Rijksinkoopsamenwerking
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Bijlage F – Concept programma van Eisen

Rijksinkoopsamenwerking

Bezoekadres
Rijkskantoor Beatrixpark
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 20011
2500 EA Den Haag

Concept Programma van Eisen

DSU managed hosting en beheer

voor het

Ministerie van Sociale Zaken en Werkgelegenheid

Directie Dienstverlening, Samenwerkingsverbanden en Uitvoering (DSU)

Datum	02 juni 2026
Inkoopadviseur	Jeroen Kuijsten
Kenmerk	201865005.011.090
Versie	0.9

Inhoudsopgave

1. Inleiding

De eisen en wensen zoals opgenomen in dit Programma van Eisen (hierna: PvE) gelden als uitgangspunt voor de Selectiefase. Gedurende de fase van de Concurrentiegerichte Dialoog kunnen de opgenomen eisen en wensen, naar aanleiding van de gevoerde dialogen, nader worden uitgewerkt, aangepast of komen te vervallen.

2. Toepasselijkheid en karakter van de eisen

2.1. Karakter van de eisen

Dit PvE bevat zowel eisen als wensen die van toepassing zijn op de Opdracht.

2.2. Eisen

Tenzij in het PvE expliciet is aangegeven dat sprake is van een Bespreekbare items, is sprake van Knock-out eisen.

2.3. Knock-out eisen

Knock-out eisen dienen bij definitieve inschrijving volledig en onvoorwaardelijk te worden geaccepteerd. Indien niet aan deze eisen wordt voldaan, wordt de inschrijving ongeldig verklaard en terzijde gelegd.

2.4. Bespreekbare items

Bespreekbare items worden gedurende de dialoogfase nader besproken, geconcretiseerd en waar nodig aangepast. De Aanbestedende Dienst behoudt zich het recht voor om deze eisen na afronding van de dialoogfase vast te stellen als definitieve minimumeisen.

2.5. Wensen

Naast eisen bevat dit PvE wensen. Wensen geven richting aan de beoogde kwaliteit, functionaliteit en meerwaarde van de oplossing.

Gegadigden worden uitgenodigd om aan te geven in hoeverre en op welke wijze zij invulling geven aan deze wensen. Wensen bieden ruimte voor optimalisatie en innovatie binnen de kaders van de opdracht.

Het niet (volledig) voldoen aan wensen heeft geen gevolgen voor de geldigheid van de inschrijving.

2.6. Relatie met Nota van Inlichtingen

De Nota van Inlichtingen (NvI) en het Programma van Eisen (PvE) vormen gezamenlijk de aanbestedingsstukken.

In geval van tegenstrijdigheden tussen het PvE en de Nota van Inlichtingen, prevaleert de meest recente Nota van Inlichtingen.

2.7. Naleving gedurende de looptijd

Inschrijver voldoet bij aanvang van de Overeenkomst aantoonbaar aan alle geldende eisen uit dit Programma van Eisen en draagt er zorg voor dat gedurende de gehele looptijd van de Overeenkomst blijvend aan deze eisen wordt voldaan.

Indien gedurende de looptijd blijkt dat niet (langer) aan één of meer eisen wordt voldaan, is sprake van een toerekenbare tekortkoming in de nakoming van de Overeenkomst, tenzij Inschrijver aantoont dat hem dit niet kan worden toegerekend.

In een dergelijk geval is de Aanbestedende Dienst gerechtigd om, onverminderd overige rechten en rechtsmiddelen:

- de Inschrijver schriftelijk in gebreke te stellen en een redelijke termijn te stellen waarbinnen alsnog volledig aan de eisen wordt voldaan;
- nadere instructies te geven en/of corrigerende en preventieve maatregelen voor te schrijven, alsmede de uitvoering daarvan te (laten) controleren;
- betalingen geheel of gedeeltelijk op te schorten zolang niet aan de eisen wordt voldaan;
- de Overeenkomst geheel of gedeeltelijk te ontbinden, conform de bepalingen in de Overeenkomst.

3. Bespreekbare items en knock-out eisen t.b.v. dialoogrondes

De eisen zijn onderverdeeld in de volgende categorieën:

1. Algemene eisen;
2. Security, Compliance en Digitale Soevereiniteit DSU;
3. Service Management;
4. Governance en Samenwerking;
5. Hosting en Beheer;
6. Architectuur eisen;
7. Applicaties eisen;
8. Migratie;
9. Innovatie.

Per eis is aangegeven of het gaat om:

- Knock-out eisen (**KO**);
- Bespreekbare items (**BI**), of;
- wensen (**WE**).

