

Bijlage 3

Programma van eisen en wensen

Control- en Procesmodelleringsapplicatie

Integrale audit, risico en procesapplicatie



Kenmerk

Z/21/091557

Datum

7 november 2023 versie definitief



Inhoudsopgave

1.	Inleiding	3
2.	Eisen.....	3
2.1	Functionele Eisen.....	3
2.2	Technische Eisen	6
2.3	Eisen Privacy en Informatiebeveiliging (PIV).....	14
3.	Wensen	16

1. Inleiding

In deze bijlage vindt u het programma van eisen en wensen. De eisen zijn minimumeisen. Het niet onvoorwaardelijk voldoen aan deze eisen heeft uitsluiting van verdere deelname aan deze aanbestedingsprocedure tot gevolg.

De wensen zijn een onderdeel van het gunningscriterium Kwaliteit. U dient per wens aan te geven of u de wens wel of niet invult. Aan ieder antwoord zal een score worden toegekend. De wijze waarop de wensen worden beoordeeld kunt u vinden bij criterium kwaliteit K4: Wensen in paragraaf 4.8 van het beschrijvend document Aanbesteding Control- en Procesmodelleringsapplicatie d.d. 7 november 2023.

2. Eisen

2.1 Functionele Eisen

Hieronder zijn de eisen omschreven die van toepassing zijn.

ALGEMEEN	
F-E1	De applicatie werkt volgens het Bronregistratie principe: alle functies in de oplossing maken gebruik van dezelfde eenduidige gegevensset.
F-E2	Gegevens worden eenmalig opgeslagen binnen de applicatie. Er is geen sprake van kopieën van gegevens.
F-E3	De zoekfunctie werkt binnen de applicatie altijd op dezelfde wijze, is eenvoudig door alle medewerkers te gebruiken en geeft correcte resultaten. De medewerker vindt wat hij/zij zoekt.
F-E4	Het is mogelijk om velden en structuren in de applicatie toe te voegen, te wijzigen en/of te verwijderen zonder tussenkomst van de leverancier. Denk hierbij aan de organisatiestructuur, rollen/functies, applicaties, risico's en beheersmaatregelen.
F-E5	Binnen de applicatie worden eenduidige iconen gebruikt om functies aan te duiden.
F-E6	Binnen de applicatie kunnen hyperlinks naar externe bestanden en locaties gebruikt worden. Met externe bestanden bedoelen wij bestanden op locaties buiten de applicatie van aanbieder. Dit kan dus zowel binnen als buiten het netwerk van de gemeente Hoeksche Waard.
F-E7	Het toevoegen, aanpassen en verwijderen van hyperlinks is afhankelijk van toe te kennen gebruikersrechten.
F-E8	Elke medewerker moet toegang hebben tot de publicatieomgeving en deze kunnen raadplegen.
F-E9	Van alle ingevoerde gegevens wordt automatisch versiebeheer bijgehouden
F-E10	Het versiebeheer is eenvoudig inzichtelijk en kan geactiveerd worden voor gebruikers of rollen.
F-E11	Onder versiebeheer valt ook het terug zetten van een vorige versie. Deze functie is alleen beschikbaar voor beheerders.
F-E12	Er is logging aanwezig in de applicatie, zodat inzichtelijk is wie en wanneer de laatste bewerking heeft uitgevoerd. Deze functie is alleen beschikbaar voor beheerders.
F-E13	Mogelijkheid om verschillende rollen aan gebruikers toe te kennen. Denk hierbij aan alleen-lezen, gebruiker en beheerder.

F-E14	Als onderdeel van deze aanbesteding levert de aanbieder een (digitale) training en/of e-learning voor de afzonderlijke gebruikersrollen.
F-E15	De applicatie werkt volgens het Three Lines model
F-E16	In de applicatie zijn standaard rapporten beschikbaar.
F-E17	Rapporten kunnen worden gekopieerd, aangepast, ingesteld, bewerkt en uitgedraaid in de meest gangbare formaten waaronder Excel, Word en PDF.
F-E18	Gegevens kunnen binnen de verschillende functies van de applicatie onderling gekoppeld, gebruikt en uitgewisseld worden. Bijvoorbeeld: • Risico's en persoonsgegevens kunnen aan processen gekoppeld worden. • Applicaties kunnen aan processtappen gekoppeld worden. • Functies kunnen aan processtappen gekoppeld worden.
F-E19	De applicatie bevat een workflow- en signaalfunctie voor de opvolging van bevindingen en overige activiteiten waarbij acties toegewezen kunnen worden aan gebruikers en/of teams.
F-E20	Inlezen of importeren van gegevens is uitsluitend mogelijk door een beheerder.
F-E21	De applicatie bevat de functionaliteit om alle vastgelegde gegevens te ontsluiten via de rapportagetool Cognos of PowerBI of te verwerken in een datawarehouse.
F-E22	De applicatie bevat de functionaliteit mogelijkheid om direct met de eindgebruiker te kunnen communiceren, zodat ze wijzigingen e.d. via de tool kunnen doorgeven.
F-E23	De applicatie bevat de mogelijkheid voor het gebruiken van standaard normensets gericht op rechtmatigheid/doelmatigheid.
F-E24	De applicatie bevat de mogelijkheid voor het gebruiken van eigen normensets.
F-E25	Normensets in de applicaties zijn ingedeeld op rubriek en op meerdere sub-rubrieken en/of niveaus.
PROCESSEN	
F-E26	De applicatie bevat de functionaliteit voor het modelleren en vastleggen van processen in processchema's met beschrijvingen.
F-E27	De applicatie bevat de functionaliteit voor het zelf kunnen toevoegen, wijzigen en verwijderen van processen.
F-E28	In de applicatie kan voor processen gebruik gemaakt worden van verschillende iconen (om zo de zichtbaarheid van verschillende soorten processtappen te vergroten)
F-E29	In de applicatie kan de gebruiker en/of beheerder zelf bepalen waar iconen in de flow geplaatst worden.
F-E30	De applicatie bevat de functionaliteit om een processtap te koppelen aan een rol/functie.
F-E31	De applicatie bevat de functionaliteit om per processtap meerdere verbindinglijnen toe te voegen, zodat meerdere iconen met elkaar verbonden kunnen worden.
F-E32	De applicatie bevat de functionaliteit om controle momenten in het proces op te nemen.
F-E33	De applicatie bevat diverse weergaven van het proces o.a. Flowchart, Swimlane en Rasci.

