

BIJLAGE 6.7: EISEN INFORMATIEBEVEILIGING EN PRIVACY

1.1 GENERIEK

- De Leverancier accepteert de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT) als leidende inkoopvoorwaarden. De GIBIT is beschikbaar via de website van VNG-Realisatie: GIBIT | VNG
- Leverancier licht toe hoe wordt voldaan aan de GIBIT-artikelen: 6 en 25
- Indien van toepassing voor de ICT-prestatie zijn de volgende open standaarden van het Forum Standaardisatie onder meer en expliciet verplicht: DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv6, SAML, SPF, STARTTLS, DANE, STIX en TAXII, TLS en WPA2.
NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002 (Informatiebeveiliging).
- De ICT-Prestatie stelt de opdrachtgever in staat te voldoen aan:
 - De (U)AVG;
 - De Baseline Informatiebeveiliging Overheid;
 - ISO 27001:2017;
 - ISO 27002:2017;
 - De beveiligingsrichtlijnen voor webapplicaties van het NCSC;
 - Archiefwet 1995, Archiefbesluit 1995;
 - Het Algemeen en Technisch Informatiebeveiligingsbeleid van Opdrachtgever
 - Leverancier licht toe hoe de ICT-Prestatie de Opdrachtgever ondersteund om hieraan te voldoen.
- Indien de Leverancier gebruik maakt van een onderaannemer gelden alle eisen onverminderd voor de onderaannemer. De Leverancier is verantwoordelijk voor een juiste invulling en werking van de eisen bij de onderaannemer.
- De Leverancier is NEN/ISO 27001 gecertificeerd. De Leverancier overlegt het certificaat.
- De Leverancier geeft transparant en kosteloos inzicht in certificeringsdocumenten en rapportages opgesteld door EDP-auditors. TPM verklaringen moeten in bezit van de opdrachtgever zijn vóór 30 oktober van het verantwoordingsjaar.
- De Leverancier licht toe hoe de principes van 'privacy bij design' en 'privacy by default' zoals beschreven in de AVG zijn toegepast.
- Leverancier treft beheersmaatregelen om onbevoegde toegang tot, schade aan en interferentie (storing/uitval) met informatie en informatieverwerkende faciliteiten van Opdrachtgever te voorkomen, zodat de bedrijfsvoering niet wordt onderbroken of aangetast.
- Leverancier heeft beheersmaatregelen tegen malware getroffen
- Risico's voor informatiebeveiliging en privacy zijn expliciet benoemd en passende beheersmaatregelen zijn expliciet belegd
- De applicatie wordt periodiek en minimaal eens per jaar op kwetsbaarheden onderzocht (kwetsbaarheidsscans en penetratietesten). Kwetsbaarheden worden geclassificeerd en krijgen opvolging.

1.2 INTEGRITEIT

- Onderliggende software componenten, zoals operating systemen, database software, browser versie, programmeer framework enz., waarop de software is gebouwd en draait dienen altijd een door de oorspronkelijke Leverancier van de betreffende software of framework ondersteund te zijn. Bijvoorbeeld: als Microsoft Windows gebruikt wordt, is dit op basis van een nog door Microsoft ondersteunde versie. Windows10 of Windows11 zou acceptabel zijn met de nog ondersteunde build versie,
- Onderliggende software (inclusief frameworks en libraries) wordt structureel voorzien van beveiligingspatches. In het contract of SLA worden hiervoor reguliere afspraken gemaakt aangaande frequentie en betaling.
- De Leverancier heeft maatregelen genomen om de toegang tot de broncode van informatiesystemen te beperken tot de medewerkers, die deze code onderhouden of installeren.
- De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijv. door checksums).
- Versies van de software worden voor de in productie name door de Leverancier onder meer getest op invoer van gegevens (grenswaarden, format, inconsistentie, SQL injectie, cross site scripting, etc.).
- Applicaties worden ontwikkeld en getest op basis van Internationale en richtlijnen voor beveiliging, zoals de richtlijnen voor beveiliging van webapplicaties. Er wordt tenminste getest op bekende kwetsbaarheden zoals vastgelegd in de Open Web Application Security Project (OWASP) top 10
- De opdrachtgever heeft het recht om in overleg met de Leverancier webapplicaties of servicekoppelingen te onderwerpen aan penetratietesten op kosten van de opdrachtgever. De Leverancier heeft hierbij de verplichting om geconstateerde kwetsbaarheden in de applicatie op te lossen zonder meerkosten. Termijnen van de oplossing worden in overleg met een gebruikersvereniging of bij gebrek hieraan in overleg met de opdrachtgever bepaald.
- De applicatie voorziet in validatiecontroles op ten minste de volgende aspecten:
 - Gegevens en verwerkingen kunnen worden gecorrigeerd vanuit de applicatie na invoer
 - Consistentiecontroles zijn in de applicatie voorzien om de correcte verwerking van gegevens te waarborgen.De logging biedt voldoende inzicht in de bijhouding, uitwisseling, en selecties van gegevens om het gebruik van een gegeven door een applicatie te kunnen achterhalen en hierop te signaleren of acteren.

