Programma van Eisen Integratievoorziening 2026





Auteur
Gemeente Bloemendaal en Heemstede

Datum
20-11-2026

Inhoud

1. Integratiefunctionaliteit 3
2. Betrouwbaarheid en foutafhandeling 4
3. Logging en monitoring 5
4. Beheer en configuratie 6
5. Servicemanagement en beheer 7
6. Beveiliging en Privacy 11
7. Beschikbaarheid, continuïteit en herstel 14
8. Architectuur, standaarden en interoperabiliteit 15
9. Implementatie, migratie en transitie 18
10. Documentatie en kennisoverdracht 21
11. Exit en portabiliteit 22
12. Performance en schaalbaarheid 24

Programma van Eisen

1. Integratiefunctionaliteit

Nr	Onderwerp	Omschrijving
IF - 01	Integratie-scenario's	De ICT-oplossing ondersteunt verschillende vormen van gegevensuitwisseling, waaronder minimaal: - tussen SaaS-applicaties onderling; - tussen SaaS-applicaties en on-premise applicaties, in beide richtingen; - met landelijke voorzieningen.
IF - 02	Synchrone en asynchrone gegevens-uitwisseling	De ICT-oplossing ondersteunt zowel synchrone als asynchrone gegevensuitwisseling.
IF - 03	API-integratie	De ICT-oplossing ondersteunt API-gebaseerde gegevensuitwisseling voor het beschikbaar stellen en afnemen van gegevens en functionaliteit.
IF - 04	Event-driven integratie	De ICT-oplossing ondersteunt event-driven gegevensuitwisseling, waarbij gebeurtenissen (events) kunnen worden gebruikt als trigger voor het beschikbaar stellen of verwerken van gegevens. Hierbij ondersteunt de ICT-oplossing, waar van toepassing, het gebruik van relevante open en gestandaardiseerde event- en notificatiestandaarden, waaronder NL GOV for CloudEvents.
IF - 05	Realtime en batch-verwerking	De ICT-oplossing ondersteunt zowel realtime als batchgewijze verwerking en uitwisseling van gegevens.
IF - 06	Routering	De ICT-oplossing ondersteunt het routeren van berichten en gegevens naar één of meerdere bestemmingen op basis van configureerbare voorwaarden en kenmerken.
IF - 07	Transformatie en translatie	De ICT-oplossing ondersteunt het transformeren en vertalen van gegevens tussen verschillende gegevensstructuren, formaten, standaarden en/of gegevensmodellen.
IF - 08	Publish/ subscribe	De ICT-oplossing ondersteunt een publish/subscribe-mechanisme waarmee afnemers zich kunnen abonneren op specifieke gegevens, berichten en/of gebeurtenissen.
IF - 09	Orchestratie	De ICT-oplossing ondersteunt het orkestreren van integratieprocessen waarbij meerdere applicaties, gegevensbronnen en/of voorzieningen in een vooraf bepaalde volgorde kunnen worden aangeroepen of aangestuurd.
IF - 10	Hergebruik en voorkomen	De ICT-oplossing ondersteunt het hergebruik van gegevens, berichten, events en integratiecomponenten voor meerdere afnemers. Gegevens die via het gegevensmagazijn

	point-to-point	beschikbaar zijn, kunnen gecontroleerd worden hergebruikt voor meerdere integraties en afnemers, zonder dat hiervoor afzonderlijke point-to-point-integraties per afnemer noodzakelijk zijn. De ICT-oplossing maakt het mogelijk om één bron, gegevens set of integratievoorziening gecontroleerd beschikbaar te stellen aan meerdere afnemers en ondersteunt daarmee het voorkomen van onnodige point-to-point-integraties.
IF - 11	Gegevens-magazijn	De ICT-oplossing ondersteunt een centraal gegevensmagazijn voor het gecontroleerd ontvangen, opslaan, synchroniseren, beschikbaar stellen en distribueren van gegevens ten behoeve van integraties en gegevensuitwisseling. Het gegevensmagazijn kan hierbij worden gebruikt in combinatie met verschillende integratiepatronen, waaronder API-gebaseerde, event-gebaseerde en legacy-/StUF-gebaseerde gegevensuitwisseling. De ICT-oplossing voorkomt leveranciersafhankelijkheid, onder andere bij het synchroniseren en controleren van gegevens .

2. Betrouwbaarheid en foutafhandeling

Nr	Onderwerp	Omschrijving
BF - 01	Controle en validatie	De ICT-oplossing controleert berichten en gegevens tijdens de verwerking op volledigheid en technische juistheid en ondersteunt het signaleren van geconstateerde afwijkingen. De semantische juistheid van gegevens valt primair onder de verantwoordelijkheid van de bronapplicatie.
BF - 02	Tijdigheids-controle	De ICT-oplossing ondersteunt configureerbare controles op de tijdigheid van berichten en gegevens en kan afwijkingen hierop signaleren.
BF - 03	Foutdetectie en foutafhandeling	De ICT-oplossing ondersteunt het detecteren, registreren en afhandelen van fouten tijdens de verwerking van berichten en gegevens.
BF - 04	Automatisch opnieuw aanbieden	De ICT-oplossing ondersteunt het automatisch opnieuw aanbieden van berichten bij tijdelijke verwerkings- of verbindingsfouten, op basis van configureerbare instellingen.
BF - 05	Buffering	De ICT-oplossing ondersteunt buffering van berichten en gegevens wanneer een ontvangend systeem tijdelijk niet beschikbaar is, zodat berichten en gegevens niet verloren gaan en na herstel gecontroleerd kunnen worden aangeboden.
BF - 06	Gecontroleerde herverwerking	De ICT-oplossing ondersteunt gecontroleerde herverwerking en her levering van berichten en gegevens. De verwerkingsstatus en eventuele her levering zijn inzichtelijk.

BF - 07	Afhandeling niet-verwerkbare berichten	De ICT-oplossing biedt de mogelijkheid om berichten die niet succesvol kunnen worden verwerkt afzonderlijk beschikbaar te stellen voor analyse en gecontroleerde herverwerking.
BF - 08	Wet- en regelgeving en normenkaders	De ICT-oplossing en de dienstverlening voldoen gedurende de looptijd van de overeenkomst aan de op de dienstverlening van toepassing zijnde wet- en regelgeving en relevante normenkaders en beveiligingsprincipes, waaronder de AVG, BIO, NIS2/Cbw. BIO of de ISO 27001/27002, aan de standaarden zoals benoemd in de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie en toegankelijkheidseisen zoals vastgelegd in EN 301 549/WCAG 2.1. Bij de inrichting en beveiliging van de ICT-oplossing worden, waar passend, Zero Trust-principes toegepast, waaronder expliciete verificatie (autorisatie, toegangsbeveiliging o.a. MFA, het gebruikte apparaat, locatie en risiconiveau), least privilege, beveiligde communicatie en monitoring. En de toepasselijke bepalingen van de Cyberbeveiligingswet.

