De "General Data Protection Regulation": persoonsgegevensverwerking in een strakker jasje

1. 25 mei 2018: GDPR treedt in voege

Over iets minder dan een jaar, op **25 mei 2018**, verkrijgt de 'General Data Protection Regulation' ("**GDPR**")[1] haar volledige uitwerking. De GDPR legt voor alle lidstaten van de Europese Unie de spelregels vast met betrekking tot de verwerking (en het vrije verkeer) van persoonsgegevens. Dergelijke regelgeving bestond al langer op Europees (en nationaal) niveau, maar de Europese regelgever was van oordeel dat er nood was aan een geactualiseerde (en op bepaalde punten meer krachtdadige) regelgeving in het licht van de steeds toenemende digitalisering en de technologische ontwikkelingen die voor een significante toename van persoonsgegevensverwerking hebben gezorgd.

De GDPR vervangt de huidige nationale privacywetgeving van de lidstaten van de Europese Unie.

Naast een bevestiging (of verstrenging) van een aantal principes die in België momenteel al zijn opgenomen in de Privacywet [2] (bijv. het recht op informatie en toegang tot persoonsgegevens, het recht op verbetering van persoonsgegevens, het recht op bezwaar tegen verwerking voor doeleinden van *direct marketing*), legt de GDPR ook heel wat nieuwe, strengere verplichtingen op aan ondernemingen.

Aangezien de GDPR een zeer ruime definitie van "persoonsgegevensverwerking" hanteert, vallen zeer veel ondernemingen (ongeacht hun omvang) onder haar toepassingsgebied: elke registratie of (geheel of gedeeltelijk) geautomatiseerde verwerking van persoonsgegevens (bijv. personeelsgegevens, klanten- of leveranciersgegevens) wordt immers geviseerd door de GDPR.

---

1 Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

2 De wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *B.S.* 18 maart 1993.

Hoewel u principieel nog een jaar de tijd heeft om uw onderneming “GDPR-proof” te maken, is het raadzaam om tijdig te anticiperen. Elke onderneming dient voor zichzelf *in concreto* de impact van de GDPR te analyseren en in kaart te brengen welke maatregelen al dan niet moeten worden genomen om “GDPR-compliant” te zijn.

Indien uw onderneming vandaag de dag al gebruik maakt van een privacyverklaring (‘privacy policy’), dan bekijkt u best of deze verklaring een update of bijsturing nodig heeft in het licht van de GDPR.

2. De nieuwigheden / verduidelijkingen van de GDPR in een notendop

Hieronder vatten wij een aantal van de belangrijkste nieuwigheden / verduidelijkingen van de GDPR voor u samen:

- **Verantwoordingsplicht**

Op elke onderneming die aan persoonsgegevensverwerking doet, rust een verantwoordingsplicht. Deze verplichting houdt in dat de verwerkingsverantwoordelijke te allen tijde zelf moet kunnen aantonen dat zij handelt in overeenstemming met de bepalingen van de GDPR. De genomen maatregelen moeten bovendien periodiek worden geëvalueerd en, waar nodig, geactualiseerd.

- **Register van de verwerkingsactiviteiten**

Om de naleving van deze verordening aan te kunnen tonen, dient de verwerkingsverantwoordelijke of de verwerker een register bij te houden van verwerkingsactiviteiten die onder zijn verantwoordelijkheid hebben plaatsgevonden.

Op elke verwerkingsverantwoordelijke of verwerker rust de verplichting tot het aanleggen (en bijhouden) van een “register van de verwerkingsactiviteiten” (dataregister) dat o.a. een overzicht biedt van de persoonsgegevens die worden verwerkt, de verwerkingsdoeleinden, waar de persoonsgegevens vandaan komen en met wie deze gegevens worden gedeeld.

Met de invoering van de verantwoordingsplicht wordt de huidige aanmeldingsplicht van bepaalde verwerkingen bij de Privacycommissie afgeschaft.

- **Vrije, specifieke, geïnformeerde en ondubbelzinnige toestemming van de betrokkene vereist**

Elke verwerking van persoonsgegevens moet verplicht steunen op een legitieme rechtsgrond. Indien de verwerking louter is gebaseerd op de toestemming van de persoon in kwestie, dient u ervoor te zorgen dat deze toestemming **vrij, specifiek, geïnformeerd én ondubbelzinnig** is (onder de bestaande wetgeving is enkel het criterium van "ondubbelzinnigheid" uitdrukkelijk van toepassing). Dit impliceert dat de aanvaarding van gegevensverwerking uitdrukkelijk dient te gebeuren, hetgeen een actieve handeling van de betrokkene veronderstelt (bijv. een schriftelijke verklaring, het klikken op een vakje bij een bezoek aan een internetwebsite ('opt-in') of een andere verklaring/handeling waaruit duidelijk blijkt dat de betrokkene instemt met de voorgestelde verwerking van zijn persoonsgegevens). Een louter stilzwijgen (bijv. het gebruik van reeds aangekruiste vakjes ('opt-out') geldt derhalve niet als een geldige toestemming.