Onderdelen die minimaal in de logging opgenomen dienen te zijn:

 - Gebruikerslogging
 - Datum/tijd van actie
 - Gebruikersnaam of gebruiker ID
 - Uitgevoerde handeling
 - Object waarop de handeling werd uitgevoerd
 - Handelingen van gebruikers met speciale bevoegdheden

- Systeemlogging
 - Opgetreden fouten (error log)
 - (Poging tot) ongeautoriseerde toegang
 - (Poging tot) wijziging van beveiligingsinstellingen

In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, etc.). In de logregel mogen ook geen persoonsgegevens worden opgenomen uit systemen van de Opdrachtgever zelf (dus wel gebruikersnamen of inlog accounts)."

- Er is sprake van logging in de applicatie. Relevante zaken om te loggen zijn:
 - Type gebeurtenis (zoals back-up/restore, reset wachtwoord, betreden ruimte);
 - (poging tot) Ongeautoriseerde toegang;
 - Handelingen met speciale bevoegdheden, waarbij alle handelingen van "superusers" worden gelogd;
 - Systeemwaarschuwingen;
 - (poging tot) Wijziging van de beveiligingsinstellingen.
- De logging is alleen beschikbaar voor daartoe geautoriseerde medewerkers.
- Een logregel bevat in ieder geval geen gegevens die tot het doorbreken van de beveiliging kunnen leiden
- De logging is read-only. Het muteren en verwijderen van log-records is niet toegestaan.
- Gelogde informatie wordt minimaal 6 maanden bewaard, zodat onderzoek kan plaatsvinden in geval van een opgetreden informatiebeveiligingsincident.
- Logging kan naar een extern logging systeem (SIEM) gestuurd worden. De uitwisseling van deze informatie is mogelijk op basis van STIX en TAXII.
- Bij interne of externe applicatiekoppelingen biedt de applicatie voldoende waarborgen tussen componenten zodat er geen verlies van berichten optreedt (bijvoorbeeld buffering van berichten) en dat de validiteit van berichten beschermd is (uitsluiting van oa spoofing, MITM).
- Bij webservice koppelingen wordt uitgegaan van "dubbel SSL," dat wil zeggen een PKI-certificaat voor TLS en een PKI-certificaat om de serveridentiteit vast te stellen.
- Voor het configureren van platformen is een worden hardeningsrichtlijnen van de vendor toegepast of bijvoorbeeld van het CIS framework

