



Programma van Eisen (PvE)

Aanbesteding applicatie Vergunning, Toezicht, Handhaving functionaliteiten

In dit document staan eisen benoemd. Het document bestaat in totaal uit 10 tabbladen incl. inleiding.
Eisen worden aangeduid met de code "E1-1", "E2-1" etc.

De indeling in dit document is als volgt:

Tabblad	Omschrijving	Toelichting
E1	Algemeen	Betreft algemene eisen t.a.v. Leverancier én de geboden Oplossing
E2	(E)- dienstverlening / functionaliteit	Betreft eisen t.a.v. eDiensten en functionaliteit
E3	Architectuur en Techniek	Betreft eisen t.a.v. architectuur, techniek en Koppelingen
E4	Beveiliging en Privacy	Betreft eisen t.a.v. beveiligings- en privacy aspecten
E5	Archivering	Betreft eisen t.a.v. wet- en regelgeving rondom archivering
E6	Functioneel Beheer	Betreft eisen t.a.v. het (functioneel) beheer
E7	SLA	Betreft eisen t.a.v. servicelevels, continuïteit, responsetijden
E8	Business Intelligence (BI)	Betreft eisen t.a.v. rapportages, dashboards en datamodel
E9	Implementatie	Betreft eisen t.a.v. installatie, training, Conversie en oplevering

Nr. E1	Eisen - Algemeen	Toelichting
E1-1	De standaard SaaS oplossing is flexibel van opzet, wordt gedurende de looptijd van de Overeenkomst verder ontwikkeld en verbeterd en houdt gelijke tred met wijzigingen in standaarden, koppelvlakken/aansluitingen op landelijke voorzieningen, met wijzigingen van deze landelijke voorzieningen (blijven voldoen aan actueel Logisch Ontwerp DigiD/eIDAS, et cetera) en wijzigingen in wet- en regelgeving om de functionaliteit van het systeem te waarborgen. De ict oplossing beweegt blijvend mee met relevante vakinhoudelijke Nederlandse wet- en regelgeving, in het bijzonder, maar niet beperkt tot, de Omgevingswet en het Digitaal stelsel omgevingswet.	
E1-2	Alle gedurende de looptijd van de Overeenkomst ontwikkelde functionaliteiten komen zonder meerkosten beschikbaar voor de gemeente. Hiermee worden alle (aanvullende) modules bedoeld die beschikbaar zijn en nog beschikbaar komen.	Dit geldt voor de jaarlijkse/structurele kosten, niet voor de eenmalige implementatiekosten. Onder functionaliteiten bedoelen we Updates en Upgrades zoals omschreven in de GIBIT 2025 voorwaarden.
E1-3	Leverancier waarborgt dat de aangeboden ict oplossing niet meer dan één major versie achterloopt ('neerwaarts compatibiliteit') op de open standaarden van het Forum Standaardisatie (www.forumstandaardisatie.nl). Aanpassingen in de hierboven genoemde standaarden worden binnen 6 maanden nadat de aanpassingen als nieuwe standaard zijn gepubliceerd op genoemd forum of Gemma online door Leverancier verwerkt. Daarnaast wordt de oude versie van de standaard nog minimaal 12 maanden ondersteund.	
