De GDPR in 10 stappen

Stap 1- Breng in kaart welke gegevens u verwerkt

De GDPR in 10 Stappen

Stap 1 – Breng in kaart welke gegevens u verwerkt

Inleiding

Elke onderneming houdt een massa gegevens bij, of het nu gaat om een eenmanszaak of een multinational. En de kans is groot dat maar weinig ondernemingen echt weten welke gegevens ze allemaal juist bijhouden. Om de GDPR in uw onderneming te implementeren, begint u dan ook best bij het begin: het in kaart brengen van de gegevens die u verwerkt. De kans is groot dat u daarbij zal vaststellen dat u meer gegevens verwerkt dan u misschien denkt. Maar daarvoor dient net deze oefening: we begeleiden u stap per stap, en de eerste stap is weten wát we juist verzamelen.

Wat is juist een 'persoonsgegeven'?

U zal misschien al gemerkt hebben dat de GDPR niet op alle gegevens van toepassing is, maar enkel op persoonsgegevens. Volgens de GDPR is een persoonsgegeven elk gegeven aan de hand waarvan een natuurlijk persoon kan worden geïdentificeerd.

Uit die definitie kunnen we twee zaken afleiden:

1) **Enkel gegevens die het mogelijk maken om een *natuurlijke persoon* te identificeren zijn relevant.**
   Gegevens die (enkel) een rechtspersoon identificeren vallen niet onder de GDPR. Zo zal uit onpersoonlijke mailadressen zoals info@unizo.be geen natuurlijke persoon kunnen worden geïdentificeerd. Die gegevens vallen dus niet onder de GDPR. Uit het mailadres jan.janssens@unizo.be kan dan weer wel een natuurlijke persoon worden geïdentificeerd, waardoor dat gegeven wél een 'persoonsgegeven' is. Op dezelfde manier is 'bvba De Blauwe Lotus' geen persoonsgegeven, maar de naam 'bvba Jan Janssens' wel.
2) ***Elk* gegeven aan de hand waarvan een natuurlijk persoon kan worden geïdentificeerd, is een persoonsgegeven.**
   Het is dus veel ruimer dan enkel de naam, het telefoonnummer of het mailadres. Ook een IP-adres, een nummerplaat, een rijksregisternummer, het ondernemingsnummer van een éénmanszaak, een bankrekeningnummer van een natuurlijke persoon, … zijn allemaal persoonsgegevens en moeten dus in kaart gebracht worden.

Welke gegevens verwerkt u?

U kan natuurlijk al uw Excel – files met adreslijsten gaan bekijken, of uw mailbox in Outlook om te weten welke gegevens u juist bewaart, maar de kans is groot dat u op die manier niet al uw gegevens in kaart zal brengen.

We raden u daarom om een aantal stappen te volgen:

A. Bepaal voor welke gegevens u 'verwerkingsverantwoordelijke' bent

Persoonsgegevens kunnen verwerkt worden in twee hoedanigheden: als verwerkingsverantwoordelijke of als verwerker.

- De verwerkingsverantwoordelijke is degene die zelf het doel van de verwerking en de middelen voor de verwerking bepaalt. Anders gezegd: de verwerkingsverantwoordelijke bepaalt waarom gegevens moeten worden verwerkt, welke gegevens moeten worden verwerkt, en hoe zij worden verwerkt. Nog anders gezegd: u bent verwerkingsverantwoordelijke als u gegevens verzamelt en verwerkt voor uzelf, en daarbij ook bepaalt hoe u die verwerking doet. Zo zal u als onderneming zelf bepalen welke gegevens u wil verzamelen van uw klanten, voor welke doeleinden, en hoe u die gegevens verwerkt. Ten aanzien van die gegevens bent u dus 'verwerkingsverantwoordelijke'.
- Een verwerker is degene die *ten behoeve van* een verwerkingsverantwoordelijke gegevens verwerkt. Hij verwerkt dus de gegevens niet voor zichzelf, maar voor iemand anders. Typisch voorbeeld is een postbedrijf: zij verwerken adressen van natuurlijke personen om hen post te bezorgen, maar niet voor zichzelf, wel voor een opdrachtgever. Een ander voorbeeld is Outlook: het adressenbestand dat u in Outlook bewaart, zijn persoonsgegevens die Outlook verwerkt. Maar Outlook mag die personen niet zelf gaan contacteren: ze mogen die gegevens enkel voor u verwerken, zodat u hen binnen Outlook mails kan toezenden. Andere voorbeelden zijn sociale secretariaten, IT-bedrijven die uw software of servers onderhouden, boekhoudsoftware, mailingsoftware, pakjesdiensten, mailinghuizen, … .

