CONSIDERATI

PRIVACY & GEGEVENSBESCHERMING KENNISDELING

Overzicht recente privacyontwikkelingen

Januari 2023

INHOUDSOPGAVE

VOORWOORD

Beste lezer,

Het nieuwe jaar begint goed met weer veel interessante ontwikkelingen op het gebied van privacy en gegevensbescherming. In het kennisdocument dat voor u ligt, zullen we de meest relevante ontwikkelingen bespreken.

Allereerst wijzen wij u op het feit dat, met de inwerkingtreding van de Digital Services Act (DSA) op 16 november, de deadline van 17 februari nadert voor alle online platforms om het aantal actieve afnemers van hun diensten te publiceren. Voorts is de Verklaring over digitale rechten en beginselen voor het digitale decennium ondertekend. De Verklaring heeft als doel de kwaliteit van ons leven in het digitale tijdperk te verhogen. Vervolgens geven wij u ook een laatste status update over de AI Act, de Data Act en de Europese Chip Act. Ook de European Data Protection Board (EDPB) heeft niet stilgezeten. Zij publiceerde onlangs bindende besluiten over Facebook, Instagram en WhatsApp, namelijk een lijst met aanbevelingen voor overheidsinstellingen in het kader van het gebruik van clouddiensten. Verder heeft de cookiebanner taskforce van de EDPB een conceptrapport gepubliceerd dat ingaat op het gebruik van cookiebanners door bedrijven. Het Europees Hof van Justitie heeft deze maand uitleg gegeven over de betekenis van het recht op inzage. Een uitspraak die impact heeft op alle verwerkingsverantwoordelijken in de EU die persoonsgegevens delen met derde partijen.

Naast Europese onderwerpen, behandelen we ook interessante ontwikkelingen binnen Nederland. Zo is de Tweede Kamer nader geïnformeerd over de wijze waarop het algoritmetoezicht, waarvoor de Autoriteit Persoonsgegevens (AP) vanaf heden verantwoordelijk is, zal worden ingericht. Verder stelt de AP deze maand beperkingen aan het gebruik van GGZ-gegevens en legt zij een boete op aan de politie wegens de inzet van mobiele camera-auto’s tijdens de pandemie.

Het kennisdocument wordt afgesloten met de aankondiging van een nieuwe ISO-norm voor privacy by design, die volgende maand zal worden aangenomen en de boete die de Franse autoriteit voor gegevensbescherming oplegt aan Apple.

Veel leesplezier!

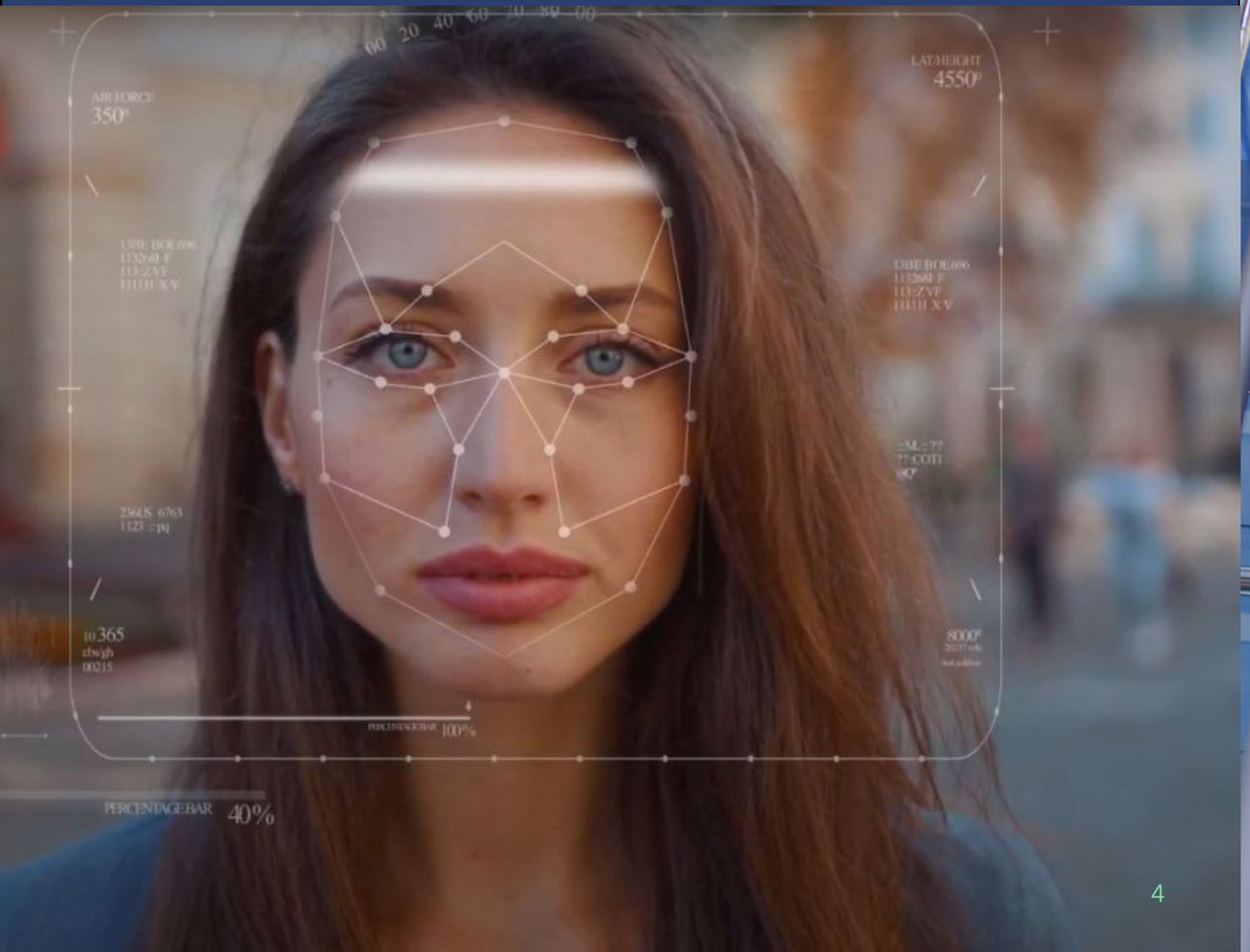
Bart Schermer
Partner Considerati

TOELICHTING

In dit overzicht nemen we met u de laatste ontwikkelingen in de wereld van privacy en gegevensbescherming door. Deze ontwikkelingen en updates verzamelen we op basis van, onder meer, richtsnoeren van nationale en internationale toezichthouders en instellingen, Nederlandse en internationale rechtspraak, uitspraken en nieuwsartikelen.

De informatie in dit overzicht vormt een selectie die op basis van relevante ontwikkelingen van de afgelopen maand, door Considerati is samengesteld. De opgenomen informatie biedt als zodanig geen uitputtend overzicht van alle relevante ontwikkelingen met betrekking tot privacy en gegevensbescherming, noch bevat dit document (juridisch) advies.

Aarzel niet om **contact** op te nemen met Considerati bij vragen en opmerkingen of indien u suggesties heeft over hoe wij onze kennisdeling kunnen verbeteren.



