# Zes vragen die u helpen bij de voorbereiding op de GDPR

Als u met persoonsgegevens werkt, dan heeft de GDPR een impact op uw organisatie. Het is niet eenvoudig te weten welke stap u nu als eerste moet nemen.

Met het volgende eenvoudige stappenplan, zorgt u ervoor dat uw onderneming klaar staat voor 25 mei 2018:

**1. Welke persoonsgegevens heeft u in huis ?**

Persoonsgegevens verzamelt en verwerkt u op allerhande manieren: bij het opmaken van een factuur, het aanwerven van nieuwe personeelsleden, de (al dan niet automatische) opname van het e-mailadres in het bestand voor nieuwsbrieven, het bijhouden van e-mails van klanten,… verwerkt u steeds persoonsgegevens.

Als eerste stap moet u dus een overzicht maken van alle persoonsgegevens die u verzamelt in alle mogelijk afdeling van uw onderneming en de wijze waarop u deze verwerkt.

Dit houdt eveneens in dat u aangeeft met wie u deze persoonsgegevens eventueel heeft gedeeld (vb. het sociaal secretariaat, de drukker voor het verzenden van kerstkaarten,..).

Wanneer u gevoelige persoonsgegevens verwerkt, zoals ras, etniciteit, gezondheid, seksuele geaardheid, politieke opvattingen, .. moet u hier extra aandacht aan schenken. Zo zal u voor deze gegevens bijvoorbeeld extra beschermingsmaatregelen moeten nemen of expliciete toestemming van de betrokkene moeten vragen.

**2. Register van de verwerkingsactiviteiten opstellen of niet?**

Wanneer u weet welke persoonsgegevens u verwerkt, kan u vervolgens nagaan aan welke verplichtingen u moet voldoen.

Wanneer u meer dan 250 werknemers in dienst heeft, indien u gevoelige persoonsgegevens verwerkt of indien u “op niet incidentele wijze” persoonsgegevens verwerkt, bent u verplicht al deze informatie in een dataregister op te nemen.

Op dit moment bestaat er nog geen duidelijkheid over wat verstaan moet worden onder “op niet incidentele wijze”. Immers, zodra personeelsgegevens verwerkt worden, gebeurt dit niet op incidentele wijze zodat het bijhouden van het register volgens deze bepaling dan toch verplicht wordt.

Allicht zal de Belgische Privacycommissie hierover in de komende maanden nog standpunt innemen.

In afwachting daarvan raden wij aan om hoe dan ook een register van verwerkingsactiviteiten op te stellen en bij te houden.

De verordening vergroot immers de verantwoordingsplicht van de ondernemer: indien u kan aantonen dat u alle stappen tot bescherming van de persoonsgegevens heeft genomen, loopt u minder risico op een (hoge) boete wanneer er toch iets mis zou lopen.

In het register moet u volgende gegevens vermelden:

- wie de gegevens verwerkt (naam en contactpersoon)
- welke gegevens verwerkt worden en hun aard, alsook de categorie van de betrokkenen

- wat de doeleinden zijn van de verwerking
- waar de gegevens bewaard worden en desgevallend aan wie ze worden overgedragen
- hoe lang de gegevens bewaard worden
- op welke wijze de gegevens en bewaring ervan beveiligd worden

**3. Hoe duidelijk is uw communicatie?**

Op basis van de informatie die u hierboven verzameld heeft, kan u vervolgens controleren of uw privacyverklaring volledig en correct werd opgesteld.

In de verordening wordt veel aandacht geschonken aan de wijze waarop u de betrokkenen informeert over de verwerking van hun persoonsgegevens: niet alleen moet u toelichten welke gegevens u verzamelt en op welke wijze u deze verwerkt, u moet ook de wettelijke grondslag van de verwerking vermelden (heeft u de toestemming van de persoon, is de verwerking noodzakelijk voor het uitoefenen van het contract,..), de termijn gedurende dewelke u de informatie bewaart, op welke wijze u de gegevens beveiligt en aan wie u de gegevens bezorgt.

Daarenboven moet u in uw privacyverklaring opnemen welke rechten de betrokken persoon heeft en op welke wijze hij deze kan uitoefenen, met inbegrip van een klachtenprocedure.

Nieuw is onder andere het recht voor de betrokkene om de toestemming te herroepen en het recht om vergeten te worden.

Tot slot moet uw privacyverklaring in een duidelijke taal zijn opgesteld, en op uw website worden geplaatst in de verschillende talen waarin de website is opgesteld of waarmee gecommuniceerd wordt met de gebruiker of klant.

Zoals eerder gesteld zal uw bestaande privacyverklaring in regel een goede vertrekbasis zijn.

Wij kunnen u altijd helpen deze na te kijken en aan te passen aan de nieuwe regelgeving.

