GDPR COMPLIANCE GUIDE

# Gegevensbescherming is niet optioneel, Het is wettelijk verplicht.

De Algemene Verordening Gegevensbescherming (AVG) is de Europese norm voor dataprivacy. De verordening is van toepassing op elke organisatie die persoonsgegevens van mensen in de EU verzamelt, opslaat of verwerkt, ongeacht waar de organisatie zelf is gevestigd.

Voor bedrijven die in Europa actief zijn, is naleving niet optioneel; het is een wettelijke verplichting. Het niet naleven van de regels kan leiden tot boetes tot € 20 miljoen of 4% van de wereldwijde jaaromzet, afhankelijk van welk bedrag hoger is.
Maar de AVG draait niet alleen om het voorkomen van sancties. Het gaat om het opbouwen van vertrouwen dat zorgt voor langdurige klantrelaties. Wanneer mensen weten dat hun gegevens bij jou veilig zijn, zijn ze sneller bereid deze te delen én blijven ze sneller klant.

SuperOffice helpt Europese bedrijven al decennialang bij het opbouwen van betrouwbare klantrelaties. Wij begrijpen het regellandschap, de lokale verwachtingen en hoe naleving er in de praktijk uitziet – en niet alleen op papier.

**€20M**

Maximale boete voor non-compliance (of 4% van de wereldwijde ARR, afhankelijk van welk bedrag hoger is)

**2018**

Het jaar waarin de AVG in de hele Europese Unie van kracht werd

**363**

Aantal datalekken dat dagelijks wordt gemeld bij Europese toezichthouders

## Wat de AVG verwacht van jouw bedrijf

- **Zorg dat je grip hebt op je data**
  Breng elk type persoonsgegevens dat je organisatie verzamelt in kaart en documenteer het doel hiervan.
- **Zorg voor een juiste bescherming**
  Implementeer beveiligingsmaatregelen en beperk de toegang tot medewerkers die dit nodig hebben voor hun functie.
- **Beschik over een rechtmatige grondslag**
  Zorg dat je de wettelijke grondslag achter elk gegevenspunt kunt uitleggen.
- **Rechten naleven**
  Beantwoord verzoeken om inzage, wissing en bezwaar binnen de wettelijke termijnen.

PERSONAL DATA CHECKLIST

# Inzicht in risico. Grip op data. Pak de controle.

- Wettelijke AVG-verplichtingen naleven en hoge boetes voorkomen.
- Klantvertrouwen opbouwen. Mensen delen meer als ze zich veilig voelen.
- Zorg dat je klaar bent voor een audit met een volledig, gedocumenteerd overzicht van uw data.

## 13 vragen om de controle over je data te pakken

### Een praktische manier om te begrijpen welke data je hebt en waarom

### De gegevens die worden verzameld

1. **Welke persoonsgegevens worden er verzameld?**
   Namen, e-mailadressen, telefoonnummers, geboortedatum, persoonlijke ID-nummers. Maak een lijst van alles waarmee een persoon kan worden geïdentificeerd.

2. **Waarom verzamel je deze gegevens?**
   Je hebt voor elk gegeven een duidelijke reden nodig, bijvoorbeeld voor een geboortedatum. Als je niet kunt uitleggen waarom je het nodig hebt, zou je het waarschijnlijk niet moeten hebben.

3. **Wat geeft je het wettelijke recht om het te verzamelen?**
   Je hebt voor elk gegeven een wettelijke reden nodig. Toestemming, overeenkomst en gerechtvaardigd belang komen het meest voor. Kies degene die van toepassing is.

4. **Waar komt de data vandaan?**
   Webformulieren, visitekaartjes, systeemintegraties of direct contact? Ken je bronnen.

5. **Vereisen bepaalde gegevens extra bescherming?**
   Gaat het om gevoelige informatie? Salaris, gezondheidsgegevens en persoonlijke ID-nummers vereisen extra bescherming.

### Hoe bewaar je het?

6. **Hoe lang bewaar je het?**
   Bewaar data niet langer dan nodig is. Stel voor elk type een duidelijke termijn in.

7. **Wie heeft er toegang toe?**
   Uitsluitend medewerkers die dit noodzakelijk hebben voor hun functie. Breng de rollen in kaart (salarisadministratie, HR, sales) en zorg dat de toegang hiertoe strikt beperkt blijft.

8

### Vindt er datadoorgifte buiten de EU plaats?

Houd persoonsgegevens waar mogelijk binnen de EU. Gaan ze toch naar buiten de EU? Leg dan schriftelijk vast waarheen en waarom.

9

### In welk systeem worden de gegevens opgeslagen?

SuperOffice CRM, salarissysteem, HR-platform? Breng ze in kaart en vink aan welke cloud-based zijn.

## Toestemming en het delen van gegevens

10

### Is er duidelijke toestemming?

Heeft de persoon er actief mee ingestemd om zijn of haar gegevens met je te delen? Dit is vooral belangrijk bij mensen met wie je geen actieve klantrelatie hebt.

11

### Is de persoon geïnformeerd?

Weten ze dat je hun gegevens hebt? Dit is meestal geregeld in je contract, onboarding of privacyverklaring.

12

### Wordt het gedeeld met derden?

Als je gegevens met anderen deelt, wees dan duidelijk over met wie en waarom. Zorg ervoor dat dit in je privacyverklaring staat.

## Security

13

### Hoe is het beveiligd?

Welke beveiligingsmaatregelen heb je getroffen? Dit is vooral belangrijk bij het verwerken van gevoelige gegevens.



*Alleen ter informatie. Raadpleeg een juridisch specialist voor advies op maat voor jouw situatie*