UNIZO SNELWIJZER

GDPR: de nieuwe Europese privacyregels

In deze wereld van digitalisering worden persoonlijke gegevens een kostbaar goed. Voor veel ondernemingen lijkt dat op het eerste gezicht een ver-van-mijn-bedshow. Maar niets is minder waar! Want wist u dat... ook uw onderneming persoonlijke gegevens gebruikt? Elke onderneming, groot én klein, gebruikt en bewaart vandaag de dag persoonsgegevens. En wist u dat er in mei 2018 nieuwe Europese privacyregels aankomen over hoe u met die gegevens mag omgaan? Hoog tijd dus om u een helder overzicht te geven van die GDPR en haar mogelijke impact op uw onderneming.

In deze snelwijzer:

UNIZO ONDERNEMERSLIJN

0800 20 750

ondernemerslijn@unizo.be

Wat is GDPR?

In mei 2018 treden de nieuwe Europese privacyregels in werking. Het gaat om de zgn. **General Data Protection Regulation**, afgekort 'GDPR'. De GDPR vervangt de nationale privacywetgeving van alle Europese lidstaten. De meeste nationale wetgevingen dateren uit de vroege jaren negentig en zijn dus al lang niet meer aangepast aan de digitale realiteit van de eenentwintigste eeuw. Deze Europese verordening zal de Privacy Commissie toelaten controles uit te voeren en ondernemingen te beboeten die niet in orde zijn. Reden te meer om als onderneming de privacyregels te respecteren.

Geldt de GDPR ook voor u als zelfstandige of KMO?

De verordening geldt voor iedereen die persoonsgegevens bijhoudt of verwerkt. Elke onderneming die een database heeft met klantengegevens, prospects, personeelsgegevens, gegevens van toeleveranciers, ... is verplicht om zich in regel te stellen.

De GDPR raakt verschillende sectoren; een bouwbedrijf houdt het e-mailverkeer en financiële gegevens bij van zijn leveranciers, een advocaat of een notaris archiveert (gevoelige) informatie van zijn cliënten, winkeliers verwerken informatie op basis van klantenkaarten, marketingbedrijven analyseren koopgedrag

UNIZO SNELWIJZER

op allerhande manieren, ondernemingen in de zorgsector houden gevoelige informatie van klanten, enz.

Het komt er met andere woorden op neer dat praktisch élke onderneming zich in regel moet stellen tegen mei 2018. De verordening maakt globaal geen onderscheid tussen kleine en grote bedrijven, met een kleine nuance voor ondernemingen die big data verwerken als 'core business' (direct marketing, profiling, ...).

Waarmee moet u rekening houden als u persoonsgegevens bijhoudt?

Een **eerste reeks** regels bepaalt hoe u persoonsgegevens mag verzamelen. Veel van die regels bestonden al, maar worden vanaf 2018 duidelijk veel strenger. Het gaat o.a. over volgende zaken:

- ✔ Wanneer een 'opt-in' nodig is (de betrokkene moet uitdrukkelijk instemmen).
- ✔ Hoe minderjarigen beschermd worden.
- ✔ Hoe persoonsgegevens doorgegeven mogen worden aan derden.
- ✔ Regels rond profiling van klanten/prospects (dit is elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij bepaalde aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen).

Welke acties moet u ondernemen binnen uw onderneming?

Een **tweede reeks** regels is écht nieuw. Die gaan over de interne organisatie binnen uw onderneming. Het gaat o.a. om volgende verplichtingen:

- ✔ **Meldplicht bij datalekken**
  Als gegevens verloren gaan of gestolen worden, moet u de overheid én de betrokken klanten binnen de 72 uur verwittigen.

- ✔ **Register voor verwerkingsactiviteiten**
  Als u persoonsgegevens verwerkt, moet u een register bijhouden. Het komt erop neer dat u een aantal gegevens (verwerkingsdoeleinden, termijn waarbinnen gegevens worden gewist, categorieën van persoonsgegevens, categorieën van ontvangers, beveiligingsmaatregelen, ...) zal moeten bijhouden in een Excelbestand.

- ✔ **Data Protection Officer (DPO)**
  Een DPO is een soort preventieadviseur voor privacy die in bepaalde ondernemingen verplicht wordt (bv. in het geval direct marketing of profiling uw core business is). Dat kan zowel een werknemer als een externe consultant zijn die enkele uren per week of per maand beschikbaar is.

- ✔ **Data Protection Impact Assessment (DPIA)**
  Dit is een soort veiligheidsaudit waarin u moet onderzoeken hoe u met data omgaat en welke risico's op verlies of diefstal van data u loopt. Op basis daarvan moet u dan een actieplan opzetten om die risico's weg te nemen. Deze verplichting is voornamelijk van toepassing op ondernemingen die op grote schaal aan profiling en direct marketing doen.

Welke rechten hebben uw klanten en andere betrokkenen?

Een **derde reeks** regels heeft betrekking op de rechten van betrokkenen waar u als onderneming ook rekening moet mee houden. De GDPR voorziet namelijk meer rechten voor betrokkenen dan voorheen. Ook hier bouwt de GDPR grotendeels verder op wat er bestond, maar worden de rechten ook uitgebreid (*) of zijn ze volledig nieuw (**):

UNIZO SNELWIJZER

✔ **Recht op informatie**
U mag persoonsgegevens niet verwerken zonder medeweten van uw klant. In de wet is bepaald welke gegevens aan uw klant moeten worden meegedeeld. Deze verplichting geldt ongeacht of de gegevens bij de klant zelf of onrechtstreeks zijn verkregen.

