Monthly newsletter GDPR: Accountability Privacy by Design and Privacy by Default (Dutch)

April 18, 2017

Nieuwsbrief AVGB: ‘Accountability’, ‘Privacy by Design’ en ‘Privacy by Default’

Introductie

Deze vierde AVGB-nieuwsbrief - de eerste sinds onze fusie met Dentons - behandelt enkele (nieuwe) belangrijke beginselen inzake de verwerking van persoonsgegevens, zijnde de beginselen van accountability, privacy by design en privacy by default.

Op grond van de Wet bescherming persoonsgegevens (Wbp) zijn organisaties die persoonsgegevens verwerken in beginsel verplicht om hiervan melding te maken bij de Autoriteit Persoonsgegevens (AP). Onder de Algemene Verordening Gegevensbescherming (AVGB) hoeft een verwerking van persoonsgegevens niet langer gemeld te worden. In plaats daarvan komen op organisaties grotere verantwoordelijkheden te liggen. De AVGB legt sterk de nadruk op accountability, de zogenaamde verantwoordingsplicht. Dit principe vereist dat organisaties passende technische en organisatorische maatregelen nemen om te voldoen aan de beginselen en verplichtingen uit de AVGB, en dit ook kunnen aantonen. Naar verwachting zullen de beginselen van *accountability*, *privacy by design* en *privacy by default* een behoorlijk effect hebben op de huidige gegevensverwerkingspraktijken van organisaties.

De AVGB verplicht organisaties om onder andere (i) een gedetailleerd register van verwerkingen bij te houden, (ii) indien van toepassing, een Privacy Impact Assessment uit te voeren en (iii) de beginselen van *privacy by design* en *privacy by default* te implementeren.

Het *accountability*-beginsel

Artikel 5 lid 2 AVGB introduceert het principe van *accountability*:

“De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen („verantwoordingsplicht”).

“Lid 1” verwijst naar Artikel 5 lid 1 AVGB dat de beginselen inzake de verwerking van persoonsgegevens opsomt. Conform Artikel 5 lid 1 AVGB moeten persoonsgegevens:

- worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is;
- voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt;
- toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden

verwerkt;

- juist zijn en zo nodig worden geactualiseerd;
- worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; en
- door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is.

Organisaties die persoonsgegevens verwerken, zijn verantwoordelijk voor de naleving van voormelde beginselen en dienen de naleving hiervan te kunnen aantonen. Daarnaast moeten organisaties bepaalde keuzes op dit gebied kunnen beargumenteren en deze argumentatie kunnen demonstreren.

Artikel 24 AVGB is een voorbeeld van de codificatie van het accountability-principe. De verwerkingsverantwoordelijke treft verplicht:

“passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.”

Op welke wijze een verwerkingsverantwoordelijke moet aantonen dat de verwerking in overeenstemming met de AVGB geschiedt, wordt niet nader gespecificeerd. Op dit gebied mogen vóór 25 mei 2018 (de datum waarop de AVGB van toepassing wordt) aanwijzingen van de Artikel 29 Werkgroep (WG 29) worden verwacht.

Het register van verwerkingsactiviteiten

Een meer concrete invulling aan het *accountability*-principe wordt gegeven in Artikel 30 AVGB. Dit artikel verplicht de meeste verwerkingsverantwoordelijken en verwerkers om een schriftelijk (waaronder elektronisch) register van hun verwerkingsactiviteiten bij te houden[1]. Het schriftelijke of elektronische register bevat in ieder geval de volgende gegevens:

a. de naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;
b. de verwerkingsdoeleinden;
c. een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
d. de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
e. indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, voor zover hiervan gebruik wordt gemaakt, de documenten inzake de passende waarborgen;
f. indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist; en
g. indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Ook verwerkers moeten een register bijhouden, namelijk van de verwerkingsactiviteiten die zij ten behoeve van de verwerkingsverantwoordelijke hebben verricht. Het schriftelijke of elektronische register bevat dan in ieder geval de volgende gegevens:

a. de naam en de contactgegevens van de verwerkers en van iedere verwerkingsverantwoordelijke voor rekening

waarvan de verwerker handelt, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker en van de functionaris voor gegevensbescherming;
b. de categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd;
c. indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie en, voor zover hiervan gebruik wordt gemaakt, de documenten inzake de passende waarborgen; en
d. indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

De beginselen van *privacy by design* en *privacy by default*

De beginselen van *privacy by design* en *privacy by default* verplichten organisaties om de bescherming van persoonsgegevens zowel in het beginstadium van de ontwikkeling van producten en diensten, als gedurende het gehele proces van gegevensverwerking in ogenschouw te nemen.

Privacy by design (gegevensbescherming door ontwerp)

Het beginsel van *privacy by design* speelt voornamelijk een rol op het moment dat er binnen organisaties nieuwe diensten en producten worden ontworpen. Artikel 25 lid 1 AVGB verplicht de verwerkingsverantwoordelijke zowel bij het bepalen van de verwerkingsmiddelen, als bij de verwerking zelf, passende technische en organisatorische maatregelen te treffen die zijn opgesteld met als doel de gegevensbeschermingsbeginselen op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen.

