1e Nota van Inlichtingen

Versie 2 – gecorrigeerd

Behorende bij de Europese openbare aanbesteding ‘Leveren, implementeren en onderhouden van een Identity and Access Management-systeem’

Gemeente Zaanstad
Kenmerk: 2026-198
CPV-code: 48000000-8 Software en informatiesystemen
Datum: 1 september 2026
Vervangt de op 31 augustus 2026 gepubliceerde versie

Deze Nota van Inlichtingen maakt integraal onderdeel uit van de aanbestedingsstukken en prevaleert daarboven. De vragen zijn weergegeven in de volgorde waarin zij zijn ingediend en zonder vermelding van de indienende partij. Bij gelijksoortige vragen wordt in het antwoord verwezen naar de vraag waarin het onderwerp volledig is behandeld.

Erratum

Deze versie vervangt de op 31 augustus 2026 gepubliceerde 1e Nota van Inlichtingen. In die versie waren de onderstaande antwoorden niet in hun definitieve vorm opgenomen. De antwoorden op alle overige vragen zijn ongewijzigd.

Vraag 1 – de passage over de gelijktijdige publicatie van het gewijzigde Prijzenblad en de daaraan verbonden uitsluiting van verdere deelname is komen te vervallen.

Vraag 5 – aangevuld: het vervallen van eis E41 laat de eisen E42 en E45 onverlet. Ondersteuning voor Customer Managed Keys blijft via eis E45 een eis en is geen wens. De verwijzing naar FIPS 140-2 Level 3 duidt het vereiste beveiligingsniveau aan en niet een verplichte technische implementatie.

Vraag 31 – antwoord teruggebracht tot de kern: in afwijking van artikel 25 GIBIT 2025 verlangt Opdrachtgever geen Software Bill of Materials.

Vraag 60 – aangevuld: voor Gemeente Zaanstad wordt één HR-systeem (YouForce) aangesloten; de identiteiten van de partnerorganisaties worden handmatig in de Oplossing ingevoerd.

Vraag 82 – aangevuld: de API-gateway OpenTunnel is eigendom van Gemeente Zaanstad en valt onder het beheer en de verantwoordelijkheid van Opdrachtgever.

Vraag 115 – verduidelijkt ten aanzien van de export van audit- en loggegevens naar het SIEM.

Vraag 129 – gecorrigeerd: de gebruikerscodes in Bijlage 15 zijn gepseudonimiseerd en voor Inschrijver niet herleidbaar tot natuurlijke personen; zij zijn niet geanonimiseerd.

Gewijzigde en nieuwe aanbestedingsstukken

Naar aanleiding van deze Nota van Inlichtingen worden de volgende documenten in gewijzigde vorm gepubliceerd:

- Bijlage 3. Prijzenblad – de kostensoort ‘Kosten beheer/onderhoud/SLA’ is vervallen; voor de SaaS-variant wordt één integrale jaarlijkse vergoeding uitgevraagd (vraag 1).
- Bijlage 4. Referentieformulier – de omschrijving van de kerncompetentie is gelijkgetrokken met paragraaf 4.2.2 van de Offerteleidraad; nummering en referentieperiode zijn gecorrigeerd (vragen 13, 14, 121, 138 en 164).
- Bijlage 5. Programma van Eisen en Wensen – eis E41 komt te vervallen; de eisen E28, E32, E33, E34, E45 en E61 zijn aangepast of verduidelijkt (vragen 4, 5, 82, 123, 139, 142, 143, 147 en 196).
- Offerteleidraad – Bijlage 17 is toegevoegd aan het overzicht van bijlagen.
- Bijlage 17. IAM-systeem Zaanstad – Technische specificatie BINT-bestand (nieuw; vragen 84 en 156).

Inschrijver dient de gewijzigde versies van deze documenten te gebruiken. Daarnaast bepalen de antwoorden op de vragen 31, 60, 82, 108, 134 en 206 de scope of de procedure nader zonder dat een document wordt gewijzigd.

Nr.	Onderwerp	Vraag	Antwoord
1	**Offerteleidraad §2.9 / Concept Overeenkomst art. 7.3 — Prijsformule On-Premise (verduidelijking)**	In paragraaf 2.9 van de Offerteleidraad en artikel 7.3 van de concept Overeenkomst wordt de jaarlijkse licentievergoeding voor de On-Premise-variant vastgesteld op 80% van de op dat moment geldende jaarlijkse SaaS-licentiekosten. Kunt u bevestigen welke kostencomponenten onder 'SaaS-licentiekosten' worden verstaan? Betreft dit het volledige all-in jaarbedrag uit het Prijzenblad (inclusief hosting, onderhoud en support), of uitsluitend de licentiecomponent? Wij verzoeken u dit te verduidelijken, mede omdat bij een On-Premise-levering de hostingcomponent vervalt terwijl de verplichtingen ten aanzien van updates, patches, beveiliging en ondersteuning (E49, E54) onverkort blijven gelden.	Opdrachtgever bevestigt dat voor de toepassing van paragraaf 2.9 van de Offerteleidraad en artikel 7.3 van de conceptovereenkomst wordt uitgegaan van de totale jaarlijkse SaaS-vergoeding zoals opgenomen in het Prijzenblad. Onder deze vergoeding worden alle in de SaaS-dienstverlening inbegrepen componenten verstaan. De verhouding waarbij de jaarlijkse vergoeding voor de On-Premise-variant 80% bedraagt van de jaarlijkse SaaS-vergoeding betreft een bewust gekozen vaste systematiek voor het bepalen van de prijs van de On-Premise-variant. Opdrachtgever acht het niet noodzakelijk dat inschrijvers afzonderlijke kostensoorten binnen de SaaS-vergoeding uitsplitsen. Om dit te verduidelijken zal Opdrachtgever het Prijzenblad aanpassen. De kostensoort‘Kosten beheer/onderhoud/SLA’ komt daarbij te vervallen, zodat voor de SaaS-variant één integrale jaarlijkse vergoeding wordt uitgevraagd.
2	**Offerteleidraad §5.2.2 — Prijsformule On-Premise (suggestie tot aanpassing)**	De kostenopbouw van een SaaS- en een On-Premise-levering verschilt per leverancier, met name in het aandeel hostingkosten. Een vast percentage van 80% sluit daardoor niet noodzakelijk aan op de werkelijke kostenverhouding en kan leiden tot niet-kostendekkende dan wel kunstmatig verhoogde prijzen. Wij stellen voor dat inschrijvers in het Prijzenblad een separate jaarprijs voor de On-Premise-variant opgeven, die als vast onderdeel van de Inschrijving meeweegt in de beoordeling van G1.1, zodat de vergelijkbaarheid behouden blijft. Bent u bereid het Prijzenblad hierop aan te passen?	Nee, Opdrachtgever is niet bereid het Prijzenblad op dit punt aan te passen en handhaaft de systematiek waarbij de jaarlijkse vergoeding voor de On-Premise-variant 80% bedraagt van de jaarlijkse SaaS-vergoeding. De keuze voor een vast percentage dient de vergelijkbaarheid. Zoals toegelicht in paragraaf 5.2.2 van de Offerteleidraad is het bij een separaat op te geven On-Premise-jaarprijs niet mogelijk de inschrijvingen op een eerlijke en objectieve wijze met elkaar te vergelijken, omdat het leveringsmodel op het moment van Inschrijving nog niet vaststaat en het zwaartepunt van de uitvraag bij SaaS ligt. De hoogte van het percentage is in de markt getoetst. Naar aanleiding van de marktconsultatie heeft Opdrachtgever de deelnemende partijen die zowel een SaaS- als een On-Premise-variant konden leveren aanvullend bevraagd over de kostenverhouding tussen beide leveringsmodellen. Het percentage van 80% is de uitkomst van die uitvraag. Opdrachtgever acht de verhouding daarmee marktconform, redelijk en voldoende ruim om rekening te houden met verschillen in kostenstructuur tussen beide leveringsmodellen. Het staat Inschrijver vrij bij het bepalen van zijn tarieven rekening te houden met zijn eigen kostenstructuur en commerciële afwegingen. Zie voor de definitie van de grondslag het antwoord op vraag 1.
3	**Offerteleidraad §2.2 — Definitie SaaS / private hosting**	Onder de On-Premise-variant verstaat u een implementatie binnen infrastructuur onder direct beheer en directe zeggenschap van de gemeente. Kunt u bevestigen dat een door de leverancier gehoste private single-tenant omgeving (private cloud, gehost binnen de EER) binnen de SaaS-definitie van deze aanbesteding valt?	Ja. Een door Opdrachtnemer gehoste omgeving, waaronder een private cloud- of single-tenantomgeving binnen de EER, valt binnen de SaaS-definitie van deze aanbesteding. Onder de On-Premise-variant verstaat Opdrachtgever een implementatie waarbij de infrastructuur onder direct beheer en directe zeggenschap van Opdrachtgever staat. Een door Opdrachtnemer gehoste omgeving, ook indien deze dedicated of single-tenant is, valt hier niet onder.

Nr.	Onderwerp	Vraag	Antwoord
4	**Bijlage 5 PvE&W, eis E34 — Weggevallen conditie**	Eis E34 begint met de tekst 'dan voldoet deze aantoonbaar aan de meest actuele OWASP richtlijnen'. Kunt u bevestigen dat hier de conditie 'Indien de Oplossing als SaaS wordt geleverd' is bedoeld, dan wel de volledige eistekst publiceren?	Ja. Eis E34 is uitsluitend van toepassing indien de Oplossing als SaaS wordt geleverd. De voorwaarde “Indien de Oplossing als SaaS wordt geleverd” dient aan het begin van eis E34 te worden gelezen.
5	**Bijlage 5 PvE&W, eisen E41/E42 — Zero Knowledge en Customer Managed Keys**	Eis E41 hanteert de formulering 'voor alle componenten waar dit technisch mogelijk is'. Kunt u bevestigen dat een gemotiveerde toelichting per component — waarin wordt aangegeven waar het Zero Knowledge-principe en Customer Managed Keys wel en niet technisch toepasbaar zijn — als voldoen aan de eisen E41 en E42 wordt beschouwd?	Opdrachtgever erkent dat eis E41 onvoldoende aansluit bij de bevindingen uit de marktconsultatie. In het marktconsultatieverslag is opgenomen dat volledige zero-knowledge encryptie binnen IAM-/IGA-oplossingen niet gangbaar wordt geacht, omdat het platform identiteitsgegevens moet kunnen verwerken ten behoeve van functies zoals analyse, policy-evaluatie en provisioning. Opdrachtgever constateert dat hierover terecht vragen zijn gesteld in de Nota van Inlichtingen. Om deze reden komt eis E41 te vervallen. Het vervallen van E41 betekent niet dat de daarin genoemde onderwerpen als geheel komen te vervallen. Voor zover deze onderwerpen afzonderlijk zijn opgenomen in E42 en E45, blijven deze eisen onverminderd van kracht. Dit geldt in het bijzonder voor de in E45 expliciet opgenomen ondersteuning voor Customer Managed Keys (CMK) bij een SaaS-levering. CMK blijft daarmee een vereiste en is geen wens. Ook de overige eisen van E42 en E45 ten aanzien van informatiebeveiliging, encryptie, sleutelbeheer, bescherming van gegevens en integriteit van gegevensverwerking blijven onverminderd van toepassing. Ten aanzien van de verwijzing in E45 naar FIPS 140-2 Level 3 gecertificeerde HSM's verduidelijkt Opdrachtgever dat hiermee het vereiste beveiligings- en zekerheidsniveau wordt beoogd. De verwijzing naar FIPS 140-2 Level 3 dient niet te worden opgevat als een verplichting om uitsluitend deze specifieke technische implementatie toe te passen. Een gelijkwaardige of betere technische invulling van het HSM- en sleutelbeheer is toegestaan, mits Inschrijver aantoonbaar maakt dat hiermee een vergelijkbaar of hoger niveau van beveiliging en sleutelbeheer wordt gerealiseerd. Dit geldt eveneens indien voor het sleutelbeheer gebruik wordt gemaakt van dienstverlening van een hyperscaler, zoals Microsoft Azure of AWS.
6	**Bijlage 5 PvE&W, eisen E41/E42 — Zero Knowledge en Customer Managed Keys**	Eis E41 hanteert de formulering 'voor alle componenten waar dit technisch mogelijk is'. Kunt u bevestigen dat een gemotiveerde toelichting per component — waarin wordt aangegeven waar het Zero Knowledge-principe en Customer Managed Keys wel en niet technisch toepasbaar zijn — als voldoen aan de eisen E41 en E42 wordt beschouwd?	Zie antwoord vraag 5.
7	**Bijlage 5 PvE&W, eis E28 (Datapakhuis) — Keuze tussen varianten**	Kunt u bevestigen dat een inschrijver mag volstaan met één van de twee beschreven varianten (datadumps via SFTP óf een data-API), en dat de eis dat het volledig ophalen van alle data binnen maximaal 5 minuten plaatsvindt uitsluitend geldt indien voor de data-API-variant wordt gekozen?	Ja. Inschrijver mag volstaan met één van de beschreven varianten, te weten datadumps via SFTP óf een data-API. Indien wordt gekozen voor de data-API-variant, geldt de eis dat het volledig ophalen van alle data binnen maximaal 5 minuten plaatsvindt. Deze termijn van maximaal 5 minuten geldt onverkort, ongeacht de omvang van de op te halen dataset.

Nr.	Onderwerp	Vraag	Antwoord
8	**Bijlage 5 PvE&W wens W4 onderdeel C / Bijlage 13 FO §4.3-4.4 — Genest opbouwen van autorisaties**	In wens W4 onderdeel C en in het Functioneel Ontwerp (§4.3 en §4.4) wordt beschreven dat een basisautorisatie (level 1, applicatieaccount en basis-AD-groepen) genest wordt opgenomen in de functionele autorisaties (level 2) van dezelfde applicatie. Kunt u bevestigen dat een functioneel gelijkwaardige oplossing — waarbij de basisautorisatie eenmalig wordt ingericht en beheerd en automatisch wordt meegeleverd bij alle functionele autorisaties en procesrollen van dezelfde applicatie, zonder technische nesting of overerving in het autorisatiemodel — als volwaardige invulling van zowel wens W4 onderdeel C als de inrichting conform het Functioneel Ontwerp (eis E52) wordt beschouwd?	Ja. Opdrachtgever beschouwt een functioneel gelijkwaardige oplossing als een volwaardige invulling van wens W4 onderdeel C en van de inrichting conform eis E52, mits de basisautorisatie slechts éénmaal hoeft te worden ingericht en beheerd en automatisch wordt meegeleverd bij de functionele autorisaties en procesrollen van dezelfde applicatie. Technische nesting of overerving binnen het autorisatiemodel is daarbij geen doel op zich. De beschreven functionaliteit en het beoogde beheerresultaat zijn leidend.
9	**Concept Overeenkomst art. 5.3 — Fatale termijn en medewerkingsafhankelijkheid**	De einddatum van de Implementatieperiode (4 oktober 2027) geldt als fatale termijn. Kunt u bevestigen dat vertraging die aantoonbaar toerekenbaar is aan Opdrachtgever of aan door Opdrachtgever gecontracteerde derden — zoals de tijdige aanlevering van conversiedata, de beschikbaarheid van specialisten voor de YouForce- en Topdesk-koppelingen en het verlenen van netwerktoegang — leidt tot evenredige opschorting van deze fatale einddatum?	Ja. Indien vertraging in de implementatie aantoonbaar wordt veroorzaakt door Opdrachtgever of door Opdrachtgever gecontracteerde derden, wordt Opdrachtnemer hiervoor niet verantwoordelijk gehouden. In dat geval wordt bij de beoordeling van de overeengekomen implementatieplanning rekening gehouden met de betreffende vertraging en de invloed daarvan op de realisatie van de einddatum.
10	**Concept Overeenkomst art. 11.2 — Kosten tijdens Implementatieperiode**	Gedurende de Implementatieperiode is geen Gebruiksrechtenvergoeding verschuldigd. Kunt u verduidelijken of de hosting en beschikbaarstelling van de productie- en test-/acceptatieomgeving (eis E51) gedurende de Implementatieperiode geacht wordt onderdeel te zijn van de Implementatievergoeding?	Ja, eventuele kosten voor het beschikbaar stellen van productie-, test- en/of acceptatieomgevingen die benodigd zijn voor de implementatie, worden geacht onderdeel uit te maken van de Implementatievergoeding. Tot aan het moment van Ingebruikname is hiervoor geen afzonderlijke Gebruiksrechtenvergoeding verschuldigd.
11	**Concept Overeenkomst art. 10.2 — Updates versus Upgrades**	Kunt u bevestigen dat reguliere functionele releases die onderdeel zijn van het standaard onderhoud (eis E54) kwalificeren als Update in de zin van de GIBIT 2025 en derhalve zonder aanvullende vergoeding worden geleverd en geïmplementeerd?	Ja. Reguliere functionele releases die onderdeel uitmaken van het standaard onderhoud als bedoeld in eis E54 worden beschouwd als Updates in de zin van de GIBIT 2025. Deze Updates maken onderdeel uit van de overeengekomen dienstverlening en worden zonder aanvullende vergoeding geleverd.
12	**Concept Overeenkomst art. 9 — Security- en penetratietesten in acceptatie**	Kunt u bevestigen dat de scope van de security- en penetratietesten binnen de acceptatieprocedure in overleg tussen partijen wordt vastgesteld, dan wel dat de jaarlijkse onafhankelijke penetratietest (eis E35) hiervoor kan worden benut?	Ja. De scope van eventuele security- en penetratietesten in het kader van de acceptatieprocedure na implementatie wordt in overleg tussen Opdrachtgever en Opdrachtnemer vastgesteld. De beoordeling van de security-eisen die onderdeel zijn van de geschiktheidsbeoordeling en de PoC maakt geen onderdeel uit van deze acceptatieprocedure. Bij de acceptatie na implementatie wordt, voor zover relevant, beoordeeld of de Oplossing conform de overeengekomen security-eisen is ingericht en functioneert, bijvoorbeeld ten aanzien van integraties en SSO. Een recente onafhankelijke penetratietest als bedoeld in eis E35 kan hierbij worden benut, mits de geteste omgeving en componenten representatief zijn voor de productieomgeving waarin de dienstverlening aan Opdrachtgever wordt geleverd.

Nr.	Onderwerp	Vraag	Antwoord
13	**Bijlage 4 Referentieformulier vs. Offerteleidraad §4.2.2 — Reikwijdte kerncompetentie**	In paragraaf 4.2.2 van de Offerteleidraad luidt de kerncompetentie '...bij een gemeente, of een gemeenschappelijke regeling of een vergelijkbare (semi)publieke organisatie'. In Bijlage 4 (Referentieformulier) ontbreekt het element 'of een vergelijkbare (semi)publieke organisatie'. Kunt u bevestigen welke formulering leidend is?	De formulering zoals opgenomen in de Offerteleidraad, paragraaf 4.2.2, is leidend. Bijlage 4. Referentieformulier wordt naar aanleiding hiervan aangepast, zodat de formulering aansluit op paragraaf 4.2.2 van de Offerteleidraad. De aangepaste versie van Bijlage 4 wordt als gewijzigd document bij deze Nota van Inlichtingen gepubliceerd.
14	**Bijlage 4 Referentieformulier / Bijlage 13 FO — Onvolkomenheden in documenten**	In Bijlage 4 springt de nummering van rij 2 naar rij 5 en lijkt in rij 6 het woord 'jaar' te ontbreken ('in de afgelopen drie uitgevoerd'). Daarnaast vermeldt Bijlage 13 (Functioneel Ontwerp) het kenmerk 2025-198, terwijl de aanbesteding kenmerk 2026-198 draagt. Kunt u bevestigen dat de documenten volledig en juist zijn, dan wel herziene versies publiceren?	Dank voor uw oplettendheid. De nummering in Bijlage 4 is gecorrigeerd en het ontbrekende woord 'jaar' is toegevoegd. Het gewijzigde Bijlage 4 (Referentieformulier) wordt als gewijzigd document bij deze Nota van Inlichtingen gepubliceerd. In bijlagen 5, 13 en 14 stond het onjuiste kenmerk 2025-198 vermeld in plaats van 2026-198. Het betrof wel de actuele documenten; daarom is uitsluitend het kenmerk aangepast.
15	**Offerteleidraad §4.2.2 / Bijlage 4 — Uitvoeringstermijn bij doorlopende contracten**	De referentie-eis stelt dat de uitvoering niet langer dan drie jaar geleden mag zijn, gerekend vanaf de sluitingsdatum van de Inschrijving. Kunt u bevestigen dat een referentieopdracht waarvan de implementatie is afgerond en waarvan de overeenkomst (levering en onderhoud) op het moment van inschrijving nog doorloopt, aan deze eis voldoet, en wat in dat geval als 'datum afronding' op het Referentieformulier dient te worden ingevuld?	Ja, met een kleine nuance. Een referentieopdracht voldoet aan de referentie-eis indien de implementatie van de aangeboden oplossing niet langer dan drie jaar vóór de sluitingsdatum van de inschrijving succesvol is afgerond - mits de aangeboden oplossing minstens zes maanden voor productieve doeleinden in gebruik is. Het feit dat de overeenkomst voor levering, gebruik en/of onderhoud op het moment van inschrijving nog doorloopt, staat hier niet aan in de weg. Op het Referentieformulier dient als datum afronding de datum te worden vermeld waarop de implementatie is afgerond en de oplossing in gebruik is genomen.
16	**Bijlage 13 FO §4.5 (Figuur 11) / Bijlage 5 wens W5 — Netto rechten in bundeltickets**	In het Functioneel Ontwerp (§4.5, Figuur 11) wordt beschreven dat een bundelticket uitsluitend de netto (nieuwe) rechten vermeldt, terwijl wens W5 vraagt dat zowel de wijziging (delta) als de reeds toegekende rechten in het bundelticket worden opgenomen. Kunt u verduidelijken welke werkwijze leidend is, en of een alternatieve presentatie (de delta met duidelijke markering van reeds bestaande rechten) als volwaardige invulling wordt beschouwd?	Wens W5 is leidend. Opdrachtgever staat een alternatieve presentatie toe, mits hiermee dezelfde functionaliteit wordt gerealiseerd. Dit betekent dat zowel de gevraagde wijziging (delta) als de reeds toegekende rechten voor de beoordelaar inzichtelijk zijn. Een presentatie waarbij de delta duidelijk wordt onderscheiden van reeds toegekende rechten wordt daarom beschouwd als een volwaardige invulling van wens W5.
17	**Bijlage 13 FO §2 — Meerdere Identiteitscontainers per persoon**	Kunt u een indicatie geven van het aantal medewerkers dat naar verwachting gelijktijdig in meerdere Identiteitscontainers voorkomt (in het Functioneel Ontwerp aangeduid als 'komt een enkele keer voor'), zodat dit correct in de implementatie kan worden meegenomen?	Opdrachtgever verwacht dat minder dan 20 medewerkers gelijktijdig in meerdere Identiteitscontainers voorkomen. In de praktijk betreft dit veelal een tijdelijke situatie als gevolg van een doorstroom van de ene organisatie naar een andere organisatie.
18	**Bijlage 13 FO §2.6 — Fasering signalering en attestatie**	In §2.6 van het Functioneel Ontwerp wordt de wens genoemd om de signalering bij doorstroom en de periodieke controle (attestatie) van procesrollen te verbeteren. Kunt u bevestigen of dit onderdeel dient te zijn van de implementatie vóór de uiterlijke implementatiedatum van 4 oktober 2027, of dat dit in een latere fase gedurende de looptijd van de Overeenkomst kan worden gerealiseerd?	Wens W1B is leidend. Deze wordt beoordeeld op basis van de functionaliteit die ten tijde van de inschrijving beschikbaar is en gedemonstreerd kan worden. Indien de functionaliteit pas in een latere fase gedurende de looptijd van de Overeenkomst beschikbaar komt, kan Opdrachtgever deze functionaliteit niet betrekken bij de beoordeling. Dit laat onverlet dat de functionaliteit, indien onderdeel van de aangeboden oplossing, uiterlijk op de overeengekomen implementatiedatum beschikbaar dient te zijn.

Nr.	Onderwerp	Vraag	Antwoord
19	**Bijlage 13 FO §2.5 — Overrulen HR-koppeling bij onmiddellijk ontslag**	Kunt u het gewenste mechanisme voor het overrulen van de HR-koppeling bij ontslag op staande voet (§2.5) nader specificeren: dient dit geautomatiseerde systeemfunctionaliteit te zijn, of volstaat een handmatige actie door een geautoriseerde beheerder waarbij het account direct wordt geblokkeerd zonder dat de toegekende autorisaties worden ingetrokken?	Wens W1C is leidend. Een handmatige actie door een geautoriseerde beheerder volstaat. Daarbij wordt het account direct geblokkeerd, wat leidt tot het direct inactief zetten van het AD-account en de toegangspas, zodat verdere toegang tot systemen en gegevens via deze account wordt voorkomen. Geautomatiseerde systeemfunctionaliteit is hiervoor niet vereist. De reeds toegekende autorisaties worden daarbij niet ingetrokken.
20	**Bijlage 13 FO, bijlage 5 (Topdesk) — Vertaling organisatiehiërarchie**	Voor de vertaling van de organisatiehiërarchie (vijf HR-niveaus) naar de drie Topdesk-niveaus worden drie realisatievormen genoemd (script, csv-import of frontend-invoer). Heeft u een voorkeur voor één van deze realisatievormen, of is de inschrijver vrij hierin een voorstel te doen?	Opdrachtgever heeft geen voorkeur voor een realisatie via script, csv-import of frontend-invoer. Het staat Inschrijver vrij een passende oplossing voor te stellen, mits daarmee de gewenste vertaling van de organisatiehiërarchie naar de Topdesk-structuur wordt gerealiseerd.
21	**Bijlage 13 FO, bijlage 5 (Topdesk) — Volledigheid vertaalregels**	Kunt u bevestigen dat de beschreven vertaalregels voor de organisatiehiërarchie (waaronder de lengte van de korte code en de genoemde uitzonderingen, zoals orgEenheidId 180 en het bereik 184–564) volledig en uitputtend zijn, of dat aanvullende uitzonderingen bestaan die niet in het document zijn opgenomen?	Nee. De organisatiehiërarchie is niet volledig en eenduidig af te leiden uit de lengte van het organisatie-id. De in het Functioneel Ontwerp genoemde voorbeelden en uitzonderingen zijn bedoeld ter illustratie van de huidige situatie en dienen niet als uitputtende set van vertaalregels. De organisatiehiërarchie dient te worden afgeleid op basis van de onderliggende structuur en relaties. Daarbij geldt dat een cluster altijd uit 2 posities bestaat. Afdelingen vallen onder een cluster waarbij de eerste 2 posities van het afdelingsnummer overeenkomen met het cluster waaronder de afdeling valt. Omdat sommige clusters meer dan 10 afdelingen bevatten, worden afdelingen soms met 3 en soms met 4 posities aangeduid. Dit werkt ook door naar de teams binnen een afdeling, die daardoor soms met 4 en soms met 5 posities worden aangeduid.
22	**Bijlage 13 FO §4 — Omvang ICT-rollenregister**	Kunt u een indicatie geven van het totale aantal autorisaties (level 1 en level 2) dat initieel in het autorisatieregister moet worden ingericht, in aanvulling op de genoemde aantallen processen en procesrollen?	Op basis van de huidige situatie gaat Opdrachtgever uit van: • circa 85 basisaccounts (level 1); • circa 1.315 rechten binnen de basisaccounts (level 2); • circa 663 eenvoudige, niet-geneste en zelfstandig aan te vragen autorisaties (level 3). Deze aantallen zijn indicatief en gebaseerd op de beschikbare conversiedata. Nadere informatie is opgenomen in Bijlage 15. IAM-systeem Zaanstad - Voorbeeld Conversiedata.xlsx. De genoemde aantallen kunnen worden afgeleid door te filteren op de relevante waarden in kolom D.
23	**Offerteleidraad §4.2.4 — SOC 2 Type II-rapportage (gelijkwaardigheid)**	In paragraaf 4.2.4 wordt bij inschrijving een assuranceverklaring van een Register EDP-Auditor in de vorm van een SOC 2 Type II-rapportage (ISAE 3000) verlangd, niet ouder dan 12 maanden. Kunt u bevestigen dat gelijkwaardige assurancevormen eveneens worden geaccepteerd, zoals een ISAE 3402 Type II-rapportage, dan wel een combinatie van een geldig ISO 27001-certificaat met Verklaring van Toepasselijkheid, de meest recente (her)certificerings- of surveillance-auditrapportage van de geaccrediteerde certificerende instelling en rapportages van onafhankelijke penetratietesten, waarmee de werking van de beveiligings- en beheersingsmaatregelen eveneens aantoonbaar wordt gemaakt?	Opdrachtgever handhaaft de eis zoals opgenomen in paragraaf 4.2.4 en verduidelijkt deze als volgt. Een ISAE 3402 Type II-rapportage wordt uitsluitend als gelijkwaardig geaccepteerd indien deze (i) is afgegeven door een Register EDP-Auditor, (ii) op de sluitingsdatum van de Inschrijving niet ouder is dan 12 maanden, en (iii) qua reikwijdte aantoonbaar de informatiebeveiligings- en beheersingsmaatregelen omvat die relevant zijn voor de aangeboden Oplossing, ten minste vergelijkbaar met de principes beveiliging, beschikbaarheid en vertrouwelijkheid uit een SOC 2 Type II-rapportage. Inschrijver dient deze gelijkwaardigheid bij Inschrijving aan te tonen. De voorgestelde combinatie van een ISO 27001-certificaat met Verklaring van Toepasselijkheid, (her)certificerings- of surveillance-auditrapportages en

Nr.	Onderwerp	Vraag	Antwoord
			penetratietestrapportages wordt niet als gelijkwaardig geaccepteerd. Een ISO 27001-certificering is een certificering van het managementsysteem en geen assuranceverklaring: zij bevat geen onafhankelijk assurance-oordeel over de effectieve werking van de individuele beheersingsmaatregelen over een aaneengesloten rapportageperiode. Certificerings- en surveillancerapportages zijn voor een ander doel opgesteld en penetratietesten betreffen een technische momentopname; ook in combinatie bieden deze documenten niet de zekerheid die met een Type II-assurancerapportage wordt verkregen. Opdrachtgever wijst er daarbij op dat het ISO 27001-certificaat met Verklaring van Toepasselijkheid in paragraaf 4.2.4 reeds afzonderlijk is vereist; de assuranceverklaring dient een aanvullend doel, namelijk het aantonen van de werking van de getroffen maatregelen. Opdrachtgever denkt graag mee met partijen die op dit moment nog niet over een SOC 2 Type II-rapportage beschikken en biedt daarom het volgende alternatief. Indien het verkrijgen van een SOC 2 Type II-rapportage binnen de inschrijvingstermijn redelijkerwijs niet haalbaar is, wordt eveneens geaccepteerd: een assurancerapportage waarbij een Register EDP-Auditor conform de ISAE 3000-standaard een audit heeft uitgevoerd met de beheersingsmaatregelen uit de Verklaring van Toepasselijkheid (ISO 27001, Annex A) als toetsingskader. Deze rapportage dient aan dezelfde eisen te voldoen als de gevraagde SOC 2 Type II-rapportage: zij bevat een onafhankelijk assurance-oordeel over de effectieve werking van de beheersingsmaatregelen over een aaneengesloten rapportageperiode (Type II) en is op de sluitingsdatum van de Inschrijving niet ouder dan 12 maanden. Opdrachtgever wil benadrukken dat het doel en niet het middel centraal staat. Een SOC 2 Type II (ISAE 3000)-rapportage is voor Opdrachtgever geen doel op zich, maar een middel om aantoonbaar en onafhankelijk inzicht te verkrijgen in de werking van de beveiligings- en beheersmaatregelen van een voor de beveiliging van Opdrachtgever kritieke voorziening. Opdrachtgever verwacht daarbij niet dat iedere tekortkoming afwezig is, maar dat tekortkomingen tijdig worden geïdentificeerd, transparant worden gemaakt, van passende verbetermaatregelen worden voorzien en binnen een redelijke termijn aantoonbaar worden beheerst of opgelost.
24	**Offerteleidraad §4.2.4 — SOC 2 Type II-rapportage (suggestie tot aanpassing)**	Een SOC 2 Type II-rapportage vereist een observatieperiode van doorgaans zes tot twaalf maanden, gevolgd door audit en rapportage. Leveranciers die niet reeds over een dergelijke rapportage beschikken, kunnen deze vóór de sluitingsdatum van 2 oktober 2026 feitelijk niet meer verwerven, ongeacht het daadwerkelijke niveau van hun informatiebeveiliging. In de Nederlandse IAM-markt is een SOC 2- of ISAE 3000-rapportage bovendien geen gangbare marktstandaard; informatiebeveiliging wordt in deze markt doorgaans aangetoond via ISO 27001-certificering, periodieke externe audits en onafhankelijke penetratietesten — óók bij opdrachtgevers in overheid, zorg en andere sterk gereguleerde sectoren. De eis beperkt daarmee de mededinging tot een klein aantal partijen dat reeds over een	Nee. Opdrachtgever handhaaft de eis uit paragraaf 4.2.4 en acht deze proportioneel. Het IAM-systeem is een voor de toegangsbeveiliging van de gemeentelijke informatievoorziening kritieke voorziening. Opdrachtgever hecht er daarom aan dat bij Inschrijving onafhankelijk is vastgesteld dat de relevante beveiligings- en beheersmaatregelen niet alleen zijn opgezet en bestaan, maar over een aaneengesloten periode ook daadwerkelijk hebben gewerkt. Dat is een ander en zwaarder zekerheidsniveau dan een certificering van het managementsysteem biedt. Opdrachtgever onderkent dat het verkrijgen van een SOC 2 Type II-rapportage een observatieperiode vergt en dat deze binnen de inschrijvingstermijn niet meer door iedere partij kan worden verworven. Om die reden accepteert Opdrachtgever naast een SOC 2 Type II-rapportage twee gelijkwaardige assurancevormen: een ISAE 3402 Type II-rapportage onder de daar genoemde voorwaarden, en een ISAE 3000 Type II-onderzoek met de Verklaring van Toepasselijkheid (ISO 27001, Annex A) als

Nr.	Onderwerp	Vraag	Antwoord
		dergelijke rapportage beschikt en staat naar onze mening niet in redelijke verhouding tot het doel (voorschrift 3.5 van de Gids Proportionaliteit). De feitelijke inrichting en werking van beheersmaatregelen is immers minstens zo relevant als de vorm waarin deze worden geattesteerd. Bent u bereid de eis zodanig aan te passen dat bij inschrijving ook kan worden volstaan met een geldig ISO 27001-certificaat met Verklaring van Toepasselijkheid, aangevuld met de meest recente auditrapportage van de geaccrediteerde certificerende instelling en rapportages van onafhankelijke penetratietesten, als gelijkwaardig bewijs van de werking van de beveiligings- en beheersingsmaatregelen?	toetsingskader. Zie hiervoor het antwoord op vraag 23. Met die verruiming is de eis naar het oordeel van Opdrachtgever niet beperkt tot partijen die reeds over een SOC 2 Type II-rapportage beschikken. Opdrachtgever ziet daarmee geen aanleiding paragraaf 4.2.4 aan te passen.
25	**Bijlage 5 PvE&W, eis E32 — Jaarlijkse assurance verklaring gedurende de looptijd**	Eis E32 verplicht de Opdrachtnemer om jaarlijks een assuranceverklaring (SOC 2 Type II of ISAE 3000 Type II) over de softwareleverancier te verstrekken gedurende de volledige looptijd van de Overeenkomst. In samenhang met onze vraag over paragraaf 4.2.4 van de Offerteleidraad: bent u bereid ook deze eis zodanig aan te passen dat de blijvende werking van de beveiligings- en beheersingsmaatregelen eveneens kan worden aangetoond met een combinatie van een geldig ISO 27001-certificaat met Verklaring van Toepasselijkheid, de jaarlijkse surveillance- of hercertificeringsauditrapportages van de geaccrediteerde certificerende instelling en de samenvattingen van de jaarlijkse onafhankelijke penetratietesten (eis E35), als gelijkwaardig alternatief voor een SOC 2- of ISAE 3000-rapportage?	Nee. Opdrachtgever handhaaft eis E32 en verwijst voor de motivering naar de antwoorden op de vragen 23 en 24. De daar gegeven overwegingen gelden onverkort voor de jaarlijkse assuranceverklaring gedurende de looptijd: een ISO 27001-certificaat met Verklaring van Toepasselijkheid, surveillance- of hercertificeringsrapportages en samenvattingen van penetratietesten bevatten geen onafhankelijk assurance-oordeel over de effectieve werking van de beheersingsmaatregelen over een aaneengesloten periode en worden daarom niet als gelijkwaardig geaccepteerd. Het doel van eis E32 is om gedurende de volledige looptijd van de Overeenkomst onafhankelijk inzicht te behouden in de opzet, het bestaan én de werking van de relevante beveiligings- en beheersmaatregelen van de softwareleverancier, alsmede in geconstateerde tekortkomingen, de daarvoor vastgestelde verbetermaatregelen en de opvolging daarvan. De in het antwoord op vraag 23 genoemde gelijkwaardige assurancevormen worden ook gedurende de looptijd van de Overeenkomst geaccepteerd.
26	**GIBIT 2025 - Aansprakelijkheid en verzekering (art. 17-18)**	"Is de opdrachtgever bereid de aansprakelijkheidsplafonds in artikel 17.3 en 17.4 te conformeren aan de maximaal verzekerde waarde van de beroeps-/bedrijfsaansprakelijkheidsverzekering van de leverancier, indien deze lager is dan de in die artikelen genoemde bedragen?"	Opdrachtgever handhaaft de aansprakelijkheidsplafonds uit artikel 17.3 en 17.4 GIBIT 2025 ongewijzigd. De vraag veronderstelt dat de verzekerde som van Inschrijver lager kan zijn dan de in die artikelen genoemde bedragen. Die situatie doet zich binnen deze aanbesteding niet voor. Paragraaf 4.2.1 van de Offerteleidraad stelt als geschiktheidseis dat Inschrijver beschikt over een afdoende en geldige verzekering ter dekking van beroeps- en bedrijfsrisico's, met een dekking van ten minste € 2.500.000 per gebeurtenis en ten minste € 5.000.000 per jaar, en dat deze verzekering gedurende de gehele contractperiode met minimaal die verzekerde bedragen wordt voortgezet. Die dekking overstijgt de plafonds van artikel 17.3 en 17.4 GIBIT 2025. Zie voor de proportionaliteit van de verzekeringseis het antwoord op vraag 186.

