Ref. Nr.	Onderwerp	Vraag	Concept antwoord
90	Vervolgvraag #27	In artikel 3.2 is opgenomen dat: Na afloop van de voornoemde looptijd kan de overeenkomst op verzoek van beide partijen worden verlengd. Kunt u zekerheidshalve bevestigen dat voor voor verlenging de instemming van beide partijen benodigd is?	Uiteraard dienen beide partijen in te stemmen met een verlenging. Evenwel stelt Opdrachtgever met nadruk dat voor Opdrachtgever een termijn van 6 maanden geldt en van Opdrachtnemer een termijn van 24 maanden geldt om een voornemen aan te nemen om niet ter verlengen. Dit stelt beide partijen instaat proactief maatregelen te nemen op een aflopende situatie.
91	Vervolgvraag #22	Het uitgangspunt van het recht is dat een eiser – behoudens specifieke uitzonderingen waarin de bewijslast wordt omgekeerd – dient aan te tonen dat sprake is van een tekortkoming, zodat een leverancier zich daartegen ook kan verweren. Ondanks de door u aangebrachte nuancering in artikel 16.6 blijft de bewijslast dat een gebrek niet onder de garantie valt volledig bij leverancier liggen. Dat is temeer bezwaarlijk nu op grond van artikel 12.1 sub i zou kunnen worden betoogd dat praktisch alle verplichtingen onder de overeenkomst als garantieverplichtingen kwalificeren. In dat kader verwijst leverancier u tevens naar de nieuwe GIBIT 2025, waarin deze bepaling is geschrapt. Volgens de toelichting van de Vereniging van Nederlandse Gemeenten leidde de formulering van het betreffende artikel ten onrechte tot een omkering van de bewijslast ten aanzien van iedere vorm van wanprestatie. Dit is volgens de VNG nooit de bedoeling geweest. Leverancier verzoekt u daarom concreet het volgende: Bent u in ieder geval bereid de garantie onder artikel 12.1 sub i GIBIT – "dat de ICT-prestatie de overeengekomen eigenschappen zal bevatten en voldoet aan het overeengekomen gebruik" – te laten vervallen?	Opdrachtgever heeft inmiddels kennis kunnen nemen van de formeel gemaakte GIBIT 2025. Het is nergens de opzet geweest hierin bewust af te wijken van de GIBIT voorwaarden. Opdrachtgever stemt derhalve in met uw verzoek de garantie onder 12.1 sub i te laten vervallen.
92	Vervolgvraag #19	Uw eis geeft helaas geen antwoord op de vraag van Leverancier nu de door u opgesomde lijst geen uitputtende lijst betreft maar bovendien wetgeving ook vervangen kan worden door volstrekt nieuwe wetgeving. Leverancier wilt u daarom nogmaals vragen haar eerste vraag in overweging te nemen.	Opdrachtgever stelt dat in haar antwoord nadrukkelijk wordt verwezen naar "bestaande" wet en regelgeving. Indien hieruit nog steeds onduidelijkheden bij u bestaan is Opdrachtgever graag bereidt met de gegunde partij hier in de verificatie nadere afstemming over te plegen.
93	Vervolgvraag #17	U stelt dat de leverancier "alle" medewerking dient te verlenen aan de uitvoering van de DPIA. Leverancier kan niet instemmen met een onbeperkte medewerkingsverplichting. Leverancier verzoekt u daarom te bevestigen dat deze medewerkingsverplichting is beperkt tot de verplichtingen die voor leverancier voortvloeien uit de AVG, waaronder het verstrekken van relevante informatie die noodzakelijk is voor het uitvoeren van de DPIA. Indien u hier niet mee kunt instemmen, verzoekt leverancier u te verduidelijken welke aanvullende medewerking u concreet van leverancier verwacht. Daarnaast verzoekt Leverancier u, ter vermijding van misverstanden, te bevestigen dat Leverancier uitsluitend gehouden is herstelmaatregelen voor (eigen rekening) te treffen indien uit de DPIA blijkt dat sprake is van non-compliance met de AVG die aan leverancier kan worden toegerekend.	Opdrachtgever stelt dat onder "alle" in beginsel alle informatieverstrekkingen vallen in het licht van de AVG. Let op dat het oplossen van tekortkomingen naar aanleiding van de DPIA voor rekening van Opdrachtnemer niet enkel beperken door de reikwijdte van de AVG maar eveneens de aanbestedingsdocumenten in brede zin.