3. Logging en monitoring

Nr	Onderwerp	Omschrijving
LM - 01	Centrale monitoring	De ICT-oplossing biedt een centrale voorziening voor het monitoren van de uitvoering en verwerking van integraties en biedt inzicht in de actuele werking en status van de integraties. Bij voorkeur kan vanuit een centrale voorziening direct worden doorgeschakeld naar de bijbehorende workflow in de backoffice.
LM - 02	Logging	De ICT-oplossing registreert gebeurtenissen en technische gegevens over de uitvoering en verwerking van integraties, waaronder ten minste: - de datum en tijd van de gebeurtenis; - de betrokken integratie, koppeling of interface; - bron en bestemming; - de verwerkingsstatus en het resultaat; - eventuele fouten, waarschuwingen en foutmeldingen; - relevante technische kenmerken van de verwerking, zoals bericht- of transactiekenmerken en verwerkingstijd.
LM - 03	Verwerkings-status	De ICT-oplossing maakt per integratie en verwerking inzichtelijk wat de actuele verwerkingsstatus is, waaronder ten minste of een verwerking succesvol is afgerond, is mislukt of nog in behandeling is.
LM - 04	Signalering	De ICT-oplossing ondersteunt configureerbare signaleringen en meldingen bij fouten, afwijkingen en andere relevante gebeurtenissen binnen integraties.
LM - 05	Zoeken en filteren	De ICT-oplossing biedt mogelijkheden om geregistreerde gebeurtenissen en technische gegevens te zoeken en te filteren op relevante kenmerken, waaronder ten minste periode, integratie, bron, bestemming en verwerkingsstatus.

LM - 06	End-to-end inzicht	De ICT-oplossing biedt inzicht in de verwerking van een bericht, gegevensuitwisseling of gebeurtenis over de verschillende stappen en componenten binnen een integratieketen, zodat de verwerking en eventuele fouten kunnen worden gevolgd en geanalyseerd.
LM - 07	Rapportage	De ICT-oplossing ondersteunt het genereren van rapportages over de werking en prestaties van integraties, waaronder ten minste aantallen verwerkingen, succesvolle en mislukte verwerkingen, fouten en verwerkingstijden over een door de gebruiker te selecteren periode.
LM - 08	Audittrail	De ICT - oplossing biedt een controleerbare audittrail van relevante gebeurtenissen en beheeractiviteiten. De audittrail kan niet achteraf door beheerders worden gewijzigd of verwijderd en bevat minimaal de actor (gebruiker of systeem), gebeurtenis, betrokken object of integratie, resultaat en datum en tijd. De audittrail blijft gedurende de door de opdrachtgever vastgestelde bewaartermijn beschikbaar. Leverancier stelt de opdrachtgever gedurende de overeengekomen bewaartermijn in staat de audittrail in te zien en te exporteren. Leverancier kondigt voorgenomen verwijdering tenminste 30 dagen vooraf aan en verstrekt op verzoek voor verwijdering een volledige, beveiligde en leesbare export, inclusief tijdstempels, gebruikersidentificaties en toelichting op de logvelden.

4. Beheer en configuratie

Nr	Onderwerp	Omschrijving
BC - 01	Rol- en tenant-gebaseerde autorisatie	De ICT-oplossing ondersteunt rolgebaseerde autorisatie, waarmee per gebruikersrol kan worden bepaald welke beheer-, configuratie- en inzageactiviteiten mogen worden uitgevoerd. Hierbij kunnen verschillende rechten worden toegekend aan onder meer functioneel beheerders, technisch beheerders en andere geautoriseerde gebruikers. De autorisaties kunnen per omgeving en per gemeente/tenant worden ingericht.
BC - 02	Scheiding van omgevingen	De ICT-oplossing beschikt over afzonderlijke omgevingen voor minimaal testen en productie, waarbij integraties, configuraties, API's en wijzigingen gecontroleerd kunnen worden getest voordat deze in productie worden gebracht. De testomgeving is zodanig gescheiden van de productieomgeving dat testen niet leidt tot ongecontroleerde gegevensuitwisseling met productie.
BC - 03	Scheiding tussen tenants	De ICT-oplossing ondersteunt meerdere gemeenten binnen één beheeromgeving en biedt daarbij een aantoonbaar afgeschermde scheiding tussen de afzonderlijke tenants. Gebruikers, configuraties, gegevens, integraties, logging en autorisaties van de verschillende gemeenten zijn onderling

		afgeschermd. Een gebruiker heeft uitsluitend toegang tot de tenants en informatie waarvoor deze gebruiker is geautoriseerd.
BC - 04	Versie- en wijzigings-beheer	De ICT-oplossing ondersteunt versie- en wijzigingsbeheer van integraties, API's en relevante configuraties. Wijzigingen worden geregistreerd, zodat inzichtelijk is welke wijziging, wanneer en door wie is uitgevoerd. De ICT-oplossing biedt de mogelijkheid om eerdere versies van configuraties te raadplegen en wijzigingen gecontroleerd terug te draaien.
BC - 05	Overbrengen van wijzigingen tussen omgevingen	De ICT-oplossing ondersteunt het gecontroleerd overbrengen van configuratie- en integratiewijzigingen van de acceptatieomgeving naar de productieomgeving. Hierbij kunnen wijzigingen in de acceptatieomgeving worden getest en gevalideerd voordat deze in productie worden doorgevoerd. Het overbrengen van wijzigingen naar productie is geautoriseerd en controleerbaar.
BC - 06	Configureer-baarheid	De ICT-oplossing ondersteunt het configureren van integraties, routeringen, transformaties en foutafhandeling zonder aanpassing van de onderliggende software. Deze werkzaamheden worden door de Inschrijver uitgevoerd, in afstemming en samenwerking met functioneel beheer van de opdrachtgever. De Inschrijver informeert functioneel beheer vooraf over voorgenomen wijzigingen en biedt inzicht in de uitgevoerde configuratiewijzigingen.
BC - 07	Testmogelijk-heden	De ICT-oplossing biedt mogelijkheden om integraties, configuraties, routeringen, transformaties en foutafhandeling in de acceptatieomgeving gecontroleerd te testen, zonder gevolgen voor de productieomgeving. Hierbij kunnen zowel succesvolle verwerkingen als fout- en uitzonderingssituaties worden getest.
BC - 08	Overzicht van integraties	De ICT-oplossing biedt een centraal en actueel overzicht van de ingerichte integraties en koppelingen. Per integratie kan ten minste inzicht worden verkregen in de betrokken systemen, interface, gegevensstroom, configuratie, status en afhankelijkheden. Bij voorkeur ook het overzicht exporteerbaar.

5. Servicemanagement en beheer

Nr	Onderwerp	Omschrijving
SB - 01	Technisch beheer door Inschrijver	De Inschrijver is gedurende de overeenkomst volledig verantwoordelijk voor het technisch beheer van de ICT-oplossing en de onderliggende infrastructuur. Dit omvat in ieder geval het technisch functioneren, monitoren, onderhouden, beveiligen, configureren, certificaten en actualiseren van de ICT-oplossing en het oplossen van technische storingen.

<table>
<tr><td>SB - 02</td><td>Functioneel beheer door opdrachtgever</td><td>De opdrachtgever is verantwoordelijk voor het functioneel beheer van de ICT-oplossing. De ICT-oplossing biedt de mogelijkheid om zelfstandig de functionele werking van integraties te monitoren en te beheren, waaronder het controleren van de verwerkingsstatus van integraties en berichten, het analyseren van functionele fouten en afwijkingen, het beheren van functionele configuraties en autorisaties en het uitvoeren van overige functionele beheeractiviteiten, zonder dat hiervoor tussenkomst van de Inschrijver noodzakelijk is. Hiertoe worden alle benodigdheden (opleiding, documentatie, toegang, etc) door inschrijver geleverd en bijgehouden. Zodat het functioneel beheer enkel in noodzakelijke incidentele gevallen onder begeleiding van inschrijver uitgevoerd kan worden.</td></tr>
<tr><td>SB - 03</td><td>Serviceniveaus en prioritering</td><td>De ICT-oplossing is 24 uur per dag, 7 dagen per week beschikbaar voor geautomatiseerde verwerking van integraties en gegevensuitwisseling, met uitzondering van vooraf overeengekomen onderhoudsvensters.

