Bijlage 5: Eisen m.b.t. Informatiebeveiliging bij Inkoop

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: Diensten en goederen

Opnemen: Service Level Agreement (SLA)

In het geval van af te nemen diensten met afgesproken serviceniveaus wordt tussen de leverancier en de gemeente een SLA afgesloten, volgens het model van de IBD.

Doel van deze bepaling:

Als diensten worden afgenomen, dan horen daar serviceniveaus bij en de manier van meten en rapporteren. Deze serviceniveaus gaan ook over beveiligingsaspecten, zoals bijvoorbeeld beschikbaarheid, melden van incidenten, doorvoeren van wijzigingen, serviceniveaus en escalatie. Artikel 8 van de GIBIT heeft betrekking op een SLA.

Onderwerp: Informatieveiligheid

Opnemen:

De leverancier accepteert de maatregelen uit de BIO, voor zover van toepassing verklaard door de gemeente, en past deze toe op de geleverde producten en/of diensten. Leveranciers maken aansluitend hun keten van toeleveranciers bekend maken en zijn transparant over de maatregelen die zij genomen hebben om aan de hun opgelegde eisen door te vertalen naar hun toeleveranciers.

Doel van deze bepaling:

Als een leverancier producten en/of diensten levert aan de gemeente, dan dient de leverancier uit te gaan van het basisbeveiligingsniveau van de gemeente, dat gebaseerd is op de BIO. Eventueel wordt een link toegevoegd of de BIO is onderdeel van de eisen en wensen. Hoofdstuk 2 uit de GIBIT heeft betrekking op informatiebeveiliging (en ook privacy en archivering) en artikel 26 gaat expliciet over informatiebeveiliging.

Onderwerp: Persoonsgegevens

Opnemen:

De leverancier accepteert dat wanneer er persoonsgegevens worden verwerkt in systemen van de leverancier buiten de gemeente (bijvoorbeeld bij SaaS), er een verwerkersovereenkomst wordt afgesloten als onderdeel van het contract. Tevens worden in het contract afspraken vastgelegd betreffende aansprakelijkheid en schade in geval van incidenten. De standaard verwerkersovereenkomst gemeenten van de IBD wordt gehanteerd.

Doel van deze bepaling:

Als persoonsgegevens van de gemeente worden gehost bij een externe partij, dan is deze 3e partij vanuit de AVG een verwerker. Of deze 3e partij zelf iets verwerkt of niet, maakt niet uit. De gemeente is en blijft verantwoordelijk voor deze persoonsgegevens. Daarmee is de gemeente verplicht om beveiligingsmaatregelen te laten uitvoeren door deze 3e partij en deze ook jaarlijks te (laten) toetsen. Deze beveiligingsmaatregelen en verantwoordelijkheden worden in een verwerkersovereenkomst vastgelegd. Artikel 24 en 25 van de GIBIT gaan expliciet over de verwerkersrelatie en de verwerkersovereenkomst.

Onderwerp: Melden van (beveiligings)incidenten

Opnemen:

In het geval van afnemen van producten en/of diensten accepteert de leverancier dat (beveiligings)incidenten direct gemeld worden aan de gemeente, en als dat wettelijk noodzakelijk is ook aan de Autoriteit Persoonsgegevens. Bij niet gemelde incidenten waar persoonsgegevens bij betrokken zijn, zal de gemeente een ontvangen boete en ontstane schade verhalen op de leverancier. Wanneer

een kwetsbaarheid is geconstateerd bij de leverancier, dan zorgt de leverancier er ook voor dat deze wordt opgelost.

Doel van deze bepaling:
Algemeen:
Als de leverancier informatie van de gemeente host op haar systemen, dienen (beveiligings)incidenten direct gemeld te worden aan de betrokken contactpersoon van de gemeente. De gemeente dient te kunnen reageren op (beveiligings)incidenten en deze melding dient door de contactpersoon van de gemeente gemeld te worden aan de IBD. Daarbij dienen de geconstateerde kwetsbaarheden door de leverancier ook opgelost te worden. Artikel 27 uit de GIBIT heeft betrekking op de meldplicht voor beveiligingsincidenten.

Incidenten met persoonsgegevens:
Bij een datalek moet de gemeente afwegen of ook aan de Autoriteit Persoonsgegevens (AP) gemeld moet worden en aanvullend betrokkenen geïnformeerd moeten worden.

Onderwerp: controle en toezicht

Opnemen:
De gemeente kan een externe audit, waaronder een penetratietest, laten uitvoeren om te controleren dat aan beveiligingseisen die van toepassing zijn wordt voldaan. Een audit is niet nodig als de contractant door middel van certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd, dan wel aantoont dat een onafhankelijke audit heeft plaatsgevonden en de relevante resultaten deelt met de gemeente.

Doel van deze bepaling:
De leverancier kan te maken krijgen met beveiligingseisen in bijvoorbeeld de verwerkersovereenkomst, de gemeente moet dan controleren dat die beveiligingseisen ook worden nageleefd. Om te voorkomen dat bij een leverancier door iedere klant jaarlijks audits worden uitgevoerd, kan de leverancier ook volstaan met een Third Party Mededeling (TPM)-verklaring waardoor de auditlast verminderd. Artikel 8.12 en artikel 21 van de GIBIT hebben betrekking op controle en rapportage.

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.

Onderwerp: Exit-strategie

Opnemen:
De contractant beschikt over een expliciete uitwerking van de exit-strategie.

Doel van deze bepaling:
Voordat een contract wordt afgesloten wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete uitwerking van de exit-strategie. Artikel 22 van de GIBIT heeft hier betrekking op (overstap van opdrachtgever naar een ander systeem, afschaling en overdracht).

Onderwerp: Ontwikkeling van software en systemen

Opnemen:
De gangbare principes rondom Security by design zijn uitgangspunt voor de ontwikkeling van software en systemen.

Doel van deze bepaling:
Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast. Het is van belang grip te hebben op Secure Software Development