# Algemene uitgangspunten AVG

Doel van de AVG is om de privacy van burgers beter te beschermen. In de praktijk is het vooral belangrijk dat je enkel persoonsgegevens verwerkt die je echt nodig hebt (‘dataminimalisatie’), en dat je deze gegevens goed beveiligt.

**Legitieme verwerking**
Volgens de AVG mag je alleen persoonsgegevens verwerken voor een duidelijk omschreven en gerechtvaardigd doel. Je mag dus geen gegevens verzamelen omdat je deze in de toekomst wellicht goed kunt gebruiken. Daarnaast mag je de persoonsgegevens niet zomaar gebruiken voor een ander doel.

**Persoonsgegevens verwijderen**
Zijn persoonsgegevens niet meer relevant voor het doel waarmee je ze verzameld hebt? Dan moet je deze zo snel mogelijk verwijderen. Uiteraard moet ook het verwijderen van de persoonsgegevens op een veilige manier gebeuren.

**Beveiliging**
De gegevens die jij verwerkt, moeten goed beveiligd zijn. Voor een juiste beveiliging kun je denken aan technische maatregelen (bijvoorbeeld het pseudonimiseren van persoonsgegevens of het toepassen van encryptie) en organisatorische maatregelen (bijvoorbeeld: zorgen dat alleen medewerkers die met persoonsgegevens moeten werken, hier toegang tot hebben).

**Verplichtingen**
De AVG kent verschillende plichten voor ondernemers. Bekijk ze hieronder.
Registerplicht
Voortaan moet je als ondernemer alle verwerkingen van persoonsgegevens documenteren in een register. In dit register noteer je onder andere welke soort persoonsgegevens je verwerkt, met welk doel en hoe je de gegevens beveiligt. Je kunt het register maken met behulp van bepaalde software. Een document in Word of Excel voldoet echter ook. Let op: In dit register neem je niet daadwerkelijk persoonsgegevens op. Het doel is enkel om inzicht te creëren in jouw verwerkingsactiviteiten.
Tip: Vaak heb je als ondernemer al veel documentatie, zoals procesbeschrijvingen. Gebruik deze documentatie om na te gaan welke persoonsgegevens je zoal verwerkt.

**Verwerkersovereenkomst**
Mogelijk werk je als ondernemer samen met partijen die in jouw opdracht persoonsgegevens verwerken. Denk bijvoorbeeld aan een

administratiekantoor of softwareleverancier. Deze partijen worden in de Wbp ‘bewerker’ genoemd. In de AVG verandert dit naar ‘verwerker’. De AVG verplicht jou om met iedere verwerker een verwerkersovereenkomst te sluiten. Hierin maak je afspraken over de omgang met persoonsgegevens. Goed om te weten: op internet zijn diverse voorbeelden van verwerkersovereenkomsten te vinden.

Let op: Ben je zelf een verwerker? Ook dan moet je je aan een aantal regels houden. Je mag bijvoorbeeld alleen persoonsgegevens verwerken in opdracht van de verantwoordelijke partij. Ook moet je voldoen aan de registerplicht en mag je niet zomaar sub-verwerkers inschakelen.

**Privacy by design**
De AVG verplicht jou om het uitgangspunt ‘Privacy by design’ te hanteren. Dit houdt in dat je bij de ontwikkeling van producten en diensten voldoende rekening houdt met privacy. Al in de ontwerpfase zorg je ervoor dat je zo min mogelijk inbreuk op de persoonlijke levenssfeer maakt. Maatregelen die je kunt treffen, zijn bijvoorbeeld:
- enkel de noodzakelijke persoonsgegevens verwerken;
- persoonsgegevens pseudonimiseren;
- persoonsgegevens goed beveiligen;
- transparant zijn over de verwerkingen die je gaat toepassen;
- betrokkenen de mogelijkheid geven om zelf controle uit te oefenen op de verwerking.

**Privacy Impact Assessment (PIA)**
Ga je een nieuw project starten, waarbij persoonsgegevens verwerkt worden? Dan is mogelijk een Privacy Impact Assessement (PIA) vereist. Een PIA is een voorafgaand onderzoek, waarbij je in kaart brengt welke privacyrisico’s er spelen en hoe je deze kunt verkleinen.
Een PIA is verplicht voor verwerkingen met een hoog risico voor de privacy van de betrokken personen. Denk aan:
- het verwerken van gevoelige gegevens (bijvoorbeeld gegevens over gezondheid of religie);
- het geautomatiseerd besluiten nemen (bijvoorbeeld het automatisch detecteren van fraude);
- het monitoren van openbare ruimten (bijvoorbeeld met camera’s).

