Verwerkersovereenkomst

Leidraad bij het opstellen van verwerkersovereenkomsten.

Steeds meer bedrijven besteden een groot deel van hun ICT-activiteiten uit aan dienstverlenende bedrijven. Deze dienstverlenende bedrijven bieden verschillende niveaus van diensten om klanten in hun processen te ondersteunen. Deze diensten worden doorgaans aangeduid als IaaS, PaaS, of SaaS. Een belangrijk onderdeel van de dienstverlening betreft de verwerking van persoonsgegevens die onder de wet van 8 december 1992 tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens (kortweg: de Privacywet) vallen. Deze Privacywet wordt echter vanaf 25 mei 2018 vervangen door de Algemene Verordening Gegevensbescherming (kortweg: de AVG). De definitie van verwerking van persoonsgegevens is zeer breed: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens. Er is aldus al snel sprake van een verwerking van persoonsgegevens en toepassing van de privacywetgeving

Met de toename van de dienstverlening, stijgt ook het risico voor de dienstverlener. Immers, als verwerker van de data van klanten neemt de dienstverlener een deel van de aansprakelijkheid op zich, o.a. in geval van diefstal of verlies van data. Hoewel deze aansprakelijkheid eventueel contractueel beperkt kan worden, kunnen niet alle risico's worden uitgesloten.

Wat is een Verwerkersovereenkomst?

Een verwerkersovereenkomst is verplicht tussen de dienstverlener (de “Verwerker”) en de klant die aan de dienstverlener vraagt om gegevens te verwerken (“de verantwoordelijke voor de gegevensverwerking” of de “Verantwoordelijke”). In een dergelijke overeenkomst worden de verantwoordelijkheden van elke betrokken partij, in geval van schade door bijvoorbeeld diefstal of verlies van data, vastgelegd. Het is van groot belang om alle verantwoordelijkheden en eventuele activiteiten van de verwerker ondubbelzinnig vast te leggen. De verwerker dient niet meer of minder uit

te voeren dan afgesproken. Indien hij, buiten de afspraken om, bewerkingen aan data van derden uitvoert, kan hij namelijk als “verantwoordelijke” (i.p.v. als “verwerker”) worden gezien en neemt zijn aansprakelijkheid significant toe.

Onder de AVG dient de verantwoordelijke zich ook te vergewissen van de kwaliteit van de verwerker, en of deze in alle opzichten een passend beschermingsniveau voor de verwerking van persoonsgegevens biedt.

Inhoud van de overeenkomst

De verwerkersovereenkomst legt de rechten en verplichtingen van de verantwoordelijke en de verwerker vast en dient in ieder geval de volgende gegevens te bevatten:

- De overeenkomst dient onder andere een beschrijving te omvatten van de soorten van te verwerken persoonsgegevens en de categoriëen van betrokkenen, het doel en de aard van de verwerking, met welke middelen dit wordt gedaan en hoe lang deze gegevens worden bewaard.
- De verplichting dient te worden opgenomen dat de persoonsgegevens uitsluitend verwerkt worden op basis van schriftelijke instructies van de verantwoordelijke, tenzij er een wettelijke bepaling de verwerker er anders toe verplicht. In dit geval dient de verantwoordelijke te worden ingelicht.
- Specificatie van wat er met de gegevens dient te gebeuren na afloop van de verwerking: dienen deze weer aan de verantwoordelijke te worden overgedragen, of eventueel vernietigd te worden?
- Een vertrouwelijkheidsverklaring voor de verwerker en zijn personeel. Hierin dient onder meer vastgelegd te worden dat alleen geautoriseerde personen toegang tot de data mogen hebben.
- Een waarborg dat de verwerker medewerking biedt aan de verantwoordelijke indien een persoon gebruik maakt van zijn recht op toegang tot, of correctie en/of vernietiging van zijn gegevens, door het nemen van de nodige technische en organisatorische maatregelen. Ook is bijstand en medewerking vereist van de verwerker bij mogelijke controles bij de verantwoordelijke.
- De verwerker dient te verzekeren dat de door hem getroffen organisatorische en technische beschermingsmaatregelen (en die van eventuele sub-verwerkers) voldoen aan de geldende wetgeving. De verwerker dient dus ook te verzekeren dat de juiste beveilingsmaatregelen zijn genomen tegen verlies of onregelmatige verwerking. Indien er toch een datalek is, dient er te worden beschreven hoe de verwerker in dat geval zal handelen.
- Dat datalekken zonder redelijke vertraging aan de verantwoordelijke en onverwijld aan betrokkenen gemeld dienen te worden en de communicatie-procedures hieromtrent.
- Een lijst van locaties waar de gegevens door verwerker (en eventuele sub-verwerkers) kunnen worden opgeslagen.
- Het recht van de verantwoordelijke om toezicht te houden en de medewerking die de verwerker hieraan dient te verlenen.
- De verplichting voor verwerker om alle redelijke instructies van de verantwoordelijke in verband met de verwerking van de Persoonsgegevens op te volgen.
- De plicht van de verwerker om alle relevante veranderingen in de functionaliteit van de dienstverlening te melden aan de verantwoordelijke.
- Vastlegging van hoe de logging en auditing van gegevens door de verwerker en eventuele sub-verwerker(s) dient te geschieden.
- De verwerker dient te verzekeren dat de door hem getroffen organisatorische en technische beschermingsmaatregelen (en die van eventuele sub-verwerkers) passend zijn en voldoen aan de geldende wetgeving ter bescherming van persoonsgegevens en zich in dat verband eventueel te doen certificeren.
- Het regelmatig monitoren van het passende beschermingsniveau door middel van bijvoorbeeld penetratietesten.
- Privacy by design en default maatregelen waaronder pseudonimiseren.
- De verwerker kan er ook aan herinnerd worden dat hij ook conform de AVG een verwerkingsregister moet aanleggen met alle categorieën van verwerkingen die voor een verantwoordelijke worden verricht, met naam en contactgegevens, doel en mogelijke doorgiften van persoonsgegevens.
- Een goede regeling voor de aansprakelijkheid (afgedekt met verzekering) met eventueel een vrijwaring van de verantwoordelijke voor de verwerker.
- Het niet zonder toestemming van de verantwoordelijke mogen inschakelen van andere (sub) verwerkers en altijd op minimaal dezelfde voorwaarden als die in de hoofdverwerkersovereekomst.
- Een bepaling dat de verwerker de persoonsgegevens enkel buiten Nederland mag verwerken met voorafgaande schriftelijke toestemming van de verantwoordelijke.

Gegevensverstrekking aan derden en sub-verwerkers

De verwerker kan een algemene toestemming vragen om sub-verwerkers in te zetten in de verwerkingsovereenkomst, bij gebreke waaraan een specifieke voorafgaande toestemming door de verantwoordelijke vereist is. De sub-verwerker dient ook dezelfde verplichtingen inzake gegevensbescherming opgelegd te krijgen als in de verwerkingsovereenkomst. Wanneer de sub-verwerker zijn verplichtingen echter niet nakomt blijft de eerste verwerker ten aanzien van de verantwoordelijke aansprakelijk.

Er dient duidelijk vastgelegd te worden dat de gegevens niet mogen worden gedeeld met derden tenzij contractueel anders is overeengekomen. Doorgifte van persoonsgegevens naar landen die geen passende bescherming bieden (landen buiten de Europese Economische Ruimte), mag alleen indien de Europese Commissie heeft bepaald dat doorgifte naar een dergelijk derde land is toegestaan dan wel waarborgen zijn ingebouwd om veilige doorgifte mogelijk te maken. Denk hierbij aan het gebruik van de standaard Europese model clausules of binding corporate rules.

Disclaimer
Dit document is geen juridisch advies en aan de inhoud kunnen geen rechten worden ontleend. Wij raden u aan een jurist of advocaat te raadplegen voor het opstellen van een verwerkersovereenkomst.

Voor vragen en/of aanvullende informatie kunt u contact met ons opnemen

Chubb
Terhulpsesteenweg 166
1170 Brussels
+32 2 516 9711

Emiel Banningstraat 41
2000 Antwerp
+32 3 241 3800

Wouter Wissink
Property & Casualty Risk Engineer & Senior ICT specialist, Risk Engineering Services
T +31 (0)23 5661 832
E wwissink@chubb.com

Chubb. Insured.℠