GDPR Update: Sanctions (Dutch)

February 23, 2018

Inleiding

In deze AVGB-update behandelen wij de verscheidene sancties die toezichthoudende autoriteiten kunnen opleggen aan organisaties die niet voldoen aan de vereisten van de AVGB (non-compliant zijn).

Aanzienlijke administratieve boetes en andere corrigerende bevoegdheden van toezichthoudende autoriteiten vormen een centraal element van het nieuwe handhavingsbeleid dat de AVGB introduceert. Vanaf 25 mei 2018 hebben verwerkersverantwoordelijken en verwerkers toegenomen verantwoordelijkheden met betrekking tot de effectieve bescherming van persoonsgegevens. Indien organisaties zich aan deze verantwoordelijkheden onttrekken, mogen de toezichthoudende autoriteiten sancties opleggen.

Om individuen een consistent en hoog beschermingsniveau te kunnen bieden, dient het niveau van bescherming in alle EU-lidstaten gelijk te zijn. In grensoverschrijdende gevallen kan consistentie van de op te leggen sancties worden bereikt via het one-stop-shop mechanisme en, tot op zekere hoogte, door de samenwerking van toezichthoudende autoriteiten onder het AVGB coherentiemechanisme. De AVGB beoogt te voorkomen dat toezichthoudende autoriteiten in vergelijkbare gevallen verschillende corrigerende maatregelen opleggen. Desalniettemin blijven de toezichthoudende autoriteiten onafhankelijk in hun keuze voor de corrigerende maatregel in een specifiek geval.

Corrigerende maatregelen

In geval van niet-naleving van de AVGB, zal de bevoegde toezichthoudende autoriteit beoordelen wat de meest geschikte corrigerende maatregel is om deze niet-naleving aan te pakken. De toezichthoudende autoriteit heeft hiertoe verschillende bevoegdheden. Mogelijke sancties omvatten meer dan alleen administratieve boetes. De bevoegde toezichthoudende autoriteit heeft de volgende bevoegdheden tot het nemen van corrigerende maatregelen:

a. de organisatie waarschuwen dat met de voorgenomen verwerkingen waarschijnlijk inbreuk zal worden gemaakt op de bepalingen van de AVGB;
b. de organisatie berispen indien met verwerkingen inbreuk op bepalingen van de AVGB is gemaakt;
c. de organisatie bevelen de verzoeken van een betrokkene tot uitoefening van zijn rechten uit hoofde van de AVGB in te willigen;
d. de organisatie bevelen verwerkingsactiviteiten in overeenstemming te brengen met de bepalingen van de AVGB;
e. de verwerkingsverantwoordelijke bevelen een inbreuk in verband met persoonsgegevens aan de betrokkene te melden;
f. een tijdelijke of definitieve beperking van de verwerking van persoonsgegevens opleggen, waaronder een verbod op die verwerking;
g. bevelen persoonsgegevens te rectificeren of te verwijderen, dan wel een verwerking te beperken (al dan niet in

combinatie met een kennisgeving van dergelijke handelingen aan ontvangers aan wie de persoonsgegevens zijn verstrekt);

h. een certificering intrekken of een certificeringsorgaan opdragen een certificering in te trekken, of het certificeringsorgaan verbieden een certificering af te geven indien niet langer aan de vereisten voor certificering wordt voldaan;
i. bevelen de gegevensstromen naar een ontvanger buiten de EER of een internationale organisatie op te schorten; en/of
j. afhankelijk van de omstandigheden van het geval - naast of in plaats van de voorgenoemde maatregelen - een administratieve geldboete opleggen.

Elke maatregel die genomen wordt door de toezichthoudende autoriteit moet passend, noodzakelijk en evenredig, maar tegelijkertijd ook afschrikkend, zijn. De bevoegde toezichthoudende autoriteiten zullen iedere zaak individueel en op basis van alle omstandigheden van het specifieke geval moeten beoordelen.