Voor technische ondersteuning geldt een regulier servicevenster op werkdagen van 08:00 tot 18:00 uur. Voor P1-incidenten dient er een piketdienst aanwezig te zijn voor na 18:00 uur inclusief weekenden en feestdagen.

Servicelevels bij een prioriteit:
<table><tr><th>Prioriteit</th><th>Maximale Reactietijd (binnen de Service Window)</th><th>Maximale Hersteltijd (binnen de Service Window)</th><th>Terugkoppeling</th></tr><tr><td>1</td><td>10 minuten</td><td>4 uur</td><td>Ieder half uur</td></tr><tr><td>2</td><td>4 uur</td><td>8 uur</td><td>Als Servicelevel Hersteltijd overschreden dreigt te worden</td></tr><tr><td>3</td><td>8 uur</td><td>16 uur</td><td>Als Servicelevel Hersteltijd overschreden dreigt te worden</td></tr></table>
De Inschrijver voldoet gedurende de looptijd van de overeenkomst aan de door de opdrachtgever vastgestelde minimale serviceniveaus voor onder meer beschikbaarheid, support, incidentafhandeling, responstijden en hersteltijden.</td></tr>
<tr><td>SB - 04</td><td>Certificaten-beheer</td><td>De Inschrijver is verantwoordelijk voor het beheer en tijdig vernieuwen van certificaten en sleutelmaterialen die noodzakelijk zijn voor het technisch functioneren en de beveiliging van de ICT-oplossing en de onderliggende infrastructuur.

Voor certificaten die onderdeel zijn van koppelingen met aangesloten applicaties of voorzieningen wordt per koppeling de verantwoordelijkheid voor aanvraag, beschikbaarstelling, installatie, configuratie, vernieuwing en verwijdering vooraf eenduidig vastgelegd tussen opdrachtgever, Inschrijver en de betreffende partij.

De ICT-oplossing ondersteunt het tijdig signaleren van het verlopen van certificaten die binnen de verantwoordelijkheid van de opdrachtgever of Inschrijver vallen. De Inschrijver</td></tr>
</table>

		informeert de opdrachtgever tijdig over certificaten waarvoor actie van de opdrachtgever of een aangesloten partij noodzakelijk is.
SB - 05	Wijzigingen door wet- en regelgeving	De Inschrijver zorgt ervoor dat de ICT-oplossing gedurende de looptijd van de overeenkomst blijft voldoen aan wijzigingen in toepasselijke wet- en regelgeving en relevante normenkaders, voor zover deze wijzigingen betrekking hebben op de bestaande functionaliteit van de ICT-oplossing. De hiervoor noodzakelijke aanpassingen aan de ICT-oplossing vallen binnen de dienstverlening en worden niet als meerwerk beschouwd. Indien naleving van nieuwe of gewijzigde wet- en regelgeving een fundamentele wijziging, uitbreiding of nieuwe functionaliteit vereist die geen onderdeel vormt van de bestaande functionaliteit van de ICT-oplossing, treden opdrachtgever en Inschrijver vooraf in overleg over de benodigde werkzaamheden en eventuele kosten. Indien de Inschrijver van mening is dat sprake is van een dergelijke situatie, onderbouwt hij dit vooraf.
SB - 06	Monitoring en signalering	De Inschrijver monitort de technische werking, beschikbaarheid en prestaties van de ICT-oplossing en signaleert en behandelt technische storingen en relevante afwijkingen conform de overeengekomen dienstverlening. De Inschrijver informeert de opdrachtgever tijdig over (dreigende) verstoringen die impact kunnen hebben op de beschikbaarheid of werking van de ICT-oplossing en over de voortgang van de afhandeling.
SB - 07	Onderhoud, updates en releases	De Inschrijver voert als onderdeel van de dienstverlening noodzakelijk technisch onderhoud, beveiligingsupdates, patches, upgrades en releases van de ICT-oplossing uit. Deze werkzaamheden vallen binnen de overeengekomen dienstverlening en worden niet als meerwerk beschouwd. De Inschrijver stelt de opdrachtgever een actuele releasekalender beschikbaar, met minimaal drie maanden vooruit inzicht in geplande releases en onderhoudswerkzaamheden. De Inschrijver informeert de opdrachtgever tijdig vooraf over de aard, planning en eventuele impact van wijzigingen die gevolgen kunnen hebben voor het gebruik, de beschikbaarheid of de werking van de ICT-oplossing. De Inschrijver voert gepland onderhoud en geplande wijzigingen zoveel mogelijk buiten de reguliere werktijden van de opdrachtgever uit. Indien werkzaamheden tijdens reguliere werktijden noodzakelijk zijn, stemt de Inschrijver dit vooraf af met de opdrachtgever. Voor spoedeisende beveiligingsupdates en andere noodzakelijke wijzigingen die niet vooraf kunnen worden gepland, informeert de Inschrijver de opdrachtgever zo spoedig mogelijk over de wijziging en de eventuele impact.

		De Inschrijver voert wijzigingen, updates en nieuwe releases zodanig uit dat bestaande integraties en configuraties behouden blijven en blijven functioneren, tenzij vooraf overeengekomen wijzigingen noodzakelijk zijn. De Inschrijver informeert de opdrachtgever tijdig over wijzigingen die gevolgen kunnen hebben voor bestaande integraties, configuraties, API's, events of gegevensuitwisseling.
SB - 08	Helpdesk en ondersteuning	De Inschrijver biedt gedurende de looptijd van de overeenkomst een Nederlandstalige helpdesk voor technische en functionele ondersteuning bij het gebruik en beheer van de ICT-oplossing. De helpdesk is het centrale aanspreekpunt voor het melden van incidenten, het stellen van vragen en het indienen van wijzigingsvoorstellen. De helpdesk registreert en volgt meldingen en verzoeken op en biedt de opdrachtgever inzicht in de status en afhandeling daarvan. De ondersteuning wordt ten minste telefonisch en via e-mail en/of een webportaal aangeboden. De helpdesk is op werkdagen bereikbaar van 08:00 tot 18:00 uur.
SB - 09	Rapportage en serviceoverleg	De Inschrijver rapporteert ten minste eenmaal per kwartaal over de geleverde dienstverlening en het behalen van de overeengekomen serviceniveaus. De rapportage bevat ten minste informatie over beschikbaarheid, incidenten, responstijden, hersteltijden en eventuele overschrijdingen van de overeengekomen serviceniveaus. De Inschrijver neemt ten minste eenmaal per kwartaal deel aan serviceoverleg met de opdrachtgever, waarin de dienstverlening, incidenten, prestaties, eventuele verbeterpunten en geplande ontwikkelingen worden besproken.
SB - 10	Incident-, probleem- en escalatie-management	De leverancier beschikt over een proces voor incident-, probleem- en escalatiemanagement (ITIL4) en is verantwoordelijk voor het registreren, classificeren, prioriteren, analyseren, opvolgen en oplossen van technische incidenten en structurele technische problemen binnen de overeengekomen serviceniveaus. De leverancier handelt incidenten af overeenkomstig de vastgestelde prioriteit en de daarbij behorende responstijden, hersteltijden en escalatieafspraken zoals gaat opgenomen worden in de SLA.