Tip: Weten hoe je zelf een PIA maakt? Bekijk dan de handreiking van NOREA, de beroepsorganisatie van IT-auditors.

**Functionaris voor gegevensbescherming**
Voor sommige ondernemers is het verplicht een functionaris voor gegevensbescherming (FG) aan te stellen. Een FG is een onafhankelijk persoon binnen de organisatie, die toezicht houdt op het naleven van de AVG. Voor jou als ondernemer is een FG enkel verplicht wanneer:

- jij je structureel en op grote schaal bezighoudt met het observeren van mensen;
- jij je voornamelijk bezighoudt met het verwerken van bijzondere persoonsgegevens en/of persoonsgegevens van strafrechtelijke aard.

Uiteraard mag je ook vrijwillig een FG aanstellen. Houd er dan wel rekening mee dat deze persoon dezelfde verantwoordelijkheden en bevoegdheden heeft als een ‘verplicht’ aangestelde FG.

**Privacyverklaring**

Hoogstwaarschijnlijk heb je al een privacyverklaring op je website staan. Om aan de AVG te voldoen, moet je privacyverklaring nog transparanter zijn. Je moet bijvoorbeeld duidelijk toelichten hoe lang je persoonsgegevens bewaart en of je deze gegevens deelt met andere partijen. Daarnaast moet je klanten attenderen op hun rechten (zie ‘Privacyrechten’ verderop in dit artikel) en de mogelijkheid tot het indienen van een klacht bij de Autoriteit Persoonsgegevens.

**Het registreren van datalekken**

Met ingang van de AVG moet je ieder datalek intern documenteren. Dit geldt ook voor datalekken die niet bij de Autoriteit Persoonsgegevens hoeven te worden gemeld.
Tip: Bekijk op de website van ICTRecht welke informatie je per datalek moet registreren.

**Privacyrechten**

De AVG geeft betrokkenen diverse rechten. Als verantwoordelijke voor de verwerking van persoonsgegevens ben je verplicht gehoor te geven aan deze rechten.

- Recht op dataportabiliteit
  Bied jij online diensten aan waarbij gebruikers persoonsgegevens opslaan? Dan moet je hen de mogelijkheid bieden om deze gegevens over te dragen naar een andere leverancier of organisatie.
- Recht op vergetelheid
  Dit houdt in dat je de persoonsgegevens van een betrokkene verwijdert, wanneer deze daarom vraagt. Bekijk op de site van de Autoriteit Persoonsgegevens in welke gevallen je aan dit verzoek moet voldoen.
- Recht op duidelijke informatie
  Je bent verplicht om mensen duidelijk te vertellen wat je met hun gegevens doet. Dit doe je bij voorkeur via je privacyverklaring.
- Recht op inzage
  Betrokkenen hebben het recht om in te zien welke persoonsgegevens jij van ze verwerkt.
- Recht op correctie van de gegevens
  Als persoonsgegevens niet kloppen of niet volledig zijn, hebben betrokkenen het recht om deze te corrigeren.

- Recht op beperking van de gegevensverwerking
  ‘Beperking’ houdt in dat iemand kan vragen om de verwerking van zijn/ haar persoonsgegevens tijdelijk stop te zetten. Bijvoorbeeld omdat de verwerking onrechtmatig is.
- Recht om bezwaar te maken tegen de verwerking
  Het kan zijn dat een betrokkene bezwaar maakt tegen een verwerking van zijn of haar persoonsgegevens. Met zo’n bezwaar moet je instemmen. Tenzij je natuurlijk dwingende gronden voor de verwerking hebt, die zwaarder wegen dan het belang van de betrokkene.
- Recht om niet onderworpen te worden aan een geautomatiseerde besluitvorming
  Neem jij besluiten op basis van automatisch verwerkte gegevens (profilering)? Betrokkenen hebben het recht om jou te vragen opnieuw een besluit te nemen, waarbij de gegevens beoordeeld zijn met een menselijke blik.

Let op: Zorg dat je verzoeken binnen 1 maand afhandelt.