GDPR: IS JOUW BEDRIJF TOE AAN DE EERSTE OF DE LAATSTE LOODJES?

JILL LEEN
Advocate

25 mei 2018. Een datum die hopelijk minstens bij één iemand binnen jouw bedrijf een belletje doet rinkelen. Die dag ging namelijk de General Data Protection Regulation (GDPR) van kracht. Ben jij er zeker van dat jouw firma helemaal mee is? Of hoor je geen belletje, maar wel een donderslag in Keulen? Negen vragen en evenveel antwoorden over de nieuwe manier waarop jouw bedrijf (hopelijk) persoonsgegevens verwerkt. Met dank aan de experts van advocatenkantoor Monard Law.

1 x Wij zijn maar een kleine KMO. De GDPR was en is niet van toepassing op mijn bedrijf.

Foute redenering en foute conclusie. De GDPR geldt voor elk bedrijf dat aan de *verwerking* doet van *persoonsgegevens*. Die twee termen zijn zo ruim gedefinieerd dat in de praktijk elk bedrijf dat klanten of personeel heeft, moet voldoen aan deze regelgeving.

2 x Ik wist van niks en ben met niets in orde. Hoelang duurt het om mijn bedrijf up-to-date te brengen?

Voor een gemiddelde KMO neemt het hele verhaal toch snel één à twee maanden in beslag. Al is het moeilijk om een precieze timing te hanteren. Alles hangt af van het type verwerkingsactiviteiten. Niet van de grootte van je bedrijf, dat is een misverstand. En of de verwerking van persoonsgegevens tot je core business behoort, dan wel eerder een gevolg is van de activiteiten. Voorbeeld: een kleine startup met als kernactiviteit de verwerking van gezondheidsgegevens van natuurlijke personen. En een groot bouwbedrijf met een driehonderdtal werknemers. Wel, die startup heeft een intensiever traject voor de boeg dan die nochtans grotere KMO. Net omdat hun gegevens én gevoeliger én een essentieel onderdeel zijn van hun business.

3 x Bestaat er zoiets als een snelle binnenweg naar GDPR-succes?

Neen. De snelste weg is om een externe partner in te schakelen die alles voor jou in orde brengt. Maar dat is niet hetzelfde als een binnenweg. Als je overhaast te werk gaat, ga je gegarandeerd bepaalde zaken over het hoofd zien. Onze aanpak begint daarom met een goede analyse van alle bedrijfsprocessen. Wat zijn de hete hangijzers en wat is minder prioritair? Daaruit volgt een plan van aanpak. Voor welke afdelingen staat wat te gebeuren? Hoeveel tijd neemt dat in beslag? Pas dan is het tijd voor de eigenlijke uitvoering.

4 x Ik dacht dat ik goed bezig was, maar ik heb geen functionaris voor gegevensbescherming of Data Protection Officer (DPO) aangesteld. Foutje?

Niet per se. Niet elke onderneming moet een DPO aanstellen. In zo'n 80% van de gevallen die wij als Monard onderzoeken is het zelfs geen wettelijke verplichting. Op grond van de GDPR is dit voor drie categorieën van organisaties verplicht. Dit is bijvoorbeeld het geval voor overheidsinstellingen (behalve het gerecht). Zo ook voor bedrijven die hoofdzakelijk belast zijn met grootschalige verwerkingen van gevoelige gegevens. Of voor organisaties die hoofzakelijk belast zijn met gegevensverwerkingen die een regelmatige en stelselmatige observatie op grote schaal vereisen. Een ziekenhuis bijvoorbeeld kan niet zonder DPO. Want zij zijn hoofdzakelijk bezig met de verwerking van gevoelige gegevens.

Behoort je onderneming niet tot één van deze drie categorieën? Gebruik de functietitel DPO dan ook niet zomaar. Als je iemand binnen je bedrijf benoemt tot DPO, moet hij of zij ook voldoen aan alle verplichtingen die deze functietitel met zich meebrengt.

