

ICT Aansluitvoorwaarden mbt de aan te bieden Dienstverlening

Eis	nummer_t mp	Eis nodig? Over- ruled	Thema	Beschrijving	In aanvulling / Afwijking op
ICT002	2	Ja	1. Algemene eisen	Inschrijver verwerkt (persoons)gegevens in beginsel enkel binnen de Europese Economische Ruimte (EER). Inschrijver mag (persoons)gegevens buiten de EER (laten) verwerken wanneer is voldaan aan de voorwaarden van artikel 45 of 46 AVG. Wanneer er sprake is van een verwerking buiten de EER, dan stelt Inschrijver Opdrachtgever daarvan vooraf op de hoogte.	AVG artikel 45 en 46
ICT003	3	Ja	1. Algemene eisen	Inschrijver ondersteunt Opdrachtgever in het uitvoeren van een Data Protection Impact Analysis (DPIA) door het beantwoorden van de voor de Inschrijver bestemde onderdelen en vraagstukken. Ook werkt de Inschrijver mee indien van toepassing aan een voorafgaande raadpleging als bedoeld in artikel 35 en 36 AVG. Deze werkzaamheden zijn onderdeel van de dienstverlening, ook in het geval van een veranderd risico op de (persoons) gegevensverwerking gedurende de looptijd van de overeenkomst.	AVG artikel 35 en 36.
ICT004	4	Ja	1. Algemene eisen	Inschrijver gaat akkoord met het sluiten van een Verwerkersovereenkomst.	
ICT005	5	Ja	1. Algemene eisen	De aangeboden dienstverlening voldoet aan geldende wet- en regelgeving. In het bijzonder verwijzen we naar de volgende kaders welke in elk geval van belang zijn: - AVG en UAVG - BIO - Forum Standaardisatie (voorgeschreven normen en standaarden) - WOO - WDT - DUTO - WCAG - Archiefwet - WMEBV - SDG verordening	Gibit 2023 art. 8.1
ICT006	6	Ja	1. Algemene eisen	De Inschrijver moet wijzigingen in wet- en regelgeving tijdig doorvoeren in de aangeboden dienstverlening. Deze diensten zijn in beginsel onderdeel van de Overeenkomst en maken onderdeel uit van de overeengekomen prijs. In uitzonderingsgevallen (b.v. nieuwe wetgeving) dient contact gezocht te worden met de Opdrachtgever.	
ICT015	15	Ja	3. Dienstverlening - eigendom	Opdrachtgever is en blijft rechthebbende van de (intellectuele) eigendomsrechten welke rusten op data, aangeleverd of ingevoerd door Opdrachtgever en/of andere eindgebruikers (daarbij inbegrepen klanten van de Opdrachtgever) bij het gebruik van de aangeboden dienstverlening.	Gibit 2023 art. 20.2

Eis	nummer_t mp	Eis nodig? Over- ruled	Thema	Beschrijving	In aanvulling / Afwijking op
ICT019	19 Ja	3. Dienstverlening - gegevens		De dienstverlening voldoet aan de geldende archiefwetgeving en daaruit voortvloeiende regelingen en het informatiesysteem is opgebouwd volgens de principes van archiving by design, waaronder: - De datum voor het vernietigen van informatie moet automatisch berekend kunnen worden. Van Informatieobjecten die voor vernietiging of overbrenging zijn aangemerkt dient op basis van het vernietigings- of overbrengingsjaar een overzicht te worden gegenereerd; - De in de applicatie opgeslagen data blijft toegankelijk gedurende de looptijd van de overeenkomst, e.e.a conform het bijgesloten document Programma van Eisen, behoudens conform protocol vernietigde data; - Van de vernietiging dient een verklaring te kunnen worden opgeleverd. Hierin wordt minimaal vermeld welke informatie is vernietigd, op welke wijze de vernietiging heeft plaatsgevonden, de omvang van de data en de bevestiging dat de vernietiging volledig is uitgevoerd; - Het moet mogelijk zijn een export te maken van informatieobjecten en gekoppelde bestanden op basis van opgegeven zoekcriteria ten behoeve van bijvoorbeeld overbrenging naar een E-depot of een andere applicatie.	
ICT021	21 Ja	3. Dienstverlening - gegevens		Persoonsgegevens "in rust" worden bij voorkeur middels encryptie opgeslagen Gevoelige persoonsgegevens "in rust" moeten middels encryptie opgeslagen worden.	