6. Beveiliging en Privacy

Nr	Onderwerp	Omschrijving
BP - 01	Authenticatie en autorisatie	De ICT-oplossing ondersteunt veilige authenticatie en autorisatie van gebruikers, beheerders, applicaties, serviceaccounts en andere technische accounts. Toegang wordt verleend op basis van de noodzakelijke rechten voor de betreffende rol, toepassing of integratie.
BP - 02	Authenticatie-protocollen en MFA	De ICT-oplossing ondersteunt voor gebruikers- en beheeraccounts Single Sign-On en federatieve authenticatie op basis van gangbare standaarden, waaronder SAML en/of OAuth 2.0/OpenID Connect. Alle gebruikers- en beheeraccounts zijn beveiligd met multi-factor authenticatie (MFA). Voor applicatie-, service- en technische accounts worden passende sterke authenticatiemethoden toegepast. Lokale accounts mogen deze beveiliging niet omzeilen. Eventuele nood accounts worden bij gebruik vooraf met de opdrachtgever volgens een overeengekomen procedure gebruikt, beveiligd en gemonitord.
BP - 03	Beveiliging van API's	De ICT-oplossing beveiligt via de API gateway ontsloten API's tegen onbevoegde toegang en misbruik. Hierbij worden ten minste authenticatie, autorisatie, versleutelde communicatie en bescherming tegen ongewenst of overmatig gebruik ondersteund. API's verstrekken uitsluitend gegevens waarvoor het aanroepende account is geautoriseerd. Relevante beveiligingsgebeurtenissen worden gelogd.
BP - 04	Secrets en sleutelmaterialen	De ICT-oplossing beschermt wachtwoorden, API-sleutels, tokens, certificaten, private keys en andere authenticatie- en sleutelmaterialen tegen onbevoegde toegang. Deze gegevens worden niet onversleuteld opgeslagen of opgenomen in logging.
BP - 05	Tenantisolatie	De ICT-oplossing waarborgt een aantoonbare beveiligde scheiding tussen de tenants. De scheiding omvat ook integraties, configuraties, back-ups en andere ondersteunende beheeromgevingen. Gebruikers, beheerders, applicaties en technische accounts kunnen uitsluitend toegang krijgen tot gegevens, integraties, configuraties, logging en andere informatie van de tenant waarvoor zij zijn geautoriseerd.
BP - 06	Beveiligings-testen	De Inschrijver laat de ICT-oplossing periodiek en bij relevante ingrijpende wijzigingen beoordelen op beveiligingskwetsbaarheden. Hierbij worden ten minste de internetbereikbare onderdelen, API's en relevante beheerinterfaces meegenomen. De Inschrijver informeert de opdrachtgever over de resultaten en opvolging van geconstateerde kwetsbaarheden. Daarnaast dient de opdrachtgever zelf alle verbindingen en technische beveiligingsmaatregelen te kunnen controleren.

BP - 07	Beveiligings-incidenten	De Inschrijver beschikt over een proces voor het detecteren, registreren, beoordelen en afhandelen van beveiligingsincidenten die betrekking hebben op de ICT-oplossing of de onderliggende infrastructuur. De Inschrijver informeert de opdrachtgever onverwijld over beveiligingsincidenten die gevolgen kunnen hebben voor de vertrouwelijkheid, integriteit of beschikbaarheid van de ICT-oplossing of de gegevens van de opdrachtgever en verstrekt daarbij informatie over de aard, impact en genomen of voorgenomen maatregelen.
BP - 08	Beveiligings-logging	De oplossing registreert beveiligingsrelevante gebeurtenissen, waaronder ten minste succesvolle en mislukte authenticatiepogingen, wijzigingen in autorisaties en beheerrechten, toegang tot en beheeractiviteiten met betrekking tot gegevens, API's, integraties en configuraties, wijzigingen in beveiligingsinstellingen en relevante beheeractiviteiten. Beveiligingsloggegevens zijn beschermd tegen onbevoegde toegang en kunnen gedurende de bewaartermijn niet achteraf worden gewijzigd of verwijderd door reguliere gebruikers of beheerders. De integriteit van de beveiligingsloggegevens kan gedurende de bewaartermijn worden gecontroleerd. Beveiligingsloggegevens zijn gedurende minimaal 12 maanden beschikbaar voor raadpleging en onderzoek. Indien een langere bewaartermijn voortvloeit uit toepasselijke wet- en regelgeving, een risicoafweging of het beleid van de opdrachtgever, geldt deze langere termijn.
BP - 09	Bescherming persoons-gegevens en vertrouwelijke gegevens	De oplossing biedt passende technische en organisatorische maatregelen voor de bescherming van persoonsgegevens en andere vertrouwelijke gegevens tegen verlies, onbevoegde toegang, wijziging of openbaarmaking. De oplossing ondersteunt het gecontroleerd (en bij voorkeur geautomatiseerd) verwijderen van persoonsgegevens en andere vertrouwelijke gegevens overeenkomstig de toepasselijke wet- en regelgeving en de door de opdrachtgever vastgestelde bewaartermijnen. In voorkomende gevallen moet kunnen worden afgeweken van deze vastgestelde bewaartermijnen.
BP - 10	EER, gegevens-verwerking en subverwerkers	De Inschrijver verwerkt en bewaart gegevens van de opdrachtgever uitsluitend binnen de EER. Verwerking buiten de EER is uitsluitend toegestaan indien wordt voldaan aan hoofdstuk V van de AVG. De Inschrijver maakt inzichtelijk in welke landen gegevens worden verwerkt en welke subverwerkers daarbij worden ingezet. De Inschrijver informeert de opdrachtgever tijdig vooraf over het voornemen om een subverwerker buiten de EER in te schakelen of bestaande verwerking door een subverwerker buiten de EER te wijzigen en vraagt