1. EUROPEAN DATA PROTECTION BOARD EN EUROPESE INSTELLINGEN

Hoogtepunten:

- De DSA-deadline van 17 februari voor online platforms nadert
- Europese Commissie, Parlement en Raad ondertekenen de Europese verklaring over digitale rechten en beginselen voor het digitale decennium
- Europees Parlement staat op het punt om standpunten betreffende de AI Act, Data Act en Chip Act af te ronden
- EDPB's bindende besluiten over Facebook, Instagram en WhatsApp zijn gepubliceerd
- De EDPB publiceert lijst met aanbevelingen voor overheidsinstellingen die persoonsgegevens opslaan in de cloud
- Taskforce EDPB publiceert conceptrapport cookiebanners
- Het Hof van Justitie: personen hebben het recht om te weten met wie hun persoonsgegevens worden gedeeld
- Het Hof van Justitie gaat fictieve namen gebruiken in prejudiciële zaken

1.1 De DSA-deadline van 17 februari voor online platforms nadert

De deadline van 17 februari voor online platforms om het aantal actieve gebruikers in de zin van de Digital Services Act ("DSA") te publiceren, komt dichtbij. De deadline geldt voor alle online platforms, ongeacht hun omvang, die gebruikersmateriaal hosten en verspreiden. De verplichting is dus niet beperkt tot "zeer grote onlineplatforms": platforms die in de EU maandelijks gemiddeld 45 miljoen of meer actieve gebruikers hebben. Op grond van artikel 23, lid 2, DSA moeten onlineplatforms ten minste elke zes maanden informatie over de gemiddelde maandelijkse actieve afnemers van de dienst in elke lidstaat bekendmaken. De gebruikersaantallen zullen worden gepubliceerd op de publiek toegankelijke online-interfaces of websites van de platforms. Hiertoe moeten zowel geregistreerde als niet-geregistreerde gebruikers toegang kunnen hebben.

Na de deadline van 17 februari zal de Europese Commissie de als "zeer grote onlineplatforms" benoemde platforms en zoekmachines bekendmaken. De deadline om de platforms aan te wijzen, is 28 april 2023. Daarna hebben de als "zeer grote onlineplatforms" gekwalificeerde platforms tussen 18 juni en 1 september 2023 de tijd om te voldoen aan de vereisten neergelegd in de DSA.

1.2 Europese Commissie, Parlement en Raad ondertekenen de Europese verklaring over digitale rechten en beginselen voor het digitale decennium

Eind 2022 hebben de voorzitters van de Europese Commissie (de Commissie), het Europees Parlement en de Europese Raad de Europese verklaring over digitale rechten en beginselen voor het digitale decennium (de Verklaring) ondertekend. De Verklaring, die in januari 2022 voor het eerst werd geïntroduceerd, waarborgt de inzet van de EU voor een veilige, beveiligde en duurzame digitale transformatie waarbij de mens centraal staat. De verklaring biedt EU-burgers een referentiekader met betrekking tot hun digitale rechten. Daarnaast is de Verklaring bedoeld als leidraad voor beleidsmakers en bedrijven in de omgang met nieuwe technologieën.

De Verklaring is opgedeeld in zes hoofdstukken die de rechten en beginselen vertegenwoordigen die de digitale transformatie van de EU en de bijbehorende aanpak moeten sturen. Het gaat om de volgende zes rechten en beginselen: 1) het centraal stellen van de mens in de digitale transformatie, 2) het bevorderen van solidariteit en inclusie, 3) de waarborging van online keuzevrijheid, 4) het bevorderen van participatie in de digitale publieke ruimte, 5) het vergoten van veiligheid, beveiliging en zelfredzaamheid in de digitale omgeving, met name voor jongeren en 6) het bevorderen van een duurzame digitale toekomst. Concreet wordt aan deze rechten en beginselen invulling gegeven door middel van: betaalbare en snelle digitale verbindingen, een veilige digitale omgeving voor kinderen, digitaal geschoolde leraren en goed uitgeruste klaslokalen, de vergaring van informatie over de effecten van digitale producten op de EU en het milieu en controle op het gebruik van persoonsgegevens.

Voorts benadrukt de Verklaring het gedeeld belang van de EU en haar lidstaten om deze rechten en beginselen te bevorderen en toe te passen, allemaal om de digitale doelstellingen voor 2030 te bereiken. De Commissie wil ervoor zorgen dat de gemeenschappelijke doelen en streefcijfers behaald worden door middel van een samenwerkingsmechanisme waarbij de Commissie en de lidstaten zijn betrokken. Dit samenwerkingsmechanisme zal, onder andere, bestaan uit een monitoringsysteem en een jaarlijks rapport over de stand van het digitale decennium.

1.3 Europees Parlement staat op het punt om standpunten betreffende de AI Act, Data Act en Chip Act af te ronden

Nu de Europese Commissie (hierna: de Commissie) in april 2021 het voorstel voor de AI Act heeft gepubliceerd en de Europese Raad in december 2022 zijn gemeenschappelijk standpunt ("algemene oriëntatie") heeft vastgesteld, is het aan het Europees Parlement (hierna: het Parlement) om het standpunt over de AI Act af te ronden. Volgens het Parlement zal het standpunt, dat in januari van dit jaar moet worden gepubliceerd, gericht zijn op de specifieke toepassingen en mogelijke risico's van AI. De twee parlementsleden die werkzaam zijn als co-rapporteurs voor de AI Act, hebben in april 2022 al een ontwerpverslag gepubliceerd met meer dan 300 voorstellen tot wijzigingen die momenteel in behandeling zijn.

Wat betreft de Data Act, ziet het volgende agendapunt van het Parlement op de vaststelling van gemeenschappelijke regels voor het delen van gegevens bij het gebruik van gekoppelde producten of gerelateerde diensten. Het voorstel richt zich op het bieden van waarborgen tegen onrechtmatige internationale gegevensoverdracht door aanbieders van clouddiensten. Daarnaast moet het voor gebruikers van cloudopslag en andere gegevensverwerkingsdiensten gemakkelijker worden om over te stappen naar een andere aanbieder.

Het Parlement wil ook zijn standpunt innemen over het voorstel van de Chip Act, die in februari door de Commissie is gepubliceerd. Onder invloed van het door de COVID-19 pandemie veroorzaakte wereldwijde tekort aan halfgeleiders, moet de Chip Act ervoor zorgen dat de EU de nodige vaardigheden, instrumenten en technologieën ontwikkelt om leider op dit gebied te worden. Dit zou het doel van de EU van digitale en groene transitie bevorderen, de productie stimuleren en verstoring van de toeleveringsketen voorkomen. Tot slot wil het Parlement in het kader van de digitale transformatie onderzoek doen naar regels voor cryptocurrencies om consumenten te beschermen en waarborgen te bieden tegen marktmanipulatie en financiële criminaliteit.

1.4 EDPB's bindende besluiten over Facebook, Instagram en WhatsApp zijn gepubliceerd

Op 06 december 2022 publiceerde de European Data Protection Board (hierna: EDPB) een persbericht waarin zij aangaf bindende besluiten te hebben genomen in antwoord op de door de Ierse commissie voor gegevensbescherming (DPC) ingediende geschillen. De geschillen vloeien voort uit een door de DPC gedeeld ontwerpbesluit over Meta's aangeboden Facebook-, Instagram- en WhatsApp-diensten. Naar aanleiding van het genomen besluit, hebben zes nationale toezichthouders (de privacy autoriteiten uit Duitsland, Finland, Frankrijk, Italië, Nederland en Noorwegen) bezwaar tegen het besluit ingediend. Op grond van de in artikel 65 van de Algemene Verordening Gegevensbescherming (AVG) voorgeschreven procedure is de EDPB bevoegd een bindend besluit te nemen wanneer een betrokken toezichthoudende autoriteit een relevant en gemotiveerd bezwaar heeft ingediend tegen een ontwerpbesluit van de leidende toezichthoudende autoriteit (de toezichthouder van de EU-lidstaat waar de hoofdvestiging van een verwerkingsverantwoordelijke).

Zoals de EDPB zelf aangeeft, gaan deze besluiten, onder meer, over de volgende vraag:

"Is de verwerking van persoonsgegevens voor de uitvoering van een overeenkomst al dan niet een geschikte rechtsgrondslag voor behavioural advertising, in het geval van Facebook en Instagram, en voor verbetering van de dienstverlening, in het geval van WhatsApp?"

Bindend besluit 03/2022 en 04/2022 gaan over de rechtmatigheid van het beroep van Facebook en Instagram op artikel 6, lid 1, onder b AVG voor de verwerking van persoonsgegevens ten behoeve van behavioural advertising (reclame op basis van surfgedrag). Het bindend besluit 05/2022 gaat in op de rechtmatigheid van het beroep van WhatsApp op artikel 6, lid 1, onder b AVG ten behoeve van de "verbetering en beveiliging van de dienst".