Nr.	Onderwerp	Vraag	Antwoord
27	**GIBIT 2025 - Maatwerkprogrammatuur (art. 1.31, 21.4-21.6)**	Kan de opdrachtgever bevestigen dat parametrisering, configuratie en inrichting van standaardsoftware zonder aanpassing van de onderliggende broncode niet kwalificeert als "Maatwerkprogrammatuur" in de zin van artikel 1.31, en dus niet onder de overdrachtsverplichting van artikel 21.4 valt?	Ja, Opdrachtgever bevestigt dat parametrisering, configuratie en inrichting van Standaardprogrammatuur, waarbij de onderliggende broncode niet wordt aangepast, niet kwalificeren als Maatwerkprogrammatuur in de zin van artikel 1.31 GIBIT 2025. De overdrachtsverplichting van artikel 21.4 GIBIT 2025 is daarop niet van toepassing. Opdrachtgever gaat er nadrukkelijk van uit dat voor deze Opdracht geen Maatwerkprogrammatuur wordt ontwikkeld. De uitvraag is erop gericht dat de gevraagde functionaliteit binnen de configuratiemogelijkheden van de Standaardprogrammatuur wordt gerealiseerd. Dit sluit aan bij eis E54 en bij de doelstelling in paragraaf 2.1 van de Offerteleidraad om het systeem stabiel te laten functioneren met minimale behoefte aan maatwerk.
28	**GIBIT 2025 - Open source-verplichting (art. 21.5)**	Is de opdrachtgever bereid om, voor zover in het kader van deze opdracht Maatwerkprogrammatuur wordt ontwikkeld die niet functioneert zonder de onderliggende Standaardprogrammatuur van de leverancier, dit vooraf vast te leggen als uitzonderingsgrond op de EUPL-publicatieplicht conform artikel 21.5?	Een afzonderlijke vastlegging vooraf is niet nodig. Artikel 21.5 GIBIT 2025 bevat deze uitzondering reeds: Maatwerkprogrammatuur die niet los van de gecontracteerde Standaardprogrammatuur kan worden gebruikt, wordt niet als Open Source-programmatuur ter beschikking gesteld. Opdrachtgever wijst er daarbij op dat hij ervan uitgaat dat binnen deze Opdracht geen Maatwerkprogrammatuur wordt ontwikkeld. Zie hiervoor het antwoord op vraag 27.
29	**GIBIT 2025 - Opzegtermijn (art. 27.2)**	Wat is de achtergrond van de asymmetrische opzegtermijn (3 maanden voor opdrachtgever, 18 maanden voor leverancier) bij overeenkomsten voor onbepaalde tijd, en is de opdrachtgever bereid hierover in de definitieve overeenkomst nadere afspraken te maken?	De opzegregeling van artikel 27.2 GIBIT 2025 ziet uitsluitend op Overeenkomsten voor onbepaalde tijd. De Overeenkomst die op grond van deze aanbesteding wordt gesloten is een overeenkomst voor bepaalde tijd, met een initiële Gebruiksperiode van zes jaar en verlengingsopties tot maximaal achttien jaar. De in artikel 27.2 genoemde termijnen van drie respectievelijk achttien maanden zijn daarop niet van toepassing. De achtergrond van het onderscheid is de continuïteit van een beveiligingskritieke gemeentelijke voorziening. Bij het wegvallen van het IAM-systeem is een zorgvuldige transitie naar een opvolger noodzakelijk, waarvoor Opdrachtgever aanmerkelijk meer tijd nodig heeft dan Opdrachtnemer. Zie voor de vraag of aan Opdrachtnemer een tussentijds opzegrecht toekomt het antwoord op vraag 95.
30	**GIBIT 2025 - Overmacht (art. 20.2)**	Kan de opdrachtgever toelichten waarom tekortkomingen van derde-toeleveranciers (zoals cloud- of hostingpartners) uitdrukkelijk zijn uitgesloten van het overmachtsbegrip voor de leverancier, en of hierover per overeenkomst nadere afspraken gemaakt kunnen worden gelet op de aard van de dienstverlening (Dienstverlening op Afstand)?	Artikel 20.2 GIBIT 2025 sluit tekortkomingen in de toelevering uit van het overmachtsbegrip omdat de keuze voor en de aansturing van toeleveranciers, waaronder cloud- en hostingpartners, tot de bedrijfsvoering en de risicosfeer van Opdrachtnemer behoren. Opdrachtnemer bepaalt zelf van welke partijen hij afhankelijk wordt en welke continuïteitsafspraken hij met hen maakt. Opdrachtgever heeft daarop geen invloed en kan dat risico niet beheersen. Dit weegt in deze aanbesteding zwaar, omdat de dienstverlening juist als Dienstverlening op Afstand wordt geleverd en het IAM-systeem een kritieke voorziening is voor de toegangsbeveiliging van de gemeentelijke informatievoorziening. Opdrachtgever ziet daarom geen aanleiding hierover nadere of afwijkende afspraken te maken. Een aantoonbare storing van nuts- of telecomvoorzieningen wordt op grond van artikel 20.2 GIBIT 2025 wel als overmacht beschouwd.

Nr.	Onderwerp	Vraag	Antwoord
31	**GIBIT 2025 - Software Bill of Materials (art. 25)**	Op welk detailniveau (bijvoorbeeld conform CycloneDX/SPDX-standaard) verwacht de opdrachtgever de Software Bill of Materials aangeleverd te krijgen, en geldt hiervoor een overgangstermijn na contractsluiting?	In afwijking van artikel 25 GIBIT 2025 verlangt Opdrachtgever binnen deze Opdracht geen Software Bill of Materials.
32	**GIBIT 2025 - Periodieke derdenverklaring (art. 38)**	Is een ISO 27001-certificering voldoende ter voldoening aan de in artikel 38.1 genoemde derdenverklaring, of verwacht de opdrachtgever specifiek een TPM (Third Party Memorandum) van een RE-auditor?	Voor de toepassing van artikel 38.1 GIBIT 2025 als zodanig geldt dat een geldige ISO 27001-certificering, afgegeven door een daartoe geaccrediteerde certificerende instelling, kwalificeert als een van de in dat artikel genoemde vormen. Een afzonderlijke TPM is in dat kader niet vereist. Opdrachtgever wijst er daarbij op dat artikel 38.1 GIBIT 2025 aanvullend van toepassing is en niet afdoet aan de verdergaande specifieke eisen uit deze aanbesteding. Eis E32 verplicht Opdrachtnemer onverkort tot het jaarlijks verstrekken van een assuranceverklaring (SOC 2 Type II of ISAE 3000 Type II) over de softwareleverancier gedurende de looptijd van de Overeenkomst. Deze verplichting kan niet worden vervuld met uitsluitend een ISO 27001-certificering; zie hiervoor de antwoorden op de vragen 23 en 25. Het bepaalde in artikel 38.4 GIBIT 2025 over kritische bevindingen en het verbeterplan geldt onverminderd voor de op grond van eis E32 te verstrekken rapportages.
33	**GIBIT 2025 - Facturatie (art. 11.2)**	Geldt de uitgestelde opeisbaarheid van 30% van de vergoeding tot na integrale Acceptatie ook voor periodieke (jaarlijkse) onderhouds- en licentievergoedingen bij Dienstverlening op Afstand, of uitsluitend voor de eenmalige implementatievergoeding?	De uitgestelde opeisbaarheid geldt uitsluitend voor de eenmalige Implementatievergoeding. Artikel 15.3 van de concept Overeenkomst wijkt in zoverre af van artikel 11.2 GIBIT 2025 en bepaalt dat de Implementatievergoeding opeisbaar is volgens het schema 30% bij ondertekening, 30% bij oplevering van de ingerichte omgeving en 40% na integrale Acceptatie. Voor de Gebruiksrechtenvergoeding geldt artikel 11.2 van de concept Overeenkomst: deze is verschuldigd vanaf de aanvang van de Gebruiksperiode en wordt maandelijks achteraf gefactureerd ter hoogte van een twaalfde van het all-in jaarbedrag uit het Prijzenblad. De Gebruiksperiode vangt aan na Acceptatie, zodat op de periodieke vergoedingen geen uitgestelde opeisbaarheid van toepassing is. Op grond van de rangorde in artikel 2.2 van de concept Overeenkomst prevaleert de Overeenkomst op dit punt boven de GIBIT 2025.
34	**GIBIT 2025 - Algoritmische toepassingen (art. 13-14)**	Kan de opdrachtgever aangeven op basis van welke criteria zij beoordeelt of (onderdelen van) de gevraagde ICT Prestatie kwalificeert als Algoritmische toepassing of AI-systeem in de zin van artikel 1.4/1.5, specifiek voor IAM/IGA-functionaliteit zoals risicogebaseerde autorisatie?	Opdrachtgever beoordeelt of sprake is van een algoritmische toepassing op basis van de definitie die is opgenomen in het Programma van Eisen en Wensen. Daaronder verstaat Opdrachtgever software waardoor op geautomatiseerde wijze voorspellingen worden gedaan, beslissingen worden genomen en/of adviezen worden gegeven op basis van data-analyse, statistiek, generatieve AI en/of zelflerende logica. Voor IAM/IGA-functionaliteit geldt dat ondersteunende functionaliteiten, zoals aanbevelingen, analyses, filters of risicosignaleringen, kunnen kwalificeren als algoritmische toepassing. Daarbij geldt dat dergelijke functionaliteit uitsluitend een ondersteunend en adviserend karakter mag hebben en geen vervanging vormt van de reguliere besluitvorming, goedkeuring of autorisatieverlening door bevoegde functionarissen. Opdrachtgever beoordeelt de kwalificatie uiteindelijk op basis van de concrete werking

Nr.	Onderwerp	Vraag	Antwoord
			van de aangeboden functionaliteit.
35	**GIBIT 2025 - Licentieduur (art. 21.3)**	Kan de opdrachtgever bevestigen dat bij een periodieke (jaarlijkse) vergoedingsstructuur de licentieduur gelijk is aan de looptijd van de overeenkomst, en dat de eeuwigdurende/onherroepelijke licentievariant uit artikel 21.3 uitsluitend van toepassing is bij een eenmalige (koop)vergoeding zonder periodieke component?	Ja, dit is juist begrepen. Artikel 21.3 GIBIT 2025 bepaalt dat indien voor de Licentie periodiek een vergoeding verschuldigd is en/of sprake is van Dienstverlening op Afstand, de duur van de Licentie gelijk is aan de looptijd van de Overeenkomst. Aangezien in deze aanbesteding sprake is van een periodieke Gebruiksrechtenvergoeding en van Dienstverlening op Afstand, is de licentieduur gelijk aan de looptijd van de Overeenkomst. De eeuwigdurende en onherroepelijke licentievariant uit artikel 21.3 is in dat geval niet aan de orde.
36	**Verwerkersovereenkomst - Certificering (Bijlage 2)**	Is een geldige ISO 27001-certificering, voldoende ter voldoening aan het normenstelsel in Bijlage 2, indien de leverancier niet (afzonderlijk) ISO 27017- en/of 27018-gecertificeerd is maar deze onderwerpen wel binnen de scope van de ISO 27001-certificering?	Nee. Voor een cloudleverancier of hostingpartij gelden de in paragraaf 4.2.4 opgenomen eisen onverkort. De vereiste ISO 27017- en ISO 27018-certificeringen kunnen niet worden vervangen door uitsluitend een ISO 27001-certificering, ook niet indien de betreffende onderwerpen binnen de scope van die certificering zijn opgenomen.
37	**Verwerkersovereenkomst - Meldtermijn datalekken (art. 5.1)**	Is de termijn van 24 uur een inspanningsverplichting of een resultaatsverplichting, en geldt deze termijn vanaf het moment van objectieve vaststelling van de inbreuk of vanaf het moment van eerste signaal/vermoeden?	De in de verwerkersovereenkomst opgenomen meldtermijn van 24 uur betreft een resultaatsverplichting. De termijn vangt aan op het moment dat Opdrachtnemer kennis neemt van een vastgestelde inbreuk of van feiten en omstandigheden waaruit redelijkerwijs kan worden afgeleid dat sprake is van een beveiligingsincident of een inbreuk in verband met persoonsgegevens. Opdrachtnemer hoeft niet te wachten totdat de omvang, oorzaak of impact volledig is onderzocht. Indien nog niet alle informatie beschikbaar is, kan een aanvullende melding plaatsvinden zodra meer informatie bekend wordt.
38	**Verwerkersovereenkomst - Bereikbaarheid buiten kantooruren (Bijlage 1)**	Welke reactietijd verwacht de opdrachtgever van de contactpersoon van de verwerker buiten kantooruren, en is hiervoor een aparte (piket-)regeling vereist, of volstaat een generiek meldpunt met de in artikel 5.1 genoemde 24-uurstermijn?	Nee, een afzonderlijke piketregeling is niet voorgeschreven. Opdrachtnemer dient er wel voor zorg te dragen dat meldingen inzake beveiligingsincidenten en datalekken ook buiten kantooruren kunnen worden ontvangen en opgevolgd, zodat aan de in artikel 5.1 gestelde meldtermijn van 24 uur kan worden voldaan. Op welke wijze Opdrachtnemer deze bereikbaarheid organiseert, is aan Opdrachtnemer.
39	**Verwerkersovereenkomst - Auditrecht (art. 4.2)**	Kan de opdrachtgever bevestigen dat het overleggen van een geldige, periodiek getoetste ISO-certificering conform Bijlage 2 een door de opdrachtgever geïnitieerde audit uitsluit, behoudens concrete aanwijzingen dat de certificering niet (langer) toereikend is?	Nee. Het overleggen van een geldige certificering sluit een door Opdrachtgever geïnitieerde audit niet uit. Certificeringen en assuranceverklaringen leveren een belangrijke bijdrage aan de aantoonbaarheid van de getroffen maatregelen, maar laten de rechten van Opdrachtgever uit hoofde van de overeenkomst, waaronder het auditrecht, onverlet. Opdrachtgever zal bij de uitoefening van auditrechten rekening houden met reeds beschikbare certificeringen, assuranceverklaringen en auditrapportages, maar behoudt zich het recht voor aanvullende verificaties uit te voeren indien daartoe aanleiding bestaat.

Nr.	Onderwerp	Vraag	Antwoord
40	**Verwerkersovereenkomst - Kosten medewerking (art. 4.6-4.7)**	Kan de opdrachtgever bevestigen dat ondersteuning bij verzoeken van betrokkenen (art. 4.6) en bij een DPIA/voorafgaande raadpleging (art. 4.7) die de reguliere, in de hoofdovereenkomst voorziene dienstverlening substantieel overstijgt, als meerwerk in rekening gebracht kan worden?	Opdrachtnemer verleent de ondersteuning die op grond van de verwerkersovereenkomst en toepasselijke wet- en regelgeving redelijkerwijs van hem mag worden verwacht. Voor zover verzoeken om ondersteuning bij verzoeken van betrokkenen, een DPIA of een voorafgaande raadpleging de reguliere dienstverlening substantieel overstijgen en aanvullende werkzaamheden vereisen die niet behoren tot de overeengekomen dienstverlening, kunnen deze werkzaamheden in overleg tussen partijen als meerwerk worden uitgevoerd. Of sprake is van meerwerk wordt beoordeeld aan de hand van de aard, omvang en benodigde inzet van de gevraagde werkzaamheden.
41	**Concept Overeenkomst - Looptijd en verlenging (art. 5.6-5.9)**	Is de opdrachtgever bereid om bij de eenzijdige verlengingen als bedoeld in artikel 5.6 een tussentijdse prijsherziening buiten de reguliere indexatie (artikel 11.8 GIBIT 2025) mogelijk te maken, gelet op de maximale looptijd van 18 jaar?	Nee. Opdrachtgever is niet bereid om naast de in de overeenkomst opgenomen indexatiemogelijkheden een aanvullende tussentijdse prijsherziening mogelijk te maken uitsluitend vanwege de looptijd van de overeenkomst. De in de overeenkomst opgenomen prijs- en indexeringsafspraken blijven ongewijzigd van toepassing gedurende de contractduur en eventuele verlengingen.
42	**Concept Overeenkomst - Rangorde GIBIT vs. Offerteleidraad/PvE (art. 2.1-2.2)**	Kan de opdrachtgever bevestigen dat de Offerteleidraad en het Programma van Eisen en Wensen geen bepalingen bevatten die de aansprakelijkheidsbeperkingen (artikel 17 GIBIT 2025), de overmachtsregeling (artikel 20 GIBIT 2025) of de opzeggingsregeling (artikel 27 GIBIT 2025) beperken of uitsluiten?	Ja, dit kan worden bevestigd. De Offerteleidraad en het Programma van Eisen en Wensen bevatten geen bepalingen die de aansprakelijkheidsbeperkingen van artikel 17 GIBIT 2025, de overmachtsregeling van artikel 20 GIBIT 2025 of de opzeggingsregeling van artikel 27 GIBIT 2025 beperken of uitsluiten. Opdrachtgever wijst er wel op dat paragraaf 4.2.1 van de Offerteleidraad een verzekeringseis stelt die uitgaat boven het minimum van artikel 18.2 GIBIT 2025. Dat is een aanvullende geschiktheidseis en geen wijziging van de aansprakelijkheidsplafonds. Voor de volledigheid: op grond van artikel 2.2 van de concept Overeenkomst geldt de rangorde Nota's van Inlichtingen, Overeenkomst, Verwerkersovereenkomst, Offerteleidraad, Programma van Eisen en Wensen, GIBIT 2025. Waar deze documenten van de GIBIT 2025 afwijken, prevaleert het hoger genoemde document.
43	**Concept Overeenkomst - Wijziging leveringsmodel (art. 7.3)**	Op basis van welke uitgangspunten is de verhouding van 80% (On-Premise-prijs t.o.v. SaaS-prijs) vastgesteld, en is deze verhouding gedurende de gehele looptijd van (maximaal) 18 jaar ongewijzigd, of kan deze bij een herziening (artikel 6) worden aangepast?	De verhouding van 80% is langs twee lijnen tot stand gekomen. De keuze voor een vast percentage in plaats van een vrij op te geven On-Premise-prijs dient de vergelijkbaarheid van de inschrijvingen; zie paragraaf 5.2.2 van de Offerteleidraad en het antwoord op vraag 2. De hoogte van het percentage is gebaseerd op de marktconsultatie en op de aanvullende uitvraag die Opdrachtgever naar aanleiding daarvan heeft gedaan onder de deelnemende partijen die zowel een SaaS- als een On-Premise-variant konden leveren. Opdrachtgever acht de verhouding op grond daarvan marktconform, redelijk en proportioneel. Opdrachtgever handhaaft de in de aanbestedingsstukken opgenomen verhouding en beoordelingssystematiek. De verhouding van 80% maakt onderdeel uit van de uitgangspunten van deze aanbesteding en wordt gedurende de looptijd van de Overeenkomst niet aangepast, ook niet in het kader van een herziening op grond van artikel 6. Wel worden de onderliggende SaaS-prijzen, en daarmee de daarvan afgeleide On-Premise-vergoeding, geïndexeerd overeenkomstig de Overeenkomst.

Nr.	Onderwerp	Vraag	Antwoord
			Zie ook de antwoorden op de vragen 1, 2 en 150.
44	**Concept Overeenkomst - Updates/Upgrades (art. 10.2)**	Blijft het weigeringsrecht van opdrachtgever uit artikel 10.16 GIBIT 2025 (met een respijtperiode van 18 maanden) onverkort van toepassing naast de verplichting van leverancier om Updates en Upgrades "zodra beschikbaar" te implementeren?	Ja. Het in artikel 10.16 GIBIT 2025 opgenomen recht van Opdrachtgever om een Update of Upgrade tijdelijk te weigeren blijft van toepassing. Opdrachtgever merkt daarbij op dat het uitgangspunt van de overeenkomst is dat Updates en Upgrades worden toegepast teneinde de Oplossing actueel, veilig en ondersteund te houden. Het weigeringsrecht is bedoeld voor uitzonderingssituaties en niet als standaard werkwijze. Opdrachtgever ziet geen aanleiding de contractuele bepalingen op dit punt te wijzigen.
45	**Concept Overeenkomst - Exit-plan vergoeding (art. 13.1/15.2)**	Geldt de kosteloosheid van het Exit-plan uitsluitend voor het initiële plan, of ook voor de jaarlijkse bijwerking daarvan zoals bedoeld in artikel 29.1 GIBIT 2025?	Artikel 15.2 van de concept Overeenkomst bepaalt dat het Exit-plan onderdeel uitmaakt van de dienstverlening en dat daarvoor geen aanvullende vergoeding verschuldigd is. Dit geldt zowel voor het opstellen van het initiële Exit-plan als voor het jaarlijks bijwerken daarvan als bedoeld in artikel 29.1 GIBIT 2025. De kosteloosheid ziet op het opstellen en actueel houden van het plan, niet op de uitvoering van de exitwerkzaamheden zelf. Zie voor de vergoeding van uitvoerende exit- en transitiewerkzaamheden het antwoord op vraag 181.
46	**Concept Overeenkomst - Dataretournering (art. 14.3)**	Wat verstaat de opdrachtgever onder "per ommegaande" voor de retournering van persoonsgegevens na beëindiging, en omvat deze verplichting uitsluitend de reguliere exportfunctionaliteit van het IAM-systeem of ook eventuele afgeleide/bewerkte gegevens?	Onder "per ommegaande" verstaat Opdrachtgever dat Opdrachtnemer zonder onnodige vertraging uitvoering geeft aan de overeengekomen exit-verplichtingen na beëindiging van de overeenkomst. De omvang van de terug te leveren gegevens wordt beschreven in het Exit-plan en de daarin vastgelegde afspraken. Opdrachtgever gaat ervan uit dat alle voor een zorgvuldige en volledige overdracht noodzakelijke gegevens beschikbaar worden gesteld.
47	**Concept Overeenkomst - Herzieningsclausules (art. 6)**	Kan de opdrachtgever de inhoud van paragraaf 2.9 van de Offerteleidraad (bijlage 4) nader toelichten, specifiek voor welke situaties een herziening van prijs, scope of leveringsmodel mogelijk is gedurende de looptijd?	De herzieningsclausules in paragraaf 2.9 van de Offerteleidraad zijn uitputtend beschreven en zien op vier situaties: 1. Wijziging van de implementatieperiode en de go-live datum, waaronder een latere start, een langere implementatieperiode of het niet halen van de geplande go-live datum. 2. Verlenging van de looptijd met maximaal twaalf maanden indien een nieuwe aanbesteding niet tijdig kan worden afgerond, bijvoorbeeld door een kortgedingprocedure of een rechterlijke uitspraak die tot herbeoordeling of heraanbesteding leidt. 3. Volume: variatie van het aantal af te nemen identiteiten binnen de bandbreedte van 20%, afname van aanvullende modules of koppelingen, en aanpassing van de prijs indien het aantal actieve identiteiten de bovengrens gedurende drie aaneengesloten maanden structureel overschrijdt. 4. Wijziging van het leveringsmodel van SaaS naar On-Premise of omgekeerd, onder de in paragraaf 2.9 en artikel 7 van de concept Overeenkomst opgenomen voorwaarden. Daarnaast is de opschortende voorwaarde met betrekking tot de wachtkamerovereenkomst opgenomen. Buiten deze gevallen vindt geen herziening van prijs, scope of leveringsmodel plaats zonder nieuwe aanbestedingsprocedure.

Nr.	Onderwerp	Vraag	Antwoord
48	**Wachtkamerovereenkomst - Maximale looptijd (art. 3.1)**	Kan de opdrachtgever een absoluut maximum stellen aan de looptijd van de Wachtkamerovereenkomst, gelet op de mogelijke duur van de Implementatieperiode van de hoofdovereenkomst?	Ja, dat maximum is reeds gesteld. Artikel 3.1 van de concept Wachtkamerovereenkomst bepaalt dat deze ingaat op de ingangsdatum van de Overeenkomst met Leverancier I en eindigt één jaar na de datum van Acceptatie van het IAM-systeem. Daarnaast bepalen paragraaf 2.9 en paragraaf 6.3 van de Offerteleidraad dat de wachtkamerovereenkomst kan worden geactiveerd tot uiterlijk één jaar na Acceptatie, dan wel, indien de Acceptatie niet wordt behaald, tot uiterlijk 4 oktober 2028. Daarmee is de looptijd in alle gevallen begrensd. Opdrachtgever ziet geen aanleiding een aanvullend absoluut maximum op te nemen.
49	**Wachtkamerovereenkomst - Prijsinstandhouding tijdens wachtperiode (art. 4.1)**	Is de opdrachtgever bereid om, voor de instandhouding van de prijsgaranties gedurende de looptijd van de Wachtkamerovereenkomst, een indexatiemechanisme toe te passen vergelijkbaar met artikel 11.8 GIBIT 2025?	Nee. Opdrachtgever ziet geen aanleiding hiervoor een afzonderlijk indexatiemechanisme op te nemen. Gedurende de looptijd van de Wachtkamerovereenkomst is er geen dienstverlening en zijn er geen doorlopende vergoedingen die voor indexering in aanmerking komen. Artikel 4.3 van de Wachtkamerovereenkomst bepaalt dat bij activering een nieuwe Overeenkomst wordt gesloten conform het bij de aanbestedingsstukken gevoegde model, inclusief de GIBIT 2025. Vanaf dat moment is de indexeringsregeling van artikel 11.8 GIBIT 2025 onverkort van toepassing. Gelet op de begrensde looptijd van de Wachtkamerovereenkomst acht Opdrachtgever dit proportioneel. Zie ook het antwoord op vraag 48.
50	**Wachtkamerovereenkomst - Mobilisatietermijn (art. 4.2)**	Welke reactie- en mobilisatietermijn hanteert de opdrachtgever in de praktijk bij activering van de Wachtkamerovereenkomst, en is hiervoor een minimumtermijn vast te leggen?	De activering van de Wachtkamerovereenkomst vindt plaats in onderling overleg tussen partijen. De benodigde planning, beschikbaarheid en mobilisatie worden daarbij afgestemd op de concrete omstandigheden van het geval. Opdrachtgever hanteert hiervoor geen vaste reactie- of mobilisatietermijn en ziet geen aanleiding om een minimumtermijn in de overeenkomst vast te leggen.
51	**Wachtkamerovereenkomst - Prijsvaststelling bij activering (art. 4.3)**	Wordt bij het sluiten van de nieuwe overeenkomst met de nummer twee inschrijver het oorspronkelijke Prijzenblad gehanteerd (al dan niet geïndexeerd sinds de oorspronkelijke inschrijfdatum), of vindt een nieuwe prijsonderhandeling plaats gelet op het mogelijk aanzienlijke tijdsverloop?	Het oorspronkelijk door de nummer twee inschrijver ingediende Prijzenblad blijft gehanteerd. Er vindt geen nieuwe prijsonderhandeling plaats. Voor zover de overeenkomst een indexeringsmechanisme bevat, wordt dit toegepast volgens de daarvoor geldende contractuele bepalingen.
52	**Wachtkamerovereenkomst - Gevolg mislukte PoC met nummer twee (art. 5.1)**	Wat gebeurt er indien de in artikel 5.1 bedoelde Proof of Concept met de nummer twee inschrijver niet succesvol wordt afgerond - vervalt de Wachtkamerovereenkomst dan definitief, of wordt de opdracht op een andere wijze (heraanbesteding) belegd?	Indien de Proof of Concept met Leverancier II niet succesvol wordt afgerond, komt de Opdracht ook met deze partij niet tot stand. Artikel 5.1 van de Wachtkamerovereenkomst bepaalt dat Opdrachtgever pas na een succesvol afgeronde PoC tot verstrekking van de Opdracht kan overgaan. De Wachtkamerovereenkomst is dan uitgewerkt. Opdrachtgever bepaalt in dat geval op basis van de dan geldende omstandigheden op welke wijze in de behoefte wordt voorzien, waaronder een nieuwe aanbestedingsprocedure. Opdrachtgever kan hierover op voorhand geen uitspraak doen.

Nr.	Onderwerp	Vraag	Antwoord
53	**Budget**	Begrijpen we het goed dat een totaalbudget tussen 850K en 2000K over een looptijd van 18 jaar neerkomt op dat de Gemeente Zaanstad hiervoor een jaarlijks budget heeft voorzien van 47K tot 111K per jaar?	Nee. De genoemde bandbreedte betreft geen jaarlijks budget en kan niet zonder meer worden omgerekend naar een jaarlijks beschikbaar budget. De bandbreedte is vastgesteld op basis van de resultaten van de marktconsultatie (implementatiekosten + licentiekosten) en de daarop gebaseerde aanbestedingsstrategie. De bandbreedte dient als kader voor de aanbesteding en de beoordeling van inschrijvingen en is niet bedoeld als weergave van een jaarlijks beschikbaar budget.
54	**On-Premise of SaaS**	Het is niet duidelijk of de gemeente Zaanstad een antwoord verwacht voor zowel een on-premise en SaaS variant van de oplossing. Is één van beide voldoende met de garantie dat de andere variant ook mogelijk is?	Nee. Inschrijver dient zowel een SaaS-variant als een On-Premise-variant aan te bieden. Het aanbieden van slechts één leveringsmodel is niet voldoende. Voor de beantwoording van eisen en wensen hoeft Inschrijver niet telkens afzonderlijk beide leveringsmodellen te beschrijven indien de aangeboden functionaliteit en werkwijze voor beide leveringsmodellen gelijk zijn. Indien sprake is van verschillen, beperkingen, aanvullende randvoorwaarden of aandachtspunten tussen de SaaS- en On-Premise-variant, dienen deze expliciet in de Inschrijving te worden vermeld. De gevraagde functionaliteit dient in beginsel beschikbaar te zijn in beide aangeboden leveringsmodellen, tenzij uit de betreffende eis of wens expliciet blijkt dat deze uitsluitend op SaaS of On-Premise van toepassing is. De omstandigheid dat een leverancier bepaalde aanvullende functionaliteit uitsluitend in de SaaS-variant aanbiedt, maakt deze functionaliteit niet automatisch tot een uitzondering op de verplichting om de gevraagde functionaliteit ook in de On-Premise-variant te leveren.
55	**On-Premise variant**	Beschouwt de gemeente Zaansted een antwoord met enkel een on-premise variant als een geldig antwoord? On-premise software kan steeds ingericht worden in een (private) cloud omgeving - gelijkwaardig aan SaaS.	Nee. Inschrijver dient conform de aanbestedingsstukken een oplossing aan te bieden die zowel als SaaS als On-Premise kan worden geleverd. Het uitsluitend aanbieden van een On-Premise-variant wordt niet beschouwd als voldoende, ook niet indien deze oplossing in een private cloudomgeving kan worden ingericht.
56	**Soort functionaliteit**	"Functionaliteit die naar haar aard uitsluitend binnen een SaaS-omgeving beschikbaar is, behoeft niet in de On-Premise-variant beschikbaar te zijn." "Kan de Gemeente Zaanstad aangeven welke soort functionaliteit (met voorbeelden) hier bedoeld wordt?"	Tijdens de marktconsultatie is gebleken dat bepaalde functionaliteit, bijvoorbeeld specifieke AI-ondersteunende functionaliteit, door leveranciers uitsluitend of primair binnen een SaaS-omgeving wordt aangeboden. Dergelijke functionaliteit maakt echter geen onderdeel uit van de door Opdrachtgever geëiste of gewenste functionaliteit en hoeft daarom ook niet in de On-Premise-variant beschikbaar te zijn. Het uitgangspunt blijft dat de aangeboden Oplossing in zowel de SaaS- als de On-Premise-variant voldoet aan de voor het betreffende leveringsmodel geldende eisen en wensen. Alleen wanneer uit de betreffende eis of wens expliciet blijkt dat functionaliteit uitsluitend voor SaaS of On-Premise wordt gevraagd, geldt daarvoor een uitzondering.
57	**Wens 5**	We begrijpen deze wens als volgt. Wanneer voor een toepassing via TopDesk meerdere resources dienen worden toegekend of ontnomen dan moet deze informatie in 1 ticket opgenomen worden. Er moet vermeden worden dat er per toe te kennen of te ontnemen resource een ticket wordt aangemaakt. Is dit een correct begrip van de wens?	Ja, dat is een correcte interpretatie van de wens. Indien voor een applicatie meerdere resources moeten worden toegekend en/of ingetrokken, verwacht Opdrachtgever dat dit in één bundelticket richting Topdesk wordt verwerkt. Het is niet de bedoeling dat per afzonderlijke resource een apart ticket wordt aangemaakt.

