbieders gedwongen worden om hun medisch beroepsgeheim te doorbreken, omdat zij verplicht worden om de gegevens van patiënten in bepaalde situaties elektronisch uit te wisselen, aldus de AP. Ook over de voorgestelde wijziging van de Wet register onderwijsdeelnemers was de AP niet te spreken. Daarnaast pleitte de AP voor de afscherming van woonadressen van ZZP'ers in het handelsregister.

Verder adviseerde de AP de Eerste Kamer om het Wetsvoorstel gegevensverwerking door samenwerkingsverbanden niet in zijn huidige vorm aan te nemen. De wet geeft overheidsorganisaties en private partijen zeer ruime bevoegdheden om persoonsgegevens met elkaar te delen, zoals bij vermoedens van fraude of georganiseerde criminaliteit. Het doel van de samenwerkingsverbanden om persoonsgegevens op grote schaal te delen, op te slaan en te analyseren is volgens de AP niet duidelijk genoeg omschreven in het wetsvoorstel. Hierdoor ligt het risico van massasurveillance op de loer. Eerder adviseerde de AP ook al om het wetsvoorstel waarmee de Nationaal

Coördinator Terrorismebestrijding en Veiligheid ('NCTV') ruimere bevoegdheden krijgt om informatie over burgers te verzamelen grondig aan te scherpen of anders helemaal niet in te dienen. In beide adviezen klinken de toeslagenaffaire en het nog lopende onderzoek door de AP naar de zwarte lijst Fraude Signalering Voorziening bij de Belastingdienst door.

Zwarte lijsten hebben in 2021 vaker de aandacht van de AP getrokken. Zo wees de AP een vergunningaanvraag van Vereniging VODIOM voor een zwarte lijst af. VODIOM wilde persoonsgegevens van vermoedelijke daders van fraude gaan uitwisselen met bedrijven in de betaalindustrie, *online retail* en telecommunicatie. Het delen van een zwarte lijst tussen bedrijven in verschillende sectoren mag echter alleen in zeer uitzonderlijke gevallen en onder strenge voorwaarden. Dit volgt ook uit de Handreiking cross-sectorale gegevensdeling tussen private partijen die de AP het afgelopen jaar publiceerde.

Naast private organisaties richtte de AP zich ook tot gemeenten. De Handreiking Wet gemeentelijke schuldhulpverlening werd gepubliceerd met daarin aandachtspunten voor gemeenten en professionals die betrokken zijn bij de uitvoering van deze wet. Ook met de aanbevelingen voor de ontwikkeling van zogenoemde smart city-toepassingen richtte de AP zich specifiek tot gemeenten.

Met de publicatie van het OR privacyboekje richtte de AP zich op een ruimer publiek, namelijk op werkgevers en werknemers die meer willen weten over de rol die de ondernemingsraad vervult bij privacy op de werkvloer.

Tot slot publiceerde de AP het voorgaande jaar uitgangspunten voor de positionering van de Functionaris Gegevensbescherming ('FG'). De uitgangspunten gaan onder meer over de informatiepositie van de FG, de middelen die de FG nodig heeft en de toegang van de FG tot het bestuur van de organisatie. Een en ander is volgens de AP niet altijd goed geregeld binnen organisaties.

Jurisprudentie

Europees niveau

Op 15 juni verduidelijkte het Hof van Justitie van de Europese Unie ('HvJEU') de voorwaarden waaronder nationale privacy toezichthouders hun bevoegdheden bij grensoverschrijdende gegevensverwerking kunnen uitoefenen. Gelet op het '*One-Stop-Shop*'-principe ligt de bevoegdheid tot optreden in principe bij de leidende toezichthouder, al zijn er in de AVG uitzonderingssituaties opgenomen waarin de niet-leidende toezichthouder toch bevoegd is handhavend op te treden. Er moet dan wel worden samengewerkt met de leidende toezichthouder volgens de vastgestelde samenwerkingsprocedure en het coherentie-mechanisme. Stelt de niet-leidende toezichthouder een rechtsvordering in voor een nationale gerechtelijke instantie, dan maakt het niet uit of de verwerkingsverantwoordelijke in een ander land is gevestigd.

