GDPR Update October 2018: Overview of developments since May 25, 2018 (Dutch)

October 4, 2018

Recente ontwikkelingen in de Europese Unie (EU)

Artikel 29 Werkgroep vervangen door de European Data Protection Board

Per 25 mei 2018 is de Artikel 29 Werkgroep opgeheven en vervangen door de *European Data Protection Board* (de EDPB). De EDPB is een onafhankelijk beslisorgaan met rechtspersoonlijkheid. De EDPB zal bijdragen aan de consistente toepassing van gegevensbeschermingsregels in de EU en zal de (grensoverschrijdende) samenwerking tussen toezichthoudende autoriteiten bevorderen. De EDPB is ingesteld op grond van de AVGB en bestaat uit de hoofden van de toezichthoudende autoriteiten van de EU-lidstaten en de Europese Toezichthouder voor Gegevensbescherming (de *European Data Protection Supervisor* (de EDPS), dan wel hun vertegenwoordigers. De EDPB is bevoegd om juridisch bindende beslissingen te nemen, bijvoorbeeld wanneer toezichthoudende autoriteiten een conflict hebben over hun competentie. De taken van de EDPB staan omschreven in artikel 70 AVGB.

EDPB-publicaties en EDPB-verklaring over de e-Privacy Verordening

Tijdens de eerste plenaire bijeenkomst op 25 mei 2018, heeft de EDPB een conceptversie van de Guidelines on Certification aangenomen. Tot 12 juli 2018 lagen deze richtlijnen voor ter publieke consultatie. De EDPB heeft ook de finale versie van de Guidelines on derogations applicable to International Transfers (artikel 49) aangenomen.

Daarnaast heeft de EDPB een verklaring aangenomen over de concept e-Privacy Verordening en de impact van die verordening op de bescherming van personen met betrekking tot de vertrouwelijkheid van hun communicatie.

Resolutie over de adequaatheid van de bescherming die het EU-US Privacy Shield biedt

Het EU-US Privacy Shield is een overeenkomst tussen de EU en de VS die het mogelijk maakt dat persoonsgegevens worden uitgewisseld tussen Europese en Amerikaanse bedrijven. Indien een Amerikaans bedrijf gecertificeerd is onder het EU-US Privacy Shield, dan wordt het bedrijf geacht te zijn gevestigd in een derde land waarvan de Europese Commissie heeft besloten dat dit land een adequaat beschermingsniveau biedt. In een dergelijk geval is doorgifte van persoonsgegevens vanuit de EU naar het betreffende bedrijf in de VS toegestaan.

In juli 2018 heeft het Europees Parlement een resolutie aangenomen waarin het Europees Parlement het standpunt inneemt dat de Privacy Shield-overeenkomst geen adequaat beschermingsniveau biedt naar maatstaven van het gegevensbeschermingsrecht zoals dat geldt in de EU en op grond van het EU-Handvest. In de resolutie pleit het Europees Parlement voor een schorsing van het EU-US Privacy Shield, tenzij de Amerikaanse autoriteiten voor 1 september 2018 volledig zouden voldoen aan de vereisten.
Momenteel is het EU-US Privacy Shield nog in werking, maar wij adviseren organisaties om terughoudend te zijn om

de doorgifte van persoonsgegevens naar de VS uitsluitend op het EU-US Privacy Shield te baseren.

Beheerder van een Facebook fan-pagina is gezamenlijke verantwoordelijke met Facebook

Het Hof van Justitie van de Europese Unie (het HvJ) heeft beslist dat de beheerder van een Facebook fan-pagina gezamenlijk verantwoordelijk is voor de verwerking van persoonsgegevens van fan-paginabezoekers door middel van het gebruik van *Facebook Insights*. In het geval waarover het HvJ besliste, is de beheerder van de fan-pagina een Duitse organisatie, *Wirtschaftsakademie Schleswig-Holstein*, die opereert in het onderwijsveld en onderwijsdiensten aanbiedt onder andere via een fan-pagina die wordt gehost door Facebook.

Het HvJ oordeelde dat *Wirtschaftsakademie* het mogelijk heeft gemaakt voor Facebook om persoonsgegevens te verzamelen van fan-paginabezoekers door de fan-pagina te creëren. Facebook werd daarmee in staat gesteld om cookies te plaatsen op de randapparatuur van de bezoekers. In die context had *Wirtschaftsakademie* de mogelijkheid om met behulp van filters die door Facebook beschikbaar waren gesteld criteria te definiëren aan de hand waarvan statistieken voor advertentiedoeleinden moesten worden samengesteld door Facebook. De beheerder van de fan-pagina heeft zelfs de mogelijkheid om de categorieën van personen aan te wijzen van wie persoonsgegevens gebruikt mogen worden door Facebook. De beheerder van de fan-pagina assisteert op deze manier in het verwerken van persoonsgegevens via haar fan-pagina en moet daarom worden aangemerkt als gezamenlijke verantwoordelijke met Facebook. Belangrijk is dat het HvJ opmerkt dat voor het bestaan van gezamenlijke verantwoordelijkheid niet is vereist dat iedere verantwoordelijke daadwerkelijk toegang heeft tot de betreffende persoonsgegevens.