		hiervoor vooraf toestemming van de opdrachtgever. De Inschrijver verstrekt daarbij de informatie die nodig is om de voorgestelde verwerking en de daarbij getroffen waarborgen te kunnen beoordelen. Er moeten standaardcontractbepalingen voor het verwerken van de gegevens opgesteld en afgesloten worden.
BP - 11	Identity Provider en SSO	De oplossing ondersteunt authenticatie via de Identity Provider (IdP) van de opdrachtgever en Single Sign-On (SSO). De Inschrijver dient zorg te dragen voor een strikte scheiding tussen de identity providers (IdP) van de test- en productieomgevingen. Voor de testomgeving dient gebruik te worden gemaakt van een afzonderlijke Azure AD/Entra ID tenant, gescheiden van de productieomgeving. Deze scheiding moet technisch en organisatorisch worden geborgd, zodat authenticatie- en autorisatieprocessen in de test omgevingen geen invloed kunnen uitoefenen op productiegebruikers of -systemen. De SSO koppelingen dienen afzonderlijk te worden ingericht en getest.
BP - 12	Versleuteling	De ICT - oplossing ondersteunt versleutelde gegevensuitwisseling en versleutelde opslag van gegevens inclusief back-ups en configuratiegegevens waarvoor dit vanuit beveiligings- of privacyrisico's noodzakelijk is. Voor gegevensuitwisseling via netwerken wordt minimaal TLS toegepast, conform de actuele versie zoals gepubliceerd door Forum Standaardisatie. Daarnaast ondersteunt de ICT - oplossing IP-whitelisting, rate limiting en het gebruik van PKIoverheid-certificaten voor het beveiligen en authenticeren van gegevensuitwisseling.
BP - 13	Least Privilege	De oplossing ondersteunt het principe van least privilege en zero trust. Toegangs- en beheerrechten worden beperkt tot de rechten die noodzakelijk zijn voor de betreffende werkzaamheden of de uitvoering van de betreffende integratie. De oplossing ondersteunt het onderscheiden van beheer-, configuratie- en inzagerechten en het scheiden van beheerrechten van reguliere gebruikersrechten. De opdrachtgever kan de autorisaties van eigen gebruikers en functioneel beheerders beheren. Technische beheerrechten worden door de Inschrijver beheerd en uitsluitend toegekend aan daartoe geautoriseerde medewerkers van de Inschrijver. Beheerhandelingen zijn herleidbaar tot de uitvoerende persoon en worden gelogd.
BP - 14	Kwetsbaarheden en beveiligings-updates	De Inschrijver voert gedurende de looptijd van de overeenkomst periodiek kwetsbaarheidsbeoordelingen uit en zorgt voor tijdige opvolging van geïdentificeerde beveiligingskwetsbaarheden. Kritieke en ernstige kwetsbaarheden worden met prioriteit verholpen. Beveiligingsupdates en patches maken onderdeel uit van de dienstverlening.
BP - 15	Verwerkersover-eenkomst	Inschrijver maakt gebruik van de standaard Verwerkersovereenkomst Gemeenten van de VNG

BP - 16	Gemeentelijke ervaring	Leverancier heeft aantoonbaar minimaal twee jaar ervaring voor wat betreft integratie voorziening binnen de Nederlandse overheid en specifiek voor gemeenten.
BP - 17	Algoritmen	Bij gebruik van algoritmen moeten de rekenregels bekend worden gemaakt aan de gemeente.
BP - 18	Kunstmatige intelligentie (AI)	Bij gebruik van andere vormen van kunstmatige intelligentie moet bekend worden gemaakt met welke databases het systeem wordt getraind
BP - 19	Landelijke autorisaties	Landelijke autorisaties moeten standaard ingericht worden.
BP – 20	Verzoek tot inzage en download	De ICT – oplossing moet de mogelijkheid bieden om voor een verzoek om inzage de gegevens van een betrokkene te kunnen downloaden uit de applicatie op eenvoudige wijze.

7. Beschikbaarheid, continuïteit en herstel

Nr	Onderwerp	Omschrijving
BCH - 01	Beschikbaarheid	Voor de gegevens geldt een beschikbaarheid van minimaal 99,6%.
BCH - 02	Continuïteit	De Inschrijver treft maatregelen om de continuïteit van de ICT-oplossing en de daarmee gerealiseerde gegevensuitwisseling te waarborgen bij storingen, uitval van onderdelen en calamiteiten. Hierbij worden ten minste de integratie laag, API-gateway, gegevensmagazijn, integratieconfiguraties en gegevens- en berichtenstromen betrokken.
BCH - 03	Redundantie en beschikbaarheid kritieke componenten	De ICT-oplossing is zodanig ingericht dat uitval van afzonderlijke componenten niet leidt tot onnodige onderbreking van de dienstverlening of verlies van gegevens, berichten, integratieconfiguraties of andere voor de werking noodzakelijke informatie. Voor bedrijfskritische componenten worden passende redundantiemaatregelen toegepast.
BCH - 04	Herstel	De Inschrijver beschikt over gedocumenteerde en periodiek geteste herstelprocedures voor de ICT-oplossing en de onderliggende gegevens, configuraties, integraties en overige noodzakelijke informatie. Na herstel wordt gecontroleerd of de integratievoorziening en de daarmee samenhangende gegevensuitwisseling correct functioneren.
BCH - 05	Berichten na verstoring	De ICT-oplossing ondersteunt het gecontroleerd hervatten van gegevensuitwisseling na een verstoring. Hierbij worden berichten en gegevens die tijdens de verstoring niet konden worden verwerkt, waar nodig gebufferd en na herstel gecontroleerd opnieuw verwerkt. De ICT-oplossing voorkomt daarbij verlies en ongewenste dubbele verwerking van berichten en gegevens.

BCH - 06	Back-up	De Inschrijver maakt beveiligde back-ups van alle gegevens, configuraties, integraties en overige informatie die nodig zijn voor de werking en continuïteit van de ICT-oplossing. Hierbij gelden een maximale RPO van 4 uur en een maximale RTO van 8 uur, tenzij op basis van BCH-07 voor specifieke onderdelen anders is bepaald. Back-ups worden minimaal 30 dagen bewaard en afgestemd op de RPO, bewaartermijn en kritikaliteit van de onderdelen (waarbij een strengere frequentie of langere bewaartermijn prevaleert). De Inschrijver test periodiek de herstelbaarheid van de back-ups.
BCH - 07	RTO en RPO	De Inschrijver hanteert voor de ICT-oplossing overeengekomen Recovery Time Objectives (RTO) en Recovery Point Objectives (RPO). De RTO en RPO worden vastgesteld op basis van de kritikaliteit van de betreffende dienstverlening, integratie, gegevensstroom of component en opgenomen in afspraken van de opdrachtgever. De Inschrijver toont aan dat de aangeboden dienstverlening, back-upvoorzieningen en herstelprocedures de overeengekomen RTO en RPO ondersteunen.

8. Architectuur, standaarden en interoperabiliteit

Nr	Onderwerp	Omschrijving
ASI - 01	SaaS leveringsmodel	De ICT-oplossing wordt volledig als Software as a Service (SaaS) geleverd en online beschikbaar gesteld, waarbij de Inschrijver verantwoordelijk is voor het technisch beheer en onderhoud van de software en de onderliggende infrastructuur. De dienstverlening omvat alle benodigde software, hardware/infrastructuur en licenties die noodzakelijk zijn voor het functioneren van de ICT-oplossing. De Inschrijver is verantwoordelijk voor het technisch applicatiebeheer en het onderhoud van het softwareplatform en de onderliggende infrastructuur. De SaaS-dienst omvat ook de voor de dienstverlening benodigde connectiviteit met het internet. De Inschrijver zorgt voor voldoende netwerkcapaciteit en performance voor het functioneren van de ICT-oplossing.