F-E34	De applicatie bevat de functionaliteit voor het op kunnen nemen van hyperlink/direct link naar een locatie buiten de processen applicatie.
F-E35	Elke medewerker moet mogelijkheid hebben tot raadplegen van de publicatieomgeving van de processen.
F-E36	De applicatie bevat een eenvoudige zoekfunctie o.a. op naam proces, product, team, functie en status.
F-E37	De applicatie bevat de functionaliteit voor het herstellen van wijzigingen in de processen.
F-E38	De applicatie bevat de functionaliteit om inzicht te krijgen in uitgevoerde wijzigingen in processen.
F-E39	Op het moment dat een proces gepubliceerd is, mag en kan deze niet gewijzigd worden.
F-E40	De applicatie bevat de mogelijkheid om de procespublicatie naar eigen wens en inzicht in te richten, zonder tussenkomst van de leverancier.
F-E41	De applicatie bevat de mogelijkheid om beschreven processen in te lezen in nieuwe applicatie. De opdrachtgever bedoelt hiermee import functionaliteit die werkt met gangbare procesformaten.
F-E42	De applicatie bevat functionaliteit voor het gebruik van foto's, plaatjes e.d.
F-E43	De applicatie ondersteunt diverse niveaus van procesbeschrijvingen, variërend in detaillering. Bijvoorbeeld Hoofd- en subprocessen.
F-E44	De applicatie bevat functionaliteit om processen aan elkaar te koppelen. Bijvoorbeeld Vergunningsverlening en handhaving volgen elkaar op.
RISICOMANAGEMENT	
F-E45	De applicatie bevat de functionaliteit voor het uitvragen, inventariseren (vastleggen), analyseren en monitoren van de risico's en beheersmaatregelen en deze, waar mogelijk, te koppelen aan processen.
F-E46	De applicatie bevat de functionaliteit voor het opvolgen en monitoren van bevindingen en adviezen uit ENSIA, BIO, Interne beheersing en Accountantsverslagen (Audits).
AVG	
F-E47	De applicatie bevat de functionaliteit voor een gegevensverwerkingsregister waarbij de data geclassificeerd worden met de processen als basis.
F-E48	De applicatie bevat functionaliteit voor het registreren van een DPIA, (verwerkers) overeenkomst, AVG Quicksan, Artikel 30 formulier.
F-E49	De applicatie bevat de mogelijkheid om te verwijzen/ koppelen naar documenten, zoals verwerkersovereenkomsten en evt. DPIA (die evt. ook elders kunnen zijn opgeslagen).
INFORMATIEBEVEILIGING	
F-E50	De applicatie bevat de functionaliteit voor het opvolgen en monitoren bevindingen uit audits zoals ENSIA, BIO, Interne beheersing en Accountantsverslagen (Audits).
F-E51	De applicatie bevat de functionaliteit voor het vastleggen van normen uit verschillende normenkaders zoals de BIO.
INTERNE CONTROLE	
F-E52	De applicatie bevat functionaliteit voor het uitvoeren van een intern onderzoek of een interne controle