De uitspraak van het HvJ is gebaseerd op de Privacy Richtlijn (zoals ingetrokken per 25 mei 2018). Echter, aangezien de het begrip ‘verantwoordelijke’ inhoudelijk niet is gewijzigd, is deze uitspraak ook van belang onder de AVGB.

In reactie op de uitspraak van het HvJ heeft Facebook een Addendum Gezamenlijke Verantwoordelijke gemaakt waarmee iedere gebruiker van *Facebook Insights* nu akkoord moet gaan.

Klachten tegen Google, Facebook, Instagram en Whatsapp door privacygroep noyb.eu

Op de eerste dag dat de AVGB van toepassing was, heeft privacygroep Nyob.eu (geleid door privacy-activist Max Schrems) vier klachten over “gedwongen toestemming” ingediend (pdf) tegen Google, Facebook, Instagram en Whatsapp bij vier verschillende toezichthoudende autoriteiten (de toezichthoudende autoriteiten in Frankrijk, België, Hamburg en Oostenrijk). Tot op heden zijn er nog geen verdere ontwikkelingen openbaar gemaakt over de consequenties of afwikkeling van deze klachten.

CNIL geeft formele waarschuwing aan twee marketing startups

De Franse toezichthoudende autoriteit (de CNIL) heeft formele waarschuwingen gegeven aan twee Franse startups in de advertentiebranche, te weten FIDZUP en TEEMO.

FIDZUP (een bedrijf dat partnerschappen heeft met verschillende uitgevers van mobiele applicaties), heeft een trackingtool ontworpen die geïmplementeerd werd in de applicaties van uitgevers van mobiele applicaties. De implementatie hiervan stelde FIDZUP in staat om MAC-adressen en advertentie-ID’s te verzamelen van de gebruikers van deze applicaties. Daarnaast plaatste FIDZUP bij verschillende winkels Wi-Fi-routers die MAC-adressen registreerden van personen die zich binnen het bereik van de router bevonden. FIDZUP combineerde de gegevens en kon vervolgens de MAC-adressen zoals verzameld via de applicaties koppelen aan de MAC-adressen zoals verzameld via de Wi-Fi-routers. Dit stelde FIDZUP in staat om gebruikers van de applicatie advertenties te laten zien gebaseerd op hun locatie.

Volgens de CNIL heeft FIDZUP geen geldige toestemming verkregen voor het verzamelen van deze persoonsgegevens. Gebruikers werd bij het installeren van de applicatie om toestemming gevraagd voor het verzamelen van locatiegegevens. De CNIL meent dat deze toestemming niet 'geïnformeerd', en dus ongeldig was. De gebruikers werden bijvoorbeeld niet geïnformeerd over de advertentiedoeleinden en de identiteit van FIDZUP. Deze informatie werd pas verstrekt nadat de persoonsgegevens waren verzameld (terwijl dit op voorhand had moeten gebeuren). Daarnaast overwoog de CNIL dat de toestemming niet 'vrij' was gegeven. Het bleek niet mogelijk om de applicaties te downloaden zonder de trackingtool van FIDZUP.

Volgens de CNIL werd ook de informatie omtrent de verzameling van persoonsgegevens via de Wi-Fi-routers te laat gegeven. De informatie werd gegeven via papieren posters die in de winkels hingen. Echter, op het moment dat betrokkenen de posters daadwerkelijk konden lezen, waren hun gegevens al verzameld.

De startup TEEMO lijkt qua werkzaamheden op FIDZUP. Ook TEEMO kon via een trackingtool geografische gegevens van applicatie gebruikers verzamelen. Door middel van de verzamelde informatie kon TEEMO profielen maken van de gebruikers om hen vervolgens gerichte advertenties aan te kunnen bieden.

Volgens de CNIL heeft ook TEEMO geen geldige toestemming verkregen. Allereerst bleken de gebruikers op het moment van het installeren van de applicatie niet geïnformeerd te zijn over het feit dat hun geografische gegevens voor profileringsdoeleinden zouden worden verzameld. De informatie werd pas verschaft na de installatie van de applicatie (op dat moment waren de persoonsgegevens al verzameld). Daarnaast was het ook in het geval van TEEMO niet mogelijk om de applicatie zonder de trackingtool te downloaden. De CNIL was van mening dat ook in dit geval toestemming daardoor niet 'vrij' kon zijn gegeven.