Uitgangspunten

1. Algemene eisen aan de opdracht

Algemene eisen **aan de opdracht**				
Eis Algemeen 1.1	Inschrijver levert de dienstverlening vanuit organisaties, personeel en datacenters binnen de Europese Economische Ruimte (EER), vallend onder Europees recht.	KO		
Eis Algemeen 1.2	Aanbestedende Dienst heeft het recht periodiek audits of onderzoeken uit te laten voeren op de dienstverlening. Inschrijver verleent zich hieraan medewerking.	KO		
Eis Algemeen 1.3	Alle productieomgevingen en dataopslag bevinden zich binnen de Europese Economische Ruimte (EER).	KO		
Eis Algemeen 1.4	Inschrijver treft passende, technische en organisatorische maatregelen om beschikbaarheid, integriteit en continuïteit van de dienstverlening te waarborgen op basis van SLA.	KO		
Eis Algemeen 1.5	Inschrijver stelt een actuele, standaard servicecatalogus beschikbaar.	KO		
Eis Algemeen 1.6	Alle data, tenantconfiguraties, domeinnamen en specifiek voor Aanbestedende Dienst ingerichte omgevingen blijven eigendom van Aanbestedende Dienst.	KO		
Eis Algemeen 1.7	Medewerkers met toegang tot systemen of vertrouwelijke informatie beschikken over een geldige VOG die bij inzet niet ouder is dan drie maanden.	KO		
Eis Algemeen 1.8	Gebruikersinterfaces, beheerportalen en servicedocumentatie zijn beschikbaar in Nederlands of Engels.	KO		
Eis Algemeen 1.9	Operationele en tactische communicatie vindt plaats in het Nederlands. Sleutelfunctionarissen beheersen Nederlands op professioneel niveau. https://detaalbrigade.nl/taalniveaus	KO		
Eis Algemeen 1.10	Inschrijver werkt mee aan noodzakelijke aanpassingen als gevolg van gewijzigde wet- en regelgeving. Indien substantiële impact ontstaat op dienstverlening of kosten, treden partijen hierover in overleg.	KO		
Eis Algemeen 1.11	Inschrijver verleent bij beëindiging van de overeenkomst medewerking aan overdracht van dienstverlening, data en documentatie conform overeengekomen exit afspraken.	KO		
Eis Algemeen 1.12	Inschrijver werkt samen met andere leveranciers en de Opdrachtgever conform de geldende Rijksvoorwaarden (waaronder de ARBIT) en governance afspraken.	KO		
Eis Algemeen 1.13	Inschrijver richt logging, monitoring en beheerprocessen zodanig in dat forensisch onderzoek mogelijk blijft.	KO		
Eis Algemeen 1.14	Inschrijver voldoet aan de Social Return verplichtingen zoals opgenomen in de bijlage van deze aanbesteding.	KO		
Eis algemeen 1.15	Inschrijver stelt Opdrachtgever onverwijld schriftelijk op de hoogte van iedere voorgenomen of gerealiseerde wijziging in de zeggenschap ("Change of Control") over Inschrijver of een bij de uitvoering van de Overeenkomst betrokken groepsmaatschappij. Onder Change of Control wordt verstaan een directe of indirecte wijziging van de feitelijke zeggenschap, waaronder een fusie, overname of overdracht van meerderheid van aandelen of stemrechten. Inschrijver blijft onverminderd verantwoordelijk voor de volledige nakoming van de Overeenkomst. Indien een Change of Control naar het redelijke oordeel van Opdrachtgever risico's oplevert voor de continuïteit, beveiliging of correcte uitvoering van de Overeenkomst, is Opdrachtgever gerechtigd aanvullende waarborgen te	KO		

	verlangen of de Overeenkomst geheel of gedeeltelijk op te zeggen. Inschrijver verstrekt op verzoek alle redelijkerwijs benodigde informatie over de Change of Control.			

2. Security, Compliance en Digitale Soevereiniteit DSU eisen

Security, Compliance en Digitale Soevereiniteit DSU eisen				
Eisen aan Inschrijver				
Eis Security, Compliance en Digitale Soevereiniteit 2.1	Inschrijver beschikt gedurende de looptijd van de overeenkomst over een aantoonbaar geïmplementeerd Information Security Management System (ISMS) en is gecertificeerd conform ISO/IEC 27001.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.2	Inschrijver maakt de leverancierskeketen inzichtelijk en borgt dat kritieke onderleveranciers aantoonbaar voldoen aan passende informatiebeveiligingsnormen en beschikken over een actueel ISO/IEC 27001-certificaat of aantoonbaar gelijkwaardige certificering.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.3	Inschrijver treft technische, organisatorische en contractuele maatregelen ter borging van digitale soevereiniteit van data en dienstverlening binnen de Europese Economische Ruimte (EER).	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.4	Doorgifte van data of toegang tot data buiten de Europese Economische Ruimte (EER) is uitsluitend toegestaan indien wordt voldaan aan de toepasselijke vereisten uit de AVG en voorafgaande schriftelijke toestemming is verkregen van Opdrachtgever.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.5	Inschrijver verleent medewerking aan Data Protection Impact Assessment (DPIA) en levert tijdig benodigde informatie aan.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.6	Inschrijver voldoet gedurende de looptijd van de overeenkomst aan de AVG.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.7	Persoonsgegevens worden uitsluitend verwerkt binnen de Europese Economische Ruimte (EER) conform AVG.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.8	Inschrijver voert periodiek kwetsbaarheidsscans uit en rapporteert bevindingen, risico's en opvolgmaatregelen.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.9	Inschrijver moet een ISMS-framework (Information Security Management System) gebruiken en de bijbehorende beveiligingsprocessen aantoonbaar implementeren en uitvoeren binnen de eigen organisatie.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.10	Inschrijver is in het bezit van of voldoen aan: • ISO 27017 (Cloud security); • IISO 27018 (bescherming van persoonsgegevens in Cloud-omgevingen) • EU Cloud Code of Conduct.			WE
Eis Security, Compliance en Digitale Soevereiniteit 2.11	Inschrijver verstrekt jaarlijks een actuele onafhankelijke assurance-rapportage, zoals SOC2 Type II of ISAE3000 Type II.	KO		
Eis Security, Compliance en	Inschrijver beschikt over een formele incidentprocedure voor informatie-beveiligingsincidenten inclusief meld-, escalatie- en rapportageprocessen.	KO		

