Programma van Eisen

<Ti

Gemeente Bergen op Zoom

Inleiding

Algemeen

De gemeente Bergen op Zoom heeft een verzameling van eisen en wensen ten aanzien van een mogelijke oplossing. In het Programma van Eisen zijn alle minimumeisen en uitvoeringsvoorwaarden opgenomen waar u aan moet voldoen om de opdracht te kunnen uitvoeren. Alle minimumeisen en uitvoeringsvoorwaarden zijn knock-out criteria.

Op het moment dat u de inschrijving indient, gaat u akkoord met alle eisen en voorwaarden die aan de opdracht worden gesteld, inclusief wijzigingen naar aanleiding van de Nota's van Inlichtingen. Het niet voldoen aan een eis kan uitsluiting betekenen van de verdere aanbestedingsprocedures.

Organisatie

Bergen op Zoom is een gemeente in Noord-Brabant met ca. 70.000 inwoners. De gemeente bestaat uit de kernen Bergen op Zoom, Halsteren, Lepelstraat en een aantal buurtschappen. Met ruim 650 medewerkers zijn we een middelgrote en slagvaardige gemeente. Samen werken we aan uitdagende maatschappelijke en organisatorische vraagstukken voor de inwoner. Meer informatie over de gemeente Bergen op Zoom is te vinden op www.bergenopzoom.nl

Beschrijving opdracht

Inleiding

Beschrijf kort de aanleiding van het vraagstuk vanuit het advies.

Beknopte inhoud van de opdracht

Beschrijf kort het gewenste resultaat vanuit het advies.

Programma van Eisen

Leverancier:	
Algemene eisen	
1.	Leverancier gaat akkoord met de Gemeentelijke Inkoopvoorwaarden GIBIT 2025.
2.	Leverancier gaat akkoord met de Gemeentelijke ICT-kwaliteitsnormen 2024-1.
3.	Leverancier voldoet aan de normen van de BIO en de Algemene verordening gegevensbescherming (AVG) in huidige situatie en toekomstige aanpassingen, zoals BIO 2.0 en Cyberbeveiligingswet.
4.	Leverancier voldoet en blijft voldoen aan de Wet Modernisering Elektronisch Bestuurlijk Verkeer en Wet Digitale Toegankelijkheid.
5.	Leverancier is ISO-27001 gecertificeerd.
6.	Leverancier beschikt over een verklaring van toepasselijkheid (VVT).
7.	Leverancier gaat akkoord met de verwerkingsovereenkomst (VWO) vanuit de gemeente, gebaseerd op de Informatiebeveiligingsdienst (VNG), als deze van toepassing is.
8.	Het Forum voor Standaardisatie is op deze PvE van toepassing.
Contract	
1.	De levering, implementatie en beheer van alle in de inschrijving opgenomen onderdelen zijn opgenomen in het prijzenblad en alle onderdelen zijn toonbaar tijdens een demonstratie. Hetgeen getoond in de demo's is hetgeen dat in productie is genomen.
2.	Het systeem is (in opeenvolgende versies) minimaal de contractperiode beschikbaar in de markt en wordt door de opdrachtnemer actief onderhouden op het gebied van security patches, wettelijke wijzigingen en functionele updates.
3.	De beschikbaarheid en bruikbaarheid van het systeem wordt door de opdrachtnemer gegarandeerd tijdens de contractperiode.
4.	Opdrachtnemer garandeert te allen tijde expliciet compliance van onderaannemers, hostingpartijen en gelieerde partners aan de overeengekomen afspraken met Opdrachtgever en is daarbij zelf volledig verantwoordelijk.
5.	In de prijs is support (helpdesk en/of ondersteuning op afstand) en bug afhandeling inbegrepen.
6.	Er worden geen aanvullende kosten in rekening gebracht voor updates en upgrades (uitgezonderd is aanvullende functionaliteit).
7.	Onderwerpen die niet zijn opgenomen in de uitvraag, waarvan leverancier weet dat deze benodigd zijn om te voldoen aan deze opdracht, dienen in de prijs te zijn verdisconteerd en mogen achteraf niet in rekening worden gebracht.
Informatie	
• Informatiebeveiliging	
1.	Opdrachtnemer levert en implementeert het systeem met een koppeling met AAD op basis van SAML 2.0 Connect ten behoeve van MFA en SingleSignOn opdat het gemeentelijke wachtwoordbeleid kan worden afgedwongen. Identiteiten worden verstrekt door de gemeente vanuit Microsoft Azure AD. • Het systeem moet voor het authenticeren van medewerkers in alle ondersteunde applicaties kunnen koppelen met SAMLv2 compatible Identity Providers, zoals ADFS, zowel on-premise als in de cloud. Alle (SaaS) applicaties koppelen wij met Azure AD voor autorisatie.