In beide scenario's heeft de EDPB geoordeeld dat "noodzakelijk voor de uitvoering van een overeenkomst" niet de passende rechtsgrondslag is voor de desbetreffende verwerkingen van persoonsgegevens. Enkele belangrijke opmerkingen van de EDPB, in zijn bindende besluiten over het gebruik en de uitlegging van artikel 6, lid 1, onder b AVG en de grond "noodzakelijk voor de uitvoering van een overeenkomst" zijn:

- Zowel Facebook, Instagram, WhatsApp als de DPC betoogden dat de gebruiksvoorwaarden voor deze diensten het contract vormden waarmee gebruikers instemden alvorens van de diensten gebruik te maken. De EDPB verzet zich tegen dit standpunt. Allereerst meent de EDPB dat de voorwaarden vaag zijn geformuleerd en een gebruiker niet volledig geïnformeerd is over de omvang van de verwerking van zijn persoonsgegevens en op grond van welke rechtsgrond dit gebeurd. Ten tweede zijn gebruikers, wanneer zij met dergelijke voorwaarden instemmen, zich waarschijnlijk niet bewust van het feit dat zij een contract aangaan.
- Daarnaast hebben zij niet de mogelijkheid om de voorwaarden aan te vechten of erover te onderhandelen. Aangezien Facebook, Instagram en WhatsApp dominant zijn in hun sector, worden gebruikers in veel opzichten gedwongen om de gebruiksvoorwaarden te aanvaarden, wat in strijd is met de beginselen van vrije toestemming op grond van het toepasselijke verbintenissenrecht.
- Bovendien observeert de EDPB, wijzend op het noodzakelijkheidsvereiste bij een beroep op artikel 6, lid, onder b AVG dat Facebook, Instragram en WhatsApp's als doel hebben gebruikers met elkaar in contact te brengen. Volgens de EDPB is het aanbieden van gepersonaliseerde advertenties en de verbetering van de dienstverlening niet noodzakelijk voor het verlenen van hun primaire dienst aan gebruikers. Het feit dat deze activiteiten wel essentieel waren voor hun bedrijfsmodellen, doet hier niet aan af.
- De EDPB gaf ook aan dat het, in gevallen zoals behavioral advertising, of verbetering en beveiliging van diensten, beter zou zijn om toestemming of gerechtvaardigd belang als rechtsgrondslag te gebruiken. De EDPB geeft hiervoor als redenen dat toestemming de betrokkenen de mogelijkheid biedt de verwerking van hun persoonsgegevens voor dergelijke processen te weigeren, terwijl gerechtvaardigd belang voor de verwerkingsverantwoordelijke de mogelijkheid biedt om de belangen van de betrokkenen af te wegen tegen zijn eigen commerciële belang.
- De EDPB concludeerde ook dat Facebook, Instagram en WhatsApp, onder meer, hun transparantieverplichtingen hadden geschonden door zich niet op een correcte rechtsgrondslag te baseren en de gebruikers niet op een duidelijke en begrijpelijke manier te informeren over de manieren waarop hun gegevens worden verwerkt.

Deze maand heeft de DPC, gebaseerd op de bindende besluiten van de EDPB, zijn definitieve besluiten vastgesteld waarbij een boete van 210 miljoen euro wordt opgelegd aan Facebook, 180 miljoen euro aan Instagram en 5,5 miljoen euro aan WhatsApp. Waarschijnlijk zal Meta in beroep gaan tegen het besluit van de DPC.

1.5 De EDPB publiceert lijst met aanbevelingen voor overheidsinstellingen die persoonsgegevens opslaan in de cloud

Op 17 januari dit jaar heeft de European Data Protection Board (EDPB), het Europese samenwerkingsverband van privacy toezichthouders, in een rapport 13 aanbevelingen gepubliceerd voor overheidsinstellingen die persoonsgegevens van burgers opslaan in de cloud.

Aanleiding voor de aanbevelingen
De aanbevelingen komen voort uit een onderzoek dat in 2022 is uitgevoerd. Aan dit onderzoek hebben 22 nationale toezichthoudende autoriteiten deelgenomen, waaronder ook de Nederlandse Autoriteit Persoonsgegevens (AP). Aanleiding voor het onderzoek waren de moeilijkheden die overheidsinstanties kunnen ondervinden bij het verkrijgen van informatie- en communicatietechnologieproducten die voldoen aan de gegevensbeschermingsregels. Door middel van gecoördineerde richtsnoeren en activiteiten willen de autoriteiten best practises bevorderen en zo een passende bescherming van persoonsgegevens garanderen

13 aanbevelingen voor overheidsinstellingen
De lijst met aanbevelingen ziet er als volgt uit:

1. Voer een Data Protection Impact Assessment (DPIA) uit. De EDPB wijst op de mogelijkheid dat het gebruik van clouddiensten door overheidsinstanties in veel situaties een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt. In dergelijke gevallen zijn overheidsorganisaties op grond van de Algemene Verordening Gevensbescherming (AVG) verplicht een DPIA uit te voeren. De uitvoering van een DPIA dient voor de start van de verwerking afgerond te zijn. Wanneer een DPIA niet verplicht is, dient op z'n minst een risicobeoordeling te worden uitgevoerd om te voldoen aan artikel 24 en 32 van de AVG.
2. Zorg ervoor dat de rollen van alle betrokken partijen duidelijk en ondubbelzinnig zijn vastgesteld in een contract. Hiervoor moeten overheidsinstanties hun rol in relatie tot het gebruik van de clouddiensten duidelijk vaststellen, bijvoorbeeld door middel van een intern assessment of een DPIA.
3. Zorg ervoor dat de clouddienstverlener slechts handelt namens de verwerkingsverantwoordelijke en dit volgens gedocumenteerde instructies doet. Benoem daarbij elke mogelijke verwerking door de clouddienstverlener. Identificeer ook verwerkingen waarvoor de clouddienstverlener mogelijk verwerkingsverantwoordelijke is, om ervoor te zorgen dat elke verwerking een rechtsgrondslag heeft.
4. Zorg ervoor dat bezwaar gemaakt kan worden tegen de samenwerking met nieuwe sub-verwerkers. Bijvoorbeeld door het recht op te nemen om wijzigingen in de lijst van sub-verwerkers te mogen herzien en binnen een bepaalde termijn bezwaar te mogen maken.
5. Zorg ervoor dat de verwerking van persoonsgegevens in relatie staat tot het doel waarvoor zij worden verwerkt.
6. Bevorder de betrokkenheid van de Functionaris Gegevensbescherming (FG). De FG dient een actieve rol te spelen bij het analyseren van de clouddienst en eventuele onderhandelingen betreffende het contract met hen.
7. Werk samen met andere overheidsinstanties bij de onderhandelingen met cloudaanbieders. Dit versterkt de onderhandelingspositie van de overheid.
8. Voer een evaluatie uit om te beoordelen of de verwerking door de clouddienst wordt uitgevoerd in overeenstemming met de DPIA. Zorg er daarnaast voor dat de uitgevoerde DPIA regelmatig wordt herzien, aangezien clouddiensten voortdurend onderhevig zijn aan veranderingen.
9. Zorg ervoor dat de aanbestedingsprocedure voorziet in alle noodzakelijke vereisten om in overeenstemming met de AVG te zijn.
10. Ga na welke doorgiften kunnen plaatsvinden binnen de standaard dienstverlening van de clouddienstverlener en wanneer overheidsinstanties uit derde landen toegang eisen tot persoonsgegevens. Zorg dat deze doorgiften voldoen aan de bepalingen neergelegd in hoofdstuk V van de AVG (doorgiften van persoonsgegevens aan derde landen).
11. Ga na of wetgeving van een derde land van toepassing is op de clouddienstverlener en of dit kan leiden tot het verzoek om toegang tot in de EU opgeslagen persoonsgegevens.
12. Onderzoek het contract nauwkeurig en onderhandel het zo nodig opnieuw.
13. Ga na onder welke voorwaarden de overheidsinstantie audits mag uitvoeren en wanneer deze kan meewerken aan audits.