Digitale Soevereiniteit 2.12				
Eis Security, Compliance en Digitale Soevereiniteit 2.13	Inschrijver beschikt over een datalekprocedure conform AVG en meldt datalekken tijdig aan Opdrachtgever.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.14	Inschrijver werkt mee aan noodzakelijke beveiligingsmaatregelen en wijzigingen die voortvloeien uit gewijzigde wet- en regelgeving, rijksbeleid of actuele informatiebeveiligingseisen.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.15	De securityarchitectuur wordt ingericht volgens Zero Trust principes.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.16	Inschrijver en Aanbestedende Dienst leggen exit afspraken contractueel vast voorafgaand aan ingebruikname van de dienstverlening.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.17	Aanbestedende Dienst wenst ondersteuning voor de volgende DigiD-eisen: • ondersteuning van DigiD-beveiligingseisen; • medewerking aan audits; • assurance-rapportages.			WE
Eis Security, Compliance en Digitale Soevereiniteit 2.18	Inschrijver laat minimaal jaarlijks onafhankelijke penetratietesten uitvoeren op de infrastructuur.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.19	Inschrijver verleent medewerking aan zowel audits als penetratietesten uitgevoerd in opdracht van Aanbestedende Dienst.	KO		
Eisen aan het product van Inschrijver				
Eis Security, Compliance en Digitale Soevereiniteit 2.20	De dienstverlening voldoet aan verplichte open standaarden van Forum Standaardisatie en relevante NCSC-richtlijnen. (https://www.forumstandaardisatie.nl/open-standaarden/verplicht)	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.21	De PaaS-omgevingen bieden ondersteuning voor 'Single-Sign-On' vanuit Ministerie Sociale Zaken & Werkgelegenheid, Directie Dienstverlening, Samenwerkingsverbanden en Uitvoering (DSU)-omgeving.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.22	De hostingproducten die geleverd worden moeten voldoen (met een mapping) aan: 1) AVG; 2) BIO2 of haar opvolger; 3) CBW; 4) NORA.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.23	Logfiles dienen geschikt te zijn voor forensisch onderzoek en dient voldoende detailniveau te bevatten om incidentanalyse en reconstructie van gebeurtenissen mogelijk te maken.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.24	Versleuteling vindt plaats met sleutels die uitsluitend door de aanbestedende dienst worden beheerd. De inschrijver toont op verzoek de naleving en effectiviteit van deze maatregelen aan. *Versleuteling van data (zowel 'in transit' als 'at rest') vindt plaats met cryptografische sleutels die uitsluitend door de Aanbestedende Dienst worden gegenereerd en beheerd (Hold Your Own Key-principe). De Inschrijver heeft onder geen beding*	KO		

	toegang tot de onversleutelde sleutels of de mogelijkheid de data zelfstandig te ontsleutelen. De Inschrijver toont op eerste verzoek de technische naleving en de effectiviteit van deze scheiding aan			
Eis Security, Compliance en Digitale Soevereiniteit 2.25	Data wordt versleuteld opgeslagen en versleuteld verzonden conform actuele beveiligingsstandaarden.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.26	Alle beheer- en gebruikersinterfaces ondersteunen Multi-Factor Authenticatie.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.27	Het is mogelijk om op de PaaS-omgevingen een netwerksensor van het Nationaal Cyber Security Centrum (of gelijkwaardig) te plaatsen.			WE
Eis Security, Compliance en Digitale Soevereiniteit 2.28	De PaaS-omgeving is beveiligd tegen DDOS-aanvallen en inschrijver verzorgt risicobeperkende services.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.29	Datacenters voldoen minimaal aan TIER III of gelijkwaardig.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.30	De dienstverlening beschikt minimaal over: • centrale logging van beveiligingsgebeurtenissen; • monitoring van infrastructuur, systemen en beveiligingsincidenten; • SIEM/SOC-functionaliteit of een gelijkwaardige voorziening voor detectie en opvolging van beveiligingsincidenten; • bewaartermijnen en rapportagemogelijkheden conform afspraken met Opdrachtgever.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.31	Toegangsbeheer wordt ingericht en beheerd volgens een erkend kader, zoals ISO 27001/27002 (bijv. A.9 Toegangsbeheer) of NIST 800-53 (AC-controls), inclusief periodieke evaluatie en logging.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.32	De dienstverlening voldoet aan de onderstaande eisen: • Inschrijver biedt 'Vulnerability scanning' als dienst aan voor de PaaS-omgeving van de aanbestedende dienst; • Deze scans worden periodiek uitgevoerd en omvatten minimaal systemen, netwerken en applicaties, zowel dynamisch als statisch; • Resultaten worden gerapporteerd, inclusief risicobeoordeling en aanbevelingen voor opvolging.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.33	De aangeboden oplossing dient te voorzien in: • Ondersteuning voor veilige TLS-configuraties met PKIoverheid-certificaten (of gelijkwaardig); • Correcte ondersteuning en configuratie van e-mailbeveiligingsstandaarden (waaronder SPF, DKIM, DMARC, STARTTLS en DANE); De mogelijkheid om deze configuraties in afstemming met de applicatieleverancier in te richten en te beheren.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.34	De aangeboden oplossing dient te voorzien in realtime mechanismen voor het detecteren en, waar passend, automatisch mitigeren van verdachte of kwaadaardige netwerk- en applicatieactiviteiten	KO		
Digitale Soevereiniteit DSU eisen				
Eis Security, Compliance en Digitale Soevereiniteit 2.35	De dienstverlening ondersteunt export van data en configuraties in open en gangbare formaten	KO		