ICT029	29 Ja	3. Dienstverlening - inrichting		De aangeboden dienst moet opzichzelfstaand zijn. Met uitzondering van de gevraagde koppelingen en integratievereisten mag er geen relatie zijn met andere binnen de gemeente aanwezige systemen om de gevraagde functionaliteit aan te bieden.	
ICT048	48 Ja	3. Dienstverlening - ontwikkeling		Ontwerp, ontwikkeling en inzet van de aangeboden dienstverlening volgt aantoonbaar Privacy by Design en Security by Design principes.	
ICT069	69 Ja	4. Beheer - backup & restore		Inschrijver dient aantoonbaar een backup mechanisme ingericht te hebben. Inschrijver beschrijft welke maatregelen genomen zijn om beschikbaarheid en veiligheid van backups bij calamiteiten zeker te stellen.	Gibit 2023, artikel 29.4
ICT076	76 Ja	5. Exitplan		Onderaannemers van de Inschrijver moeten kunnen verklaren dat zij, bij een eventueel faillissement van de Inschrijver of vanwege een andere situatie waarin de Inschrijver zijn SaaS-dienst niet kan continueren, bereid zijn om tegen tussen Inschrijver en onderaannemer overeengekomen vergoeding de dienst blijven leveren voor de duur van 6 tot 12 maanden.	
ICT077	77 Ja	5. Exitplan		Eventuele kosten voor het uitvoeren van de werkzaamheden voortvloeiende uit het opstellen of uitvoeren van het Exit-plan worden in de Inschrijving meegenomen. Er worden achteraf geen extra kosten voor Exit-werkzaamheden door Inschrijver in rekening gebracht.	
ICT078	78 Ja	5. Exitplan		De Inschrijver dient mee te werken aan de migratie van data naar een nieuw systeem op eerste verzoek van Opdrachtgever gedurende de SaaS-dienstverlening én uit eigen beweging bij het einde van de SaaS-dienstverlening. Hierbij garandeert Inschrijver de volledigheid van de data. Na migratie en of levering van de data, dient de Inschrijver op het eerste verzoek van Opdrachtgever de data aantoonbaar te verwijderen van haar systemen en te vernietigen. Dit geldt uitdrukkelijk ook voor data bestaande uit persoonsgegevens en data in de backup.	

Eis	nummer_t mp	Eis nodig? Over- ruled	Thema	Beschrijving	In aanvulling / Afwijking op
ICT079	79 Ja	5. Exitplan		De Inschrijver draagt aan het einde van de looptijd van het contract alle data (inclusief metadata) uit de aangeboden dienstverlening in een origineel en duurzaam DIGITAAL bestandsformaat, kosteloos over aan de Opdrachtgever. Na bevestiging van overdracht wordt alle data van de systemen van de Inschrijver vernietigd. De Inschrijver levert een verklaring van vernietiging; de Opdrachtgever wil alle in de aangeboden dienstverlening opgenomen gegevens in goede (uitwisselbare) vorm op een eenduidige manier overgedragen krijgen wanneer nodig is (outsourcing van taken of overstappen naar een andere dienstverlener na afloop van het contract). Inschrijver zal meewerken aan het volledig overdragen van onderhoud, beheer en ondersteuning aan de Opdrachtgever en/of een opvolgend dienstverlener.	
ICT080	80 Ja	7. Implementatie		Opdrachtgever wenst een open dialoog te kunnen voeren binnen het aan te gane partnerschap over het functioneren van het projectteam, ingezet bij/voor Opdrachtgever. Als er aandachtspunten / zorgen zijn omtrent het functioneren van projectleden, maakt Opdrachtgever dat kenbaar. De verwachting is dat Inschrijver hierover bereidheid toont actief mee te willen denken over wat een optimale bemensing is de project-activiteiten tot het best mogelijke resultaat te laten leiden.	
ICT083	83 Ja	7. Implementatie		Als onderdeel van de oplevering van de aangeboden dienstverlening dient een kwetsbaarheidscans uitgevoerd te worden en als rapport opgeleverd te worden aan Opdrachtgever. De kosten en uitvoering van een kwetsbaarheidscans mogen meegenomen worden in de Inschrijving. Het achteraf indien van een factuur is niet toegestaan. Inschrijver mag ook een gelijkwaardig en recent (niet ouder dan 6 maanden) rapport indienen.	