E1-4	Op basis van het afgesloten contract garandeert Leverancier dat de ict oplossing, gedurende de contractperiode zal worden doorontwikkeld. Hieronder wordt, naast correctief en preventief Onderhoud, ook verstaan dat binnen de ict oplossing innovatief Onderhoud wordt uitgevoerd om te blijven voldoen aan geldende wet- en regelgeving. Zie artikel 10 e.v. van de GIBIT 2025.	
E1-5	Geboden ict oplossing is workflow gestuurd. Legt bedrijfsprocessen vast in heldere digitale routes, van start tot eindresultaat	
E1-6	De ict oplossing waarborgt de integriteit van informatie door te garanderen dat gegevens accuraat, betrouwbaar, volledig en ongewijzigd blijven gedurende de hele levenscyclus, ongeacht hoe ze worden opgeslagen, verzameld of gebruikt.	
E1-7	Er wordt minimaal een test- en productieomgeving beschikbaar gesteld, beiden inclusief alle in dit Programma van Eisen en wensen geëiste en later toegevoegde Koppelingen. De testomgeving geeft ten allen tijde een representatie van de productieomgeving en dient continu beschikbaar te zijn (ook tijdens en na de implementatieperiode).	
E1-8	De test- en productieomgeving hebben gescheiden datasets.	
E1-9	De testomgeving bevat relevante data van Opdrachtgever. Hierin mag uitsluitend gebruik worden gemaakt van fictieve persoonsgegevens.	
E1-10	De testomgeving werkt geïsoleerd en is niet gekoppeld aan de productieomgeving.	
E1-11	De ict oplossing beschikt over een webbased userinterface (dus géén Citrix of gelijkwaardige omgeving) zonder beperking van functionaliteit. En werkt in de laatste versie -1 van de browsers Edge en Chrome.	De applicatie werkt plaats onafhankelijk, wat betekent dat dit zowel geldt voor de thuiswerkplek, als op kantoor, of welke locatie dan ook, zonder gebruik te maken van Citrix of andere soortgelijke oplossingen.
E1-12	De ict oplossing moet in meerdere tabbladen binnen de webbrowser gelijktijdig te openen zijn. Denk hierbij aan het vergelijken van dossiers binnen de ict oplossing.	
E1-13	Voor alle onderdelen in de ict oplossing dienen eenduidige procedures, schermen, menuopbouw te zijn.	
E1-14	De ict oplossing dient benaderbaar te zijn via een "fully qualified domain name" via een beveiligde verbinding.	
E1-15	De gebruikersinterface van de ict oplossing is volledig Nederlandstalig.	
E1-16	De leverancier is zonder enig voorbehoud verantwoordelijk voor back-up, restore, recovery en uitwijk met betrekking tot de gehele ICT-oplossing. Hierbij geldt een RPO van maximaal 24 uur en een RTO van maximaal 4 uur. Inschrijver moet deze onderdelen jaarlijks testen en de resultaten hiervan kenbaar maken aan Opdrachtgever	
E1-17	Leverancier zorgt ervoor dat ten tijde van de Implementatie (inclusief nazorg) er binnen 24 uur inhoudelijk antwoord wordt gegeven op vragen die spelen tijdens implementatie.	
E1-18	De ict oplossing biedt de mogelijkheid om te kunnen exporteren naar open standaarden (bijvoorbeeld Excel, Word en pdf)	