2.	Opdrachtnemer hanteert een duidelijk patchschema om alle componenten (zoals firmware, operating systems, applicaties) van de voor de oplossing dient actueel te houden om verbeteringen door te voeren en bekende fouten op te lossen.
3.	De laatste (beveiligings-)patches zijn geïnstalleerd en deze worden volgens een patchmanagement-proces doorgevoerd.
4.	Kritische beveiligingsupdates worden binnen 24 uur na uitgifte geïnstalleerd en beschikbaar gesteld in het systeem.
5.	Opdrachtnemer zorgt ervoor dat de gemeente geen last heeft van onwenselijk gedrag van andere klanten van opdrachtnemer (bijv. spamming vanuit eenzelfde IP-adres).
6.	Opdrachtnemer zorgt ervoor dat netwerkverkeer tussen verschillende omgevingen niet kan worden onderschept door andere klanten van opdrachtnemer die actief zijn binnen de systeemomgeving van opdrachtnemer.
7.	Opdrachtnemer voorkomt dat gebruik van gedeelde componenten door andere klanten van opdrachtnemer in de infrastructuur de performance bij de gemeente bedreigen.
8.	Bij het opslaan van wachtwoorden dient hashing en salting te worden gebruikt.
9.	Bij het openbaar actief maken van documenten dienen inzichtelijke metagegevens te worden weggenomen.
10.	Beperk het gebruik van emailverkeer vanaf (externe) servers of cloudomgevingen. Dit zorgt ervoor dat er geen aanpassingen gemaakt moeten worden in het SPF-record. Sluit aan bij de mailfunctionaliteit van Exchange Online. Voor Exchange Online wordt gebruik gemaakt van het SPF-record include:spf.protection.outlook.com. Een SPF-record is een DNS-record dat aangeeft welke mailservers gemachtigd zijn om e-mail te verzenden namens een domein.
Back-up & Restore	
1.	De gemeente gebruikt back-up en recovery om de gevolgen van de uitval en/of het verlies van informatie te minimaliseren.
2.	Dataverlies wordt beperkt tot maximaal 24 uur. De maximaal toelaatbare hoeveelheid gegevensverlies noemen we RPO (Recovery Point Objective).
3.	De hersteltijd in geval van incidenten bedraagt maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen. De maximaal toelaatbare hersteltijd noemen we RTO (Recovery Time Objective).
4.	De back-ups van alle gemeentelijke informatie, software en besturingssystemen (en instellingen) wordt bewaard, zodat de computerbesturingssystemen, applicaties en informatie volledig hersteld kunnen worden in geval van een calamiteit (zowel bij ICT-leverancier als niet ICT-leverancier). Dit wordt bereikt met behulp van een combinatie van kopieën, incrementele back-ups, differentiële back-ups en transactielogboeken en systeem baselines om te kunnen voldoen aan de maximale RPO en RTO.
5.	De frequentie van back-ups wordt bepaald door de volatiliteit van de gegevens. De bewaartermijn voor reservekopieën wordt bepaald door het kritieke karakter van de gegevens en wetgeving. De frequentie en bewaartermijnen dienen in overeenstemming met de proces- en applicatie eigenaar afgestemd te worden. De afdeling I&A faciliteert dit op basis van hetgeen afdelingen in hun BCM hebben opgenomen en waar I&A bij betrokken is.
6.	We hanteren de 3-2-1 regel voor back-up en restore waarbij onderstaande geregeld is: o Minstens drie versies van een back-up moeten worden bewaard, op tenminste twee verschillende opslagmedium, waarvan er 1 op een andere fysieke plek bewaard moet worden; o Er dient minimaal één volledige back-up te worden opgeslagen in een veilige, off-site locatie. Een off-site locatie dient een veilige ruimte in een apart gebouw van de gemeente te zijn of een locatie van een off-site storage-leverancier; o Zorg dat tenminste één back-up niet online benaderbaar is en beschermd wordt tegen veranderingen (air-gapped);