Indien de inbreuk op de AVGB slechts als een geringe niet-naleving kan worden beschouwd, dan zal bijvoorbeeld een berisping eerder op zijn plaats zijn dan een administratieve boete.

Administratieve geldboetes

Terwijl de huidige Richtlijn Gegevensbescherming (Richtlijn 95/46/EG) slechts bepaalt dat de EU-lidstaten zelf sancties zullen moeten vaststellen, bepaalt de AVGB de (hoogte van de) administratieve boetes in geval van een inbreuk op de uitvoering daarvan. Bij het opleggen van een boete, zijn de toezichthoudende autoriteiten verplicht om rekening te houden met alle omstandigheden van het geval, waaronder:

- de aard, de ernst en de duur van de inbreuk, het doel en de duur van de verwerking in kwestie, alsmede het aantal getroffen betrokkenen en de omvang van de door hen geleden schade;
- de opzettelijke of nalatige aard van de inbreuk;
- de door de organisatie genomen maatregelen om de door de betrokkenen geleden schade te beperken (dat wil zeggen: de gevolgen van de inbreuk te beperken);
- de mate waarin de organisatie verantwoordelijk is gezien de technische en organisatorische maatregelen die deze heeft uitgevoerd;
- eerdere relevante inbreuken door de organisatie;
- de mate waarin er met de toezichthoudende autoriteit is samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen daarvan te beperken;
- de categorieën van persoonsgegevens waarop de inbreuk betrekking heeft (bijzondere of gevoelige categorieën van persoonsgegevens?);
- de wijze waarop de toezichthoudende autoriteit kennis heeft gekregen van de inbreuk, in het bijzonder of de organisatie de inbreuk zelf heeft gemeld;
- de naleving van eventuele eerder aan de organisatie opgelegde maatregelen met betrekking tot hetzelfde onderwerp;
- het aansluiten bij goedgekeurde gedragscodes of certificeringsmechanismen. Indien deze reeds adequate sanctiebepalingen bevatten, kunnen deze doeltreffend, evenredig en voldoende afschrikkend zijn, waardoor de noodzaak voor een toezichthoudende autoriteit om aanvullende maatregelen te nemen wordt beperkt; en

- elke andere verzwarende of verzachtende zijnde factor, zoals gemaakte winsten, of vermeden verliezen.

De Artikel 29-werkgroep (de WG29) heeft onlangs richtlijnen gepubliceerd met betrekking tot de toepassing en vaststelling van administratieve boetes. In dit document geeft de WG29 nadere invulling aan de bovengenoemde omstandigheden.

Twee niveaus van maximale boetes

Op grond van de Wet Bescherming Persoonsgegevens (de Wbp) heeft de Autoriteit Persoonsgegevens (de AP) de bevoegdheid om boetes op te leggen aan organisaties die inbreuk maken op de Wbp (deze bevoegdheid bestaat overigens pas sinds 1 januari 2016). Momenteel bedragen deze administratieve boetes maximaal €820.000 per overtreding. Slechts in het geval van opzet of ernstig verwijtbare nalatigheid kan de AP onmiddellijk een boete opleggen. In alle andere gevallen moet de AP eerst een bindende aanwijzing geven voordat zij een boete mag opleggen. De AP heeft beleidsregels gepubliceerd, waarmee inzicht wordt gegeven in de relevante factoren die bepalend zijn voor de hoogte van een boete in een concreet geval.

De AVGB bevat twee niveaus van maximale boetes die opgelegd kunnen worden in het geval de AVGB niet wordt nageleefd. Afhankelijk van de specifieke bepaling die door een organisatie is overtreden, bedragen administratieve boetes maximaal €20.000.000, of, wanneer dit bedrag hoger is, 4% van de totale wereldwijde jaaromzet van de organisatie. Het tweede niveau van boetes is maximaal een bedrag van €10.000.000 of 2% van de totale wereldwijde jaaromzet. Deze bedragen zijn maximumbedragen, wat betekent dat de toezichthoudende autoriteiten bevoegd zijn om lagere, maar geen hogere boetes op te leggen.