2.2 Technische Eisen

CLOUD-APPLICATIE	
T-E1	De applicatie wordt aangeboden als cloud- applicatie (off-premise gemeente Hoeksche Waard).
T-E2	Leverancier van de applicatie en de hostingpartij zijn gevestigd onder Nederlands of Europees recht. Hosting van de applicatie en de gegevens vindt fysiek plaats in en in overeenstemming met de eisen van de Europese Unie.
T-E3	De applicatie is volledig webbased te gebruiken, binnen de Citrix-omgeving van de gemeente Hoeksche Waard zonder gebruik van een extra Citrix-omgeving en zeker niet met andere vormen van remote-app clients.
T-E4	De applicatie moet gedurende de gehele looptijd van de Overeenkomst, inclusief eventuele verlengingen, functioneren binnen de ICT-omgeving van gemeente Hoeksche Waard en binnen de meest gangbare besturingssystemen en webbrowsers en aansluiten op de nieuwste updates en releases hiervan.
T-E5	De integriteit van data blijft gewaarborgd door bedrijfskritische data van gemeente Hoeksche Waard aantoonbaar te scheiden van andere klanten. Leverancier heeft ISO 20000, ISO 27000, ISAE 3402 en/of vergelijkbare certificeringen om aan te tonen dat interne procedures bij de cloudprovider op orde zijn.
BROWSERS	
T-E6	Alle gebruikersinterfaces van de applicatie dienen volledig webbased te zijn – zonder dat daarbij clientside plug-ins als Java, ActiveX, Flash, SilverLight, etc. benodigd zijn – en als zodanig ten minste benaderbaar met (de meest actuele versies van) de volgende browsers, zonder enige beperking v.w.b. weergave en functionaliteit: • Microsoft Edge (standaard); • Mozilla Firefox, de laatste en voorlaatste released versie; • Google Chrome, de laatste en voorlaatste released versie.
MICROSOFT 365	
T-E7	De applicatie ondersteunt MS 365 64-bit versie.
T-E8	Vanuit de applicatie moet beveiligd worden gemaïld, conform BIO regelgeving
PRODUCTIE- EN TESTOMGEVING	
T-E9	De installatie van de applicatie vindt plaats in een productie- en een testomgeving zoals aangeven (productie, testomgeving gebruiker en testomgeving beheerders): • De productie- en testomgevingen zijn gescheiden omgevingen; • Beide omgevingen moeten altijd, zonder tussenkomst van leverancier, bruikbaar zijn; • De testomgeving geeft te allen tijde een representatie van de productieomgeving; • De testomgeving wordt, net als de productieomgeving, geback-up't in een omgeving die minimaal zo veilig en compliant is als de productieomgeving; • De data in de testomgeving mag niet hetzelfde zijn als in de productieomgevingen (geanonimiseerde, niet herleidbare gegevens), AVG compliant; • De testomgeving werkt geïsoleerd en is niet gekoppeld aan de productieomgeving.
COMMON GROUND	

T-E10	De applicatie dient zo veel mogelijk te zijn ontwikkeld volgens de principes van Common Ground (VNG): • Gegevens en data gescheiden van processen en applicaties; • Gebruik van een gemeenschappelijke integratielaag; • Gegevens blijven bij de bron; • Gegevens worden niet gekopieerd en/of dubbel opgeslagen.
KOPPELINGEN	
T-E11	Data uitwisseling voor onder andere koppelingen, integraties, import/export vindt plaats via bestanden en protocollen die voorkomen op de lijst van open standaarden (zoals onder andere StUF, API's; zie https://www.forumstandaardisatie.nl).
T-E12	Opdrachtnemer verzorgt de complete technische en functionele implementatie van de koppelingen met andere (SAAS-)aanbieders voor zover het haar kant van de koppeling betreft.
T-E13	Wanneer er een koppeling gebouwd moet worden tussen applicaties ligt de voorkeur bij het gebruik van OpenTunnel van Enable-U.
T-E14	Alle eventuele applicatie datastromen vinden plaats op basis van ten minste HTTPS verkeer TLS 1.3, SSL of gelijkwaardig certificaat (en indien bij hoge uitzondering en alleen bij vooraf schriftelijke toestemming van de TISO een andere vorm van ontsluiten wordt gekozen op basis van HTTPS, SSL V2 en 2 way SSL certificaat) en de mogelijkheid om een reverse proxy oplossing van de gemeente in te kunnen zetten (NetScaler).
T-E15	Leverancier garandeert dat de gevraagde koppelingen voldoen en ook in de toekomst blijven voldoen aan nieuwe versies van de betreffende landelijke standaarden.
T-E16	Koppelingen met landelijke voorzieningen dienen te lopen o.b.v. berichtenverkeer, conform de betreffende landelijke standaarden (GEMMA). Dit geldt ook voor de levering van administratieve gegevens aan afnemende applicaties.
DATA, DATAMODEL EN DATABASE	
T-E17	De database en data zijn gescheiden van de applicatie.
T-E18	Gemeente Hoeksche Waard is en blijft te allen tijde eigenaar van de gegevens binnen de applicatie en heeft daar als zodanig ook te allen tijde toegang toe. Gemeente Hoeksche Waard kan haar gegevens bovendien te allen tijde terugtrekken of vernietigen zonder tussenkomst van Leverancier.
T-E19	Leverancier geeft inzage in het datamodel van de database, indien gewenst onder non-disclosure agreement. In de applicatie moet van ieder schermveld eenvoudig te achterhalen zijn wat de naam van het veld in de database is en in welke tabellen dit veld voorkomt.
T-E20	Leverancier garandeert dat toevoegingen aan en veranderingen van het datamodel van de applicatie mogelijk zijn en blijven en zorgt ervoor dat de bijbehorende functionaliteiten beschikbaar blijven in alle latere versies van de applicatie.
T-E21	Leverancier biedt gemeente Hoeksche Waard te allen tijde, uiteraard m.u.v. de afgesproken service windows, toegang tot de databron voor bevraging via ETL.
T-E22	Leverancier voert alleen wijzigingen door in de database van de applicatie, nadat gemeente Hoeksche Waard hierover is geïnformeerd. Dit geldt zowel voor individuele wijzigingen, als voor massale wijzigingen al dan niet via de applicatie of rechtstreeks in de database.