De CNIL heeft beide bedrijven opgedragen om binnen drie maanden (alsnog) geldige toestemming te verkrijgen van de gebruikers. Doen zij dit niet dan zullen er vermoedelijk sancties volgen.

Recente ontwikkelingen in Nederland

Meer dan 600 klachten ingediend bij Autoriteit Persoonsgegevens

Meer dan 600 personen hebben inmiddels een klacht ingediend bij de Autoriteit Persoonsgegevens (de AP). Op 29 juni 2018 had de AP de eerste 400 klachten al geanalyseerd. Bijna een derde van de klachten is gerelateerd aan problemen met verwijderingsverzoeken. Andere klachten gaan voornamelijk over ongewenste doorgifte van persoonsgegevens aan derde partijen (18%) en over problemen met inzageverzoeken (5%).

Toezichtkader van de Autoriteit Persoonsgegevens

Op 25 mei 2018 heeft de AP haar toezichtkader gepubliceerd. In dit document zijn de uitgangspunten voor het toezicht voor het jaar 2018 – 2019 opgenomen. Volgens het toezichtkader zal de AP zich in eerste instantie richten op de naleving van het zogeheten *accountability*-beginsel door middel van onderzoek en het doen van verzoeken tot informatieverstrekking.

In deze context heeft de AP inmiddels onderzocht of de organisaties die verplicht zijn om een Functionaris Gegevensbescherming (een FG) aan te stellen dit ook daadwerkelijk hebben gedaan. Daarbij heeft de AP zich gericht op overheden en zorginstellingen. De AP is bij meer dan 400 overheidsorganisaties nagegaan of zij een FG hadden aangesteld en geregistreerd. De eerste resultaten van deze steekproef (of 'speldenprikactie') toonden aan dat minder dan 4% van de organisaties (nog) geen FG had aangesteld. Deze organisaties kregen van de AP tot 11 juni om alsnog aan deze verplichting te voldoen. Op 3 september liet de AP weten dat nog slechts één van de onderzochte organisaties nog geen FG had aangewezen, maar dat deze organisatie dit spoedig zou doen.

Volgens het toezichtkader van de AP zijn andere focusgebieden van de AP: (i) de verwerking van medische gegevens,

(ii) de handel in persoonsgegevens en (iii) datalekken (in het bijzonder niet-gemelde datalekken en datalekken die het gevolg zijn van ernstige tekortkomingen in de beveiliging).

Op 17 juli 2018, heeft de AP een onderzoek aangekondigd naar de naleving van de AVGB door grote organisaties in de private sector. Bij dertig grote organisaties in tien verschillende private sectoren werd gecontroleerd op de implementatie van het verplichte register van verwerkingsactiviteiten. De AP meent dat het hebben van een compleet en accuraat register van verwerkingsactiviteiten een belangrijke eerste stap is waarmee een organisatie laat zien dat zij de privacyregels serieus neemt.

Op 17 september kondigde de voorzitter van de AP in een radio-interview aan dat een aantal bedrijven een last onder dwangsom is opgelegd die verbeurd zal worden op het moment dat deze bedrijven niet binnen een door de AP gestelde termijn voldoen aan de AVGB. De AP heeft niet bekend gemaakt welke bedrijven het betreft, om wat voor soort overtredingen het gaat en hoelang de periode is die de organisaties hebben gekregen om overtredingen te herstellen. Voorgaande bevestigt wel de voorzetting van de pre-AVGB-praktijk door de AP waarbij er in geval van een overtreding eerst een waarschuwing wordt gegeven alvorens er een boete volgt. De AP heeft echter wel duidelijk gemaakt dat wanneer bedrijven bewust de AVGB overtreden, zij wel onmiddellijk tot het opleggen van boetes zal overgaan.

Aanpassing van nationale wetgeving aan de AVGB (Aanpassingswet AVGB)

Als gevolg van de AVGB (die rechtstreeks doorwerkt in het Nederlandse recht) en de Uitvoeringswet AVGB, is het noodzakelijk dat de nationale wet- en regelgeving die nog steeds verwijzingen naar de Wet bescherming persoonsgegevens bevat of verouderde terminologie hanteert, wordt aangepast. De Aanpassingswet AVGB/UAVGB is in werking getreden en heeft terugwerkende kracht tot 25 mei 2018, de datum waarop de AVGB van toepassing is geworden.

Belastingdienst verwerkt BSN in strijd met de AVGB

De AP heeft geoordeeld dat de Belastingdienst geen wettelijke grondslag heeft om het Burgerservicenummer (het BSN) in het btw-identificatienummer van ZZP’ers te gebruiken. Volgens de AP maakt gebruik van het BSN tevens inbreuk op artikel 5(1)(a) en artikel 6(1) AVGB (respectievelijk de beginselen van rechtmatigheid, behoorlijkheid en transparantie, en de wettelijke grondslagen voor de gegevensverwerking).