Nr. E2	Eisen Omschrijving Functionaliteit	Toelichting
Automatische zaakaanmaak		
E2-1	De ict oplossing maakt bij ontvangst van een aanvraag via het Digitaal Stelsel Omgevingswet (DSO) automatisch en zonder handmatige tussenkomst een zaak aan in het zaaksysteem. De zaak wordt automatisch gekoppeld aan het juiste zaaktype op basis van vooraf ingestelde configuratie of routeringsregels.	
E2-2	De ict oplossing moet automatisch een zaak kunnen aanmaken, wanneer een aanvraag binnenkomt die betrekking heeft op een andere behandeldienst, maar waarvan de gemeente het bevoegd gezag is. Dit moet zonder handmatige tussenkomst van medewerkers kunnen plaatsvinden. In de zaak moet duidelijk zichtbaar zijn dat de behandeldienst bij een andere organisatie ligt.	Showcase
E2-3	De aangemaakte zaak wordt volledig en correct gevuld met alle relevante gegevens uit de DSO-aanvraag.	
E2-4	De ict oplossing wijst de zaak automatisch toe aan de juiste behandeldienst, conform het bevoegd gezag of ingestelde routeringslogica. Het is mogelijk om handmatig het bevoegd gezag of de behandeldienst te wijzigen.	
E2-5	Aanvullingen die door het Digitaal Stelsel Omgevingswet (DSO) worden aangeleverd, worden automatisch en direct toegevoegd aan de reeds bestaande juiste zaak binnen het zaaksysteem. Het systeem herkent op basis van unieke DSO-kenmerken bij welke zaak de aanvulling hoort. De behandelaar van de betreffende zaak ontvangt automatisch een notificatie zodra een aanvulling via het DSO is ontvangen.	
E2-6	Intrekkingen die via het DSO worden ingediend, worden automatisch verwerkt in de betreffende zaak. Het systeem koppelt de intrekking aan de juiste bestaande zaak. Alle bijbehorende gegevens worden in de zaak opgeslagen. De behandelaar van de betreffende zaak ontvangt automatisch een notificatie zodra een intrekking via het DSO wordt ontvangen.	
E2-7	De oplossing moet op basis van specifieke veldwaarden/acties in een zaak automatisch een nieuwe zaak kunnen aanmaken van het juiste zaaktype, deze direct logisch koppelen aan de bronzaak, en relevante gegevens zoals relaties, locatie en zaakomschrijving meenemen naar de nieuwe zaak.	
Zaakdossier		
E2-8	Binnen de ict oplossing moet er bij het configureren van een zaaktype de mogelijkheid zijn om per zaaktype eigen velden te maken met aanduiding van verplicht of niet verplicht.	
E2-9	De ict oplossing moet de mogelijkheid bieden om zaaktypes, adviezen, taken, controles, documenten als vertrouwelijk aan te merken, zodat alleen de mensen uit het team of die daar gerechtigd tot zijn deze gegevens in kunnen zien.	
E2-10	De ict oplossing moet de juiste legesverordening automatisch selecteren aan de hand van de startdatum van de zaak.	
E2-11	In de ict oplossing moeten de leges automatisch berekend kunnen worden en ook handmatig kunnen worden toegevoegd.	Showcase
E2-12	In de oplossing moeten behandelaars procedures toe kunnen voegen aan een zaak, op het moment dat een procedure aan een zaak wordt toegevoegd of gewijzigd dient de fatale datum automatisch te worden aangepast.	
Portaalfunctionaliteit		
E2-13	De ICT-oplossing moet kunnen integreren met het "Mijn Molenlanden"-portaal binnen ons zaaksysteem Djuma. Alternatief mag de leverancier een eigen portaal aanbieden, mits dit naadloos kan koppelen met Djuma en voldoet aan onze functionele en beveiligingseisen. Het portaal moet gebruikmaken van de door de overheid erkende authenticatiemiddelen, namelijk DigiD, eIDAS en eHerkenning.	Werkend bij livegang