BEVEILIGING	
T-E23	De applicatie stelt gemeente Hoeksche Waard in staat om voor de betreffende aspecten te voldoen aan de Baseline Informatiebeveiliging Overheid en dient qua beschikbaarheid, integriteit en vertrouwelijkheid te functioneren op een niveau dat consistent is met het informatiebeveiligingsniveau dat vereist is voor de bedrijfsprocessen die door de applicatie worden ondersteund. Leverancier conformeert zich daarbij aan het informatiebeveiligingsbeleid van gemeente Hoeksche Waard en sluit onder andere daarvoor met gemeente Hoeksche Waard een SLA en Verwerkersovereenkomst af.
T-E24	Een jaarlijkse Third Party Mededeling (TPM-verklaring) ten behoeve van het jaarlijkse ICT-Beveiligingsassessment zal op verzoek van Gemeente Hoeksche Waard door Inschrijver beschikbaar worden gesteld.
T-E25	Gemeente Hoeksche Waard heeft een 'right to audit', waarbij Gemeente Hoeksche Waard in overleg met Inschrijver een auditor aanwijst.
T-E26	Alle communicatie met de applicatie geschiedt volledig o.b.v. HTTPS aangevuld met certificaten. De securitylagen van de verbindingen mogen maximaal 1 versie achterlopen (N-1) van wat als de nu hoogste mogelijke security standaard wordt beschouwd.
T-E27	Alle communicatie tussen de applicatie en clients is adequaat beschermd tegen af luisteren en manipulatie middels versleuteling (TLS 1.3, SSL of gelijkwaardig).
T-E28	De actieve gebruikerssessies met de applicatie zijn beveiligd tegen overname, manipulatie en Denial of Service (DoS).
T-E29	Het is de verantwoordelijkheid van Leverancier om de applicatie tijdens de betreffende (door)ontwikkeling te controleren op mogelijke beveiligingsissues. Leverancier dient actief kwetsbaarheden te volgen die gepubliceerd worden (via www.cvedetails.com bijvoorbeeld) en in voorkomend geval de nodige acties te nemen, incl. het informeren en adviseren van gemeente Hoeksche Waard over de eventueel te nemen maatregelen om beveiligingslekken te dichten.
T-E30	Medewerkers van Leverancier mogen niet zonder voorafgaande toestemming van gemeente Hoeksche Waard de gegevens van gemeente Hoeksche Waard in de database benaderen.
AUTHENTICATIE EN AUTORISATIE	
T-E31	Authenticatie (toegang tot de applicatie) en autorisatie (rechten binnen de applicatie) vinden plaats o.b.v. de gebruikers en gebruikersgroepen met een (beveiligd tegen schrijven) Microsoft (Azure) Active Directory (MS (A)AD) server van gemeente Hoeksche Waard; de authenticatie vindt plaats via single sign-on met Multi Factor Authentication (MFA). Het koppelen van gebruikers aan gebruikersgroepen gebeurt bij voorkeur vanuit de MS (A)AD-server van gemeente Hoeksche Waard.
T-E32	Bij authenticatie van gebruikers is er geen mogelijkheid om inloggegevens van andere gebruikers te achterhalen, te manipuleren of opnieuw te gebruiken. Het onthouden van inloggegevens binnen de browser is beperkt in tijd en gebaseerd op een mechanisme van unieke, éénmalige waarde en versleuteling. De wachtwoord reset procedure ontsluit geen informatie die voor aanvallers bruikbaar is.
T-E33	Autorisaties van gebruikers kunnen ook binnen de applicatie worden vastgelegd. Hiertoe worden de rechten in de applicatie gekoppeld aan rollen (role based access).

	Rollen binnen de applicatie zijn door gemeente Hoeksche Waard zelf vrij te definiëren (incl. verwijderen) en kunnen daarbij gekoppeld worden aan één of meer gebruikers(groepen)
LOGGING	
T-E34	De applicatie beschikt over automatische mutatielogging op handeling, gebruiker en tijdstip ten behoeve van audittrail. De systeem en/of functioneel beheerder van de gemeente met een admin account dient hier zelfstandig toegang tot te krijgen.
EENMALIGE DIENSTEN	
T-E35	Leverancier verzorgt de volledige Implementatie van de software. Hieronder wordt onder meer verstaan: • Alle onderdelen van de software die benodigd zijn voor uitvoering van de functie(s) waar de software voor aangeschaft is worden volledig werkend opgeleverd in de test- en productie-omgevingen; • Beschikbaarstelling, op basis van toegangsrechten, van alle benodigde onderdelen/modules van de software die nodig zijn voor uitvoering van het beheer; • Opleveren van werkende Koppelingen tussen de software en genoemde andere systemen (bijvoorbeeld, DDS, en landelijke voorzieningen) conform de betreffende standaarden; • Opleveren van werkende Koppeling voor single-sign-on via (Azure) ADFS; • Verzorgt eventuele datamigratie die nodig is, inclusief historie en aanwezige plusgegevens; • Opleveren van een procedure om data van de productieomgeving veilig te kopiëren naar de testomgeving; • Alle trainingen; • Leverancier is in staat om deze Implementatie conform K1: Implementatieplan te voltooien, inclusief Acceptatieprocedure. Leverancier beschikt over voldoende capaciteit om dit te bereiken en committeert zich aan deze planning.
T-E36	Leverancier levert voor aanvang van de Implementatie een Implementatieplan overeenkomstig en neemt hierin onder meer zaken op als: • Initiële inrichting/configuratie, realisatie Koppelingen, Conversie en initiële vulling, training, Acceptatietest en uitrol naar productie; • Het wie (taken en verantwoordelijkheden over en weer), wat (activiteitenplanning incl. deliverables) en wanneer (doorlooptijden en mijlpalen) m.b.t. voornoemde onderdelen; • Welke technische randvoorwaarden er nodig zijn voor alle genoemde Koppelingen, incl. welke certificaten daartoe nodig zijn en welke daarvan door gemeente Hoeksche Waard verzorgd dienen te worden; • Grafisch inzicht in de doelarchitectuur van de geboden applicatie en koppelingen; • Een risicoanalyse; • Planning van de trainingen;
T-E37	Leverancier voert de projectleiding van de Implementatie, in samenspraak met gemeente Hoeksche Waard. De projectleider van Leverancier beheert tijd en risico's, reageert proactief en signaleert problemen; hierbij communiceert hij/zij veelvuldig met de projectleider van gemeente Hoeksche Waard. Over Koppelingen communiceert Leverancier direct met de betreffende leverancier(s) van de betreffende gemeentelijke / landelijke applicaties/voorzieningen, indien nodig nadat gemeente Hoeksche Waard met de betreffende leverancier(s) een opdracht heeft besproken.