	o Back-ups worden dagelijks gecontroleerd.
7.	Het back-up proces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.
8.	Alle gemeentelijke informatie welke staat op werkstations, laptops of andere draagbare apparaten moeten worden opgeslagen op een afgeschermde beheerde omgeving om back-up mogelijk te maken.
9.	Documenteren en up2date houden van de volledige back-up voorziening en recovery procedures. Dit resulteert in plannen voor back-up, testen, recovery en registreren van loggegevens. Daarin komen alle essentiële gegevens, rollen en taken terug om een hersteloperatie uit te kunnen voeren conform de continuïteitsvereisten.
10.	Data in SaaS-applicaties dient ook te voldoen aan de BIO maatregelen en leverancier kan aantonen dat hieraan voldaan wordt.
11.	Er zijn geteste ICT-procedures voor back-up en recovery.
12.	De back-up en recovery procedures moet worden getest conform de documentatie en deze moet regelmatig worden bijgewerkt om rekening te houden met nieuwe technologie, veranderingen in het bedrijf, en de migratie van toepassingen naar alternatieve platforms.
13.	Recovery procedures moeten minimaal op jaarbasis worden getest.
14.	Van back-up en recovery activiteiten en de verblijfplaats van de media wordt een logboek bijgehouden.
15.	De back-up media worden vernietigd in overeenstemming met het beleid omtrent behandeling van digitale media van de gemeente.
16.	Voor de toegang tot back-ups wordt (onder regie van de afdeling I&A) versleutelingstechnologie toegepast. De gemeente ziet toe op de uitvoering van deze beveiligingsmaatregel in termen van autorisatie, toegangssleutels en sleutelbeheer.
17	Back-up en recovery moet voldoen aan AVG-wetgeving.
18	Back-up en recovery valt niet onder de archiefwet.
Opslaglocaties	
1.	De opslag van data vindt plaats binnen de Europese Economische Ruimte (EER). Het is niet toegestaan gebruik te maken van beheerdiensten van partijen gevestigd buiten de EER en/of gebruik te maken van ontwikkeldiensten van partijen gevestigd buiten de EER.
2.	De fysieke locaties van waar het systeem wordt gehost is beveiligd tegen toegang door onbevoegden. De locatie is adequaat – minimaal naar marktstandaarden - beveiligd tegen onheil van buitenaf, waaronder in ieder geval weersomstandigheden, vandalisme en terrorisme.
Kwetsbaarheden	
1.	Opdrachtnemer dient gebruik te maken van een hardeningsproces zodat alle ICT-componenten zijn gehard tegen aanvallen. Hardenen van systemen bestaat uit verschillende stappen om een gelaagde bescherming te bieden. Met behulp van antivirus, -spyware, -spam en -phishing software, regelmatig installeren van de laatste patches van opdrachtnemer, het uitschakelen van onnodige software en diensten leidt tot een beter beveiligd systeem dat moeilijk door kwaadwillenden is te misbruiken. Opdrachtnemer levert bewijsmiddelen op m.b.t. genoemde tests.
3.	Situaties waarin meer dan normale kwetsbaarheden (high/high) of risico's aanwezig zijn, dienen onmiddellijk (binnen 24 uur) gemeld te worden aan en besproken met de gemeente.
SIEM/SOC	
1.	Opdrachtnemer dient, indien hij (pogingen tot) ongeautoriseerde toegang tot de systeemomgeving signaleert, alle noodzakelijke maatregelen te nemen teneinde de eventuele schade tot een minimum te beperken en herhaling te voorkomen. De (poging tot)

	ongeautoriseerde toegang, alsmede alle getroffen maatregelen, worden direct aan de gemeente gerapporteerd.
2.	Opdrachtnemer kan aansluiten op SIEM/SOC oplossing gemeente, zijnde MS Defender, nog nader in te richten.
Registeren en archiveren	
1.	Het systeem voldoet aan de geldende Archiefwet en eventuele toekomstige aanpassingen van de Archiefwet met de daaruit voortvloeiende regelingen 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 gecreëerd.
2.	De in het systeem opgeslagen data blijven toegankelijk gedurende de looptijd van de overeenkomst, e.e.a. conform dit Programma van Eisen en wensen, behoudens conform protocol vernietigde data en dienen voor het verstrijken van de looptijd van de overeenkomst geëxporteerd te worden conform de op dat moment geldende eisen.
3.	Het moet mogelijk zijn om informatie tussentijdig uit het systeem te halen, deze te kopiëren, verplaatsen, exporteren en te vernietigen.
4.	Het systeem moet ingericht kunnen worden op basis van zowel de TMLO (oude te migreren gegevens) als de MDTO (gegevens t.a.v. nieuwe informatieobjecten)
5.	Bergen op zoom hanteert de Selectielijst 2020 voor het selecteren van te bewaren en te vernietigen informatie. Informatie opgeslagen in het systeem moet voorzien kunnen worden van een bewaartermijn. Na afloop van de bewaartermijn, moet de informatie automatisch uit de applicatie verwijderd kunnen worden. Van de vernietigde informatie moet een overzicht in Excel gegenereerd kunnen worden. Permanent te bewaren informatie moet uit de applicatie geëxporteerd kunnen worden in een CSV-bestand. Het gaat hierbij niet alleen om de bestanden, maar ook om de vastgelegde metadata per informatieobject.
6.	Om informatie vindbaar, beschikbaar, leesbaar, interpreteerbaar, betrouwbaar en toekomstbestendig te maken en te houden gebruikt de gemeente Bergen op Zoom het DUTO-raamwerk. (DUTO=Duurzaam Toegankelijke Overheidsinformatie). Het systeem dient ingericht te worden op basis van het DUTO-raamwerk. Als bijlage is het DUTO procesmodel toegevoegd.
Data	
1.	Met behulp van het aangeboden systeem wordt data geproduceerd of gemuteerd. Deze gegevens zijn en blijven eigendom van de gemeente. In het geval dat deze gegevens niet op systemen van de gemeente worden opgeslagen geldt het volgende: Ongeacht waar deze gegevens opgeslagen worden, bij opdrachtnemer of een van zijn onderaannemers, hetzij on premise, hetzij in de cloud, de gegevens zijn eigendom van en database technisch toegankelijk voor het uitlezen van de data voor de gemeente (bij voorkeur via een API koppeling of anders een sql-dump). Deze omschrijving bevat minimaal de volgende items: ▪ Welke gegevens betreft het? ▪ Logisch en technisch datamodel: ontologie, entiteiten en relaties, tabellen, constraints, wijze van opslag, tevens: onder welke jurisdictie valt de opslag? ▪ Metadata ▪ Gegevenswoordenboek ▪ Definities ▪ Frequentie van levering ▪ Beschrijving berichtenverkeer