Het HvJEU oordeelde op 22 juni 2021 dat het Letse registratiesysteem waarin strafpunten worden aangetekend die aan bestuurders van voertuigen zijn toegekend vanwege verkeersovertredingen in strijd is met de AVG. De strafpunten kwalificeren als strafrechtelijke persoonsgegevens en vallen daarom onder de werking van de AVG. Aangezien er minder ingrijpende mogelijkheden bestaan om het doel – het verhogen van de verkeersveiligheid – te bereiken, wordt niet voldaan aan het vereiste van subsidiariteit en noodzakelijkheid. Bovendien leidt het feit dat het om een min of meer openbaar register gaat, doordat iedereen zonder direct belang persoonsgegevens van anderen kan inzien, tot het oordeel dat het registratiesysteem niet voldoet aan de eisen uit de AVG.

Nationaal niveau

In 2021 werden op rechtspraak.nl. 324 uitspraken gepubliceerd waarin de term AVG voorkomt. Wij hierna een selectie.

Op 2 februari 2021 oordeelde het Gerechtshof Amsterdam dat niet de kortgedingprocedure maar de verzoekschrift-procedure uit artikel 35 UAVG de geëigende weg is om verwijdering van persoonsgegevens op grond van artikel 21 AVG te bewerkstelligen. In gevallen waarin de zes weken-termijn uit artikel 35 UAVG is verstreken, moet worden bedacht dat de betrokkene een nieuw AVG-verzoek kan indienen, tenzij er sprake is van misbruik van (proces)recht. Bovendien kan, als de situatie daar om vraagt, in een verzoekschriftprocedure een voorlopige voorziening worden gevraagd. In dit artikel kunt u meer lezen over deze verzoekschriftprocedure.

Op 18 maart 2021 oordeelde de voorzieningenrechter in de Rechtbank Den Haag dat de Nederlandse wetgeving die ten grondslag ligt aan het registreren van persoonsgegevens van *Ultimate Beneficial Owners* ('UBO's') in het UBO-register niet buiten werking gesteld hoeft te worden. Hoewel op voorhand niet valt uit te sluiten dat het openbare karakter van het UBO-register zich in het licht van de doelstelling ervan niet verhoudt met het door de Europese wetgever te respecteren evenredigheidsbeginsel, wordt niet tegemoet

gekomen aan het verzoek prejudiciële vragen te stellen aan het HvJEU. Redengevend daartoe is dat het *Tribunal d'arrondissement* te Luxemburg reeds op 13 november 2020 vragen aan het HvJEU heeft gesteld. Op 16 november 2021 werd de uitspraak van de voorzieningenrechter door het Gerechtshof Den Haag bekrachtigd.

Het Gerechtshof Amsterdam bekrachtigde op 1 juni 2021 de uitspraak van de Rechtbank Amsterdam waarin werd bepaald dat de UvA gebruik mag maken van online surveillancesoftware (*proctoring*) bij het afnemen van tentamens. Het gebruik van de *proctoring* software is in verband met de Covid-maatregelen noodzakelijk voor de vervulling van de taak van de UvA, er worden niet meer gegevens verwerkt dan noodzakelijk en ook aan de overige vereisten uit de AVG wordt voldaan. Bovendien had de Studentenraad geen instemmingsrecht over de inzet van de software.

In een zaak over het vernietigen van bepaalde onderdelen van een hulpverleningsplan en aanvullingen op een eindverslag in een dossier dat werd bijgehouden op grond van de Jeugdwet oordeelde de Hoge Raad op 16 juli 2021 dat vader geen beroep kon doen op de vernietigingsregeling uit de Jeugdwet maar wel aanvullende bescherming genoot op grond van de Wbp (oud). De Hoge Raad oordeelt dat het oordeel van het hof, dat artikel 11 Wbp uitgaat van een objectieve basis voor de verwerking van persoonsgegevens en dat constateringen en observaties van een jeugdhulpverlener, die naar hun aard subjectief zijn, in beginsel buiten het bereik van de vernietiging vallen, tenzij is vast te stellen dat deze constateringen en observaties iedere objectieve grondslag ontberen, stand kan houden omdat het niet onbegrijpelijk of onvoldoende gemotiveerd is.

