

Programma van eisen

Voor de Europese aanbesteding voor

Onderdeel Techniek, SLA, Architectuur, Privacy en
beveiliging



Inhoud

1 Eisen omtrent applicaties	3
2 Eisen en wensen Techniek	5
2.1 Leverancier	5
2.2 Wet- en regelgeving en certificeringen	5
2.3 Functioneel	5
2.4 Technisch	6
3 Informatiebeveiliging en privacy	8
4 Continuïteit	9
5 Interoperabiliteit	10
5.1 uitfasering en exit	10
5.2 Contractmanagement en governance	10
5.3 Eisen omtrent service level agreement	11
6 Eis omtrent common ground	13
7 Eisen omtrent implementatie	14
8 Eis omtrent opleidingen	15

1 Eisen omtrent applicaties

1.1	De Oplossingen wordt geleverd als Software as a Service (SaaS). De Opdrachtnemer is verantwoordelijk voor: • de levering, hosting (incl. data opslag) en het onderhoud van het hardware en softwareplatform; inclusief de benodigde licenties; • onderhoud van de software (correctief onderhoud, preventief onderhoud, adaptief onderhoud en functioneel onderhoud, updates/ releases, patches) • technisch applicatiebeheer (installeren updates, releases, patches), het onderhoud van het hardware en softwareplatform, continu en actief monitoren van beschikbaarheid, performance, capaciteit, beveiliging en data-integriteit;	Eis
1.2	De Oplossing ondersteunt het gebruik van tablets en andere mobiele devices via aangepaste interface of responsive design zonder kwaliteit in te leveren op leesbaarheid van tekst met behoud van alle functionaliteiten.	Eis
1.3	De Opdrachtnemer waarborgt dat de aangeboden Oplossing niet meer dan één major versie achterloopt ('neerwaartse compatibiliteit') op de open standaarden van het Forum Standaardisatie en op de standaarden uit GEMMA die voor de Oplossing relevant zijn. Aanpassingen in de hierboven genoemde standaarden worden binnen 6 maanden door de Opdrachtnemer verwerkt nadat de aanpassingen als nieuwe standaard zijn gepubliceerd op genoemd forum of Gemma online. Daarnaast wordt de oude versie van de standaard nog minimaal 12 maanden ondersteund.	Eis
1.4	Binnen de Oplossing worden de (actuele) versies van de volgende standaarden gehanteerd: • Het Referentiemodel Stelsel van Gemeentelijke Basisgegevens (RSGB), • Referentiemodel Gemeentelijke Basisgegevens Zaken (RGBZ) • Informatiemodel Zaaktype Catalogus (ImZTC) • Referentie Informatiemodel Handhaving (RiHa) • Berichtenstandaarden StUF-ZKN en StUF-BG • de Zaakgericht Werken API (voorkeur) of Zaak- en Documentservices • Berichtenstandaarden voor het Digitaal Stelsel Omgevingswet zoals bijvoorbeeld DSO LV, STAM, REST API's en stelselcatalogus.	Eis
1.5	De opslag van gegevens vindt fysiek plaats binnen de Europese Economische Ruimte.	Eis
1.6	De Opdrachtnemer garandeert dat de Oplossing een acceptabele performance voor 30 concurrent gebruikers heeft. Dit houdt in dat de resultaten van tenminste de volgende handelingen in de Oplossing binnen 3 seconden worden weergegeven: 1. Het starten van een nieuwe zaak.	Eis

	2. Het tonen van een zaak. 3. Het zetten van een nieuwe status. 4. Het toevoegen van een document kent geen beperkingen in omvang van het bestand. 5. Het afronden van een zaak. 6. Het tonen van een zaak in zoekresultaten. 7. Het tonen van een adres, subject of object in zoekresultaten . 8. Het tonen van de werkvoorraad. 9. Een locatie toevoegen 10. Een locatie muteren Het aanpassen van een objectregistratie	
--	---	--

Eisen en wensen Techniek

1.1 Leverancier

2.1.1	Indien er derden leveranciers (zoals toeleveranciers of onderaannemers) zijn, zijn dezelfde voorwaarden van toepassing als voor de leverancier, met inachtneming van GIBIT 2023 artikel 7 , afhankelijkheid van en afstemming met derde partijen.	Eis
-------	---	-----

