Bijlage 3: Programma van Eisen

Algemeen

1. De oplossing past alle relevante Open standaarden toe die op de 'pas toe of leg uit'- lijst van Forum Standaardisatie staan.
2. De oplossing voldoet aan de eisen, richtlijnen en kaders geschetst in de Project Startarchitectuur (PSA).
3. De oplossing voldoet aan de toegankelijkheidsnorm WCAG 2.1, niveau A + AA. Dit blijkt uit een gepubliceerde toegankelijkheidsverklaring die niet ouder dan een jaar is.
4. De opslag en de verwerking van gegevens vindt plaats in de EU of EER. De leverancier kan dit aantonen.
5. De oplossing is een standaard en bewezen product met minimaal maatmerk
   Als toch bepaalde functionaliteit specifiek voor deze aanbesteding is ontwikkeld, dan wordt deze in de eerstvolgende release opgenomen als standaardfunctionaliteit van de oplossing.
6. De Opdrachtnemer levert functionele en technische documentatie ten behoeve van de koppelingen, inrichting, techniek en beheer en gebruikershandleidingen.
7. Er worden minimaal twee gescheiden omgevingen beschikbaar gesteld inclusief met indien mogelijk in dit PvE geëiste interfaces/koppelingen. De 2e omgeving kan gebruikt worden voor test- en opleidingsdoeleinden. Deze omgeving bevat testdata maar geeft qua werking een representatie van de productieomgeving en kan door de Opdrachtnemer binnen een werkdag beschikbaar gesteld worden indien Opdrachtgever hier om vraagt.
8. De 2^{e} omgeving werkt geïsoleerd en is niet gekoppeld aan de productieomgeving. Ook heeft deze omgeving een eigen dataset. Opdrachtgever moet zelf kunnen beslissen of en wanneer productiedata gekopieerd kan worden naar de testomgeving t.b.v. testen van significante wijzigingen. Deze actie maakt deel uit van de standaard beheerkosten.

Integratie en uitwisseling (koppelingen)

9. Het moet mogelijk zijn om een datadump van alle gegevens te maken. De datadump moet door een ETL-tool te gebruiken zijn. In deze datadump zijn entiteiten, relaties, attributen en waardenbereik integraal opgenomen. Daarbij is metadata aanwezig met een omschrijving van alle entiteiten, relaties, attributen en waardenbereiken. Met de datadump moet het mogelijk zijn zelfstandig (zonder tussenkomst van leverancier) gegevens met een ETL-data in te laden in een andere database.
10. De oplossing maakt gebruik van standaard uitwisselingstechnieken en berichtenopbouw (wsdl) voor de uitwisseling van gegevens via webservices
11. De applicatie beschikt over standaard API's voor alle relevante datavelden en functies in de applicatie, waarmee externe applicaties kunnen communiceren. Hierbij wordt zoveel mogelijk gebruik gemaakt van OpenAPI Specification (OAS 3.0).
12. De oplossing kan overweg met asynchrone berichtenverkeer inclusief een instelbaar retry mechanisme bij fouten
13. De oplossing moet uitgebreide logging van de koppelingen bijhouden.
14. De oplossing beschikt over een mogelijkheid voor het automatisch afhandelen van events vanuit andere systemen.
15. Gegevensuitwisseling maakt gebruik van een basisversleuteling (https)

16. Opdrachtnemer zorgt voor minimaal 256 bits versleuteling volgens Advanced Encryption Standard (AES) voor opslag en transport van gevoelige gegevens.
17. De Opdrachtnemer garandeert de integriteit van berichten van en naar de cloud-oplossing.
18. De Opdrachtgever houdt zelf de regie over de door Opdrachtnemer te realiseren koppelingen. Dat wil zeggen dat alle koppelingen (inclusief SaaS - SaaS) via de integratie laag van de Opdrachtgever verlopen, waarbij de uitwisseling van gegevens gelogd en/of gemonitord