Op 10 december 2021 heeft de Hoge Raad in een belastingzaak over de Fraude Signalering Voorziening van de Belastingdienst 'ten overvloede' geoordeeld dat in uitzonderlijke situaties waarin een belastingcontrole voortvloeit uit risicoselectie of op basis van een criterium dat jegens de belastingplichtige leidt tot een schending van een grondrecht zoals een schending van het verbod op discriminatie naar afkomst, geaardheid of geloofsovertuiging, de rechter kan oordelen dat het toepassen van de risicoselectie zozeer indruist tegen dat wat van een behoorlijk handelende overheid mag worden verwacht dat het gebruik van de resultaten van die controle onder alle omstandigheden ontoelaatbaar moet worden geacht. In dergelijke uitzonderlijke gevallen komt aan de belastinginspecteur niet de bevoegdheid toe om de aangifte van de belastingplichtige te corrigeren naar aanleiding van die bij de controle aan het licht gekomen punten. De enkele schending van de AVG is volgens de Hoge Raad overigens niet zo een uitzonderlijke situatie en kan niet leiden tot de verlaging van een – op zich juist berekende – aanslag. Eventueel kan ter compensatie van de schending in een afzonderlijke procedure schadevergoeding bij de algemene bestuursrechter (en niet bij de belastingrechter) of de civiele rechter worden gevorderd.

BKR

Over de verwerkingsgrondslag van een kredietaanbieder voor het opnemen van persoonsgegevens in het Centraal Krediet Informatie Systeem ('CKI') van BKR bestond onduidelijkheid na de uitspraken in 2020 van Gerechtshof Den Bosch en Gerechtshof Arnhem-Leeuwarden enerzijds en Gerechtshof Den Haag anderzijds. Heeft de kredietaanbieder een wettelijke verplichting of een gerechtvaardigd belang? Het antwoord op de vraag is relevant, aangezien een betrokkene in het geval er sprake is van een wettelijke verplichting geen recht op gegevenswissing en bezwaar toekomt. Reden genoeg voor de voorzieningenrechter in de Rechtbank Amsterdam om prejudiciële vragen te stellen aan de Hoge Raad, die op 3 december 2021 een zeer lezenswaardige uitspraak deed.

De Hoge Raad oordeelt dat er geen sprake is van een wettelijke verplichting tot het doen van een kredietregistratie, aangezien de wettelijke bepalingen waarop de kredietaanbieder zich beroept onvoldoende duidelijk en nauwkeurig zijn en de toepassing ervan niet voldoende voorspelbaar is voor degenen op wie de kredietregistratie betrekking heeft. Wel heeft de kredietaanbieder een gerechtvaardigd belang om de kredietregistratie te doen. De persoon op wie de kredietregistratie betrekking heeft, kan dus verzoeken om gegevenswissing en bezwaar maken tegen de kredietregistratie. Maar ook als die rechten niet kunnen worden ingeroepen omdat er een wettelijke verwerkingsplicht rust op de verwerkings-verantwoordelijke, is de betrokkene niet verstoken van rechtsbescherming: via de civiele rechter kan met een beroep op artikel 6:162 BW, al dan niet in samenhang met 8 EVRM, opgekomen worden tegen de verwerking van persoonsgegevens.

Noemenswaardig is verder de passage waarin de Hoge Raad opmerkt dat de grondslagen voor gegevenswerking uit de AVG kunnen cumuleren. Dat volgt uit de woorden 'ten minste' in artikel 6 lid 1 AVG. De passage vormt een mooie aanvulling op de uitspraak van de ABRvS van 22 september 2021, waarin is geoordeeld dat de veronderstelling dat persoonsgegevens nooit verwerkt kunnen worden als daar geen toestemming voor is verleend, niet in overeenstemming met de AVG is.

Schadevergoeding

In 2021 is net als in 2020 weer heel wat schadevergoeding gevorderd vanwege schending van de AVG. Om immateriële schadevergoeding toegewezen te krijgen, geldt als uitgangspunt dat met concrete gegevens moet worden aangetoond dat er schade is geleden als gevolg van de schending van de AVG. Ondanks dat dit vaak lastig is, bevestigde de Rechtbank Midden-Nederland dat uitgangspunt op 4 mei 2021 in een zaak tegen de Sociale Verzekeringsbank en op 31 mei 2021 kwam de Rechtbank Overijssel in een zaak tegen de gemeente Almelo tot eenzelfde oordeel.

Dit uitgangspunt - dat schade moet worden onderbouwd met concrete gegevens - geldt niet als de schade zo voor de hand ligt, dat een 'aantasting in de persoon' kan worden aangenomen. Op 12 januari 2021 oordeelde de Rechtbank Noord-Nederland dat daarvan sprake was omdat door herhaaldelijke publicatie van onder andere het BSN van de betrokkene op een gemeentelijke website, identiteitsfraude voor de hand lag.