Nr.	Onderwerp	Vraag	Antwoord
58	**Verschillende eisen**	Eis 5: Indien een natuurlijk persoon meerdere identiteiten heeft, dan heeft deze ook meerdere AD en TopDesk persoonskaarten. Correct? Eis 6: Kan u de vaakst voorkomende afwijkingen en fouten in het HR systeem omschrijven? Eis 6: Is HR betrokken in het IAM programma en zodoende bewust van de gevolgen van fouten en afwijkingen in de door haar verstrekte data voor de rest van de organisatie? Eis 11: Op welke identiteitsgegevens vereist de gemeente Zaanstad dat dubbele identiteiten worden vastgesteld? Bv. combinatie van voornaam, achternaam en tussenletters of bv. persoonlijk e-mail adres Eis 15: Kan de gemeente Zaanstad de noodzaak van deze eis toelichten? In onze ervaring zijn Medewerkers en Rolhouders nooit strikt gescheiden. Bv. dezelfde IAM-persoonskaart die Rolhouder is, heeft nood aan het aanvragen van een rol als Medewerker. Het gebruik van verschillende portalen in functie van de uit te voeren taak, is voor de eindgebruiker in onze ervaring verwarrend, contraproductief en biedt geen enkele verbetering in veiligheid. De eis dat de beschikbare functionaliteiten (schermen en knoppen) van één enkel centraal platform zich aanpassen aan de context van de gebruiker is de manier van werken van ongeveer elke commerciële IGA oplossing. Eis 28: wat is de grondslag voor het verwerken van geslacht en geboortedatum in de context van een IAM systeem? Eis 28: bevat Active Directory geneste groepen? Zo ja, wat is het maximale niveau van groep nesting? Eis 28: I.v.m. de integratie van het datapakhuis, kan u de term "alle data" nader omschrijven? Bv. logs, configuratiedata, audit logs, broncode, certificaten, etc. zijn ook data maar zijn mogelijks niet van toepassing op deze eis. Merk op dat sommige oplossingen ook configuratiedata in hun databasetabellen bewaren. Eis 29: wat wordt bedoeld met transportnummer? Eis 29: welke metrieken worden in rekening genomen om de peformance van de Oplossing te meten? Eis 34: de vraagstelling lijkt hier niet volledig. Kan u dit aanvullen? Eis 36: Welke periodiciteit wordt voor de uitvoering van dit recht gehanteerd? Bv. maximaal eenmaal per jaar. Zo weten wij ook hoe vaak onze medewerking verwacht wordt. Eis 41: Welke gevoelige data wenst de gemeente Zaanstad te verwerken met de Oplossing? Is dit op wettelijke basis bepaald? Eis 54: Fouten kunnen altijd gebeuren. Erkent de gemeente Zaanstad dat de opdrachtnemer onmogelijk het functioneren van de Oplossing kan garanderen na een foutieve aanpassing door de	Eis 5 (meerdere identiteiten): Ja. Indien een natuurlijk persoon gelijktijdig meerdere identiteiten heeft, resulteert dit in meerdere accounts/personenkaarten binnen de betreffende doelsystemen, waaronder Active Directory en Topdesk. Eis 6 (afwijkingen HR-systeem): De meest voorkomende afwijkingen betreffen situaties waarin een medewerker reeds eerder in dienst is geweest en onbedoeld opnieuw wordt geregistreerd, alsmede situaties waarin personeelsgegevens na verwerking worden gewijzigd of verwijderd. Daarnaast komen situaties voor waarbij een uitdienstmelding wordt verwerkt terwijl een dienstverband alsnog wordt verlengd. Eis 6 (betrokkenheid HR): Ja. HR is betrokken bij het IAM-programma en is zich bewust van de gevolgen die fouten en afwijkingen in de bronregistratie kunnen hebben voor de identiteits- en autorisatieprocessen. Daarnaast werkt Opdrachtgever aan verdere verbetering van de administratie met een administratieprotocol. Eis 11 (dubbele identiteiten): Opdrachtgever verwacht dat potentiële dubbele identiteiten worden gesignaleerd op basis van een combinatie van identificerende persoonsgegevens en denken aan achternaam i.c.m. geboortedatum. De exacte inrichting en matchingregels worden tijdens de implementatie nader vastgesteld. Potentiële dubbelen dienen te worden gesignaleerd en niet automatisch worden verwerkt. Eis 15 (medewerkers versus rolhouders): Opdrachtgever schrijft niet voor dat sprake moet zijn van technisch gescheiden portalen. Eén portaal waarin de beschikbare functionaliteit zich aanpast aan de context en rol van de ingelogde gebruiker voldoet eveneens aan de eis. Daarbij is een leidinggevende tevens medewerker kan zijn beide rollen combineren. Eis 28 (geslacht en geboortedatum): Opdrachtgever registreert momenteel geslacht en geboortedatum in de bronregistratie. Tijdens de implementatie zal kritisch worden beoordeeld welke persoonsgegevens daadwerkelijk noodzakelijk zijn voor de IAM-processen en de inrichting van de Oplossing. Eis 28 (AD nesting): Nee. Opdrachtgever maakt geen gebruik van geneste Active Directory-groepen binnen de vanuit IAM beheerde autorisatiestructuur. Eis 28 ("alle data") Met "alle data" wordt gedoeld op de gegevens die binnen de Oplossing zijn geregistreerd en geconfigureerd en die benodigd zijn voor beheer, rapportage, migratie en continuïteit. Hiermee wordt niet zonder meer bedoeld dat alle technische componenten zoals broncode of certificaten onderdeel van de uitwisseling moeten zijn. Eis 29 (transportnummer): Met transportnummer wordt het recordnummer of ID bedoeld: een unieke sleutel die verwijst naar de logregistratie waarbinnen het betreffende transport of de gegevensuitwisseling heeft plaatsgevonden. Eis 29 (performance): Voor zover met deze vraag wordt gedoeld op performance- en beschikbaarheidsmetingen van de Oplossing, verwijst Opdrachtgever naar het Programma van Eisen en Wensen onder het hoofdstuk Service Level Agreement (SLA), en in het bijzonder naar wens W10. De daarin opgenomen uitgangspunten zijn leidend voor de beoordeling van de prestaties van de Oplossing. Eis 34 (onduidelijke): Klopt, de eis is niet volledig. "Indien de Oplossing als SaaS wordt geleverd" dient aan het begin van eis E34 te worden gelezen. Eis 36 (auditrecht): Opdrachtgever hanteert hiervoor geen vaste periodiciteit. Het

Nr.	Onderwerp	Vraag	Antwoord
		Opdrachtgever van de configuratie of ingerichte functionaliteit van de Oplossing? Eis 54: welke metrieken worden in rekening genomen om vast te stellen dat de Oplossing naar behoren functioneert?	betreft een recht dat incidenteel en indien daartoe aanleiding bestaat kan worden uitgeoefend. Eis 41 (gevoelige data): Opdrachtgever verwijst naar de in de aanbestedingsstukken beschreven gegevensset. Naast persoonsgegevens kunnen ook identiteits-, account-, rol- en autorisatiegegevens als beveiligingsgevoelig worden beschouwd. Eis 54 (fouten opdrachtgever): Opdrachtgever erkent dat fouten in de door Opdrachtgever aangebrachte inrichting, configuratie of autorisaties gevolgen kunnen hebben voor de werking van de inrichting. De eis ziet op het correct functioneren van de aangeboden programmatuur en functionaliteit overeenkomstig de overeengekomen specificaties. Eis 54 (metrieken): Opdrachtgever kan deze vraag niet plaatsen in de context van eis E54. Mogelijk is sprake van een dubbeling met de vraag over eis E29. Op basis van de huidige formulering kan Opdrachtgever niet vaststellen op welke metrieken wordt gedoeld.
59	**Beschikbare rollen bij Gemeente Zaanstad**	"Kan gemeente Zaanstad aangeven welke medewerkers of rollen (PM, functioneel beheer, HR, AD-beheer, proceseigenaren, ..) tijdens de implementatie beschikbaar zullen zijn? Is het ook mogelijk om een indicatie te geven van de verwachte inzet van deze personen tijdens het project? Ik kon nergens terugvinden welke mensen vanuit gemeente Zaanstad actief zullen meewerken aan de implementatie. Dit is nodig voor workshops, validaties, testen, project beslissingen, .. Als bijvoorbeeld functioneel beheer of HR slechts beperkt beschikbaar is, heeft dit directe impact op de planning en doorlooptijd v/h project."	Gemeente Zaanstad zal gedurende de implementatie de voor een succesvolle uitvoering van het project benodigde rollen beschikbaar stellen, waaronder in ieder geval projectmanagement, functioneel beheer, technische beheerders, vertegenwoordiging vanuit P&O en proceseigenaren, voor zover relevant voor de betreffende projectfase. De benodigde capaciteit wordt georganiseerd conform de overeengekomen projectplanning. De rollen waarvan gedurende de implementatie een bijdrage wordt verwacht, vallen onder de directe aansturing van Opdrachtgever. Opdrachtgever voorziet geen knelpunten ten aanzien van de beschikbaarheid van deze rollen voor de uitvoering van het project. Op voorhand kan geen generieke indicatie worden gegeven van de inzet per rol, aangezien deze afhankelijk is van de gekozen oplossing, de implementatieaanpak en de projectfasering. Tijdens de implementatiefase zullen partijen hierover gezamenlijk nadere afspraken maken.
60	**Uitrol van implementatie**	"Kan gemeente Zaanstad verduidelijken hoe ze de implementatie voor zich zien? Worden de verschillende partnerorganisaties, bron- en doelsystemen in één keer meegenomen of wordt hiervoor een gefaseerde aanpak verwacht? Indien gefaseerd, gewenste prioriteit of volgorde? Uit de documenten blijkt dat er meerdere partnerorganisaties en bron- en doelsystemen deel uitmaken van de scope, maar niet hoe gemeente Zaanstad verwacht dat deze worden uitgerold. Dit maakt een groot verschil voor de projectplanning. Indien alles gelijktijdig geïmplementeerd moet worden, zullen er meerdere zaken in parallel moeten worden uitgevoerd. Indien gefaseerd (eerst gemeente Zaanstad, daarna Oostzaan, Wormerland,..), dient de planning anders opgebouwd te worden en kunnen risico's beter worden beheerst."	Opdrachtgever schrijft geen specifieke implementatieaanpak voor. Het is aan Inschrijver om op basis van de in de aanbestedingsstukken beschreven scope een passende implementatieaanpak voor te stellen. Opdrachtgever gaat uit van implementatie van de volledige uitgevraagde scope in de initiële implementatie. Alle in scope zijnde partnerorganisaties, bron- en doelsystemen dienen bij de initiële livegang te zijn aangesloten. Een gefaseerde aansluiting van partnerorganisaties na go-live is niet toegestaan. Voor de duidelijkheid met betrekking tot de identiteiten: voor Gemeente Zaanstad wordt één HR-systeem (YouForce) aangesloten. De identiteiten van de partnerorganisaties worden handmatig in de Oplossing ingevoerd. Indien Inschrijver de werkzaamheden binnen de implementatie gefaseerd wil uitvoeren, kan deze aanpak inclusief onderbouwing in de inschrijving worden beschreven, mits de volledige scope bij de initiële livegang is gerealiseerd.

Nr.	Onderwerp	Vraag	Antwoord
61	**On-premise variant**	"Indien de inschrijver er voor kiest om aan te bieden met een on-premise variant. Mogen we er dan vanuit gaan dat de gemeente Zaanstad of de gemeente gecontracteerde private omgeving onder gemeentelijke regie de nodige computing resources vrij heeft om dit project te dragen of wordt de aanbieder geacht deze zelf te voorzien binnen de project scope?"	Indien Opdrachtgever kiest voor de On-Premise-variant, zorgt Opdrachtgever voor een passende infrastructuuromgeving die voldoet aan de eisen en voorwaarden uit de aanbestedingsstukken en aan de door Opdrachtnemer tijdig opgegeven technische randvoorwaarden die daarbinnen passen. Opdrachtnemer is verantwoordelijk voor het tijdig specificeren van de benodigde infrastructuur-, capaciteits- en technische vereisten. Opdrachtgever organiseert binnen de gekozen On-Premise-inrichting de daarvoor benodigde infrastructuur en capaciteit. De verantwoordelijkheid van Opdrachtgever voor het beschikbaar stellen van de infrastructuuromgeving ontslaat Opdrachtnemer niet van de verantwoordelijkheid om de benodigde technische en capaciteitsvereisten tijdig, volledig en concreet kenbaar te maken. Deze vereisten dienen passend te zijn binnen de uitgangspunten en randvoorwaarden van de in de aanbestedingsstukken beschreven On-Premise-variant.
62	**SOC 2 certificaat**	Volstaat een ISO/IEC 27001-certificering als bewijs van het informatiebeveiligingsmanagementsysteem, of wordt specifiek een SOC 2-certificering verwacht?	Nee. Een geldige ISO/IEC 27001-certificering wordt niet beschouwd als gelijkwaardig aan de in de aanbestedingsstukken gevraagde assuranceverklaring. Een ISO/IEC 27001-certificering toont aan dat een informatiebeveiligingsmanagementsysteem aanwezig is en wordt onderhouden, maar biedt naar het oordeel van Opdrachtgever niet zonder meer een gelijkwaardig zekerheidsniveau ten aanzien van de onafhankelijke beoordeling van de werking van relevante beveiligings- en beheersmaatregelen gedurende een periode. Opdrachtgever verwacht derhalve een SOC2 Type II-, ISAE3000 Type II- en staat open voor een gelijkwaardige assuranceverklaring die een vergelijkbaar zekerheidsniveau biedt. Zie ook antwoord op vraag 23.
63	**Wijze van indienen van de vragen voor de NVI**	Geachte heer/mevrouw, Kunt u aangeven hoe de gemeente Zaanstad de vragen voor de NVI wenst te ontvangen? Ik zie in deze omgeving geen optie om een bijlage toe te voegen. Kan ik daaruit opmaken dat we alle vragen 1 voor 1 in dienen te voeren? Met vriendelijke groet, Mike van Zetten Intragen	Vragen dienen te worden ingediend via de vragenmodule van TenderNed, per vraag afzonderlijk ingevoerd. Het toevoegen van een bijlage met vragen is binnen deze module niet mogelijk. Opdrachtgever verzoekt u per vraag het betreffende document, de paragraaf of het eisnummer te vermelden waarop de vraag betrekking heeft.
64	**Extra bepaling**	Wij dienen ons als organisatie te houden aan de op ons van toepassing zijn (beroeps)regelgeving. Graag nemen wij hiertoe de volgende bepaling op: “1. Opdrachtnemer voert de opdracht uit in overeenstemming met de toepasselijke (beroeps)regelgeving en hetgeen bij of krachtens de wet van hem wordt geëist. Opdrachtgever zal de daaruit voor opdrachtnemer voortvloeiende verplichtingen steeds volledig respecteren. Onder beroepsregelgeving wordt verstaan de relevante gedrags- en beroepsregels van de bij de uitvoering betrokken (bestuurders van) members/vennoten, bestuurders, werknemers en/of ingeschakelde derden, zoals de regels van	Nee. Opdrachtgever gaat niet akkoord met het opnemen van de voorgestelde bepaling. Paragraaf 2.7 van de Offerteleidraad sluit de toepasselijkheid van door Inschrijver gehanteerde algemene voorwaarden en voorwaarden van derden uitdrukkelijk uit. Het opnemen van een aanvullende bepaling met een eigen normenkader verhoudt zich niet tot dat uitgangspunt en tot de gelijke behandeling van inschrijvers. Dat Opdrachtnemer de op hem rustende wettelijke en beroepsregelgeving naleeft, spreekt voor zich en behoeft geen afzonderlijke contractuele vastlegging. Opdrachtgever ziet geen aanleiding de aanbestedingsstukken op dit punt aan te passen.

Nr.	Onderwerp	Vraag	Antwoord
		bijvoorbeeld NBA, NOREA, NOB en FB. 2. Opdrachtnemer houdt in dit verband een werkdossier aan met daarin kopieën van relevante stukken, welk dossier eigendom is van Opdrachtnemer.”	
65	**Bijlage 9. Concept Verwerkersovereenkomst artikel 4.2**	Bijlage 9. Concept Verwerkersovereenkomst artikel 4.2 omvat een uitgebreidere auditbepaling dan waar wij mee akkoord kunnen gaan. Kunt u daarom akkoord gaan met de vervanging van Bijlage 9. Concept Verwerkersovereenkomst artikel 4.2 door de volgende bepalingen? 1. Opdrachtnemer stelt Opdrachtgever in de gelegenheid de naleving van deze Overeenkomst periodiek te controleren. De controle kan namens Opdrachtgever worden uitgevoerd door een (externe) onafhankelijke professionale auditor voor zover deze auditor geen directe concurrent van Opdrachtnemer is. Deze periodieke controle is beperkt tot het (maximaal één (1) keer per jaar) beantwoorden door Opdrachtnemer van door Opdrachtgever schriftelijk gestelde vragen over de naleving van Opdrachtnemer van relevante Wet- en regelgeving met betrekking tot de dienstverlening onder deze Overeenkomst. 2. Gelet op de op Opdrachtnemer rustende geheimhoudingsverplichtingen ten opzichte van andere cliënten, erkent en accepteert Opdrachtgever dat Opdrachtnemer aan Opdrachtgever en de onafhankelijke auditor die door Opdrachtgever wordt aangewezen, geen toegang zal geven tot haar IT-systemen en/of haar IT-infrastructuur.	Nee, Opdrachtgever gaat niet akkoord met de voorgestelde vervanging van artikel 4.2. Opdrachtgever erkent dat bij de uitvoering van audits rekening moet worden gehouden met vertrouwelijkheid, beveiliging van andere klanten en de aard van de dienstverlening. Het auditrecht mag echter niet worden beperkt tot uitsluitend het beantwoorden van schriftelijke vragen en kan niet op voorhand iedere vorm van verificatie uitsluiten. Opdrachtgever verwacht dat passende controlemaatregelen mogelijk blijven, waarbij rekening wordt gehouden met proportionaliteit, vertrouwelijkheid, beschikbare assurance-rapportages en andere relevante auditinformatie.
66	**GIBIT 2025 artikel 18 en Offerteleidraad artikel 4.2.1**	In GIBIT 2025 artikel 18 en Offerteleidraad artikel 4.2.1 is bepaald dat toestemming van de Opdrachtgever nodig is om de verzekerde bedragen en polisvoorwaarden die opdrachtnemer met zijn verzekeraar is overeengekomen, (ten nadele van de opdrachtgever) te wijzigen. Het is voor ons ondoenlijk om onze klanten ieder jaar om toestemming te vragen, indien de verzekeringsvoorwaarden licht (en mogelijk ook licht ten nadele van de klant) wijzigen. Wij zijn doorlopend verzekerd, maar de precieze verzekeringsvoorwaarden worden jaarlijks opnieuw afgestemd met onze verzekeraar. De voorwaarden en dekking wijzigen daarbij niet substantieel, maar bepaalde condities kunnen wel licht wijzigen. Deze gewijzigde voorwaarden kunnen wij niet steeds vooraf met al onze klanten afstemmen. Gelet hierop willen wij verzoeken GIBIT 2025 artikel 18 en Offerteleidraad artikel 4.2.1 niet van toepassing te verklaren.	Nee. Opdrachtgever verklaart artikel 18 GIBIT 2025 en paragraaf 4.2.1 van de Offerteleidraad niet buiten toepassing. Opdrachtgever verduidelijkt de strekking wel als volgt. De eis is dat Opdrachtnemer gedurende de gehele contractperiode verzekerd blijft met ten minste de genoemde verzekerde bedragen. Een reguliere jaarlijkse prolongatie waarbij de dekking en de verzekerde bedragen materieel gelijk blijven, behoeft geen voorafgaande toestemming van Opdrachtgever. Voorafgaande instemming is uitsluitend aan de orde bij een wijziging die de dekking materieel ten nadele van Opdrachtgever beperkt, bijvoorbeeld doordat de verzekerde bedragen onder het gestelde minimum komen of doordat de voor deze Opdracht relevante risico's van dekking worden uitgesloten. Opdrachtnemer informeert Opdrachtgever in dat geval onverwijld.

Nr.	Onderwerp	Vraag	Antwoord
67	**GIBIT 2025 artikel 21**	Dit artikel is vanwege de beroepsregelgeving niet uitvoerbaar. Op grond van onze beroepsregels mogen wij de IE-rechten niet aan onze cliënten overdragen. Dit zou immers tot gevolg (kunnen) hebben dat onze cliënten de door ons afgegeven verklaringen en / of rapporten zouden mogen aanpassen. Derhalve stellen wij voor om de tekst van dit artikel te vervangen door de volgende tekst: 1. Opdrachtnemer behoudt zich alle rechten voor met betrekking tot producten van de geest welke hij gebruikt of heeft gebruikt of ontwikkelt of heeft ontwikkeld in het kader van de uitvoering van de opdracht, voor zover deze niet reeds aan derden toekomen. 2. Het is de Opdrachtgever uitdrukkelijk verboden die producten, waaronder mede begrepen adviezen, rapporten, computerprogramma's, systeemontwerpen, werkwijzen, (model)contracten en andere geestesproducten van opdrachtnemer, een en ander in de ruimste zin des woords, al dan niet met inschakeling van derden, te verveelvoudigen, te openbaren of te exploiteren. 3. Het is de Opdrachtgever niet toegestaan die producten aan derden ter hand te stellen, anders dan ter inwinning van een deskundig oordeel omtrent de werkzaamheden van opdrachtnemer. Kunt u hiermee akkoord gaan?	Nee. Opdrachtgever gaat niet akkoord met de voorgestelde vervanging van artikel 21 GIBIT 2025. Opdrachtgever wijst erop dat het bezwaar naar zijn oordeel feitelijke grondslag mist. Artikel 21.1 GIBIT 2025 bepaalt dat de intellectuele eigendomsrechten op de ter beschikking gestelde ICT Prestatie bij Leverancier of diens licentiegevers berusten. Overdracht is uitsluitend aan de orde bij Maatwerkprogrammatuur (artikel 21.4). Opdrachtgever gaat ervan uit dat binnen deze Opdracht geen Maatwerkprogrammatuur wordt ontwikkeld; zie hiervoor het antwoord op vraag 27. De voorgestelde tekst gaat aanmerkelijk verder dan het geschetste bezwaar en zou onder meer de rechten van Opdrachtgever op zijn eigen Data (artikel 21.2 GIBIT 2025) en het overeengekomen gebruik raken. Opdrachtgever ziet geen aanleiding de aanbestedingsstukken op dit punt aan te passen.
68	**GIBIT 2025 artikel 31, Bijlage 6. Concept Overeenkomst artikel 14 en Bijlage 9. Concept Verwerkersovereenkomst**	De onderlinge afspraken met betrekking tot het verwerken van persoonsgegevens (o.a. een eventuele verwerkersovereenkomst) wordt bij de overeenkomst nader geregeld. Als zakelijk dienstverlener zullen wij doorgaans optreden als verwerkingsverantwoordelijke vanwege onze onafhankelijke, objectieve en deskundige positie. Daarnaast is het mogelijk dat Opdrachtnemer, maar ook andere (buitenlandse) lidfirma's - die behoren tot hetzelfde mondiale netwerk als waartoe Opdrachtnemer behoort - en externe dienstverleners zoals bedoeld onder het kopje geheimhouding, in het kader van de werkzaamheden voor Opdrachtgever in aanraking kunnen komen met informatie over de Opdrachtgever, waaronder persoonsgegevens. Uiteraard vindt het delen van de betreffende informatie enkel plaats als dit noodzakelijk is voor het doel van de dienstverlening, een en ander volgens de toepasselijke wetgeving. Om deze reden stellen we voor om de volgende bepaling op te nemen als GIBIT 2025 artikel 31, Bijlage 6. Concept Overeenkomst artikel 14 en Bijlage 9. Concept Verwerkersovereenkomst. "Informatie over Opdrachtgever, waaronder persoonsgegevens, kan worden verwerkt door Opdrachtnemer, andere lidfirma's die	Nee. Opdrachtgever gaat niet akkoord met de voorgestelde vervanging van GIBIT 2025 artikel 31, artikel 14 van de Concept Overeenkomst en de Concept Verwerkersovereenkomst. De verwerking van persoonsgegevens in het kader van deze opdracht wordt beheerst door de in de aanbestedingsstukken opgenomen overeenkomst en verwerkersovereenkomst. Opdrachtgever acht het niet wenselijk om generiek vooraf toestemming te verlenen voor verwerking van informatie en persoonsgegevens door andere lidfirma's, netwerkorganisaties of externe dienstverleners buiten de in de overeenkomst opgenomen afspraken. Indien Inschrijver van mening is dat voor de uitvoering van de opdracht specifieke derden of groepsmaatschappijen moeten worden betrokken bij de verwerking van persoonsgegevens, dient dit inzichtelijk en toetsbaar te worden gemaakt binnen de daarvoor in de aanbestedingsstukken opgenomen kaders. Opdrachtgever ziet geen aanleiding de aanbestedingsstukken op dit punt aan te passen.

Nr.	Onderwerp	Vraag	Antwoord
		behoren tot hetzelfde mondiale netwerk als waartoe Opdrachtnemer behoort en externe dienstverleners in de verschillende landen waarin zij actief zijn. De verwerking van informatie die Opdrachtnemer van de Opdrachtgever heeft ontvangen vindt plaats in overeenstemming met de toepasselijke wet- en beroepsregelgeving. De doorgifte van persoonsgegevens binnen het netwerk van lidfirma's waartoe Opdrachtnemer behoort, is onderworpen aan de Binding Corporate Rules-policies van Opdrachtnemer. Opdrachtgever garandeert dat die bevoegd is om in verband met de uitvoering van de diensten Persoonsgegevens aan Opdrachtnemer te verschaffen, en dat enige aan Opdrachtnemer verstrekte Persoonsgegevens in overeenstemming met de toepasselijke wetgeving zijn verwerkt."	
69	**GIBIT 2025 artikel 19 en Bijlage 9. Concept Verwerkersovereenkomst**	'Opdrachtnemer bestaat uit een netwerk van gelieerde lidfirma's die ieder op zichzelf staande juridische entiteiten zijn en tot hetzelfde mondiale netwerk behoren. Gezien de wijze waarop Opdrachtnemer is georganiseerd is het voor Opdrachtnemer van belang dat Opdrachtnemer informatie met andere lidfirma's kan delen. Om deze reden stelt Opdrachtnemer voor om aan GIBIT 2025 artikel 19 en Bijlage 9. Concept Verwerkersovereenkomst het volgende toe te voegen: "Het is Opdrachtnemer toegestaan vertrouwelijke informatie te delen met Opdrachtnemer's lidfirma's indien dat noodzakelijk is in het kader van het verrichten van de werkzaamheden. Opdrachtnemer staat ervoor in dat deze lidfirma's de geheimhoudingsverplichtingen na leven''	Nee. Opdrachtgever gaat niet akkoord met de voorgestelde aanvulling op GIBIT 2025 artikel 19 en de Concept Verwerkersovereenkomst. Opdrachtgever acht het van belang dat de verwerking en het delen van vertrouwelijke informatie en persoonsgegevens uitsluitend plaatsvindt binnen de in de overeenkomst en verwerkersovereenkomst opgenomen kaders. Het generiek toestaan van gegevensdeling met andere lidfirma's binnen een mondiaal netwerk past niet binnen deze uitgangspunten. Indien voor de uitvoering van de opdracht specifieke groepsmaatschappijen, lidfirma's of andere derden moeten worden betrokken, dient dit inzichtelijk en toetsbaar te worden gemaakt binnen de daarvoor in de aanbestedingsstukken opgenomen afspraken. Opdrachtgever ziet geen aanleiding de aanbestedingsstukken op dit punt aan te passen.
70	**GIBIT 2025 artikel 17 en Bijlage 9. Concept Verwerkersovereenkomst artikel 6**	In dit artikel is opgenomen dat opdrachtnemer de opdrachtgever dient te vrijwaren voor schade als gevolg van aanspraken van derden. Dit houdt in dat de aansprakelijkheid van opdrachtnemer verder strekt dan de aansprakelijkheid die wij als opdrachtnemer bereid zijn te aanvaarden. Wij aanvaarden alleen aansprakelijkheid jegens onze opdrachtgever, omdat wij daar immers de werkzaamheden voor verrichten. Het is aan de opdrachtgever om de risico's in te schatten en de eigen aansprakelijkheid jegens haar wederpartijen te beperken. Kunt u derhalve instemmen met het buiten toepassing verklaren van GIBIT 2025 artikel 17 en Bijlage 9. Concept Verwerkersovereenkomst artikel 6? Mocht u dit verzoek niet honoreren, kunt u dan bevestigen dat de aansprakelijkheid die voortvloeit uit de vrijwaring (1) onder de overeengekomen aansprakelijkheidsbeperking (zoals door ons	Nee. Opdrachtgever is niet bereid GIBIT 2025 artikel 17 en artikel 6 van de Concept Verwerkersovereenkomst buiten toepassing te verklaren. Opdrachtgever acht het redelijk dat Opdrachtnemer aansprakelijk blijft voor aanspraken van derden voor zover deze voortvloeien uit een aan Opdrachtnemer toerekenbare tekortkoming, onrechtmatige daad of schending van de op Opdrachtnemer rustende verplichtingen. Opdrachtgever ziet geen aanleiding de aanbestedingsstukken op dit punt aan te passen.

Nr.	Onderwerp	Vraag	Antwoord
		verzocht) valt en dat (2) de vrijwaring uitsluitend ziet op de aanspraken van derden die het gevolg zijn van een toerekenbare tekortkoming van opdrachtnemer?"	
71	**GIBIT 2025 artikel 17 en Bijlage 9. Concept Verwerkersovereenkomst artikel 6**	Opdrachtnemer bestaat uit een netwerk van gelieerde lidfirma's die ieder op zichzelf staande juridische entiteiten zijn en tot hetzelfde mondiale netwerk behoren. Opdrachtnemer gaat zelfstandig overeenkomsten aan. Op grond van de wet is de Opdrachtnemer aansprakelijk voor de door haar ingeschakelde hulppersonen (inclusief onderaannemers). In het belang van Opdrachtnemer, maar ook in dat van de Opdrachtgever gelet op eventuele niet-ontvankelijkheid en ter bescherming van Opdrachtnemer's hulppersonen, verzoeken wij om aan GIBIT 2025 artikel 17 en Bijlage 9. Concept Verwerkersovereenkomst artikel 6 het volgende toe te voegen: "Opdrachtgever zal eventuele klachten, vorderings- en verhaalsrechten uitsluitend kenbaar maken en/of uitoefenen jegens Opdrachtnemer, namelijk de contractspartij bij de Overeenkomst."	Opdrachtgever begrijpt de strekking van het verzoek. De contractspartij blijft verantwoordelijk voor de uitvoering van de overeenkomst en voor de door haar ingeschakelde hulppersonen. Opdrachtgever ziet echter geen aanleiding de aanbestedingsstukken op dit punt aan te passen.
72	**GIBIT 2025 artikel 17 en Bijlage 9. Concept Verwerkersovereenkomst artikel 6**	Graag verzoeken wij u onderstaande bepaling toe te voegen aan GIBIT 2025 artikel 17 en Bijlage 9. Concept Verwerkersovereenkomst artikel 6. Gaat u hiermee akkoord? "Opdrachtgever vrijwaart Opdrachtnemer voor vorderingen van derden wegens schade die veroorzaakt is doordat Opdrachtgever of niet door opdrachtnemer ingeschakelde derden aan opdrachtnemer onjuiste of onvolledige bescheiden of informatie heeft c.q. hebben verstrekt, tenzij Opdrachtgever kan aantonen dat de schade geen verband houdt met verwijtbaar handelen of nalaten zijnerzijds dan wel veroorzaakt is door opzet of grove schuld van Opdrachtnemer."	Nee. Opdrachtgever gaat niet akkoord met de voorgestelde aanvulling op GIBIT 2025 artikel 17 en artikel 6 van de Concept Verwerkersovereenkomst. Opdrachtgever acht het niet wenselijk een aanvullende vrijwaringsverplichting ten gunste van Opdrachtnemer op te nemen. De aansprakelijkheid en risicoverdeling worden beheerst door de in de aanbestedingsstukken opgenomen contractuele bepalingen. Daarbij geldt dat zowel Opdrachtgever als Opdrachtnemer verantwoordelijk zijn voor de correcte uitvoering van hun eigen verplichtingen. Opdrachtgever ziet geen aanleiding de aanbestedingsstukken op dit punt aan te passen.
73	**GIBIT 2025 artikel 17 en Bijlage 9. Concept Verwerkersovereenkomst artikel 6**	Wij waarderen het dat u bereid bent om de aansprakelijkheid te beperken. De gehanteerde staffel bevat een hogere aansprakelijkheid dan die wij gewend zijn overeen te komen met onze Opdrachtgevers. Gelet op voorgaande verzoeken wij u de tekst van GIBIT 2025 artikel 17 en Bijlage 9. Concept Verwerkersovereenkomst artikel 6 te vervangen door onderstaand tekstvoorstel. Kunt u hiermee akkoord gaan? 1. Indien opdrachtgever aantoont dat hij schade heeft geleden door fouten van opdrachtnemer die hem kunnen worden toegerekend, is elke aansprakelijkheid van opdrachtnemer voor schade, hetzij op grond van wanprestatie dan wel onrechtmatige daad, hetzij op grond van de wet of anderszins, beperkt tot maximaal driemaal het aan opdrachtgever gefactureerde bedrag	Nee. Opdrachtgever gaat niet akkoord met de voorgestelde aanvulling op GIBIT 2025 artikel 17 en artikel 6 van de Concept Verwerkersovereenkomst. Opdrachtgever acht het niet wenselijk een aanvullende vrijwaringsverplichting ten gunste van Opdrachtnemer op te nemen. De aansprakelijkheid en risicoverdeling worden beheerst door de in de aanbestedingsstukken opgenomen contractuele bepalingen. Daarbij geldt dat zowel Opdrachtgever als Opdrachtnemer verantwoordelijk zijn voor de correcte uitvoering van hun eigen verplichtingen. Opdrachtgever ziet geen aanleiding de aanbestedingsstukken op dit punt aan te passen.

