contrast

Privacy / Data Protection – Bedrijven: 1 – 0

november 2016

Stel je voor...

Zoals elke middag, ga je rond 12u30 naar de cafetaria van je bedrijf om met collega's te lunchen. Meteen merk je dat het gesprek onder de collega's deze middag geanimeerder is dan anders. Jan van *human resources* spreekt over een grondige oefening die zal moeten gebeuren, met de eventuele aanstelling van een *DPO* en het uitvoeren van een *DPIA*. Sofie van *marketing* reageert dat de invoering van de *GDPR* uitgebreide bevoegdheden voorziet voor de *DPAs*, met op Europees niveau een *EDPB*. Marc, de *compliance officer*, kijkt ernstig en mompelt dat gelet op de voorziene sancties, hij nu al immense druk ondervindt van het management om te zorgen dat het bedrijf in orde is met de nieuwe regels.

Jij hebt werkelijk geen idee waarover het gaat… *DPO*, *DPIA*, *GDPR*, … ? Sancties?

Even verduidelijken.

Meer dan 4 jaar nadat de Europese Commissie aankondigde dat zij de EU regels omtrent bescherming van persoonsgegevens zou hervormen, is op 24 mei 2016 de **nieuwe Algemene Verordening**

Gegevensbescherming (in het Engels “*General Data Protection Regulation*”, afgekort “*GDPR*”) in werking getreden. De GDPR is van toepassing op alle ondernemingen gevestigd in de Europese Unie evenals op ondernemingen gevestigd buiten de Europese Unie die diensten aanbieden binnen de Europese Unie. Ondernemingen hebben tot 25 mei 2018 de tijd om zich aan te passen aan de nieuwe regels omtrent de bescherming van persoonsgegevens.

Waarover gaat de GDPR?

De GDPR vervangt het aanmeldingssysteem bij de nationale privacy autoriteiten (in het Engels “*Data Protection Authorities*”, afgekort “*DPAs*”), dat vandaag in vele lidstaten bestaat, door een systeem van “**verantwoordingsplicht**” (“*accountability*”). Ondernemingen zullen zelf moeten nagaan of hun verwerking van persoonsgegevens in lijn is met de GDPR. Een onderdeel hiervan is het bijhouden van een **register met alle verwerkingsactiviteiten** die plaatsvinden onder de verantwoordelijkheid van de onderneming. Daarnaast voorziet de GDPR voor bepaalde verwerkingsactiviteiten een voorafgaande **gegevensbeschermingseffectbeoordeling** (in het Engels “*Data Protection Impact Assessment*”, afgekort “*DPIA*”). Opnieuw afhankelijk van de verwerkingsactiviteiten die zij uitvoeren, zullen sommige bedrijven ook een **gegevensbeschermingsfunctionaris** (in het Engels “*Data Protection Officer*”, afgekort “*DPO*”) moeten aanstellen. De GDPR voorziet nog in een aantal **andere verplichtingen**: ondernemingen moeten heel wat informatie verstrekken aan de betrokkenen (in het Engels “*data subjects*”) omtrent de verwerking van hun persoonsgegevens; er gelden strikte regels over het antwoord aan betrokkenen die hun rechten (op inzage, rectificatie, etc.) wensen uit te oefenen; overeenkomsten met verwerkers van persoonsgegevens (bijv. server providers) moeten verplicht bepaalde clausules bevatten; datalekken (in het Engels “*data breaches*”) moeten binnen een bepaalde termijn aan de privacy autoriteit gemeld worden; enz.

Wat is de sanctie?

Verschillende DPAs, waaronder de Belgische Privacycommissie kunnen op vandaag geen boetes opleggen. Inbreuken op de GDPR zullen daarentegen kunnen worden gesanctioneerd met administratieve geldboeten tot 20 miljoen EUR of tot 4% van de totale wereldwijde jaaromzet van de onderneming in het voorgaande boekjaar, indien dit cijfer hoger is. Deze boetes kunnen worden opgelegd door de bevoegde DPA, die onderzoeks- en vervolgingsbevoegdheden krijgen die zeer gelijkend zijn aan de bestaande bevoegdheden van mededingingsautoriteiten. Zo zullen DPAs verzoeken om informatie kunnen richten aan ondernemingen en inspecties ter plaatse (“*dawn raids*”) kunnen uitvoeren.

Hoe te voorkomen?

Ook in het privacyrecht geldt dat voorkomen beter is dan genezen. Het is belangrijk dat ondernemingen nu reeds actie ondernemen om ervoor te zorgen dat de verwerking van persoonsgegevens tegen 25 mei 2018 in lijn is met de GDPR. Een duidelijke *compliance policy* kan daarbij inbreuken op de GDPR voorkomen.

Concreet.

Het “ABC van de GDPR” kan u hier raadplegen.

Wat moet uw onderneming doen vooraleer de GDPR op 25 mei 2018 van toepassing wordt?

- U dient in de eerste plaats alle verwerkingsactiviteiten die binnen de onderneming worden uitgevoerd (zowel wat betreft de persoonsgegevens van werknemers als leveranciers / klanten en consumenten), in kaart te brengen.
- Vervolgens dient u voor elke verwerkingsactiviteit na te gaan of zij in lijn is met de GDPR, zoals: is er een rechtmatige verwerkingsgrond? Werden de betrokkenen correct geïnformeerd? Wordt de data correct bewaard? Desgevallend dient u het nodige te doen om de naleving van de GDPR te verzekeren.
- Parallel dient u best een interne *compliance policy* op te stellen met daarin procedures voor o.m. het opstarten van verwerkingsactiviteiten, het bijhouden van een register met verwerkingsactiviteiten, de opvolging van verzoeken van betrokkenen en het melden van datalekken. U dient de betrokkenen binnen de onderneming te trainen, opdat zij de *compliance policy* zouden kennen en in de praktijk ook effectief toepassen.

Meer weten?

Raadpleeg de website van de Belgische Privacycommissie of de Werkgroep Artikel 29 en het “ABC van de GDPR” van **contrast.**