94	Vervolgvraag #68	Enkele jaren geleden heeft de IBD in haar dreigingsrapport gewaarschuwd voor informatiebeveiligingsrisico's in de keten tussen gemeente en leverancier. De koppeling met Entra ID voor het inloggen is zo'n ketenverbinding met verhoogde risico's. Het gebruik van MFA is daarom de norm, zoals letterlijk gesteld in de NIS2. Zoals de beantwoording nu beschreven is ligt de verantwoordelijkheid voor toepassing en controle van de MFA wel erg eenzijdig aan de kant van de leverancier. In de praktijk zien we dat ook vanuit de zorgplicht van leveranciers verwacht wordt dat er bij leverancier een failsafe aanwezig om te valideren en af te dwingen dat de MFA daadwerkelijk is uitgevoerd. Hiermee wordt het inlogproces ook aan de kant van leverancier beveiligd, en ontstaat er bescherming tegen situaties waarbij er als gevolg van misconfiguratie of een beveiligingsincident geen MFA meer wordt afgedwongen aan de zijde van de gemeente. Kan opdrachtgever bevestigen dat het ook van leverancier verwacht dat er validatie plaatsvindt op de daadwerkelijke uitvoering van de MFA aan de gemeentelijke Entra ID zijde zodat opdrachtgever een grotere mate van zekerheid heeft dat er daadwerkelijk met MFA is ingelogd.	Opdrachtgever onderschrijft dat het gebruik van MFA de norm is bij toegang via de koppeling met Microsoft Entra ID, conform de uitgangspunten uit de NIS2 Directive en de adviezen van de Informatiebeveiligingsdienst voor gemeenten. De primaire verantwoordelijkheid voor het configureren en afdwingen van MFA ligt bij de Opdrachtgever als beheerder van de eigen identity omgeving. De controle op de daadwerkelijke uitvoering van MFA door Opdrachtnemer is geen eis binnen deze aanbesteding. Opdrachnemer wordt hier dus niet toe verplicht. Wanneer een Opdrachtnemer wel een controle of validatie uitvoert op basis van claims of signalen uit de authenticatie via Microsoft Entra ID, ziet Opdrachtgever dit als een aanvullende beveiligingsmaatregel. Dit kan bijdragen aan extra bescherming tegen situaties waarin MFA door een configuratiefout of incident aan Opdrachtgever haar zijde tijdelijk niet wordt afgedwongen. Deze aanvullende maatregel kan de robuustheid van de keten versterken, maar blijft een keuze van de Opdrachtnemer.
95	Vervolgvraag #42	In de BIO 2 staat letterlijk beschreven dat (gemeentelijke) organisaties de opzet, bestaan en werking van maatregelen aantonen. Dit gaat dus verder dan de ISO27001 waar enkel de opzet van maatregelen wordt aangetoond. Leverancier vindt het vanuit deze verplichting daarom een logisch gevolg dat opdrachtgever om een assuranceverklaring vraagt die naast opzet, ook bestaan en werking aantoont. Uit de beantwoording van ref. 43 geeft opdrachtgever aan dat ook andere ISAE-type verklaringen als gelijkwaardig worden beschouwd. Kan opdrachtgever bevestigen dat het hier in alle gevallen om een 'type 2' verklaring moet gaan waarbij naast opzet en bestaan ook de effectieve werking van de beheersmaatregelen wordt aangetoond?	Opdrachtgever stelt dat de wens ten aanzien van de gevraagde certificering, en eventuele daarmee vergelijkbare varianten, eenduidig is omschreven. Opdrachtgever stelt dat in alle gevallen een rapportage wordt verwacht waarin de opzet, het bestaan en de werking zijn getoetst.
96	Vervolgvraag #42 en #43	Opdrachtgever geeft aan dat gelijkwaardige verklaringen ook acceptabel zijn. Welke ISAE-variant je ook gebruikt, het gaat uiteindelijk om de beheerprocessen die in scope zijn de assuranceverklaring. Je kunt namelijk ook prima de processen van het bedrijfsrestaurant in de verklaring opnemen, maar daarmee krijgt een ISAE-verklaring natuurlijk niet de waarde die opdrachtgever zoekt. De beheerprocessen die concreet binnen de scope van onze ISAE 3402 Type II-verklaring vallen zijn: a.Service Level Management (SLA); b.Leveranciersmanagement (dit is ook een NIS2 vereiste); c.Securitymanagement; d.Toegang- en identiteitsbeheer (dit is ook belangrijk voor de ENSIA); e.Wijzigingenbeheer; f.Continuïteitsbeheer (waaronder monitoring, patch management, back-upmanagement en failovermanagement). Dit is relevant voor de bescherming van de BRP-data en de procesgegevens van burgerzaken; g.Incidentenbeheer; h.Privacymanagement. Kan opdrachtgever bevestigen dat het verwacht dat de volgende beheerprocessen in scope van ISAE-assuranceverklaring moeten zijn? En zo niet, kan opdrachtgever dan aangeven welke beheerprocessen het minimaal in scope verwacht?	Opdrachtgever stelt dat in de wens reeds staat aangeven dat een verklaring van toepassellijkheid ten aanzien van deaangeboden ICT Prestatie en gerelateerde dienstverlening of aantoonbaar gelijkwaardig meegeleverd dient te worden. Tevens stelt Opdrachtgever dat deze certificering verder gaat dan de reeds vereiste ISO-27001 en in gaat op de verplichtingen die voorvloeien uit de BIO 2.0 en NIS 2. De meegeleverde verklaring van toepassellijkheid zal dus in alle redelijkheid en billelijkheid een weerspiegeling moet geven op de beheerprocessen die hierin vastgelegd zijn.
