

Checklist bewerkersovereenkomst

Als een opdrachtgever een dienstverlener inschakelt die persoonsgegevens verwerkt ten behoeve van de opdrachtgever moeten partijen afspraken vastleggen over de omgang met die persoonsgegevens. Die afspraken kunnen worden vastgelegd in een bewerkersovereenkomst. De opdrachtgever blijft verantwoordelijk voor de verwerking van de persoonsgegevens ook al besteedt hij de verwerking van bepaalde persoonsgegevens uit. Het is daarom belangrijk goede afspraken te maken over de omgang met en de beveiliging van de persoonsgegevens, of de dienstverlener derden mag inschakelen etc. In deze checklist staan de onderdelen die in ieder geval in een bewerkersovereenkomst moeten worden opgenomen om te voldoen aan de huidige en toekomstige privacyregelgeving. Het gaat dan om de Wet bescherming persoonsgegevens en de uitleg die de Autoriteit Persoonsgegevens daaraan geeft en de Algemene Verordening Gegevensbescherming (verordening (EU) 2016/679).

Inhoud dienstverlening en rol partijen

- Korte omschrijving van de opgedragen werkzaamheden
- Verwijzing naar de overeenkomst van opdracht
- Rol van beide partijen (verantwoordelijke/bewerker)

Basisafspraken over de verwerking

- Beide partijen leven de privacyregelgeving na
- Bewerker mag uitsluiten bewerken op basis van (schriftelijke) instructies van de verantwoordelijke – verwerkingsverbod buiten de opdracht
- Partijen zullen elkaar informeren over relevante wijzigingen in de dienstverlening of met betrekking tot de persoonsgegevens

Geheimhouding

- Bewerker dient de persoonsgegevens geheim te houden en deze verplichting op te leggen aan zijn personeel en ingeschakelde derden (zie ook sub-bewerkers)
- Bewerker mag de persoonsgegevens niet aan derden verstrekken tenzij in opdracht van opdrachtgever of op grond van een wettelijke verplichting

Beveiliging

- Bewerker dient passende technische en organisatorische maatregelen te treffen en in stand te houden om een op het risico afgestemd beveiligingsniveau te waarborgen
 - Concrete maatregelen opnemen in een bijlage. Of de beveiliging passend is ligt aan de aard van de persoonsgegevens en de risico's van verlies of onrechtmatige toegang. De verantwoordelijke (opdrachtgever) en bewerker zullen dit samen moeten afstemmen.

Controle

- Opdrachtgever heeft het recht om zelf of door onafhankelijke deskundigen een audit te laten uitvoeren
- Bewerker zal alle redelijke medewerking dienen te verlenen aan een audit

- Omdat de opdrachtgever verantwoordelijk blijft voor de verwerking zal die ook moeten toezien op de verwerking door bewerker
- Partijen kunnen er ook voor kiezen dat bewerker zelf periodiek een onafhankelijke audit laat uitvoeren en opdrachtgever daar het rapport of de verklaring van toestuuft

Meldplicht datalekken

- Bewerker dient opdrachtgever zo snel mogelijk te informeren over ieder beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan of mogelijk toegankelijk zijn geworden voor onbevoegden
- Bewerker moet maatregelen treffen om de gevolgen van het incident te beperken en volgende incidenten te voorkomen
- Afspraken over wie een datalek meldt en hoe de communicatie tussen partijen moet verlopen

Rechten betrokkenen

- Bij een verzoek of bezwaar van een betrokkene, zoals een verzoek om informatie, inzage, rectificatie, gegevenswissing, verwerkingsbeperking of overdracht van de persoonsgegevens, dient bewerker het verzoek onmiddellijk door te sturen naar opdrachtgever
- Bewerker zal alle medewerking verlenen om ervoor te zorgen dat opdrachtgever kan voldoen aan zijn verplichtingen richting betrokkenen

Inschakelen derden (sub-bewerkers)

- Bewerker heeft toestemming nodig van opdrachtgever om een sub-bewerker te mogen inschakelen
- Bewerker zal met sub-bewerkers een overeenkomst sluiten die in overeenstemming is met de relevante privacyregelgeving en de bewerkersovereenkomst
 - De gegevens over de sub-bewerkers opnemen in een bijlage. Opdrachtgever kan toestemming worden gevraagd bij de inschakeling van iedere nieuwe sub-bewerker of kan een algemene toestemming geven met een termijn om zich te verzetten. In alle gevallen dient opdrachtgever als verantwoordelijke van de persoonsgegevens geïnformeerd te worden over de inschakeling van sub-bewerkers. Daarom is het handig dat op te nemen in een bijlage die kan worden aangevuld.

Verwerking buiten de EU

- Bewerker mag de persoonsgegevens niet buiten de EU verwerken, tenzij opdrachtgever schriftelijke toestemming heeft gegeven.
- Als bewerker de persoonsgegevens wel buiten de EU mag verwerken, dan zal hij in overeenstemming met de privacyregelgeving passende waarborgen moeten treffen
 - De gegevens over de verwerking buiten de EU opnemen in een bijlage. Daarbij moeten de landen en de getroffen maatregelen worden opgenomen. Denk bij verwerking buiten de EU ook aan cloud-opslag op servers buiten de EU en onderhoud aan systemen door personen van buiten de EU.

Overige aandachtspunten

- Toegang tot de persoonsgegevens – ook bij conflict over einde van de dienstverlening
- Medewerking bij een onderzoek van een toezichthouder
- Aansprakelijkheid en vrijwaring – eventueel boetebepaling
- Duur en beëindiging – teruggave en vernietiging persoonsgegevens
- Wijzigingsbepaling voor wijziging wetgeving of omstandigheden
- Toepasselijk recht en bevoegde rechter

Monique Hennekens - april 2017

Hekkelman Advocaten