2.	De gemeente blijft te allen tijden eigenaar van alle gegevens. Toegang tot gegevens zal altijd kosteloos zijn.
3.	Gegevens mogen nooit zonder toestemming worden gebruikt door of gedeeld met derden.
4.	Pas toe leg uit standaarden worden toegepast: Pas toe leg uit' standaarden (verplicht) | Forum Standaardisatie.
Artificial Intelligence (AI)	
1.	De gemeente wenst algoritmes op een verantwoorde wijze in te zetten. Leverancier voldoet bij het aanbieden van een algoritme en/of Artificial Intelligence aan de Europese AI-Verordening (AI-Act) en gaat akkoord met de *Bijlage Y Contractbepalingen AI toepassingen*. Ook wanneer gedurende de looptijd van het contract algoritme en/of Artificial Intelligence van toepassing wordt in de geleverde dienst, verklaart leverancier aan de Europese AI-Verordening (AI-Act) en *Bijlage Y Contractbepalingen AI toepassingen* te voldoen.
2.	Indien het systeem een generatieve AI-toepassing of integratie van generatieve AI-modellen in de software heeft, dient leverancier inzicht te geven in hoe gebruikersdata wordt gebruikt, opgeslagen en gedeeld door middel van een DPIA (Data Protection Impact Assessment). De DPIA wordt als onderdeel van de aanbesteding als bijlage meegeleverd. Aanvullend wordt een IAMA geleverd door de leverancier wanneer implicaties van mensenrechten kunnen optreden.
3.	Indien het algoritme een bepalende invloed heeft in een besluit richting personen onderbouwt de leverancier in hoeverre dit wel of niet het geval is.
4.	Persoonsgegevens en Bedrijfsgevoelige gemeentelijk data worden in beginsel niet gebruikt. Indien niet anders kan, worden persoonsgegevens en bedrijfsgevoelige gemeentelijke data geanonimiseerd. Data wordt niet gebruikt voor trainingsdoeleinden.
5.	Integratie zoals API's en een eventuele datapipeline zijn voorzien van privacy beschermingsmaatregelen i.g.v. persoonsgegevens volgens BIO.
6.	Datakwaliteit is inzichtelijk (kwaliteit van data is bepalend voor accuraatheid van resultaat van AI) door middel van de mogelijkheid om data te classificeren.
7.	Logging is ingeregeld van het gebruik en van het AI-systeem zelf.
8.	Indien er sprake is van gebruikskosten: kostenbeheersing is ingericht, continue monitoring van de kosten, kostenplafond ingesteld.
9.	CI/CD omgeving voor continue monitoring van de performance AI-toepassing is ingericht.
10.	SAE3000 SOC2 verklaring is gegeven. Met deze verklaring wordt het ontwerp en de operationele effectiviteit van de beveiligings-, risico- en controlepraktijken aangetoond.
11.	NEN 7510 informatiebeveiliging indien van toepassing
12.	Sovereign Cloud SCS Standards (NORA) Sovereign Cloud Standards | One platform — standardized, built and operated by many is afgegeven
13.	Prompt invoer: zero trust principces zijn toegepast en least-priveleges toegang. LLM moet behandeld worden als een trusted user om de invloed van een kwaadwillende zoveel mogelijk in te perken.
14.	Strikte dataverbruik-limieten (rate limits) zijn ingesteld op de context window van AI. Instellen van API-rate limits en het inzichtelijk maken van de gebruikte hardware-resources ter voorkoming Denial-of-Service.
15.	Software plugins zijn zoveel mogelijk ingeperkt als het gaat om input data. Ook moet men ervoor zorgen dat er voldoende verificatiemethoden toegepast zijn.
16.	Verificatiestappen door medewerker zijn toegevoegd. LLM (of AI-agent) mag niet zelf kunnen bepalen waar het toegang toe heeft, eerst moeten verificatiestappen uitgevoerd worden voordat applicatie/bron gebruikt en aangesloten wordt.