U zal in de eerste plaats een verwerkingsverantwoordelijke zijn. Indien u toch voor bepaalde activiteiten als 'verwerker' zou worden beschouwd, moet u voor die activiteiten dit stappenplan eveneens doorlopen.

B. Ga na voor welke doeleinden u gegevens verwerkt

Gegevens worden niet zomaar verwerkt, maar steeds om een bepaald doel te realiseren. U verwerkt gegevens van klanten om producten of diensten te kunnen verkopen. Gegevens van personeel houdt u daarentegen bij om hen loon te kunnen uitbetalen. U zal merken dat we met doeleinde dus niet bedoelen in welke systemen u de gegevens bijhoudt. Met 'doeleinde' wordt eerder bedoeld: voor welke reden verwerkt u die gegevens?

In het kader van de GDPR is het heel belangrijk dat u goed nagaat voor welke doeleinden u juist gegevens verwerkt. Dit is één van de belangrijkste stappen binnen de GDPR. De doeleinden die u kiest, zullen immers de grondslag vormen voor alle verdere stappen in de implementatie van de GDPR en bepalen wat u met uw gegevens mag doen, hoelang u ze mag bijhouden, … .

In onze sector zijn de volgende doelstellingen relevant, afhankelijk van de vraag of er personeel in dienst is en/of gebruik wordt gemaakt van camerabewaking:

1. Klantenbeheer
2. Prospectenbeheer (of Direct Marketing)
3. Leveranciersbeheer
4. Boekhouding
5. Communicatie/Public Relations
6. Track & trace
7. Indien van toepassing: personeelsbeheer
8. Indien van toepassing: camerabewaking

Deze doeleinden zijn niet de enige mogelijke doeleinden. Het kan uiteraard zijn dat u binnen uw onderneming gegevens verwerkt voor andere doeleinden (bijvoorbeeld bezoekersregistratie of surfgedrag op de website), die u dan gewoon aan de lijst van doeleinden dient toe te voegen.

TO DO

1) Breng goed in kaart voor welke doeleinden u juist gegevens verwerkt
2) Breng vervolgens *voor elk doeleinde afzonderlijk* in kaart welke gegevens u binnen dat doeleinde verwerkt (zie hieronder).

C. Welke soorten gegevens verwerkt u?

TIP

Het is niet nodig om in detail te beschrijven welke gegevens u verwerkt. Het volstaat om te werken met 'soorten' gegevens. Zo is het niet noodzakelijk om te zeggen 'ik verzamel voornaam, achternaam, postadres, mailadres, telefoonnummer, …', maar volstaat het om te zeggen ' ik verzamel identificatiegegevens'