Nr.	Onderwerp	Vraag	Antwoord
		van het honorarium voor de desbetreffende opdracht. Bij een opdracht met een doorlooptijd van meer dan twaalf maanden, is de hier bedoelde aansprakelijkheid beperkt tot maximaal driemaal het honorarium dat in het kader van de desbetreffende opdracht in de laatste twaalf maanden voorafgaande aan de fouten aan opdrachtgever is gefactureerd. De voorgaande beperking is niet van toepassing op schade die is veroorzaakt doordat er aan de zijde van opdrachtnemer sprake is van opzet of grove schuld of een dergelijke beperking bij wet of regelgeving verboden is.	
74	**GIBIT 2025 (ontbindingsartikelen); Offerteleidraad §2.9 en §6.4. Redelijke hersteltermijn bij tekortkoming.**	Kan Zaanstad bevestigen dat ontbinding van de overeenkomst wegens een tekortkoming pas mogelijk is nadat de Opdrachtnemer schriftelijk in gebreke is gesteld en een redelijke hersteltermijn is gegund (conform art. 6:265 BW)? Kan Zaanstad voor een eventuele Proof of Concept (PoC) bevestigen dat de voorwaarden en garanties hiervoor in onderling overleg worden afgestemd op basis van de standaard evaluatievoorwaarden?	Er is geen sprake van een eventuele PoC. Opdrachtgever zal een PoC uitvoeren zoals beschreven in de aanbestedingsstukken. De invulling, reikwijdte en beoordeling van de PoC vinden plaats overeenkomstig de aanbestedingsstukken. Opdrachtgever ziet geen aanleiding om vooraf overeenstemming te bereiken over door Inschrijver gehanteerde standaard evaluatievoorwaarden.
75	**GIBIT 2025 (personeelsbepalingen); Offerteleidraad §2.8 (initieel 6 jaar, max. 18 jaar). Vervanging van bij de uitvoering betrokken personen.**	Aangezien de dienstverlening primair het ter beschikking stellen van gestandaardiseerde SaaS-software betreft en geen detachering van specifiek individueel personeel, kan Zaanstad bevestigen dat de strikte toestemmingsprocedure voor personeelsvervanging niet van toepassing is op de SaaS-dienstverlening? (software provider verplicht zich uiteraard om bij relevante contactpersonen te zorgen voor gekwalificeerd personeel en de klant hierover tijdig te informeren).	De GIBIT 2025 bevat geen algemene toestemmingsprocedure voor personeelsvervanging bij generieke Dienstverlening op Afstand. Voor zover uw vraag ziet op de vervanging van medewerkers van de softwareleverancier die de generieke SaaS-dienst leveren, bevestigt Opdrachtgever dat daarvoor geen voorafgaande toestemming is vereist. Voor de personen die Opdrachtnemer bij de uitvoering van deze Opdracht inzet en die in de Inschrijving of het Plan van Aanpak met naam of rol zijn aangeboden, waaronder de projectleider en de technisch consultant, geldt wel dat vervanging vooraf met Opdrachtgever wordt afgestemd. Opdrachtgever verleent daaraan zijn medewerking, mits de vervanger over ten minste gelijkwaardige kwalificaties en ervaring beschikt.
76	**GIBIT 2025 (geheimhoudingsartikel); bijlage 9 verwerkersovereenkomst. Delen vertrouwelijke informatie binnen netwerk van gelieerde ondernemingen.**	Om de dienstverlening en ondersteuning effectief uit te voeren, kan het noodzakelijk zijn vertrouwelijke informatie te delen binnen ons netwerk van gelieerde entiteiten (gebaseerd op de standaard affiliate-definities zoals opgenomen in onze SSA). Kan Zaanstad bevestigen dat het de Opdrachtnemer is toegestaan vertrouwelijke informatie te delen met gelieerde entiteiten, mits deze gebonden zijn aan dezelfde geheimhoudingsverplichtingen?	Zie hiervoor het antwoord op vraag 69.
77	**GIBIT 2025 (IE-artikelen); Offerteleidraad §2.7. Intellectueel eigendom van standaardprogrammat**	Staat Zaanstad ervoor open om bij standaard SaaS-oplossingen die uitsluitend licenties op propriëtaire cloud-software via een abonnementsmodel betreffen (zonder softwareontwikkeling of op maat gemaakte intellectuele eigendom), de bepalingen omtrent overdracht van Intellectueel Eigendom (IE) niet van toepassing te verklaren en hiervoor uitsluitend een licentie/gebruiksrecht voor	Opdrachtgever bevestigt dat voor Standaardprogrammatuur die uitsluitend in licentie wordt verstrekt, geen overdracht van intellectuele eigendomsrechten plaatsvindt. Artikel 21.1 GIBIT 2025 bepaalt dat die rechten bij Leverancier of diens licentiegevers berusten; artikel 21.3 GIBIT 2025 voorziet in een gebruiksrecht voor de duur van de Overeenkomst. Zie ook het antwoord op vraag 35.

Nr.	Onderwerp	Vraag	Antwoord
	uur.	de duur van de overeenkomst te verlenen?	Het buiten toepassing verklaren van artikel 21 GIBIT 2025 is niet nodig en niet wenselijk. Dat artikel regelt daarnaast onder meer de rechten op Data van Opdrachtgever (artikel 21.2) en de vrijwaring tegen aanspraken van derden wegens inbreuk op intellectuele eigendomsrechten (artikel 21.7). Die bepalingen blijven onverkort van toepassing. De bepalingen over Maatwerkprogrammatuur worden alleen relevant indien Maatwerkprogrammatuur wordt ontwikkeld. Zie hiervoor het antwoord op vraag 27.
78	**GIBIT 2025 (bijlage 7); Offerteleidraad §2.2 (SaaS én On-Premise). Escrow bij SaaS.**	Gezien het feit dat de aangeboden oplossing een pure SaaS/cloud-dienst betreft (en geen on-premise software), kan Zaanstad bevestigen dat een klassieke broncode-escrow niet van toepassing is? Tevens vragen wij of een Cloud Escrow-regeling optioneel kan worden aangeboden (onder voorbehoud van meerkosten en wederzijdse overeenstemming over de escrow-provider) in plaats van dat dit een verplichte minimumeis is?	Ja, dit kan worden bevestigd. Opdrachtgever verlangt in deze aanbesteding geen broncode-escrow. Een escrowregeling is geen eis en ook geen wens. Opdrachtgever hecht wel aan continuïteit en heeft dit langs twee lijnen geborgd: een Exit-plan (artikel 13 van de concept Overeenkomst, eis E55 en wens W13) en de continuïteitsbepaling van artikel 39 GIBIT 2025. Zie voor de reikwijdte daarvan het antwoord op vraag 99. Een aanvullende Cloud Escrow-regeling behoeft niet te worden aangeboden en maakt geen onderdeel uit van de beoordeling.
79	**GIBIT 2025 (bijlage 7); bijlage 6 concept Overeenkomst. Proportionaliteit boetebepalingen.**	Aangezien de GIBIT 2025 reeds voorziet in een passend aansprakelijkheidsregime, vragen wij of Zaanstad bereid is de boetebepalingen te schrappen? Is Zaanstad als alternatief bereid om risico’s af te dekken via gedifferentieerde/verhoogde aansprakelijkheidslimieten (zoals een specifieke verhoogde aansprakelijkheidslimiet voor databescherming in plaats van boetebepalingen), en te bevestigen dat boetes/schadeclaims niet gelden bij overmacht of niet-toerekenbare vertragingen?	Nee. Opdrachtgever is niet bereid de boetebepalingen te schrappen of te vervangen door verhoogde aansprakelijkheidslimieten. Boetebepalingen en aansprakelijkheid dienen een verschillend doel. Een boete werkt prikkelend en maakt handhaving mogelijk zonder dat Opdrachtgever schade hoeft aan te tonen; het aansprakelijkheidsregime ziet op vergoeding van daadwerkelijk geleden schade. Bij een beveiligingskritieke voorziening acht Opdrachtgever beide instrumenten passend. Opdrachtgever bevestigt wel dat een boete of schadevergoeding niet verschuldigd is voor zover sprake is van overmacht in de zin van artikel 20 GIBIT 2025 of van een niet aan Opdrachtnemer toerekenbare vertraging. Zie ook het antwoord op vraag 9.
80	**Offerteleidraad §4.2.1 en §2.6 (raming € 850K – € 2M); bijlage 6 concept Overeenkomst; GIBIT 2025. Verlaging aansprakelijkheidsplafonds.**	"Zaanstad eist een verzekering met dekking van ten minste € 2,5 miljoen per gebeurtenis en € 5 miljoen per jaar. Gelet op de geraamde totale opdrachtwaarde, dit betekent dat dit aanzienlijk hoger ligt dan de gemiddelde jaarlijkse opdrachtwaarde. Wij hanteren als standaard een cumulatieve aansprakelijkheid van driemaal (3x) de over de opdracht gefactureerde vergoeding. Is Zaanstad bereid de aansprakelijkheid onder de Overeenkomst te beperken tot 3x de over de opdracht gefactureerde vergoeding, met een proportioneel absoluut maximum (bijvoorbeeld € 1.250.000 per gebeurtenis en € 2.500.000 per jaar)? Kan Zaanstad tevens bevestigen dat deze beperking ook geldt voor vrijwaringen richting derden, dat deze vrijwaringen uitsluitend zien op aanspraken uit toerekenbare tekortkomingen van Opdrachtnemer, en dat indirecte schade (waaronder gederfde winst, gemiste besparingen, verlies van gegevens, bedrijfsstagnatie) van aansprakelijkheid is uitgezonderd behoudens opzet of bewuste roekeloosheid?"	Nee. Opdrachtgever is niet bereid de aansprakelijkheid te beperken tot driemaal de gefactureerde vergoeding met een absoluut maximum van € 1.250.000 respectievelijk € 2.500.000. De GIBIT 2025 bevat in artikel 17.3 en 17.4 een landelijk gehanteerd en tussen gemeenten en marktpartijen afgewogen aansprakelijkheidsregime. Opdrachtgever handhaaft dit ongewijzigd. Het IAM-systeem reguleert de toegang tot alle gemeentelijke systemen en gegevens; de potentiële schade bij een ernstig falen van deze voorziening houdt geen directe relatie met de contractwaarde. Op uw aanvullende vragen: • De aansprakelijkheidsbeperkingen zijn ook van toepassing op vrijwaringen jegens derden, behoudens de in artikel 17.5 GIBIT 2025 genoemde uitzonderingen. • De vrijwaring ziet op aanspraken van derden voor zover deze voortvloeien uit een aan Opdrachtnemer toerekenbare tekortkoming, onrechtmatige daad of schending van zijn verplichtingen. • Opdrachtgever sluit indirecte schade niet categorisch uit. Artikel 17.4 GIBIT 2025 begrenst de aansprakelijkheid voor overige schade reeds tot tweemaal de

Nr.	Onderwerp	Vraag	Antwoord
			Jaarvergoeding per gebeurtenis en maximaal viermaal de Jaarvergoeding per kalenderjaar. Een aanvullende uitsluiting acht Opdrachtgever niet nodig. Zie voor de proportionaliteit van de verzekeringseis het antwoord op vraag 186.
81	**Offerteleidraad §5.2.1 en §2.7 / §2.8 (max. 18 jaar); bijlage 6 concept Overeenkomst; GIBIT 2025. Prijsindexering gedurende de contractlooptijd.**	Gezien een maximale contractduur van 18 jaar is een adequate indexeringsclausule essentieel voor het uitbrengen van een marktconforme prijs. Kan Zaanstad expliciet bevestigen op basis van welk indexcijfer prijzen (inschrijfsom, jaarlijkse licentie- en beheerkosten, uurtarieven) worden geïndexeerd? Wij denken hierbij aan de CBS Dienstenprijsindex (DPI) categorie J6202 of vergelijkbaar.	De indexering is geregeld in artikel 11.8 GIBIT 2025 en geldt onverkort voor deze Overeenkomst. Dit betekent concreet: • Index: het door het CBS gepubliceerde definitieve prijsindexcijfer dienstenprijzen commerciële dienstverlening en transport (2021 = 100), groep J6202. Vervalt die groep, dan geldt groep J62; vervalt de reeks, dan de opvolger daarvan. • Indexatiemoment en frequentie: jaarlijks per 1 januari. • Aankondiging: uiterlijk op de voorafgaande 30 november, met vermelding van de hoogte. • Maximum: de stijging is gelimiteerd tot de stijging van het laatst gepubliceerde definitieve indexcijfer over het gehele jaar ten opzichte van het jaar daarvoor. • Eerste moment: op grond van artikel 11.9 GIBIT 2025 kan geen indexering plaatsvinden per de eerstvolgende 1 januari indien de Overeenkomst op of na 1 september van dat jaar is gesloten. De indexering geldt voor de overeengekomen jaartarieven en doorlopende vergoedingen, waaronder de Gebruiksrechtenvergoeding en de uurtarieven. De eenmalige Implementatievergoeding wordt niet geïndexeerd. Artikel 15.5 van de concept Overeenkomst bepaalt aan wie indexeringsaankondigingen worden gezonden.
82	**Bijlage 5 PvE eis E24, E25, E26 en Wens W6-B. Voorkeur bij filterbeperkingen in in-scope API's: ESB-integratie versus JAVA-maatwerk.**	Sommige API's van door u in scope genoemde applicaties kennen beperkingen in filter-, paging- en delta-mogelijkheden. Deze beperkingen kunnen op twee manieren worden opgevangen: (a) via een ESB-integratie waarin de ESB de filter-, transformatie- en delta-logica op zich neemt; of (b) via zwaar (JAVA of vergelijkbaar) maatwerk aan de IAM-zijde. Waar geeft Zaanstad in dergelijke gevallen de voorkeur aan?	Opdrachtgever streeft naar zo veel mogelijk gestandaardiseerde koppelingen met het HR-systeem en de doelsystemen. Functionele logica zoals filtering, paging, transformatie en delta-verwerking dient binnen de Oplossing te worden afgehandeld en niet in de ESB/API-gateway of als maatwerk buiten de Oplossing. De in eis E24 genoemde ESB en/of API-gateway betreft de API-gateway OpenTunnel. OpenTunnel is eigendom van Gemeente Zaanstad en valt onder het beheer en de verantwoordelijkheid van Opdrachtgever. Deze wordt door Opdrachtgever ingezet als beveiligde verbindingslaag (proxy) voor de communicatie met externe bron- of doelsystemen. De verbindingslaag heeft geen functionele verwerkingslogica. Voor de koppeling met YouForce geldt dat, indien ten tijde van de PoC of implementatie een IAM-API van YouForce beschikbaar is en deze voldoet aan de gestelde functionele en technische eisen, deze API dient te worden gebruikt. Indien een dergelijke API niet beschikbaar is of niet aan de gestelde eisen voldoet, wordt gebruikgemaakt van de bestaande BINT-bestandsuitwisseling. IAM – On-Premise • IAM → lokale AD (On-Premise) → Microsoft Entra ID, zie ook het antwoord op vraag 147. • IAM → TOPdesk (On-Premise). • IAM → Appsdata (gezipte BINT-bestanden) → API van HR-core → YouForce (SaaS). Indien een geschikte YouForce IAM-API beschikbaar is: IAM → API-gateway OpenTunnel (proxy) → YouForce (SaaS).

Nr.	Onderwerp	Vraag	Antwoord
			IAM – SaaS • IAM → Microsoft Entra ID → lokale AD (On-Premise), zie ook het antwoord op vraag 147. • IAM → API-gateway OpenTunnel (proxy) → TOPdesk (On-Premise). • IAM → BINT-bestanden → API van HR-core → YouForce (SaaS), tenzij er ten tijde van de implementatie een geschikte YouForce IAM-API beschikbaar is, dan: IAM → API-gateway OpenTunnel (proxy) → YouForce (SaaS).
83	**Bijlage 5 PvE eis E24 (integratievoorziening); Offerteleidraad §2.2. Externe koppelingen via ESB / API-gateway.**	"In eis E24 wordt gesteld dat koppelingen met systemen ""kunnen worden gerealiseerd via een door de Opdrachtgever voorgeschreven ESB en/of API-gateway, indien dit een vereiste is om systemen te ontsluiten"". Kan Zaanstad per koppeling in de initiële scope expliciet aangeven of een ESB- of API-gateway-integratie wordt voorgeschreven of dat directe integratie is toegestaan? Indien een ESB is voorgeschreven: zijn er reeds standaard-koppelingen voor YouForce beschikbaar op deze ESB? Wie is verantwoordelijk voor het bouwen en beheer van de ESB-adapters aan bron-/doelsysteemzijde?"	Zie antwoord op vraag 82.
84	**Bijlage 5 PvE eis E28 (HR-systeem); Bijlage 13 Functioneel Ontwerp bijlage 4. YouForce/Beaufort-koppeling: BINT-XML nu, REST-API in de toekomst.**	"In eis E28 wordt gesteld dat de HR-koppeling plaatsvindt via een BINT-bestand (Beaufort Interface-bestand, XML) en ""in de toekomst mogelijk Rest-Api"". Betreft de te realiseren koppeling op moment van implementatie uitsluitend het ontvangen en verwerken van BINT-XML bestanden, of moet de Oplossing bij oplevering óók de Youforce/Beaufort REST-API kunnen aanroepen? Zijn er reeds afspraken met Visma|Raet over aansluiting op de standaard-Youforce API, en wijkt de bij Zaanstad in gebruik zijnde Beaufort-koppeling af van de standaard Youforce-API? Kan Zaanstad de technische specificatie van het BINT-bestand met de kandidaten delen? Hoe wordt het BINT-bestand beschikbaar gesteld? "	Voor de wijze van integratie met YouForce en de keuze tussen de beschikbare IAM-API en de bestaande BINT-bestandsuitwisseling wordt verwezen naar het antwoord op vraag 82. De technische specificatie van het BINT-bestand en de wijze waarop dit beschikbaar wordt gesteld, zijn opgenomen in/worden beschikbaar gesteld als bijlage 17.
85	**Bijlage 5 PvE eis E4 en eis E28 (onderdeel 2. Email). E-mailplatform: Exchange Online of Exchange on-premise.**	"Kan Zaanstad expliciet bevestigen welk e-mailplatform in de doelarchitectuur wordt gebruikt: Exchange Online (M365, cloud), Exchange on-premise, of een hybride variant? En kan Zaanstad bevestigen dat mailbox-provisioning volledig plaatsvindt via AD-groepslidmaatschap?"	Opdrachtgever maakt gebruik van een hybride Exchange-omgeving. Mailbox-provisioning vindt niet plaats op basis van AD-groepslidmaatschap. In de huidige situatie wordt het mailbox-provisioningproces vanuit het IAM-systeem aangestuurd via een PowerShell-script, waarmee de mailbox wordt aangemaakt.

Nr.	Onderwerp	Vraag	Antwoord
86	**Offerteleidraad §5.3.2 (Plan van Aanpak) en §6.4 (Proof of Concept); Bijlage 5 PvE §4.2.2. KPI's ter monitoring van het implementatietraject.**	"Welke KPI's hanteert Zaanstad om een succesvol implementatietraject te monitoren en te beoordelen? Wij denken hierbij bijvoorbeeld aan doorlooptijd IDU-mutaties. Zijn KPI's reeds gedefinieerd? "	Opdrachtgever heeft voor het implementatietraject geen afzonderlijke set KPI's gedefinieerd. Het uitgangspunt is dat de implementatie succesvol wordt afgerond binnen de overeengekomen planning en dat de aangeboden Oplossing aantoonbaar voldoet aan de eisen en wensen uit de aanbestedingsstukken. Het PvE vormt daarbij de basis voor zowel de Proof of Concept als de acceptatie van de Oplossing. De Proof of Concept en de acceptatie van de geïmplementeerde Oplossing vormen belangrijke beoordelingsmomenten. Nadere afspraken over planning, voortgang en mijlpalen worden in overleg tussen partijen uitgewerkt tijdens de PoC en de voorbereiding en uitvoering van de implementatie. Deze afspraken vormen geen aanvulling op of wijziging van de in de aanbestedingsstukken opgenomen eisen en wensen.
87	**Offerteleidraad §2.1 (Doelstellingen) en §2.3 (Optionele werkzaamheden); Bijlage 5 PvE §2 en Wens W9. Potentie doorontwikkeling en business-adoptie.**	"In de scope ligt de nadruk op de technische implementatie van achtergrondprocessen. Doorontwikkeling wordt slechts summier benoemd. Kan de gemeente Zaanstad haar visie op de doorontwikkeling na initiële implementatie nader toelichten? Welke ambities heeft de gemeente ten aanzien van onboarding van aanvullende bron- en doelsystemen, self-service voor eindgebruikers, integratie met business-workflows, RBAC/ABAC-toepassingen en verbreding richting business-processen? Op welke termijn (jaar 2 t/m 6) verwacht Zaanstad deze verbreding te realiseren, en ziet de gemeente de Opdrachtnemer als leidende partij bij deze verbreding of primair als leverancier van de technische enabler waarna Zaanstad zelf regie voert op de business-adoptie?"	Opdrachtgever heeft de scope van deze aanbesteding bewust beperkt gehouden en kiest daarbij voor een beheersbare en doelmatige inrichting van de IAM-oplossing. De beoogde doorontwikkeling is beschreven in wens W6 (tweede en derde bullet), wens W7 en wens W9 van het Programma van Eisen en Wensen. Opdrachtgever heeft op dit moment geen concrete ambities voor uitbreiding van integraties met andere bron- en doelsystemen dan de in paragraaf 3.2.5 opgenomen integraties. Eventuele toekomstige doorontwikkeling zal worden bepaald op basis van de dan geldende behoeften, prioriteiten en beheerbaarheid van de oplossing. Het is daarmee niet de bedoeling dat gedurende de looptijd zonder nadere besluitvorming een omvangrijke uitbreiding van de integraties of functionaliteit plaatsvindt. Opdrachtgever voert zelf de regie over eventuele toekomstige doorontwikkeling. De rol van Opdrachtnemer is daarbij primair het leveren en doorontwikkelen van de Oplossing binnen de overeengekomen scope en het ondersteunen van Opdrachtgever waar dat voor de uitvoering daarvan nodig is.
88	**Bijlage 5 PvE eis E56 en E57; Offerteleidraad §3.15. Taaleis 2e- en 3e-lijns support.**	Is Zaanstad bereid de taaleisen uit PvE-eisen E56 en E57 te verruimen, zodat ondersteuning in de tweede en derde lijn tijdens de beheerfase ook in het Engels mag worden aangeboden? Een dergelijke verruiming kan bijdragen aan een kostenefficiëntere inrichting van de ondersteuning, zonder afbreuk te doen aan de kwaliteit van de dienstverlening.	Nee. Opdrachtgever handhaaft de taaleisen zoals opgenomen in eis E56 en E57. De ondersteuning in de tweede en derde lijn is gericht op de ondersteuning van de door Opdrachtgever aangewezen functioneel en technisch beheerders. Voor een effectieve communicatie en afstemming met deze beheerders acht Opdrachtgever Nederlandstalige ondersteuning noodzakelijk.
89	**Offerteleidraad §5.2.1 Prijsplafond**	Het vastgestelde prijsplafond van € 735.000 lijkt naar onze inschatting onvoldoende aan te sluiten bij het huidige marktniveau. Is Zaanstad bereid de gehanteerde bandbreedte, zowel de drempel als het plafond, met € 150.000 tot € 200.000 te verhogen? Dit biedt inschrijvers meer ruimte om een marktconforme en kwalitatief hoogwaardige oplossing aan te bieden.	Nee. Opdrachtgever is niet bereid de prijsdrempel en het prijsplafond te verhogen. De bandbreedte is vastgesteld op basis van de resultaten van de marktconsultatie, waarin leveranciers is gevraagd de eenmalige implementatiekosten en de structurele jaarkosten voor circa 3.000 identiteiten op te geven. Daarnaast is de scope van deze aanbesteding bewust beperkt gehouden: het betreft de vervanging van een bestaande, inhoudelijk stabiele autorisatiestructuur, met een beperkt aantal bron- en doelsystemen en zonder herontwerp van het autorisatiemodel. Opdrachtgever acht de vastgestelde bandbreedte daarmee marktconform en passend bij de uitgevraagde scope, en handhaaft deze. Zie ook het antwoord op vraag 191.

Nr.	Onderwerp	Vraag	Antwoord
90	**Maximale aansprakelijkheid**	Bijlage 7 (GIBIT 2025), art. 17.3 en 17.4: Kan de aanbestedende dienst bevestigen dat de maximale aansprakelijkheid van de leverancier – behoudens de categorieën van art. 17.5 – is begrensd tot € 1.250.000 per gebeurtenis (max. € 2.500.000 per kalenderjaar) voor persoons- en zaakschade (art. 17.3), respectievelijk tweemaal de Jaarvergoeding per gebeurtenis (max. viermaal de Jaarvergoeding per jaar) voor overige schade (art. 17.4)?	Ja, dit kan worden bevestigd. Behoudens de in artikel 17.5 GIBIT 2025 genoemde uitzonderingen geldt: • voor persoons- en zaakschade en daaruit voortvloeiende schade: maximaal € 1.250.000 per gebeurtenis, met een maximum van tweemaal dat bedrag per kalenderjaar (artikel 17.3); • voor overige schade: maximaal tweemaal de Jaarvergoeding per gebeurtenis, met een maximum van viermaal de Jaarvergoeding per kalenderjaar (artikel 17.4). Samenhangende gebeurtenissen worden aangemerkt als één gebeurtenis. Zie voor de definitie van de Jaarvergoeding het antwoord op vraag 119.
91	**Verzekeringsdekking**	Bijlage 7 (GIBIT 2025), art. 18.2: Art. 18.2 eist dekking voor “ten minste twee gebeurtenissen” per jaar en “ten minste de bedragen” van art. 17.3/17.4 per jaar. Kan de aanbestedende dienst bevestigen dat hiermee wordt aangesloten bij de gangbare polisstructuur (verzekerd bedrag per aanspraak met een maximum van tweemaal het verzekerd bedrag per verzekeringsjaar) en dat een combinatie van een beroepsaansprakelijkheids- en een bedrijfsaansprakelijkheidsverzekering (AVB) volstaat?	Ja, op beide punten. Artikel 18.2 GIBIT 2025 sluit aan bij de gangbare polisstructuur waarbij een verzekerd bedrag per aanspraak geldt met een maximum per verzekeringsjaar. De eis is dat de dekking ten minste twee gebeurtenissen per jaar omvat en per jaar ten minste de in artikel 17.3 en 17.4 genoemde bedragen. Een combinatie van een beroepsaansprakelijkheids- en een bedrijfsaansprakelijkheidsverzekering volstaat, mits de gecombineerde dekking voldoet aan de in paragraaf 4.2.1 van de Offerteleidraad gestelde minimumbedragen van € 2.500.000 per gebeurtenis en € 5.000.000 per jaar.
92	**Aansprakelijkheid datalek**	Bijlage 9 (Verwerkersovereenkomst), art. 6.1 jo. Bijlage 7 (GIBIT) art. 17: Art. 6.1 Verwerkersovereenkomst verklaart de aansprakelijkheidsbeperkingen uit de Hoofdovereenkomst van toepassing op de Verwerkersovereenkomst. Kan de aanbestedende dienst bevestigen dat schade en boetes die voortvloeien uit een inbreuk in verband met persoonsgegevens (datalek) zonder opzet/grove schuld eveneens onder de caps van art. 17.3/17.4 GIBIT vallen en dus niet onbeperkt zijn?	Ja, dit kan worden bevestigd. Artikel 6.1 van de Verwerkersovereenkomst bepaalt uitdrukkelijk dat de in de Hoofdovereenkomst overeengekomen beperkingen van de aansprakelijkheid ook betrekking hebben op de Verwerkersovereenkomst. Schade en boetes die voortvloeien uit een inbreuk in verband met persoonsgegevens vallen daarmee onder de plafonds van artikel 17.3 en 17.4 GIBIT 2025, tenzij zich een van de in artikel 17.5 GIBIT 2025 genoemde uitzonderingen voordoet. Voor boetes van de toezichthoudende autoriteit geldt de specifieke regeling van artikel 17.5 sub iv, waaronder de daarin opgenomen voorwaarden over informatie en betrokkenheid van Leverancier bij het verweer.
93	**Facturering derde partijsoftware**	Bijlage 6 (Concept Overeenkomst), art. 11.2 vs. Bijlage 7 (GIBIT) art. 11.2: Art. 11.2 van de Overeenkomst bepaalt dat de kosten van derdepartijsoftware geacht worden te zijn inbegrepen in de Implementatievergoeding (en dus volgens het schema van art. 15.3 gefactureerd), terwijl art. 11.2 GIBIT bepaalt dat voor Derdenprogrammatuur 100% verschuldigd is bij levering. Deze bepalingen zijn strijdig. Kan de aanbestedende dienst bevestigen welke regeling prevaleert voor de facturering van derdepartijsoftware?	Artikel 11.2 van de concept Overeenkomst prevaleert. Op grond van artikel 2.2 van de concept Overeenkomst gaat de Overeenkomst voor op de GIBIT 2025. Artikel 11.2 van de Overeenkomst bepaalt uitdrukkelijk dat Opdrachtnemer gedurende de Implementatieperiode geen kosten in rekening kan brengen die verband houden met Gebruiksrechten, licenties of derdepartijsoftware, en dat deze geacht worden te zijn inbegrepen in de Implementatievergoeding. Dit sluit aan bij de definitie van de Implementatievergoeding in artikel 1.1 van de Overeenkomst. De facturering van de Implementatievergoeding, inclusief de daarin begrepen derdepartijsoftware, verloopt daarmee volgens het schema van artikel 15.3 van de concept Overeenkomst. Zie ook de antwoorden op de vragen 10 en 33.

Nr.	Onderwerp	Vraag	Antwoord
94	**Fatale implementatiedatum**	Bijlage 6 (Concept Overeenkomst), art. 5.3/5.4 jo. Bijlage 7 (GIBIT) art. 4.2: De implementatie kent een “vaste en fatale” einddatum (4 oktober 2027), die de aanbestedende dienst bovendien eenzijdig kan wijzigen met behoud van het fatale karakter (art. 5.3). Nu de implementatie mede afhankelijk is van tijdige medewerking en aanlevering door de aanbestedende dienst, kan zij bevestigen dat het fatale karakter vervalt of opschuift voor zover de vertraging is toe te rekenen aan de aanbestedende dienst of aan overmacht?	Zie antwoord vraag 9.
95	**Looptijd en opzegrecht**	Bijlage 6 (Concept Overeenkomst), art. 5.9 jo. Bijlage 7 (GIBIT) art. 27.2 e.v.: De overeenkomst kent een looptijd van maximaal 18 jaar (art. 5.9) en kan door de leverancier niet tussentijds worden opgezegd (art. 27.2 GIBIT), terwijl de aanbestedende dienst diverse tussentijdse opzeggings- en ontbindingsrechten heeft (o.a. art. 27.3–27.5 en 27.11). Kan de aanbestedende dienst deze onevenwichtigheid toelichten en aangeven of ook voor de leverancier een redelijk tussentijds opzegrecht geldt?	Opdrachtgever licht dit als volgt toe. De Overeenkomst wordt aangegaan voor bepaalde tijd. Op grond van artikel 27.2 GIBIT 2025 kunnen overeenkomsten voor bepaalde tijd niet tussentijds worden opgezegd, behoudens de specifieke opzeggingsgronden. De in artikel 27.2 genoemde termijnen van drie en achttien maanden zien uitsluitend op overeenkomsten voor onbepaalde tijd en zijn hier niet van toepassing. Zie ook het antwoord op vraag 29. De achtergrond van het verschil is de continuïteit van een beveiligingskritieke gemeentelijke voorziening. Het IAM-systeem reguleert de toegang tot alle gemeentelijke systemen en gegevens. Bij het wegvallen daarvan is een zorgvuldige transitie naar een opvolger noodzakelijk, waarvoor Opdrachtgever aanzienlijk meer tijd nodig heeft dan Opdrachtnemer. Daarnaast doet Opdrachtgever een aanzienlijke implementatie-investering die over de looptijd moet worden terugverdiend; dat geldt wederzijds. Opdrachtgever is bereid in de definitieve Overeenkomst een tussentijds opzegrecht voor Opdrachtnemer op te nemen dat kan worden uitgeoefend na afloop van de initiële Gebruiksperiode van zes jaar, met inachtneming van een opzegtermijn van achttien maanden en onder de voorwaarde dat Opdrachtnemer volledige medewerking verleent aan het Exit-plan. Gedurende de initiële Gebruiksperiode blijft tussentijdse opzegging door Opdrachtnemer uitgesloten.
96	**Opzegtermijn (asymmetrie)**	Bijlage 7 (GIBIT 2025), art. 27.2: De opzegtermijn voor overeenkomsten voor onbepaalde tijd bedraagt 3 maanden voor de aanbestedende dienst en 18 maanden voor de leverancier. Deze asymmetrie is onevenredig ten nadele van de leverancier. Is de aanbestedende dienst bereid tot een evenwichtiger opzegregeling?	Zie hiervoor het antwoord op vraag 95.
97	**IE-rechten maatwerk**	Bijlage 7 (GIBIT 2025), art. 21.4 en 21.5: Art. 21.4 draagt alle IE-rechten op Maatwerkprogrammatuur (incl. broncode, met afstand van persoonlijkheidsrechten) over aan de aanbestedende dienst, waarbij de koopprijs geacht wordt in de Vergoeding te zijn begrepen; art. 21.5 levert maatwerk bovendien standaard als Open Source op. Kan de aanbestedende dienst bevestigen dat standaard-/productprogrammatuur en de daaraan ten grondslag liggende (achtergrond-)IE bij de leverancier blijven, en is zij bereid	Ja. Opdrachtgever bevestigt dat de intellectuele eigendomsrechten op de Standaardprogrammatuur en de daaraan ten grondslag liggende achtergrondrechten bij Leverancier of diens licentiegevers berusten. Dit volgt uit artikel 21.1 GIBIT 2025. Op uw drie deelvragen: a. Opdrachtgever ziet geen aanleiding de definitie van Maatwerkprogrammatuur aan te passen. De definitie van artikel 1.31 GIBIT 2025 is voldoende bepaald. Opdrachtgever gaat er nadrukkelijk van uit dat binnen deze Opdracht geen Maatwerkprogrammatuur wordt ontwikkeld; zie het antwoord op vraag 27.

Nr.	Onderwerp	Vraag	Antwoord
		(a) “Maatwerk” eng te definiëren, (b) een afzonderlijke vergoeding voor IE-overdracht overeen te komen en (c) de open-sourceplicht te laten vervallen voor concurrentiegevoelige componenten?	b. Nee. Artikel 21.4 GIBIT 2025 bepaalt dat de koopprijs voor de overdracht geacht wordt in de Vergoeding besloten te liggen. Nu Opdrachtgever geen maatwerk verwacht, ontstaat op dit punt naar verwachting geen discussie. c. Nee, en dat is ook niet nodig. Artikel 21.5 GIBIT 2025 zondert Maatwerkprogrammatuur die niet los van de gecontracteerde Standaardprogrammatuur kan worden gebruikt reeds uit van de open-sourceverplichting. Zie het antwoord op vraag 28.
98	**Overmacht**	Bijlage 7 (GIBIT 2025), art. 20.2: Art. 20.2 sluit onder meer personeelstekort, ziekte (m.u.v. pandemie), staking en liquiditeits-/solvabiliteitsproblemen uit als overmacht aan de zijde van de leverancier. Is de aanbestedende dienst bereid ziekte/uitval van niet-vervangbaar personeel en niet-toerekenbare uitval van toeleveranciers als overmacht te erkennen?	Nee. Opdrachtgever is niet bereid ziekte of uitval van niet-vervangbaar personeel en niet-toerekenbare uitval van toeleveranciers als overmacht te erkennen. De beschikbaarheid van gekwalificeerd personeel en de keuze voor en aansturing van toeleveranciers behoren tot de bedrijfsvoering en de risicosfeer van Opdrachtnemer. Opdrachtgever kan die risico's niet beïnvloeden of beheersen. Bij een beveiligingskritieke voorziening die als Dienstverlening op Afstand wordt geleverd, mag van Opdrachtnemer worden verwacht dat hij zijn dienstverlening zo inricht dat deze niet afhankelijk is van één individuele medewerker. Artikel 20.2 GIBIT 2025 erkent een aantoonbare storing van nuts- of telecomvoorzieningen wel als overmacht, evenals ziekte van Personeel als gevolg van een pandemie. Zie ook het antwoord op vraag 30.
99	**Continuïteitsmaatregelen / escrow**	Bijlage 7 (GIBIT 2025), art. 39.1–39.2: Art. 39 verplicht de leverancier op eerste verzoek mee te werken aan aanvullende continuïteitsmaatregelen, waaronder data-escrow en een hoofdelijke borgstelling door een derde. Kan de aanbestedende dienst de reikwijdte hiervan begrenzen (bijv. tot data-escrow) en bevestigen dat de kosten van dergelijke maatregelen voor rekening van de aanbestedende dienst komen?	Opdrachtgever begrenst de reikwijdte van artikel 39 GIBIT 2025 niet vooraf, maar licht het volgende toe. Artikel 39.1 bevat een bereidverklaring om op eerste verzoek aanvullende afspraken te maken; het legt niet zelfstandig een verplichting op tot een bepaalde maatregel. Artikel 39.2 bepaalt bovendien uitdrukkelijk dat de daar genoemde maatregelen worden getroffen tegen een redelijke vergoeding. De kosten van dergelijke maatregelen komen daarmee voor rekening van Opdrachtgever, tenzij Partijen anders overeenkomen. Opdrachtgever verlangt in deze aanbesteding geen escrow en geen borgstelling. De continuïteit is geborgd via het Exit-plan (artikel 13 concept Overeenkomst, eis E55 en wens W13). Zie ook het antwoord op vraag 78.
100	**Kosteloze exit-medewerking**	Bijlage 7 (GIBIT 2025), art. 29.7 en 29.11: Art. 29.7/29.11 verplichten de leverancier tot kosteloze exit-medewerking bij (gestelde) toerekenbare tekortkoming respectievelijk bij aan de leverancier toe te rekenen vertraging. Kan de aanbestedende dienst bevestigen dat “kosteloos” pas geldt nadat de toerekenbare tekortkoming in rechte of bij minnelijke regeling is komen vast te staan?	Nee, die uitleg volgt Opdrachtgever niet. Artikel 29.7 GIBIT 2025 knoopt aan bij de beëindiging van de Overeenkomst wegens toerekenbaar tekortschieten door Leverancier, niet bij het onherroepelijk vaststaan daarvan in rechte. Zou de kosteloosheid pas intreden na een rechterlijk oordeel of een minnelijke regeling, dan zou de exit-medewerking in de praktijk juist in de situatie waarin die het hardst nodig is worden vertraagd. Dat verhoudt zich niet tot de continuïteit van een beveiligingskritieke voorziening. Opdrachtgever bevestigt wel dat indien achteraf komt vast te staan dat van een toerekenbare tekortkoming geen sprake was, Opdrachtnemer alsnog aanspraak heeft op vergoeding van de verrichte exitwerkzaamheden conform artikel 29.4 GIBIT 2025. De werkzaamheden bedoeld in artikel 29.6 sub ii worden hoe dan ook kosteloos verricht.