		De onderliggende cloudhosting voldoet aan de toepasselijke standaarden en normen voor cloudhosting, waaronder HAVEN, voor zover het toepassingsgebied van deze standaard van toepassing is.
ASI - 02	Open en Common Ground-conforme architectuur	De ICT-oplossing ondersteunt een open en Common Ground-conforme architectuur en ondersteunt voor de binnen de ICT-oplossing gerealiseerde gegevensuitwisselingen de daarvoor door de VNG vastgestelde Common Ground-standaarden.
ASI - 03	Centraal API-beheer	De API-gateway ondersteunt het centraal registreren, beheren, publiceren en versiebeheer van API's voor verschillende gemeentelijke applicaties en voorzieningen. De ICT-oplossing ondersteunt het gelijktijdig beheren en beschikbaar stellen van meerdere versies van een API, zodat wijzigingen gecontroleerd kunnen worden doorgevoerd en bestaande afnemers gedurende een overgangsperiode gebruik kunnen blijven maken van een bestaande API-versie.
ASI - 04	Monitoring en logging API's	De ICT-oplossing ondersteunt centrale monitoring en logging van via de API-gateway ontsloten API's. Hierbij kan inzicht worden verkregen in het gebruik, de beschikbaarheid, prestaties en fouten van API's en API-verkeer.
ASI - 05	Digi-koppeling	De ICT-oplossing ondersteunt de voor de gemeentelijke gegevensuitwisseling relevante koppelvlakken en specificaties van Digikoppeling, waaronder waar van toepassing REST API, WUS, ebMS en relevante berichtstandaarden en beveiligingsprofielen. De ondersteuning sluit aan op de eisen en specificaties die gelden voor de betreffende landelijke voorziening, overheidsorganisatie of gegevensuitwisseling.
ASI - 06	Flexibele aansluiting en ontkoppeling	De ICT-oplossing maakt het mogelijk om nieuwe samenwerkingspartijen en afnemers op een gestandaardiseerde en gecontroleerde wijze aan te sluiten en bestaande partijen te ontkoppelen, zonder onnodige aanpassingen aan bestaande integraties.
ASI - 07	EUDI-wallet	De ICT-oplossing ondersteunt de mogelijkheid om voorzieningen voor de Europese digitale identiteit (EUDI-wallet) en daarmee samenhangende vertrouwensdiensten en voorzieningen via gestandaardiseerde koppelingen te integreren. De ICT-oplossing maakt het mogelijk om een generieke voorziening of broker voor EUDI-walletfunctionaliteit via de integratie laag te verbinden met gemeentelijke applicaties, API's en andere relevante voorzieningen, zonder dat hiervoor afzonderlijke point-to-point-integraties met deze systemen noodzakelijk zijn.
ASI - 08	Toekomst-bestendigheid	De ICT-oplossing is gedurende de beoogde looptijd van de overeenkomst geschikt voor de gemeentelijke integratiebehoefte en kan worden onderhouden, geactualiseerd en uitgebreid zonder dat een ingrijpende

		vervanging van de ICT-oplossing noodzakelijk is. De ICT-oplossing ondersteunt daarbij de ontwikkeling van nieuwe integratiepatronen, standaarden, API's en event-gebaseerde gegevensuitwisseling.
ASI - 09	Interoperabiliteit	De ICT-oplossing ondersteunt interoperabiliteit overeenkomstig de relevante architectuurprincipes en standaarden van NORA en GEMMA. De oplossing maakt gegevensuitwisseling mogelijk tussen verschillende SaaS-applicaties, on-premise applicaties, landelijke voorzieningen en andere relevante systemen, ongeacht de gebruikte Inschrijver of technologie. De oplossing ondersteunt hierbij de voor de betreffende gegevensuitwisseling relevante open standaarden, koppelvlakken en protocollen, waaronder waar van toepassing NL API Strategie, API Design Rules, Digikoppeling en StUF.
ASI - 10	Multitenant architectuur	De oplossing ondersteunt het gebruik door meerdere gemeenten binnen één ICT-omgeving, waarbij de gegevens, configuraties, integraties, autorisaties en beheeractiviteiten van de afzonderlijke gemeenten van elkaar logisch zijn gescheiden. De leverancier toont door middel van architectuurdocumentatie en onafhankelijke beveiligingstesten aan dat toegang tussen tenants wordt voorkomen.
ASI - 11	API-gateway	De ICT-oplossing biedt API gateway-functionaliteit en kan als centrale API-gateway voor de gemeente worden ingezet voor het centraal beschikbaar stellen, ontsluiten, beheren, beveiligen, monitoren en documenteren van API’s. De API-gateway ondersteunt het centraal toepassen van toegangs-, beveiligings- en gebruiksbeleid op de ontsloten API’s, waaronder waar relevant authenticatie, autorisatie, rate limiting en throttling.
ASI - 12	Open standaarden	De ICT-oplossing ondersteunt het gebruik van open en breed geaccepteerde standaarden voor gegevensuitwisseling, integratie, beveiliging en interoperabiliteit. De ICT-oplossing voldoet aan de voor de betreffende functionaliteit relevante landelijke standaarden. De oplossing maakt daarbij geen onnodige afhankelijkheid van Inschrijversspecifieke standaarden of technologieën noodzakelijk.
ASI - 13	Gegevens- en bericht-formaten	De oplossing ondersteunt gangbare gegevens- en berichtformaten, waaronder JSON en XML. Waar relevant ondersteunt de oplossing ook andere formaten, zoals platte tekst (plain text), CSV of door de gemeente gebruikte specifieke berichtformaten. Zoals opgenomen in de standaardenlijst die onderdeel uitmaakt van dit Programma van Eisen.

ASI - 14	Bestaand landschap en transitie naar moderne integratie	De ICT-oplossing ondersteunt de relevante integratiestandaarden, protocollen en berichtformaten die binnen het bestaande gemeentelijke applicatie- en integratielandschap worden gebruikt, waaronder waar van toepassing StUF en aan StUF gerelateerde koppelvlakken. De ICT-oplossing ondersteunt daarnaast moderne, open en gestandaardiseerde integratiepatronen, waaronder API-gebaseerde en event-gebaseerde gegevensuitwisseling. StUF wordt daarbij ondersteund voor het behouden en gecontroleerd migreren van bestaande legacy-integraties en wordt niet als uitgangspunt gehanteerd voor nieuwe integraties wanneer een passend modern en open alternatief beschikbaar is. De ICT-oplossing ondersteunt een gefaseerde overgang van bestaande legacy-integraties naar moderne, open en gestandaardiseerde integratiepatronen.

9. Implementatie, migratie en transitie

Nr	Onderwerp	Omschrijving
IMT - 01	Implementatie-plan	De Inschrijver stelt een integraal implementatieplan op voor de inrichting en ingebruikname van de ICT-oplossing. Het plan beschrijft minimaal de implementatiefasen, planning, activiteiten, afhankelijkheden, verantwoordelijkheden van Inschrijver en opdrachtgever, benodigde technische en functionele inrichting, test- en acceptatieactiviteiten, opleiding en kennisoverdracht, risico's en mitigerende maatregelen en de voorbereiding op ingebruikname en beheer. Het implementatieplan bevat een onderbouwde planning waaruit blijkt dat de volledige migratie van de bestaande integratieplatformen naar de ICT-oplossing en de daaropvolgende uitfasering van de bestaande integratieplatformen kan worden afgerond (zie aanbestedingsdocument voor de datum) Het implementatieplan houdt rekening met de bestaande integratievoorzieningen, het gegevensmagazijn, de API gateway, API- en eventgebaseerde integraties, bestaande legacy-/StUF-integraties en de inrichting van meerdere gemeenten/tenants.
IMT - 02	Migratie van bestaande integraties	De Inschrijver ondersteunt de gecontroleerde migratie van bestaande integraties, koppelingen, configuraties en relevante gegevens vanuit de huidige integratievoorzieningen naar de nieuwe ICT-oplossing.

