Bijlage 14. De Verwerking van Persoonsgegevens
In deze bijlage moet in ieder geval het volgende worden gespecificeerd:

Het onderwerp/aard en doel van de Verwerking

Het soort Persoonsgegevens

Beschrijving categorieën Persoonsgegevens

Beschrijving categorieën Betrokkenen

Beschrijving categorieën ontvangers van Persoonsgegevens

Voor de inhoud van deze bijlage kan onder meer gebruik worden gemaakt van de registratie die de Verwerkingsverantwoordelijke op grond van artikel 30 van de Verordening dient aan te houden.

Deel 2. Passende technische en organisatorische maatregelen

Opdrachtnemer heeft een (informatie)beveiligingsbeleid opgesteld en de hierin beschreven maatregelen aantoonbaar geïmplementeerd. Dit beleid wordt met regelmaat getoetst en geactualiseerd. De beveiligingsmaatregelen zijn passend voor en in overeenstemming met de waarde van de te verwerken gegevens.

Wanneer Opdrachtnemer gebruik maakt van subverwerkers, dienen deze expliciet te zijn beschreven en bekend te zijn bij Opdrachtgever. De subverwerker houdt zich aan minimaal dezelfde beveiligingseisen en –maatregelen als Opdrachtnemer.

Organisatie van informatiebeveiliging

Verantwoordelijkheden ten aanzien van het beschermen van Persoonsgegevens zijn binnen de organisatie Opdrachtnemer expliciet benoemd en belegd.

Personele maatregelen

Verwerker heeft aantoonbaar bevoegd en bekwaam personeel. Zowel bevoegd en bekwaam voor het verwerken van de gegevens als voor het beveiligen en beschermen van de gegevens.

De personeelsleden zijn via een schriftelijke overeenkomst verplicht tot geheimhouding van alle informatie van Opdrachtgever.

Toegang tot Persoonsgegevens

Toegang tot Persoonsgegevens is beperkt op basis van het need-to-know principe. Alleen wanneer toegang tot Persoonsgegevens daadwerkelijk benodigd is voor het uitvoeren van de werkzaamheden wordt deze toegang ook ingeregeld. Zodra bevoegdheden van personen veranderen, wordt de toegang tot gegevens hierop aangepast.

Verwerking op mobiele apparatuur

Wanneer Persoonsgegevens worden verwerkt op mobiele apparatuur, waaronder tablets, laptops en/of smartphones, dan dienen deze apparaten versleuteld (encrypted) te zijn conform marktstandaarden.

Fysieke beveiliging

Opdrachtnemer zorgt ervoor dat Persoonsgegevens worden verwerkt in een fysiek beveiligde omgeving, met passende bescherming tegen dreigingen van buitenaf.

IT-technische maatregelen

Opdrachtnemer neemt passende maatregelen om de IT-omgeving te beveiligen. Informatiesystemen, componenten en middelen zijn actueel en worden door de fabrikant officieel ondersteund.

Alle software wordt op basis van een gestructureerd proces voorzien van de laatste patches en updates. Waar technisch mogelijk wordt gebruik gemaakt van antivirussoftware.

Netwerken en informatiesystemen worden passend afgeschermd op basis van fysieke of logische scheiding, waarbij wordt gewaarborgd dat informatie van Opdrachtgever niet vermengd kan worden met dat van andere klanten van Opdrachtnemer.

Wanneer informatie over openbare netwerken of anderszins publiek beschikbaar kan komen, worden cryptografische maatregelen genomen om de informatie te beschermen tegen onbevoegde inzage.

Periodiek worden vulnerability scans en penetratietests uitgevoerd voor het toetsen van de beveiliging.

Toegang op afstand

Wanneer medewerkers van Opdrachtnemer toegang op afstand (bijvoorbeeld telewerken via internet) kunnen krijgen tot Persoonsgegevens, is deze toegang afgeschermd met een versleutelde verbinding. Toegang op afstand kan alleen worden verkregen door middel van het toepassen van 2 factor authenticatie.

Beheer van incidenten

Opdrachtnemer verplicht zijn medewerkers incidenten met betrekking tot informatiebeveiliging en privacy zo snel mogelijk te melden en deze op basis van de ernst op te volgen. Enkele voorbeelden van incidenten zijn:

- Uitval van dienstverlening, apparatuur of voorzieningen;
- Systeemstoringen of –overbelasting;
- Menselijke fouten;
- Niet-naleven van beleid en/of richtlijnen;
- Inbreuk op fysieke beveiligingsmaatregelen;
- Ongecontroleerde systeemwijzigingen;
- Storingen aan software of hardware;
- Virusuitbraak;
- Toegangsovertredingen (digitaal of fysiek).

- datalek

Alle medewerkers, tijdelijke medewerkers, onderaannemers en derde partijen die op enigerlei wijze gebruik maken van informatie of informatiesystemen van Opdrachtnemer zijn verplicht om (mogelijke) lekken en inbreuken in de informatiebeveiliging te melden als incident. Hiertoe wordt aan deze betrokkenen het incidentmeldingsproces van Opdrachtnemer kenbaar gemaakt.

Opdrachtnemer monitort toegang tot Persoonsgegevens en het mogelijk lekken hiervan.

Continuïteit van de dienstverlening

Opdrachtnemer neemt binnen de dienstverlening passende technische en organisatorische maatregelen om continuïteit te waarborgen. Wanneer de overeenkomst tussen Opdrachtgever en Opdrachtnemer eindigt, verplicht Opdrachtnemer zich te zorgen dat de dienstverlening van Opdrachtgever gewaarborgd blijft in de transitie naar de nieuwe leverancier van Opdrachtgever.

Overige maatregelen

De maatregelen beschreven in deze bijlage pretenderen niet concreet of volledig te zijn. Opdrachtgever verwacht dat Opdrachtnemer zich actief opstelt bij het beschermen van Persoonsgegevens en het nemen van maatregelen om deze te beschermen. In wederzijds overleg kunnen verbeteringen ten aanzien van de Verwerkersovereenkomst en de beschreven maatregelen worden besproken.