17.	Input van data gegeven door de gebruiker of output data mag niet gebruikt worden voor training van een generatief AI-model, bijv. een Large Language model. Tenzij hier toestemming voor is gegeven.
18.	Wanneer een eigen AI-systeem wordt opgezet, sla de gebruikte data op in een afgescheiden omgeving voor data en modellen.
19.	Communicatie met het AI-systeem vindt plaats via API van leveranciers.
Audits en testen	
1.	Een onafhankelijke externe expert voert minstens één keer per jaar een beveiligingscontrole uit op het product van de leverancier en deelt de auditresultaten op aanvraag met de klant. U kunt op eerste verzoek de volgende informatie aanleveren aan de gemeente: de externe auditor de frequentie van auditing, wanneer de laatste audit werd uitgevoerd en de manieren waarop de gemeente op verzoek inzichten in resultaten kan hebben.
2.	Opdrachtnemer laat minimaal jaarlijks door een onafhankelijk externe expert een privacy/legal review uitvoeren, toetsend op privacywaarborgen zoals dataminimalisatie, privacy by design, security by design, etc, waarbij de resultaten op verzoek met de gemeente worden gedeeld.
3.	Penetratietests dienen periodiek uitgevoerd te worden (minimaal één (1) maal per jaar) inclusief verslaglegging aan de gemeente binnen 2 weken na afronding van de test.
Beheer en Onderhoud	
• Ontwikkeling	
1.	Wanneer er nieuwe functionaliteiten worden ontwikkeld binnen de kaders van de aanbesteding, dan maken deze automatisch deel uit van het geïntegreerde systeem.
2.	Opdrachtnemer faciliteert naast de productie-omgeving een volledig ingerichte en representatieve test- /acceptatieomgeving, inclusief alle in dit Programma van Eisen en wensen geëiste en later toegevoegde koppelingen op verzoek van de opdrachtgever.
3.	Opdrachtnemer beschrijft hoe de inrichting in de test-/acceptatieomgeving gelijk gemaakt kan worden aan de productieomgeving. Eventuele kosten voor het gelijk maken zijn inbegrepen in de prijsopgave. De beschrijving wordt geleverd als onderdeel van het implementatietraject.
4.	De inrichting in de test-/acceptatieomgeving dient op verzoek van de gemeente ververst te worden zonder meerkosten. De testomgeving moet na het indienen van een verzoek uiterlijk binnen 5 werkdagen ververst zijn.
5.	De test-/acceptatieomgeving en de productieomgeving zijn gescheiden en autonoom. De test-/acceptatieomgeving dient minimaal op werkdagen, tijdens kantooruren beschikbaar te zijn. Deze omgevingen maken onderdeel uit van de jaarlijkse all-in prijs.
6.	Alle wijzigingen worden door opdrachtnemer altijd eerst getest voordat deze in productie worden genomen en worden via wijzigingsbeheer doorgevoerd. De wijzigingen worden niet eerder in productie genomen dan dat de nieuwe release aantoonbaar zonder problemen de testfase is doorlopen.
Autorisaties	
1.	Het systeem voorziet in een goede scheiding tussen functioneel applicatiebeheer, superusers en gebruikers. Alle rechten moeten op basis van rollen/gebruikersgroepen worden toegekend (RBAC). Het aantal rollen/gebruikersgroepen is niet aan een maximum gebonden.
2.	Inzichtelijk is hoe vaak door wie ingelogd wordt in het systeem.
3.	De applicatie bevat, indien van toepassing, de mogelijkheid om een fijnmazige autorisatiestructuur in te richten, zodat de informatiebeveiliging zorgvuldig geborgd is. De applicatie beschikt hiervoor over een zelf te configureren rechtenstructuur, waarin in ieder geval geautoriseerd kan worden op basis van:

	▪ gebruikersgroepen en individuen ▪ rollen/functies ▪ organisatie eenheden ▪ activiteiten (zoals het aanmaken/ontwerpen van een nieuw proces, het wijzigen of vernietigen van een proces, goedkeuren en publiceren van processen, en raadplegen van processen) ▪ het aanmaken, wijzigen en verwijderen: ▪ instructies ▪ risico's, kansen en beheersmaatregelen
4.	Rollen en rechten van zowel opdrachtnemer (technisch beheer) als de gemeente (functioneel en applicatiebeheerders) zijn inzichtelijk, middels RBAC. Er dient op geen enkele wijze sprake te zijn van inlogmogelijkheden door opdrachtnemer of diens voor deze opdracht in te zetten derden (backdoor) waar de gemeente niet van op de hoogte is. Toegang tot het systeem gaat altijd na overleg en goedkeuring vooraf. Het aantal rollen/gebruikersgroepen is niet aan een maximum gebonden.
5	• Autorisaties dienen middels een beheerinterface gebruiksvriendelijk te kunnen worden geconfigureerd. • De opdrachtnemer heeft een actieve rol in de invulling van de autorisatiematrix en biedt ondersteuning bij de inrichting van role based access control.
6.	• Het is mogelijk om configuraties in rollen en rechten te stapelen, waardoor het onder andere mogelijk is om gebruikers te autoriseren op basis van verschillende rollen voor meerdere functies en in groepen toe te kennen. Hiervoor wordt Hello-ID gebruikt als IAM oplossing. Opdrachtnemer kan autorisaties hierop aansluiten.
7.	• User provisioning wordt geautomatiseerd conform eis Beveiliging (voorgaande eis). Er zal geen LDAP-koppeling worden gebruikt. Bij voorkeur wordt geen gebruik gemaakt van scripting.
Functioneel beheer	
1.	Dagelijkse functionele beheertaken kunnen worden uitgevoerd, zonder dat dit invloed heeft op de werking van het systeem voor de overige gebruikers en op andere ICT-oplossingen. Gebruikers kunnen ingelogd blijven en volledig gebruik blijven maken van het systeem tijdens dagelijkse functionele beheertaken.
Support	
1.	Gebruikers en beheerders worden door Opdrachtnemer voorzien van alle benodigde documentatie in de Nederlandse taal (indicatie B2 niveau) (incl. alle technische documenten) en eventuele hulpmiddelen.
2.	De opdrachtnemer beschikt over een Nederlandstalige helpdesk voor zowel technische en functionele ondersteuning. De helpdesk is het centrale punt voor het melden van incidenten, het stellen van vragen, indienen van wijzigingsvoorstellen en geeft informatie/inzicht in de afhandeling daarvan.
Rapportages en logging	
1.	Logging dient te voldoen aan alle onderstaande maatregelen afkomstig uit de BIO: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. • Een logregel bevat minimaal: ○ (a) de gebeurtenis; ○ (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; ○ (c) het gebruikte apparaat; ○ (d) het resultaat van de handeling;