1.3 VERTROUWELIJKHEID

- De Opdrachtgever blijft eigenaar van de gegevens binnen applicatie en deze gegevens mogen niet voor andere doeleinden gebruikt worden door de Leverancier van de applicatie. Dit geldt zowel voor gegevens in de Test-, Acceptatie- als Productieomgevingen.
- Het is de Leverancier verboden, zonder voorafgaande uitdrukkelijke schriftelijke toestemming van de opdrachtgever, de uitvoering van een overeenkomst geheel of gedeeltelijk aan derden over te dragen of uit te besteden.
- De Leverancier heeft een geheimhoudingsplicht aangaande alle vertrouwelijke gegevens dan wel anderszins gevoelige informatie van de opdrachtgever die de Leverancier in het kader van de opdracht ter kennis is gekomen.
- De Leverancier heeft een geheimhoudingsplicht aangaande de informatie opgenomen in de systemen.
- De Leverancier is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. Leverancier waarborgt hierbij tevens ook met scheiding van taken onbedoelde of ongeautoriseerde toegang. De opdrachtgever heeft het recht hierop te controleren.
- De Leverancier is verantwoordelijk voor de kwalificaties en screening van het eigen personeel. Op verzoek van opdrachtgever dient een VOG te worden overlegd, van personen die worden ingezet op de opdracht.
- Alle voorwaarden en eisen die gelden voor personeel van de Leverancier zijn ook van toepassing op derden, die in opdracht van de Leverancier diensten verrichten voor de Opdrachtgever
- Autorisaties kunnen worden ingericht op basis van functies (rol-gebaseerd) waarbij functie-scheiding is toegepast.(RBAC model)
- Leverancier geeft aan welke accounts nodig zijn voor beheer en ondersteuning
- Binnen de test omgeving wordt geen gebruik gemaakt van productie data
- Bij gebruik van PKI(o) certificaten beschikt de Leverancier over vastgestelde procedures voor sleutelbeheer. De Leverancier geeft bij de aanbesteding inzicht in de manier waarop sleutelbeheer is geregeld.
- De hosting en opslag van data vindt plaats binnen de Europese Economische Ruimte (EER)

1.4 PRIVACY

- De Leverancier stelt opdrachtgever in staat om zelf access management uit te voeren. Opdrachtgever dient direct invloed uit te kunnen oefenen over de accounts (en bijbehorende autorisaties) van de eigen medewerkers.
- De Leverancier houdt een actuele registratie bij van geautoriseerde accounts/gebruikers.
- De Leverancier verschaft relevante informatie over de wijze waarop – en onder welke voorwaarden – cryptografie wordt gebruikt om persoonsgegevens van betrokkenen te beschermen.
- De Leverancier maakt gebruik van een proces waarbij logbestanden periodiek gecontroleerd worden teneinde onrechtmatig gebruik of andere onregelmatigheden vast te stellen. De logbestanden dienen informatie te verschaffen over de vertrouwelijkheid, beschikbaarheid en integriteit van persoonsgegevens, en of daarop een inbreuk is geweest.
- Uitwisseling van persoonsgegevens dienen altijd te voorzien van encryptie, zowel voor fysieke media als transport
- Bij informatiebeveiligingsincidenten aan de kant van de Leverancier wordt door de Leverancier expliciet onderzocht of bij dat incident persoonsgegevens zijn gemoeid, tenzij dat redelijkerwijs niet aannemelijk is.
- Indien het uitvoeren van audits door opdrachtgever onwenselijk of redelijkerwijs niet mogelijk is, overlegt de Leverancier – voorafgaand aan het afsluiten van het servicecontract – onafhankelijk bewijs waaruit blijkt dat de getroffen beveiligingsmaatregelen conformeren aan de door opdrachtgever gestelde eisen en beleid.
- De Leverancier zorgt dat tijdelijke bestanden (cache) die persoonsgegevens bevatten periodiek worden verwijderd.
- De Leverancier legt alle verstrekkingen van persoonsgegevens (waar opdrachtgever verwerkingsverantwoordelijke voor is) aan andere partijen schriftelijk vast.
- De Leverancier en opdrachtgever maken schriftelijke afspraken over de manier waarop persoonsgegevens worden verwijderd of geanonimiseerd. De Leverancier heeft over dit onderwerp beleid opgesteld. In dat beleid wordt ook ingegaan op de bewaartermijn van persoonsgegevens na eindigen van het contract.
- De Leverancier dient (doorlopend) inzichtelijk te maken in welke landen persoonsgegevens (kunnen) worden opgeslagen. Eventuele contractuele waarborgen in het kader van hoofdstuk V van de AVG dient de Leverancier eveneens inzichtelijk te maken.
- Indien er algoritmes en/of Artificial Intelligence (AI) wordt toegepast, dient de Leverancier dit aan te geven inclusief toelichting op de werking van dit algoritme en/of AI.