Eis Security, Compliance en Digitale Soevereiniteit 2.36	Inschrijver maakt op verzoek inzichtelijk welke onderaannemers en onderleveranciers worden ingezet voor de dienstverlening.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.37	Back-upvoorzieningen worden opgeslagen binnen de EER conform overeengekomen continuïteits- en beveiligingseisen.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.38	Wijzigingen in kritieke onderaannemers, ketenpartners of de eigendoms- en zeggenschapsstructuur van Inschrijver worden vooraf schriftelijk gemeld aan Opdrachtgever. Opdrachtgever behoudt het recht deze wijzigingen te beoordelen op impact voor informatiebeveiliging en dienstverlening.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.39	De oplossing ondersteunt sturing op geografische locatie van dataverwerking binnen de EER.		BI	
Eis Security, Compliance en Digitale Soevereiniteit 2.40	De dienstverlening ondersteunt beveiligingsmaatregelen zoals versleuteling en pseudonimisering waar relevant.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.41	Aanbestedende Dienst behoudt zich het recht voor gemotiveerd bezwaar te maken tegen inzet van kritieke onderaannemers.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.42	Inzet van onderaannemers buiten de Europese Economische Ruimte (EER) is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van Opdrachtgever, mits geen toegang bestaat tot persoonsgegevens, vertrouwelijke gegevens, productieomgevingen of beheerinterfaces van Opdrachtgever.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.43	Toegang door onderaannemers wordt gelogd en inzichtelijk gemaakt voor Opdrachtgever.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.44	Opdrachtgever behoudt te allen tijde eigenaarschap over data, configuraties, tenantinrichtingen en bijbehorende intellectuele eigendomsrechten voor zover deze specifiek voor Opdrachtgever zijn ingericht of ontwikkeld.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.45	De dienstverlening ondersteunt overdraagbaarheid naar alternatieve leveranciers door middel van exporteerbare dataformaten, overdraagbare configuraties, documentatie en redelijke exit-ondersteuning bij beëindiging van de overeenkomst.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.46	Encryptiesleutels worden uitsluitend beheerd onder verantwoordelijkheid en zeggenschap van de Aanbestedende Dienst. Inschrijver heeft geen toegang tot of controle over de gebruikte encryptiesleutels, tenzij schriftelijk anders overeengekomen.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.47	Inschrijver voldoet aan het Sovereignty Effectiveniss Assurance Level 3 (SEAL-3), zoals opgetekend in het Cloud Sovereignty Framework (version 1.2.1) van de Europese Commissie.	KO		

3. Service Management eisen

Service Management eisen				
Eis Service Management 3.1	Inschrijver en Aanbestedende Dienst stellen gezamenlijk een calamiteitenorganisatie vast inclusief bevoegdheden, escalaties en contactpersonen, aangevuld met een calamiteitenprocedure Details worden in het DAP uitgewerkt.	KO		
Eis Service Management 3.2	Bij calamiteiten informeert Inschrijver en Aanbestedende Dienst onverwijld conform overeengekomen escalatieprocedures.	KO		
Eis Service Management 3.3	PRIO1-incidenten moeten telefonisch kunnen worden gemeld.	KO		
Eis Service Management 3.4	Inschrijver stelt een servicedesk beschikbaar gedurende overeengekomen servicewindows.	KO		
Eis Service Management 3.5	Meldingen kunnen 24x7 worden ingediend via overeengekomen communicatiekanalen.	KO		
Eis Service Management 3.6	Inschrijver beschrijft maatregelen voor continuïteit en beheersing van afhankelijkheden binnen de dienstverlening.	KO		
Eis Service Management 3.7	Inschrijver monitort capaciteit proactief en adviseert tijdig over benodigde schaalvergroting/-verkleining of optimalisatie.	KO		
Eis Service Management 3.8	Inschrijver onderhoudt actuele configuratie- en beheerdocumentatie inclusief CMDB.	KO		
Eis Service Management 3.9	Inschrijver en Aanbestedende Dienst stellen gezamenlijk een SLA en DAP op voorafgaand aan ingebruikname van de dienstverlening.	KO		
Eis Service Management 3.10	Responstijden en KPI's worden vastgelegd in de SLA. Hiervoor gelden de volgende minimale responstijden: • Prioriteit 1 meldingen: maximaal 15 minuten; • Overige prioriteitsklassen: maximaal 1 uur. De exacte toepasselijkheid van servicewindows per prioriteitsklasse wordt vastgelegd in de SLA. Inschrijver realiseert maandelijks minimaal 95% naleving van de overeengekomen responstijden, gemeten per prioriteitsklasse op basis van geregistreerde meldingen in het IT Service Management systeem.	KO		
Eis Service Management 3.11	Prioriteiten van meldingen worden vastgesteld conform gezamenlijk overeengekomen classificaties.	KO		
Eis Service Management 3.12	Oplostijden per prioriteitsklasse worden vastgelegd in de SLA. De volgende minimale oplostijden gelden: • Prioriteit 1: binnen 4 uur, 24x7. • Prioriteit 2: binnen 8 uur binnen overeengekomen servicewindows. • Prioriteit 3: binnen 3 werkdagen binnen overeengekomen servicewindows. • Prioriteit 4: binnen 10 werkdagen binnen overeengekomen servicewindows. Inschrijver realiseert maandelijks minimaal 95% naleving van de overeengekomen oplostijden, gemeten per prioriteitsklasse. Metingen vinden plaats op basis van geregistreerde meldingen in het IT Service Management systeem.	KO		