	○ (e) een datum en tijdstip van de gebeurtenis. • Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden. Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang. ▪ Er is een overzicht van logbestanden die worden gegenereerd. ▪ Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd. ▪ Er is een (onafhankelijke) interne audit procedure die minimaal halfjaarlijks toetst op het ongewijzigd bestaan van logbestanden. ▪ Oneigenlijk wijzigen of verwijderen van loggegevens of pogingen daartoe worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten. Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.
2.	Het is voor de gemeente mogelijk om zelfstandig en real-time binnen de applicatie inzicht te krijgen in het gebruik van het product op organisatieniveau en andere inzichten die nodig zijn om gebruik en risico's te monitoren. NB. Verwijzing naar logging of een andere applicatie hiervoor is niet voldoen aan deze eis. De software dient zelf over logging te beschikken.
3.	De logging die het product biedt is direct/real-time in te zien en eenvoudig te exporteren naar gangbare formaten (.csv en/of .json).
4.	Opdrachtnemer biedt inzicht in de rapportagemogelijkheden
Soft- en Hardware	
• Het systeem	
1.	Het door opdrachtnemer aangeboden systeem betreft een SaaS-oplossing, waarbij het beheer door de leverancier (opdrachtnemer) wordt uitgevoerd. Daarnaast beheert opdrachtnemer koppelingen als onderdeel van de SaaS-oplossing en draagt zorg voor benodigd contact met derden hierover.
2.	Het aangeboden systeem bevat geen maatwerkfunctionaliteiten. Indien toch een bepaalde functionaliteit specifiek voor deze aanbesteding is ontwikkeld, dan wordt deze in de eerstvolgende release opgenomen als standaardfunctionaliteit van het systeem.
3.	Als de (cloud)dienst kan worden benaderd door een browser geldt dat de (cloud)dienst op basis van een gangbare en ondersteunde browser Microsoft Edge (Chromium) juist, volledig en optimaal kan worden gebruikt, onafhankelijk van de onderliggende hardware en zonder toevoeging van extra plug-ins of add-ons.
4.	Het systeem beschikt over een webbased userinterface (dus géén Citrix of gelijkwaardige omgeving) zonder beperking van functionaliteit. Het systeem moet de laatste HTML versie ondersteunen binnen één (1) jaar nadat deze is uitgebracht. Er zijn ook geen verdere instellingen of installaties (op het client device en/of in de webbrowser) benodigd, met uitzondering van client certificaten.
5.	De gebruikersinterface van het systeem is volledig Nederlandstalig.
6.	Het is mogelijk per gebruiker meerdere sessies gelijktijdig te openen en te bewerken
Architectuur	
• Integratie en koppelingen	
1.	Indien de gemeente gedurende de looptijd van de overeenkomst nieuwe geautomatiseerde koppelingen wenst te realiseren, zal opdrachtnemer daarvoor per koppeling vooraf een marktconforme prijsopgave verstrekken. De gemeente behoudt zich het recht voor om de

