

## Procedure verwerkersovereenkomst

Een verwerkersovereenkomst is een overeenkomst waarin partijen afspraken maken over de overdracht van en omgang met persoonsgegevens waarvoor zij verantwoordelijk zijn. De verwerkersovereenkomst dient een los document te zijn, welke als bijlage bij de overeenkomst van opdracht wordt gevoegd.

### Wanneer stel je een verwerkersovereenkomst op?

Indien je persoonsgegevens verwerkt voor en in opdracht van een klant, zijn jij en jouw klant volgens de Algemene Verordening Gegevensbescherming (AVG) verplicht om hiervoor een 'Verwerkersovereenkomst' te sluiten. Jij bent de 'verwerker' en jouw klant is de 'verwerkingsverantwoordelijke'.

Denk hier bijvoorbeeld aan de opdracht of een onderdeel van de opdracht om mailings en nieuwsbrieven te versturen voor de klant.

Maar ook als jij een andere partij opdracht geeft om persoonsgegevens te verwerken waarover jij beschikking hebt en dus verantwoordelijk voor bent, dienen jullie een verwerkersovereenkomst op te stellen. In dit geval ben jij de 'verwerkingsverantwoordelijke' en de andere partij de 'verwerker'.

Denk hierbij aan het gebruik van software waarbij persoonsgegevens in een cloud worden opgeslagen of bij het uitbesteden van de personeels- en salarisadministratie.

### Inhoud verwerkersovereenkomst

In de verwerkersovereenkomst moet op grond van art. 28 van de AVG onder andere worden opgenomen:

1. Welke partijen persoonsgegevens aan elkaar overdragen.
2. Met welk doel partijen persoonsgegevens aan elkaar overdragen, bijvoorbeeld in het kader van de dienstverlening. De verwerker is uitsluitend bevoegd de persoonsgegevens te gebruiken voor dat specifieke doel en niet voor eigen doeleinden.
3. Welke persoonsgegevens de verwerkingsverantwoordelijke aan jou als verwerker verstrekt. Denk hierbij aan de categorieën van betrokkenen en de persoonsgegevens.
4. Afspraken over de bewaartermijn van die persoonsgegevens door de verwerker. Denk hierbij aan de wettelijke verplichting gegevens te bewaren.
5. Afspraken over het eventueel terug leveren van de persoonsgegevens door de verwerker.
6. Welke beveiligingsmaatregelen door de verwerker moeten worden genomen voor het opslaan en verwerken van de persoonsgegevens. Denk hierbij aan pseudonimisering en versleuteling van persoonsgegevens, permanente informatiebeveiliging, herstel van beschikbaarheid en toegang tot de gegevens bij incidenten en regelmatige beveiligingstesten.
7. Welke beveiligingsmaatregelen de verwerkingsverantwoordelijke en de verwerker moeten nemen voor een veilige overdracht van de persoonsgegevens
8. Hoe er met de meldplicht datalekken wordt omgegaan.
9. Hoe er met het uitvoeren van een data protection impact assessment (DPIA)<sup>1</sup> wordt omgegaan.

---

<sup>1</sup> Met een data protection impact assessment (DPIA) worden vooraf privacyrisico's van de gegevensverwerking in kaart gebracht. Ook worden maatregelen beschreven om de risico's te verkleinen. Dit moet doorlopend gemonitord worden.

Een DPIA is alleen verplicht als de gegevensverwerking een hoog privacyrisico oplevert voor de mensen van wie de organisatie gegevens verwerkt. De verwerkingsverantwoordelijke moet zelf de hoogte van het risico beoordelen.

10. Op welke manier de verwerkingsverantwoordelijke toezicht kan en mag uitoefenen op een correcte verwerking van de persoonsgegevens door de verwerker. Denk hier bijvoorbeeld aan afspraken over het terugkoppelen dat de gegevens tijdig zijn verwijderd etc.
11. De verplichting van de verwerker om mee te werken aan audits van de verwerkingsverantwoordelijke of een derde partij. Daarvoor stelt de verwerker alle benodigde informatie beschikbaar om te controleren of de verwerker zich houdt aan de verplichtingen.
12. Overige rechten en plichten van de verwerker.
13. Overige rechten en plichten van de verwerkingsverantwoordelijke.
14. Afspraken over het inschakelen van subverwerkers door de verwerker. Hiervoor moet de verwerkingsverantwoordelijke vooraf schriftelijk toestemming verlenen of er moeten in de verwerkersovereenkomst duidelijke afspraken zijn gemaakt wanneer die toestemming is verleend. Daarnaast dient de verwerker met de subverwerker een subverwerkersovereenkomst op te stellen met minimaal dezelfde verplichtingen als de verwerker richting de verwerkingsverantwoordelijke heeft op basis van de verwerkersovereenkomst. Belangrijk hierbij is je te realiseren dat de verwerker volledig aansprakelijk is richting de verwerkingsverantwoordelijke indien de subverwerker zijn verplichtingen niet nakomt. Afspraken over het overdragen van persoonsgegevens naar partijen in andere landen.
15. Garanties van beide partijen over het correct naleven van de privacywetgeving
16. Hoe er met verzoeken van betrokkenen wordt omgegaan. Denk hier aan wie er de verzoeken ontvangt, beantwoordt, behandelt en administreert.
17. Hoe er met rechten van betrokkenen wordt omgegaan. Denk hier aan wie de betrokkene beantwoordt, de verzoeken behandelt en administreert.
18. Eigendom van de persoonsgegevens.
19. Vrijwaringen inzake claims van betrokkenen en derden (denk hierbij aan toezichthouders).
20. Geheimhouding van de persoonsgegevens. Denk hierbij aan welke personen toegang hebben tot de persoonsgegevens en hiervoor een geheimhoudingsplicht hebben. Stel die personen daarvan op de hoogte en zorg voor een bevestiging van het nakomen van die geheimhoudingsplicht.
21. Duur, verlenging en opzegging van de verwerkersovereenkomst.
22. Wijzigen van de verwerkersovereenkomst.

Let op: bovengenoemde lijst is indicatief. In een specifiek geval kan het dus zijn dat er nadere gegevens of afspraken in de overeenkomst moeten worden opgenomen.