T-E38	Leverancier verzorgt de training van minimaal 2 beheerders, zodanig dat zij na afloop hiervan volledig zelfstandig met de software applicatie overweg kunnen en deze aldus kunnen gebruiken, configureren en beheren. Training vindt plaats op locatie bij gemeente Hoeksche Waard en omvat tevens alle eventuele betreffende voorbereidingen en documentatie.
T-E39	Alle aan Leverancier gerelateerde personen die rechtstreeks contact hebben met gemeente Hoeksche Waard, dienen Nederlands te spreken en te schrijven.
T-E40	Als onderdeel van de Implementatie stelt Leverancier een exitplan op. Het aanleveren van dit exitplan is een voorwaarde voor Acceptatie. In dit plan wordt ten minste beschreven: • Op welke wijze, bij (reguliere of onverwachte) beëindiging van het contract, de (meta)data wordt overdragen aan een andere partij (bijvoorbeeld de eerstvolgende partij bij de aanbesteding); • Op welke wijze de betreffende (meta)data vervolgens wordt verwijderd en vernietigd.
T-E41	De initiële Implementatie wordt afgesloten met een Acceptatieprocedure. Gemeente Hoeksche Waard behoudt zich het recht voor om in het kader van de Acceptatieprocedure één of meer (deel)tests door derden te laten uitvoeren. Leverancier zegt hiervoor op voorhand zijn volledige medewerking toe. Leverancier werkt actief mee aan en ondersteunt gemeente Hoeksche Waard bij (de uitvoering van) de Acceptatietests. Hiertoe is Leverancier met één of meer personen op locatie bij gemeente Hoeksche Waard, om te assisteren bij problemen (zoals bij koppelingen) en om bijvoorbeeld de communicatie met de ontwikkelaars / technici te faciliteren. Er is alleen sprake van Acceptatie bij een wederzijdse akkoordverklaring, die schriftelijk wordt geformaliseerd door zowel gemeente Hoeksche Waard als Leverancier.
T-E42	Leverancier zegt op voorhand haar volledige medewerking toe wanneer er, bijv. bij beëindiging van de overeenkomst, een conversie/migratie naar een andere applicatie plaats dient te vinden. Hiertoe krijgt gemeente Hoeksche Waard van Leverancier kosteloos de beschikking over alle gegevens- en configuratiebestanden met alle bijbehorende documentatie zodat gemeente Hoeksche Waard of een derde partij namens haar een en ander kan migreren. Bovendien zal Leverancier hierbij desgevraagd aanvullende dienstverlening verzorgen zodanig dat de continuïteit van de bedrijfsvoering van gemeente Hoeksche Waard niet in gevaar komt. Deze medewerking vindt plaats o.b.v. een nadere offerteaanvraag.

DOORLOPENDE DIENSTEN - HOSTING

T-E43	De applicatie moet een SAAS oplossing zijn, waarbij de verantwoordelijkheid voor de Hosting ligt bij Leverancier. Onder de betreffende verantwoordelijkheid van Leverancier vallen onder andere maar niet uitsluitend het in een fysiek en logisch voldoende beveiligde omgeving – bestaande uit alle daartoe benodigde software (zoals besturingssystemen, firewalls, technische beheertools, virtualisatiesoftware, etc.) en hardware (zoals servers, opslag, back-up, netwerken, et cetera) – beschikbaar stellen van de applicatie, incl. back-up, recovery en uitwijk(test).
T-E44	De applicatie behoort in een werkende productiefase een acceptabele performance te vertonen voor circa 50 concurrent gebruikers.