Het hoogste boeteniveau is beperkt tot de meest zwaarwegende schendingen van de AVGB, waaronder inbreuken met betrekking tot:

- de basisbeginselen inzake verwerking, zoals de voorwaarden voor toestemming;
- de rechten van de betrokkenen; en
- de doorgiften van persoonsgegevens aan een ontvanger in een land buiten de EER.

Overtredingen van de meeste andere bepalingen vallen onder de tweede categorie van boetes. Deze boetes hebben betrekking op overtredingen die verband houden met:

- toestemmingsmechanismen voor de verwerking van persoonsgegevens van kinderen;
- de implementatie van ‘privacy by design’ en ‘privacy by default’ ;
- de verplichting om een register van verwerkingsactiviteiten bij te houden;
- het meewerken met de toezichthoudende autoriteit;
- de beveiliging van het verwerken van persoonsgegevens;
- de melding van een datalek aan de toezichthoudende autoriteit;
- de melding van een datalek aan de betrokkene;
- gegevensbeschermingseffectbeoordelingen; en
- de aanwijzing van een functionaris voor de gegevensbescherming.

Handhaving en rechtsmiddelen

De bevoegde toezichthoudende autoriteit is gerechtigd om uit eigen beweging de naleving van de AVGB te monitoren en te handhaven (bijvoorbeeld door het uitvoeren van audits). In de praktijk zullen toezichthoudende autoriteiten vermoedelijk echter voornamelijk reageren op de klachten van betrokkenen (een recht waar de verantwoordelijken betrokkenen expliciet op moeten wijzen alvorens zij hun persoonsgegevens verwerken, en tevens indien zij reageren op een inzageverzoek) of berichtgeving in de media.

In geval van een juridisch bindend besluit van een toezichthoudende autoriteit (bijvoorbeeld een opgelegde geldboete), moeten organisaties het recht hebben een effectief rechtsmiddel in te stellen tegen een dergelijke beslissing. In Nederland hebben organisaties in eerste instantie het recht om bezwaar te maken tegen een aan hen gericht besluit van de Autoriteit Persoonsgegevens. Vervolgens kunnen zij van de beslissing op bezwaar in beroep bij de bestuursrechter.

Conclusie

De bevoegdheden van de toezichthoudende autoriteiten tot het opleggen van aanzienlijke boetes of andere sancties voor de niet-naleving van de AVGB, tonen het belang aan van een goede voorbereiding op de AVGB. Deze boetes en sancties stimuleren accountability (de naleving van de beginselen inzake verwerking van persoonsgegevens).

In onze visie zou de vrees voor aanzienlijke administratieve boetes of andere sancties evenwel niet de belangrijkste motivatie van organisaties moeten zijn om aan de AVGB te voldoen. Naleving van de AVGB moet primair gebaseerd zijn op de intrinsieke motivatie van organisaties om de privacy en fundamentele rechten van individuen (waaronder werknemers) te beschermen en om belangrijke klanten (zowel B2B als B2C) te binden door het vertrouwen te creëren dat persoonsgegevens op een eerlijke en transparante wijze worden verwerkt.

Het valt niet te verwachten dat de toezichthoudende autoriteiten onmiddellijk (maximale) administratieve boetes zullen opleggen aan organisaties die op 25 mei 2018 al goed op weg zijn met de implementatie van de AVGB. Zij zullen waarschijnlijk eerst met andere corrigerende maatregelen geconfronteerd worden.

Bovenstaande betekent natuurlijk niet de naderende deadline van 25 mei 2018 kan worden genegeerd. Organisaties die nog niet klaar zijn voor de AVGB adviseren wij allereerst te concentreren op hun risicovolle verwerkingsactiviteiten.

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

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