Wat zijn de algemene verplichtingen om persoonsgegevens te beschermen?

Administratieve verplichtingen

01 Een intern verwerkingsregister bijhouden

Een verwerkingsregister brengt de gegevensstromen binnen de onderneming in kaart. Het register moet schriftelijk (lees: digitaal) worden bijgehouden. De toezichthoudende autoriteit beveelt aan dat iedereen, ook KMO's, een register opmaakt.

02 Een gegevensbeschermingseffectbeoordeling uitvoeren

Een onderneming moet voldoende beveiligingsmaatregelen nemen om bijvoorbeeld een scenario van hacking of diefstal te vermijden (gevoelige persoonsgegevens) zodat deze gegevens niet in handen komen van derden. Een onderneming moet om die reden een goede inschatting maken van de gevolgen dat dergelijk verlies van gegevens met zich kan meebrengen.

Technische verplichtingen

01 Gegevensbescherming door ontwerp ('by design')

Stel dat u een start-up bent, is het belangrijk dat je bij de opbouw van uw website/webshop en ICT systemen zoveel als mogelijk rekening houdt met de privacy van uw klant door het treffen van de nodige veiligheidsmaatregelen. Zorg er onder andere voor dat gegevens niet zichtbaar zijn, geanonimiseerd zijn en dat er slechts minimaal gegevens worden verwerkt (cookiebeleid, privacyverklaring).

02 Gegevensbescherming door standaardinstellingen ('by default')

De verwerkingsverantwoordelijke moet de passende beveiligingsmaatregelen treffen om ervoor te zorgen dat gegevensbescherming de standaardinstelling is. Van zodra u als onderneming een dienst of product aanbiedt, moet u er dus voor zorgen dat dit een hoge mate van privacybescherming heeft. Voorbeeld: opt-in; men dient steeds actief de toestemming te vragen van de klant. Een vakje mag niet vooraf standaard staan aangevinkt.

03 Beveiliging

Als onderneming dient men passende technische en organisatorische maatregelen te nemen om het beveiligingsniveau binnen de onderneming te waarborgen zodat hacking, verlies van gegevens, inbraak etc. wordt vermeden. Voorbeeld van een technische maatregel: anonimiseren en versleutelen van persoonsgegevens. Voorbeeld van een organisatorische maatregel: een onderneming die beschikt over een datalekkenbeleid.

04 Melding van een inbreuk aan de autoriteit

Indien er een datalek plaatsvindt binnen de onderneming dan dient men dit te melden aan de toezichthoudende autoriteiten (de gegevensbeschermingsautoriteit en de Vlaamse Toezicht commissie), behalve als er geen impact is op de bescherming van de persoonsgegevens van de klant.

05 Melding van een inbreuk aan de betrokkene

Bij een hoog risico, wordt er ook melding gemaakt aan de klant zelf. Voorbeeld: in het geval één of meerdere computers binnen de organisatie worden gehackt en de fraudeurs op deze manier beschikken over de interne klantenlijsten met diverse - gevoelige - persoonsgegevens.

Organisatorische verplichtingen

01 Een functionaris voor gegevensbescherming (FG) aanstellen

Wanneer de onderneming hoofdzakelijk belast wordt met grootschalige verwerkingen (van gevoelige persoonsgegevens) dan moet er verplicht een FG worden aangesteld. Een FG handelt volledig onafhankelijk.

02 Een verwerkingsovereenkomst afsluiten met een verwerker

In de relatie tussen een verwerkingsverantwoordelijke (vb. de zaakvoerder van een onderneming) en een verwerker (vb. een leverancier van software) moet er een verwerkersovereenkomst worden afgesloten volgens strikte voorschriften. Deze voorschriften houden onder andere in dat de verwerker voldoende beveiligingsmaatregelen moet nemen om de gegevens te beschermen.

mint ADVOCATEN

09 391 79 18

karel@mintadvocaten.be

/company/mint-advocaten

/mintadvocaten