	marktconformiteit van de prijsopgave onafhankelijk te laten toetsen. Indien blijkt dat de prijsopgave naar mening van de gemeente niet marktconform is, treden partijen in overleg om tot een gezamenlijke oplossing te komen.
2.	Alle koppelingen met andere omgevingen en systemen moet plaatsvinden via versleutelde verbindingen en opdrachtnemer zorgt voor een topologietekening.
Data en conversie	
1.	Alle documenten moeten opgeslagen worden in OOXML-formaat (en opvolgende versies), alle documenten voor archivering en ontsluiting via internet in .pdf of .pdf/A-1 formaat.
2.	Opdrachtnemer verzorgt de conversie-werkzaamheden, inclusief proefconversies bij implementatie, inclusief de actuele data (Zoals stamdata, beginbalans, openstaande posten en vaste activa etc.), vanuit het huidige pakket. Vooraf, gedurende het implementatietraject, stelt opdrachtnemer met de gemeente vast welke keuzes gemaakt moeten worden over de gegevens/inrichting die geconverteerd moeten worden en welke implicaties de gemaakte keuzes hebben.
3.	De gegevens uit het huidig gebruikte pakket dienen voor zover van toepassing, dit ter beoordeling van de gemeente, volledig en automatisch mee te worden genomen bij de implementatie van het nieuwe systeem.
4.	Opdrachtnemer maakt bij de conversie gebruik van controles met een duidelijke verslaglegging (waaronder tenminste verwerkings- en mutatieverslag, signaal- c.q. uitvallijst) waaruit blijkt dat alle aangeleverde gegevens daadwerkelijk correct zijn overgezet naar het nieuwe systeem (opdrachtnemer verleent op verzoek medewerking aan IT audit).
5.	Alle betrokken systeemcomponenten zijn ontworpen en getest op het voorkomen van inbreuken op beschikbaarheid, integriteit en vertrouwelijkheid.
6.	De software moet moderne beveiligingsmaatregelen zoals authenticatie en autorisatie ondersteunen in haar API's (Oauth2) zoals vastgelegd in de Pas Toe Leg Uit lijst.
Exit strategie	
1.	Opdrachtnemer draagt aan het einde van de looptijd van de overeenkomst alle data (incl. metadata) uit het systeem in een origineel en duurzaam bestandsformaat, kosteloos over aan de gemeente. Na bevestiging van de gemeente van succesvolle overdracht worden alle data van de systemen van de gemeente vernietigd. Opdrachtnemer levert een verklaring van vernietiging binnen de afgesproken termijn in het re-transitieplan. Hierin wordt minimaal vermeld welke informatie is vernietigd, op welke wijze de vernietiging heeft plaatsgevonden, de omvang van de data (tb, mb etc.) en de bevestiging dat de vernietiging volledig is uitgevoerd.
2.	Opdrachtnemer verleent in de periode vóór het verstrijken van de uiterste looptijd van de overeenkomst c.q. de beëindiging daarvan zijn volledige medewerking aan een migratie naar een andere partij. Hiertoe krijgt de gemeente een omschrijving van een re-transitieplan minimaal in de lijn van PON (Platform Outsourcing Nederland) en de beschikking over alle databases (incl. gegevensmodel-beschrijving), gegevens, en configuratiebestanden, wachtwoorden, etc., incl. alle eventuele bijbehorende documentatie, zodanig dat de gemeente of een derde partij namens haar alle gegevens (incl. content), configuraties, etc. kan migreren. Bovendien zal opdrachtnemer hierbij desgevraagd aanvullende dienstverlening verzorgen zodanig dat de continuïteit van de dienstverlening en bedrijfsvoering van de gemeente niet in gevaar komt, uitgezonderd beperkte downtime (hooguit enkele uren) tijdens feitelijke (deel)migratie en bij problemen. Deze medewerking vindt plaats o.b.v. een nadere offerteaanvraag, tegen (maximaal) de uurtarieven zoals aangeboden in de inschrijving.
3.	Bij einde van de overeenkomst dient u kosteloos, tijdig en actief de overdracht aan de gemeente of een opvolgende leverancier te faciliteren.

	Als het contract gedurende de looptijd van het project beëindigd , wordt, dient leverancier alle techniek, inhoud en documentatie zo over te dragen dat een andere leverancier de opdracht kan overnemen.
Implementatie en projectsturing	
• Implementatie	
1.	Ten behoeve van de voorbereiding van de implementatie levert de leverancier een implementatieplan aan dat volgens GIBIT 2025 H6 minimaal gericht is op: • De wijze waarop het implementatietraject is georganiseerd (inclusief fasering, planning, verslaglegging en projectmanagement). De implementatieplanning neemt u op als bijlage bij het implementatieplan • De werkverdeling en verdeling van verantwoordelijkheden en tijdsindicatie per functie, waaronder de van de gemeente te verwachten inzet en beschikbaarheid.
• Projectsturing	
1.	De leverancier benoemt vanaf de start van de implementatie een Nederlandstalige projectleider (en indien van toepassing ook projectleden) die de regie over de implementatie uitvoert in samenspraak met de opdrachtgever.
2.	Tot de oplevering van de implementatie en tijdens de nazorg, zal de projectleider vanuit de leverancier betrokken zijn, samenwerken met en het aanspreekpunt zijn voor de gemeente.
Service Level Agreement *(onderdelen nader te bepalen in samenspraak met opdrachtgever)*	
1.	De leverancier beschrijft in de aangeboden support en SLA's: • Hoe en in welke frequentie actief gemonitord en gerapporteerd wordt aan opdrachtgever op het gebied van: • Omvang en gebruik van de applicatie; • Soort gebruik van de applicatie; • Piektijden en periodes met beperkt gebruik; • Inzicht in continuïteit en beschikbaarheid; • Open en afgehandelde incidenten, changes en problems; • Performance van de systemen • De leverancier beschrijft hoe de continuïteit en performance wordt gegarandeerd en rapporteert hierover eens per maand, hierin opgenomen de volgende onderwerpen: • Continue monitoring van de server, de verbinding en de applicaties; • Updaten en beveiliging van de serversoftware; • Back-ups; • Bereikbaarheid en responstijd; • Uptime garantie • Het opnemen van video's, foto's en afbeeldingen beïnvloedt niet de laadsnelheid van de site. • Leverancier dient een Nederlandssprekende en schrijvende supportorganisatie te hebben, die technische support en hulp via de helpdesk biedt.
4.	Opdrachtnemer voegt een SLA toe in zijn inschrijving. Met deze SLA moet worden voldaan aan de minimumeisen opgenomen in dit Programma van Eisen. In de SLA moet opgenomen zijn welke ondersteuning wordt geboden aan de gemeente voor de door opdrachtnemer aangeboden prijs. Na gunning wordt deze SLA definitief afgesloten.
6.	De Leverancier levert zowel telefonisch als ondersteuning via email en/of een web-portaal/kennisbank.