1.2 Wet- en regelgeving en certificeringen¹

2.2.1	De leverancier voldoet aan de Algemene Verordening Gegevensbescherming.	Eis
2.2.2	De leverancier verwerkt persoonsgegevens van de gemeente op grond van een verwerkersovereenkomst, zoals beschreven in artikel 28 van de GIBIT 2023.	Eis
2.2.4	De leverancier heeft informatiebeveiliging procesmatig ingericht en toont dit aan door middel van een geldige ISO 27001-certificering of gelijkwaardig. De leverancier toont de meest recente auditrapportage waaruit blijkt dat de leverancier nog steeds voldoet aan de eisen van deze certificering. De gemeente Nieuwkoop beoordeelt of de scope van de certificering overeenkomt met de behoefte van de gemeente.	Eis
2.2.5	De leverancier heeft risicomanagement procesmatig ingericht en toont dit aan door middel van een geldige ISO 31000-certificering of gelijkwaardig. De leverancier toont de meest recente auditrapportage waaruit blijkt dat de leverancier nog steeds voldoet aan de eisen van deze certificering.	Eis
2.2.6	De leverancier heeft kwaliteitsmanagement procesmatig ingericht en toont dit aan door middel van een geldige ISO 9001-certificering of gelijkwaardig. De leverancier toont de meest recente auditrapportage waaruit blijkt dat de leverancier nog steeds voldoet aan de eisen van deze certificering.	Eis
2.2.7	GIBIT 2023, artikel 35, Periodieke derdenverklaring, is aanvullend van toepassing op de eisen 2.2.3, 2.2.4 en 2.2.5.	Eis

1.3 Functioneel

2.3.1	Gebruikers kunnen alleen toegang krijgen tot de ICT-prestatie en de data waarvoor zij geautoriseerd zijn.	Eis
-------	---	-----

2.3.2	De gemeente Nieuwkoop kan zelfstandig rollen definiëren in de ICT-prestatie.	Eis
2.3.3	De rollen kunnen door functioneel beheerders van de gemeente eenvoudig gekoppeld worden aan één of meer groepen.	Eis
2.3.4	In lijn met BIO artikel 12.4.2 kan de gemeente Nieuwkoop beschikken over logging-gegevens binnen de ICT-prestatie die in logbestanden worden gepresenteerd en kunnen worden gedownload in een CSV, Word of Excel bestand	Eis
2.3.5	De ICT-prestatie ondersteunt zowel het bewaren als het periodiek verwijderen van gegevens op aanwijzing van de gemeente Nieuwkoop, volgens de AVG.	Eis

1.4 Technisch

2.4.1	De ICT-prestatie wordt gekoppeld met Azure AD van de gemeente Nieuwkoop. Door middel van deze koppeling wordt Single Sign-On (SSO) en Multi Factor Authenticatie (MFA) in Azure AD ingericht.	Eis
2.4.2	Alle onderdelen van de ICT-prestatie bevinden zich in de cloud en dus niet on-premise bij de gemeente Nieuwkoop.	Eis
2.4.3	De leverancier past aantoonbaar relevante standaarden van de GEMMA standaardenlijst toe voor de opzet en exploitatie van de ICT-prestatie en de interactie.	Eis
2.4.4	De locatie van de gegevens en de programmatuur is bekend en bevindt zich binnen de Europese Economische Ruimte.	Eis
2.4.5	De leverancier voldoet aan de binnen de gemeente Nieuwkoop geldende standaarden voor e-mailbeveiliging, te weten: • Een geldig SPF record. • De inrichting van DKIM op een door de gemeente aan te wijzen (sub)domein. • Indien van toepassing: DMARC	Eis
2.4.6	In lijn met GIBIT 2023 artikel 32 wordt een compleet ingerichte test (of -acceptatie) omgeving geleverd, waarin de gemeente Nieuwkoop nieuw aangeboden functionaliteit kan testen en accepteren.	Eis
2.4.7	Ontwikkel-, test- en acceptatieomgevingen (separaat of geïntegreerd) zijn gescheiden van de nieuw in te richten productieomgeving.	Eis
2.4.8	In de test- en acceptatieomgevingen (separaat of geïntegreerd) wordt gewerkt met anonieme gegevens.	Eis