Nr.	Onderwerp	Vraag	Antwoord
101	**Kosteloze exit-medewerking**	Bijlage 7 (GIBIT 2025), art. 29.7 en 29.11: Art. 29.7/29.11 verplichten de leverancier tot kosteloze exit-medewerking bij (gestelde) toerekenbare tekortkoming respectievelijk bij aan de leverancier toe te rekenen vertraging. Kan de aanbestedende dienst bevestigen dat “kosteloos” pas geldt nadat de toerekenbare tekortkoming in rechte of bij minnelijke regeling is komen vast te staan?	Zie hiervoor het antwoord op vraag 100.
102	**Betaling na acceptatie**	Bijlage 7 (GIBIT 2025), art. 11.2 jo. Bijlage 6 art. 15.3: 30% van de eenmalige vergoeding is pas opeisbaar na integrale Acceptatie (art. 11.2 GIBIT; art. 15.3 Overeenkomst: 40% na Acceptatie), terwijl de implementatie een fatale einddatum kent. Is de aanbestedende dienst bereid het na Acceptatie opeisbare deel te verlagen of te koppelen aan deelacceptaties/mijlpalen?	Nee. Opdrachtgever handhaaft het in artikel 15.3 van de concept Overeenkomst opgenomen betaalschema van 30% bij ondertekening, 30% bij oplevering van de ingerichte omgeving en 40% na integrale Acceptatie. Opdrachtgever wijst erop dat dit schema Opdrachtnemer op onderdelen gunstiger behandelt dan de GIBIT 2025: 60% van de Implementatievergoeding is opeisbaar vóór Acceptatie, waarvan 30% direct bij ondertekening. Daarmee is een groot deel van de implementatie-inspanning tussentijds gefinancierd. De koppeling van het laatste deel aan integrale Acceptatie is voor Opdrachtgever een wezenlijke prikkel om te borgen dat het IAM-systeem daadwerkelijk voldoet aan het Programma van Eisen en Wensen en aan de Inschrijving. Zie voor de samenhang met de fatale einddatum het antwoord op vraag 9.
103	**Meldtermijn datalek**	Bijlage 9 (Verwerkersovereenkomst), art. 5.1: Art. 5.1 verplicht de verwerker een (vermoedelijke) inbreuk uiterlijk binnen 24 uur te melden. Is de aanbestedende dienst bereid deze termijn te verruimen naar 48–72 uur na ontdekking, aansluitend bij hetgeen in de markt gebruikelijk is en bij de meldtermijn van art. 33 AVG voor de verwerkingsverantwoordelijke?	Nee. Opdrachtgever ziet geen aanleiding de meldtermijn aan te passen. De door Inschrijver aangehaalde termijn van 72 uur uit artikel 33 AVG ziet op de meldplicht van de verwerkingsverantwoordelijke aan de toezichthouder en niet op de meldplicht van de verwerker aan de verwerkingsverantwoordelijke. Juist om Opdrachtgever voldoende tijd te geven een incident te beoordelen en, indien nodig, tijdig aan zijn wettelijke verplichtingen te voldoen, acht Opdrachtgever een meldtermijn van 24 uur passend. Opdrachtgever handhaaft daarom de in de Verwerkersovereenkomst opgenomen meldtermijn van 24 uur. Zie ook de antwoorden op vraag 37 en 38.
104	**Certificeringseisen (ISO/SOC 2)**	Bijlage 9 (Verwerkersovereenkomst), Bijlage 2 (normenstelsel): Bijlage 2 verlangt ISO 27001, ISO 27017 én ISO 27018, alsmede een SOC 2-assurancerapport (NOREA-TPM) en aansluiting bij de BIO. Zijn ISO 27017/27018 en het SOC 2-rapport harde (knock-out)eisen, of volstaat een ISO 27001-certificering aangevuld met een verklaring van toepasselijkheid en passende aanvullende maatregelen, zoals het binnenkort verkrijgen van SOC 2 type II-verklaring en overige certificeringen?	De in Bijlage 2 bij de Verwerkersovereenkomst en in paragraaf 4.2.4 van de Offerteleidraad opgenomen certificerings- en assurance-eisen zijn harde eisen. Het niet voldoen daaraan bij Inschrijving leidt tot terzijdelegging van de Inschrijving. Een ISO 27001-certificering met Verklaring van Toepasselijkheid, aangevuld met passende aanvullende maatregelen of met een voorgenomen dan wel lopend certificeringstraject, volstaat niet. De gevraagde stukken dienen bij Inschrijving te worden overgelegd; een op dat moment nog te verkrijgen SOC 2 Type II-verklaring kwalificeert niet. Zie voor de assurancevormen die Opdrachtgever als gelijkwaardig accepteert het antwoord op vraag 23, en voor ISO 27017 en ISO 27018 het antwoord op vraag 36.

Nr.	Onderwerp	Vraag	Antwoord
105	**Risicoverdeling risicoanalyse**	Bijlage 7 (GIBIT 2025), art. 4.4 en 6.8: Art. 4.4 geeft de aanbestedende dienst een kosteloos ontbindingsrecht indien een voorstel uit de risicoanalyse onaanvaardbaar is, en art. 6.8 legt de kosten van “te voorziene” aanpassingen bij de leverancier. Kan de aanbestedende dienst bevestigen dat deze risicoverdeling is begrensd tot hetgeen de leverancier op basis van de bij inschrijving verstrekte informatie redelijkerwijs kon voorzien?	Ja, dit is juist begrepen. Artikel 6.8 GIBIT 2025 knoopt zelf al aan bij hetgeen Leverancier had behoren te voorzien in zijn aanbod dan wel in de risicoanalyse. Kosten van aanpassingen die Leverancier redelijkerwijs niet kon voorzien op basis van de bij Inschrijving verstrekte informatie, komen dus niet op grond van dat artikel voor zijn rekening. Ten aanzien van artikel 4.4 GIBIT 2025 merkt Opdrachtgever op dat de daarin genoemde mogelijkheid om de risicoanalyse na totstandkoming van de Overeenkomst uit te voeren, blijkens de tekst van dat artikel niet bestaat indien sprake is van een aanbesteding als bedoeld in artikel 3.6 GIBIT 2025. Opdrachtgever hecht eraan dat Inschrijver de bij de Inschrijving verstrekte informatie, waaronder het Functioneel Ontwerp en de Voorbeeld Conversiedata, zorgvuldig bestudeert en eventuele onduidelijkheden in deze inlichtingenronde adresseert.
106	**SOC 2 / ISAE-assurance bij open source**	Offerteleidraad §4.2.4 jo. Bijlage 5 (PvE) E32: De eisen verlangen een SOC 2 Type II / ISAE 3000 Type II-assurance “over de softwareleverancier”. Een van onze oplossingen is gebaseerd op open-source software (Evolveum MidPoint); de softwareleverancier daarvan is een open-source community/leverancier die deze assurance en een machtigingsverklaring in de regel niet afgeeft. Kan de aanbestedende dienst bevestigen dat voor een op open source gebaseerde SaaS-dienst een assurancerapport over de dienst van de inschrijver (inclusief de door hem toegevoegde componenten en het beheer), aangevuld met de certificering van de hostingpartij, volstaat?	Nee. De eis dat de softwareleverancier beschikt over een assuranceverklaring blijft onverkort gelden, ook indien de aangeboden Oplossing is gebaseerd op open-source software. Paragraaf 4.2.4 van de Offerteleidraad koppelt de eis aan de softwareleverancier omdat de kern van de beveiliging van de Oplossing daar wordt bepaald: het ontwikkelproces, het beheer van kwetsbaarheden en de release- en patchcyclus. Een assurancerapport dat uitsluitend ziet op de dienst van Inschrijver en op de door hem toegevoegde componenten geeft Opdrachtgever geen zekerheid over die keten. Aanvulling met de certificeringen van de hostingpartij verandert dat niet. Indien Inschrijver zelf de partij is die de betreffende softwarecomponent onderhoudt, distribueert en ondersteunt, kan hij in die hoedanigheid als softwareleverancier optreden en zelf aan de eis voldoen. Zie voor de assurancevormen die als gelijkwaardig worden geaccepteerd het antwoord op vraag 23.
107	**Zero-knowledge encryptie**	Bijlage 5 (PvE) E41 (jo. E42/E45): E41 verlangt dat de opdrachtnemer de gegevens “niet kan ontsleutelen” (Zero-Knowledge), met tenant-side encryptie. Een IAM-systeem moet identiteitsattributen juist verwerken en provisionen, waardoor volledige onontsleutelbaarheid door de verwerkende dienst voor de kernfunctie technisch niet haalbaar is. Kan de aanbestedende dienst bevestigen dat deze eis, conform de eigen formulering “op alle componenten waarbij dit technisch mogelijk is”, niet geldt voor de gegevens die het IAM-systeem functioneel moet verwerken?	Zie antwoord vraag 5.
108	**Beschikbaarheid (SLA)**	Bijlage 5 (PvE) E60: E60 eist 99,9% beschikbaarheid per kalenderjaar, exclusief gepland onderhoud (max. 20 uur/jaar). Wordt de beschikbaarheid 24x7 over het volledige kalenderjaar gemeten of binnen een servicewindow, en welke prioriteits-/verstoringsklassen tellen mee in de berekening?	De beschikbaarheid wordt gemeten over het volledige kalenderjaar, 24 uur per dag, met uitzondering van vooraf aangekondigd gepland onderhoud zoals bedoeld in eis E60. Voor de berekening van de beschikbaarheid worden verstoringen meegewogen die leiden tot volledige of nagenoeg volledige onbeschikbaarheid van de Oplossing, dan wel tot een ernstige verstoring van kernfunctionaliteit voor alle of het merendeel van de Gebruikers. Dit sluit aan bij de omschrijving van de hoogste prioriteitscategorie in eis

Nr.	Onderwerp	Vraag	Antwoord
			E61. Niet iedere afzonderlijke verstoring of beperking van functionaliteit leidt daarmee tot een vermindering van de in eis E60 bedoelde beschikbaarheid; dergelijke verstoringen vallen wel onder het incidentmanagementproces van eis E61. Opdrachtgever verduidelijkt daarbij de werking van de SLA. Conform eis E59 levert Opdrachtnemer tijdens de Proof of Concept een concept-SLA aan, gebaseerd op de in het Programma van Eisen en Wensen gestelde eisen en wensen. Opdrachtgever stelt zelf geen SLA op. De SLA van Opdrachtnemer wordt onderdeel van de Overeenkomst en neemt daarin een lage plaats in de rangorde in: bij strijdigheid prevaleren het Programma van Eisen en Wensen, de Offerteleidraad en de overige hoger gerangschikte documenten. Dit betekent dat de normen zelf niet ter discussie staan. De beschikbaarheidsnorm van 99,9% en het maximum van twintig uur gepland onderhoud volgen uit eis E60 en kunnen niet door de SLA van Opdrachtnemer worden gewijzigd. De door Opdrachtnemer gehanteerde meetmethode, meetintervallen en rapportagesystematiek kunnen wel uit diens SLA worden overgenomen, mits deze aantoonbaar aansluiten bij de hierboven beschreven uitgangspunten en de gestelde norm daarmee niet feitelijk wordt verlaagd. Zie ook het antwoord op vraag 124.
109	**Supportafbakening (lijnen)**	Bijlage 5 (PvE) E57/E61 en W11: Kan de aanbestedende dienst de afbakening van support bevestigen: functioneel beheer en 0e/1e-lijns eindgebruikerssupport bij de opdrachtgever, en 2e–4e-lijns support bij de opdrachtnemer? De formulering “functionele vragen” bij de opdrachtnemer (E57) is nu voor meerdere uitleg vatbaar.	Ja. Opdrachtgever bevestigt de volgende afbakening van de ondersteuning: 0e en 1e lijn: ondersteuning van eindgebruikers en de eerste analyse en afhandeling van vragen en meldingen ligt bij Opdrachtgever. Functioneel en technisch beheer: Opdrachtgever is verantwoordelijk voor het beheer van de Oplossing en voor de afhandeling van vragen en incidenten die binnen de eigen beheerorganisatie kunnen worden opgelost. 2e en 3e lijn: Opdrachtnemer ondersteunt de door Opdrachtgever aangewezen functioneel en technisch beheerders bij vraagstukken die niet binnen de beheerorganisatie van Opdrachtgever kunnen worden opgelost. 4e lijn: Opdrachtgever onderscheidt geen afzonderlijke vierde supportlijn. Indien voor het oplossen van een incident of vraagstuk aanvullende ondersteuning van bijvoorbeeld de softwareproducent of een andere onderliggende partij noodzakelijk is, valt het organiseren en aansturen daarvan onder de verantwoordelijkheid van Opdrachtnemer. Dit ontslaat Opdrachtnemer niet van de verantwoordelijkheid voor de afhandeling richting Opdrachtgever.
110	**On-premise licentiekosten (80%-regel)**	Bijlage 6 (Concept Overeenkomst) art. 7.3 jo. Offerteleidraad §2.2/§5.2.2: Art. 7.3 stelt de jaarlijkse On-Premise-licentiekosten op 80% van de SaaS-licentiekosten. Bij een op open source gebaseerde oplossing bestaan er geen klassieke (per-seat) licentiekosten. Hoe wenst de aanbestedende dienst dat het Prijzenblad en de 80%-regel worden ingevuld voor een open-source-/abonnementsmodel? We denken dat bij open source de support voor on-premise duurder is dan bij SaaS.	De 80%-regel ziet op de structurele kosten van het On-Premise-model ten opzichte van het SaaS-model. Ook indien sprake is van een open-source- of abonnementsmodel zonder afzonderlijke licentiekosten, verwacht Opdrachtgever dat Inschrijver de kosten voor ondersteuning, onderhoud, beheer en overige structurele dienstverlening inzichtelijk maakt binnen de systematiek van het Prijzenblad. Opdrachtgever acht het niet wenselijk deze activiteiten volledig zelf uit te voeren of daarvoor afhankelijk te zijn van eigen specialistische kennis. Van Inschrijver wordt daarom verwacht dat deze inzichtelijk maakt welke ondersteuning en dienstverlening onderdeel uitmaken van het aangeboden On-Premise-model en hoe deze zich

Nr.	Onderwerp	Vraag	Antwoord
			verhouden tot het SaaS-model. De systematiek van het Prijzenblad en de in de aanbestedingsstukken opgenomen 80%-regel blijven daarbij ongewijzigd van toepassing.
111	**IP-filtering en SSL-inspectie**	Bijlage 5 (PvE) E48 en E50: Kan de aanbestedende dienst de verwachtingen rond IP-filtering (statische IP's, E48) en SSL-inspectie op het verkeer tussen de gemeente en de SaaS (E50) verduidelijken?	Het doel van eis E48 is dat Opdrachtgever in staat wordt gesteld om netwerkverkeer naar en van de Oplossing adequaat te beveiligen en waar nodig te beperken tot vooraf bekende en controleerbare bronnen of bestemmingen. Voor SaaS-oplossingen geldt daarom als uitgangspunt dat Opdrachtnemer transparantie biedt over de netwerkconnectiviteit die nodig is voor de dienstverlening. Indien beschikbaar hebben één of meerdere vaste (statische) IP-adressen de voorkeur, met name voor integratieverkeer tussen de Oplossing en systemen van Opdrachtgever of andere gecontroleerde koppelingen. Toegang van eindgebruikers tot de SaaS-oplossing verloopt in beginsel via internet en valt niet noodzakelijk onder deze eis. Opdrachtgever staat gelijkwaardige beveiligingsmaatregelen toe, zoals FQDN-allowlisting, private endpoints, private-connectivity-oplossingen, service tags of vergelijkbare mechanismen, mits aantoonbaar hetzelfde of een hoger beveiligingsniveau wordt gerealiseerd en de oplossing beheersbaar blijft binnen de beveiligingsarchitectuur van Opdrachtgever. Ten aanzien van SSL-inspectie (E50) geldt dat de Oplossing geen technische beperkingen mag opleggen die het gebruik van door Opdrachtgever toegepaste beveiligingsmaatregelen onmogelijk maken. Opdrachtgever begrijpt dat end-to-end versleuteling, certificaatvalidatie, mutual TLS (mTLS), certificaat-pinning of vergelijkbare beveiligingsmechanismen in bepaalde situaties SSL-inspectie kunnen beperken of uitsluiten. In dergelijke gevallen dient Opdrachtnemer dit expliciet te beschrijven en aan te tonen welke alternatieve beveiligings-, detectie- en monitoringsmaatregelen worden toegepast. Opdrachtgever beoordeelt dergelijke voorstellen op basis van het gerealiseerde beveiligingsniveau en de beheersbaarheid van de oplossing.
112	**Aantal identiteiten / sizing**	Bijlage 5 (PvE) / Bijlage 3 (Prijzenblad): Voor een sluitende prijsopgave: kan de aanbestedende dienst het verwachte totale aantal te beheren identiteiten opgeven, uitgesplitst naar medewerkers, externe/partneridentiteiten en niet-menselijke/technische identiteiten, alsmede het aantal aan te sluiten bron- en doelsystemen?	Zie het antwoord op vraag 153. Opdrachtgever hanteert circa 3.000 actieve identiteiten als uitgangspunt, met een bandbreedte van circa ±20%. Een verdere uitsplitsing naar type identiteit is niet nodig om een prijsopgave te kunnen maken. Voor de in scope zijnde bron- en doelsystemen wordt verwezen naar de aanbestedingsstukken.
113	**Customer Managed Keys (HSM)**	Bijlage 5 (PvE) E45 (jo. E41): E45 verlangt Customer Managed Keys met FIPS 140-2 Level 3 gecertificeerde HSM's. Is Level 3 een harde eis, en welke cloud-/Key Management-voorzieningen worden als gelijkwaardig aanvaard?	Zie antwoord vraag 5.

Nr.	Onderwerp	Vraag	Antwoord
114	**Overheidsstandaarden e-mail**	Bijlage 5 (PvE) E38: E38 verlangt de overheidsstandaarden (SPF, DKIM, DMARC, DNSSEC, STARTTLS, DANE, IPv4/IPv6, HTTPS, HSTS). Gelden deze ook voor het IAM-systeem als, of uitsluitend voor de door de gemeente verzorgde uitgaande e-mailfunctie? Wij willen namelijk altijd uitsturen via een ‘smart host’ van de gemeente.	Opdrachtgever hanteert als uitgangspunt dat e-mail vanuit de Oplossing wordt verzonden via de gemeentelijke mailinfrastructuur (smart host), conform eis E28 en het marktconsultatieverslag. Indien de Oplossing hiervan gebruikmaakt, gelden de domein- en DNS-gerelateerde standaarden uit E38, zoals SPF, DKIM, DMARC, DNSSEC en DANE, voor de gemeentelijke mailinfrastructuur. De Oplossing hoeft deze standaarden niet zelfstandig te implementeren voor zover deze functionaliteit door de gemeentelijke mailinfrastructuur wordt geleverd. Opdrachtnemer blijft verantwoordelijk voor een correcte en veilige integratie met de gemeentelijke mailvoorziening en voor de correcte werking en configuratie van de e-mailfunctionaliteit binnen de Oplossing, waaronder het ondersteunen van de voor de verbinding vereiste beveiligingsstandaarden. Indien Opdrachtnemer ervoor kiest om e-mail via een eigen mailvoorziening te verzenden, is Opdrachtnemer zelf verantwoordelijk voor naleving van de in E38 genoemde standaarden voor die mailvoorziening.
115	**Auditlog-export naar SIEM**	Bijlage 5 (PvE) E29–E31: Kan de aanbestedende dienst bevestigen dat export van audit-/loggegevens naar het SIEM van de gemeente (bijv. Splunk) volstaat.	Ja, met betrekking tot de export van audit-/loggegevens naar het SIEM kan Opdrachtgever dit (zie ook EIS 29).
116	**Access certification**	Bijlage 5 (PvE) W3: Verwacht de aanbestedende dienst periodieke toegangs-/rechtencertificering (access certification/attestation-campagnes), of volstaat doorlopende regie en inzicht per rolhouder? Dit bepaalt de inrichting van de certificationfunctionaliteit.	De opdrachtgever schrijft geen specifieke periodieke toegangs- of rechtencertificeringscampagnes voor. De vraag lijkt vooral invulling te geven aan wens W1(B): “Signalering en inzicht bij wijzigingen in identiteiten en HR-attributen.” Wellicht kan deze functionaliteit daarom onder deze wens worden opgenomen.
117	**Toelichting PvE-vraag W5**	Bijlage 5 (PvE) W5: Wat wordt bedoeld met vraag C, anders dan is bedoeld bij vraag A?	Met vraag A wordt gevraagd te beschrijven hoe de functionaliteit voor het beheren van autorisaties operationeel werkt binnen de Oplossing. Opdrachtgever is hierbij met name geïnteresseerd in wat een functioneel beheerder te zien krijgt, welke informatie beschikbaar is en in welke mate een bundelticket ondersteunt bij het toevoegen, wijzigen en verwijderen van autorisaties. Vraag C richt zich op het onboarden van nieuwe applicaties binnen de Oplossing. Opdrachtgever wil inzicht krijgen in de wijze waarop een nieuwe applicatie wordt ingericht en aangesloten en in hoeverre dit op een gebruiksvriendelijke en efficiënte wijze kan plaatsvinden.
118	**Onderscheid BML/LML**	Bijlage 13 pagina 8: Wat is precies het onderscheid tussen een BML en een LML?	Een BML (Bedrijfsmiddelenlijst) en een LML (Leidinggevendenmiddelenlijst) zijn HR-attributen, zoals beschreven in de begrippenlijst. Aan deze HR-attributen zijn autorisaties gekoppeld die automatisch worden toegekend aan medewerkers die over het betreffende HR-attribuut beschikken. Het onderscheid is dat een BML wordt toegekend op basis van het type dienstverband, bijvoorbeeld medewerker in vaste dienst, inhuurkracht of wethouder. Een LML wordt toegekend aan medewerkers die een leidinggevende functie vervullen. De aan deze HR-attributen gekoppelde autorisaties worden vervolgens automatisch toegekend via de

Nr.	Onderwerp	Vraag	Antwoord
			IAM-processen.
119	**Concept Overeenkomst art. 17.3 / 17.4**	Artikel 17.3 en 17.4 van de conceptovereenkomst stellen de volgende aansprakelijkheidsplafonds: (i) voor letselschade, zaakschade en daaruit voortvloeiende gevolgschade €1.250.000 per gebeurtenis, met een maximum per kalenderjaar van tweemaal dat bedrag; en (ii) voor overige schade tweemaal de Jaarvergoeding per gebeurtenis, met een maximum per kalenderjaar van viermaal de Jaarvergoeding. Kan de gemeente bevestigen (a) welke kostencomponenten worden meegenomen in de 'Jaarvergoeding' die als grondslag voor deze berekening dient - bijvoorbeeld alleen terugkerende licentie-, onderhouds- en supportkosten, of ook eenmalige implementatiekosten - en (b) of deze aansprakelijkheidsplafonds uitsluitend gelden voor de opdrachtnemer, of ook wederkerig voor de opdrachtgever?	Op uw beide deelvragen. a. De Jaarvergoeding is gedefinieerd in artikel 1.27 GIBIT 2025: de gemiddelde jaarlijkse vergoeding, berekend door de Vergoeding te delen door de initieel beoogde looptijd van de Overeenkomst in jaren. De Vergoeding omvat het geheel van de aan Opdrachtnemer verschuldigde bedragen, dus inclusief de eenmalige Implementatievergoeding. Voor deze Opdracht wordt daarbij uitgegaan van de initiële Gebruiksperiode van zes jaar. b. De aansprakelijkheidsplafonds van artikel 17.3 en 17.4 GIBIT 2025 gelden wederkerig. Artikel 17 spreekt van de aansprakelijkheid van Partijen en artikel 17.5 verwijst naar opzet of grove schuld aan de zijde van "de andere Partij".
120	**E35 Eisenlijst (verplicht indien SaaS)**	Eis E35 stelt dat de opdrachtnemer, indien de oplossing als SaaS wordt geleverd, minimaal eenmaal per kalenderjaar een onafhankelijke penetratietest moet laten uitvoeren op de applicatie en de bijbehorende infrastructuur. Kan de gemeente bevestigen of aan deze jaarlijkse eis ook kan worden voldaan door een combinatie van continue geautomatiseerde kwetsbaarheids-/beveiligingsscanning samen met een onafhankelijke penetratietest eens per twee jaar, mits de inschrijver aantoont dat deze combinatie een gelijkwaardig niveau van zekerheid biedt?	Nee. Opdrachtgever acht een jaarlijkse onafhankelijke penetratietest noodzakelijk en proportioneel gelet op het beveiligingsniveau dat voor de IAM-oplossing wordt vereist. Een combinatie van continue geautomatiseerde scanning en een onafhankelijke penetratietest eens per twee jaar wordt daarom niet als gelijkwaardig beschouwd. Eis E35 blijft ongewijzigd van kracht. Opdrachtgever ziet een jaarlijkse penetratietest als minimum en heeft er de voorkeur voor dat penetratietesten vaker dan eenmaal per jaar worden uitgevoerd. Zie voor de wijze waarop een onafhankelijke penetratietest als bedoeld in eis E35 kan worden benut in het kader van de acceptatie na implementatie tevens het antwoord op vraag 12.
121	**§4.2.2 Kerncompetentie 1 / Bijlage 4**	Kerncompetentie 1 vereist een referentie voor het leveren, implementeren en onderhouden van een IAM-systeem bij een gemeente, een gemeenschappelijke regeling, of een vergelijkbare (semi-)publieke organisatie. Kan de gemeente bevestigen of een referentie bij een (semi-)publieke organisatie buiten het gemeentelijk domein - bijvoorbeeld een zorginstelling die onder publieke financiering en toezicht opereert - kwalificeert als vergelijkbare (semi-)publieke organisatie voor deze eis?	Ja. Een referentie bij een (semi)publieke organisatie buiten het gemeentelijk domein kwalificeert, mits deze vergelijkbaar is met een gemeente of gemeenschappelijke regeling en aan de overige voorwaarden van kerncompetentie 1 wordt voldaan. Opdrachtgever beoordeelt de vergelijkbaarheid aan de hand van het publieke karakter van de organisatie, de aard van de identiteits- en autorisatieprocessen en het toepasselijke normenkader voor informatiebeveiliging. Een zorginstelling die onder publieke financiering en toezicht opereert kan daaraan voldoen. Zie ook de antwoorden op de vragen 13 en 138.
122	**§5.2.1 / §5.2.2 G1 Prijs**	Subgunningscriteria G1.1 en G1.2 hanteren een vaste prijsvloer en -plafond, waarbij een inschrijving onder de vloer of boven het plafond leidt tot uitsluiting van de procedure. Kan de gemeente toelichten hoe de prijsvloer (€350.000) en het prijsplafond (€735.000) voor de inschrijfsom, en de bijbehorende vloer/plafond voor de uurtarieven, tot stand zijn gekomen, en of er ruimte is in dit mechanisme voor inschrijvingen die hier marginaal buiten vallen maar aantoonbaar realistisch en goed onderbouwd zijn?	De prijsdrempel en het prijsplafond zijn gebaseerd op de resultaten van de marktconsultatie, waarin aan de deelnemende leveranciers is gevraagd de eenmalige implementatiekosten en de structurele jaarkosten voor circa 3.000 identiteiten op te geven, in combinatie met de bewust beperkt gehouden scope van deze aanbesteding. Ook de drempel en het plafond voor de uurtarieven zijn uit de marktconsultatie afgeleid. Zie ook de antwoorden op de vragen 190 en 191. Er is binnen dit mechanisme geen ruimte voor inschrijvingen die buiten de bandbreedte vallen. Paragraaf 5.2.1 en 5.2.2 van de Offerteleidraad bepalen ondubbelzinnig dat een inschrijfsom of een totaal consultancy-/meerwerkbedrag onder de drempel of boven het

Nr.	Onderwerp	Vraag	Antwoord
			plafond leidt tot uitsluiting. Van dat objectieve criterium kan Opdrachtgever niet afwijken zonder de gelijke behandeling van inschrijvers te schaden, ook niet indien de inschrijving marginaal buiten de bandbreedte valt en goed is onderbouwd. Inschrijvers die verwachten dat hun aanbieding buiten de bandbreedte valt, wordt verzocht dit onderbouwd aan de orde te stellen in de tweede inlichtingenronde.
123	**E60 / E61**	E60 en E61 vereisen 99,9% beschikbaarheid en 24/7 support met een responstijd van 1 uur voor P1-incidenten. Kan de gemeente verduidelijken of dit harde knock-out eisen zijn, of dat een onderbouwd alternatief beschikbaarheids-/supportniveau - proportioneel aan de kritikaliteit van een IGA-systeem ten opzichte van bijvoorbeeld een primair procesapplicatie - ook acceptabel kan zijn?	De eisen E60 en E61 zijn uitvoeringseisen uit het Programma van Eisen en dienen gedurende de looptijd van de overeenkomst te worden nageleefd. De invulling van E61 is nader verduidelijkt in het antwoord op vraag 196, waarbij de wijze waarop Opdrachtnemer de organisatorische invulling realiseert proportioneel mag zijn aan het gekozen leveringsmodel en de inrichting van de dienstverlening. De in E60 en E61 opgenomen beschikbaarheids- en continuïteitseisen blijven daarbij ongewijzigd van kracht.
124	**E60 Beschikbaarheid SLA**	E60 stelt dat gepland onderhoud aan de SaaS-oplossing niet meer dan 20 uur per kalenderjaar mag bedragen. Kan de gemeente bevestigen of dit maximum alleen geldt voor downtime die zichtbaar is voor de eindgebruiker, of ook voor onderhoudswerkzaamheden zonder impact op productie (bijvoorbeeld in een aparte omgeving of met zero-downtime deployment-technieken)? Is er daarnaast ruimte voor een hogere frequentie van kleinere, niet-verstorende releases, zolang het maximum van 20 uur daadwerkelijke onbeschikbaarheid wordt gerespecteerd?	Ja. Het maximum van twintig uur gepland onderhoud per kalenderjaar geldt uitsluitend voor onderhoud dat leidt tot daadwerkelijke onbeschikbaarheid van de productieomgeving voor eindgebruikers. Niet-verstorend onderhoud, zoals werkzaamheden in niet-productieomgevingen of via zero-downtime deployment, valt hier niet onder. Er is geen beperking op de frequentie van niet-verstorende releases, mits de continuïteit van de dienstverlening wordt geborgd en de daadwerkelijke onbeschikbaarheid door gepland onderhoud binnen de twintig uur per kalenderjaar blijft. De aankondigingstermijn van minimaal vijf werkdagen en de uitvoering buiten reguliere werktijden volgen uit eis E60 en blijven onverkort gelden. Nadere invulling van onderhoudsvensters en communicatie kan worden opgenomen in de door Opdrachtnemer aan te leveren SLA, met inachtneming van de rangorde zoals toegelicht in het antwoord op vraag 108.
125	**§4.2.4 Kwaliteitsborging**	Paragraaf 4.2.4 vereist op het moment van inschrijving zowel een geldig ISO 27001-certificaat als een SOC 2 Type II assurance-rapport (ISAE 3000, maximaal 12 maanden oud). Kan de gemeente bevestigen of een geldig ISO 27001-certificaat met bijbehorende Verklaring van Toepasselijkheid, samen met gelijkwaardig gedocumenteerd bewijs van het informatiebeveiligingsmanagementsysteem, ook als voldoende assurance kan worden geaccepteerd, of is een apart SOC 2 Type II / ISAE 3000-rapport een harde eis zonder alternatief?	Nee. Een geldig ISO 27001-certificaat met Verklaring van Toepasselijkheid, aangevuld met gedocumenteerd bewijs van het informatiebeveiligingsmanagementsysteem, volstaat niet. Paragraaf 4.2.4 vraagt beide documenten: het ISO 27001-certificaat met Verklaring van Toepasselijkheid én een assuranceverklaring waaruit de werking van de beheersingsmaatregelen over een aaneengesloten periode blijkt. Het zijn geen alternatieven van elkaar; de assuranceverklaring dient een aanvullend doel. Opdrachtgever accepteert naast de SOC 2 Type II-rapportage twee gelijkwaardige assurancevormen. Zie hiervoor het antwoord op vraag 23.
126	**§5.3.2 G2.2**	Wordt het Plan van Aanpak primair beoordeeld op de volledigheid van de beschreven methodiek, of op de mate waarin de aanpak aantoonbaar is toegesneden op de specifieke situatie van de gemeente Zaanstad?	Het Plan van Aanpak wordt beoordeeld op zowel de kwaliteit van de voorgestelde methodiek als de mate waarin deze aantoonbaar is toegesneden op de specifieke situatie van de gemeente Zaanstad. Daarbij wegen de samenhang, concreetheid en herkenbaarheid van de implementatieaanpak als geheel zwaarder dan de volledigheid van afzonderlijke onderdelen. Een generieke beschrijving van een implementatiemethodiek zonder duidelijke vertaling naar de situatie, scope en

Nr.	Onderwerp	Vraag	Antwoord
			uitgangspunten van Zaanstad zal daarom minder hoog worden beoordeeld dan een aanpak die deze aspecten concreet en overtuigend met elkaar verbindt.
127	**§5.3.1 Beoordelingswijze**	Als meerdere oplossingsrichtingen tot hetzelfde functionele resultaat leiden, wordt de beoordeling dan gebaseerd op het behaalde resultaat of op de specifieke methode of aanpak waarmee dit resultaat is bereikt?	De beoordeling richt zich primair op het te bereiken functionele resultaat. Indien meerdere oplossingsrichtingen tot hetzelfde functionele resultaat leiden en aan de gestelde eisen en wensen voldoen, staat het inschrijvers vrij hun eigen aanpak te kiezen.
128	**W5 Bundelticketmechanisme**	Klopt de aanname dat bundeltickets rechtstreeks leiden tot operationeel werk in Topdesk, of is voorafgaand een aanvullende functionele beoordeling door de betreffende afdeling vereist voordat een ticket in behandeling wordt genomen?	Ja, die aanname klopt. Bundeltickets leiden rechtstreeks tot operationeel werk voor Functioneel Beheer in TOPdesk. Een aanvullende functionele beoordeling door de betreffende afdeling voorafgaand aan de behandeling van het ticket is hierbij niet voorzien.
129	**Bijlage 15 / E52**	Mogen inschrijvers de demonstratieomgeving inrichten met de door Zaanstad beschikbaar gestelde conversiedata, mits deze veilig wordt behandeld en uitsluitend voor demonstratiedoeleinden wordt gebruikt?	Bijlage 15 bevat geen namen, personeelsnummers of andere direct identificerende persoonsgegevens. De in het tabblad Lidmaatschappen opgenomen gebruikerscodes zijn gepseudonimiseerd; zij zijn voor Inschrijver niet herleidbaar tot natuurlijke personen. Inschrijvers mogen deze gegevens gebruiken voor het inrichten van hun demonstratieomgeving, mits zij deze zorgvuldig en beveiligd behandelen, uitsluitend voor het doel van deze aanbesteding gebruiken en na afronding van de procedure verwijderen.
130	**§2.2 / §4.2.4**	Kunt u bevestigen dat de on-premise variant alleen aantoonbaar beschikbaar hoeft te zijn op het moment van inschrijving (bijvoorbeeld via architectuur- en productdocumentatie) en geen operationele, in gebruik zijnde referentie-installatie hoeft te zijn?	Ja, Opdrachtgever bevestigt dat voor de On-Premise-variant geen operationele, in gebruik zijnde referentie-installatie hoeft te worden aangetoond. De On-Premise-variant dient wel als aangeboden leveringsmodel beschikbaar te zijn en op het moment van inschrijving aantoonbaar te kunnen worden gemaakt, bijvoorbeeld aan de hand van architectuur- en productdocumentatie.
131	**PvE / Bijlage 13 Functioneel Ontwerp**	Kunt u bevestigen of Gov4Gem gedurende de gehele implementatiefase de leidende procesrolstructuur blijft, of dat tijdens het project een migratie naar een nieuwe structuur vereist is?	Ja. Opdrachtgever bevestigt dat de Gov4Gem-procesrolstructuur gedurende de gehele implementatiefase de leidende procesrolstructuur blijft. Een migratie naar een andere procesrolstructuur maakt geen onderdeel uit van de implementatie.
132	**§6.4 Proof of Concept**	Kunt u de objectieve acceptatiecriteria voor de Proof of Concept beschrijven en aangeven hoe wordt bepaald of de PoC succesvol is afgerond?	Zie hiervoor het antwoord op vraag 206.
133	**§5.3.1 / Bijlage 12**	In hoeverre mogen inschrijvers tijdens de demonstratie aanvullende functionaliteit of alternatieve processtappen laten zien, mits de gevraagde functionaliteit wordt onderbouwd en de vereiste scenario's volledig worden doorlopen?	Ja, dat is toegestaan. Inschrijvers mogen tijdens de demonstratie aanvullende functionaliteit of alternatieve processtappen tonen, mits de in Bijlage 12. Demonstratiescript opgenomen scenario's volledig binnen de daarvoor beschikbare tijd worden doorlopen. De beoordeling vindt uitsluitend plaats op basis van de in het Demonstratiescript en de gunningscriteria opgenomen onderdelen. Aanvullend getoonde functionaliteit wordt niet afzonderlijk gewaardeerd en leidt dus niet tot een hogere score.