Wanneer u persoonsgegevens verwerkt, moet u er rekening mee houden dat bepaalde gegevens door de betrokkene als 'gevoelig' kunnen worden ervaren. Dat noemt met **feitelijk gevoelige** gegevens. Typisch voorbeeld is het loon van een werknemer. Binnen die feitelijk gevoelige gegevens zijn er in het bijzonder ook de gegevens van kwetsbare groepen, zoals werknemers, kwetsbare segmenten van de bevolking (zoals geesteszieken, asielzoekers, bejaarden, patiënten, kinderen), … Als u dus gegevens verwerkt van dergelijke kwetsbare groepen, moet u die sowieso beschouwen als een gevoelig gegeven. Daarnaast zal u moeten proberen in te schatten welke gegevens als gevoelig kunnen worden ervaren door de betrokkenen. Het is belangrijk dat u deze oefening doet, want in de volgende stappen zullen we zien dat deze gevoelige gegevens extra waakzaamheid vragen. Het monitoren van locaties via Track & Trace -systemen kan in hij bijzonder als 'gevoelig' worden ervaren.

Daarnaast moet u ook rekening houden met '**bijzondere categorieën van persoonsgegevens**'. Die zijn wel duidelijk bepaald in de GDPR. Het gaat om :

a. Gegevens met betrekking tot ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, seksueel gedrag of seksuele geaardheid,
b. Gezondheidsgegevens, genetische gegevens en biometrische gegevens

Ook deze gegevens moet u goed detecteren, aangezien de GDPR de verwerking van deze gegevens verbiedt, tenzij in heel strikt omschreven gevallen.

Voorbeelden van persoonsgegevens:

- ✓ Persoonlijke identificatiegegevens (naam, adres, telefoon, mail)
- ✓ Rijksregisternummer/identificatienummer van de sociale zekerheid
- ✓ Elektronische identificatiegegevens (IP-adres, Cookies)
- ✓ Financiële identificatiegegevens (bankrekeningnummer)
- ✓ Financiële transacties (betalingen die de persoon heeft gedaan of nog moet doen)
- ✓ Beroepsactiviteit (werkgever, titel, …)
- ✓ Persoonlijke bijzonderheden (leeftijd, geslacht, geboortedatum, geboorteplaats, burgerlijke staat, nationaliteit, …)
- ✓ Samenstelling van het gezin (naam van de partner, aantal, kinderen, …)
- ✓ Vrijetijdsbesteding en interesses (hobby's, sport, andere interesses)
- ✓ Lidmaatschap van een vakvereniging
- ✓ Lidmaatschap van een politieke partij
- ✓ Lidmaatschap van een andere vereniging
- ✓ Opleiding en vorming
- ✓ Beeldopnamen
- ✓ Sociale netwerkaccounts (gegevens m.b.t. facebook, twitter, linked-in, …)
- ✓ …
- ✓ Gegevens van kwetsbare groepen?
- ✓ Bijzondere categorieën van persoonsgegevens (ras, gezondheid, biometrische /genetische gegevens, seksuele geaardheid, …)?

D. Over wie houdt u gegevens bij?

De ‘betrokkenen’ zijn de natuurlijke personen van en over wie er persoonsgegevens worden verwerkt. Zij moeten niet bij naam worden aangeduid. Het volstaat ze via algemene categorieën te omschrijven, zoals ‘klanten’, ‘leveranciers’, ‘prospecten’, ‘werknemers’, ‘sollicitanten’, … .

Hoe heeft u die gegevens verkregen?

Ga tot slot zeker ook na op welke manier u die gegevens heeft verkregen. Heeft de klant bijvoorbeeld de gegevens zelf gegeven? Heeft u adressenbestanden aangekocht of gezocht op internet? Houdt u gegevens bij van mensen die uw website bezoeken?

Als u dit alles in kaart heeft gebracht, bent u klaar voor stap 2.

Checklist

- ❑ Ik heb een overzicht van de doeleinden waarvoor ik gegevens verwerk.
- ❑ Voor elk doeleinde heb ik een overzicht van de categorieën van persoonsgegevens die ik binnen dat doeleinde verwerk en van de categorieën van personen op wie die gegevens betrekking hebben.
- ❑ Ik heb nagekeken of ik gevoelige gegevens of bijzondere categorieën van gegevens verwerk.
- ❑ Ik heb nagekeken op welke manier ik momenteel gegevens verkrijg.