DOORLOPENDE DIENSTEN - BEHEER

T-E45	Het technisch applicatiebeheer wordt door, of indien mogelijk, in nauwe samenwerking met de Leverancier uitgevoerd. Leverancier voert Updates en Upgrades door in zowel de productie- en testomgeving. De applicatie dient correct en probleemloos te functioneren na het doorvoeren van de Updates en Upgrades.
T-E46	Leverancier stelt tijdig release notes beschikbaar van Updates en Upgrades, zodat gemeente Hoeksche Waard inzicht heeft in evt. veranderingen die aldus in de applicatie worden aangebracht.
T-E47	Leverancier verschaft gemeente Hoeksche Waard voor zover mogelijk (dus m.u.v. van ad-hoc fixes / patches etc.) vooraf inzicht in de releaseplanning van Updates en Upgrades.
T-E48	Het functioneel applicatiebeheer wordt door gemeente Hoeksche Waard uitgevoerd, waarbij gemeente Hoeksche Waard de volledige vrijheid heeft de applicatie functioneel naar eigen wens in te richten binnen de mogelijkheden die de applicatie biedt en door Leverancier wordt ondersteund.
T-E49	De beheeromgeving voor het configureren, instellen en beheren van de applicatie is zodanig dat de functioneel beheerders van gemeente Hoeksche Waard de applicatie zelfstandig kunnen beheren zonder tussenkomst van de Leverancier.
T-E50	Alle functionele beheertaken kunnen worden uitgevoerd zonder dat dit invloed heeft op de werking van de applicatie voor de overige gebruikers; gebruikers kunnen ingelogd blijven en gebruik blijven maken van de applicatie gedurende het uitvoeren van functionele beheerstaken.
T-E51	Voor het uitvoeren van functioneel beheer moet de functioneel beheerder zelf de autorisaties en stamtabellen kunnen inrichten en beheren met begin- en einddatum en gebruikmakend van logfiles (aanmaken en wijzigen van gebruikers, functierollen, stuur- en stamgegevens en het beheren van de helpteksten). Kortom: centrale beheer van autorisaties binnen de applicatie. De autorisatie dient rol gebaseerd te zijn.

DOORLOPENDE DIENSTEN - ONDERHOUD

T-E52	Leverancier verzorgt gedurende de looptijd van de overeenkomst het aanbrengen van wijzigingen in de programmatuur en/of de gegevensstructuur van (delen van) de softwareapplicatie; dit omvat zowel Correctief, Preventief als Innovatief (adaptief én functioneel) onderhoud: • Correctief onderhoud omvat het aanbrengen van wijzigingen in de programmatuur en/of de gegevensstructuur van (delen van) de applicatie om gebreken te herstellen. • Preventief onderhoud omvat het aanbrengen van wijzigingen in de programmatuur en/of de gegevensstructuur van (delen van) de applicatie om gebreken te voorkomen. • Adaptief innovatief onderhoud omvat het aanbrengen van wijzigingen in de programmatuur en/of de gegevensstructuur van (delen van) de applicatie als gevolg van wijzigingen in de omgeving. • Functioneel innovatief onderhoud omvat het planmatig uitbreiden en/of aanpassen (door ontwikkelen) van de functionaliteit van (delen van) de applicatie op initiatief van Leverancier zelf. Onderhoud resulteert in Updates en Upgrades van de applicatie. Dergelijke Updates en Upgrades en de uitrol daarvan worden door Leverancier eerst zelf getest alvorens e.e.a. wordt opgeleverd aan gemeente Hoeksche Waard. Elk van voornoemde vormen van Onderhoud omvat tevens het dienovereenkomstig aanpassen van alle evt. betreffende gebruikers- en beheerdocumentatie.
-------	--

DOORLOPENDE DIENSTEN - SUPPORT	
T-E53	Leverancier verzorgt een Nederlandstalige service-/supportdesk, die voor gemeente Hoeksche Waard als "single point of contact" dienstdoet voor het stellen van vragen, melden van incidenten en indienen van wijzigingsvoorstellen, alsmede voor informatie over de afhandeling daarvan. Voor het stellen van vragen, melden van incidenten en indienen van wijzigingsvoorstellen worden geen kosten gerekend. Het beantwoorden van gestelde vragen en het afhandelen van gemelde incidenten in het kader van ondersteuning dient inclusief te zijn voor zover dit geen wijzigingsvoorstellen (changes) behelst; hiervoor kan dus geen (aanvullende) vergoeding worden gevraagd. Aanmeldingen (incidenten, wijzigingen) Vragen, meldingen van incidenten en wijzigingsvoorstellen kunnen ten minste online (formulier), per e-mail en telefonisch worden ingediend en zijn vervolgens 24/7 online in te zien (incl. actuele status / voortgang). Daarnaast moet het mogelijk zijn om bekende problemen en/of issues te raadplegen zodat 'known errors' kunnen worden geïdentificeerd.
DOORLOPENDE DIENSTEN – SERVICE LEVEL AGREEMENT	
T-E54	Leverancier levert een SLA aan welke zal worden beoordeeld door opdrachtgever.
T-E55	De volgende onderwerpen moeten benoemd worden in de SLA: • Beschikbaarheidspercentages van de omgeving als geheel; • Reactietijden van de doorlopende diensten; • Oplostijden van de doorlopende diensten • Periodieke rapportage door leverancier aan opdrachtgever over de geleverde prestatie, waarbij minimaal de volgende onderwerpen benoemd zijn: ○ Beschikbaarheid ○ Reactietijden ○ Oplostijden • Procedures voor Veiligheid en Bedrijfszekerheid, waaronder minimaal: ○ Assetmanagement; ○ Back-up en Restore; ○ Business Continuïteitsmanagement; ○ Risicomanagement; ○ Changemanagement; ○ Autorisatie en toegangsprocedure; ○ Logging en Monitoring; ○ Incidentmanagement en response; ○ Malware, patching, hardening, versleuteling procedures. • Updates belangrijke (besturings)software; • Toegangsbeveiliging; • Virusbescherming; • Firewalls (invullen verkeersstromen tabel¹ door Leverancier);

¹ In de verkeerstromen tabel wordt bij start van de implementatie beschreven welke IP-adressen, poortnummers et cetera worden gebruikt tussen zender en ontvanger, in zowel de acceptatie als de productie omgeving.