2.4.9	De leverancier heeft de ICT-prestatie zo ingericht, dat gebruikers en beheerders van verschillende organisaties niet bij elkaars gegevens kunnen en geen verstoring voor elkaars dienstverlening op kunnen leveren.	Eis
2.4.10	Gegevensoverdracht vindt uitsluitend plaats via een beveiligde infrastructuur.	Eis
2.4.11	De leverancier past de voorlaatste versie van Transport Layer Security (TLS) toe.	Eis
2.4.12	De leverancier past de meest recente versie van Transport Layer Security (TLS) toe.	Eis
2.4.13	De leverancier maakt het mogelijk gegevens en documenten vanuit de applicatie te exporteren.	Eis
2.4.14	De leverancier stelt (REST)API-endpoints ter beschikking ter ontsluiting van de (meta)data die de applicatie ter beschikking heeft.	Eis
2.4.15	Het systeem kan data naar gangbare bestandsformaten exporteren, tenminste tekst, MsExcel, CSV, PDF, en XML-documenten.	Eis
2.4.16	De Haven standaard is van toepassing op het hosting gedeelte.	Eis

2 Informatiebeveiliging en privacy

3.1	De gemeente Nieuwkoop is en blijft eigenaar van de data en kan hier ten alle tijden over beschikken	Eis
3.2	De leverancier voldoet aan de normen uit de meest recente versie Baseline Informatiebeveiliging Overheid (BIO) door aantoonbaar de beschreven maatregelen toe te passen.	Eis
3.3	De leverancier versleutelt alle gegevens tijdens transport via netwerken en opslag.	Eis
3.4	De leverancier neemt gepaste beveiligingsmaatregelen op basis van een dataclassificatie en een risico-impact-analyse. In een multi-tenant omgeving kan er geen sprake zijn van individuele dataclassificatie door de gemeente Nieuwkoop. De leverancier levert dan de generieke dataclassificatie aan.	Eis
3.5	Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen worden vastgelegd in audit-logbestanden die, bij voorkeur vanuit een applicatie-interface of een standaard koppelvlak, aan het SIEM-systeem van de gemeente Nieuwkoop geleverd kunnen worden. De gemeente Nieuwkoop kan te allen tijde deze bestanden raadplegen voor nadere analyse.	Eis
3.6	De partijen hebben een beveiligingsfunctie benoemd en een beveiligingsorganisatie ingericht, waarin de organisatorische positie, taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen en de rapportagelijnen zijn vastgelegd.	Eis
3.7	Bij beveiligingsincidenten draagt de leverancier er zorg voor dat een ter zake deskundige medewerker beschikbaar is. Afhankelijk van de classificatie van het informatiesysteem wordt de beschikbaarheid bepaald.	Eis
3.8	De leverancier informeert de gemeente Nieuwkoop als zich een beveiligingsincident voordoet. Deze incidenten worden ook vermeld in de periodieke rapportages.	Eis
3.9	Structurele mitigerende maatregelen ter voorkoming respectievelijk oplossing van beveiligingsincidenten is de verantwoordelijkheid van de leverancier, voor zover het de dienstverlening van de leverancier betreft. De leverancier onderneemt zo snel mogelijk actie om acute beveiligingsincidenten te stoppen en meldt dit na afloop direct aan de gemeente Nieuwkoop.	Eis

3 Continuïteit

4.1	De leverancier garandeert een beschikbaarheid van 98 % tot de verleende service en de data op werkdagen van maandag t/m vrijdag van 08.00 tot 17.00 uur. Buiten deze windows is onderhoud toegestaan, mits vooraf aangekondigd. GIBIT Artikel 34 (indien er niets is afgesproken geldt beschikbaarheid op werkdagen van 09:00-17:00)	Eis
4.2	In de SLA-rapportages wordt het percentage geslaagde back-ups vermeld. Minimaal 95% van de back-ups moeten slagen. Als een back-up niet is gelukt, wordt dit direct de volgende werkdag doorgegeven.	Eis
4.3	De leverancier is transparant over zijn change- en releasebeleid: - Kondigt tijdig het testen en in productie nemen van nieuwe releases aan; - Levert tijdig releasenotes; - Informeert de gemeente Nieuwkoop tijdig over de activiteiten die bij het uitbrengen van een nieuwe release van de gemeente worden verwacht.	Eis
4.4	De leverancier stuurt met de offerte een SLA mee met de servicelevels die de leverancier voor de SAAS oplossing hanteert. Ter beoordeling door de aanbestedende partij.	Eis