Logging / Informatiebeveiliging

19. De oplossing beschikt over een niet-muteerbare audit-trail om van elk van onderstaande handelingen te registreren door wie de handeling op welk moment vanaf welke locatie werd uitgevoerd:
    - Raadplegen;
    - Creëren/toevoegen;
    - Wijzigen;
    - Verwijderen;
20. De bewaarperiode van log-entries is instelbaar. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.
21. Om Opdrachtgever in staat te stellen om te beoordelen of Opdrachtnemer efficiënte informatiebeveiligingsmaatregelen heeft geïmplementeerd, dient Opdrachtnemer jaarlijks een Assurance verklaring (bijvoorbeeld ISAE 3000 of ISAE3402 type 2) aan Opdrachtgever beschikbaar te stellen. Hiermee krijgt Opdrachtgever zekerheid omtrent de werking van maatregelen in relatie tot de gevraagde dienstverlening. De Assurance verklaring dient minimaal in te gaan op volgende onderwerpen:
    a. Changemanagement.
    b. Risicomanagement.
    c. Logische- en fysieke toegangsbeveiliging.
    d. Veilig personeel.
    e. Patchmanagement.
    f. Back-up en restore proces.
    g. Continuïteitsmanagement.

    Als Opdrachtnemer hierin niet kan voorzien dan wel in gebreke blijft, heeft Opdrachtgever na voorafgaande schriftelijke kennisgeving met een termijn van ten minste 30 dagen en maximaal eenmaal per jaar, het recht een geautoriseerde partij die door Opdrachtgever is ingeschakeld bij Opdrachtnemer een audit uit te laten voeren.
    De kosten van de Assurance verklaring zijn voor rekening van de Opdrachtnemer.
    Indien Opdrachtnemer gebruik maakt van diensten van derden, zoals datacenterdiensten of infrastructuur(beheer) dan gelden deze beheersingsmaatregelen ook voor die derde partij en dient de Opdrachtnemer vast te stellen dat deze partij de beheersmaatregelen heeft geïmplementeerd.

Privacy

22. De oplossing moet voldoen aan en functioneren binnen:
    - De Wet Basisregistratie Personen;
    - De AVG;

- De BIO;
- De beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum;

23. Uitgewisselde persoonsgegevens en andere vertrouwelijke informatie wordt veilig (versleuteld) verzonden.
24. De oplossing ondersteunt het opschonen van persoonsgegevens na het verstrijken van de bewaartermijn (anonimiseren en/of wissen) in het kader van gegevensbeheer.
25. Opdrachtgever laat op reguliere basis penetratietesten uitvoeren door een onafhankelijke partij en stelt het verslag van deze test beschikbaar op verzoek van Opdrachtgever. Daarnaast is Opdrachtgever aangesloten bij het CERT Watermanagement. Geconstateerde kwetsbaarheden op het gebied van informatiebeveiliging worden doorgegeven aan de Opdrachtnemer. De Opdrachtnemer zal op dezelfde werkdag actie ondernemen.
    - Binnen 4 uur brengt de Opdrachtnemer een advies uit over hoe naar aanleiding van de geconstateerde kwetsbaarheid moet worden geacteerd.
    - Als er sprake is van een hoog risico dan biedt Opdrachtnemer binnen 8 uur een workaround voor de geconstateerde kwetsbaarheid.
    - Binnen twee weken na melding van de geconstateerde kwetsbaarheid biedt Opdrachtnemer een definitieve oplossing in de vorm van een patch, dan wel een instructie hoe de kwetsbaarheid op te heffen. De functionaliteit van de applicatie mag hierbij niet worden beperkt.
    - Op aangeven van de Opdrachtgever dient de Opdrachtnemer patches in geval van hoog risico security issues, binnen 24 uur door te voeren.

