

Bijlage F Programma van Eisen Integratieplatform HLTsamen

1.	Algemeen
1.1	De Opdrachtnemer gaat akkoord met de GIBIT2020, incl. de ICT kwaliteitsnormen A1, B1, B2, B3, C1, C2, D1, D2, E1, H1, H2.
1.2	De Opdrachtnemer gaat akkoord met de standaard verwerkersovereenkomst van HLTsamen.
1.3	De oplossing kent geen maatwerk. Als toch een bepaalde functionaliteit specifiek voor deze aanbesteding is ontwikkeld, dan wordt deze in de eerstvolgende release opgenomen als standaardfunctionaliteit van de oplossing. De Opdrachtnemer vermeldt in de vraag-en-antwoordronde (Nota van inlichtingen) voor welke eisen in dit Programma van Eisen maatwerk nodig is. Bij voldoende blijk van maatwerk, zal Opdrachtgever de gestelde eisen hier eventueel op aanpassen.
1.4	De leverancier heeft het Groeipact Common Ground ondertekend of heeft voornemens binnen een half jaar te ondertekenen en kan in een product strategie/release agenda aantonen dat hier naartoe wordt gewerkt.
1.5	De aangeboden oplossing voldoet aan en loopt niet meer dan één major versie achter op de standaarden van VNG-Realisatie of Forum Standaardisatie die voor de oplossing relevant zijn. Aanpassingen in de hierboven genoemde standaarden worden binnen zes maanden doorgevoerd nadat deze als nieuwe standaard zijn gepubliceerd. Daarnaast wordt de oude versie van de standaard nog minimaal één jaar ondersteund.
1.6	De aangeboden oplossing voldoet aan de volgende standaarden van VNG-Realisatie of Forum Standaardisatie: - Digikoppeling - Digitoegankelijk (EN 301 549 met WCAG 2.1) - DNSSEC - HTTPS en HSTS - NEN-ISO/IEC27001 - NEN-ISO/IEC27002 - NL GOV Assurance profile for OAuth 2.0 - OpenAPI Specification - REST-API Design Rules - RPKI - SAML - security.txt - StUF - TLS

1.7	Door Opdrachtnemer wordt voor de in gebruik name van de applicatie een exit overeenkomst opgesteld, zoals benoemd in de GIBIT2020. Opdrachtnemer beschrijft hierbij de wijze waarop de gegevens terug beschikbaar worden gesteld aan de gemeenten vanuit de gehele applicatie, decommissioning van de totale applicatie (inclusief acceptatie hiervan) plaatsvindt, welke termijnen gelden gedurende deze exit procedure en welke capaciteit hiermee gemoeid gaan. Alle opgebouwde gegevens en instellingen/inrichting moeten overgedragen kunnen worden. Alle gegevens dienen daarna te worden vernietigd en de Opdrachtnemer levert hiervoor een verklaring aan. De kosten voor het opstellen en uitvoeren van deze (concept-)exit overeenkomst (incl. exit plan) dienen in de Inschrijving opgenomen te zijn.
1.8	Opdrachtgever is en blijft eigenaar van de gegevens en heeft daar te allen tijde de zeggenschap over. Gegevens zijn altijd toegankelijk en mogen door de leverancier niet voor andere doeleinden worden gebruikt.
2.	ICT
2.1	De oplossing wordt aangeboden als SaaS-oplossing aan de eindgebruiker, inclusief beveiligde verbindingen. Het is hierbij niet toegestaan om een VDI- of Citrix sessie te gebruiken noch hiervoor een VPN op te zetten. Ten behoeve van de SaaS-oplossing mag on premise uitsluitend iets in het DMZ van opdrachtgever worden geïnstalleerd.
2.2	De Opdrachtnemer actualiseert na afloop van de implementatie de visualisatie van de aangeboden applicatie, modules en koppelingen door middel van een architectuurschets waarin wordt aangegeven welke componenten worden geleverd en hoe deze op elkaar aansluiten.
2.3	Voor de logische communicatielaag dient het verkeer gebaseerd te zijn op het https protocol, zowel intern als extern
2.4	De integriteit van de gegevens blijft gewaarborgd door deze aantoonbaar te scheiden van andere klanten.
2.5	Alle gegevens uit de database van de oplossing kunnen tenminste o.b.v. API en webservices (SOAP/REST), worden geëxtraheerd via een beschikbaar koppelylak, zodat gebruik in een datawarehouse of andere omgeving mogelijk is.
2.6	De installatie van de oplossing dient plaats te vinden in een productie- en een testomgeving, waarbij de applicatielaag en de data laag echt volledig gescheiden zijn tussen de productie- en testomgeving. Dit dient te geschieden binnen de geoffreerde prijsopgave.
2.7	De inrichting en het onderhoud van de test- en productieomgevingen dienen te worden meegenomen in de prijsopgave met inbegrip van de eventuele consequenties voor licentiekosten.
2.8	De Oplossing ontsluit zowel via internet als DigiNetwerk
2.9	De applicatie heeft een webbased user-interface. Deze is zonder beperking van functionaliteit, benaderbaar met Microsoft Edge, zonder gebruik te maken van plug-ins (zoals Flash, Silverlight, ActiveX, etc.), met uitzondering van JAVA.
2.10	De oplossing werkt volledig zonder aanvullende client installaties.
2.11	Gebruikersbeheer; User provisioning wordt automatisch gedaan vanuit AzureAD. De authenticatie van gebruikers gaat via SSO met Microsoft AzureAD. De autorisatie (rechten/rollen) van gebruikers geschiedt binnen het pakket.
2.12	Inloggen door lokale gebruikers (bv. consultant Opdrachtnemer) binnen de SaaS oplossing, vereist MFA om in te loggen
2.13	Wanneer een gebruikte basisregistratie ontsloten wordt door API's zal de leverancier zo spoedig als mogelijk deze API's gebruiken om deze gegevens in zijn applicatie te gebruiken in plaats van kopieën op te slaan
2.14	API's worden via een standaard integratiefaciliteit ontsloten zoals bijvoorbeeld extern op NLX maar dit kan waar van toepassing ook een interne integratiefaciliteiten zijn zoals een gemeentelijke servicebus of API Gateway.