**4. Is de organisatie technisch klaar voor de aanpassingen?**

Nu u weet welke gegevens u verwerkt en welke rechten de betrokkene heeft, moet u nagaan of de wijze waarop u de werking van uw onderneming organiseert, hieraan tegemoet komt.

Zo kan u enkel persoonsgegevens verzamelen in bepaalde omstandigheden: omdat dit noodzakelijk is voor de uitoefening van de overeenkomst met de betrokkene, omwille van een wettelijke verplichting die op u rust of vanwege een gerechtvaardigd belang.

Indien aan geen van deze voorwaarden is voldaan, kan u enkel gegevens verwerken wanneer u de toestemming heeft van de betrokkene.

Wanneer u met andere woorden nieuwsbrieven verstuurt aan uw klanten, gegevens verzamelt voor direct marketing, om interne analyses te maken,… moet u steeds de toestemming verkregen hebben van uw klant: zorg bv dat de betrokkene een vakje kan aanvinken op de website of neem bepalingen op in de contracten die u afsluit.

Hetzelfde geldt voor uw personeelsbeleid: indien u andere dan de meest noodzakelijke persoonsgegevens verzamelt, moet u hiervoor de toestemming hebben: neem dit op in het arbeidsreglement, de ICT policy,…

Wees bovendien extra aandachtig wanneer het risico bestaat dat kinderen jonger dan 16 jaar persoonsgegevens zouden verstrekken: deze kan je immers enkel opvragen en verwerken mits toestemming van ouder of voogd.

In geval van controle of een inbreuk, zal u steeds de toestemming moeten aantonen.

Anderzijds heeft de betrokkene het recht om te vragen zijn persoonsgegevens aan te passen, te verwijderen of om de overdracht van zijn gegevens in een leesbare vorm te vragen: zorg ervoor dat uw informatica systeem deze mogelijkheid voorziet.

Tot slot, wanneer u zelf gegevens verwerkt voor een derde of wanneer een derde gegevens verwerkt voor u, moet er steeds een duidelijke overeenkomst afgesloten worden waarin de wederzijdse verplichtingen inzake de gegevensbescherming worden omschreven.

**5. Wat met datalekken?**

Waar onder de huidige regelgeving een voorafgaande aangifte moet gebeuren in geval van gegevensverwerking, is deze nu vervangen door het register.

Datalekken moeten evenwel steeds gerapporteerd worden binnen de 72 uur.

Ook is het van belang een policy op te stellen waarin omschreven wordt op welke wijze datalekken vermeden worden en wat er moet gebeuren ingeval een datalek zich voordoet.

Hoewel de verplichting dergelijke procedures op te stellen voornamelijk bestaat voor grote bedrijven en ondernemingen die gevoelige gegevens verwerken, raden wij aan een dergelijke policy op te stellen.

Deze kan al bestaan uit een omschrijving van de stappen die u als onderneming onderneemt om de gegevens te beschermen vb, gebruik van login en paswoord, beperkte toegang tot bepaalde (personeels) gegevens, antivirusbescherming die u hanteert,…

Zoals gezegd legt de verordening de nadruk op de verantwoordingsplicht van de verwerker of de verwerkingsverantwoordelijke: in geval van controle of inbreuk zal u moeten aantonen dat u de toestemming van de betrokkene heeft verkregen, een register heeft opgesteld (of indien u dit niet gedaan heeft: dat dit niet noodzakelijk was), het nodige gedaan heeft om de gegevens te beschermen,.. het opstellen van policies zal hierbij helpen en zal het risico op effectieve sancties of boetes verminderen.

**6. Hoe zit dit met de Data Protection Officer: nodig of niet?**

De data protection officer is ongetwijfeld een van de meest besproken functies de afgelopen maanden, maar is deze noodzakelijk of niet?

Voor bedrijven wiens hoofdactiviteit bestaat uit of die hoofdzakelijk bezig zijn met het verwerken van persoonsgegevens is dit noodzakelijk.

De meeste ondernemingen zullen dus geen functionaris voor gegevensbescherming of DPO moeten aanduiden.

Maar ook hierover moet de Privacycommissie nog verder standpunt innemen, dus dit zal nog verduidelijkt worden in de komende maanden.

***Als u in antwoord op deze 6 vragen de nodige aanpassing in de organisatie van uw onderneming doorvoert, bent u in grote lijnen klaar voor de inwerkingtreding van de verordening.***

***Bedrijven die op grote schaal gegevens verwerken, zullen bijkomende maatregelen moeten treffen***

***Indien u specifieke vragen heeft over de werking van uw onderneming en de toepassing van de GDPR, aarzel dan zeker niet contact met ons op te nemen zodat wij u bij dit proces kunnen begeleiden***.