Authenticatie en autorisaties

26. De oplossing ondersteunt Single Sign-on (SSO) op basis van Azure Active Directory credentials van het domein van de Opdrachtgever. De huidige standaard van Opdrachtgever is SAML/OUUTH2. Aanvullend dient Two Factor Authentication (2FA) mogelijk te zijn voor authenticatie buiten het domein van Opdrachtgever. Na authenticatie hebben gebruikers direct toegang tot alle onderdelen van de aangeboden oplossing, uiteraard voor zover ze daartoe zijn geautoriseerd. SSO wil zeggen dat de gebruiker niet apart hoeft in te loggen in de oplossing nadat de gebruiker zich reeds eenmalig heeft geauthentiseerd (binnen het netwerk op basis van de initiële Active Directory login en buiten het netwerk met zijn/haar Active Directory credentials op het portaal).
27. In de oplossing en bijbehorende database opgeslagen gegevens moeten alleen toegankelijk zijn voor geautoriseerde gebruikers. Dit zijn persoonlijke accounts en geen algemene beheeraccounts.
28. Binnen de oplossing kunnen de specifieke toegangsrechten tot gegevens en functies verleend worden op basis van een rol gebaseerde autorisatie (Role Based Access Control).
29. De rollen voor de autorisaties in de oplossing kunnen door de beheerder gedefinieerd en toegekend worden aan gebruikers en gebruikersgroepen.
30. Het is in de oplossing mogelijk om rolscheiding af te dwingen (BIO: maatregel 6.1.2.)
31. De oplossing ondersteunt dat van de toegekende autorisaties en rollen rapportages gemaakt kunnen worden.

Operationele eisen

32. De oplossing beschikt over een webbased userinterface die zonder beperking van functionaliteit, benaderbaar is met de 2 laatste major versies van meest gangbare browsers zoals Microsoft Edge, Google Chrome, Apple Safari en Mozilla Firefox of vergelijkbaar zonder gebruik te maken van plug-ins (zoals Flash, Silverlight, ActiveX, of vergelijkbaar etc.).
33. De SaaS-applicatie is geschikt voor verschillende soorten apparaten (laptop, tablet, smartphone etc.) en schaalt, met uitzondering van beheerfuncties, mee met de afmetingen van een scherm van mobile devices tot tabletniveau, zonder in te leveren op leesbaarheid van tekst of bruikbaarheid van de gebruikersinterface (responsive design)

Service en support

34. Het systeem moet een acceptabele performance kunnen bieden voor minimaal 100 gelijktijdige gebruikers. Een uitzondering hierop is complexe zoekopdrachten en (grote) rapportages
35. Opdrachtnemer garandeert mee te werken aan externe audits als hierom door Opdrachtgever gevraagd wordt.
36. Opdrachtnemer werkt bij contractbeëindiging actief mee aan de overdracht van de dienstverlening naar een andere partij gedurende een periode van 2 maanden voorafgaand aan de datum van contractbeëindiging. Actief meewerken houdt in:
    - Het opleveren van alle data (inclusief de metadata, entiteiten, relaties, attributen en waardenbereik) in een systeemonafhankelijk digitaal formaat (XML/JSON) via een beveiligd medium (DVD's, secure FTP, etc.);
    - Het opleveren van gebruikersdata (accountnamen, overzicht rollen en autorisaties, etc.);
    - Het realiseren van een actieve datasynchronisatie-koppeling naar de nieuwe SaaS-oplossing als dit technisch mogelijk is.
37. Opdrachtnemer garandeert op aanvraag van Opdrachtgever mee te werken aan een exit-strategie.
38. De Opdrachtnemer verzorgt een Nederlandstalige helpdesk voor zowel technische als functionele ondersteuning. De helpdesk is het centrale punt voor het melden van incidenten, het stellen van vragen, indienen van wijzigingsvoorstellen en geeft informatie/ inzicht in de afhandeling daarvan. De helpdesk van de Opdrachtnemer levert zowel telefonische ondersteuning als ondersteuning via e-mail en/of een web portaal. De helpdesk is telefonisch bereikbaar op werkdagen tussen 08.00 en 17.00 uur (CET). Naast de helpdesk is 24/7 een storingsdesk bereikbaar voor Categorie 1 incidenten. Voor ondersteuning door de helpdesk en storingsdesk van de Opdrachtnemer worden geen aanvullende kosten in rekening gebracht.
39. Van 08.00 - 18.00 uur wordt de beschikbaarheid van de oplossing voor minimaal 99,5% per maand gegarandeerd met een downtime van maximaal 1 uur. Voor de overige uren wordt dit voor minimaal 99,0% per maand gegarandeerd met een downtime van maximaal 4 uur. De Opdrachtnemer levert 1 keer per kwartaal een rapportage aan, welke is gebaseerd op een heldere rekenmethode.
40. De helpdesk is verantwoordelijk voor de gehele behandeling van meldingen, incidenten m.b.t. de oplossing volgens de procedure zoals vastgelegd in de Service Level Agreement (SLA). De Opdrachtgever bepaalt de prioriteit van incidenten. Ten aanzien van de ondersteuning wordt minimaal de volgende prioriteitsbepaling gehanteerd: Prioriteitentabel:

Categorie 1	De oplossing is volledig niet beschikbaar (naar mening van de Opdrachtgever een Critical Problem)
Categorie 2	De oplossing is deels niet beschikbaar of deels niet beschikbaar voor meer dan 10% van de gebruikers (naar mening van de Opdrachtgever een Major Problem)
Categorie 3	De oplossing is beschikbaar maar er is sprake een klein deel van de oplossing is niet beschikbaar/werkbaar. Er is sprake van een kleine verstoringen (naar mening van de Opdrachtgever een Minor Problem)
Categorie 4	Gebruikers/beheerdersvraag

De helpdesk draagt tevens zorg voor relateren van incidenten aan reeds bekende problemen m.b.t. de oplossing. De Opdrachtnemer maakt voor de Opdrachtgever inzichtelijk wanneer een incident in behandeling is genomen en wat de status van afhandeling is. De Opdrachtnemer is eindverantwoordelijk voor het beheren van incidenten. De Opdrachtnemer hanteert de onderstaande reactietijden per categorie per servicewindow:
Service Windows:

SW1	Van maandag t/m vrijdag tussen 08:00 en 17:00
SW2	Van maandag t/m vrijdag tussen 17:00 en 21:00
SW3	Tussen vrijdag 21:00 en maandag 08:00 Van maandag t/m vrijdag tussen 21:00 en 08:00

Prioriteit	Actie	Service Window
Categorie 1	Reactietijd van 30 minuten beantwoorden met oplossing van 8 uur met workaround van 4 uur	SW1, SW2
Categorie 2	Reactietijd van 2 uur beantwoorden met oplossing van 8 uur met workaround van 4 uur	SW3
Categorie 3	Reactietijd van 1 werkdag met oplossing in volgende reguliere release met workaround binnen 48 uur	SW1
Categorie 4	Reactietijd van 1 werkdag met antwoord binnen een week	SW1

41. De leverancier garandeert dat gegevens die in de Cloud worden ondergebracht altijd het eigendom blijven van Opdrachtgever, waaronder begrepen alle rechten van intellectuele eigendom, zoals het auteursrecht en databankenrecht.
42. De Opdrachtnemer kan de kwaliteit van informatiebeveiliging aantonen aan de hand van certificaten (ISO27001). De scope, verklaring van toepasselijkheid en actualiteit van het certificaat moeten voldoen. Binnen de scope valt ook fysieke toegang.
43. De Opdrachtnemer dient keten van toeleveranciers bekend te maken en transparant te zijn over de maatregelen die zij genomen hebben om de aan hun opgelegde eisen ook door te vertalen naar hun toeleveranciers
44. De Opdrachtnemer garandeert dat op aanvraag van Opdrachtgever gegevens aantoonbaar volledig vernietigd worden.
45. De Opdrachtnemer werkt op verzoek van Opdrachtgever mee aan het uitvoeren van een Broncode Escrow overeenkomst.

46. De Opdrachtnemer garandeert adequate back-up- en restorevoorzieningen van de oplossing waarbij, in het geval een restore van data nodig is, de afgesproken dienstverlening binnen 24 uur kan worden gecontinueerd waarbij sprake is van maximaal 24 uur dataverlies. In geval van corrupte data kan een herstel/rollback worden uitgevoerd om een eerdere (consistente) staat te herstellen. Het herstel/rollback mechanisme van de oplossing is zodanig dat het mogelijk is om de volledige oplossing vanaf een bepaalde transactie te herstellen. Back-ups worden gemaakt terwijl de volledige oplossing “online” is.