<table>
<tr><td>7.</td><td>De helpdesk van Leverancier is op werkdagen tussen 09.00u en 17.00u telefonisch bereikbaar voor eerstelijns ondersteuning. Hiervoor worden geen extra kosten voor in rekening gebracht.</td></tr>
<tr><td>8.</td><td>De helpdesk van de leverancier is verantwoordelijk voor de gehele behandeling van meldingen, incidenten m.b.t. het systeem volgens de procedure zoals vastgelegd in de Service Level Agreement (SLA). De gemeente bepaalt de prioriteit van incidenten.
T.a.v. ondersteuning wordt de volgende prioriteitsbepaling gehanteerd:
<table>
<tr><th>Prio</th><th>Omschrijving</th></tr>
<tr><td>1.</td><td>• Het systeem is volledig niet beschikbaar (naar mening van de gemeente een Critical Problem)
• De performance van het systeem is zo slecht dat het onmogelijk is om met het systeem te werken
• De fout is groot genoeg dat het behalen van het serviceniveau niet mogelijk is. Er is geen tijdelijke oplossing beschikbaar
• Groot beveiligingsprobleem</td></tr>
<tr><td>2.</td><td>• Het systeem is deels niet beschikbaar of deels niet beschikbaar voor meer dan 10% van de gebruikers (naar mening van de gemeente een Major Problem)
• Het systeem wisselt af tussen beschikbaar en niet beschikbaar
• De performance van het systeem is sterk verminderd
• Een fout die het werken met het systeem erg moeilijk maakt, er is een tijdelijke oplossing beschikbaar
• Aanzienlijk beveiligingsprobleem</td></tr>
<tr><td>3.</td><td>• Kleine verstoringen (naar mening van de gemeente een Minor Problem)
• De performance van het systeem is acceptabel
• Een fout die moet worden opgelost. Veroorzaakt moeilijkheden, maar het doel kan worden bereikt
• Klein beveiligingsprobleem</td></tr>
<tr><td>4.</td><td>• Gebruikers/beheerdersvraag die niet overeenkomen met de bovenstaande categorieën.</td></tr>
</table>

De helpdesk draagt tevens zorg voor het relateren van incidenten aan reeds bekende problemen m.b.t. het systeem. Opdrachtnemer maakt voor de gemeente inzichtelijk wanneer een incident in behandeling is genomen en wat de status van afhandeling is. Opdrachtnemer is eindverantwoordelijk voor het beheren van incidenten.
<table>
<tr><th>Nr.</th><th>Reactietijd</th><th>Oplossing binnen</th></tr>
<tr><td>Prio 1.</td><td>0-1/2 uur beantwoorden</td><td>Work-around binnen 4 uur
Oplossing binnen 8 uur</td></tr>
<tr><td>Prio 2.</td><td>2 uur (op werkdagen tussen 8.00 en 17.30 uur)</td><td>Work-around binnen 8 uur op werkdagen
Oplossing binnen 48 uur op werkdagen</td></tr>
<tr><td>Prio 3.</td><td>4 uur (op werkdagen tussen 8.00 en 17.30 uur)</td><td>Work-around binnen 2 werkdagen ‘
Oplossing in volgende reguliere versie</td></tr>
<tr><td>Prio 4.</td><td>8 uur (op werkdagen tussen 8.00 en 17.30 uur)</td><td>Antwoord binnen 1 week</td></tr>
</table></td></tr>
<tr><td>9.</td><td>Onderhoudstijden van opdrachtnemer worden ingepland buiten reguliere werktijden. Gepland onderhoud vindt derhalve plaats op avonden, weekenden of op nationale feestdagen. Werktijden worden als volgt gedefinieerd: maandag tot en met vrijdag: 08:00 – 17:30 uur, na overleg en akkoord met Gemeente Bergen op Zoom.</td></tr>
</table>

10.	Een uitzondering op de vaste onderhoudstijden (inclusief communicatie) zijn calamiteiten met een hoge prioriteit zoals onvoorziene zaken waarbij de integriteit van de gegevens in gevaar is, informatieveiligheidsincidenten en rampen.
11.	Werkzaamheden door opdrachtnemer worden altijd minimaal veertien (14) kalenderdagen van tevoren gecommuniceerd.
13.	De beschikbaarheid van het systeem is voor minimaal 99,5% per maand gegarandeerd, berekend met 24 uur per dag en zeven (7) dagen per week. Binnen werkuren (7:30u - 18:00u) is de beschikbaarheid van 99,9% gegarandeerd. Er wordt uitgegaan van een beschikbaarheid van de verbinding vanuit de Opdrachtgever van 100%, waarbij gepland onderhoud niet wordt meegenomen.
14.	De beschikbaarheid wordt op basis van de volgende formule bepaald: (([aantal dagen maand x] * 24 * 60 – [aantal minuten gepland onderhoud maand x]) – [aantal minuten downtime]) / ([aantal dagen maand x] * 24 * 60 – [aantal minuten gepland onderhoud maand x]) * 100 = beschikbaarheid maand x.