		De migratie omvat zowel bestaande API- en moderne integraties als legacy-/StUF-integraties. Per te migreren integratie wordt vooraf vastgesteld welke functionaliteit, configuratie, gegevensstromen, afhankelijkheden en eventuele transformaties moeten worden overgenomen of opnieuw ingericht. De Inschrijver legt de migratieaanpak en de status van de migratie vast en zorgt dat de opdrachtgever inzicht heeft in de voortgang en resterende afhankelijkheden.
IMT - 03	Gefaseerde overgang	De overgang van de bestaande integratieplatformen naar de ICT-oplossing wordt gefaseerd en gecontroleerd uitgevoerd, waarbij integraties gecontroleerd kunnen worden gemigreerd en in gebruik genomen. Waar noodzakelijk ondersteunt de ICT-oplossing een tijdelijke periode waarin bestaande en nieuwe integratievoorzieningen naast elkaar functioneren. De Inschrijver borgt dat gedurende deze overgang de gegevensuitwisseling en bedrijfsprocessen zo veel mogelijk ononderbroken kunnen worden voortgezet. De volledige migratie van de bestaande integratieplatformen naar de ICT-oplossing, inclusief de ingebruikname van de gemigreerde integraties en de uitfasering van de bestaande integratieplatformen, moet uiterlijk (zie aanbestedingsdocument voor datum) zijn afgerond. De Inschrijver houdt bij de fasering rekening met afhankelijkheden tussen integraties, applicaties, landelijke voorzieningen, API's, events, legacy-/StUF-koppelingen en het gegevensmagazijn. Er moet een totaaloverzicht gegenereerd kunnen worden (bij voorkeur in een centrale voorziening), waarin factoren als logging, autorisatie en authenticatie tijdens de overgangsfase met zowel berichten via StUF als API's worden gemonitord.
IMT - 04	Testen en acceptatie	De Inschrijver stelt een test- en acceptatieplan op en voert de noodzakelijke technische en functionele tests uit in samenwerking met de opdrachtgever. De tests omvatten minimaal de werking van integraties, API's, events, gegevensuitwisseling, transformaties, foutafhandeling, logging en monitoring en, waar relevant, de werking van het gegevensmagazijn en de aansluiting op legacy-/StUF-integraties. Migraties worden voorafgaand aan ingebruikname gecontroleerd en gevalideerd. De ingebruikname vindt plaats nadat de overeengekomen acceptatiecriteria zijn behaald.
IMT - 05	Terugval-scenario	Voor iedere migratiefase en de ingebruikname van de ICT-oplossing beschikt de Inschrijver over een vooraf

		vastgesteld en getest terugvalscenario. Het scenario beschrijft de voorwaarden, verantwoordelijkheden en maatregelen voor het gecontroleerd terugkeren naar de bestaande situatie indien de nieuwe integratievoorziening niet voldoet aan de overeengekomen acceptatiecriteria of leidt tot een onaanvaardbare verstoring van de dienstverlening. Het terugvalscenario wordt afgestemd op de overeengekomen RTO/RPO en continuïteitseisen.
IMT - 06	Migratie-planning en afhankelijk-heden	De Inschrijver stelt in samenwerking met de opdrachtgever een gedetailleerde migratieplanning op waarin per migratiefase en integratie minimaal de betrokken systemen, afhankelijkheden, benodigde werkzaamheden, testmomenten, acceptatiecriteria, geplande ingebruikname en eventuele tijdelijke voorzieningen zijn opgenomen. De planning houdt rekening met afhankelijkheden tussen integraties, applicaties, landelijke voorzieningen, API's, events, legacy-/StUF-koppelingen en het gegevensmagazijn. Wijzigingen in de migratieplanning worden tijdig afgestemd met de opdrachtgever.
IMT - 07	Kennisover-dracht	De Inschrijver verzorgt voorafgaand aan ingebruikname voldoende kennisoverdracht aan medewerkers van de opdrachtgever voor het uitvoeren van het functioneel beheer van de ICT - oplossing. De kennisoverdracht omvat minimaal het beheren en monitoren van integraties, API's, events, autorisaties, logging en configuraties en het analyseren en opvolgen van functionele fouten en afwijkingen. De Inschrijver levert daarnaast de voor technisch beheer benodigde documentatie en draagt het technisch beheer gedurende de overeenkomst uit volgens de overeengekomen dienstverlening.
IMT - 08	Transitie	De leverancier dient een concreet transitieplan op te leveren voor de gefaseerde migratie van bestaande StUF-koppelingen naar API-gebaseerde gegevensuitwisseling, inclusief planning, migratiestrategie, risicoanalyse, testaanpak, continuïteit en borging van informatiebeveiliging en privacy. Na de transitie moeten data en verbindingen die niet meer actief zijn, vernietigd dan wel beëindigd worden, waarbij wel rekening wordt gehouden met de Selectielijst indien van toepassing.
IMT - 09	Overgangs-kosten	De implementatie en ingebruikname van de nieuwe integratievoorziening mogen niet leiden tot dubbele kosten voor de opdrachtgever. Dit betekent dat de facturatie voor de ICT-oplossing mag worden gestart op het moment van ingebruikname. Reeds betaalde

		functionaliteiten, licenties, koppelingen en diensten mogen niet opnieuw in rekening worden gebracht.

10. Documentatie en kennisoverdracht

Nr	Onderwerp	Omschrijving
DK - 01	Taal	Alle documentatie met betrekking tot de ICT-oplossing wordt beschikbaar gesteld in de Nederlandse taal.
DK - 01	Actuele documentatie	De Inschrijver levert en onderhoudt actuele functionele, technische en beheerdocumentatie van de ICT-oplossing en de daarin gerealiseerde integraties. De documentatie wordt gedurende de looptijd van de overeenkomst actueel gehouden en beschikbaar gesteld aan de opdrachtgever. Bij relevante wijzigingen in de ICT-oplossing, configuratie, integraties of architectuur wordt de documentatie bijgewerkt. De documentatie is zodanig opgesteld en bijgehouden dat deze gedurende en bij beëindiging van de overeenkomst bruikbaar is voor het beheer, onderhoud, migratie, continuering of vervanging van de ICT-oplossing door de opdrachtgever of een opvolgende Inschrijver.
DK - 02	Integratie-documentatie	De Inschrijver legt de ingerichte integraties, koppelingen en relevante configuraties vast en houdt deze documentatie actueel. De documentatie bevat minimaal de betrokken systemen, gegevensstromen, interfaces, API's, events, routeringen, transformaties, afhankelijkheden en relevante configuratie-instellingen. Voor zover van toepassing worden ook gebruikte standaarden, protocollen, berichtformaten en relevante beveiligings- en autorisatie-instellingen vastgelegd. Bij relevante wijzigingen wordt de documentatie bijgewerkt.
DK - 03	Beheerdocu-mentatie en werkinstructies	De Inschrijver levert documentatie en werkinstructies die de opdrachtgever in staat stellen het functioneel beheer van de ICT-oplossing uit te voeren. De documentatie beschrijft minimaal het monitoren en beheren van integraties, API's, events, autorisaties, logging en configuraties en het analyseren en opvolgen van functionele fouten en afwijkingen.
DK - 04	Wijzigings-documentatie	De Inschrijver documenteert relevante wijzigingen aan de ICT-oplossing, configuraties, integraties, API's, events en technische inrichting.