Eis Service Management 3.13	Back-up, recovery en continuïteitsafspraken inclusief RPO en RTO worden vastgelegd in de SLA, met een minimale RPO van 4 uur en een RTO van 24 uur.	KO		
Eis Service Management 3.14	Inschrijver levert periodiek rapportages over dienstverlening, incidenten, wijzigingen en afgesproken KPI's.	KO		
Eis Service Management 3.15	Inschrijver rapporteert periodiek over lifecycle-management van relevante hardware- en softwarecomponenten.	KO		
Eis Service Management 3.16	Na ernstige incidenten levert de Inschrijver, binnen 5 werkdagen, een Root Cause Analysis (RCA) inclusief verbetermaatregelen.	KO		
Eis Service Management 3.17	Minimale servicewindows worden vastgelegd in de SLA. Van maandag t/m vrijdag van 8:00 tot 18:00 uur, uitgezonderd erkende Nederlandse feestdagen. Inschrijver biedt de mogelijkheid om dit service window te verruimen naar maximaal 24 uur x 7, bij verandering van de dienstverlening van Aanbestedende Dienst.	KO		
Eis Service Management 3.18	De IT Service Management tooling van Inschrijver dient koppelbaar zijn aan de IT Service Management tooling van de Aanbestedende Dienst.			WE
Eis Service Management 3.19	Geplande onderhoudswerkzaamheden worden uitgevoerd binnen overeengekomen onderhoudsvensters en tijdig aangekondigd. Bij wijzigingen die leiden tot down-time van de applicatie wordt onderhoud altijd buiten kantooruren (na 18.00 uur) uitgevoerd en minimaal 5 werkdagen van te voren aangekondigd. Bij spoedwijzigingen mag, in overleg met Opdrachtgever, hiervan wordt afgeweken.	KO		

4. Governance en Samenwerking eisen

Governance en Samenwerking eisen				
Eis Governance en Samenwerking 4.1	Inschrijver werkt aantoonbaar samen met Aanbestedende Dienst en betrokken leveranciers door tijdige afstemming, informatievoorziening en deelname aan governance-overleggen.	KO		
Eis Governance en Samenwerking 4.2	Inschrijver neemt deel aan operationele, tactische en strategische overleggen conform overeengekomen governance afspraken.	KO		
Eis Governance en Samenwerking 4.3	Innovatie en continue verbetering maken onderdeel uit van de governance cyclus. Inschrijver en Aanbestedende Dienst evalueren periodiek technologische ontwikkelingen en optimalisaties.		BI	
Eis Governance en Samenwerking 4.4	Inschrijver stelt vaste contactpunt beschikbaar voor operationeel, tactisch en strategisch niveau.	KO		
Eis Governance en Samenwerking 4.5	Inschrijver levert periodiek een roadmap voor lifecycle management en doorontwikkeling van de dienstverlening.	KO		
Eis Governance en Samenwerking 4.6	Inschrijver faciliteert kennisoverdracht en samenwerking tussen betrokken beheer- en ontwikkelteams.	KO		
Eis Governance en Samenwerking 4.7	Rollen, verantwoordelijkheden en afhankelijkheden worden vastgelegd in een gezamenlijk vastgesteld RACI-model tussen alle betrokken partijen	KO		
Eis Governance en Samenwerking 4.8	Inschrijver adviseert periodiek over relevante technologische ontwikkelingen en optimalisaties.		BI	
Eis Governance en Samenwerking 4.9	Inschrijver richt de dienstverlening zodanig in dat migratie naar een andere leverancier redelijk uitvoerbaar blijft. De dienstverlening ondersteunt: • open standaarden;	KO		

	• overdraagbaarheid; • exporteerbaarheid van data en configuraties; • actuele documentatie.			
Eis Governance en Samenwerking 4.10	Inschrijver beschikt over een formeel escalatieproces voor operationele, tactische en strategische issues.	KO		
Eis Governance en Samenwerking 4.11	Governance afspraken over besluitvorming, wijzigingen en risicoacceptatie worden vastgelegd in het DAP.	KO		
Eis Governance en Samenwerking 4.12	Inschrijver is verplicht om binnen een multi-vendor omgeving te acteren.		BI	