Samenvattend benadrukt de EDPB met deze lijst de verantwoordelijkheid van de overheid om te waarborgen dat de gegevens van burgers veilig zijn.

Bevindingen van de Autoriteit Persoonsgegevens
De Autoriteit Persoonsgegevens (hierna: AP) concludeert dat andere landen kunnen leren van de Nederlandse overheid. Zo voeren Nederlandse overheidsorganen steeds vaker gezamenlijk een DPIA uit. Omdat de overheid deze DPIA's vaak publiceert, kunnen andere organisaties leren hoe zij het beste de risico's van bepaalde clouddiensten moeten beoordelen. Daarnaast zorgt gezamenlijke analyse voor een betere onderhandelingspositie voor Nederlandse overheidsorganisaties.

Niettemin bestaat er ruimte voor verbetering wat betreft het cloudgebruik door de Nederlandse overheid. De AP heeft daarom een brief opgesteld, gericht aan alle Nederlandse ministeries. In deze brief deelt de AP observaties en aanbevelingen. Zo vindt de AP dat de minister zich moet realiseren zelf verantwoordelijk te zijn voor de inkoop van clouddiensten. Deze dient dus niet bij de gezamenlijke inkooporganisatie belegd te zijn. De ministeries dienen hierbij de wijze waarop privacy wordt meegenomen in het inkoopproces te uniformeren. Ten slotte dient de minister na te gaan op welke terreinen nog meer gezamenlijke inkoop kan plaatsvinden.

1.6 Taskforce EDPB publiceert conceptrapport cookiebanners

De cookie banner taskforce van de European Data Protection Board (EDPB) heeft op 17 januari een conceptrapport gepubliceerd dat ingaat op het gebruik van cookiebanners door bedrijven. Het conceptrapport is een reactie op de klachten van de privacy organisatie None Of Your Business (Noyb) over het gebruik van cookiebanners door bedrijven.

Noyb verstuurde eind mei 2021 aan 560 Europese bedrijven een informatieve AVG-klacht. In de klacht werd gesteld dat de bedrijven illegale cookiebanners gebruikten met het doel de bezoeker zoveel mogelijk te frustreren om op 'OK' te klikken. Hoewel een aantal bedrijven de overtreding verhielpen, stopte een grote meerderheid van de bedrijven niet met het gebruik van de illegale cookiebanners. Tegen deze 422 bedrijven diende Noyb bij de nationale toezichthouders klachten in.

Naar aanleiding van de indiening van deze klachten, werd in september 2021 de taskforce cookiebanners opgericht. Het conceptrapport stelt een minimumdrempel vast om cookiebanners te beoordelen en zo internetters te beschermen tegen misbruik door middel van cookiebanners.

In het rapport worden de volgende praktijken onwettig bevonden:
- Het ontbreken van een optie voor de afwijzing van cookies op de eerste laag van de cookiebanner (maar verbogen in een sub-laag);
- Vooraf aangevinkte vakjes, in plaats van het geven van toestemming door middel van een actieve actie;
- Het gebruik van links in klein en ander lettertype, die niet de aandacht van de internetgebruiker trekken, om toestemming te weigeren;
- Het plaatsen van links buiten te cookiebanner om toestemming te weigeren, met een gebrek aan voldoende visuele ondersteuning om het oog van de gebruiker naar deze link te leiden;
- Bij het aanbieden van andere opties anders dan het geven van toestemming (bijv. "afwijzen" of "alleen noodzakelijke cookies accepteren") een knop met tekst gebruiken die, door het ontbreken van contrast tussen de kleur van de tekst en de achtergrond van de knop, voor gebruikers lastig is te lezen;
- Het, onterecht, claimen van een gerechtvaardigd belang voor het installeren van niet-essentiële cookies (en niet om toestemming vragen);
- Geen permanente mogelijkheid op websites bieden om toestemming in te trekken.

Daarnaast benoemd de taskforce dat bepaalde praktijken, zoals het gebruik van misleidende kleuren voor de knoppen in de cookiebanner, als problematisch worden beschouwd. De beoordeling van cookiebanners moet volgens de taskforce echter per geval worden beoordeeld.

Ook kaart de taskforce aan dat sommige organisaties onterecht bepaalde cookies classificeren als 'essentieel' of 'strikt noodzakelijk'. Volgens de taskforce is het echter lastig om bijvoorbeeld een betrouwbare lijst van essentiële cookies op te stellen, omdat de eigenschappen en functies van cookies constant veranderen. Op dit punt onderzoekt de taskforce de mogelijkheden om de eigenaren van websites de verantwoordelijkheid te geven om een dergelijke lijst bij te houden. Daarnaast bekijkt de taskforce of bepaalde tools ingezet kunnen worden die het gebruik van cookies door bepaalde websites kunnen analyseren.

1.7 Het Hof van Justitie: personen hebben het recht om te weten met wie hun persoonsgegevens worden gedeeld

Het Hof van Justitie van de Europese Unie (het Hof) heeft onlangs uitspraak gedaan in een zaak tussen een natuurlijk persoon (de betrokkene) en de Osterreichische Post, de nationale postdienstverlener van Oostenrijk. De persoon in kwestie had aan de Österreichische Post om inzage gevraagd in de persoonsgegevens die de Österreichische Post van hem verwerkte en om informatie gevraagd over de derde partijen met wie zijn persoonsgegevens werden gedeeld.

Artikel 15, lid 1, sub, c AVG: recht van inzage van de betrokkene
Hij baseerde zijn verzoek op artikel 15, eerste lid, sub c, van de Algemene Verordening Gegevensbescherming (AVG). Op grond van dit artikel heeft de betrokkene het recht om van de verwerkingsverantwoordelijke uitsluitsel te krijgen over het al dan niet verwerken van persoonsgegevens van hem en, wanneer dit het geval is, inzage te krijgen in de persoonsgegevens die worden verwerkt. Daarbovenop heeft de betrokkene het recht op informatie over de ontvangers of categorieën van ontvangers aan wie persoonsgegevens zijn of zullen worden verstrekt.

Verloop van het geschil
De Österreichische Post beperkte de informatie in zijn reactie tot het feit dat hij als uitgever van telefoongidsen gebruik maakt van persoonsgegevens en dat hij die persoonsgegevens voor marketingdoeleinden aanbiedt aan zakelijke klanten. Het postbedrijf heeft aan de betrokkene niet meegedeeld wie de concrete ontvangers van de gegevens waren. De betrokkene besloot daarop een juridische procedure aanhangig te maken bij de nationale rechtbank. Het geschil is uiteindelijk beland bij het Oberste Gerichtshof, de hoogste federale rechter in civiele en strafzaken, in Oostenrijk.

Het Oberste Gerichtshof vroeg zich af hoe artikel 15, eerste lid, sub c AVG moet worden uitgelegd en besloot daartoe de volgende prejudiciële vraag te stellen aan het Hof: Moet artikel 15, lid 1, onder c, AVG zo worden uitgelegd dat het recht van inzage beperkt is tot categorieën van ontvangers als de specifieke ontvangers nog niet bekend zijn, maar dit recht ook moet uitstrekken tot de identiteit van ontvangers van informatie wanneer de persoonsgegevens al met hen zijn gedeeld?

Behandeling door het Hof van Justitie
Het Hof overweegt, onder andere, dat artikel 15, eerste lid, sub c AVG moet wordt gelezen in het licht van de context en het doel van de bepaling en de AVG. Hieruit volgt dat de betrokkene moet kunnen controleren of zijn persoonsgegevens rechtmatig worden verwerkt, of de gegevens juist zijn en of zij zijn meegedeeld aan bevoegde ontvangers. Ook overweegt het Hof dat het recht van inzage voor betrokkenen noodzakelijk is om andere rechten van betrokkenen, zoals het recht op vergetelheid, het recht op rectificatie en het recht om bezwaar te maken, uit te voeren. Dit is slechts mogelijk wanneer de identiteit van de ontvanger bekend is. Als gevolg daarvan oordeelt het Hof dat de betrokkene het recht heeft om de identiteit van de ontvangers van zijn persoonsgegevens te weten.