Werkvoorraad		
E2-14	Binnen de ict oplossing dient er een werkvoorraad scherm te zijn dat per zaak de volgende gegevens kan tonen toont: Zaaktype, Omschrijving, Locatie, Uniek zaaknummer, DSO nr, Status, Fatale datum en een doorklikmogelijkheid naar de betreffende zaak.	
E2-15	Binnen de ict oplossing moet binnen de werkvoorraad een zoekfunctie aanwezig zijn.	
E2-16	Een zaak die de status heeft van 'zaak afgerond' of gearhiveerd, komt niet meer voor in de actuele werkvoorraad van de behandelaar(s).	
Adviezen/Controles/Taken		
E2-17	Binnen de ict oplossing moeten uitgezette controles, taken of adviezen in de zaak zichtbaar zijn met de volgende data/kenmerken per controle/taak/advies: Soort advies, Behandelaar Controle/Taak/Advies, Datum aangevraagd, Verwachte einddatum, Werkelijke einddatum, Resultaat en Toelichting	
E2-18	De ICT oplossing moet het mogelijk maken om agenda's aan te maken en af te handelen. Bij een zaak moet een agendadatum kunnen worden vastgelegd. Op basis van deze datum moet een gebruiker vanuit het systeem een agenda kunnen genereren en exporteren met alle zaken die aan die datum zijn gekoppeld. Het systeem moet kunnen vastleggen of een agenda en de bijbehorende zaken zijn afgehandeld.	
E2-19	Binnen de ict oplossing moet Opdrachtgever de mogelijkheid hebben om door het hele systeem te zoeken, zonder begrenzingen en de mogelijkheid om door te klikken op het resultaat.	
E2-20	Bij het zoeken binnen de ICT oplossing worden alle gevonden zaken getoond met vermelding van Zaaknummer, Zaaktype, Locatie, Aanvraagdatum, Zaaksysteemnr, Behandelaar, Status	
E2-21	Bij een uitgevoerde zoekopdracht binnen de ict oplossing wordt er duidelijk getoond hoeveel zaken/resultaten er gevonden zijn	
E2-22	Binnen de ict oplossing moet het mogelijk zijn om in een oogopslag alle lopende en gesloten zaken op een locatie te kunnen raadplegen.	
Zaakdocumenten		
E2-23	De ict oplossing moet gebruikers in staat stellen om documenten direct binnen het systeem te kunnen bewerken, zonder dat deze eerst lokaal hoeven te worden gedownload, gewijzigd en opnieuw geupload. Dit geldt voor zowel nieuw aangemaakte documenten als reeds bestaande documenten die deel uitmaken van een zaak of dossier.	
E2-24	Binnen de ict oplossing moet er de mogelijkheid zijn om vanuit de zaak meerdere documenten toe te voegen aan een te maken emailbericht	
E2-25	Binnen de ict oplossing is binnen het dossier een zoekfunctie aanwezig.	
E2-26	Binnen de ict oplossing moet het mogelijk zijn om de toelichting bij het bestand aan te passen	
E2-27	Binnen de ict oplossing is het mogelijk om één of meerdere documenten/emails aan de zaak toe te voegen te slepen vanuit de verkenner of vanuit een mailprogramma.	
Sjabloon inrichting		
E2-28	De ict oplossing moet de mogelijkheid bieden om sjablonen en hun opmaak in te laten richten door de functioneel beheerder - ook moet een eindgebruiker de mogelijkheid hebben om na het generen nog wijzigingen op het gegenereerde document aan te brengen.	
E2-29	Binnen de ict oplossing moeten alle velden, inclusief zelfgemaakte, eenvoudig te gebruiken zijn in de sjablonen.	
E2-30	Binnen de ict oplossing is het mogelijk om 'lijstjes' te gebruiken in de sjablonen. Denk hierbij aan de activiteiten bij een omgevingsvergunningsaanvraag.	
Controlebezoeken		
E2-31	De toezichthouder moet in de toezichtzaak controlebezoeken vast kunnen leggen (datum, type controle en constatering).	