✔ **Recht op verwijdering**
In een aantal specifieke gevallen kan de persoon van wie u gegevens bijhoudt, vragen om 'vergeten te worden' en te worden verwijderd uit uw database. U kan de vraag tot verwijdering ook weigeren in een aantal gevallen.

✔ **Recht op correctie**
De persoon van wie u gegevens bijhoudt, heeft het recht om onjuiste of onvolledige persoonsgegevens te verbeteren. U moet binnen de maand reageren (verlengbaar met 2 maanden). U moet ook derden aan wie deze gegevens werden bezorgd, hierover informeren en aan de betrokkene meedelen aan welke derden de persoonsgegevens werden bezorgd.

✔ **Recht van verzet**
De persoon van wie u gegevens bijhoudt, heeft het recht zich te verzetten tegen de verwerking van zijn gegevens op basis van ernstige en gerechtvaardigde redenen (tenzij wettelijk bepaald of wanneer noodzakelijk voor uitvoeren van een overeenkomst). Wanneer gegevens worden verzameld met het oog op direct marketing, dan kan de betrokken persoon zich kosteloos en zonder verantwoording verzetten tegen de verwerking van zijn gegevens. U moet de betrokken persoon in elk geval informeren over zijn recht op verzet en het uitdrukkelijk vermelden in de privacy policy.

✔ **Recht van inzage***
De persoon van wie u gegevens bijhoudt, heeft het recht om bepaalde gegevens in te kijken en bijkomende informatie te ontvangen over heel wat zaken. U moet ook een gratis kopie verstrekken van de verwerkte persoonsgegevens binnen de maand (verlengbaar met 2 maanden).

✔ **Geautomatiseerde besluitvorming en profiling***
Elke persoon van wie u gegevens bijhoudt, heeft het recht om niet te worden onderworpen aan een volledig geautomatiseerde besluitvorming. Het recht geldt niet wanneer 1) de besluitvorming nodig is om een overeenkomst te sluiten of uit te voeren; 2) wettelijk is toegestaan; 3) gebaseerd is op uitdrukkelijke toestemming.

✔ **Recht op overdraagbaarheid van gegevens****
De persoon van wie u gegevens bijhoudt, heeft het recht om persoonsgegevens die hij heeft verstrekt, te laten overdragen aan een andere verwerker. De gegevens moeten gratis worden overgedragen, binnen een tijdspanne van een maand (verlengbaar met 2 maanden), in een gestructureerde gangbare en leesbare vorm. Dit kan enkel voor gegevens die de betrokken persoon heeft verstrekt op basis van toestemming of overeenkomst.

UNIZO SNELWIJZER

UNIZO-expert Anna Craps:
Hoe gaat u nu best tewerk?

✔ **Stap 1: denk na over uw privacybeleid**
Uw privacy policy wordt de komende jaren steeds belangrijker. U zal steeds vaker van klanten en toeleveranciers te horen krijgen dat u moet kunnen aantonen dat u 'privacy compliant' bent. Een van de verplichtingen onder de nieuwe verordening is immers om enkel te werken met 'veilige' bedrijven en om altijd en overal geschreven contracten met de nodige garanties te voorzien.

✔ **Stap 2: wacht niet te lang**
Daarnaast is het belangrijk om te weten dat 25 mei 2018 een einddatum is, zonder uitzondering. Vanaf die datum kan u boetes oplopen (tot 20 miljoen of 4% van uw wereldwijde omzet).

✔ **Stap 3: licht uw onderneming door op vlak van gebruik van data en persoonlijke gegevens**
Wat er verder precies nodig is, zal verschillen van bedrijf tot bedrijf. Allereerst zal u in kaart moeten brengen welke data worden gebruikt binnen uw onderneming, waar die vandaan komt, wie er toegang toe heeft, waarom u die bijhoudt, welke onderaannemers (bv. online marketing bedrijf) die gegevens in handen krijgen, etc. We raden u aan om uw bevindingen goed te documenteren en bij te houden; enerzijds voor uzelf om meer zicht te krijgen op uw onderneming, en anderzijds als bewijs dat u de oefening heeft gemaakt.

✔ **Stap 4: doe de nodige aanpassingen**
Op basis van deze analyse kan u dan aan de slag gaan met het doorvoeren van de nodige aanpassingen op **drie niveaus**:

1. Bijkomende technische beveiliging waar nodig;
2. Aanpassen van processen binnen uw bedrijf;
3. Aanpassen van uw contracten met leveranciers, arbeidsovereenkomsten, arbeidsreglementen, privacy policy, 'bring your own device policies', etc.

De mate waarin u aanpassingen moet doen, zal afhangen van meerdere factoren (aard, grootte, complexiteit, … van uw onderneming). In ieder geval raden we u aan om dit tijdig te bekijken en u eventueel te laten bijstaan door een gespecialiseerd advocatenkantoor en/of IT consultant.

Deze bijdrage kwam tot stand met medewerking van Advocatenkantoor Sirius Legal (www.siriuslegal.be).