Desondanks bestaat er uitzondering op deze regel. Zo wijst het Hof op het feit dat het recht op de bescherming van persoonsgegevens niet absoluut is en altijd afgewogen dient te worden tegen andere grondrechten. Om deze reden neemt het Hof aan dat het in sommige omstandigheden niet mogelijk is om informatie te verstrekken over concrete ontvangers. In deze gevallen kan een verwerkingsverantwoordelijke zich beperken tot het delen van de categorieën van ontvangers. Voorts kan de verwerkingsverantwoordelijke, op grond van artikel 12, lid 5, onder b, AVG weigeren gevolg te geven aan een inzageverzoek wanneer deze kennelijk ongegrond of buitensporig van aard is. Het is dan wel aan de verwerkingsverantwoordelijke om dit aan te tonen.

Alle organisaties die persoonsgegevens verwerken en deze delen met derde partijen doen er, op grond van deze uitspraak, goed aan om te bekijken wat deze uitspraak betekent voor de processen die zijn geïmplementeerd en de documentatie die bestaat rondom het faciliteren van inzageverzoeken van betrokkenen.

1.8 Het Hof van Justitie gaat fictieve namen gebruiken in prejudiciële zaken

Begin deze maand kondigde het Hof van Justitie van de Europese Unie (hierna: HvJEU) aan dat het fictieve namen zal gebruiken voor alle nieuwe geanonimiseerde zaken die vanaf 1 januari 2023 worden ingediend. De fictieve namen worden toegekend door een geautomatiseerde naamgenerator. De fictieve namen zullen worden gebruikt voor alle procedures tussen natuurlijke personen (waarvan de namen sinds 1 juli 2018 zijn vervangen door initialen met het oog op de bescherming van persoonsgegevens) of procedures tussen natuurlijke personen en rechtspersonen die geen onderscheidende naam hebben. Het doel van dit initiatief is om de aanduiding en identificatie van geanonimiseerde zaken te vergemakkelijken en het makkelijker te maken de namen en citaten te onthouden.

Belangrijk om te benadrukken, is dat de fictieve namen op geen enkele wijze verband houden of overeenkomen met een partij. Ook vertegenwoordigt de fictieve naam geen bestaande naam.

Verder heeft het HvJ-EU aangegeven dat de fictieve namen niet toegekend worden aan:
- Verwijzingen naar prejudiciële vragen waarin de naam van de rechtspersoon voldoende onderscheidend is. In die gevallen zal de naam van die rechtspersoon worden gebruikt als naam van de zaak;
- Rechtstreekse beroepen, waarvoor het HvJEU een conventionele naam zal blijven toekennen;
- Verzoeken om advies;
- Hogere voorzieningen en aan zaken voor het Gerecht.

De namengenerator zal namen in elk van de officiële talen van de EU kunnen genereren. Daarbovenop zullen er extra generatoren worden ontwikkeld die zo nodig fictieve namen leveren in de talen van landen buiten de EU.

2. NATIONAAL NIEUWS

Hoogtepunten:

- De AP stelt beperkingen aan het gebruik van GGZ-gegevens
- Van Huffelen verheldert contouren rondom de inrichting van het algoritmetoezicht door de AP
- De AP oordeelt dat het wetsvoorstel over uitlenen tijdelijk personeel tekortschiet
- Boete voor het ontbreken DPIA voor de inzet van camera-auto's in Rotterdam
- Landmacht verzamelt informatie tijdens de pandemie zonder juridische grondslag

2.1 De AP stelt beperkingen aan het gebruik van GGZ-gegevens

De Autoriteit Persoonsgegevens (AP) heeft grenzen gesteld aan het gebruik van ggz-gegevens door de Nederlandse Zorgautoriteit (NZa). In het kader van het zogeheten zorgprestatiemodel wil de NZa zorgverleners in de ggz verplichten om informatie over hun patiënten te verstrekken om zo meer zicht te krijgen op de toekomstige zorgvraag en om zorgkosten nauwkeuriger te kunnen berekenen. Het doel van dit alles is, met name, om complexe zorg nauwkeuriger te bekostigen. Hoewel de NZa expliciet heeft verklaard dat ggz-gegevens zijn versleuteld, dat de herleidbaarheid tot personen tot een minimum is beperkt en dat patiënten via een opt-out constructie de gegevensuitwisseling kunnen tegenhouden, stelt de AP strikte voorwaarden aan de invulling van dit plan.

De Tweede Kamer was al van mening dat deze verwerkingsactiviteiten door de NZa te ver gaan, onder meer omdat er te veel bekend zou worden over de psychische aandoening van een cliënt. Dit wordt, met name met het oog op de bescherming van de privacy van patiënten, als zorgelijk beschouwd. De AP heeft, aan de hand van door de NZa verstrekte aanvullende informatie, beoordeeld of voldoende aannemelijk is gemaakt dat de verplichte aanlevering aan de NZa van ggz-gegevens van alle ggz-patiënten geschikt is de nagestreefde doelstelling van algemeen belang te (kunnen) verwezenlijken (geschiktheid). Ook heeft zij bekeken of inmenging in het recht op bescherming van persoonsgegevens daarbij beperkt blijft tot het strikt noodzakelijke (subsidiariteit en proportionaliteit). Daarnaast is zij nagegaan of de Regeling ggz en forensische zorg duidelijke en nauwkeurige regels over de reikwijdte en of deze een toepassing bevat die waarborgen dat de verwerking tot het noodzakelijke beperkt blijft en dat betrokkenen over voldoende garanties beschikken zodat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik en in overeenstemming met het recht (duidelijkheid en waarborgen).

Op basis van deze toetsing is de AP tot de conclusie gekomen dat de Regeling ggz en forensische zorg in beginsel een grondslag biedt voor de rechtmatige verwerking van ggz-gegevens van alle ggz-patiënten door de NZa. Als de NZa deze gegevens op een later moment opnieuw wil gebruiken, zal daarvoor echter eerst een nieuwe wettelijke regeling moeten komen met een onderbouwing van de noodzaak daarvan en zal deze ook voor advies aan de AP moeten worden voorgelegd.

2.2 Van Huffelen verheldert contouren rondom de inrichting van het algoritmetoezicht door de AP

In december 2022 heeft Staatssecretaris Alexandra van Huffelen (Digitalisering) de Tweede Kamer nader geïnformeerd over de wijze waarop het algoritmetoezicht bij de AP zal worden ingericht. De introductie van het algoritmetoezicht is een direct resultaat van de ambitie van de Tweede Kamer en het kabinet om via de AP te regelen dat algoritmes worden gecontroleerd op transparantie, discriminatie en willekeur. Middels de door Van Huffelen geïntroduceerde contouren wordt hier nader invulling aan gegeven.

De Autoriteit Persoonsgegevens (hierna: AP) heeft via het regeerakkoord 2022 extra budget gekregen voor de inrichting van de Nederlandse algoritmetoezichthouder. In de Kamerbrief wordt beschreven welke nieuwe activiteiten de AP – al dan niet in samenwerking met andere spelers – in 2023 onder haar hoede zal nemen en wordt aangekondigd dat het al bestaande toezicht op algoritmes in 2023 wordt versterkt. Meer in het bijzonder zal de AP zich vanaf januari 2023 gaan richten op het signaleren en analyseren van sector- en domeinoverstijgende risico's van algoritmes, op het faciliteren en intensiveren van de samenwerking met andere organisaties en op het komen tot gezamenlijke normuitleg en het scheppen van overzicht in wettelijke en andere kaders. Voor de verdere opschaling van het algoritmetoezicht, zal verder duidelijkheid geschept moeten worden over de doelen en activiteiten van de toezichthouder vanaf 2024, zal dialoog gevoerd moeten worden over de mogelijke (nieuwe) toezichtstaken op het gebied van algoritmen en zal de (potentiële) rol van de algoritmetoezichthouder in relevante (BZK-) beleidstrajecten en opkomende wet- en regelgeving verkend moeten worden.