ICT087	87 Ja	8. Continuïteit, Veiligheid, Beschikbaarheid		Inschrijver dient te beschikken over een continuïteitsplan. Dit plan dient aan Opdrachtgever te worden verstrekt. Het continuïteitsplan dient helder uit te leggen op welke manier de continuïteit is gewaarborgd en dient richtlijnen, rollen en verantwoordelijkheden, procedures, communicatieprocessen en testbenaderingen te beschrijven voor de situaties waarin zich een calamiteit voordoet die de continuïteit van de dienstverlening bedreigt.	Gibit 2023 art. 10.3.i
ICT088	88 Ja	8. Continuïteit, Veiligheid, Beschikbaarheid		De Inschrijver houdt aantoonbaar alle data integer, betrouwbaar en beschikbaar. De daartoe genomen maatregelen dienen zowel de omgeving waar data zal worden verwerkt en opgeslagen, als de personen met toegang tot de data, elektronische verzending van data en het vervoer van data op draagbare media, af te dekken.	
ICT089	89 Ja	8. Continuïteit, Veiligheid, Beschikbaarheid		De Inschrijver en dienst mag geen informatie en persoonsgegevens vergaren zonder doelbinding vanuit Opdrachtgever. De toegestane, vergaarde gegevens moeten uitsluitend voor het gestelde doel gebruikt worden.	
ICT091	91 Ja	8. Continuïteit, Veiligheid, Beschikbaarheid		Patching dient door de Inschrijver binnen de door de Informatie BeveiligingsDienst (IBD) en het Nationaal Cyber Security Centrum (NCSC) gestelde termijn uitgevoerd te worden.	Gibit 2023 art. 10.12.iii

Eis	nummer_t mp	Eis nodig? Over- ruled	Thema	Beschrijving	In aanvulling / Afwijking op
ICT098	98 Ja	8. Continuïteit, Veiligheid, Beschikbaarheid		De Inschrijver laat periodiek (minimaal jaarlijks en na grote wijzigingen) onafhankelijk pentesten uitvoeren omv. vast te stellen of software veilig is en bekende risico's niet aanwezig zijn. Risico's die getoetst worden volgen hierbij uit de OWASP top 10 voor web applicaties en API koppelingen. Rapportages met bevindingen en de opvolging worden gedeeld met de CISO functie van de Opdrachtgever. Let op: een Pentest is geen geautomatiseerde kwetsbaarheden scan in deze context. Inschrijver zal ook periodiek kwetsbaarheden scan's uitvoeren, vanuit haar zelf of vanuit partners. Denk hierbij aan periodieke Nessus scan's (of vergelijkbaar) en controles van de richtlijnen forumstandaardisatie (internet.nl). Opdrachtgever behoudt zich wel het recht voor om zelf testen / scans te laten uitvoeren, in overleg met Inschrijver en op kosten van Opdrachtgever. In dat geval is een vrijwaringsovereenkomst van toepassing.	Gibit 2023 art. 10.15 en 10.16 en artikel 25.
ICT099	99 Ja	8. Continuïteit, Veiligheid, Beschikbaarheid		De Inschrijver hanteert t.a.v. alle beveiligingsafwijkingen een classificatie model met gehanteerde oplostijden, passend op het risico. Dit model wordt ter beschikking gesteld. Indien Opdrachtgever van mening is dat dit niet passend is, zal het door Opdrachtgever gehanteerde model leidend zijn. Dit classificatie model verschilt wezenlijk van dienstverleningsincidenten, in de zin dat mogelijke incidenten en mogelijke risico's een classificatie hoog kunnen krijgen.	
ICT101	101 Ja	8. Continuïteit, Veiligheid, Beschikbaarheid		De data laag mag niet gedeeld worden met derden, er moet logische scheiding zijn toegepast.	
ICT104	104 Ja	8. Continuïteit, Veiligheid, Beschikbaarheid		(Eventuele) security incidenten en (mogelijke) datalekken worden per ommekeer en uiterlijk binnen 24 uur aan Opdrachtgever gerapporteerd, conform gemaakte afspraken dan wel de Verwerkersovereenkomst. Het meldingsproces is hierbij gekoppeld aan risico inschatting en classificatie. De Inschrijver houdt voorts een overzicht bij van alle inbreuken. Dit overzicht bevat in elk geval de feiten en de (persoons)gegevens die het betreft.	