		De documentatie bevat minimaal de aard en aanleiding van de wijziging, de gewijzigde onderdelen, eventuele afhankelijkheden en relevante gevolgen voor beheer, beveiliging en gegevensuitwisseling.
DK - 05	Architectuur- en technische documentatie	De Inschrijver levert in afstemming met de Opdrachtgever de actuele (tijdens implementatie en houdt het actueel tijdens de looptijd van de overeenkomst) architectuur- en technische documentatie van de ICT-oplossing en de inrichting daarvan voor de opdrachtgever. De documentatie beschrijft minimaal de relevante componenten, onderlinge afhankelijkheden, gegevensstromen, integratiepatronen, API-gateway, gegevensmagazijn, koppelingen met externe voorzieningen en de inrichting van de afzonderlijke gemeenten/tenants. De documentatie maakt inzichtelijk hoe de oplossing technisch is ingericht en hoe de verschillende onderdelen met elkaar samenhangen.
DK - 06	Kennis-overdracht	De Inschrijver verzorgt gedurende de implementatie en bij relevante wijzigingen voldoende kennisoverdracht aan medewerkers van de opdrachtgever om het functioneel beheer van de ICT-oplossing zelfstandig te kunnen uitvoeren. De kennisoverdracht omvat minimaal het beheren en monitoren van integraties, API's, events, autorisaties, logging en configuraties en het analyseren en opvolgen van functionele fouten en afwijkingen. De Inschrijver stemt de vorm en inhoud van de kennisoverdracht af op de rollen en verantwoordelijkheden van de betrokken medewerkers.

11. Exit en portabiliteit

Nr	Onderwerp	Omschrijving
EP - 01	Kennis- en informatieover-dracht	De Inschrijver draagt bij beëindiging van de dienstverlening de benodigde kennis en informatie over aan de opdrachtgever of opvolgende Inschrijver om de ICT-oplossing te kunnen migreren, continueren of vervangen. De overdracht omvat minimaal de relevante functionele en technische documentatie, configuratie-informatie, integraties, API's, events, gegevensstromen, afhankelijkheden en beheerinformatie.

		De Inschrijver werkt gedurende de exitperiode mee aan kennisoverdracht en beantwoording van vragen die noodzakelijk zijn voor een gecontroleerde overgang.
EP - 02	Continuïteit tijdens exit	De Inschrijver blijft gedurende de overeengekomen exitperiode verantwoordelijk voor de continuïteit, beschikbaarheid en beveiliging van de dienstverlening totdat de overdracht en uitfasering gecontroleerd zijn afgerond. De Inschrijver werkt mee aan de gefaseerde overgang naar de opdrachtgever of opvolgende Inschrijver en voorkomt dat de dienstverlening, gegevensuitwisseling of gegevensbeschikbaarheid als gevolg van de exit onnodig wordt onderbroken. De overeengekomen RTO- en RPO-eisen blijven gedurende de exitperiode van toepassing, tenzij hierover vooraf schriftelijk andere afspraken zijn gemaakt.
EP - 03	Verwijdering en aantoonbaar-heid van gegevens	Na beëindiging van de dienstverlening verwijdert de Inschrijver de gegevens van de opdrachtgever, inclusief eventuele kopieën, overeenkomstig de overeengekomen bewaartermijnen en toepasselijke wet- en regelgeving. De Inschrijver verstrekt de opdrachtgever een schriftelijke verklaring waaruit blijkt welke gegevens zijn verwijderd, op welke wijze en op welk moment de verwijdering heeft plaatsgevonden. Als gegevens vanwege technische of wettelijke verplichtingen niet direct uit back-ups kunnen worden verwijderd, beschrijft de Inschrijver hoe deze gegevens ontoegankelijk worden gemaakt en wanneer zij definitief worden verwijderd.
EP - 04	Exitplan	De Inschrijver stelt op verzoek van de opdrachtgever een exitplan op voor een gecontroleerde beëindiging van de dienstverlening en overdracht naar de opdrachtgever of een opvolgende Inschrijver. Het exitplan beschrijft minimaal de activiteiten, verantwoordelijkheden, planning, benodigde informatie, overdracht van gegevens, configuraties, integraties, API-definities, documentatie en kennis, en de wijze waarop de continuïteit van de dienstverlening tijdens de overgang wordt geborgd. Het exitplan en de bijbehorende exit verplichtingen die voldoen aan de op de overeenkomst van toepassing verklaarde GIBIT 2025, artikel 29. Het exitplan houdt rekening met de verschillende gemeenten/tenants, de integratielaag, het gegevensmagazijn, de API gateway, API- en eventgebaseerde integraties en legacy-/StUF-integraties.

EP - 05	Export en portabiliteit	De ICT-oplossing maakt het mogelijk om gedurende en bij beëindiging van de overeenkomst de voor continuering of migratie relevante informatie te exporteren in een bruikbaar en gangbaar formaat. Dit omvat ten minste: - gegevens uit het gegevensmagazijn; - integraties en integratieconfiguraties; - API-definities en relevante API-configuraties; - eventdefinities en relevante configuraties; - routeringen, transformaties en andere relevante integratieconfiguraties; - relevante logging en auditinformatie; - documentatie en overige informatie die noodzakelijk is voor continuering of migratie. De geëxporteerde informatie moet door de opdrachtgever of een opvolgende Inschrijver kunnen worden gebruikt voor beheer, migratie, continuering of vervanging van de integratievoorziening.

12. Performance en schaalbaarheid

Nr	Onderwerp	Omschrijving
PS - 01	Schaalbaarheid	De ICT-oplossing is schaalbaar en kan meegroeien met toenemende aantallen gebruikers, applicaties, integraties, API-verzoeken, berichten, events, gegevensvolumes en tenants. De ICT-oplossing ondersteunt uitbreiding van de capaciteit zonder dat hiervoor een fundamentele wijziging van de architectuur of vervanging van de ICT-oplossing noodzakelijk is.
PS - 02	Verwerkings-capaciteit	De ICT-oplossing ondersteunt de verwerking van de voor de opdrachtgever relevante volumes aan gegevens, berichten, API-verzoeken en events. De oplossing kan deze verwerkingsvolumes verwerken zonder dat dit leidt tot een onaanvaardbare vermindering van de werking of prestaties van de integratievoorziening. De Inschrijver specificeert de beschikbare verwerkingscapaciteit van de aangeboden oplossing, waaronder minimaal de maximale en gegarandeerde throughput (requests per seconde) en het aantal gelijktijdige verbindingen (concurrency), onder vermelding van de omstandigheden en uitgangspunten waaronder deze capaciteit geldt.

		De Inschrijver toont aan dat de aangeboden capaciteit aansluit op de verwachte belasting en groei van de opdrachtgever en beschrijft hoe de capaciteit gedurende de looptijd kan worden opgeschaald.
PS - 03	Piekbelasting en gelijktijdige verwerking	De oplossing ondersteunt piekbelastingen en gelijktijdige verwerking van meerdere integraties, API-verzoeken, berichten en events. De oplossing ondersteunt maatregelen om verwerkingscapaciteit en prestaties tussen tenants en integraties beheersbaar te houden. Een hoge belasting binnen één tenant, integratie, API of gegevensstroom mag niet leiden tot een onaanvaardbare vermindering van de prestaties of beschikbaarheid van andere tenants, integraties of gegevensstromen.
PS - 04	Verwerkingsperformance	De oplossing levert voor synchrone, realtime en asynchrone gegevensuitwisseling prestaties die passen bij het betreffende integratiescenario en de overeengekomen serviceniveaus. De oplossing ondersteunt tijdige verwerking van API-verzoeken, berichten en events en voorkomt onnodige vertraging in de gegevensuitwisseling.