

## Wettelijke aspecten

### Algemene Verordening Gegevensbescherming

Voor het verwerken van persoonsgegevens zijn er zes wettelijke grondslagen vastgesteld in artikel 5 AVG. De grondslagen zijn als volgt:

- Rechtmatigheid, behoorlijkheid en transparantie (lid 1 sub a);
- Doelbinding (lid 1 sub b);
- Dataminimalisatie (lid 1 sub c);
- Gegevens moeten juist en actueel zijn (lid 1 sub d);
- Opslagbeperking (lid 1 sub e);
- Integriteit en vertrouwelijkheid (lid 1 sub f).

Artikel 5 lid 2 AVG bepaalt dat de verwerkingsverantwoordelijke zorg draagt om de beginselen na te leven en dit te kunnen aantonen.

Daarnaast moet er door de verwerkingsverantwoordelijke worden overwogen of de verzamelde gegevens relevant zijn voor het verwerkingsdoel. De verwerking van de persoonsgegevens dient volgens artikel 6 AVG te worden gebaseerd op een rechtsgrond.

Die zijn als volgt:

- Toestemming (lid 1 sub a);
- Noodzakelijk voor de overeenkomst (lid 1 sub b);
- Wettelijke verplichting (lid 1 sub c);
- Bescherming van de vitale belangen (lid 1 sub d);
- Uitvoering van overheidstaak of algemeen belang (lid 1 sub e);
- Gerechtvaardigd belang (lid 1 sub f).

*Op welke rechten dient de betrokkene gewezen te worden?*

De betrokkene heeft te allen tijde recht op dat zijn gegevens: gewist, ingezien en gerectificeerd mogen worden, dat zij bewaar mogen maken tegen verwerken, dat eerder gegeven toestemming ingetrokken mag worden en dat klachten over de verwerking kunnen worden ingediend bij de AP.

*Wanneer ben je een verwerkingsverantwoordelijke?*

De AVG maakt onderscheid tussen verwerkingsverantwoordelijken en verwerkers. Bij de verwerking van persoonsgegevens kunnen diverse partijen betrokken zijn. Allereerst is er de organisatie die de persoonsgegevens verwerkt, bekend als de verwerkingsverantwoordelijke volgens artikel 4 AVG. Indien de organisatie gegevens verwerkt namens een opdrachtgever, wordt deze aangeduid als de verwerker.

Een persoon is een verwerkingsverantwoordelijke indien er sprake is van:

1. Feitelijke invloed. De organisatie bepaalt met welk doel de persoonsgegevens worden verwerkt en op welke manier dat gebeurt. De tweede partij moet de instructies opvolgen.

2. Uitdrukkelijke juridische bevoegdheid. In de wet is uitdrukkelijk bepaald welke persoonsgegevens de organisatie mag of moet verwerken;
3. Impliciete bevoegdheid. De wet stelt niet uitdrukkelijk welke persoonsgegevens verwerkt mogen of moeten worden, maar het ligt wel voor de hand dat de organisatie dit moet doen.

Wanneer persoonsgegevens worden verwerkt in opdracht van een andere organisatie en deze persoonsgegevens niet voor eigen doeleinden worden gebruikt, beschouwt artikel 4 lid 8 AVG de verwerkingsverantwoordelijke als verwerker. De verwerkingsverantwoordelijke blijft verantwoordelijk voor de verwerking die aan de verwerker is uitbesteed.

#### *Hoe zit het dan bij doorgifte van persoonsgegevens?*

Een organisatie mag niet zomaar persoonsgegevens doorgeven aan andere partijen. De algemene regel is dat dit alleen mag wanneer dit verenigbaar is met het doel waarvoor de gegevens in eerste instantie verzameld zijn. Persoonsgegevens mogen worden doorgegeven als er aan een van de volgende eisen is voldaan:

- U heeft toestemming voor doorgifte gekregen van de verstrekker van de persoonsgegevens;
- Het doel van de verstrekking moet overeenkomen met het oorspronkelijke doel van de verzameling van de persoonsgegevens.

Om dit te bepalen kunt u zichzelf de volgende vragen stellen:

- Wat is het verband met het oorspronkelijke doel van gegevensverzameling?
- Wat is de verhouding tussen u en de verstrekker van de persoonsgegevens?
- Hoe gevoelig zijn de gegevens?
  - Gaat het om bijzondere gegevens?
  - Gaat het om strafrechtelijke persoonsgegevens
- Wat zijn de gevolgen van de doorgifte van de persoonsgegevens?
- Is versleuteling of pseudonimisering nodig?
- Wat zijn de verwachtingen van de vertrekker van de persoonsgegevens?

Wanneer is vastgesteld dat de gegevens doorgegeven worden doorgegeven, mogen de gegevens worden verwerkt op basis van de oorspronkelijke verwerking. U heeft geen nieuwe grondslag nodig.

In het geval van gegevens delen met derde partijen moeten er passende technische en organisatorische maatregelen worden genomen. Gegevens kunnen gepseudonimiseert worden om minder risicovol te worden overgedragen.

#### **Hoe zit dit dan in de praktijk?**

Uit interviews met experts in de praktijk is gebleken dat door MKB'ers in Nederland weinig tijd wordt besteed aan het opstellen van hun privacyvoorwaarden. Experts stellen dat sinds de aanpassing van de wet in 2018 nog steeds organisatie zijn die niet of niet kloppende privacyvoorwaarden hebben gesteld. Omdat MKB'ers door de AP vrijwel niet worden gecontroleerd wordt de noodzaak er niet van ingezien. De volgende vraag wordt door de experts gesteld: waarom zouden de MKB'ers er tijd en geld in steken om hun privacyvoorwaarden kloppend en transparant op te stellen, als er toch geen consequentie aan zit wanneer zij dit niet hebben gedaan?