Nr.	Onderwerp	Vraag	Antwoord
134	**Begrippenlijst / PvE scope**	Klopt de aanname dat alle partnerorganisaties tijdens de initiële implementatie moeten zijn aangesloten, of staat Zaanstad ook een gefaseerde aanpak toe waarbij partnerorganisaties na go-live worden aangesloten?	Aanname klopt, alle partnerorganisaties moeten bij de initiële implementatie zijn aangesloten. Een gefaseerde aansluiting van partnerorganisaties na go-live is niet toegestaan. Zie ook antwoord op vraag 60.
135	**aanbestedingskenmerk**	Het aanbestedingskenmerk verschilt tussen de documenten: de Offerteleidraad vermeldt “2026-198”, terwijl het Programma van Eisen en Wensen, het Functioneel Ontwerp en het Marktconsultatieverslag “2025-198” vermelden. Welk kenmerk is leidend?	Dank voor uw oplettendheid. Zie antwoord op vraag 14.
136	**Kwaliteitsborging**	De Offerteleidraad (§4.2.4) stelt dat de Hostingpartij moet voldoen aan ISO 27017- en ISO 27018-certificeringen. Kan Opdrachtgever bevestigen dat een geldige SOC 2 Type II-rapportage als gelijkwaardig alternatief voor ISO 27017 en ISO 27018 wordt geaccepteerd, mits aantoonbaar is dat de voor deze opdracht relevante beheersmaatregelen op het gebied van cloudbeveiliging en bescherming van persoonsgegevens binnen de scope van de SOC 2-rapportage vallen?	Nee. Een SOC 2 Type II-rapportage wordt niet geaccepteerd als vervanging van de ISO 27017- en ISO 27018-certificeringen van de cloudleverancier of hostingpartij. Deze normen en een SOC 2-rapportage dienen een verschillend doel. ISO 27017 en ISO 27018 leggen een genormeerd stelsel van beheersmaatregelen voor respectievelijk cloudbeveiliging en de bescherming van persoonsgegevens in de cloud vast, waarvan de naleving door een geaccrediteerde instelling wordt getoetst. De scope van een SOC 2-rapportage wordt daarentegen per opdracht bepaald en is niet genormeerd, waardoor Opdrachtgever de dekking niet objectief kan vergelijken. Conform paragraaf 4.2.4 wordt een gelijkwaardig certificaat van een in een andere EU-lidstaat gevestigde geaccrediteerde instelling wel geaccepteerd, mits Inschrijver de gelijkwaardigheid aantoont. Zie ook het antwoord op vraag 36.
137	**Normenkader**	De Offerteleidraad (§2.1) noemt als kader “BIO”, terwijl het PvE&W (E3, E33) “BIO2” hanteert. Aangezien BIO2 sinds 1 januari 2026 van kracht is, kunt u bevestigen dat BIO2 (gebaseerd op ISO 27001:2023 / 27002:2022) het leidende kader is?	Ja, dat kunnen wij bevestigen. Waar in de aanbestedingsdocumenten wordt verwezen naar de BIO, wordt de op dat moment geldende versie bedoeld. Voor deze aanbesteding is dat BIO2. De verwijzing naar “BIO” in de Offerteleidraad en naar “BIO2” in het Programma van Eisen en Wensen heeft derhalve dezelfde strekking. Inschrijvers dienen uit te gaan van naleving van de actuele versie van de BIO, zijnde BIO2.
138	**Referentie**	Voor kerncompetentie 1 (een IAM-systeem voor minimaal 1.000 identiteiten bij een gemeente, gemeenschappelijke regeling of vergelijkbare (semi)publieke organisatie, inclusief SSO): telt een referentie bij een (semi)publieke organisatie die geen gemeente is volwaardig mee, en mag deze referentie worden ingebracht door een combinatie lid of door de als onderaannemer opgegeven softwareleverancier?	Op uw beide deelvragen. Een referentie bij een (semi)publieke organisatie die geen gemeente is telt volwaardig mee, mits deze vergelijkbaar is met een gemeente of gemeenschappelijke regeling en aan de overige voorwaarden van kerncompetentie 1 wordt voldaan. Zie ook het antwoord op vraag 121. De referentie mag worden ingebracht door een combinant of door een derde op wiens technische bekwaamheid Inschrijver zich beroept, waaronder de als onderaannemer opgegeven softwareleverancier. In dat geval gelden de voorwaarden van paragraaf 3.10 tot en met 3.12 van de Offerteleidraad: de betreffende partij dient een eigen UEA in te dienen en bij een beroep op de bekwaamheid van een derde dient Bijlage 16. Ter beschikking-verklaring derde te worden overgelegd. Zie ook het antwoord op vraag 210.

Nr.	Onderwerp	Vraag	Antwoord
139	**Assurance**	De kwaliteitsborging (par. 4.2.4) vereist van de softwareleverancier een SOC 2 Type II-rapportage (ISAE 3000), niet ouder dan 12 maanden, naast een ISO 27001-certificaat. Wordt een ISAE 3402 Type II-rapportage als gelijkwaardig geaccepteerd, en hoe beoordeelt u “gelijkwaardige” assurance indien een leverancier nog geen SOC 2 Type II heeft maar wel een gelijkwaardig rapport of een aantoonbaar lopend certificeringstraject? Wij nemen tevens aan dat met de “Register EPD-Auditor” in eis E32 een Register EDP-Auditor (RE) wordt bedoeld, conform par. 4.2.4; kunt u dit bevestigen?	Opdrachtgever beantwoordt uw vragen per onderdeel. Een ISAE 3402 Type II-rapportage wordt onder voorwaarden als gelijkwaardig geaccepteerd. Zie hiervoor het antwoord op vraag 23, waarin Opdrachtgever tevens een alternatieve route beschrijft voor partijen die nog niet over een SOC 2 Type II-rapportage beschikken. Een aantoonbaar lopend certificeringstraject volstaat niet. De gevraagde assuranceverklaring dient bij Inschrijving te worden overgelegd en mag op de sluitingsdatum van de Inschrijving niet ouder zijn dan 12 maanden. Zie ook het antwoord op vraag 104. Uw aanname is juist: in eis E32 is met "Register EPD-Auditor" een Register EDP-Auditor (RE) bedoeld, conform paragraaf 4.2.4 van de Offerteleidraad. Deze verschrijving wordt in het Programma van Eisen en Wensen gecorrigeerd.
140	**Prijs**	Voor G1.1 gelden een prijsdrempel (€ 350.000) én een prijsplafond (€ 735.000), waarbij een inschrijfsom lager dan de drempel of hoger dan het plafond tot uitsluiting leidt. Kunt u exact definiëren welke posten in de “inschrijfsom” vallen (de eenmalige implementatiekosten A plus de jaarlijkse all-in kosten over 6 jaar B), en of de kosten voor het gebruik van de Oplossing gedurende het implementatiejaar meetellen in de inschrijfsom?	De inschrijfsom bestaat uit de eenmalige implementatiekosten (A) en de jaarlijkse all-in kosten over de initiële looptijd van zes jaar (B), zoals opgenomen in het Prijzenblad. De uurtarieven worden afzonderlijk beoordeeld onder G1.2 en maken geen deel uit van de inschrijfsom. De kosten voor het gebruik van de Oplossing gedurende de Implementatieperiode tellen niet afzonderlijk mee in de inschrijfsom. Artikel 11.2 van de concept Overeenkomst bepaalt dat gedurende de Implementatieperiode geen Gebruiksrechtenvergoeding verschuldigd is en dat deze kosten geacht worden begrepen te zijn in de Implementatievergoeding. Zij maken daarmee onderdeel uit van post A. Zie ook het antwoord op vraag 10. De zes jaarlijkse all-in kosten onder B betreffen de zes Gebruiksjaren van de initiële Gebruiksperiode, die aanvangt na Acceptatie.
141	**E-Mail**	Eis E38 verlangt de volledige set voor overheden verplichte e-mailstandaarden (SPF, DKIM, DMARC, DNSSEC, STARTTLS, DANE, IPv4/IPv6, HTTPS, HSTS), toetsbaar via internet.nl. Uit het Marktconsultatieverslag (vraag 21) en eis E28 blijkt een voorkeur voor e-mailverzending via de gemeentelijke mailinfrastructuur. Indien e-mail via de gemeentelijke mailomgeving wordt verzonden, liggen deze domein- en DNS-standaarden bij de gemeente; hoe wordt de naleving van E38 in dat scenario aan de Opdrachtnemer toegerekend?	Zie antwoord vraag 114.
142	**Redactioneel**	De eisen E33 en E34 lijken tekstueel onvolledig: E33 verwijst naar de NCSC “ICT-beveiligingsrichtlijnen voor webapplicaties” en E34 begint met “dan voldoet deze aantoonbaar aan de meest actuele OWASP-richtlijnen” zonder voorafgaande voorwaarde. Kunt u E33 en E34 verduidelijken — geldt E34 uitsluitend indien de Oplossing als SaaS wordt geleverd, en bevestigt u dat met de NCSC-richtlijn de meest actuele versie wordt bedoeld?	Ja. Voor E34 geldt de voorwaarde “Indien de Oplossing als SaaS wordt geleverd”. Deze voorwaarde dient aan het begin van E34 te worden gelezen. Zie ook het antwoord op vraag 4. Voor E33 dient onder de verwijzing naar de NCSC ICT-beveiligingsrichtlijnen voor webapplicaties de op het moment van uitvoering geldende, meest actuele versie van deze richtlijnen te worden verstaan.

Nr.	Onderwerp	Vraag	Antwoord
143	**Service Accounts**	Eis E40 vereist dat serviceaccounts voor koppelingen “uitsluitend via de IdP worden ingericht (bijvoorbeeld service principals)” en dat lokale accounts standaard zijn uitgeschakeld. De AD-koppeling (E28) is echter gespecificeerd als een “beveiligde LDAP(S)-verbinding met service account”, en E8 voorziet in wachtwoordresets in AD vanuit de Oplossing. Hoe verhoudt de eis “serviceaccounts uitsluitend via de IdP” zich tot een LDAP(S)-serviceaccount voor de koppeling met de on-premise Active Directory?	E40 ziet op de inrichting van accounts binnen de Oplossing. De eis dat serviceaccounts voor koppelingen via de IdP worden ingericht, is het uitgangspunt voor SaaS-leveringen. Voor een on-premise levering geldt hierop een uitzondering voor de in E28 vereiste beveiligde LDAP(S)-koppeling met Active Directory. Voor deze koppeling mag een specifiek technisch AD-serviceaccount worden gebruikt. Dit account dient uitsluitend voor de koppeling te worden gebruikt en mag niet over meer rechten beschikken dan noodzakelijk. Deze uitzondering geldt eveneens voor de functionaliteit uit E8 waarmee de Oplossing wachtwoordresets in Active Directory kan uitvoeren. Hiervoor mag het hiervoor bedoelde technische AD-serviceaccount worden gebruikt. Bij een SaaS-levering blijft het uitgangspunt van E40 onverkort van toepassing. De beoogde architectuur is daarbij gebaseerd op Microsoft Entra ID als koppellaag tussen de Oplossing en Active Directory (zie ook de antwoorden op vragen 82 en 147). Een rechtstreekse LDAP(S)-koppeling vanuit de SaaS-oplossing naar de on-premise Active Directory behoort daarbij niet tot de beoogde inrichting.
144	**Integratie**	Eis E24 verwijst naar een door de Opdrachtgever voorgeschreven ESB en/of API-gateway “zoals OpenTunnel”. Geldt het gebruik van OpenTunnel voor alle koppelingen of alleen voor specifieke doelsystemen, en kunt u de technische specificaties en randvoorwaarden van deze integratievoorziening verstrekken?	Zie antwoord op vraag 82.
145	**Toegangspas**	Toegangspassen en fysieke middelen zijn onderdeel van het IDU-proces (Functioneel Ontwerp figuur 4, de resource-definitie, eis E4 en wens W1-C, waarin blokkeren óók de toegangspas inactief zet), maar in de integratietabel (E28) is geen doelsysteem of koppeling voor een toegangspas-/pasjessysteem opgenomen. Via welk kanaal (bijvoorbeeld ticket-based via Topdesk of een afzonderlijke koppeling) verloopt de provisioning en blokkering van toegangspassen, en valt een dergelijke koppeling binnen de scope van deze aanbesteding?	Toegangspassen en overige fysieke middelen worden binnen de huidige scope verwerkt via het ticket-based proces. Toekenning, wijziging, blokkering en intrekking van toegangspassen verlopen via een door het IAM-systeem gegenereerde opdracht (ticket) aan de verantwoordelijke uitvoering. Een directe technische koppeling met een toegangspas- of pasjessysteem maakt geen onderdeel uit van de scope van deze aanbesteding.
146	**Offboarden**	Het offboarding-tijdschema van AD-accounts is niet eenduidig. E4 stelt dat het AD-account bij contractbeëindiging wordt gedeactiveerd en “na 30 dagen automatisch wordt verwijderd”, terwijl het Functioneel Ontwerp (bijlage 3) stelt dat accounts “4 dagen ná datum uitdienst disabled” worden en “1 maand ná uitdienst worden verwijderd”. Wat is het exacte, leidende tijdschema voor het moment van deactiveren en van verwijderen?	Leidend is: AD-account wordt gedeactiveerd (disabled): 4 dagen na de datum van uitdiensttreding. AD-account wordt verwijderd: 30 dagen na de datum van uitdiensttreding. Hiermee wordt de tekst in eis E4 verduidelijkt.

Nr.	Onderwerp	Vraag	Antwoord
147	**Entra ID**	De Begrippenlijst (Bijlage 2, §5 Provisioning) benoemt Active Directory én Microsoft Entra ID als “geautomatiseerde uitvoeringskanalen op basis van directe koppeling met het IAM-systeem”. Eis E20 noemt echter uitsluitend AD als geautomatiseerd doelsysteem, de Offerteleidraad noemt “Microsoft Entra ID voor SSO”, en W6-D behandelt Entra ID-provisioning als wens. Is geautomatiseerde provisioning naar Microsoft Entra ID een eis, uitsluitend bedoeld voor SSO, of een wens?	Verduidelijking E20 en E28 – provisioning en Microsoft Entra ID Opdrachtgever verduidelijkt dat zowel SSO via Microsoft Entra ID als geautomatiseerde provisioning onderdeel zijn van de vereiste functionaliteit. Hierbij is de wijze van koppeling afhankelijk van de gekozen leveringsvorm van de Oplossing. • SSO via Microsoft Entra ID is verplicht conform E28. • Geautomatiseerde provisioning naar Active Directory is verplicht conform E20: o Bij een on-premises IAM-oplossing vindt deze provisioning rechtstreeks plaats vanuit het IAM-systeem naar Active Directory. Active Directory wordt vervolgens gesynchroniseerd met Microsoft Entra ID en is verplicht conform E28. o Bij een SaaS-IAM-oplossing wordt Microsoft Entra ID als koppellaag tussen het IAM-systeem en Active Directory geplaatst. Dit is verplicht en een aanvulling op E28. De gewenste keten is dan: IAM → Microsoft Entra ID → Active Directory. Ook in deze situatie blijft geautomatiseerde provisioning naar Active Directory onderdeel van de vereiste functionaliteit. W6-D Integratie met Microsoft Entra ID betreft vervolgens een aanvullende wens. Deze wens gaat verder dan de hierboven beschreven verplichte basisfunctionaliteit. De gemeente wenst inzicht in de mogelijkheden om ook autorisaties en beheerhandelingen die momenteel rechtstreeks in Microsoft Entra ID plaatsvinden, en daarmee buiten de bestaande AD-synchronisatie vallen, verder te automatiseren en binnen de Oplossing te integreren.
148	**Encryptie/HS**	E41 spreekt van “FIPS 140-2 gecertificeerde HSM’s” en E45 van “FIPS 140-2 Level 3 gecertificeerde HSM’s”. Welk niveau is vereist? Zijn Customer Managed Keys (CMK) een harde eis of een wens, en geldt deze eis ook wanneer de SaaS wordt gehost op een hyperscaler (bijvoorbeeld Microsoft Azure of AWS)?	Zie antwoord vraag 5.
149	**Zero Knowledge**	Eis E41 verlangt een Zero Knowledge-model waarbij de Opdrachtnemer gevoelige gegevens niet kan ontsleutelen, “voor alle componenten waar dit technisch mogelijk is”, inclusief tenant-side encryptie en Customer Managed Keys. In het Marktconsultatieverslag (vraag 27) is echter vastgelegd dat “volledige zero-knowledge encryptie niet gangbaar wordt geacht binnen IGA-oplossingen, omdat het platform identiteitsgegevens moet kunnen verwerken voor functies zoals analyse, policy-evaluatie en provisioning”. Kunt u verduidelijken hoe E41 moet worden geïnterpreteerd, welke minimale invulling vereist is om aan de eis te voldoen, en of E41 een knock-out-eis is?	Zie antwoord vraag 5.

Nr.	Onderwerp	Vraag	Antwoord
150	**Prijs On-Premise**	De On-Premise jaarlijkse licentiekosten zijn vastgesteld op 80% van de SaaS-licentiekosten (par. 2.9 / 5.2.2). Voor veel leveranciers zijn de werkelijke kosten van een On-Premise-variant niet lager dan die van SaaS. Kunt u onderbouwen waarom een korting van 20% proportioneel is, en biedt het Prijzenblad ruimte om de On-Premise-prijs afzonderlijk en kostendekkend op te geven?	De verhouding van 80% is niet als korting bedoeld en is langs twee lijnen tot stand gekomen. De keuze voor een vast percentage in plaats van een vrij op te geven On-Premise-prijs dient de vergelijkbaarheid. Zoals toegelicht in paragraaf 5.2.2 van de Offerteleidraad is het zonder vast percentage niet mogelijk de prijzen van de verschillende inschrijvingen eerlijk en objectief met elkaar te vergelijken, omdat op het moment van Inschrijving nog niet vaststaat welk leveringsmodel wordt afgenomen en het zwaartepunt van de uitvraag bij SaaS ligt. De hoogte van het percentage is in de markt getoetst. Naar aanleiding van de marktconsultatie heeft Opdrachtgever de deelnemende partijen die zowel een SaaS- als een On-Premise-variant konden leveren aanvullend bevraagd over de kostenverhouding tussen beide leveringsmodellen. Het percentage van 80% is de uitkomst van die uitvraag. Opdrachtgever acht de verhouding op grond daarvan marktconform en voldoende ruim om rekening te houden met verschillen in kostenstructuur. Het Prijzenblad biedt geen ruimte om de On-Premise-prijs afzonderlijk op te geven. Inschrijver kan bij het bepalen van zijn SaaS-tarief rekening houden met zijn eigen kostenstructuur en met de mogelijkheid dat Opdrachtgever gedurende de looptijd tot een wijziging van het leveringsmodel besluit. Zie ook de antwoorden op de vragen 1, 2, 43 en 110.
151	**Leveringsmodel**	Een groot deel van de niet-functionele eisen (o.a. E30, E31, E35, E38–E42, E44–E46, E48, E50, E60) is geformuleerd als “indien de Oplossing als SaaS wordt geleverd”, terwijl de On-Premise-variant “ten minste aan alle als eis geformuleerde functionaliteit” moet voldoen. Betekent dit dat deze SaaS-gebonden eisen bij een On-Premise-levering niet van toepassing zijn, of verwacht u gelijkwaardige maatregelen? Hoe worden inschrijvingen op deze eisen beoordeeld, gegeven dat SaaS primair wordt uitgevraagd maar de On-Premise-variant verplicht moet worden aangeboden?	Indien bij een eis expliciet is opgenomen “indien de Oplossing als SaaS wordt geleverd”, is die eis of dat onderdeel van de eis uitsluitend van toepassing op de SaaS-variant. Voor een On-Premise-oplossing is die specifieke eis of dat onderdeel niet van toepassing. De On-Premise-variant dient wel te voldoen aan alle overige eisen die niet expliciet tot de SaaS-variant zijn beperkt. Bij de beoordeling van de Inschrijving wordt per leveringsmodel uitgegaan van de eisen die voor dat leveringsmodel van toepassing zijn. De verplichting om zowel een SaaS- als een On-Premise-variant aan te bieden blijft onverkort van kracht.
152	**Inrichting**	Bijlage 2 van het Functioneel Ontwerp (Identiteitscontainers) vermeldt dat deze “volgt en tijdens de PoC wordt verstrekt”. Aangezien de containerindeling bepalend is voor de inrichting, de scope en de prijs, kunt u de definitieve containerindeling reeds vóór de inschrijvingsdatum verstrekken?	Nee. De definitieve uitwerking van de identiteitscontainers wordt niet voorafgaand aan de inschrijvingsdatum verstrekt. De passage in Bijlage 13 dat de identiteitscontainers “tijdens de PoC worden verstrekt” betekent dat Opdrachtgever de benodigde informatie over de identiteitscontainers tijdens de PoC beschikbaar kan stellen. Indien dit voor de uitvoering van de PoC gewenst of noodzakelijk is, kunnen de identiteitscontainers en de daarvoor benodigde inrichting tijdens de PoC worden verstrekt of nader worden toegelicht. De definitieve indeling van de identiteitscontainers en de verdeling van de partnerorganisaties daarbinnen wordt tijdens de implementatie in overleg met Opdrachtnemer nader bepaald. Dit betreft een nadere concretisering binnen de beschreven scope en geen uitbreiding daarvan. De huidige inrichting bestaat uit een identiteitscontainer voor Gemeente Zaanstad en meerdere identiteitscontainers voor partnerorganisaties. Tot de partnerorganisaties

Nr.	Onderwerp	Vraag	Antwoord
			behoren momenteel onder andere Stichting Jeugdteam, Sociaal Wijkteam, Omgevingsdienst, Gemeente Oostzaan, Gemeente Wormerland en Pact Zaandam Oost. Naar verwachting worden Stichting Jeugdteam en Sociaal Wijkteam ieder in een afzonderlijke identiteitscontainer ondergebracht en worden de overige partnerorganisaties gezamenlijk in één identiteitscontainer ondergebracht. Dit geeft een indicatie van de omvang en aard van de benodigde inrichting. Opdrachtgever verwacht hierbij geen bijzondere complexiteit. De Oplossing dient de mogelijkheid te bieden om identiteitscontainers flexibel en beheersbaar in te richten en te beheren.
153	**Omvang**	De Offerteleidraad en het PvE&W gaan uit van circa 3.000 identiteiten (±20%), terwijl het Functioneel Ontwerp (§2) uitkomt op ca. 2.675 (ca. 2.250 Zaanstad + ca. 400 Jeugd-/Sociaal Wijkteams + 25 kleine partners). Kunt u bevestigen dat 3.000 de contractuele licentiegrondslag is en toelichten hoe dit aantal is opgebouwd (inclusief groeiruimte en toekomstige partnerorganisaties)? Kunt u tevens definiëren hoe een “inactieve identiteit”, die niet in rekening wordt gebracht, precies wordt bepaald en gemeten?	Opdrachtgever gaat uit van circa 3.000 actieve identiteiten als uitgangspunt voor de omvang van de Oplossing. Inschrijver dient rekening te houden met een bandbreedte van circa ±20% ten opzichte van dit aantal. Momenteel zijn ongeveer 2.800 identiteiten actief. De bandbreedte biedt ruimte voor de verwachte ontwikkeling van de organisatie, waaronder groei en krimp van Zaanstad en de aangesloten partnerorganisaties gedurende de contractperiode. Opdrachtgever verwacht gedurende de initiële contractperiode geen substantiële afwijkingen buiten deze bandbreedte. Onder een inactieve identiteit verstaat Opdrachtgever een identiteit die niet langer actief is en uitsluitend in de Oplossing wordt bewaard voor audit-, historie-, bewaartermijn- of eventuele herindiensttredingsdoeleinden. Een dergelijke identiteit heeft geen actieve relatie meer met Zaanstad of een aangesloten partnerorganisatie en wordt niet gebruikt voor actieve toegang of autorisatie. Een inactieve identiteit wordt niet als licentieerbare identiteit aangemerkt en telt daarom niet mee voor het aantal identiteiten waarvoor de licentieomvang wordt bepaald. De inactieve status dient binnen de Oplossing als zodanig herkenbaar en beheersbaar te zijn.
154	**Offerteleidraad – §6.4 Proof of Concept (PoC); §3.2 Planning / §3.8 Gestanddoeningstermijn**	Kunt u de planning van de Proof of Concept (PoC) met Leverancier I nader specificeren (duur, beoordelingscriteria en wat er gebeurt indien de PoC niet succesvol wordt afgerond)?	De Proof of Concept vindt plaats na de bezwaartermijn en neemt circa drie maanden in beslag, zoals toegelicht in paragraaf 3.8 en paragraaf 6.4 van de Offerteleidraad. Pas na een succesvol afgeronde PoC wordt de Overeenkomst gesloten. Voor de beoordelingscriteria en voor de gevolgen indien de PoC niet succesvol wordt afgerond, verwijst Opdrachtgever naar het antwoord op vraag 206. Indien de PoC met Leverancier I niet succesvol wordt afgerond, kan Opdrachtgever de Wachtkamerovereenkomst met Leverancier II activeren; zie paragraaf 6.3 van de Offerteleidraad en de antwoorden op de vragen 48 tot en met 52.
155	**Offerteleidraad – §2.2 Scope / definitions AD & Entra ID; related technical detail: Bijlage 13 Functioneel Ontwerp**	Kunt u voor de integratie met Microsoft Entra ID (par. D, PvE) aangeven welk deel van de circa 3.000 identiteiten/autorisaties momenteel rechtstreeks in Entra ID wordt beheerd, buiten de AD-synchronisatie om, en om welk aantal/type autorisaties het gaat?	Opdrachtgever kan aangeven dat op dit moment circa 35-45 identiteiten rechtstreeks in Microsoft Entra ID worden beheerd, buiten de IAM-AD-synchronisatie om. Het betreft een beperkte groep identiteiten waarvoor beheer momenteel niet via de reguliere IAM-processen verloopt. Opdrachtgever verwacht dat deze omvang beperkt blijft ten opzichte van het totale aantal identiteiten. Deze identiteiten maken geen gebruik van de standaard autorisatiestructuur en beschikken over specifieke middelen en bijbehorende autorisaties.

Nr.	Onderwerp	Vraag	Antwoord
156	**Offerteleidraad – §2.2 Scope (integrations); Bijlage 13 Functioneel Ontwerp – Bijlagen 3–5 (AD, YouForce, Topdesk)**	Kunt u aangeven voor welke integraties (YouForce, AD, Topdesk, e-mail, datapakhuis, Entra ID) reeds bestaande en gedocumenteerde API's/interfaces beschikbaar zijn en of de technische specificaties hiervan aan inschrijvers worden verstrekt?	De beschikbare integraties en interfaces zijn beschreven in Bijlage 13 – IAM-systeem Zaanstad - Functioneel Ontwerp.pdf. Hierin zijn onder meer de integraties met Active Directory (bijlage 3), YouForce (bijlage 4) en TOPdesk (bijlage 5) uitgewerkt. Voor YouForce betreft de huidige koppeling geen API-koppeling, maar een bestandsuitwisseling op basis van BINT-bestanden. Voor de wijze waarop de toekomstige koppeling met YouForce wordt gerealiseerd en de voorwaarden waaronder een beschikbare IAM-API van YouForce dient te worden gebruikt, wordt verwezen naar het antwoord op vraag 82. Voorbeeldbestanden zijn via de Nota van Inlichtingen beschikbaar gesteld, zie bijlage 17. Voor Microsoft Entra ID, Active Directory en TOPdesk gaat Opdrachtgever uit van gangbare, gedocumenteerde integratiemogelijkheden die door IAM-oplossingen worden ondersteund. Voor e-mail en het datapakhuis zijn de relevante functionele en technische uitgangspunten beschreven in de aanbestedingsdocumenten. Voor e-mail is de wijze van integratie nader verduidelijkt in het antwoord op vraag 114.
157	**Bijlage 13 Functioneel Ontwerp – §5 Conversie; also Bijlage 12 Demonstratiescript / Bijlage 15 Conversiedata**	Is de huidige autorisatiestructuur in G4Gem (bron voor de migratie) beschikbaar als voorbeeldexport/datamodel voor inschrijvers, zodat de migratieaanpak nader kan worden onderbouwd?	Inschrijvers kunnen de opbouw van de huidige autorisatiestructuur en de migratie-uitgangspunten afleiden uit de beschikbaar gestelde conversiedata in bijlage 15.
158	**Offerteleidraad – §2.2 Scope van de Opdracht (SaaS én On-Premise mogelijk); §2.9 Herzieningsclausule**	De Offerteleidraad vereist dat iedere inschrijver zowel een SaaS- als een On-Premise-leveringsmodel aanbiedt. Geldt dit ook voor oplossingen die primair cloud-native zijn en geen aparte 'On-Premise'-variant als product aanbieden (bijvoorbeeld private cloud/dedicated hosting als alternatief) — wordt een dergelijke variant geaccepteerd om aan de On-Premise-eis te voldoen?	Nee. Een door Opdrachtnemer gehoste private cloud- of dedicated-hostingomgeving geldt binnen deze aanbesteding als SaaS en niet als On-Premise, ongeacht of deze omgeving single-tenant of specifiek voor Opdrachtgever ingericht is. Onder de On-Premise-variant verstaat Opdrachtgever een implementatie waarbij de infrastructuur onder direct beheer en directe zeggenschap van Opdrachtgever staat. Inschrijver dient daarom zowel een SaaS-variant als een On-Premise-variant aan te bieden die aan de daarvoor geldende eisen voldoet. Een oplossing die uitsluitend als cloud-native SaaS, private cloud of dedicated hosting kan worden geleverd, zonder dat deze ook binnen infrastructuur onder direct beheer en directe zeggenschap van Opdrachtgever kan worden geleverd, voldoet niet aan deze verplichting.
159	**Offerteleidraad – §2.9 Herzieningsclausule; §5.2 G1 Prijs (On-Premise variant)**	Voor de On-Premise-licentiekosten (80% van de SaaS-licentiekosten, PvE par. 2.9/5.2 Offerteleidraad): omvat dit percentage ook hosting-, beheer- en onderhoudskosten, of uitsluitend de licentiecomponent?	Het percentage van 80% ziet op de volledige jaarlijkse vergoeding voor de On-Premise-variant en niet uitsluitend op een licentiecomponent. Binnen die vergoeding dient dezelfde dienstverlening te worden geleverd als binnen de SaaS-vergoeding, met uitzondering van de hosting en de daarmee samenhangende infrastructurele werkzaamheden die bij een On-Premise-levering door Opdrachtgever worden verzorgd. Inbegrepen zijn in ieder geval het gebruiksrecht, het reguliere onderhoud inclusief Updates, patches en beveiligingsupdates, en de tweede- en derdelijns ondersteuning conform de eisen E49, E54, E57 en E61.