In Nederland zijn ZZP’ers die onder de btw-wetgeving vallen verplicht zich te registreren voor een btw-nummer bij de Belastingdienst. Het btw-nummer bestaat voornamelijk uit het BSN van de ZZP’er. Het BSN is een uniek en persoonsgebonden nummer dat wordt gebruikt om communicatie te faciliteren tussen de burger en de overheid.

Btw-nummers moeten worden weergegeven op facturen en op de website van ZZP’ers, wat betekent dat iedereen de mogelijkheid heeft het BSN van de ZZP’ers te achterhalen. Dit kan leiden tot identiteitsfraude en andere vormen van misbruik.

Artikel 87 AVG geeft lidstaten de mogelijkheid hun eigen voorwaarden te stellen aan het verwerken van nationale identificatienummers. Deze mogelijkheid is geïmplementeerd in artikel 46 van de UAVGB: het verwerken van het BSN is slechts toegestaan als er regelgeving is die expliciet verwerking van het BSN voor een specifiek doel toestaat. Dit is niet het geval voor btw-nummers.

De Belastingdienst moet voor 1 januari 2019 stoppen met het verwerken van het BSN. Het is echter al duidelijk geworden dat de Belastingdienst niet in staat is om haar systemen voor deze datum aan te passen. Het is de vraag hoe de AP hiermee in de praktijk zal omgaan.

De Nationale Politie beboet voor het niet monitoren van toegang tot

persoonsgegevens

In 2015 heeft de AP een onderzoek gedaan naar de verwerking van persoonsgegevens door de Nationale Politie met het computersysteem dat gebruikt wordt om inkomende en uitgaande goederen en personen in het Schengengebied te monitoren. In dat onderzoek heeft de AP meerdere kwetsbaarheden gevonden in het systeem. Een van deze kwetsbaarheden was dat de Nationale Politie niet (zorgvuldig) de logbestanden met informatie over wie zich op welk moment toegang tot had verschaft tot de persoonsgegevens monitorde. De AP benadrukte dat het monitoren van dergelijke logbestanden een belangrijk hulpmiddel is om te achterhalen of persoonsgegevens onrechtmatig worden ingezien of gebruikt. De Nationale Politie heeft dit probleem niet binnen de door de AP gestelde termijn opgelost en kreeg daarvoor een boete van EUR 40.000. Hoewel dit besluit is genomen onder de Richtlijn, blijft dit ook in de AVGB-praktijk relevant.

Waarschuwing voor misleidend AVGB-keurmerk

In een recent nieuwsbericht heeft de AP organisaties gewaarschuwd voor misleidende AVGB-keurmerken. Er zijn bedrijven die beweren dat zij AVGB-keurmerken kunnen afgeven waarmee organisaties kunnen aantonen dat zij voldoen aan de privacyregelgeving. Dit soort bedrijven zegt soms nauw samen te werken met de AP, maar dit is niet het geval. Slechts certificatie-instellingen die zijn goedgekeurd (geaccrediteerd) door de Raad voor Accreditatie zijn bevoegd om dergelijke certificaten uit te schrijven. Op dit moment zijn er in Nederland nog geen organisaties geaccrediteerd voor het afgeven van een AVGB-keurmerk.

Klik hier om u aan te melden voor deze nieuwsbrief.

Overzicht behandelde onderwerpen

Januari 2017	Territoriale reikwijdte van de AVGB
Februari 2017	Het concept van toestemming
Maart 2017	Bijzondere persoonsgegevens
April 2017	'Accountability', 'Privacy by Design' en 'Privacy by Default'
Mei 2017	Rechten van betrokkenen (informatievoorziening)
Juni 2017	Rechten van betrokkenen (inzage, correctie en overdraagbaarheid)
Juli 2017	Rechten van betrokkenen (wissing, beperking, bezwaar en geautomatiseerde besluitvorming)
Augustus 2017	Verwerkers
September 2017	Datalekken en meldplichten
Oktober 2017	Functionaris voor de Gegevensbescherming
November 2017	Doorgifte van persoonsgegevens (buiten de EER)
December 2017	Toezichthouders (competenties, taken en bevoegdheden)
Januari 2018	One Stop Shop
Februari 2018	Sancties
Maart 2018	Verwerkingen van persoonsgegevens in arbeidsverhoudingen
April 2018	Profiliering en Retail
Mei 2018	Overview
Oktober 2018	Overzicht van ontwikkelingen sinds 25 mei 2018

Your Key Contacts

Marc Elshof
Partner, Amsterdam
D +31 20 795 36 09
M +31 6 46 37 61 08
marc.elshof@dentons.com

Celine van Es
Associate, Amsterdam
D +31 20 795 31 22
M +31 6 11 16 30 45
celine.vanes@dentons.com