Met deze nieuwe taak kijkt de AP naar risico's die sectoren en domeinen overstijgen en de versterking van de samenwerking met andere colleges, marktoezichthouder en rijksinspecties is hierin van belang zodat risico's effectiever aangepakt kunnen worden.

2.3 De AP oordeelt dat het wetsvoorstel over uitlenen tijdelijk personeel tekortschiet

De AP heeft bezwaar gemaakt tegen de wijziging van de Wet allocatie arbeidskrachten door intermediairs (Waadi) waarmee het kabinet de markt voor het ter beschikking stellen van arbeidskrachten beter wil reguleren. Het wetsvoorstel maakt het voor uitzend- en detacheringsbureaus mogelijk om alleen nog tijdelijk personeel uit te lenen aan inleners als zij over een special certificaat beschikken waarmee kan worden aangetoond dat deze bureaus aan bepaalde normen voldoen. Deze certificaten worden door een nieuwe, nog op te richten instantie, verstrekt die op haar beurt inspectiediensten aanwijst die zullen toezien op de naleving van de nieuwe regelgeving.

Om te controleren of inleners zich aan deze nieuwe regel houden, kunnen zij aan inspecties worden onderworpen. Volgens de AP blijft het echter onduidelijk hoe er in dit keurmerksysteem wordt omgegaan met persoonsgegevens en het gevolg hiervan is dat de privacy van betrokkenen onvoldoende wordt beschermd. Hoewel het wetsvoorstel de uitwisseling van persoonsgegevens noodzakelijk acht, blijft het onduidelijk of inleners verplicht zijn om bij de uitvoering van inspecties persoonsgegevens te verstrekken van individuele arbeidskrachten, aan wie deze persoonsgegevens verstrekt dienen te worden, welke persoonsgegevens verstrekt dienen te worden en waarom dit noodzakelijk is. Door dit gebrek aan begrenzing, transparantie en motivatie is de AP tot de conclusie gekomen dat het momenteel niet vaststaat dat de gegevensverwerking überhaupt noodzakelijk is voor het certificeringsstelsel.

De AP maakte al eerder bezwaar tegen arbeidsmarktwetgeving die onvoldoende in staat bleek grenzen te stellen aan de verwerking van persoonsgegevens. Dat opeenvolgende arbeidsmarktwetten vergelijkbare onduidelijkheden bevatten, is volgens de AP onwenselijk en vereist dat er duidelijke grenzen worden getrokken.

2.4 Boete voor het ontbreken DPIA voor de inzet van camera-auto's in Rotterdam

De Autoriteit Persoonsgegevens (AP) heeft in december een boete van 50.000 euro opgelegd aan de korpschef van de Politie. Reden voor de boete is de onrechtmatige inzet van camera-auto's in Rotterdam tijdens de coronapandemie. Wat ging er precies mis?

De gemeente Rotterdam en de politie hebben in 2020 voor vijf weken lang twee auto's ingezet die waren uitgerust met 360-gradencamera's. Met de inzet van de auto's wilden de gemeente en de politie controleren of mensen zich aan de 1,5 meter regel hielden. De beelden die met de camera's werden gemaakt, kwamen binnen in de zogeheten meldkamer Handhaving en werden doorgestuurd naar de 'uitkijkruimte cameratoezicht' waar de beelden werden bekeken. De camerabeelden konden eventueel worden doorgestuurd naar andere onderdelen van de politie. De AP heeft naar aanleiding van de inzet van de camera-auto's een onderzoek ingesteld.

De Wet op politiegegevens
De camerabeelden worden in deze context gezien als politiegegevens. Er is immers sprake van een verwerking van persoonsgegevens in het kader van de uitvoering van de politietaak. Als gevolg is de politie wettelijk gezien verantwoordelijk voor de beelden. Op politiegegevens is de Wet politiegegevens (Wpg) van toepassing. Dit is een speciale wet die de verwerking van persoonsgegevens voor politietaken regelt. De AP is tevens toezichthouder op de Wpg.

Ontbreken van DPIA voorafgaand de verwerking van persoonsgegevens
Voorafgaand aan de inzet van de camerawagens is geen Data Protection Impact Assessment (DPIA) uitgevoerd. Volgens de AP was dit wel vereist. Uit het boetebesluit blijkt dat de camera-auto's namelijk vanaf 26 april 2020 zijn ingezet en de DPIA, een maand later, op 26 mei 2020 definitief is vastgesteld en goedgekeurd. Net zoals de AVG, stelt de Wpg de uitvoering van een DPIA voorafgaand aan de verwerking verplicht voor verwerkingen die een hoog risico voor de rechten en vrijheden van personen inhouden.

Voor deze overtreding legt de AP de korpschef, de verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens bij de politie een boete van 50.000 euro op. Bij het bepalen van de hoogte van de boete houdt de AP rekening met het feit dat, in dit concrete geval, de inzet van de camera-auto's plaatsvond aan het begin van de COVID-19 uitbraak in Nederland en de korpschef waarschijnlijk de uitvoering van een DPIA voorafgaand aan de verwerking van de camerabeelden minder goed voor ogen had of dat hij zich genoodzaakt voelde een afweging te maken.

De verwerking van persoonsgegevens was niet noodzakelijk en bovenmatig
Ten tweede constateert de AP dat de verwerking van de camerabeelden niet noodzakelijk en bovenmatig was. Volgens de AP zijn op verschillende dagen camerabeelden gemaakt terwijl geen sprake was van groepsvorming of een andere overtreding van coronamaatregelen. Daarnaast zijn ook beelden gemaakt terwijl de auto zich niet in een drukbezocht gebied bevond, maar onderweg was van A naar B. Hieruit maakt de AP op dat camerabeelden zijn gemaakt die niet noodzakelijk waren voor de uitvoering van de politietaak. De korpschef heeft deze overtreding erkend. De AP kan op grond van de Wpg voor deze overtreding echter geen boete opleggen.

Tegenstrijdige opvattingen over de rechtmatigheid van de verwerking
Ten slotte neemt de AP het standpunt in dat de camerabeelden onrechtmatig zijn verkregen. Dit laatste punt betwist de korpschef. De camera-auto's zijn ingezet op grond van artikel 3 van de Politiewet. De AP meent dat artikel 3 Politiewet alleen als grondslag kan dienen voor incidentele en kortstondige inzet van camera's door de politie. Nu er verschillende opvattingen bestaan over deze vraag, heeft de AP besloten om te werken aan normuitleg over dit wetsartikel.

Al met al, is het boetebesluit een goede reminder voor organisaties om hun DPIA's uit te voeren vóór de inzet van nieuwe technologieën of start van projecten. Want ook een te late uitvoering van een DPIA betreft een schending van de Wpg of AVG.

