Aanvullende eisen m.b.t. informatiebeveiliging

Onderwerp: Geheimhouding

Opnemen:
Leverancier zal het bestaan, de aard en de inhoud van de contract, evenals overige bedrijfsinformatie van de gemeente geheimhouden en niets daaromtrent openbaar maken zonder schriftelijke toestemming van de gemeente.
De leverancier staat er voor in dat personeel van de leverancier, overige personeelsleden en derden de bepalingen betreffende gedrag, vertrouwelijkheid en bescherming van gegevens naleven.

Doel van deze bepaling:
De leverancier zal geen informatie van de gemeente openbaar maken zonder toestemming van de gemeente. Eventueel wordt een geheimhoudingsverklaring door de leverancier getekend. Als dit niet collectief kan, dient iedere ingehuurde medewerker apart een geheimhoudingsovereenkomst te tekenen. Artikel 15 uit de GIBIT gaat over geheimhouding.

Onderwerp: Verklaring Omtrent het Gedrag (VOG)

Opnemen:
Medewerkers van de leverancier overleggen voor aanvang van de werkzaamheden bij de gemeente een recente Verklaring Omtrent het Gedrag (VOG). De leverancier stemt voorafgaand aan de aanvraag de noodzaak, inhoud en aard hiervan af met de gemeente.

Doel van deze bepaling:
Externe medewerkers moeten, net zo goed als interne medewerkers, een VOG kunnen overleggen bij aanvang van de werkzaamheden voor de gemeente. Overigens hoeft dit niet voor alle medewerkers te gelden. Als iemand helemaal niet in aanraking komt met gevoelige gegevens of systemen is een VOG misschien wat te veel gevraagd.

Onderwerp: Gedragsregels

Opnemen:
De leverancier zal voor de prestaties voldoende personen inzetten met voldoende opleiding, vaardigheden en kennis van de bedrijfsvoering en organisatie van de gemeente, om de prestaties te verrichten.
Wanneer de hierboven genoemde personen zich bij de gemeente bevinden, of in direct contact met de gemeente staan, zal het personeel van de leverancier de gedragsvoorschriften van de gemeente naleven. Hiermee zal gevolg gegeven worden aan redelijke verzoeken van de gemeente.

Doel van deze bepaling:
De leverancier moet blijk geven van het hebben van personeel met voldoende kennis en kunde om de werkzaamheden binnen de gemeente te verrichten. Dit hangt samen met beveiligingseisen, die bijvoorbeeld door scholing en/of voldoende kennis en kunde gebruikersfouten beperken. Daarnaast moet extern personeel zich net zo goed houden aan de gedragsregels van de gemeente als de gemeenteambtenaar.

Onderwerp: Informatieveiligheid en privacy

Opnemen:
De leverancier stelt de gemeente in staat, bij het overeengekomen gebruik van de Oplossing, te voldoen aan de BIO en AVG en draagt hiervoor actief zorg bij de ontwikkeling, implementatie, beheer en onderhoud van de oplossing.

Doel van deze bepaling:
De in het PvE vermelde verplichting om ISO 27001 gecertificeerd te zijn richt zich op het aanbrengen van waarborgen in het proces bij de leverancier. De aanwezigheid van deze waarborgen hoeven niet noodzakelijkerwijs te betekenen dat de Oplossing de gemeente in staat stelt te voldoen aan de BIO en AVG. Hoofdstuk 2 uit de GIBIT heeft betrekking op informatiebeveiliging (en ook privacy en archivering) en artikel 26 gaat expliciet over informatiebeveiliging.

Onderwerp: Controle en toezicht

Opnemen:
De contractant levert verantwoordingsrapportages aan de gemeente conform afgesproken prestatie-indicatoren.

Doel van deze bepaling:
In de inkoopcontracten dient de gemeente expliciete prestatie-indicatoren en bijbehorende verantwoordingsrapportages op te nemen. Voor controle en toezicht is het van belang dat voor afsluiting van het contract welke prestatie-indicatoren van toepassing zijn en afspraken te maken met de leverancier dat hier periodiek over wordt gerapporteerd. Artikel 8.12 en artikel 21 van de GIBIT hebben betrekking op controle en rapportage.

Onderwerp: Escrow

Opnemen:
De leverancier draagt zorg voor een Escrow. Zo heeft de gemeente in voorkomend geval de mogelijkheid om bij het in vervulling gaan van één of meer in de Escrow genoemde voorwaarden, software die onderdeel is van het contract, eigenmachtig te (laten) gebruiken voor het herstellen van fouten en anderszins het onderhouden en beheren van de standaardprogrammatuur.

Doel van deze bepaling:
De gemeente die software gebruikt van een leverancier op haar eigen ICT-infrastructuur of in een Cloud toepassing, moet de mogelijkheid hebben om bijvoorbeeld in het geval dat de software leverancier failliet gaat te waarborgen dat de software onderhouden en gebruikt kan blijven worden. Artikel 32 ‘Waarborgen continuïteit’ van de GIBIT heeft betrekking op data-escrow.