Organisaties moeten ervoor zorgen en moeten kunnen aantonen dat de bescherming van persoonsgegevens een aandachtspunt is geweest vanaf het moment van aanvang van het ontwerpproces. Wanneer pas in een later stadium de relevante producten en diensten in overeenstemming met de vereisten uit de AVGB worden gebracht, zullen hiermee hoogstwaarschijnlijk onnodige kosten gepaard gaan.

Privacy by default (gegevensbescherming door standaardinstellingen)

Artikel 25 lid 2 AVGB verplicht verwerkingsverantwoordelijken passende technische en organisatorische maatregelen te treffen om ervoor te zorgen dat in beginsel slechts persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid ervan. Deze maatregelen moeten er in het bijzonder voor zorgen dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal personen toegankelijk worden gemaakt.

Het beginsel van *privacy by default* is voornamelijk van belang voor diensten en producten waarbij de betrokkene zelf de keuze heeft om al dan niet zijn persoonsgegevens te delen. *Privacy by default* verplicht organisaties tot het beschermen van de persoonsgegevens van de betrokkene door de systemen op de meest privacy vriendelijke wijze in te stellen. Dit speelt in het bijzonder een rol in de verwerking van persoonsgegevens ten aanzien van *online* en *social media platforms*. In principe voldoen vooraf aangekruiste hokjes en applicaties die automatisch de locatie van betrokkene volgen niet aan de vereisten van *privacy by default*.

Hoe deze verplichtingen na te leven?

Om de naleving van deze verordening aan te kunnen tonen, zullen organisaties hun interne beleid moeten aanpassen en maatregelen moeten treffen die voldoen aan de beginselen van *privacy by design* en *privacy by default*. Dergelijke maatregelen kunnen onder meer zijn het minimaliseren van de verwerking van persoonsgegevens, het zo spoedig

mogelijk pseudonimiseren van persoonsgegevens, transparantie met betrekking tot de functies en de verwerking van persoonsgegevens, het in staat stellen van de betrokkene om controle uit te oefenen op de informatieverwerking, en het in staat stellen van de verwerkingsverantwoordelijke om beveiligingskenmerken te creëren en te verbeteren.

Bij de ontwikkeling, de uitwerking, de keuze en het gebruik van applicaties, diensten en producten die zijn gebaseerd op de verwerking van persoonsgegevens, of waarvan het gebruik de verwerking van persoonsgegevens meebrengt, dienen producenten te worden gestimuleerd om rekening te houden met het recht op bescherming van persoonsgegevens zodat de verwerkingsverantwoordelijken en de verwerkers in staat zijn te voldoen aan hun verplichtingen inzake gegevensbescherming.

Een goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat aan de voorschriften van *privacy by design* en *privacy by default* is voldaan.

Aanbevelingen voor de praktijk

Vanaf het moment dat de AVGB van toepassing is, is het niet langer de AP die een meldingsregister bijhoudt van de verwerking van persoonsgegevens binnen organisaties. In plaats daarvan zal de verwerkingsverantwoordelijke, als uitvloeisel van het *accountability*-principe, een accuraat register van verwerking van persoonsgegevens moeten bijhouden. Tevens rekening houdend met beginselen van *privacy by design* en *privacy by default*, valt het te verwachten dat binnen een aanzienlijk deel van de organisaties wijzingen in het interne beleid en de technische systemen nodig zullen zijn.

Het zal enige tijd vergen om alle verwerkingen van persoonsgegevens in kaart te brengen, in het bijzonder voor grotere organisaties die een aanzienlijke hoeveelheid aan en verschillende categorieën van persoonsgegevens verwerken. De vereiste veranderingen zullen voor 25 mei 2018 moeten zijn doorgevoerd. Vanaf die datum zal de AP actief toezien op de implementatie en naleving van de AVGB. Organisaties die de AVGB niet (behoorlijk) naleven, lopen het risico op forse boetes. Ons advies is daarom om tijdig te beginnen met de implementatie van de AVGB. Een goed begin daarbij is het in kaart brengen van de verschillende verwerkingen van persoonsgegevens binnen uw organisatie.

Klik hier om u aan te melden voor deze nieuwsbrief.

Overzicht van te behandelen 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

1. De plicht om een register van verwerkingsactiviteiten bij te houden is niet van toepassing op ondernemingen of organisaties die minder dan 250 personen in dienst hebben, tenzij het waarschijnlijk is dat de verwerking die zij verrichten een risico inhoudt voor de rechten en vrijheden van de betrokkenen, de verwerking niet incidenteel is, of de verwerking bijzondere categorieën van persoonsgegevens omvat (zie onze vorige nieuwsbrief). De uitzonderingen op de plicht om een register van verwerkingsactiviteiten bij te houden zijn derhalve beperkt en de meeste organisaties zullen verplicht zijn om een dergelijk register bij te houden.↩

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