	• Inrichten van een toereikend recovery proces waar back-up en restore onderdeel van uit maken; – Er moet op reguliere basis (tenminste 1 x per jaar) worden aangetoond dat het terugzetten (restore) van de backups (volledige Oplossing) succesvol verloopt, dit uiteraard in een specifiek daarvoor ingerichte omgeving, dus niet direct in Acceptatie-/ of Productie omgevingen; • Veiligheidseisen andere overheden of instanties; • Calamiteitenplannen; • Uitwijkplannen.
T-E56	Oplostijden worden in een prioriteringstabel in de SLA opgenomen.
T-E57	De SLA bevat een procedure waarmee aangetoond wordt op welke wijze voldaan wordt aan audits conform het 3 Lines model.

2.3 Eisen Privacy en Informatiebeveiliging (PIV)

NUMMER	OMSCHRIJVING
PIV-E1	Leverancier garandeert te voldoen aan het vigerende privacybeleid (bijlage 12) en informatiebeveiligingsbeleid (bijlage 13) van gemeente Hoeksche Waard, en de Componentarchitectuur Authenticatie & autorisatie en Beveiliging en NCSC-ICT-Deel1&2-beveiligingsrichtlijn webapplicaties. Leverancier zorgt ook voor passende technische en organisatorische maatregelen om vertrouwelijkheid en integriteit van (ICT-) systemen en informatie te waarborgen conform het voornoemde beleid. Dit beleid is van toepassing op alle ketenpartners (in welke hoedanigheid dan ook) en (sub-) verwerkers.
PIV-E2	Leverancier garandeert dat de ICT Prestatie gedurende de gehele contractperiode incl. verlengingen volledig en ondubbelzinnig voldoet, en gedurende de gehele looptijd van de overeenkomst blijft voldoen, ook in het geval van veranderende wet- en regelgeving, aan alle niet-functionele en technische vereisten.
PIV-E3	Leverancier zorgt ervoor dat (meta)data van gemeente Hoeksche Waard strikt gescheiden zijn van (meta)data van andere klanten van leverancier
PIV-E4	Leverancier mag geen (meta)data van gemeente Hoeksche Waard verwerken voor eigen doeleinden zonder voorafgaande, schriftelijke toestemming van Opdrachtgever..
PIV-E5	Leverancier zorgt ervoor dat m.b.t. de omgeving waarin de data binnen de ICT Prestatie worden verwerkt, passende technische en organisatorische maatregelen zijn genomen om te kunnen voldoen aan de wettelijke eisen waaraan de Aanbestedende Dienst moet voldoen. Hiervoor geldt de BIO en ook alle toekomstige wettelijke vereisten. Leverancier sluit een VNG standaard verwerkersovereenkomst met opdrachtgever (zie bijlage 5). Hierin staan de privacy, security en informatiebeheervoorwaarden specifiek benoemd. Na gunning van de opdracht wordt in onderlinge overeenstemming invulling gegeven aan de verwerkersovereenkomst.
PIV-E6	Opdrachtgever is aan te merken als Verwerkingsverantwoordelijke in de zin van de Algemene Verordening Gegevensbescherming (AVG). Leverancier is aan te merken als Verwerker in de zin van de Algemene Verordening Gegevensbescherming (AVG). Leverancier gebruikt de door opdrachtgever verstrekte en in het kader van de (uitvoering van de) overeenkomst ontvangen – al dan niet bijzondere – persoonsgegevens slechts voor het verrichten van de Prestatie zoals omschreven en vastgelegd in de overeenkomst. Deze persoonsgegevens gebruikt leverancier niet voor andere doeleinden, al dan niet commercieel, dan beschreven in de opdrachten voor het verrichten van de Prestatie, evenmin voor eigen (verdere dan wel door-) ontwikkeling van producten, diensten en/of prestaties. De betrokken persoonsgegevens mogen niet (verder) worden verwerkt, verstrekt, uitgewisseld en gedeeld met derden, tenzij door opdrachtgever op schriftelijk verzoek van Inschrijver daartoe uitdrukkelijke voorafgaande schriftelijke toestemming is gegeven. In dit kader maken Partijen derhalve onderhavige afspraken over de verwerking van persoonsgegevens (verwerkersovereenkomst conform model gemeente Hoeksche Waard), in het bijzonder op het gebied van informatiebeveiliging en gegevensbescherming.
PIV-E7	Leverancier garandeert compliant te zijn aan geldende en van toepassing zijnde landelijke en Europese wet- en regelgeving (en internationale) standaarden en normen voor