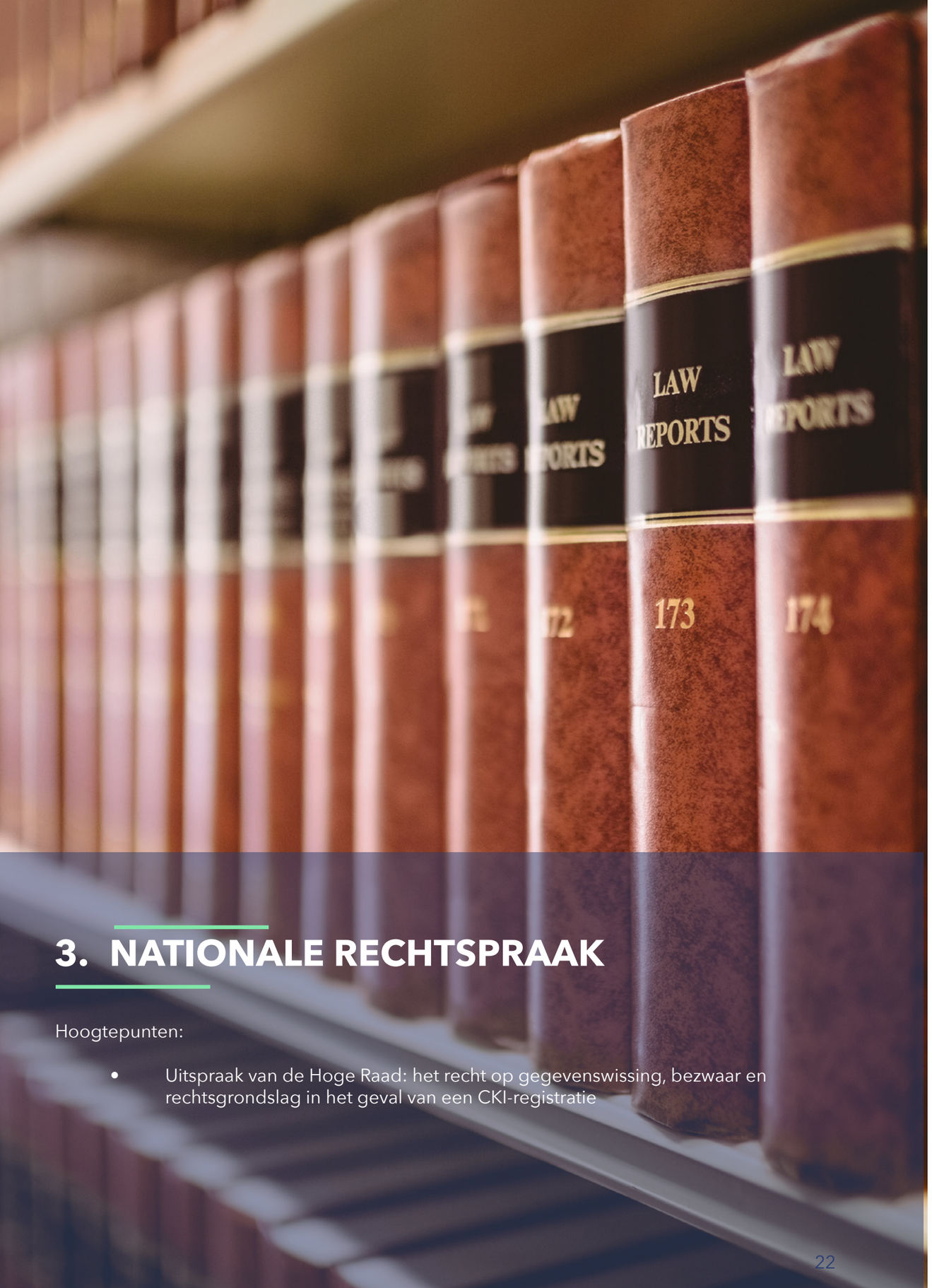
2.5 Landmacht verzamelt informatie tijdens de pandemie zonder juridische grondslag

Het Land Information Manouvre Centre (LIMC), deel van de Koninklijke Landmacht, heeft tijdens de coronapandemie onrechtmatig persoonsgegevens verwerkt. Dit blijkt uit een onderzoek dat is uitgevoerd door de Commissie van onderzoek Land Information Manoeuvre Centre (de Commissie). Het LIMC maakte en deelde analyserapporten over COVID-19 en de verspreiding van desinformatie. Met de publicatie van het onderzoek, wordt voldaan aan een verzoek van de Tweede Kamer om informatie over LIMC.

Het LIMC is vlak na de uitbraak van corona in Nederland opgericht en was tussen maart en november 2020 actief. In het LIMC kwamen medewerkers van verschillende eenheden bij elkaar om informatie over de impact van corona te verzamelen en te analyseren. Het LIMC was daarnaast, onder meer, ook bedoeld om te experimenteren met informatiegestuurd optreden. Nadat in mediaberichtgeving onder andere bleek dat het LIMC "gegevens had verzameld over de Nederlandse samenleving", en de FG van Defensie een onderzoek aankondigde, is het LIMC stilgelegd.

De Tweede Kamer heeft op 26 mei 2021 om een onafhankelijk onderzoek naar de besluitvorming rond het LIMC gevraagd. De minister van Defensie heeft vervolgens de Commissie van onderzoek Land Information Manoeuvre Centre ingesteld. De taak van de Commissie was om onderzoek te doen naar de besluitvorming rond zowel de oprichting als de uitvoering van de taken van het LIMC en lessen te formuleren voor de toekomst. In het rapport dat de Commissie heeft opgesteld, worden heldere conclusies getrokken. Zo wordt geconcludeerd dat er geen grondslag bestond voor de uitvoering van de activiteiten van de LIMC. Als gevolg bestond er ook geen rechtsgrond voor de persoonsgegevens die in dat kader werden verwerkt.

Defensie geeft aan dat aan de slag wordt gegaan met de conclusies en lessen uit het onderzoek om verder te werken aan de ontwikkeling van informatiegestuurd optreden, hierbij de waarborgen te versterken en verder te bouwen aan de toekomstige krijgsmacht.



3. NATIONALE RECHTSPRAAK

Hoogtepunten:

- Uitspraak van de Hoge Raad: het recht op gegevenswissing, bezwaar en rechtsgrondslag in het geval van een CKI-registratie

3.1 Uitspraak van de Hoge Raad: het recht op gegevenswissing, bezwaar en rechtsgrondslag in het geval van een CKI-registratie

In deze zaak doet de Hoge Raad uitspraak in een geschil tussen twee natuurlijke personen (de verzoekers) en de Rabobank. De verzoekers eisen een bevel inhoudende dat de Rabobank de kredietgegevens van verzoekers die in het Centraal Krediet Informatiesysteem (CKI) bij de Stichting Bureau Krediet Registratie (BKR) zijn geregistreerd, laat verwijderen. Zij beroepen zich daarbij op het recht van gegevenswissing en het recht op bezwaar, neergelegd in de Algemene Verordening Gegevensbescherming (AVG).

Het Centraal Krediet Informatiesysteem (CKI)
In het CKI worden kredietgegevens, zoals doorlopende kredieten, persoonlijke leningen, hypotheken en andere schulden van Nederlanders geregistreerd. Hierbij wordt onder andere het kredietbedrag, de persoonsgegevens van de desbetreffende persoon, de looptijd, de aflossingsdatum en eventuele achterstanden of andere onregelmatigheden bijgehouden. Aangesloten organisaties betreffen kredietaanbieders zoals banken, hypotheekaanbieders, gemeenten, telecombedrijven en autoleasebedrijven. Door het CKI te raadplegen krijgen zij een beter beeld van een (potentiële) klant en kunnen zij kredietrisico's beter inschatten. Ook is het raadplegen van het CKI bedoeld om de klant te beschermen tegen overkreditering en om aan de zorgplicht van kredietaanbieders te voldoen.

Behandeling door het gerechtshof
Nadat de rechtbank zich over het geschil heeft gebogen, is de zaak bij het hof terechtgekomen. Allereerst bekijkt het hof wat de rechtsgrond van de registratie in het CKI is. Volgens de verzoekers is de juiste grondslag voor de registratie artikel 6, eerste lid, onder f AVG (het gerechtvaardigd belang). Volgens de Rabobank is (ook) artikel 6, eerste lid, onder c AVG (wettelijke verplichting) de grondslag voor de verwerking. Het hof concludeert dat de CKI registratie plaatsvindt op grond van een wettelijke verplichting (sub c) welke is neergelegd in de Wet op het financieel toezicht (Wft). Omdat sprake is van een wettelijke verplichting, hebben de verzoekers geen recht op bezwaar en gegevenswissing. Volgens het hof zijn deze rechten immers gelinkt aan de rechtsgrondslagen 'taak van algemeen belang' en 'het gerechtvaardigd belang'.

