

# Algemene Verordening voor Gegevensbescherming (AVG)

## TO DO-LIJST

### 1. Verwerking van persoonsgegevens

- 1.1. Maak een **Verwerkingsregister** (een lijst) van alle plekken in je bedrijf waar je persoonsgegevens noteert ('verwerkt').

Noteer per verwerking\*:

- waar je gegevens noteert
- welke gegevens je noteert (naam, adres, gezondheidsgegevens\*\*)
- met welk doel je de gegevens noteert
- maak je gebruik van een externe partij die voor jou persoonsgegevens noteert? Ja → zie 1.2.
- Wat is de bewaartermijn van de gegevens?
- Welke beveiligingsmaatregelen heb je genomen: organisatorisch + IT?

\* Verwerken van persoonsgegevens gebeurt zowel digitaal als niet-digitaal + Exporteren van persoonsgegevens (gegevens doorgeven, bijvoorbeeld via een mailbericht) is ook een vorm van verwerking van persoonsgegevens.

\*\*Gezondheidsgegevens vallen onder *bijzondere* persoonsgegevens. Dit mag je alleen bijhouden als het noodzakelijk is voor een goede behandeling/verzorging van de klant én je bent gehouden aan geheimhouding (ambt, beroep of via overeenkomst).

- 1.2. Neem in het verwerkingsregister ook **de verwerkers** op, dat zijn de externe partijen die voor jou met persoonsgegevens werken. (Voorbeelden: de salarisadministratie, de host van je website, telefoondienst, zoals Google, Microsoft of Mailchimp.)

- 1.3. Sluit met de verwerkers een **verwerkingsovereenkomst** af.

*Een format van een verwerkingsovereenkomst staat in de Bibliotheek van de Procesregistratie. Grotere partijen (Google, mailchimp) zullen zelf initiatief nemen.*

### 2. Stel een privacy-reglement op (voor je klanten en personeel).

- 2.1. Zorg ervoor dat je de persoonsgegevens alleen gebruikt voor dingen die in het privacy-reglement staan.
- 2.2. Zorg ervoor dat het reglement goed vindbaar is op je website.
- 2.3. Attendeer een klant op het reglement als je de persoonsgegevens niet via de website verzamelt (bijvoorbeeld bij de bevestiging van een intake).
- 2.4. Geef het reglement aan je personeel + zorg voor een handtekening dat het gelezen is.
- 2.5. Als je cookies gebruikt, informeer de klant daarover op je website.

*Formats van het privacy-reglement en een cookieverklaring staan in de Bibliotheek van de Procesregistratie.*

### 3. Zorg ervoor dat je gebruik maakt van een antivirusprogramma en firewall.

### 4. Direct Marketing (commerciële aanprijzingen van je diensten, via email of sociale media)

- 4.1. Direct marketing mag alleen met expliciete toestemming. Zorg ervoor dat je kunt aantonen dat de mensen op je verzendlijsten expliciet toestemming hebben gegeven.
- 4.2. Zorg ervoor dat mensen zich kunnen uitschrijven voor je nieuwsbrief of reclame-uiting.
- 4.3. Zorg voor een verwerkingsovereenkomst met de externe partij die de direct marketing verstuurt (bv. mailchimp).