

AVG : Algemene Verordening Gegevensbescherming

Op 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming (AVG) in werking. De AVG is de opvolger van de Wet bescherming persoonsgegevens (Wbp) en is van toepassing op iedereen die met persoonsgegevens werkt. Voor veel ondernemingen geldt dat daarbij onderscheid gemaakt kan worden in twee soorten personen van wie gegevens worden gebruikt. Het betreft personeel van de onderneming en de klanten. Welke gegevens van klanten worden vastgelegd is afhankelijk van de aard van het bedrijf. Naarmate meer en ook bijzondere gegevens vastgelegd worden, gelden strengere voorschriften.

Persoonsgegevens

Alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon gelden als persoonsgegevens. Binnen de persoonsgegevens gelden gradaties. Aan bijzondere persoonsgegevens, zoals medische gegevens, etnische gegevens, seksuele of politieke voorkeuren worden strengere eisen gesteld bij de verwerking dan aan bijvoorbeeld NAW-gegevens.

Verwerking van persoonsgegevens

Verwerking is iedere vorm van verzamelen, vastleggen of gebruiken van persoonsgegevens in een bestand. Verwerking van persoonsgegevens moet rechtmatig zijn. Dat kan op basis van toestemming van de betrokkene of op basis van een wettelijke verplichting. Persoonsgegevens mogen alleen worden gebruikt voor het doel waarvoor zij verzameld zijn c.q. waarvoor de betrokkene toestemming heeft gegeven. Er mogen niet meer gegevens gevraagd of bewaard worden dan nodig is voor het doel. Toestemming moet expliciet worden gegeven, bijvoorbeeld voor het toesturen van nieuwsbrieven of aanbiedingen. Voor het vastleggen van gegevens van personeel gelden wettelijke verplichtingen, zoals het bewaren van een kopie van een identiteitsbewijs.

Bewaren persoonsgegevens

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk. Is het doel waarvoor gegevens zijn verzameld bereikt dan moeten zij vernietigd of teruggegeven worden.

Verwerkersovereenkomst

De AVG schrijft het bestaan van een verwerkersovereenkomst voor tussen de verantwoordelijke voor de verwerking van persoonsgegevens en de derde aan wie de verantwoordelijke de verwerking heeft uitbesteed.

Als deze derde zelf het doel en de middelen van de verwerking vaststelt, is hij geen verwerker maar verwerkingsverantwoordelijke.

Verwerkers die persoonsgegevens verwerken voor een groot aantal verwerkersverantwoordelijken doen er goed aan te werken met één

(model)verwerkersovereenkomst. Waar een verwerker gebruik maakt van de diensten van andere verwerkers is sprake van sub-verwerking.

Sub-verwerking is alleen toegestaan met instemming van de verwerkingsverantwoordelijke.

Ook tussen verwerker en sub-verwerker moet een verwerkersovereenkomst worden gesloten. De voorwaarden in de sub-verwerkersovereenkomst moeten aansluiten bij de verwerkersovereenkomst die de verwerker met de verwerkingsverantwoordelijke heeft gesloten.

Aandachtspunten bij invoering AVG

1. Bewustwording

Zorg ervoor dat de mensen in uw organisatie op de hoogte zijn van de nieuwe privacyregels. Maak een inschatting van de gevolgen van de AVG zijn voor uw bedrijfsvoering en van de aanpassingen die nodig zijn om aan de AVG te voldoen.

2. Rechten van betrokkenen

Onder de AVG hebben mensen van wie u persoonsgegevens verwerkt meer rechten als voorheen. Zorg ervoor dat zij deze rechten goed kunnen uitoefenen.

3. Inventariseer verwerkingen

- Inventariseer welke gegevensverwerkingen u verricht.
- Leg vast welke persoonsgegevens u verwerkt met welk doel, waar deze gegevens vandaan komen en met wie u ze deelt.
- Beoordeel of u zich daarbij beperkt tot het minimum dat nodig is voor het doel.
- Wie heeft binnen uw organisatie toegang tot persoonsgegevens en hoe is de toegang daartoe beveiligd?
- Hoe gaat u om met gegevens die niet meer nodig zijn?
- Worden die vernietigd en is daar beleid voor (Hoe lang worden gegevens bewaard, wanneer worden gegevens vernietigd en wie is daarvoor verantwoordelijk)?
- Leg dit alles vast in een register, of document zoals WORD of EXCEL.

Onder de AVG heeft u een verantwoordingsplicht. U moet kunnen aantonen dat u in overeenstemming met de AVG handelt.

4. Uitgangspunten AVG voor verwerkingsbeleid en -processen

De AVG gaat uit van privacy by design en privacy by default. Dat houdt in dat al bij het ontwerpen van producten en diensten rekening met de bescherming van persoonsgegevens moet worden gehouden. Privacy by default houdt in dat u de nodige maatregelen neemt om ervoor te zorgen dat u als standaard alleen die persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel.

5. Functionaris gegevensbescherming

Sommige organisaties zijn verplicht om een functionaris voor gegevensbescherming (FG) aan te stellen. Wellicht geldt dat voor uw organisatie. Uw organisatie mag vrijwillig een FG aanstellen.

6. Denk aan de meldplicht voor datalekken

De meldplicht datalekken bestond al onder de Wbp. Daar verandert onder de AVG niet veel in. De AVG stelt wel strengere eisen aan de registratie van datalekken. U moet alle datalekken documenteren, zodat de Autoriteit Persoonsgegevens kan controleren of u aan de meldplicht heeft voldaan.

7. Toestemming

De AVG stelt strenge eisen aan toestemming voor verwerking. Evalueer de manier waarop u toestemming vraagt, krijgt en registreert en pas deze zo nodig aan. U moet kunnen aantonen dat u geldige toestemming heeft om persoonsgegevens te verwerken. Het intrekken van toestemming mag niet moeilijker zijn dan het geven daarvan.