3.	Privacy en Informatiebeveiliging - security
3.1	De leverancier kan aantonen door middel van ISO 27001 certificering dat de beveiliging van de omgeving van de leverancier voldoet aan geldende beveiligingsnormen.
3.2	Leverancier en de hostingpartij zijn gevestigd onder Nederlands of Europees recht. Hosting van het portaal en de gegevens vindt fysiek plaats binnen de Europese Economische Ruimte, in overeenstemming met de eisen van de Europese Unie.
3.3	De applicatie biedt zodanige functionaliteit m.b.t. auditing/logging dat van alle relevante handelingen en pogingen daartoe - door zowel door gebruikers als applicaties - d.m.v. logging een historie wordt vastgelegd. Het is mogelijk om in te richten dat er alerts verzonden worden bij bepaalde events.
3.4	Inschrijver is bereid op eigen kosten jaarlijks een verklaring van getrouwheid (of vergelijkbaar) te verkrijgen via een onafhankelijke derde partij, om aan te tonen dat zij als Contractant veilig om gaat met vertrouwelijke informatie.
3.5	Inschrijver garandeert dat ongeautoriseerde personen geen toegang hebben tot het systeem
3.6	Voorafgaand aan het afsluiten van de overeenkomst wordt een Data Protection Impact Assessment uitgevoerd (DPIA) om de risico's en maatregelen in kaart te brengen. HLTsamen voert dze DPIA uit, Opdrachtnemer werkt hier aan mee.
3.7	Het systeem voldoet aan het principe van "privacy en informatieveiligheid by design"; privacyoverwegingen zijn vanaf het allereerste begin geïntegreerd in het ontwerp en de ontwikkeling ervan.
3.8	Het systeem voldoet aan het principe "privacy en informatieveiligheid by default"
3.9	De applicatie en Opdrachtnemer voldoen aan de AVG. De Opdrachtnemer is in dit kader aangemerkt als Verwerker. Niet alleen de data moet zijn opgeslagen binnen de Europese Economische Ruimte, maar tevens is de vestigingsplaats van de Opdrachtnemer binnen de Europese Economische Ruimte
4.	Functionaliteit
4.1	De Oplossing ondersteunt de datadistributie tussen alle applicaties zoals getoond in het document de huidige en gewenste situatie (biilagen G en H)
4.2	De oplossing is flexibel in te zetten voor routeringen en protocolwisselingen van berichten tussen applicaties van Opdrachtgever onderling.
4.3	De oplossing is flexibel in te zetten voor routeringen en protocolwisselingen van berichten tussen applicaties van Opdrachtgever en ketenpartners.
4.4	De oplossing is flexibel in te zetten voor routeringen en protocolwisselingen van berichten tussen applicaties van Opdrachtgever en landelijke voorzieningen.
4.5	De oplossing biedt functionaliteit voor orkestratie, translatie en validatie van berichten
4.6	De oplossing is in staat om een inkomend bericht te vertalen in een andere berichtenstandaard en deze door te sturen. Dit betreft minimaal een binnenkomend XML bericht en een binnenkomend JSON bericht dat kan worden omgezet in een StUF bericht, en omgekeerd.
4.7	De oplossing kan worden gebruikt voor het opzetten van beveiligde verbindingen tussen applicaties in verschillende cloudomgevingen, dan wel tussen een cloud en on-premise omgeving.
4.8	De oplossing voorziet in een Digikoppeling voorziening (oplossing voor koppeling met landelijke basisregistraties).