	gegevensbescherming en informatiebeveiliging, waaronder in ieder geval de AVG, en daarnaast aan de BIO of voor kwaliteitsmanagementsysteem ISO-certificering (ISO27001) of NEN normen (NEN-7510).
PIV-E8	Bij gebruik van (sub)verwerkers / onderaannemers gelden dezelfde beveiligingseisen als voor de leverancier. De Inschrijver is verantwoordelijk voor de borging bij de (sub)verwerkers / onderaannemer van de gemaakte afspraken.
PIV-E9	Ten behoeve van authenticatie en autorisatie (rollen) van gebruikers dient de ICT Prestatie te kunnen koppelen met bestaande identity providers van de Aanbestedende Dienst op basis van ADFS en de SAML2 standaard dan wel OpenID Connect en oAuth2.
PIV-E10	Alle gegevens (data en metadata) zijn en blijven te allen tijde eigendom van de gemeente ook na beëindiging van de overeenkomst. De gemeente kan deze gegevens op elk moment opvragen, waarna Leverancier deze onmiddellijk beschikbaar zal stellen.
PIV-E11	Persoonsgegevens worden verwerkt en opgeslagen in één van de volgende landen (dit geldt tevens voor door leverancier ingeschakelde derde partijen): binnen de EU plus Noorwegen, Liechtenstein, IJsland (E.E.R), of in een ander land, mits aldaar passend en aantoonbaar privacybeschermingsniveau is gewaarborgd van een vergelijkbaar niveau als dat van de EU.
PIV-E12	Leverancier garandeert dat relevante wetswijzigingen worden opgevolgd en deze wijzigingen op functioneel, beveiligings- en/of technisch niveau per ingangsdatum effectief zijn en blijven gedurende de looptijd van de overeenkomst in de betreffende (ICT-) systemen. In het geval er dergelijke wijzigingen worden doorgevoerd zullen Partijen elkaar daarover voorafgaand schriftelijk informeren.
PIV-E13	Leverancier moet gemeente en/of door een daartoe door gemeente aangewezen derde partij toegang geven tot de logfiles en audit trails indien gewenst door gemeente.
PIV-E14	De leverancier is verplicht per omgaande beveiligingsincidenten te melden bij de in de verwerkersovereenkomst aangegeven contactpersoon van gemeente. Potentiële datalekken dienen binnen 24 uur na ontdekking aan gemeente Hoeksche Waard gemeld te worden. Hierbij wordt door Leverancier alle relevante informatie verstrekt aan de gemeente. Op verzoek van opdrachtgever worden logging gegevens en rapportages over informatiebeveiliging geleverd door Leverancier.
PIV-E15	Leverancier is verplicht mee te werken aan (IT)audits van Opdrachtgever. De opdrachtgever behoudt de mogelijkheid om zelf audits uit te (laten) voeren alsook het (laten) uitvoeren van een penetratietest. Aanvullend geldt dat opdrachtgever verplicht is de volgende mate van Assurance moet geven aan de opdrachtgever behorend bij BBN2+ classificatie: ISAE 3402 Type II / SOC 2 Type II verklaring of gelijkwaardige TPM's." (Opzet, bestaan & werking).
PIV-E16	Er kan een Risicoanalyse (RIA) en/of DPIA op de betreffende ICT Prestatie plaatsvinden. Mogelijk volgen er uit deze RIA en/of DPIA aanvullende security, privacy en/of informatiebeheermaatregelen die door de leverancier nageleefd dienen te worden.
PIV-E17	Leverancier voldoet aan de bepalingen uit de Archiefwet.
PIV-E18	Bij beëindiging van de contractrelatie zal Leverancier alle gegevens in een gangbaar en bruikbaar format zorgvuldig, tijdig en volledig beschikbaar stellen aan de opdrachtgever dan

	wel, na schriftelijke toestemming van opdrachtgever, aan een opvolgende dienstverlener. Ook na beëindiging van de overeenkomst/werkzaamheden zal leverancier eventuele kennis van, en gegevens over, personeelsleden en andere bedrijfsgegevens als strikt vertrouwelijk blijven beschouwen en niet aan derden verstrekken tenzij daartoe een wettelijke verplichting bestaat. Na beëindiging van de overeenkomst dient Leverancier, na overleg, de gegevens van de opdrachtgever in haar eigen bedrijfshuishouding te vernietigen binnen de daarvoor geldende wettelijke kaders.
PIV-E19	Leverancier draagt bij beëindiging van de overeenkomst alle informatie, documentatie en andere bescheiden over aan de opdrachtgever, waar de opdrachtgever redelijkerwijs om kan verlangen en/of wat leverancier vanuit zijn expertise redelijkerwijs opdrachtgever dient te verstrekken behoudens beperkingen binnen wet- en regelgeving. Dit teneinde van een soepele exit.

3. Wensen

ALGEMEEN	
F-W1	Rapportages in de applicatie kunnen worden uitgevoerd in huisstijl.
F-W2	Normen in de applicatie kunnen worden voorzien van hulpteksten, juridische onderbouwing, werkinstructie.
F-W3	De applicatie bevat de functionaliteit voor import van normensets vanuit een Excel bestand.
PROCESSEN	
F-W4	De applicatie bevat de functionaliteit om processen weer te geven en uit te printen in huisstijl.
F-W5	De applicatie biedt mogelijkheid om de NVVB-processen te importeren.
RISICOMANAGEMENT	
F-W6	De applicatie bevat de functionaliteit voor een risicokaart/ risicomatrix.
F-W7	De applicatie bevat de functionaliteit voor het berekenen van de benodigde weerstandscapaciteit aan de hand van Monte Carlo simulatie.
AVG	
F-W8	De applicatie ondersteunt een DPIA-model voor het vastleggen van een DPIA (evt. zelf een DPIA-model invoeren).
INTERNE CONTROLE	
F-W9	De applicatie bevat de functionaliteit om achterliggende documentatie per onderzoek veilig te stellen of op te slaan bij het onderzoek