Wat betreft de hoogte van toegekende schadevergoeding waren er in 2021 twee uitschieters. Allereerst het Gerechtshof Arnhem-Leeuwarden dat op 6 april 2021 een immateriële schadevergoeding van € 5000.- (minus € 1000.- immateriële schadevergoeding die in de strafzaak al was toegewezen) toekende omdat appellant jarenlang op een zwarte lijst van Stichting SIN stond. En ten tweede Rechtbank Rotterdam die op 12 juli 2021 vanwege de aard, duur en ernst van de overtreding een schadevergoeding van € 2.500.- toekende. De gemeente Rotterdam had in die zaak meermaals ten onrechte geweigerd medische gegevens uit een dossier te verwijderen, deze medische gegevens te lang (tien jaar) bewaard en toegankelijk gemaakt voor meerdere personen en instanties.

Collectieve acties

In 2021 werden diverse collectieve vorderingen op grond van de Wet afwikkeling massaschade in collectieve acties ('WAMCA') ingesteld. Tegen TikTok werden op 3 juni 2021, 31 augustus 2021 en 3 september 2021 collectieve acties gestart. In de rolbeslissing van 13 oktober 2021 heeft de Rechtbank Amsterdam de drie zaken tegen TikTok voor beraad voortgang procedure verwezen naar de rol van 2 februari 2022.

Ook waren er in 2021 de eerste uitspraken in collectieve acties die in 2019 en 2020 werden gestart. In de zaak van Data Privacy Stichting ('DPS') tegen Facebook – nog gestart voor inwerkingtreding van de WAMCA – oordeelde de Rechtbank Amsterdam op 30 juni 2021 in een tussenvonnis dat zij bevoegd is kennis te nemen van de zaak, dat de DPS ontvankelijk is omdat zij voldoet aan de vereisten van collectieve actie-organisatie en dat het stellen van prejudiciële vragen, zoals Facebook verzocht, niet nodig is. De inhoudelijke behandeling van de zaak vindt vermoedelijk dit jaar plaats.

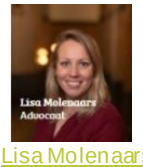
Op 22 september 2021 bepaalde de Rechtbank Den Haag dat etnisch profileren in het kader van Mobiel Toezicht Veiligheid ('MTV') door de Koninklijke Marechaussee is toegestaan. MTV-controles zijn een vorm van vreemdelingentoezicht en gericht op bestrijding van illegaal verblijf in Nederland. De Koninklijke Marechaussee gebruikt etniciteit als mogelijke indicator bij het nemen van concrete selectiebeslissingen. Bij het vaststellen van de verblijfsstatus kan nationaliteit een belangrijke rol spelen en kan etniciteit een objectieve aanwijzing zijn voor iemands vermeende nationaliteit. Aangezien etniciteit nooit de enige indicator is bij selectiebeslissingen en deze beslissingen uitlegbaar moeten zijn, wordt een algemeen verbod op het gebruik van etniciteit bij MTV-controles afgewezen. Op 22 december 2021 is hoger beroep ingesteld tegen de uitspraak.

In de zaak van The Privacy Collective ('TPC') tegen Oracle en SalesForce oordeelde de Rechtbank Amsterdam op 29 december 2021 dat TPC niet-ontvankelijk is omdat zij niet had kunnen aantonen voldoende representatief te zijn, een vereiste dat de WAMCA stelt. Volgens de rechtbank kan op basis van 75.000 *Facebook-likes* niet worden vastgesteld of TPC opkomt voor een voldoende groot deel van de groep getroffen benadeelden en of de mensen die de *like*-knop gebruikten überhaupt tot de groep getroffen benadeelden behoorden. Bovendien voldeed TPC niet aan het vereiste contact met haar achterban te kunnen onderhouden, aangezien TPC geen contactgegevens registreerde. De rechtbank komt door de niet-ontvankelijkheid niet toe aan een inhoudelijke behandeling van de zaak en merkt op dat in toekomstige zaken daarom nog moet worden geoordeeld over de vraag hoe de AVG en de WAMCA zich tot elkaar verhouden.

Meer weten?

Neem dan contact op met een van onze privacy specialisten:

Huub de Jong



Lisa Molenaars

Marijn Rooke

Esmee Fonville

Evelyn Peerboom

Tom de Wit