4.9	Wanneer er gegevens van een entiteit wijzigen, worden alle afnemers door middel van kennisgevingsberichten hierover geïnformeerd, <u>als zij een abonnement hebben op de entiteit én geautoriseerd zijn voor het gewijzigde gegeven.</u>
4.10	Het is voor een aangesloten applicatie mogelijk om, via de oplossing voor gegevensdistributie, een integrale zoekvraag te stellen aan de Landelijke Voorziening GBA-V. Voor buitengemeentelijke personen wordt er eerst in de eigen database van de oplossing gezocht, <u>bij geen resultaat wordt de LV GBA-V bevraagd.</u>
4.11	Het is voor een aangesloten applicatie mogelijk om, via de oplossing voor gegevensdistributie, een integrale zoekvraag te stellen aan de Landelijke Voorzieningen. De database van de oplossing bevat geen opslag van LV's gegevens (uitgezonderd BRP), dus de <u>bevraging gaat meteen naar de LV's.</u>
4.12	Alle zoekvragen, inclusief integrale zoekvragen, worden gelogd en deze logging is op eenvoudige wijze raadpleegbaar en in een open <u>formaat te exporteren.</u>
4.13	Het is mogelijk om bij het onderdeel van het beantwoorden van een interne integrale zoekvraag dat de geleverde persoon wordt toegevoegd aan de database en dat een afnemerindicatie voor de vragende applicatie wordt geplaatst, zonder extra handelingen <u>vanuit de vragende applicatie of de oplossing.</u>
4.14	Het is mogelijk om VOA-berichten automatisch te verwerken in de gegevens van de buitengemeentelijke personen waarop deze <u>berichten betrekking hebben. Dit leidt vervolgens tot mutatieberichten aan de aangesloten afnemers.</u>
4.15	Het plaatsen en verwijderen van de VOA-indicaties moet automatisch kan zowel automatisch (volgens in te stellen regels) als <u>handmatig. Bij handmatig kunnen deze indicaties individueel geplaatst en verwijderd worden.</u>
4.16	Het plaatsen en verwijderen van de volgindicaties door afnemende applicaties in de oplossing kan zowel automatisch (volgens in te stellen regels) als handmatig. Bij handmatig kunnen deze indicaties individueel geplaatst en verwijderd worden.
4.17	De oplossing beschikt over zoekfunctionaliteit waarmee de beheerder kan zoeken naar berichten op basis van minimaal de volgende filters: Identificatie van het bericht van de zendende en ontvangende applicatie; Interne identificatie van de servicebus; Ontvangende <u>applicatie; Zendende applicatie; Verwerkingsstatus; Datum en tijdstip verzenden.</u>
4.18	De oplossing beschikt over functionaliteit om de inhoud van het bericht handmatig aan te passen.
4.19	De servicebus verifieert of berichten daadwerkelijk ontvangen zijn door de ontvangende applicatie (indien ontvangende applicatie daarin voorziet).
4.20	Als een afnemende applicatie niet beschikbaar is, dan worden de berichten voor die applicatie in een wachtkamer geplaatst en alsnog <u>afgeleverd zodra de afnemende applicatie weer beschikbaar is.</u>
4.21	'End-to-end' monitoring per berichtstroom is mogelijk binnen de Oplossing. Onder de monitoring verstaan wij ook de pro-actieve <u>signalering die plaatsvindt als berichten niet succesvol kunnen worden verwerkt of verstuurd.</u>
4.22	De oplossing biedt overzichtelijke functionaliteit voor monitoring (logging, foutregistratie, signalering en dergelijke) van de <u>berichtstromen, alsmede voor het afvangen en behandelen van storingen.</u>
4.23	Er is een dashboard beschikbaar waarop alle ontvangen en verzonden berichten getoond worden zodat een beheerder in één <u>oogopslag ziet waar iets misgaat.</u>
4.24	Het is mogelijk om een notificatie te ontvangen zodra een storing geconstateerd wordt. Beschrijf via welke kanalen (mail, SMS, WhatsApp, etc.) <u>notificaties mogelijk zijn.</u>
4.25	De oplossing biedt mogelijkheden om, naar aanleiding van bijv. kwaliteitscontroles, gegevens in het gegevensmagazijn gericht op te <u>schonen en fouten te herstellen.</u>
4.26	Er zijn kwaliteitscontroles beschikbaar die de gegevens vergelijken met de gegevens in de (LV van de) basisregistratie.