5. Hosting- en Beheer eisen

Hosting- en Beheer eisen				
Eis Hosting en Beheer 5.1	Inschrijver verzorgt het technisch beheer van de overeengekomen infrastructuur en platformdiensten inclusief monitoring en operationeel beheer.	KO		
Eis Hosting en Beheer 5.2	Inschrijver bewaakt en controleert de werking van back-upvoorzieningen en rapporteert hierover periodiek.	KO		
Eis Hosting en Beheer 5.3	Inschrijver test periodiek fail-over- en back-upvoorzieningen en stelt resultaten beschikbaar aan opdrachtgever.	KO		
Eis Hosting en Beheer 5.4	Inschrijver voert periodieke restoretesten uit en documenteert de resultaten.	KO		
Eis Hosting en Beheer 5.5	Inschrijver richt geautomatiseerd logbeheer en logretentie in conform wet- en regelgeving en overeengekomen bewaartermijnen.	KO		
Eis Hosting en Beheer 5.6	Voor OTAP-omgevingen gelden passende logretentie- en opschoningsprocessen conform classificatie van gegevens.	KO		
Eis Hosting en Beheer 5.7	De SLA bevat per kritieke dienst de overeengekomen beschikbaarheidsdoelstellingen. Waarbij een minimaal percentage van 99,95% wordt gehanteerd. De Opdrachtnemer biedt de mogelijkheid om dit te verhogen naar max. 99,995% bij verandering in de dienstverlening van de Aanbestedende Dienst.		BI	
Eis Hosting en Beheer 5.8	Inschrijver verleent medewerking aan performancetesten en ondersteunt opvolging van bevindingen binnen de eigen verantwoordelijkheid.	KO		
Eis Hosting en Beheer 5.9	De dienstverlening omvat bescherming tegen malware, virussen en schadelijke software. De software uit landen met een offensief cyberprogramma tegen Nederlandse belangen (zoals Rusland, China, Iran, Noord-Korea).is niet toegestaan	KO		
Eis Hosting en Beheer 5.10	De Inschrijver definieert en beheert de infrastructuur conform Infrastructure as Code (IaC).	KO		
Eis Hosting en Beheer 5.11	Inschrijver levert en beheert alle benodigde licenties voor de overeengekomen dienstverlening.	KO		
Eis Hosting en Beheer 5.12	De oplossing ondersteunt aansluiting op de Haagse Ring VPN van SSC-ICT.	KO		
Eis Hosting en Beheer 5.13	Inschrijver is verplicht ondersteuning aan te bieden voor veilige koppelingen met externe infrastructuur en dienstverlening van derden.	KO		
Eis Hosting en Beheer 5.14	De dienstverlening ondersteunt geografische redundantie tussen fysiek gescheiden datacenterlocaties.	KO		
Eis Hosting en Beheer 5.15	Inschrijver voorziet in synchrone replicatie op het moment dat de dienstverlening van Aanbestedende Dienst daarom vraagt (bijv. dienstverlening voor burgers)		BI	
Eis Hosting en Beheer 5.16	Inschrijver heeft aantoonbare betrokkenheid bij relevante Nederlandse datacenter- en Cloud initiatieven, zoals de Dutch Datacenter Association (DDA)			WE

Eis Hosting en Beheer 5.17	De dienstverlening omvat lifecycle-management inclusief: • periodieke updates; • security patching; • gecontroleerde upgrades; • compatibiliteitsbeheer.	KO		
Eis Hosting en Beheer 5.18	Inschrijver monitort beschikbaarheid, capaciteit en technische gezondheid van de dienstverlening proactief.	KO		
Eis Hosting en Beheer 5.19	Securitypatches worden tijdig verwerkt conform overeengekomen classificaties en risico-inschattingen	KO		
Eis Hosting en Beheer 5.20	De dienstverlening ondersteunt aantoonbaar herstel van systemen, data en configuraties.	KO		

6. Architectuur eisen

Architectuur eisen				
Eis Architectuur 6.1	De oplossing ondersteunt monitoring, alerting en end-to-end ketenmonitoring, met bijbehorende tooling (zoals Prometheus, Loki en Grafana)	KO		
Eis Architectuur 6.2	De Inschrijver draagt zorg voor een Low-level design (LLD) en High-level design (HLD) voor aanvang van de dienstverlening en onderhoud deze geduurde de gehele looptijd van de overeenkomst.	KO		
Eis Architectuur 6.3	Architectuur ondersteunt scheiding tussen productie, test, acceptatie en ontwikkelomgevingen. OTAP-omgevingen zijn logisch en/of fysiek gescheiden ingericht.	KO		
Eis Architectuur 6.4	De architectuur ondersteunt netwerk-, tenant- en data-isolatie inclusief role-based toegangsbeheer.	KO		
Eis Architectuur 6.5	Inschrijver beschikt aantoonbaar over ervaring met: • containerplatformen; • orkestratieplatformen (beheer); • virtualisatie; • bare-metal infrastructuur.	KO		
Eis Architectuur 6.6	De oplossing ondersteunt gangbare CI/CD- en GitOps-processen inclusief integratie met bestaande deploymenttooling.	KO		
Eis Architectuur 6.7	Inschrijver past moderne beheerprincipes toe gericht op automatisering, betrouwbaarheid en schaalbaarheid, zowel op -als afschalen.	KO		
Eis Architectuur 6.8	Kosten en resourceverbruik zijn inzichtelijk en herleidbaar.	KO		
Eis Architectuur 6.9	De oplossing ondersteunt hybride infrastructuurmodellen en integratie met verschillende hostingomgevingen.	KO		
Eis Architectuur 6.10	Inschrijver treft passende technische en organisatorische maatregelen om hoge beschikbaarheid van kritische systemen te waarborgen.	KO		
Eis Architectuur 6.11	De architectuur ondersteunt redundantie over meerdere fysiek gescheiden datacenterlocaties.	KO		
Eis Architectuur 6.12	Architectuur ondersteunt schaalbare opslag en compute-capaciteit	KO		
Eis Architectuur 6.13	Inschrijver neemt deel aan periodieke architectuur overleggen en ondersteunt doorontwikkeling binnen overeengekomen scope.	KO		
Eis Architectuur 6.14	De oplossing ondersteunt een container registry compatibel met gangbare container- en CI/CD-tooling.	KO		
Eis Architectuur 6.15	SSL/TLS-terminatie wordt zodanig ingericht dat beschikbaarheid, schaalbaarheid en beveiliging van applicaties worden ondersteund.	KO		