4 Interoperabiliteit

5.1	Indien voor gebruik van de ICT prestatie een webbrowser is vereist, dan dient de ICT Prestatie correct te functioneren in de meest recente en nog ondersteunde versie van alle gangbare browsers (als Edge, Chrome, Firefox en Safari) zonder dat daarbij nadere plug-ins zijn vereist of andere eisen aan het Applicatielandschap worden gesteld (conform GIBIT Artikel 31.2)	Eis
5.2	De leverancier bewaakt en beheerst binnen de ICT-prestatie de werking van de koppelvlakken waarop hij invloed heeft. Deze bewaking is onder meer gericht op beveiliging en continuïteit van de dienstverlening. Hierover wordt gerapporteerd conform de afspraken in de SLA.	Eis
5.3	De leverancier is zich bewust van zijn positie in de keten c.q. het netwerk met andere applicaties en houdt daartoe het eerder genoemde architectuuroverzicht actueel.	Eis
5.4	De gemeente Nieuwkoop en de betrokken leveranciers maken gezamenlijk afspraken over een juiste samenwerking in de keten.	Eis
5.5	Wijzigingen in de keten worden doorgevoerd nadat deze een ketentest met goed resultaat hebben doorstaan.	Eis

4.1 uitfasering en exit

5.1.1	Op eerste verzoek van de gemeente Nieuwkoop zullen partijen gezamenlijk een exit-plan opstellen. In een exit-plan wordt uitgebreid ingegaan op alle aspecten van de exit, waaronder de gevolgen van de beëindiging en de criteria voor enig voortgezet gebruik. Dit in aanvulling op GIBIT 2023, artikel 26	Eis
5.1.2	Bij beëindiging van het contract draagt de leverancier de data over aan de gemeente. Dit in aanvulling op GIBIT 2023, artikel 26	Eis

4.2 Contractmanagement en governance

5.2.1	De GIBIT voorwaarden 2023 zijn van toepassing verklaard.	Eis
5.2.2	De leverancier heeft risicomanagement en interne beheersing aantoonbaar procesmatig en organisatorisch ingericht. Aantoonbaar via ISO-certificaat of Accountantsverklaring (TPM).	Eis

5.2.3	De looptijd van de clouddienst en tussentijdse beëindiging zijn onderdeel van het contract. Een contract voor onbepaalde duur is niet toegestaan.	Eis
5.2.4	De leverancier beschrijft de impact voor het contract in relatie tot het op- en afschalen van verschillende soorten gebruikers.	Eis

4.3 Eisen omtrent service level agreement

5.3.1	De Service Level Agreement (SLA) is gebaseerd op de handreiking van de IBD.	Eis
5.3.2	Diensten voor onderhoud en ondersteuning, voor zover deze door de Opdrachtnemer moeten worden geleverd, kunnen op afstand worden uitgevoerd.	Eis
5.3.3	De Opdrachtnemer verzorgt een Nederlandstalige helpdesk voor zowel technische als functionele ondersteuning. De helpdesk is het <i>enige</i> centrale punt voor het melden van incidenten, het stellen van vragen, indienen van wijzigingsvoorstellen en geeft informatie/ inzicht in de afhandeling daarvan. De helpdesk van de Opdrachtnemer levert zowel telefonische ondersteuning als ondersteuning via e-mail en/of een webportaal. De helpdesk is telefonisch bereikbaar op werkdagen tussen 08.00 en 17.00 uur (CET). Voor ondersteuning door de helpdesk van de Opdrachtnemer worden geen aanvullende kosten in rekening gebracht.	Eis
5.3.4	De helpdesk is verantwoordelijk voor de gehele behandeling van meldingen, incidenten m.b.t. de Oplossing volgens de procedure zoals vastgelegd in de Service Level Agreement (SLA). De Opdrachtgever bepaalt de prioriteit van incidenten. Ten aanzien van de ondersteuning wordt de volgende prioriteitsbepaling gehanteerd:	Eis
Categorie		Omschrijving
1	De Oplossing is volledig niet beschikbaar of kritieke functionaliteit is niet beschikbaar (naar mening van de Opdrachtgever een Critical Problem en kritieke functionaliteit).	
2	De Oplossing is deels niet beschikbaar of deels niet beschikbaar voor meer dan 10% van de gebruikers (naar mening van de Opdrachtgever een Major Problem).	
3	Kleine verstoringen (naar mening van de Opdrachtgever een Minor Problem).	