Nr.	Onderwerp	Vraag	Antwoord
			Zie ook de antwoorden op de vragen 150 en 174.
160	**Offerteleidraad – §2.9 Herzieningsclausule; §5.2 G1 Prijs (On-Premise variant)**	Voor de On-Premise-licentiekosten (80% van de SaaS-licentiekosten, PvE par. 2.9/5.2 Offerteleidraad): omvat dit percentage ook hosting-, beheer- en onderhoudskosten, of uitsluitend de licentiecomponent?	Zie hiervoor het antwoord op vraag 159.
161	**Concept Overeenkomst – art. 7.4 (as cited in the question); Offerteleidraad – §2.9 Herzieningsclausule / §5.2**	In geval van een latere overstap van On-Premise naar SaaS (art. 7.4 Overeenkomst): op basis van welk prijsniveau worden de dan geldende SaaS-prijzen bepaald — het oorspronkelijke Prijzenblad, geïndexeerd, of op basis van een nieuwe prijsopgave?	Bij een wijziging van On-Premise naar SaaS gelden de in het Prijzenblad opgegeven SaaS-prijzen, zoals geïndexeerd overeenkomstig de Overeenkomst. Dit volgt uit artikel 7.3 van de concept Overeenkomst en uit paragraaf 2.9 van de Offerteleidraad. Er vindt geen nieuwe prijsopgave plaats. De migratie- en transitiewerkzaamheden die met de wijziging samenhangen worden uitgevoerd tegen de in het Prijzenblad opgenomen uurtarieven, op basis van een door Opdrachtnemer op te stellen en door Opdrachtgever goed te keuren migratieplan (artikel 7.4). Zie ook het antwoord op vraag 175.
162	**Offerteleidraad – §5.2.1 G1.1 Inschrijfsom; Prijzenblad (Bijlage 3)**	Kunt u bevestigen of de prijsdrempel (€350.000) en het prijsplafond (€735.000) voor de totale inschrijfsom gelden voor zowel de SaaS- als de On-Premise-aanbieding, aangezien in het Prijzenblad slechts één prijs (SaaS) wordt uitgevraagd?	Ja. De prijsdrempel van € 350.000 en het prijsplafond van € 735.000 gelden voor de inschrijfsom zoals die op basis van het Prijzenblad wordt berekend. Aangezien het Prijzenblad uitsluitend de SaaS-prijzen uitvraagt, wordt de inschrijfsom op basis van die prijzen bepaald en beoordeeld. Er wordt geen afzonderlijke inschrijfsom voor de On-Premise-variant berekend of getoetst. De On-Premise-vergoeding wordt afgeleid van de SaaS-vergoeding conform de systematiek van artikel 7.3 van de concept Overeenkomst. Zie ook de antwoorden op de vragen 140 en 150.
163	**Offerteleidraad – §5.2.2 G1.2 Uurtarieven; Prijzenblad (Bijlage 3)**	Voor de fictieve uren (2x 500 uur, projectleider en technisch consultant): zijn dit realistische ramingen van het verwachte volume aan aanvullende werkzaamheden, of uitsluitend een vergelijkingsmechanisme zonder relatie tot de daadwerkelijk verwachte opdracht?	De in het Prijzenblad opgenomen uren zijn fictief en dienen uitsluitend als vergelijkingsmechanisme voor de beoordeling van de uurtarieven onder G1.2. Dit is expliciet vermeld in paragraaf 5.2.2 van de Offerteleidraad. Aan deze uren kunnen geen rechten worden ontleend. Zij vormen geen raming van het verwachte volume aan aanvullende werkzaamheden en geen afnameverplichting.
164	**Offerteleidraad – §4.2.2 Technische bekwaamheid en beroepsbekwaamheid, Kerncompetentie 1**	De kerncompetentie-eis vraagt om een referentie bij ‘een gemeente of gemeenschappelijke regeling’ met minimaal 1.000 beheerde identiteiten — geldt een vergelijkbare publieke organisatie (bijvoorbeeld provincie, waterschap of ZBO) eveneens als geldige referentie, of is dit strikt beperkt tot gemeenten/GR’s?	Een vergelijkbare (semi)publieke organisatie, waaronder een provincie, waterschap of zelfstandig bestuursorgaan, kwalificeert als geldige referentie. Opdrachtgever wijst erop dat de kerncompetentie in paragraaf 4.2.2 van de Offerteleidraad reeds spreekt van een gemeente, een gemeenschappelijke regeling of een vergelijkbare (semi)publieke organisatie. Bijlage 4. Referentieformulier wordt hierop aangepast. Zie de antwoorden op de vragen 13 en 121.
165	**Offerteleidraad – §4.2.2 Technische bekwaamheid en beroepsbekwaamheid; Referentieformulier (Bijlage 4)**	Hoeveel referenties moeten worden ingediend (het Referentieformulier toont er één, maar er wordt niet expliciet aangegeven of dit tevens het minimum of maximum is)?	Er dient één referentie te worden ingediend waarmee kerncompetentie 1 wordt aangetoond. Eén referentie is daarmee zowel het minimum als het maximum. Indien Inschrijver meerdere referenties indient, beoordeelt Opdrachtgever uitsluitend de eerst ingediende referentie.

Nr.	Onderwerp	Vraag	Antwoord
166	**Offerteleidraad – Leveren, implementeren en onderhouden van een Identity and Access Management-systeem – §2.6 Omvang van de Opdracht**	Kan Opdrachtgever aangeven hoeveel van de circa 3.000 identiteiten momenteel actief respectievelijk inactief zijn en wat de verwachte ontwikkeling van het aantal actieve identiteiten gedurende de initiële contractperiode is?	Opdrachtgever gaat uit van circa 2.800 actieve identiteiten. Het exacte aantal inactieve identiteiten is op dit moment niet afzonderlijk vastgesteld. Voor de omvang van de Oplossing dient Inschrijver uit te gaan van circa 3.000 actieve identiteiten, met een bandbreedte van circa ±20%. Deze bandbreedte biedt ruimte voor de verwachte ontwikkeling van de organisatie, waaronder groei en krimp van de eigen organisatie en deelnemende partnerorganisaties gedurende de contractperiode. Opdrachtgever verwacht gedurende de initiële contractperiode geen substantiële afwijkingen buiten deze bandbreedte. Zie ook het antwoord op vraag 153.
167	**Offerteleidraad – Leveren, implementeren en onderhouden van een Identity and Access Management-systeem – §2.6 Omvang van de Opdracht / §2.9 Herzieningsclausule**	Welke commerciële prijssystematiek geldt wanneer het aantal actieve identiteiten gedurende de looptijd boven de genoemde bandbreedte van +20% uitkomt? Mag hiervoor een aanvullende prijs worden overeengekomen?	Paragraaf 2.9 van de Offerteleidraad voorziet hierin. Indien het aantal actieve identiteiten de bovengrens van de bandbreedte structureel overschrijdt, dat wil zeggen gedurende een aaneengesloten periode van drie maanden, treden Partijen in overleg over aanpassing van de prijs. De op dat moment geldende jaarlijkse prijs voor 3.000 identiteiten, inclusief indexering conform de Overeenkomst, dient daarbij als basis voor de nieuw overeen te komen prijs. Er mag dus een aanvullende prijs worden overeengekomen, maar deze wordt afgeleid van de reeds overeengekomen prijssystematiek en niet vrij bepaald. Inactieve identiteiten tellen niet mee bij de bepaling van de bandbreedte. Zie het antwoord op vraag 153.
168	**Concept Overeenkomst + Offerteleidraad – Concept Overeenkomst art. 5.3–5.4; Offerteleidraad §2.9**	Indien de implementatieperiode of go-live door oorzaken aan de zijde van Opdrachtgever wordt uitgesteld, kunnen aantoonbare aanvullende kosten voor bijvoorbeeld gereserveerde capaciteit, projectmanagement en technische resources als meerwerk worden vergoed?	Ja, voor zover het uitstel aantoonbaar aan Opdrachtgever is toe te rekenen en daardoor redelijkerwijs niet voorziene aanvullende kosten voor Opdrachtnemer ontstaan. Het gaat daarbij uitsluitend om aantoonbare en redelijkerwijs noodzakelijke extra kosten die rechtstreeks het gevolg zijn van het uitstel, bijvoorbeeld voor het opnieuw reserveren van capaciteit of aanvullende projectmanagement- en technische inzet. Opdrachtnemer dient dergelijke kosten tijdig te melden en voorafgaand aan de uitvoering van de betreffende aanvullende werkzaamheden ter goedkeuring aan Opdrachtgever voor te leggen. Kosten die behoren tot de reguliere uitvoering van de opdracht of die het gevolg zijn van onvoldoende tijdige planning of inzet door Opdrachtnemer komen niet voor vergoeding als meerwerk in aanmerking. De eventuele vergoeding wordt vastgesteld op basis van de in het Prijzenblad opgenomen tarieven en de bepalingen inzake meerwerk uit de overeenkomst.
169	**Concept Overeenkomst / Plan van Aanpak requirements – Concept Overeenkomst art. 5 and 8; implementation requirements**	Welke concrete capaciteit en beschikbaarheid stelt Opdrachtgever beschikbaar tijdens de implementatie voor projectmanagement, functioneel beheer, architectuur, security, testen, acceptatie en integraties, en wat zijn de commerciële gevolgen wanneer deze capaciteit niet tijdig beschikbaar is?	Opdrachtgever stelt gedurende de implementatie de voor een succesvolle uitvoering benodigde capaciteit beschikbaar, waaronder projectmanagement, functioneel beheer, technische beheerders, architectuur, security, P&O/HR, proceseigenaren en capaciteit voor testen en acceptatie. De benodigde inzet wordt afgestemd op de overeengekomen projectplanning en de door Opdrachtnemer tijdig kenbaar gemaakte concrete behoefte. Op voorhand kan geen generieke uren- of capaciteitsindicatie worden gegeven, omdat de benodigde inzet mede afhankelijk is van de aangeboden Oplossing, implementatieaanpak en fasering. Partijen maken hierover tijdens de implementatie nadere afspraken.

Nr.	Onderwerp	Vraag	Antwoord
			Opdrachtgever verwacht dat de benodigde capaciteit binnen de overeengekomen planning beschikbaar wordt gesteld. Indien Opdrachtgever aantoonbaar in gebreke blijft met het tijdig beschikbaar stellen van overeengekomen capaciteit en dit aantoonbaar leidt tot vertraging of aanvullende kosten voor Opdrachtnemer, worden de gevolgen daarvan door partijen besproken en kunnen hierover nadere afspraken worden gemaakt.
170	**Offerteleidraad + Functioneel Ontwerp / Programma van Eisen en Wensen – Implementation scope – conversion and initial setup**	Kan Opdrachtgever kwantificeren hoeveel autorisaties, procesrollen, HR-attributen, mappings en overige configuratieobjecten uit de huidige IAM-omgeving moeten worden gemigreerd of opnieuw opgebouwd?	Inschrijvers kunnen de aantallen autorisaties en procesrollen voor een belangrijk deel afleiden uit de beschikbaar gestelde conversiedata in Bijlage 15. Niet alle HR-attributen, mappings, business rules en overige configuratieobjecten zijn daarin afzonderlijk gekwantificeerd. De conversiedata en het Functioneel Ontwerp vormen samen de basis voor het maken van een reële inschatting van de migratie- en implementatieopgave. Aanvullende informatie die bij Opdrachtgever beschikbaar is en die nodig is voor de uitvoering van de migratie en implementatie, wordt tijdens de implementatie met Opdrachtnemer gedeeld. Zie ook het antwoord op vraag 201.
171	**Offerteleidraad – §2.2 Scope – integrations (YouForce, AD, TOPdesk, e-mail, data warehouse, Entra ID)**	Kan Opdrachtgever per integratie aangeven welke partij verantwoordelijk is voor ontwikkeling/configuratie aan de zijde van het doelsysteem en bevestigen of eventuele kosten van derde leveranciers voor rekening van Opdrachtgever komen?	De realisatie van koppelingen betreft een gezamenlijke inspanning van Opdrachtgever, Opdrachtnemer en waar van toepassing leveranciers van bron- en doelsystemen. De exacte taakverdeling wordt per koppeling vastgesteld tijdens de implementatiefase. Opdrachtnemer is verantwoordelijk voor de werkzaamheden aan de zijde van de aangeboden IAM-oplossing. Voor werkzaamheden aan de zijde van bron- en doelsystemen zijn respectievelijk de betreffende systeemeigenaren en/of leveranciers verantwoordelijk. Eventuele kosten van derden, waaronder leveranciers van bron- en doelsystemen, maken geen onderdeel uit van de verantwoordelijkheid van Opdrachtnemer en komen voor rekening van Opdrachtgever, tenzij Inschrijver deze werkzaamheden expliciet als onderdeel van zijn aanbieding aanbiedt.
172	**Offerteleidraad – §2.3 Optionele werkzaamheden / §5.2.2 Koppelingen**	Kan worden bevestigd dat wijzigingen of uitbreidingen van bestaande koppelingen die ontstaan door wijzigingen in systemen van Opdrachtgever als meerwerk worden beschouwd indien deze niet het gevolg zijn van een tekortkoming van Opdrachtnemer?	Ja, mits de wijziging niet het gevolg is van een tekortkoming van Opdrachtnemer en niet voortvloeit uit door Opdrachtnemer aangebrachte updates, upgrades of wijzigingen aan de Oplossing. In dat geval behoort de aanpassing tot de verantwoordelijkheid van Opdrachtnemer. Eventueel meerwerk wordt per situatie beoordeeld.
173	**Programma van Eisen en Wensen + Concept Overeenkomst – PvE E54; Concept Overeenkomst art. 10**	Kan Opdrachtgever nader afbakenen welke wijzigingen onder inbegrepen adaptief onderhoud vallen en vanaf welk moment sprake is van consultancy/meerwerk dat separaat mag worden gefactureerd?	Onder adaptief onderhoud verstaat Opdrachtgever aanpassingen die noodzakelijk zijn om de Oplossing blijvend te laten voldoen aan geldende wet- en regelgeving, beveiligingsrichtlijnen, ondersteunde standaarden en wijzigingen in de onderliggende technologie, infrastructuur, hostingvoorzieningen of platformen. Adaptief onderhoud ziet op het in stand houden van de bestaande functionaliteit en werking van de Oplossing. Verbeteringen en verdere ontwikkelingen van de standaardfunctionaliteit die Opdrachtnemer generiek aan zijn klanten beschikbaar stelt, vallen onder doorontwikkeling en maken onderdeel uit van de overeengekomen dienstverlening. Specifiek voor Opdrachtgever ontwikkelde functionaliteit of werkzaamheden die buiten de reguliere dienstverlening vallen, kunnen afzonderlijk worden overeengekomen en worden uitgevoerd tegen de in het Prijzenblad opgenomen uurtarieven, na voorafgaande schriftelijke opdracht conform paragraaf 2.3 van de Offerteleidraad. Zie

Nr.	Onderwerp	Vraag	Antwoord
			ook de antwoorden op de vragen 172 en 199. Upgrades worden op grond van artikel 10.2 van de concept Overeenkomst tegen vergoeding uitgevoerd, na voorafgaande schriftelijke opdracht. Zie ook het antwoord op vraag 11. De praktische uitwerking van de afbakening wordt vastgelegd in het Document Afspraken en Procedures (DAP) als bedoeld in eis E59. Die uitwerking laat de in de Overeenkomst en het Programma van Eisen en Wensen vastgelegde afbakening onverlet.
174	**Concept Overeenkomst + Offerteleidraad – Concept Overeenkomst art. 7.3–7.5; Offerteleidraad §2.9 / G1 pricing**	Kan Opdrachtgever bevestigen welke dienstverlening, onderhoud en support precies binnen de 80% On-Premise licentieprijs moeten worden geleverd en welke werkzaamheden/diensten separaat mogen worden gefactureerd?	Binnen de jaarlijkse On-Premise-vergoeding van 80% dient dezelfde dienstverlening te worden geleverd als binnen de SaaS-vergoeding, met uitzondering van de hosting en de daarmee samenhangende infrastructurele werkzaamheden die bij een On-Premise-levering door Opdrachtgever worden verzorgd. Inbegrepen zijn in ieder geval: het gebruiksrecht, het reguliere onderhoud inclusief Updates, patches en beveiligingsupdates, en de tweede- en derdelijns ondersteuning conform de eisen E49, E54, E57 en E61. Afzonderlijk factureerbaar zijn: Upgrades conform artikel 10.2 van de concept Overeenkomst, en meerwerk en consultancy conform paragraaf 2.3 van de Offerteleidraad. Zie ook de antwoorden op de vragen 110 en 173.
175	**Concept Overeenkomst – Art. 7.4 Wijziging leveringsmodel**	Kan worden bevestigd dat alle migratie-, projectmanagement-, consultancy- en technische werkzaamheden die noodzakelijk zijn voor een wijziging van het leveringsmodel tussen SaaS en On-Premise aanvullend factureerbaar zijn tegen de tarieven uit het Prijzenblad?	Ja, dit kan worden bevestigd. Artikel 7.4 van de concept Overeenkomst bepaalt dat de migratie- en transitiewerkzaamheden die samenhangen met een wijziging van het leveringsmodel worden uitgevoerd tegen de in het Prijzenblad opgenomen uurtarieven. Voorwaarde is dat Opdrachtnemer daarvoor een migratieplan opstelt dat door Opdrachtgever wordt goedgekeurd. Opdrachtnemer draagt daarbij zorg voor een volledige en gecontroleerde overdracht van data, configuraties en inrichting, waarbij de kernfunctionaliteit volledig behouden blijft. Zie ook het antwoord op vraag 161.
176	**Concept Overeenkomst – Art. 7.3 and art. 15.5; also GIBIT 2025 as applicable conditions**	Kan Opdrachtgever verduidelijken welke indexeringsmethodiek gedurende de volledige looptijd van de Overeenkomst van toepassing is op de gebruiksrechtenvergoeding, onderhoud/support en de aangeboden uurtarieven, inclusief de toepasselijke index, peildatum, eerste indexatiemoment, indexatiefrequentie en eventuele maximale jaarlijkse indexering?	Zie hiervoor het antwoord op vraag 81.
177	**Offerteleidraad – §2.6 Omvang van de Opdracht / contract value estimate**	Kan Opdrachtgever aangeven of gedurende de initiële contractperiode sprake is van een minimale gegarandeerde afname of contractwaarde voor licenties en dienstverlening?	Er is geen gegarandeerde minimumafname in de vorm van een contractwaarde. Wel geldt dat Opdrachtgever uitgaat van circa 3.000 actieve identiteiten met een bandbreedte van circa 20% meer of minder, zoals opgenomen in paragraaf 2.6 en 2.9 van de Offerteleidraad. De ondergrens van die bandbreedte vormt daarmee het feitelijke uitgangspunt voor de afname gedurende de initiële contractperiode. Inactieve identiteiten worden niet in rekening gebracht en tellen niet mee bij de bepaling van de bandbreedte. Zie ook de antwoorden op de vragen 153 en 167.

Nr.	Onderwerp	Vraag	Antwoord
			De in paragraaf 2.6 opgenomen raming van de opdrachtwaarde is een inschatting waaraan geen rechten kunnen worden ontleend.
178	**Offerteleidraad – PoC / award procedure and §2.9 wait-list agreement**	Zijn alle kosten die de voorkeursleverancier maakt voor de Proof of Concept voor rekening van de leverancier, of mogen (delen van) deze werkzaamheden na een succesvolle PoC onderdeel vormen van de implementatievergoeding?	De kosten die de beoogd Opdrachtnemer maakt voor de Proof of Concept komen voor zijn eigen rekening. Paragraaf 3.17 van de Offerteleidraad sluit een kostenvergoeding voor de aanbestedingsprocedure uit. Na een succesvol afgeronde PoC en het sluiten van de Overeenkomst kunnen de tijdens de PoC verrichte inrichtingswerkzaamheden wel worden voortgezet en benut binnen de implementatie, zodat deze inspanning niet verloren gaat. Deze werkzaamheden worden geacht begrepen te zijn in de bij Inschrijving opgegeven Implementatievergoeding en leiden niet tot een aanvullende vergoeding. Zie ook het antwoord op vraag 184.
179	**Offerteleidraad – §2.9 Herzieningsclausule – wachtkamerovereenkomst / Proof of Concept**	Welke objectieve acceptatiecriteria bepalen of de Proof of Concept succesvol is en krijgt Opdrachtnemer gelegenheid om tijdens de PoC geconstateerde tekortkomingen binnen een redelijke hersteltermijn te corrigeren voordat de PoC als niet succesvol wordt beschouwd?	De PoC wordt beoordeeld aan de hand van de in de aanbestedingsstukken beschreven eisen, wensen, uitgangspunten en de vooraf vastgestelde PoC-doelstellingen. De beoordeling richt zich op de mate waarin de aangeboden Oplossing de gevraagde functionaliteit en werking aantoonbaar realiseert. Indien tijdens de PoC tekortkomingen worden vastgesteld, wordt per situatie beoordeeld of deze binnen de beschikbare PoC-periode redelijkerwijs kunnen worden hersteld en opnieuw aangetoond. Dit betekent niet dat Opdrachtnemer zonder meer recht heeft op een aanvullende hersteltermijn of een verlenging van de PoC. De concrete werkwijze en eventuele herstelmogelijkheden worden voorafgaand aan de PoC tussen partijen afgestemd.
180	**Concept Overeenkomst – Art. 9 Acceptatie**	Welke maximale acceptatieperiode geldt en wat gebeurt er wanneer Opdrachtgever niet binnen deze termijn accepteert of bevindingen rapporteert? Geldt in dat geval stilzwijgende acceptatie?	De acceptatieprocedure verloopt conform artikel 9.1 van de concept Overeenkomst, op basis van het testprotocol in het Plan van Aanpak van Opdrachtnemer. Het overige bepaalde in artikel 9 GIBIT 2025 blijft onverkort van toepassing, waaronder de daarin opgenomen termijnen en de regeling voor het geval Opdrachtgever niet tijdig reageert. Opdrachtgever ziet geen aanleiding daarnaast een afzonderlijke maximale acceptatieperiode of een regeling voor stilzwijgende acceptatie op te nemen. Acceptatie van een beveiligingskritieke voorziening dient uitdrukkelijk en gemotiveerd plaats te vinden op basis van vastgestelde testresultaten. De concrete doorlooptijden en termijnen van de acceptatieprocedure worden in het testprotocol vastgelegd, dat Partijen voorafgaand aan de acceptatiefase gezamenlijk afstemmen.
181	**Concept Overeenkomst + Programma van Eisen en Wensen – Concept Overeenkomst art. 13 and 15.2; PvE W13 / E55**	Welke exitwerkzaamheden zijn inbegrepen in de periodieke vergoeding en welke exit- of transitiewerkzaamheden mogen bij beëindiging van de Overeenkomst tegen de aangeboden uurtarieven worden gefactureerd?	Inbegrepen in de periodieke vergoeding zijn het opstellen en jaarlijks bijwerken van het Exit-plan (artikel 15.2 van de concept Overeenkomst) en de in artikel 29.6 sub ii GIBIT 2025 bedoelde werkzaamheden. De uitvoerende exit- en transitiewerkzaamheden bij beëindiging van de Overeenkomst, waaronder de dataconversie en -overdracht, kennisoverdracht en ondersteuning van de opvolgend leverancier, worden op grond van artikel 29.4 GIBIT 2025 tegen vergoeding verricht, tegen de in het Prijzenblad opgegeven uurtarieven.

Nr.	Onderwerp	Vraag	Antwoord
			Dit lijdt uitzondering indien de Overeenkomst wordt beëindigd wegens toerekenbaar tekortschieten door Opdrachtnemer; in dat geval worden deze werkzaamheden kosteloos verricht. Zie het antwoord op vraag 100. Zie ook het antwoord op vraag 45.
182	**Concept Overeenkomst + tender documents – Concept Overeenkomst art. 1.1 (Implementatie vergoeding) / pricing requirements**	Kan worden bevestigd dat kosten van derde partijen die rechtstreeks door Opdrachtgever zijn gecontracteerd, of kosten die ontstaan door wijzigingen in systemen van Opdrachtgever, niet in de inschrijfsom hoeven te worden opgenomen?	Ja, dit kan worden bevestigd. Kosten van derde partijen die rechtstreeks door Opdrachtgever zijn gecontracteerd, en kosten die ontstaan door wijzigingen in systemen van Opdrachtgever, hoeven niet in de inschrijfsom te worden opgenomen. Deze komen voor rekening van Opdrachtgever. Opdrachtgever wijst er wel op dat kosten voor derdepartijsoftware die noodzakelijk is voor de door Opdrachtnemer aangeboden Oplossing zelf, wél in de inschrijfsom moeten zijn begrepen. Dit volgt uit de definitie van de Implementatievergoeding in artikel 1.1 en uit artikel 11.2 van de concept Overeenkomst. Zie ook de antwoorden op de vragen 10 en 93. Zie voor de verdeling van verantwoordelijkheden per koppeling het antwoord op vraag 171.
183	**Nvi vraag 17**	Offerteleidraad 'Leveren implementeren en onderhouden van een Identity and Access Management-systeem. Paragraaf 2.2 Vraag: Kan opdrachtgever toelichten waarom een aantoonbaar beschikbare On-Premise-variant als knock-out eis noodzakelijk wordt geacht, terwijl de uitvraag primair is gericht op een SaaS-oplossing, en hoe is vastgesteld dat deze eis proportioneel is en niet leidt tot onnodige beperking van het aantal geschikte IAM-oplossingen in de markt?	Opdrachtgever handhaaft de eis en licht de proportionaliteit daarvan als volgt toe. Het IAM-systeem verwerkt identiteitsgegevens, autorisatiegegevens en gerelateerde log- en auditinformatie en vormt daarmee een kritieke voorziening voor de toegangsbeveiliging van de gehele gemeentelijke informatievoorziening. Opdrachtgever wil de mogelijkheid behouden om deze gegevensverwerking gedurende de looptijd volledig binnen de eigen infrastructuur te brengen, indien wijzigingen in (buitenlandse) wet- en regelgeving, geopolitieke ontwikkelingen of discontinuïteit van een onderliggende cloudaanbieder daartoe aanleiding geven. Deze overweging is toegelicht in paragraaf 2.2 van de Offerteleidraad. Opdrachtgever heeft de proportionaliteit langs twee lijnen getoetst. Ten eerste is in de marktconsultatie gebleken dat meerdere marktpartijen zowel een SaaS- als een On-Premise-variant kunnen leveren; zie het antwoord op vraag 203. Ten tweede is de eis beperkt gehouden: de On-Premise-variant hoeft niet te worden geïmplementeerd, hoeft geen operationele referentie-installatie te kennen en hoeft geen functionaliteit te bevatten die naar haar aard uitsluitend binnen een SaaS-omgeving beschikbaar is. Aantoonbare leverbaarheid met productdocumentatie volstaat. Zie ook de antwoorden op de vragen 54, 130, 151 en 158.
184	**Nvi vraag 16**	Offerteleidraad 'Leveren implementeren en onderhouden van een Identity and Access Management-systeem. Paragraaf 6.4 Vraag: Kan opdrachtgever bevestigen dat eventuele kosten voor tijdelijke licenties, consultancy-inzet en technische inrichting ten behoeve van de PoC voor vergoeding in aanmerking komen?	Nee. De kosten voor tijdelijke licenties, consultancy-inzet en technische inrichting ten behoeve van de Proof of Concept komen niet voor afzonderlijke vergoeding in aanmerking. Paragraaf 3.17 van de Offerteleidraad sluit een kostenvergoeding voor de aanbestedingsprocedure uit. Zie voor de wijze waarop de tijdens de PoC verrichte inrichtingswerkzaamheden na een succesvolle afronding binnen de implementatie kunnen worden benut het antwoord op vraag 178.

Nr.	Onderwerp	Vraag	Antwoord
185	**Nvi vraag 15**	Offerteleidraad 'Leveren implementeren en onderhouden van een Identity and Access Management-systeem. Paragraaf 6.4 Vraag: Kan opdrachtgever toelichten welke functionaliteiten en integraties minimaal onderdeel zullen uitmaken van de Proof of Concept?	Zie hiervoor het antwoord op vraag 206.
186	**Nvi vraag 14**	Offerteleidraad 'Leveren implementeren en onderhouden van een Identity and Access Management-systeem. Paragraaf 4.2.1. Vraag: Kan opdrachtgever toelichten waarom voor deze opdracht is gekozen voor een minimale verzekeringsdekking van €2,5 miljoen per gebeurtenis en €5 miljoen per jaar, en hoe opdrachtgever de proportionaliteit hiervan beoordeelt in relatie tot de omvang, aard en contractwaarde van de opdracht?	Opdrachtgever handhaaft de verzekeringseis uit paragraaf 4.2.1 van de Offerteleidraad en licht de proportionaliteit daarvan als volgt toe. De verzekeringseis is niet gerelateerd aan de contractwaarde, maar aan het risico dat zich bij falen van de dienstverlening kan verwezenlijken. Het IAM-systeem reguleert de toegang tot alle gemeentelijke systemen en gegevens. Bij een ernstig falen kan de schade aanzienlijk zijn en de contractwaarde ver overstijgen, bijvoorbeeld bij onterecht toegekende toegang tot persoonsgegevens, bij het niet tijdig intrekken van toegang na uitstroom, of bij een datalek waarbij identiteits- en autorisatiegegevens betrokken zijn. De gevraagde dekking van € 2.500.000 per gebeurtenis en € 5.000.000 per jaar sluit aan bij de aansprakelijkheidsplafonds van artikel 17.3 en 17.4 GIBIT 2025, gelezen in samenhang met artikel 18.2 GIBIT 2025, dat dekking voor ten minste twee gebeurtenissen per jaar verlangt. Zonder deze dekking zou de contractueel overeengekomen aansprakelijkheid feitelijk oninbaar kunnen blijken. Opdrachtgever acht een dergelijke dekking in de ICT-markt voor partijen die beveiligingskritieke voorzieningen aan overheden leveren gangbaar en daarmee proportioneel. Zie ook de antwoorden op de vragen 26, 80 en 91.
187	**Nvi vraag 13**	Offerteleidraad 'Leveren implementeren en onderhouden van een Identity and Access Management-systeem. Paragraaf 2.2 Vraag: Veel IAM-oplossingen worden aangeboden op basis van een gebruikers- of identiteitsgebonden licentiemodel waarbij licentiekosten direct gekoppeld zijn aan het daadwerkelijk aantal actieve identiteiten. Kan Opdrachtgever toelichten: a. Hoe inschrijvers met een dergelijk volumegebaseerd licentiemodel worden geacht om te gaan met de gevraagde bandbreedte van ±30%; b. Of Opdrachtgever verwacht dat zowel groei als krimp van het aantal identiteiten binnen deze bandbreedte volledig voor rekening en risico van opdrachtnemer blijft; c. Of Opdrachtgever bereid is toe te staan dat licentiekosten worden aangepast zodra het aantal actieve identiteiten afwijkt van het gecontracteerde volume, conform het commerciële licentiemodel van de aangeboden oplossing; d. Hoe deze eis zich verhoudt tot het uitgangspunt van marktconforme gebruikerslicenties, waarbij kosten normaliter direct samenhangen met het aantal afgenomen identiteiten.	Opdrachtgever beantwoordt uw vragen als volgt. a. Inschrijver dient zijn prijs te baseren op circa 3.000 actieve identiteiten. Fluctuaties binnen de bandbreedte leiden niet tot aanpassing van de prijs; Inschrijver kan dit in zijn tariefstelling verdisconteren. Opdrachtgever merkt op dat de bandbreedte circa 20% bedraagt en niet 30%. b. Ja, binnen de bandbreedte blijft de vergoeding ongewijzigd, zowel bij groei als bij krimp. Deze symmetrie is bewust gekozen: Opdrachtgever betaalt bij krimp binnen de bandbreedte niet minder en bij groei binnen de bandbreedte niet meer. c. Nee. Aanpassing van de licentiekosten bij iedere afwijking van het gecontracteerde volume wordt niet toegestaan. Paragraaf 2.9 van de Offerteleidraad voorziet uitsluitend in prijsoverleg indien het aantal actieve identiteiten de bovengrens van de bandbreedte gedurende drie aaneengesloten maanden structureel overschrijdt. Zie het antwoord op vraag 167. d. Opdrachtgever onderkent dat volumegebonden licentiemodellen gangbaar zijn. Een bandbreedte van circa 20% acht Opdrachtgever daarbij passend en beheersbaar, en zij dient de begrotingszekerheid van een publieke organisatie. Zie ook het antwoord op vraag 153.

Nr.	Onderwerp	Vraag	Antwoord
188	**Nvi vraag 12**	Offerteleidraad 'Leveren implementeren en onderhouden van een Identity and Access Management-systeem. Paragraaf 2.8 Vraag: Kan Opdrachtgever toelichten waarom is gekozen voor een maximale contractduur van 18 jaar, terwijl de technologische ontwikkelingen binnen IAM-oplossingen, cloudplatformen en securitydiensten doorgaans aanzienlijk kortere innovatiecycli kennen?	Opdrachtgever licht dit als volgt toe. De initiële duur van de Overeenkomst bedraagt zes jaar. De verlengingen zijn opties: vier eenzijdige verlengingen van elk één jaar, gevolgd door maximaal acht verlengingen van elk één jaar op basis van wederzijds schriftelijk akkoord. Er is dus geen sprake van een vaste looptijd van achttien jaar, maar van een maximum dat alleen wordt bereikt indien Opdrachtgever daar bij iedere verlenging opnieuw voor kiest. De achtergrond is toegelicht in paragraaf 2.8 van de Offerteleidraad: de vervanging van een IAM-systeem vergt een aanzienlijke implementatie- en migratie-inspanning, het systeem is beveiligingskritiek en frequente heraanbesteding en migratie zouden tot onevenredige kosten en risico's leiden. De door u genoemde innovatiecycli worden binnen de Overeenkomst opgevangen. Eis E54 en artikel 10 GIBIT 2025 verplichten Opdrachtnemer de Oplossing actueel, veilig en ondersteund te houden, en artikel 17 van de concept Overeenkomst voorziet in een jaarlijkse evaluatie waarin Partijen wijzigingen kunnen voorstellen. Opdrachtgever acht de looptijd daarmee proportioneel.
189	**Nvi vraag 11**	Offerteleidraad 'Leveren implementeren en onderhouden van een Identity and Access Management-systeem Vraag: Wij constateren dat een groot deel van het PvE aansluit op de huidige inrichting rondom HR-attributen, procesrollen, autorisaties, bundeltickets en de bestaande autorisatiestructuur. Kan Opdrachtgever bevestigen dat het uitgangspunt van deze aanbesteding primair bestaat uit het migreren en moderniseren van de bestaande IAM-inrichting en niet uit een fundamentele herontwerp van het autorisatiemodel of governanceproces?	Ja, dat is correct. Opdrachtgever beoogt primair de vervanging en modernisering van de bestaande IAM-inrichting. De bestaande autorisatiestructuur, procesrollenstructuur en governance vormen daarbij het uitgangspunt. Een fundamenteel herontwerp of herinrichting van het autorisatiemodel, de procesrollenstructuur of de governance maakt nadrukkelijk geen onderdeel uit van deze opdracht. Opdrachtgever verwacht dat de bestaande inrichting als uitgangspunt wordt gemigreerd en binnen de mogelijkheden van de aangeboden Oplossing wordt ondersteund. De implementatie is daarmee nadrukkelijk niet bedoeld als een traject om de bestaande IAM-inrichting, autorisatiestructuur of governance opnieuw te ontwerpen.
190	**Nvi vraag 10**	Prijzenblad Vraag: Gezien het specialistische karakter van de opdracht en de benodigde expertise op het gebied van IAM, identity lifecycle management, autorisatiebeheer, integraties en migraties, verzoeken wij opdrachtgever toe te lichten hoe het prijsplafond van €140.000 voor consultancy- en meerwerkdiensten tot stand is gekomen. Kan Opdrachtgever aangeven: a. Op welke marktbenchmark of referenties dit bedrag is gebaseerd; b. Of Opdrachtgever van mening is dat de benodigde specialistische IAM-capaciteit binnen deze financiële kaders marktconform kan worden aangeboden; c. Welke overwegingen zijn gemaakt tussen prijsstelling en de gewenste kwaliteit en ervaring van de in te zetten consultants	Opdrachtgever beantwoordt uw vragen als volgt. a. De prijsdrempel van € 75.000 en het prijsplafond van € 140.000 voor het totaal consultancy/meerwerk zijn afgeleid van de resultaten van de marktconsultatie. Het bedrag van € 140.000 betreft geen budget voor consultancy, maar het plafond van een fictieve rekensom: tweemaal 500 fictieve uren voor een projectleider/procesconsultant en een technisch consultant/developer. Aan die uren kunnen geen rechten worden ontleend; zie het antwoord op vraag 163. b. Ja. Het plafond van € 140.000 over 1.000 fictieve uren correspondeert met een gemiddeld uurtarief van € 140. De drempel van € 75.000 correspondeert met een gemiddeld uurtarief van € 75. Opdrachtgever acht deze bandbreedte voor de gevraagde functies marktconform en in overeenstemming met hetgeen in de marktconsultatie is opgehaald. c. Opdrachtgever heeft de bandbreedte zodanig gekozen dat zij ruimte laat voor ervaren en specialistische inzet, terwijl bovenmatige tarieven worden begrensd. Dit sub-subgunningscriterium weegt met vijftien van de duizend punten bovendien beperkt mee. De kwaliteit en ervaring van de in te zetten consultants worden beoordeeld binnen G2 Kwaliteit.

