

Bijlage 12 Aanleveren gegevens tbv toetsen informatiebeveiliging en privacy

De opdrachtgever vraagt bewijsstukken aan te leveren om een eerste toetsing uit te kunnen voeren op de toereikendheid van de getroffen maatregelen op gebied van informatieveiligheid en privacy. Dit is tevens vermeld in paragraaf 5.5 van de aanbestedingsleidraad.

1. Ingeschakelde subverwerkers

Indien de inschrijver gebruik maakt van de diensten van derden zoals een (niet limitatief) datacenter/hostingpartij/overig dan vooraf inzage te worden gegeven in:

- Naam en contactgegevens;
- Aard afgenomen dienst;
- Uitbestede verwerkingen.

(Artikel 28 lid 2 en 4 AVG)

2. Doorgifte gegevens

De inschrijver dient vooraf aan te geven of bij het verlenen van de diensten sprake is van doorgifte van persoonsgegevens buiten de Europese Economische Ruimte (EER) door de leverancier en/of door derden (subverwerkers) zoals een (niet limitatief) datacenter/hostingpartij/overig indien de leverancier gebruikt maakt van de diensten van derden.

(Artikel 44 AVG)

3. Certificeringen

Indien de leverancier gebruik maakt van de diensten van derden zoals een (niet limitatief) datacenter/hostingpartij/overig dan dient vooraf te worden aangetoond dat deze partij(en) ISO 27001 of soortgelijk zijn gecertificeerd. Dit dient vooraf per partij afzonderlijk te worden aangetoond door middel van het overleggen van (kopie) van het geldige en actueel ISO 27001 certificaat inclusief de bijbehorende conformiteitsverklaring of op een overige wijze indien het een soortgelijke certificering betreft.

De verwerker/eigenaar van het datacenter waar de leverancier eventuele server c.q. clouddiensten heeft ondergebracht beschikt over een actuele en geldige assurance verklaring zoals een ISAE3xxx SOC type II of soortgelijke verklaring met daarin als toetsingscriteria de Trust Services Principles (Security, Availability, Processing Integrity, Confidentiality en Privacy op basis van de Europese wetgeving) waaruit blijkt welke op het risico afgestemde technische en organisatorische maatregelen de verwerker of eigenaar van het datacenter waar de server c.q. cloudoplossing is ondergebracht heeft genomen, daadwerkelijk worden uitgevoerd en in stand worden gehouden.

4. Beveiliging van de verwerking

De leverancier dient vooraf inzage te geven in welke op het risico afgestemde informatiebeveiligingsmaatregelen binnen de hieronder genoemde domeinen aangaande de verwerking zijn getroffen en in stand worden gehouden:

- Border Protection (Firewalls, Network Security Zoning, enzovoorts);
- Detection Services (Event Detection, Event Monitoring, Security Alerting, enzovoorts);
- Physical Security Technology (Physical Intrusion Detection, Physical Access Control, enzovoorts);
- Content Control Services (Content Filtering, File Transfer, enzovoorts);
- Identity & Access Management (Credentials, Access Management, logging, enzovoorts);
- Data Recovery (Beackup Services en Restore Services);
- Cryptographic Services (Encryption of Data in Flight, Encryption of Data at Rest, enzovoorts);
- Application Security (Design, Testing, enzovoorts);
- Auditing Services (Security Assessment, Compliance Scanning, enzovoorts);
- Configuration Management (Patch Testing, Change Control, enzovoorts).

Dit is ook van toepassing op de verwerking(en) die de leverancier heeft uitbesteed/ondergebracht bij sub verwerkers. Dit kan aangetoond worden door middel van een assurance verklaring ISAE3xxx SOCType II of een een Third Party Memorandum (TPM). Op een andere wijze mag ook. Indien gewenst zal vooraf aan deze inzage een geheimhoudingsverklaring / non-disclosure agreement (NDA) worden opgesteld.