Eis Architectuur 6.16	De architectuur ondersteunt netwerksegmentatie en veilige scheiding tussen intern en extern verkeer conform gangbare architectuurprincipes.	KO		
Eis Architectuur 6.17	De oplossing ondersteunt veilige en flexibel configureerbare koppelingen met externe systemen.	KO		
Eis Architectuur 6.18	Inschrijver heeft de oplossing een voorkeur voor open standaarden en breed ondersteunde open-source componenten.		BI	

7. Applicaties eisen

Applicaties eisen				
Eis Applicaties 7.1	Inschrijver werkt gedurende de uitvoering van de Overeenkomst samen met huidige leveranciers van Aanbestedende Dienst voor zover dit noodzakelijk is voor een goede uitvoering van de dienstverlening.	KO		
Eis Applicaties 7.2	De oplossing kan onder belasting naar tevredenheid werken. Dit betekent: • Concurrent users: 6.000 tegelijkertijd ingelogde gebruikers • Belastende gebruikers: 10.000 ingevulde formulieren per uur op het portaal, uitgaande van een doorlooptijd van een half uur per gebruiker • Het op- en afschalen van resources is mogelijk.	KO		
Eis Applicaties 7.3	Het laden van een pagina of een andere actie op het klantportaal mag maximaal 3 seconden duren, ook bij maximale belasting. Vertraging aan de Client zijde wordt hierin niet meegenomen (meten op server-side). Als voorbeelden van acties: • Het openen van schermen en webformulieren; • Het toevoegen van documenten; • Het zetten van een nieuwe status; • Het tonen van zoekresultaten; • Het aanmaken van een contactmoment.	KO		
Eis Applicaties 7.4	De Inschrijver dient aan te tonen hoe de aangeboden infrastructuur en configuratie bijdragen aan het behalen van de performance-eisen zoals deze gelden voor Venus. Hiertoe wordt voorafgaand aan implementatie een meetmethodiek vastgesteld, inclusief tooling, meetmomenten en acceptatiecriteria.	KO		
Eis Applicaties 7.5	Data & Back-Up: • Backups encrypted (AES-256) • Opslag in NL/EU • Test restore 2x per jaar		BI	
Eis Applicaties 7.6	Compliance & audits: • Verwerkersovereenkomst; • Data Protection Impact Assessment (DPIA); • Jaarlijkse ISAE3402 type II rapportage van de leverancier.	KO		
Eis Applicaties 7.7	De oplossing moet ondersteuning bieden voor managed PostgreSQL en voorzien in • automatische back-ups; • point-in-time recovery.	KO		
Eis Applicaties 7.8	De aangeboden oplossing dient tooling (zoals Prometheus, Loki en Grafana) te bieden voor centrale en geïntegreerde monitoring, logging en visualisatie (dashboards) van platform- en applicatiegegevens.	KO		
Eis Applicaties 7.9	De aangeboden oplossing dient aantoonbaar geschikt te zijn voor het hosten van een bestaande container-gebaseerde	KO		

	applicatieomgeving die afhankelijk is van een Kubernetes-gebaseerde orchestratie.			
Eis Applicaties 7.10	De aangeboden oplossing dient ondersteuning te bieden voor: • het geautomatiseerd en reproduceerbaar uitrollen van applicaties en bijbehorende configuraties; • het kunnen definiëren en beheren van uitbreidingen op de standaard platformfunctionaliteit; • het betrouwbaar uitvoeren en beheren van zowel stateless als stateful applicatie-componenten, inclusief opslag-intensieve processen.	KO		
Eis Applicaties 7.11	De aangeboden oplossing dient ondersteuning te bieden voor gestandaardiseerde mechanismen voor ingress en routering van verkeer, zodanig dat bestaande configuraties zonder ingrijpende aanpassingen kunnen worden voortgezet.	KO		
Eis Applicaties 7.12	De aangeboden oplossing dient te voorzien in logging die centraal ontsloten, doorzoekbaar en beschikbaar is voor de opdrachtgever en applicatiebeheerpartij van Venus, zodat beheer, troubleshooting en analyse zonder belemmeringen kunnen plaatsvinden.	KO		
Eis Applicaties 7.13	Bewaartermijnen voor logging worden vastgesteld op basis van een risicoafweging volgens de BIO en het noodzakelijkheidbeginsel uit de AVG. Afhankelijk van het doel (bijv. detectie, forensisch onderzoek, audit) kunnen verschillende bewaartermijnen gelden.	KO		
Eis Applicaties 7.14	De aangeboden oplossing dient geschikt te zijn voor het beheren van meerdere projecten en clusters, waarbij: • Role-based access control per project of omgeving kan worden ingericht; • Centrale governance over meerdere clusters mogelijk is.	KO		