5 x Ik denk dat mijn bedrijf met alles in orde is. Maar hoe kan ik 100% zeker zijn?
Door bijvoorbeeld een controle laten uit te voeren door een externe partner. Dit is zeker nuttig als je alles op eigen houtje deed: van het plan van aanpak opstellen tot de eigenlijke uitvoering. Dan bestaat de kans dat je iets vergat of een bepaald deel van de GDPR-wetgeving verkeerd interpreteerde. Een check-up biedt je meer zekerheid. Anders is de eerste controle die je krijgt het moment van de waarheid...

"DE GDPR GELDT VOOR ELK BEDRIJF DAT AAN DE VERWERKING DOET VAN PERSOONSGEGEVENS."

6 x Wie voert die controles uit?
De Gegevensbeschermingsautoriteit (GBA), een overheidsinstelling. De GBA vervangt de vroegere Privacycommissie. De nieuwe autoriteit is - net als haar voorganger - opgericht bij de Kamer van Volksvertegenwoordigers. Op 25 mei 2018, de dag dat ook de GDPR van kracht ging, werd de Privacycommissie opgeheven en kwam de GBA in de plaats. Eén onderdeel van haar ruimere takenpakket, is toezien op de naleving van de GDPR-wetgeving.

7 x Wanneer mag ik een controle verwachten?
Vanaf 25 mei 2018 kan in principe elk bedrijf zich aan een controle verwachten. Die controles gebeuren proactief en reactief. Proactief in die zin dat het initiatief vanuit de GBA zelf komt. Daarvoor bepalen zij zelf waar hun prioriteiten liggen. Reactief in die zin dat ze binnenkomende klachten opvolgen. Als pakweg een klant, leverancier of werknemer van jouw bedrijf een onregelmatigheid meldt, is het de plicht van de GBA om die klacht te onderzoeken. Je ontvangt in beide gevallen een brief die de controle aankondigt.

8 x Ik las dat de boetes kunnen oplopen tot 20 miljoen euro. Klopt dat?
Ja, de GDPR schrijft maximumboetes voor van 20 miljoen euro of - indien dit cijfer hoger is - 4% van de totale wereldwijde jaaromzet. Maar neen, zo'n vaart loopt het niet. Om twee redenen. Ten eerste omdat de voorzitter van de GBA al liet weten dat hij in eerste instantie vooral wil sensibiliseren. Het is hen er niet om te doen om zoveel mogelijk boetes uit te schrijven. Ten tweede omdat de boete onder andere in verhouding moet staan met de ernst en omvang van de inbreuk. Als de politie jou tegen 60 kilometer per uur flitst in de bebouwde kom, krijg je geen levenslang rijverbod.

Daarnaast zijn er nog andere factoren die meespelen. Meldde je een datalek bijvoorbeeld zelf? Of stapte een klant van jou naar de GBA? Samengevat: een monsterboete voor een KMO voor wie gegevenswerking niet hun *core business* is én die hun uiterste best deden om alles in orde te zetten? Dat zien we niet gauw gebeuren. Het zijn vooral de bedrijven die én gevoelige gegevens verwerken én die bewust hun voeten aan de GDPR vegen, die zich zorgen moeten maken.

9 x Moet ik na 25 mei nog iets doen?
Zeker. De GDPR is een continu proces. De lijnen die je tot 25 mei uitzette, moet je daarna doortrekken. Het is niet zo dat je vanaf die dag geen inspanningen meer hoeft te doen op vlak van de privacyregelgeving. Ook in de toekomst zal je bepaalde zaken moeten aftoetsen aan deze regels. En dat in elke betrokken afdeling: van IT tot de boekhouding en van marketing tot HR. Hoe intensief die inspanningen zullen zijn, heeft dan weer te maken met jouw specifieke bedrijf en welke rol gegevensverwerking speelt. Voor een KMO waar dat aandeel miniem is, liggen de kaarten anders dan voor een bedrijf dat big data verzamelt.