97	Vervolgvraag #33	In de beantwoording van ref. 33 geeft Opdrachtgever aan de eis niet te willen wijzigen, maar dat soevereine hosting wel de voorkeur heeft. Daarin klinkt een kwaliteitswens door. Leverancier zou het in dat geval redelijk vinden dat er voor het soeverein hosten van de uitgevraagde oplossing kwaliteitspunten behaald kunnen worden. Enerzijds omdat het Opdrachtgever in staat stelt om de oplossing van inschrijvers op te beoordelen, anderzijds omdat soevereine hosting ook met andere investeringen en kosten gepaard gaat dan het gebruik van de publieke cloud van Amerikaanse hyperscalers. Hiermee worden investeringen in soevereiniteit van inschrijver ook meegewogen in de beoordeling bij aanbestedingen. Stemt Opdrachtgever ermee in, gegeven de eigen voorkeur voor soevereine hosting, om de waarde van soevereine hosting in een wens terug te laten komen waarmee kwaliteitspunten behaald kunnen worden? Hierbij doen we een tekstvoorstel voor een dergelijke wens: "De gegevens van de burgerzakenapplicatie, waaronder de BRP-gegevens, die verwerkt worden in de applicatie moeten te allen tijde worden opgeslagen op servers die zich fysiek in Nederland bevinden, en in beheer zijn van Nederlandse bedrijven die niet onder de reikwijdte van buitenlandse wetgeving zoals de Amerikaanse Cloudact of FISA (section 702) vallen?"	Opdrachtgever acht het in deze aanbestedingsfase niet meer passend dergelijke invloed te willen nemen op het gestelde Programma van Eisen en Programma van Wensen, anderzijds dan bijstelling binnen opgestelde kaders om voldoende kwalitatieve Inschrijvingen mogelijk te maken. Opdrachtgever stemt niet in met uw voorstel. Evenwel kan het door u genoemde een aspect van meerwaarde zijn in het licht een van de reeds geformuleerde wensen uit het Programma van Wensen.
98	Vervolgvraag #40	Opdrachtgever stelt in eis 188 de geëiste normen voor oplostijd. Kan Opdrachtgever bevestigen dat een workaround of een aangewezen oorzaak (niet binnen de invloed van leverancier) ook gezien wordt als oplossing?	Opdrachtgever stelt dat gesproken wordt over een oplossing; een workaround die resulteert in het herstellen van de functionaliteit binnen de gestelde termijn gezien wordt gezien als oplossing, maar dit Opdrachtnemer niet ontslaat van de verantwoordelijkheid een structurele oplossing te realiseren.

99	Programma van Wensen- Wens 5 Implementatieplan	Draait uw huidige JCC Betalen-kassaoplossing on-premise of in de cloud? Indien de oplossing on-premise wordt gebruikt, verzoeken wij u aan te geven welke functionaliteit de huidige koppeling op dit moment ondersteunt.	Opdrachtgever stelt dat JCC Betalen is opgesplitst in twee applicaties. Opdrachtgever gebruikt JCC Betalen en JCC Betalen Beheer. JCC Betalen Beheer wordt alleen gebruikt door functioneel beheerders en JCC Betalen wordt gebruikt aan de balies. JCC Betalen Beheer draait on-premise en JCC Betalen in de cloud. Daarnaast is momenteel de bestaande Burgerzaken oplossing gekoppeld met deze JCC Betalen en ondersteund het doorgeven van betalingen vanuit de Burgerzaken oplossing naar JCC betalen en de achterliggende pinterminals. De reeds gestelde eis 130 blijft in stand.