8. Migratie eisen

Migratie eisen				
Eis Migratie 8.1	Inschrijver hanteert een aantoonbare migratieaanpak gericht op: • continuïteit van dienstverlening; • beperking van verstoringen; • minimale noodzakelijke aanpassingen aan applicaties en configuraties.	KO		
Eis Migratie 8.2	Migraties worden uitgevoerd met minimale impact op beschikbaarheid van dienstverlening.		BI	
Eis Migratie 8.3	OTAP-omgevingen worden gecontroleerd en gefaseerd gemigreerd conform overeengekomen migratieplanning.	KO		
Eis Migratie 8.4	De migratieaanpak omvat: • kennisoverdracht; • gecontroleerde overgangsfasen; • overdracht van beheer- en architectuur documentatie.	KO		
Eis Migratie 8.5	Voorafgaand aan migratie wordt een risicoanalyse uitgevoerd inclusief beheersmaatregelen en fallbackscenario's.	KO		
Eis Migratie 8.6	End-of-life componenten worden voorafgaand aan of tijdens migratie geïnventariseerd en voorzien van passende mitigerende maatregelen of vervanging.	KO		
Eis Migratie 8.7	Inschrijver stelt voorafgaand aan migratie een migratieplan op inclusief: • fasering; • risicoanalyse; • fallbackscenario's; • testaanpak; • communicatiestructuur.	KO		

Eis Migratie 8.8	De migratieaanpak ondersteunt gecontroleerde terugvalscenario's bij verstoringen of mislukte migratiestappen.	KO		
Eis Migratie 8.9	Productie-ingebruikname vindt plaats na gezamenlijke acceptatie van overeengekomen test- en migratieresultaten.	KO		
Eis Migratie 8.10	Inschrijver borgt overdracht van kennis, configuraties en documentatie gedurende de migratieperiode.	KO		

9. Innovatie eisen

Innovatie eisen				
Eis Innovatie eisen 9.1	Inschrijver levert periodiek voorstellen voor optimalisatie van dienstverlening, beheer, beveiliging of kostenbeheersing		BI	
Eis Innovatie eisen 9.2	Inschrijver en Aanbestedende Dienst evalueren periodiek technologische ontwikkelingen en mogelijke verbeteringen van de dienstverlening		BI	
Eis Innovatie eisen 9.3	Voorstellen voor doorontwikkeling sluiten aan op: • beleidsdoelstellingen; • beveiligings- en compliance-eisen; • architectuur- en soevereiniteitskaders.		BI	
Eis Innovatie eisen 9.4	Inschrijver ondersteunt samenwerking gericht op continue optimalisatie van dienstverlening.		BI	
Eis Innovatie eisen 9.5	Inschrijver adviseert periodiek over technologische vernieuwing en lifecycle management van infrastructuur en hostingdiensten.		BI	
Eis Innovatie eisen 9.6	Inschrijver adviseert periodiek over optimalisatie van: • prestaties; • schaalbaarheid; • beschikbaarheid; • kosten van de dienstverlening.		BI	
Eis Innovatie eisen 9.7	Inschrijver informeert opdrachtgever periodiek over relevante technologische ontwikkelingen die impact kunnen hebben op de dienstverlening.		BI	
Eis Innovatie eisen 9.8	Inschrijver levert periodiek een roadmap voor technologische doorontwikkeling van de dienstverlening.		BI	
Eis Innovatie eisen 9.9	Inschrijver adviseert proactief over lifecycle-risico's en noodzakelijke modernisering.		BI	
Eis Innovatie eisen 9.10	Inschrijver ondersteunt verdere automatisering van beheer- en deployment processen		BI	
Eis Innovatie eisen 9.11	Inschrijver en Aanbestedende Dienst evalueren periodiek mogelijke verbeteringen op gebied van: • beschikbaarheid; • beveiliging; • beheerbaarheid; • kosten; • schaalbaarheid.		BI	

10. Gevolgen van niet naleving

Het Programma van Eisen bevat zowel niet-Bespreekbare eisen als eisen die betrekking hebben op de uitvoering van de Overeenkomst.

Tijdens de aanbestedingsfase
Inschrijver dient bij inschrijving te verklaren dat aan de niet-Bespreekbare eisen uit het Programma van Eisen zal worden voldaan.

Indien uit de Inschrijving blijkt dat Inschrijver niet voldoet aan één of meerdere niet-Bespreekbare eisen, of deze niet accepteert, wordt de inschrijving ongeldig verklaard en niet verder beoordeeld.

Tijdens de uitvoering van de Overeenkomst
De eisen uit het Programma van Eisen maken onderdeel uit van de Overeenkomst en dienen gedurende de looptijd van de Overeenkomst te worden nageleefd.

Indien tijdens de uitvoering van de Overeenkomst blijkt dat niet wordt voldaan aan één of meerdere eisen uit het Programma van Eisen, geldt dit als een tekortkoming in de nakoming van de Overeenkomst.

De Aanbestedende Dienst is in dat geval gerechtigd de Opdrachtnemer in de gelegenheid te stellen het gebrek binnen een redelijke termijn te herstellen.

Indien herstel uitblijft, of indien sprake is van een ernstige tekortkoming, is de Aanbestedende Dienst gerechtigd de Overeenkomst geheel of gedeeltelijk te ontbinden, onverminderd overige rechten van de Aanbestedende Dienst.