Het hof meent evenwel dat elke verwerking van persoonsgegevens moet voldoen aan de eisen van proportionaliteit en subsidiariteit. Daarom dient er een belangenafweging te worden gemaakt tussen het belang van de verzoekers om de registratie te verwijderen en het belang van de (handhaving van de) registraties. Wanneer een registratie, onder meer, op grond van een wettelijke verplichting is gebaseerd, valt, volgens het hof, een belangenafweging altijd in het nadeel van de betrokkene uit, tenzij sprake is van een schrijnende situatie. In deze casus meent het hof dat de verzoekers weliswaar hinder ondervinden van de registratie, maar er geen sprake is van een schrijnende situatie als gevolg van de registratie.

De belangenafweging valt dan ook in het nadeel van de verzoekers uit en het hof bekrachtigt de beschikking van de rechtbank. De verzoekers besluiten tegen deze beslissing van het hof in cassatie bij de Hoge Raad te gaan.

Uitspraak van de Hoge Raad
Het besluit van de verzoekers om in cassatie te gaan, pakt voor hen goed uit. De Hoge Raad verwijst in haar beslissing naar een eerdere prejudiciële beslissing van 3 december 2021 (HR 3 december 2021, NJ 2022/258, m.nt. E.J. Dommering) waarin de Hoge Raad uitspraak doet in een vergelijkbare zaak waarin zij de Wft onder de loep neemt.

Volgens de Hoge Raad kan artikel 6, lid 1, sub c, AVG (wettelijke verplichting) niet dienen als grondslag voor de verwerking van persoonsgegevens in het CKI. Volgens haar zijn artikel 4:32 lid 1 en artikel 4:34 lid 1 Wft, welke kredietaanbieders tot deelname aan en raadpleging van een stelsel van kredietregistratie verplichten, namelijk niet voldoende duidelijk en nauwkeurig. Daarnaast is de toepassing ervan niet voldoende voorspelbaar voor degenen op wie de wettelijke bepalingen van toepassing zijn. Uit de wettelijke bepalingen blijkt namelijk niet welke persoonsgegevens in het CKI geregistreerd moeten of mogen worden, onder welke voorwaarden dit gebeurt en onder welke voorwaarden en termijnen de persoonsgegevens verwijderd moeten worden. Dit wordt wel geregeld in het CKI-reglement, maar dat reglement berust niet op een wettelijke grondslag. Daarnaast vindt de registratie van persoonsgegevens in het CKI plaats op grond van een overeenkomst tussen het BKR en kredietaanbieders.

Omdat de grondslag van artikel 6, lid 1, sub c, AVG (wettelijke verplichting) niet opgaat, moet de verwerking worden getoetst aan artikel 6, lid 1, sub f, AVG. Zodoende komt aan de verzoekers wel degelijk het recht op gegevenswissing en bezwaar toe. De Hoge Raad verwijst het geschil terug naar het hof. Deze moet de zaak, met deze nieuwe inzichten, opnieuw beoordelen.

4. WERELDWIJDE ONTWIKKELINGEN

Hoogtepunten:

- Privacy by Design wordt volgende maand een ISO-norm
- Franse Autoriteit voor gegevensbescherming (CNIL) legt Apple een boete van 8 miljoen euro op

4.1 Privacy by Design wordt volgende maand een ISO-norm

Veertien jaar nadat het onderwerp door een Canadese privacy commissaris werd geïntroduceerd, staat het in de AVG opgenomen vereiste van Privacy by Design (hierna: 'PbD') op het punt een internationale privacy norm te worden. Op 8 februari 2023 zal de Internationale Organisatie voor Standaardisatie (hierna: 'ISO') namelijk de standaard ISO 31700 aannemen dat een leidraad biedt voor de operationalisering van het PbD-principe.

De ISO is een netwerk van 167 nationale normalisatie-instituten. Zij stelt meer dan 24.000 normen vast, waaronder ISO 27001 voor beheersystemen voor informatiebeveiliging. Hoewel organisaties ten aanzien van sommige van deze standaarden certificering kunnen verkrijgen nadat zij door auditbedrijven zijn gecontroleerd, zal ISO 31700 aanvankelijk echter geen conformiteitsnorm zijn. In zijn oorspronkelijke vorm omvat PbD zeven beginselen, waaronder de bepaling dat privacy de standaardinstelling van een organisatie moet zijn, dat privacy moet worden ingebed in het ontwerp van IT-systemen en bedrijfspraktijken en dat privacy deel moet uitmaken van de gehele levenscyclus van gegevens. De definitieve ISO 31700 standaard biedt hierop een aanvulling en introduceert in totaal 30 voorschriften.

De standaard omvat algemene richtsnoeren voor het ontwerpen van mogelijkheden om consumenten in staat te stellen hun privacyrechten af te dwingen, het toewijzen van relevante rollen en autoriteiten, het verstrekken van privacyinformatie aan consumenten, het uitvoeren van privacyrisicobeoordelingen, het vaststellen en documenteren van eisen voor privacycontroles, hoe privacycontroles te ontwerpen, levenscyclusbeheer van gegevens en voorbereiding op en beheer in geval van een datalek. Bovendien verwijst de bibliografie van het document naar andere normen met meer gedetailleerde vereisten inzake de identificatie van persoonsgegevens, toegangscontroles, toestemming van de consument, corporate governance en andere onderwerpen.
Samen met de norm zal een afzonderlijk document mogelijke case studies schetsen om de praktische implementatie van PbD te vergemakkelijken.
Tot slot zal de officiële publicatie van de standaard worden gemarkeerd door een webinar met een overzicht van de norm voor bedrijfsmanagers, bedrijfseigenaren, voorvechters van consumentenprivacy en technologen.

4.2 Franse Autoriteit voor gegevensbescherming (CNIL) legt Apple een boete van 8 miljoen euro op

De CNIL heeft Apple onlangs een boete van 8 miljoen euro opgelegd omdat het bedrijf de gebruikers niet om toestemming heeft gevraagd voor de verwerking van hun persoonsgegevens om gepersonaliseerde advertenties aan te bieden.

De zaak draait om een eerdere versie van de door Apple gebruikte software voor mobiele telefoons, IoS versie 14.6, waarin persoonlijke gegevens van gebruikers, namelijk identifiers die waren opgeslagen op hun telefoons, door Apple werden verwerkt voor het aanbieden van gepersonaliseerde advertenties door middel van een vooraf aangevinkt vakje. Deze versie van IoS stond dus standaard toe dat Apple de op de telefoons van de gebruikers opgeslagen identificatiegegevens gebruikte voor reclamedoeleinden. Bovendien was het niet eenvoudig deze optie uit te schakelen en moesten gebruikers door ingebedde instellingen navigeren om hun toestemming voor deze verwerking te weigeren.

Volgens de CNIL betreft dit een inbreuk op artikel 82 van de Franse Data Beschermingswet, een wet ter uitvoering van de Europese e-privacyrichtlijn. Volgens deze bepaling is de verwerkingsverantwoordelijke verplicht om toestemming van de gebruikers van een elektronische-communicatiedienst te verkrijgen, alvorens de op de eindapparatuur van de gebruikers opgeslagen identificatiegegevens te gebruiken of te raadplegen. Hier bestaat wel een uitzondering op wanneer de verwerking noodzakelijk is om de door de gebruiker gewenste diensten te verlenen of "de elektronische communicatie te vergemakkelijken".

De CNIL was van mening dat het aanbieden van gepersonaliseerde advertenties niet onder een van de bovengenoemde uitzonderingen van artikel 82 viel. Voorts stelde de CNIL vast dat de toestemming die de gebruikers, door middel van het vooraf aangevinkte vakje, hadden gegeven, niet geldig was. Voor geldige toestemming is immers een actieve handeling van de betrokkene nodig. Zodoende is een boete van 8 miljoen euro opgelegd. Apple zal waarschijnlijk tegen deze beslissing in beroep gaan.