ICT106	106 Ja	9. Inschrijver - Certificering en Compliance		Inschrijver zal gedurende de looptijd van de overeenkomst beschikken over een ISO27001 of gelijkwaardige certificering. De Verklaring van Toepasselijkheid (VVT) mag hierbij geen relevante uitsluitingen kennen en de scope moet de af te nemen dienstverlening in de breedte afdekken. Bij inzet derden door Inschrijver geldt een doorzetverplichting op de maatregelen waarop Inschrijver op toeziet. Zowel kopie van het certificaat als de VVT dienen aan Opdrachtgever geleverd te worden.	
ICT107	107 Ja	9. Inschrijver - Certificering en Compliance		Opdrachtgever krijgt op verzoek inzage in audit bevindingen en opvolging hierop t.a.v. van alle onafhankelijke externe toetsingen en beschikbare assurance rapportages en security assessments relevant voor de dienstverlening. Desgewenst op basis van een NDA. Inzage ligt bij de CISO onder vertrouwelijkheid en behelst (niet uitputtend) DIGID, ISO9001, ISO27001, ISO27017, ISO27018, ISAE3402, Pentest resultaten etc.	

Eis	nummer_t mp	Eis nodig? Over- ruled	Thema	Beschrijving	In aanvulling / Afwijking op
ICT108	108 Ja	9. Inschrijver - Certificering en Compliance		Gedurende de looptijd van de overeenkomst beschikt Inschrijver over een ISAE 3402 Type 2 verklaring en levert deze jaarlijks aan Opdrachtgever. Middels de aangeleverde ISAE 3402 Type 2 verklaring worden de informatie- en organisatierisico's van Opdrachtgever door Inschrijver adequaat afgedekt. Aangezien de ISAE3402 vormvrij is, verwacht Opdrachtgever dat de volgende onderwerpen en risico's in het controle raamwerk zijn afgedekt: - Back-up en Restore resultaten van een jaarlijks uit te voeren hersteltest - Business Continuïteitsmanagement - Risicomanagement - Changemanagement - Toegangsbeveiliging en autorisaties - Logging en Monitoring - Incidentmanagement en response - Beheer kwetsbaarheden - Fysieke beveiliging Het niet voldoen op onderdelen of elementen is geen optie. Indien Opdrachtgever hiaten in de verklaring ziet, gaat Inschrijver akkoord met een terugkoppelingsgesprek waarin afspraken gemaakt worden om bij de volgende iteratie van de ISAE verklaring tot een hoger niveau te komen. Verbeteringen en opvolging worden op verzoek gedeeld met opdrachtgever als onderdeel van de service rapportage (SLA). Indien Opdrachtgever een ongekend hoog aantal Risico's in de verklaring ziet, kan dit alsnog tot uitsluitel van deelname leiden.	
ICT109	109 Ja	9. Inschrijver - Certificering en Compliance		Indien er sprake is van verwerking van persoonsgegevens in de cloud zal de Inschrijver voldoen aan de ISO27018 of vergelijkbaar. De beheersmaatregelen en management systematiek wordt onafhankelijk extern getoetst in opdracht van de Inschrijver. Het rapport krijgt Opdrachtgever ter inzage.	
ICT110	110 Ja	9. Inschrijver - Certificering en Compliance		Indien er sprake is van verwerking van bijzondere persoonsgegevens zal de Inschrijver voldoen aan de ISO27701 of vergelijkbaar. De beheersmaatregelen en management systematiek wordt onafhankelijk extern getoetst door de Inschrijver.	
ICT112	112 Ja	9. Inschrijver - Certificering en Compliance		De Inschrijver stelt overeenkomstig het “doorzetprincipe” vigerende wet- en regelgeving, beheer-, servicelevel - en beveiligingsafspraken en -maatregelen contractueel door naar ingezette derden. De inschrijver ziet hier actief op toe.	
ICT113	113 Ja	9. Inschrijver - Certificering en Compliance		De Opdrachtgever heeft het recht om dienstverlening en maatregelen (o.a. eventuele verwerkingsovereenkomsten) en best practices onafhankelijk te (laten) toetsen door een aantoonbaar gekwalificeerde IB/IT auditor en/of pentester. Dit audit recht is onbeperkt. De kosten voor inzet auditor en Inschrijver zijn voor de Opdrachtgever. Inzet uren van Inschrijver voor herstel afwijkingen zijn voor kosten van Inschrijver. Bevindingen en afwijkingen worden binnen gezamenlijk overeen te komen termijn hersteld en voortgang gerapporteerd.	