Opdat toestemming met kennis van zaken wordt gegeven, moet de betrokkene ten minste bekend zijn met de identiteit van de verwerkingsverantwoordelijke en de doeleinden van de verwerking van de persoonsgegevens. Indien de verwerking meerdere doeleinden heeft, moet toestemming voor elk daarvan worden verleend. Belangrijk is ook dat de verleende toestemming wordt geregistreerd, aangezien u te allen tijde moet kunnen aantonen dat de toestemming op een correcte manier werd verkregen.

- **Recht op gegevenswissing ("recht op vergetelheid")**

Personen van wie persoonsgegevens worden verwerkt, hebben in een aantal gevallen het recht om zonder onredelijke vertraging de wissing van hen betreffende persoonsgegevens te verkrijgen, bijvoorbeeld wanneer de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of werden verwerkt of wanneer de toestemming tot de verwerking wordt ingetrokken door de betrokkenen (en er geen andere rechtsgrond voor de verwerking aanwezig is).

- ***'Privacy by design' & 'privacy by default'***

'*Privacy by design*' (gegevensbescherming door ontwerp) en '*privacy by default*' (gegevensbescherming door standaardinstellingen) zijn de uitgangspunten die worden vooropgesteld door de GDPR. Deze principes impliceren dat een onderneming bij de

ontwikkeling en uitwerking van (nieuwe) producten en diensten (bijv. data systemen) moet waken over de beveiliging van persoonsgegevens door het nemen van passende technische en organisatorische maatregelen (bijv. 'pseudonimisering', d.i. een techniek van informatiebeveiliging waarbij bepaalde persoonsgegevens worden versleuteld zodat deze niet meer rechtstreeks herleidbaar zijn tot een persoon) met als doel om de persoonsgegevensbescherming overeenkomstig de GDPR te waarborgen. De instellingen van een data systeem moeten standaard dusdanig ingesteld zijn dat ze maximaal persoonsgegevens beschermen.

- **Aanstelling van '*data protection officer*'**

Volgens de GDPR moet een onderneming in bepaalde gevallen een zogenaamde 'data protection officer' ("functionaris voor gegevensbescherming") aanduiden (met name in het geval van *direct marketing* of *profiling* de kernactiviteit van de onderneming uitmaakt). Deze persoon, die zowel een personeelslid of een externe consultant kan zijn, fungeert als een soort preventieadviseur.

- **Gegevensbeschermingseffectbeoordeling**

De GDPR legt in welbepaalde gevallen de verplichting op aan de verwerkingsverantwoordelijke om een 'gegevensbeschermingseffectbeoordeling' uit te voeren, d.i. een voorafgaande beoordeling van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Deze verplichting is met name van toepassing wanneer de verwerking – gelet op de aard, de omvang, de context en de doeleinden ervan – waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van de betrokken personen.

- **Meldingsplicht i.g.v. vastgestelde inbreuken**

Uw onderneming is verplicht om bepaalde inbreuken op de beveiliging of datalekken te melden aan de toezichthoudende overheid (voor België: de Privacycommissie) binnen de 72 uur. Indien de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, dienen ook de betrokken personen te worden ingelicht. Bovendien dienen de nodige procedures te worden ingebouwd om eventuele datalekken op te sporen, te documenteren en te onderzoeken.

- **Overdraagbaarheid van persoonsgegevens**

Elke persoon waarvan persoonsgegevens worden verwerkt, heeft onder de GDPR het recht om zijn persoonsgegevens op te vragen in een "*gestructureerde, gangbare en machinaal leesbare vorm*" en deze rechtstreeks en ongehinderd over te dragen aan een andere verwerkingsverantwoordelijke.

3. Financiële sancties

Een belangrijke, afzonderlijk te vermelden nieuwigheid is ten slotte dat de Europese regelgever voor het eerst de mogelijkheid heeft gecreëerd voor lidstaten om in bepaalde gevallen (substantiële) financiële sancties op te leggen aan ondernemingen die de regels van de GDPR overtreden. Zo kunnen de administratieve geldboetes voor de meest ernstige inbreuken oplopen tot 20.000.000 EUR of 4% van de jaaromzet (indien dit een bedrag van 20.000.000 EUR overstijgt).

Uw onderneming heeft er dus alle belang bij om de regels van de GDPR correct toe te passen!

*

* *