Nr.	Onderwerp	Vraag	Antwoord
191	**Nvi vraag 9**	Prijzenblad Vraag: Gezien de omvang van de gevraagde dienstverlening (levering, implementatie, migratie, meerdere integraties, inrichting conform functioneel ontwerp, support en onderhoud) constateren wij dat het gehanteerde prijsplafond van €735.000 voor implementatie en zes jaar dienstverlening relatief beperkt lijkt. Kan Opdrachtgever toelichten: a. Waar het prijsplafond op gebaseerd is; b. Welke uitgangspunten zijn gehanteerd voor implementatieomvang, licenties, support en beheer.	Opdrachtgever beantwoordt uw vragen als volgt. a. De prijsdrempel en het prijsplafond zijn gebaseerd op de resultaten van de marktconsultatie. Daarin is aan de deelnemende leveranciers gevraagd om, uitgaande van het functionaliteitenoverzicht en circa 3.000 identiteiten, de eenmalige implementatiekosten en de structurele kosten per jaar op te geven, inclusief een staffel voor afwijkende aantallen identiteiten. De opgegeven bedragen vormen de basis voor de vastgestelde bandbreedte. b. Uitgangspunt is de in paragraaf 2.2 van de Offerteleidraad beschreven scope: circa 3.000 identiteiten, de daar genoemde componenten en integraties, migratie van de bestaande autorisatiestructuur uit G4Gem, inrichting conform het Functioneel Ontwerp, en zes jaar licentie, hosting, onderhoud en tweede- tot vierdelijns ondersteuning. Opdrachtgever heeft de scope bewust beperkt gehouden: het autorisatiemodel wordt niet herontworpen (zie het antwoord op vraag 189), de HR-systemen van Partnerorganisaties worden niet gekoppeld (zie het antwoord op vraag 134), en aanvullende koppelingen en modules maken geen deel uit van de uitvraag. Opdrachtgever handhaaft de bandbreedte. Zie ook de antwoorden op de vragen 89 en 122.
192	**Nvi vraag 8**	Bijlage 13 Functioneel ontwerp Vraag: Staat Opdrachtgever open voor het aanpassen van processen en rollenmodel?	Nee. Opdrachtgever beoogt geen fundamentele aanpassing of herinrichting van de bestaande autorisatiestructuur, procesrollenstructuur of governance. De bestaande inrichting vormt het uitgangspunt voor de implementatie. Zie ook het antwoord op vraag 189.
193	**Nvi vraag 7**	Offerteleidraad 'Leveren implementeren en onderhouden van een Identity and Access Management-systeem. Vraag: In de begripsbepaling geeft u aan dat u ook identiteiten van partnerorganisaties beheert. Vallen deze identiteiten onder de eerder genoemde 3000 identiteiten, of staan deze daar los van en kunt u dan aangeven om hoeveel identiteiten het gaat?	De identiteiten van partnerorganisaties maken onderdeel uit van de totale omvang van de Oplossing. De eerder genoemde circa 3.000 actieve identiteiten hebben betrekking op zowel de identiteiten van medewerkers van Opdrachtgever als de actieve identiteiten van aangesloten partnerorganisaties. Opdrachtgever gaat uit van circa 3.000 actieve identiteiten, met een bandbreedte van circa ±20%. Deze bandbreedte biedt ruimte voor de verwachte ontwikkeling van het aantal identiteiten gedurende de contractperiode, waaronder groei en krimp van zowel de eigen organisatie als de deelnemende partnerorganisaties. Zie ook het antwoord op vraag 153.

Nr.	Onderwerp	Vraag	Antwoord
194	**Nvi vraag 6**	Offerteleidraad 'Leveren implementeren en onderhouden van een Identity and Access Management-systeem Vraag: In paragraaf 2.2 geeft u aan dat Implementatie en configuratie van de IAM-oplossing conform het Functioneel Ontwerp van Zaanstad moet geschieden. Staat de Gemeente ervoor open om het Functionele Ontwerp aan te passen o.b.v. de best practices van inschrijver en het gebruik van de door de inschrijver gebruikte softwarepakket?	Nee. Opdrachtgever staat niet open voor het aanpassen van het Functioneel Ontwerp vanuit de best practices of de standaardinrichting van de door Inschrijver aangeboden Oplossing, indien dit leidt tot een andere functionele inrichting of afbreuk doet aan de beschreven eisen, wensen en uitgangspunten. Het Functioneel Ontwerp en de eisen en wensen uit Bijlage 5 vormen het uitgangspunt voor de implementatie. Inschrijver is wel vrij om binnen deze kaders de eigen technische mogelijkheden en best practices te benutten voor de technische inrichting en configuratie van de Oplossing, mits daarmee aantoonbaar aan de gevraagde functionaliteit, beheersbaarheid en beoogde resultaten wordt voldaan. Zie ook de antwoorden op de vragen 189 en 192.
195	**Nvi vraag 5**	Offerteleidraad 'Leveren implementeren en onderhouden van een Identity and Access Management-systeem. Paragraaf 2.9 Vraag: De wachtkamerovereenkomst die u opneemt in de offerteleidraad is buitenproportioneel lang. Ons vakgebied is vol in beweging en inzichten en producten kunnen binnen 1 jaar, maar zeker binnen 2 jaar (maximal okt 2028) flink veranderen. Staat u ervoor open de wachtkamerovereenkomst dermate aan te passen dat wanneer u gebruik maakt van deze voorwaarde u in gesprek gaat met de volgende inschrijver om in gezamenlijk overleg te toetsen of de inschrijver nog steeds de mogelijkheden heeft om aan de vraag van opdrachtgever te voldoen conform de aangeboden aanbieding.	Nee. Opdrachtgever past de Wachtkamerovereenkomst op dit punt niet aan. De Wachtkamerovereenkomst is naar het oordeel van Opdrachtgever niet buitenproportioneel lang. Zij eindigt één jaar na Acceptatie van het IAM-systeem, dan wel, indien de Acceptatie niet wordt behaald, uiterlijk op 4 oktober 2028. Zie het antwoord op vraag 48. Het voorgestelde overleg over de vraag of de aanbieding nog actueel is, verhoudt zich niet tot de systematiek van de Wachtkamerovereenkomst. Artikel 4.1 bevat een garantie die gedurende de gehele looptijd geldt; het openstellen van een heroverweging op het moment van activering zou die garantie uithollen en de gelijke behandeling van inschrijvers raken. Opdrachtgever wijst erop dat bij activering eerst een gelijkwaardige Proof of Concept wordt uitgevoerd (artikel 5.1 Wachtkamerovereenkomst). Daarin wordt getoetst of de aangeboden Oplossing op dat moment daadwerkelijk aan de eisen en aan de Inschrijving voldoet. Dat biedt naar het oordeel van Opdrachtgever een passend en objectief moment van verificatie.
196	**Nvi vraag 4**	Bijlage 5. IAM-systeem Zaanstad - Programma van Eisen en Wensen. Paragraaf E61 Vraag: Voor kritieke (P1-)incidenten wordt een 24x7 beschikbaarheids- en bereikbaarheidsdienst gevraagd. Gezien de aard van IAM-dienstverlening komen P1-incidenten buiten kantoortijden in de praktijk relatief beperkt voor, terwijl een 24x7 dienstverlening aanzienlijke kosten met zich mee kan brengen. Staat u ervoor open om de 24x7 ondersteuning voor P1-incidenten als optionele dienstverlening apart te laten prijzen? Dit biedt u de mogelijkheid om de meerkosten af te wegen tegen het daadwerkelijke risico en de behoefte aan ondersteuning buiten kantoortijden.	Opdrachtgever verduidelijkt eis E61 als volgt. Opdrachtgever verwacht niet dat Opdrachtnemer buiten kantooruren een algemene bereikbaarheidsdienst voor gebruikers of beheerders van Opdrachtgever organiseert, noch dat hiervoor een separate piketorganisatie beschikbaar wordt gehouden uitsluitend ten behoeve van meldingen door Opdrachtgever. Voor incidenten met de hoogste prioriteit (P1) blijft echter van belang dat verstoringen die leiden tot (nagenoeg) volledige onbeschikbaarheid van de Oplossing of ernstige verstoring van de kernfunctionaliteit niet tot de volgende werkdag onbeheerd blijven wanneer deze door Opdrachtnemer of diens hosting- of cloudleverancier worden geconstateerd. Opdrachtgever gaat er daarom van uit dat Opdrachtnemer passende maatregelen heeft ingericht voor monitoring, detectie, escalatie en herstel van dergelijke verstoringen buiten reguliere werktijden. De wijze waarop Opdrachtnemer de in E61 vereiste bereikbaarheid en opvolging organisatorisch invult, is aan Opdrachtnemer, mits tijdige opvolging, escalatie en herstel van P1-verstoringen buiten reguliere werktijden zijn geborgd. Opdrachtgever acht het

Nr.	Onderwerp	Vraag	Antwoord
			niet wenselijk dat een ernstige verstoring pas wordt opgepakt nadat gebruikers of beheerders van Opdrachtgever de volgende werkdag melding maken van de uitval. De initiële gedachte achter E61 blijft daarmee gehandhaafd: kritieke verstoringen dienen buiten reguliere werktijden adequaat te worden beheerd. De organisatorische invulling hiervan mag proportioneel zijn aan het gekozen leveringsmodel en de inrichting van de dienstverlening.
197	**Nvi vraag 3**	Bijlage 5. IAM-systeem Zaanstad - Programma van Eisen en Wensen. Paragraaf E56/57 en offerteleidraad 3.15 vraag: In de aanbestedingsdocumentatie is opgenomen dat de oplossing en de bijbehorende dienstverlening beschikbaar en bruikbaar dienen te zijn in de Nederlandse taal. Is het tevens toegestaan om (onderdelen van) de oplossing, documentatie, dienstverlening en support in het Engels aan te bieden? Zo nee, kunt u beargumenteren waarom niet?	Zie antwoord vraag 88.
198	**Nvi vraag 2**	Bijlage 5. IAM-systeem Zaanstad - Programma van Eisen en Wensen. Paragraaf W9 Vraag: Kunt u aangeven of de gevraagde doorontwikkeling betrekking heeft op de functionaliteit van de oplossing zelf, dan wel op de verdere uitbreiding en optimalisatie van de bestaande implementatie, bijvoorbeeld door het onboarden van aanvullende applicaties en het inrichten van nieuwe koppelingen, workflows en use cases?	Opdrachtgever kan aangeven dat de gevraagde doorontwikkeling betrekking heeft op de verdere ontwikkeling van de functionaliteit van de Oplossing zelf. De gevraagde doorontwikkeling ziet daarmee niet op een vooraf bepaalde uitbreiding van de implementatie met aanvullende bron- en doelsystemen, nieuwe koppelingen, workflows of use cases. Eventuele toekomstige uitbreidingen worden afzonderlijk beoordeeld op basis van de dan geldende behoefte en de beheerbaarheid van de Oplossing. Indien dergelijke werkzaamheden buiten de reguliere dienstverlening vallen, kunnen hierover afzonderlijk afspraken worden gemaakt.
199	**Nvi vraag 1**	Bijlage 5. IAM-systeem Zaanstad - Programma van Eisen en Wensen. Paragraaf E54 Vraag: Kunt u nader toelichten wat binnen de scope van deze opdracht onder "doorontwikkeling" wordt verstaan? Beschikt u over een concreet beeld van de gewenste doorontwikkelingen, of verwacht u dat de opdrachtnemer hier invulling aan geeft en de afbakening nader bepaalt?	E54 ziet op zowel onderhoud als doorontwikkeling van de Oplossing. Onderhoud en doorontwikkeling maken onderdeel uit van de overeengekomen dienstverlening, waarbij de wijze van uitvoering afhankelijk is van het gekozen leveringsmodel. Onder onderhoud wordt verstaan: correctief onderhoud, preventief onderhoud en adaptief onderhoud. Adaptief onderhoud betreft aanpassingen die noodzakelijk zijn om de Oplossing blijvend te laten voldoen aan geldende wet- en regelgeving, beveiligingsrichtlijnen, ondersteunde standaarden en wijzigingen in de onderliggende technologie, infrastructuur, hostingvoorzieningen of platformen. Deze vormen van onderhoud zijn gericht op het in stand houden van de bestaande functionaliteit en werking van de Oplossing. Onder doorontwikkeling verstaat Opdrachtgever verbeteringen en verdere ontwikkelingen van de standaardfunctionaliteit van de Oplossing die Opdrachtnemer generiek aan haar klanten beschikbaar stelt. Opdrachtgever verwacht dat Opdrachtnemer hier gedurende de contractperiode invulling aan geeft als onderdeel van de reguliere dienstverlening. Doorontwikkeling ziet daarmee op de verdere ontwikkeling van de functionaliteit van de Oplossing en niet op een vooraf bepaalde uitbreiding van de implementatie met aanvullende bron- en doelsystemen, nieuwe koppelingen, workflows of use cases.

Nr.	Onderwerp	Vraag	Antwoord
			Specifiek voor Opdrachtgever ontwikkelde functionaliteit of werkzaamheden die buiten de reguliere dienstverlening vallen, kunnen afzonderlijk worden overeengekomen. Daarnaast geldt dat configuraties en ingerichte functionaliteit die onderdeel uitmaken van de implementatie, na updates en wijzigingen van de Oplossing behouden blijven en naar behoren blijven functioneren.
200	**Bijlage 13 – Functioneel Ontwerp / ruimte voor standaardinrichting**	Bijlage 13 beschrijft concreet de inrichting met onder meer IAM-persoonskaarten, Identiteitscontainers, HR-attributen, Procesrollen, Autorisaties en Resources. Kan Opdrachtgever bevestigen dat het Functioneel Ontwerp primair de vereiste functionele uitkomsten en proceswerking beschrijft, en dat een Inschrijver een technisch of conceptueel afwijkende standaardinrichting mag toepassen, mits aantoonbaar dezelfde functionele resultaten, governance, traceerbaarheid en beheerbaarheid worden gerealiseerd?	Zie het antwoord op vraag 194. Opdrachtgever staat open voor een afwijkende technische inrichting of configuratie van de Oplossing, mits daarmee de in het PvE (bijlage 5) en Functioneel Ontwerp (bijlage 13) beschreven functionele werking en resultaten worden gerealiseerd. Opdrachtgever staat niet open voor een fundamenteel afwijkend functioneel of conceptueel model van de IAM-inrichting, indien dit leidt tot een andere autorisatiestructuur, procesrollenstructuur of governance. Zie ook de antwoorden op de vragen 189 en 192.
201	**Migratie G4Gem / beschikbaarheid huidige configuratie en business rules**	Kan Opdrachtgever bevestigen dat alle business rules, uitzonderingen, mappings, scripts en configuratielogica die noodzakelijk zijn voor de migratie vanuit G4Gem en de inrichting van de IDU-keten beschikbaar worden gesteld aan de toekomstige Opdrachtnemer? Indien dit niet volledig in de huidige Aanbestedingsdocumenten is opgenomen, welke aanvullende documentatie, exports, datamodellen, configuraties of ondersteuning worden tijdens de implementatie beschikbaar gesteld?	Opdrachtgever verwacht dat een ervaren IAM-leverancier op basis van het Functioneel Ontwerp (Bijlage 13) en de beschikbaar gestelde conversiedata (Bijlage 15) een reële inschatting kan maken van de migratie- en implementatieopgave. De bestaande inrichting en de beschikbare documentatie vormen het uitgangspunt voor de implementatie. Aanvullende informatie die bij Opdrachtgever beschikbaar is en die nodig is voor de uitvoering van de migratie en implementatie, wordt tijdens de implementatie met Opdrachtnemer gedeeld.
202	**Integraties – ruimte voor equivalente technische koppelmethoden**	In E28 en Bijlage 13 worden concrete technische koppelmethoden beschreven, waaronder BINT/XML voor YouForce, LDAP(S) voor Active Directory en REST-API's voor Topdesk. Kan Opdrachtgever bevestigen dat een andere standaardintegratiemethode is toegestaan indien daarmee minimaal dezelfde functionele werking, beveiliging, logging en beheerbaarheid wordt gerealiseerd?	Opdrachtgever kan niet op voorhand bevestigen dat iedere andere standaardintegratiemethode is toegestaan. Indien Inschrijver een alternatieve standaardintegratiemethode voorstelt, dient deze concreet in de inschrijving te worden beschreven en dient Inschrijver aan te tonen dat hiermee minimaal dezelfde functionele werking, beveiliging, logging en beheerbaarheid wordt gerealiseerd en aan de overige eisen uit de aanbestedingsstukken wordt voldaan. Opdrachtgever beoordeelt de voorgestelde methode aan de hand van de aanbestedingsstukken.
203	**SaaS en On-Premise – validatie marktconsultatie**	Uit Bijlage 14 blijkt dat meerdere leveranciers hebben deelgenomen aan de marktconsultatie en demonstraties. Kan Opdrachtgever, zonder leveranciers te identificeren, bevestigen dat de uiteindelijke eis om zowel een SaaS- als een On-Premise-variant aan te bieden door meerdere marktpartijen als haalbaar is bevestigd? Kan hetzelfde worden aangegeven voor de definitieve security-eisen E41 en E42?	Ja. Uit de marktconsultatie is gebleken dat meerdere marktpartijen in staat waren om zowel een SaaS- als een On-Premise-variant van de aangeboden IAM-oplossing te leveren. Opdrachtgever heeft de combinatie van beide leveringsmodellen daarom als haalbaar en proportioneel meegenomen in de aanbesteding. Voor de definitieve security-eisen E41 en E42 verwijst Opdrachtgever naar het antwoord op vraag 5.

Nr.	Onderwerp	Vraag	Antwoord
204	**E41 – definitie Zero Knowledge en gevoelige gegevens**	E41 verlangt voor een SaaS-oplossing toepassing van het Zero Knowledge-principe, waaronder dat gevoelige gegevens waar toepasbaar niet door Opdrachtnemer kunnen worden ontsleuteld en dat Customer Managed Keys worden ondersteund. Kan Opdrachtgever nader definiëren welke gegevens binnen de IAM-oplossing als “gevoelige gegevens” worden aangemerkt en welke concrete technische invulling minimaal vereist is om aan E41 te voldoen?	Zie antwoord vraag 5.
205	**E40/E42 – MFA, FIDO2 en authenticatiesecrets**	E40 bepaalt dat MFA en FIDO2 door de centrale IdP van Opdrachtgever worden aangestuurd en dat Opdrachtnemer deze functionaliteit niet zelf hoeft te leveren. E42 stelt vervolgens eisen aan onder meer FIDO2/WebAuthn-, TOTP- en andere authenticatiesecrets. Kan Opdrachtgever bevestigen dat deze onderdelen van E42 uitsluitend van toepassing zijn voor zover dergelijke secrets daadwerkelijk binnen de Oplossing worden opgeslagen of verwerkt?	Ja. De onderdelen van E42 die betrekking hebben op FIDO2/WebAuthn-, TOTP- en andere authenticatiesecrets zijn van toepassing voor zover dergelijke secrets daadwerkelijk binnen de Oplossing worden opgeslagen of verwerkt. Indien authenticatie, waaronder MFA en FIDO2, wordt verzorgd door de centrale IdP van Opdrachtgever en de betreffende authenticatiesecrets uitsluitend binnen de IdP worden opgeslagen en verwerkt, hoeft de Oplossing deze secrets niet zelf te beheren of te beveiligen. Zie ook het antwoord op de vraag 143 over E40 en de inrichting van serviceaccounts.
206	**Paragraaf 6.4 – Proof of Concept / objectieve succescriteria**	Paragraaf 6.4 bepaalt dat scope, planning en objectieve succescriteria van de Proof of Concept na de voorlopige gunning gezamenlijk worden vastgesteld, terwijl een niet succesvol afgeronde PoC gevolgen kan hebben voor de gunning. Kan Opdrachtgever voorafgaand aan de Inschrijving de minimale PoC-scope en belangrijkste objectieve pass/fail-criteria publiceren? Kan tevens worden bevestigd dat tijdens de PoC geen functionaliteit of technische eis wordt getoetst die niet reeds voortvloeit uit de Aanbestedingsdocumenten en de Inschrijving?	Opdrachtgever publiceert de minimale scope en de belangrijkste criteria van de Proof of Concept niet voorafgaand aan de Inschrijving, maar verduidelijkt het volgende. De PoC dient ertoe vast te stellen of de beoogd Opdrachtnemer kan voldoen aan de eisen en wensen uit het Programma van Eisen en Wensen en aan hetgeen hij in zijn Inschrijving heeft aangeboden. Daarmee bevestigt Opdrachtgever dat tijdens de PoC geen functionaliteit of technische eis wordt getoetst die niet reeds voortvloeit uit de aanbestedingsstukken en uit de Inschrijving. Het zwaartepunt van de PoC ligt bij de onderdelen die zich het minst goed in een demonstratieomgeving laten aantonen: de werkende koppelingen met de bron- en doelsystemen in de scope, de migratie vanuit G4Gem op basis van de werkelijke conversiedata, de IDU-processen in samenhang met de HR-koppeling, de bundeltickets richting Topdesk en de in de eisen opgenomen beveiligingsmaatregelen. De scope, de planning, de wederzijdse verplichtingen en de objectieve criteria worden voorafgaand aan de start van de PoC door Partijen gezamenlijk vastgelegd in een plan, conform paragraaf 6.4 van de Offerteleidraad. Opdrachtgever kiest hiervoor omdat de concrete invulling mede afhangt van de aangeboden Oplossing. Het oordeel of aan de criteria is voldaan is voorbehouden aan Opdrachtgever en wordt schriftelijk en gemotiveerd meegedeeld. Ten aanzien van herstel van tijdens de PoC geconstateerde bevindingen maakt Opdrachtgever een uitdrukkelijk onderscheid. Indien een bevinding een kwestie van inrichting, configuratie of parametrisering betreft en de aangeboden Oplossing de gevraagde functionaliteit wél bevat, kan Opdrachtnemer dit binnen de looptijd van de PoC herstellen. De PoC dient in dat geval alsnog binnen de in paragraaf 6.4 van de Offerteleidraad genoemde periode succesvol te worden afgerond; die periode wordt daarvoor niet verlengd.

Nr.	Onderwerp	Vraag	Antwoord
			Indien blijkt dat de aangeboden Oplossing niet aan een gestelde eis kan voldoen, dan wel dat de in de Inschrijving aangeboden functionaliteit niet beschikbaar is, wordt de PoC als niet succesvol afgerond aangemerkt. Er wordt in dat geval geen hersteltermijn geboden en de Inschrijver wordt conform paragraaf 6.4 van de Offerteleidraad uitgesloten van verdere deelname. De PoC is een verificatie van hetgeen bij Inschrijving is aangeboden en niet een gelegenheid om functionaliteit alsnog te ontwikkelen.
207	**SaaS en On-Premise – functionele gelijkwaardigheid**	De Inschrijver dient zowel een SaaS- als een On-Premise-variant aan te bieden. Dienen beide varianten op het moment van Inschrijving volledig functioneel gelijkwaardig te zijn voor alle Eisen en Wensen, of zijn verschillen toegestaan indien beide varianten afzonderlijk voldoen aan de voor het betreffende leveringsmodel toepasselijke eisen? Welke variant dient als uitgangspunt voor de demonstratie en de Proof of Concept?	Beide aangeboden leveringsmodellen dienen te voldoen aan de eisen en wensen die voor het betreffende leveringsmodel van toepassing zijn. De gevraagde functionaliteit dient in beginsel beschikbaar te zijn in zowel de aangeboden SaaS-variant als de On-Premise-variant, tenzij uit de betreffende eis expliciet blijkt dat deze uitsluitend van toepassing is op SaaS of On-Premise. De enkele omstandigheid dat een functionaliteit door een Inschrijver aanvullend of uitsluitend in de SaaS-variant wordt aangeboden, maakt deze functionaliteit niet automatisch tot functionaliteit die buiten de scope van de On-Premise-variant valt. Eventuele verschillen, beperkingen of aanvullende randvoorwaarden tussen beide leveringsmodellen dienen expliciet in de Inschrijving te worden vermeld. Voor de demonstratie en de Proof of Concept geldt de SaaS-variant als uitgangspunt.
208	**Externe cloudleverancier – Bijlage 16**	Indien voor de SaaS-oplossing gebruik wordt gemaakt van een standaard publieke cloudleverancier zoals Microsoft Azure of AWS, dient deze cloudleverancier dan ook een ondertekende Bijlage 16 “Ter beschikking-verklaring derde” aan te leveren? Of volstaat in dat geval vermelding als onderaannemer in combinatie met de toepasselijke certificeringen en contractuele documentatie?	Voor een standaard publieke cloudleverancier als Microsoft Azure of AWS is een ondertekende Bijlage 16. Ter beschikking-verklaring derde niet vereist. Bijlage 16 ziet op de situatie waarin Inschrijver zich beroept op de draagkracht of bekwaamheid van een derde om aan een geschiktheidseis te voldoen. Bij het afnemen van generieke hostingdiensten van een publieke cloudleverancier is daarvan geen sprake. Wel gelden de eisen van paragraaf 4.2.4 van de Offerteleidraad onverkort: de cloudleverancier of hostingpartij dient te beschikken over een geldig ISO 27001-certificaat en over geldige ISO 27017- en ISO 27018-certificeringen, en Inschrijver voegt de daarop betrekking hebbende documenten bij zijn Inschrijving. Daarnaast dient deze partij als onderaannemer te worden opgegeven in het UEA. Zie ook de antwoorden op de vragen 36 en 136.
209	**Licenties – definitie inactieve Identiteit**	In de Aanbestedingsdocumenten is aangegeven dat inactieve Identiteiten niet in rekening worden gebracht. Kan Opdrachtgever definiëren wanneer een Identiteit als inactief wordt beschouwd? Kan tevens worden bevestigd dat een uitgestroomde of inactieve Identiteit die uitsluitend voor audit-, historie-, bewaartermijn- of herindiensttredingsdoeleinden in de Oplossing aanwezig blijft, niet als licentieerbare Identiteit wordt meegeteld?	Zie het antwoord op vraag 153 voor de toelichting van Opdrachtgever op wat wordt verstaan onder een ‘inactieve identiteit’. Opdrachtgever kan bevestigen dat een uitgestroomde of inactieve identiteit die uitsluitend voor audit-, historie-, bewaartermijn- of herindiensttredingsdoeleinden in de Oplossing aanwezig blijft, niet als licentieerbare identiteit wordt meegeteld.

Nr.	Onderwerp	Vraag	Antwoord
210	**Paragraaf 4.2.2 – Kerncompetentie / beroep op draagkracht softwareleverancier**	Paragraaf 4.2.2 verlangt een referentie voor het leveren, implementeren en onderhouden van een IAM-systeem voor minimaal 1.000 identiteiten bij een gemeente of vergelijkbare (semi)publieke organisatie. Kan Opdrachtgever bevestigen dat een Inschrijver die als implementatiepartner inschrijft voor deze kerncompetentie een beroep mag doen op de technische bekwaamheid en referentie van de softwareleverancier, mits deze softwareleverancier als derde/onderaannemer bij de Inschrijving wordt betrokken en de daarvoor vereiste verklaringen en UEA worden ingediend?	Ja, dit kan worden bevestigd. Een Inschrijver die als implementatiepartner inschrijft mag zich voor kerncompetentie 1 beroepen op de technische bekwaamheid en de referentie van de softwareleverancier. Voorwaarden zijn dat de softwareleverancier als derde of onderaannemer bij de Inschrijving wordt betrokken en als zodanig in het UEA wordt vermeld, dat een eigen UEA van die partij wordt ingediend, en dat Bijlage 16. Ter beschikking-verklaring derde wordt overgelegd. Dit volgt uit paragraaf 3.11 en 3.12 van de Offerteleidraad. Opdrachtgever wijst erop dat paragraaf 4.2.4 daarnaast eigen eisen stelt aan de implementatiepartner en aan de softwareleverancier, waaronder een verklaring van de softwareleverancier dat Inschrijver bevoegd is de Oplossing te leveren en te implementeren. Zie ook de antwoorden op de vragen 106 en 138.
211	**Concept Overeenkomst artikel 7.3 – prijsstelling On-Premise**	Artikel 7.3 van de Concept Overeenkomst bepaalt dat de jaarlijkse licentiekosten voor de On-Premise-variant 80% bedragen van de op dat moment geldende jaarlijkse SaaS-licentiekosten. Kan Opdrachtgever bevestigen of deze verhouding van 80% verplicht geldt, ongeacht het standaard licentiemodel van de aangeboden Oplossing? Kan tevens worden verduidelijkt welke kosten onder deze 80% vallen, en of eventuele noodzakelijke kosten voor bijvoorbeeld derdepartijsoftware, databasecomponenten of andere specifiek voor de On-Premise-variant benodigde componenten afzonderlijk mogen worden opgenomen?	De verhouding van 80% geldt verplicht, ongeacht het standaard licentiemodel van de aangeboden Oplossing. Zie de antwoorden op de vragen 1, 2, 43, 110 en 150. Onder de 80% valt dezelfde dienstverlening als binnen de SaaS-vergoeding, met uitzondering van de hosting en de daarmee samenhangende infrastructurele werkzaamheden. Zie het antwoord op vraag 174. Kosten voor derdepartijsoftware, databasecomponenten of andere componenten die specifiek voor de On-Premise-variant benodigd zijn, mogen niet afzonderlijk in het Prijzenblad worden opgenomen. Inschrijver dient in zijn Inschrijving wel expliciet te vermelden welke componenten en licenties bij een On-Premise-levering aan de zijde van Opdrachtgever aanwezig moeten zijn en welke technische randvoorwaarden gelden. Zie het antwoord op vraag 61.
212	**E48 – statische IP-adressen en IP-filtering**	E48 bepaalt dat bij SaaS één of meerdere vaste (statische) IP-adressen beschikbaar worden gesteld ten behoeve van IP-filtering door Opdrachtgever. Kan Opdrachtgever verduidelijken voor welk verkeer deze statische IP-adressen vereist zijn: toegang van Gebruikers tot de Oplossing, uitgaand verkeer vanuit de Oplossing naar systemen van Opdrachtgever, of beide? Kan tevens worden bevestigd of gelijkwaardige mechanismen zoals FQDN-allowlisting, private endpoints, service tags of vergelijkbare netwerkbeveiligingsmechanismen zijn toegestaan indien daarmee hetzelfde beveiligingsdoel wordt bereikt?	Zie antwoord op vraag 111.
213	**E50 – SSL-inspectie SaaS-On-Premise integraties**	E50 vereist dat de SaaS-Oplossing zonder verstoring functioneert wanneer SSL-inspectie wordt toegepast op netwerkverkeer tussen de SaaS-Oplossing en on-premises systemen van Opdrachtgever. Kan Opdrachtgever bevestigen of voor specifieke beveiligde koppelingen een uitzondering op SSL-inspectie mogelijk is wanneer inspectie technisch niet verenigbaar is met bijvoorbeeld mutual TLS (mTLS), certificate-based authentication of certificate pinning, mits voor deze koppelingen passende alternatieve beveiligingsmaatregelen worden toegepast?	Zie antwoord op vraag 111.

Nr.	Onderwerp	Vraag	Antwoord
214	**E35/E36 – penetratietesten en right to audit bij SaaS**	E35 verlangt jaarlijks een onafhankelijke penetratietest op de SaaS-applicatie en infrastructuur. E36 geeft Opdrachtgever daarnaast een right to audit, waaronder het laten uitvoeren van pentesten. Kan Opdrachtgever bevestigen of voor een multi-tenant SaaS-dienst de jaarlijkse onafhankelijke penetratietest, inclusief het beschikbaar stellen van de vereiste samenvatting en opvolging, kan volstaan voor dit onderdeel van het right to audit? Indien Opdrachtgever zelf een aanvullende penetratietest moet kunnen laten uitvoeren, kan dan worden verduidelijkt onder welke voorwaarden, scope en technische randvoorwaarden dit dient plaats te vinden?	Ja, in belangrijke mate. De jaarlijkse onafhankelijke penetratietest van eis E35, inclusief het verstrekken van de samenvatting van bevindingen, verbetermaatregelen en opvolging, vormt voor Opdrachtgever de reguliere invulling van dit onderdeel van het right to audit. Opdrachtgever zal in de regel niet zelf een aanvullende penetratietest laten uitvoeren op een multi-tenant SaaS-dienst. Het right to audit van eis E36 blijft echter bestaan en wordt niet uitgesloten. Opdrachtgever kan daarvan gebruikmaken indien daartoe concrete aanleiding bestaat, bijvoorbeeld na een beveiligingsincident, bij kritische bevindingen die niet tijdig worden opgevolgd, of bij aanwijzingen dat de getroffen maatregelen niet toereikend zijn. Zie ook het antwoord op vraag 39. Indien Opdrachtgever van dat recht gebruikmaakt, geldt het volgende. Scope, tijdstip en methode worden vooraf in overleg tussen Partijen vastgesteld, waarbij rekening wordt gehouden met de belangen van andere afnemers van een multi-tenant dienst. Een test wordt uitgevoerd door een onafhankelijke partij, bij voorkeur op een representatieve acceptatieomgeving, en met inachtneming van de door Opdrachtnemer te stellen redelijke technische randvoorwaarden.
215	**E28/E39/E40 – authenticatie via Active Directory en Entra ID**	E28 noemt voor SSO zowel ADFS/Azure AD (Entra ID) als authenticatie op basis van AD-accounts (username/password) of een Azure AD-identiteit. E39 en E40 stellen voor SaaS tegelijkertijd centrale authenticatie via de IdP van Opdrachtgever als uitgangspunt en beperken het gebruik van lokale wachtwoorden. Kan Opdrachtgever bevestigen dat voor een SaaS-Oplossing centrale SSO-authenticatie via Microsoft Entra ID, bijvoorbeeld via OIDC/OAuth 2.0 of SAML, volstaat en dat directe verwerking of validatie van het AD-username/password door de IAM-Oplossing niet verplicht is?	Voor SaaS-oplossingen geldt centrale authenticatie via de Identity Provider van Opdrachtgever als uitgangspunt. Authenticatie via Microsoft Entra ID met gangbare federatieve standaarden zoals OpenID Connect (OIDC)/OAuth 2.0 of SAML 2.0 voldoet hieraan. Ook andere in E28 genoemde IdP-scenario's blijven toegestaan voor zover deze als Identity Provider door Opdrachtgever worden ingezet. De Oplossing hoeft daarbij geen Active Directory-gebruikersnaam en wachtwoord rechtstreeks te verwerken of te valideren. Authenticatie dient plaats te vinden via de Identity Provider van Opdrachtgever, waarbij de Oplossing gebruikmaakt van door de Identity Provider uitgegeven tokens of assertions voor authenticatie en autorisatie.
216	**E38 – e-mailbeveiliging bij gebruik mailvoorziening Opdrachtgever**	E38 stelt voor SaaS eisen aan onder meer SPF, DKIM, DMARC, DNSSEC, STARTTLS, DANE, IPv4/IPv6, HTTPS en HSTS. Indien notificaties vanuit de IAM-Oplossing worden verzonden via de e-mailvoorziening van Opdrachtgever, kan Opdrachtgever bevestigen dat de eisen die betrekking hebben op de daadwerkelijke e-mailtransportinfrastructuur door de mailvoorziening van Opdrachtgever worden ingevuld en niet tevens zelfstandig door de IAM-Oplossing hoeven te worden gerealiseerd?	Zie antwoord vraag 114.
217	**E44 – reikwijdte API-beveiliging**	Kan Opdrachtgever bevestigen dat de eisen uit E44 ten aanzien van OAuth 2.0/OIDC en secretless authentication betrekking hebben op de door de Oplossing aangeboden en beheerde API’s, en dat voor koppelingen met externe bron- en Doelsystemen de door het betreffende externe systeem ondersteunde beveiligde authenticatiemethode mag worden toegepast?	Ja. De eisen uit E44 hebben betrekking op de door de Oplossing aangeboden en beheerde API’s. Voor koppelingen met externe bron- en doelsystemen wordt aangesloten op de door het betreffende systeem ondersteunde beveiligde authenticatiemethode