4.27	Het datamodel van het gegevensmagazijn van de oplossing voldoet aan het RSGB.
4.28	De documentatie bevat een gedetailleerd inzicht in het datamodel van het gegevensmagazijn. Alle tabellen zijn beschreven, ook de <u>onderlinge relaties</u> . En elk gegevensveld dient <u>eveneens semantisch beschreven te zijn</u> .
4.29	Uw oplossing dient minimaal het gebruik van diakritische tekens te ondersteunen zoals wettelijk voorgeschreven.
4.30	De oplossing voorziet in een API gateway, inclusief security en logging.
4.31	De applicatie sluit aan op de beschikbare LV API's zoals door het Kadaster, KvK of binnengemeentelijk aangeboden. Deze API's zijn <u>conform de door VNG gestandaardiseerde API specificaties voor het zoeken en raadplegen van gegevens</u> .
4.32	De oplossing legt per gegevenselement vast welke applicatie de leverancier is van dit gegevenselement en welke applicaties afnemer zijn.
4.33	De oplossing is in staat om de afnemende applicaties per gegevenselement te autoriseren.
4.34	Per entiteit is te zien waar de gegevens vandaan komen en wanneer deze voor het laatst zijn gewijzigd.
5.	Implementatie
5.1	Opdrachtgever verwacht van de Opdrachtnemer maximale ontzorging. In het implementatieplan nemen inschrijvers op hoeveel inzet van welke functionarissen van HLTsamen benodigd is.
5.2	De opdrachtnemer communiceert tijdens het implementatieproces over de wijzigingen tov het implementatieplan.
5.3	De opdrachtnemer traint en ondersteunt de gebruikers tijdens de implementatie.
5.4	De opdrachtnemer treedt op als projectleider tijdens de implementatie.
6.	Beheer
6.1	Opdrachtnemer voert het technisch beheer uit. De technisch beheerder is verantwoordelijk voor het functioneren en beheren van de server(s) en database, alsmede voor de noodzakelijke verbindingen en de beschikbaarheid van de applicatie,: - Zorgdragen voor een dagelijkse back-up van de systeemprogrammatuur en databases - Tijdig plaatsen van updates en serverpatches - Technisch en functioneel onderhoud van de database - Monitoren geldigheid van cpa's en certificaten en informeren opdrachtgever uiterlijk 1 maand voor einddatum geldigheid - Opschonen logging volgens vooraf afgesproken bewaartermijnen - Afstemming nieuwe of gewijzigde functionaliteit en verstoringen met de functioneel beheerder - Tijdig beschikbaar stellen van nieuwe en geüpdatete standaardkoppelvlakken - Beheer van de infrastructuur (koppelingen naar opdrachtgever en ketenpartners) - De technisch beheerder is bevoegd om direct maatregelen te treffen als de continuïteit van de applicatie of de in de database opgeslagen informatie acuut in het geding is en is verplicht om in dit geval achteraf ter zake te rapporteren aan de functioneel beheerder -Voorzien in de fysieke beveiliging van de applicatie

6.2	De Oplossing kent geen beperkingen met betrekking tot aantallen van gebruikers en/of te koppelen informatiesystemen en hoeveelheden data.
6.3	De Opdrachtnemer zorgt voor backups waarbij de maximale RPO (Recovery Point Objective) 24 uur bedraagt. De maximale RTO (Recovery Time Objective) is 8 uur.
6.4	Herstelmaatregelen, waaronder back-up en recovery procedures, zijn geïmplementeerd en worden periodiek getest door opdrachtnemer. De opdrachtgever ontvangt hierover een terugkoppeling.