4	Gebruikers / beheedersvraag.	
5.3.5	De helpdesk draagt tevens zorg voor relateren van incidenten aan reeds bekende problemen m.b.t. de Oplossing. De Opdrachtnemer maakt voor de Opdrachtgever inzichtelijk wanneer een incident in behandeling is genomen en wat de status van afhandeling is. De Opdrachtnemer is eindverantwoordelijk voor het beheren van incidenten.	Eis
5.3.6	De Opdrachtnemer is verantwoordelijk voor de gehele afhandeling van wijzigingsvoorstellen m.b.t. de Oplossing. De Opdrachtnemer is verantwoordelijk voor het inbrengen van wijzigingsvoorstellen ten behoeve van het oplossen van reeds geïdentificeerde problemen.	Eis
5.3.7	Opdrachtnemer rapporteert periodiek aan Opdrachtgever over de nakoming van overeengekomen Service Levels waaronder tenminste wordt verstaan: beschikbaarheid, afhandeling en opvolging van (beveiligings) incidenten, onderhoudswerkzaamheden en het niveau van de diensten. Inhoud en frequentie worden nader omschreven in de SLA.	Eis
5.3.8	Opdrachtnemer heeft een back-up en recovery beleid dat voldoet aan de eisen uit de BIO en waarbij minimaal de volgende eisen van toepassing zijn op de back-up en restorevoorzieningen van Oplossing:. • De 3-2-1-1-0 regel of een vergelijkbare veilige back-up strategie • Een incident op de ene locatie kan niet leiden tot schade op de andere locatie (ook niet in het geval van ransomware). Locaties dienen een ander risicoprofiel te hebben. Bijvoorbeeld een uitwijklocatie heeft een ander risicoprofiel dan de primaire locatie(s) • Gegevensverlies bedraagt maximaal 24 uur. • Hersteltijd in geval van incidenten is maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen. • Het restoren van back-ups wordt minimaal jaarlijks of na een grote wijziging getest waarbij recovery-procedures voortdurend worden bijgewerkt. • Er is sprake van een reconstructiemechanisme als geen data verloren mag gaan. • Back-ups worden beschermd tegen onbevoegde toegang. • In het geval van ketensoftware is data-integriteit van de keten gewaarborgd. • Opdrachtnemer zorgt voor adequate afspraken over back-up en recovery en voldoet aantoonbaar aan relevante punten uit het beleid. In het geval van noodscenario's is toegang tot Oplossing geborgd door de inzet van zogenaamde "break glass accounts".	Eis

5 Eis omtrent common ground

Nr. Omschrijving

6.1	Opdrachtnemer heeft het VNG covenant common ground ondertekend.	Eis
-----	---	-----

6 Eisen omtrent implementatie

Nr. Omschrijving

7.1	De Opdrachtnemer levert binnen vier weken na definitieve gunning een gedetailleerd plan van aanpak (PvA) aan voor de technische en functionele implementatie	Eis
7.2	De Opdrachtnemer levert dienstverlening ten behoeve van de installatie, de configuratie van de software en de implementatie van de Oplossing. Opdrachtnemer maakt daarbij gebruik van projectleider en consultancy die in dienst zijn van Opdrachtnemer.	Eis
7.3	De Opdrachtnemer verzorgt de technische implementatie (inclusief koppelingen) van de Oplossing.	Eis
7.4	Opdrachtgever en Opdrachtnemer zorgen samen met onze andere leveranciers voor werkende koppelingen van de Oplossing naar Nieuwkoop-applicaties, in acceptatie/test- en productieomgeving van de Oplossing	Eis
7.5	De Opdrachtnemer garandeert uiterlijk binnen 6 weken na de definitieve gunning een eerste werkende versie van de oplossing in acceptatie/test en productieomgeving.	Eis

7 Eis omtrent opleidingen

Nr. Omschrijving

8.1	De Opdrachtnemer zorgt ervoor dat twee beheerder(s) van de gemeente Nieuwkoop tijdens de implementatie zodanig worden getraind in het werken met de Oplossing, dat zij zelf instaat zijn om de gebruikers van de gemeente Nieuwkoop te trainen in het gebruik van de Oplossing.	Eis
8.2	Hierbij worden zij voorzien van alle benodigde (actuele en digitale) documentatie in de Nederlandse taal (incl. alle technische documenten) en eventuele (digitale) hulpmiddelen voor het opleiden van eindgebruikers.	Eis