Rapportage/analyse		
E2-32	De Opdrachtgever kan zonder tussenkomst van de leverancier zelf rapportages vanuit de Oplossing creëren en opslaan. Dit geldt voor zowel beheerders als eindgebruikers.	
E2-33	De Oplossing biedt de mogelijkheid om (door de functioneel beheerder) op maat gemaakte rapportages aan te bieden aan eindgebruikers	
E2-34	Vanuit de Oplossing kan eenvoudig een gemaakte rapportage worden geëxporteerd voor verdere externe verwerking.	
E2-35	De Oplossing biedt een gestructureerde (en geautoriseerde) toegang tot productiedata voor gebruik in externe systemen als een datawarehouse of BI-tooling. Opdrachtgever kan hiermee zelfstandig de benodigde data benaderen en/of exporteren. Wijzigingen in het datamodel worden zo vroeg mogelijk voor release aangekondigd.	

Nr. E3	Eisen Omschrijving - Architectuur en Techniek	Toelichting
E3-1	De ict oplossing moet koppelen met de Azure Active Directory van Opdrachtgever.	
E3-2	De ict oplossing moet Single Sign On ondersteunen in relatie tot de Azure Active Directory.	
E3-3	De ict oplossing moet 2 factor authentication ondersteunen.	
E3-4	De data moet voldoen aan het Gemeentelijk Gegevensmodel (GGM) Het GGM geldt als referentiemodel. Volledige aansluiting op het GGM geldt niet als zelfstandige uitsluitingsgrond. Gemotiveerde afwijkingen en functioneel gelijkwaardige gegevensstructuren blijven mogelijk.	
E3-5	De ict oplossing moet koppelen met de BRP voor het ophalen en actueel houden van authentieke natuurlijke personen.	
E3-6	De ict oplossing moet koppelen met de KVK API voor het ophalen van authentieke niet natuurlijke persoonsgegevens.	Werkend bij livegang
E3-7	Binnen de ict oplossing wordt het overlijden van aanvrager/betrokkenen altijd getoond in lopende zaken	
E3-8	De ict oplossing moet koppelen met het Digitaal Stelsel Omgevingswet (DSO) (Triggerbericht, STAM en samenwerkingsvoorziening) om zo aanvragen vanuit het DSO te ontvangen, verwerken en de verschillende zaaktypes automatisch worden aangemaakt.	
E3-9	Binnen de ict oplossing moeten alle gegevens die meekomen vanuit het DSO te mappen zijn naar velden binnen het zaakdossier zodat gebruikers geen gegevens handmatig hoeven toe te voegen.	
E3-10	De ict oplossing moet koppelen met DROP inclusief het publiceren van openbare documenten en GML's voor publicatie op regels op de kaart.	
E3-11	De ict oplossing moet alle financiële gegevens zoals leges en heffingen beschikbaar kunnen stellen aan het financiële pakket ERPx (van Unit4).	
E3-12	Aanvullend op voorgaande eis moet het mogelijk zijn om de velden kenmerken binnen een financiële export zelf aan te passen op de eisen van het financiële pakket.	
E3-13	De functioneel beheerder van Opdrachtgever moet de mogelijkheid hebben om (binnen de ict oplossing) berichtenverkeer van Koppelingen te monitoren en daarop te kunnen acteren (herzenden van berichten bijvoorbeeld) om het te herstellen.	
E3-14	De ict oplossing voldoet aan de eisen die gesteld worden vanuit de Wmebv.	
E3-15	De ict oplossing heeft ervaring met migraties vanuit andere systemen en is in staat een plan op maat te bieden zodat aanvragen altijd ingediend kunnen worden ook tijdens implementatie periode. Ook de verzoeken die niet verwerkt zijn in de oplossing. Deze verzoeken moeten alsnog kunnen worden aangeboden binnen de oplossing.	
E3-16	Binnen de ict oplossing is er de mogelijkheid om alle verzoeken vanuit het DSO te raadplegen	
E3-17	Binnen de ict oplossing moet het mogelijk zijn om zaaktypes in te richten op basis van I-navigator, ZTC omgevingswet en daar eventueel nog maatwerk op te kunnen aan te brengen.	
E3-18	De ict oplossing kan de kaartlagen van een externe gisviewer (kaartviewer) in de applicatie integreren.	
E3-19	De ict oplossing moet koppelen met het zaaksysteem Djuma	Werkend bij livegang

Nr. E4	Beveiliging	Toelichting
E4-1	De verwerking en opslag van data vindt encrypted en fysiek plaats binnen de Europese Economische Ruimte (EER)	
E4-2	Leverancier dient aan te kunnen tonen dat de gestelde (ICT-)kwaliteitsnormen en eisen aan beveiliging van (persoons)gegevens zijn geborgd in de gehele Leveranciersketen van de ICT-prestatie. Denk hierbij aan een TPM verklaring of andere auditverklaringen c.q. ISO-certificeringen van de toeleveranciers.	
E4-3	In de Overeenkomst zal worden beschreven op welke fysieke locaties de data van Opdrachtgever wordt/is ondergebracht. Zowel productie-omgeving als back-up.	
E4-4	De volgende risicovolle situaties zijn niet toegestaan zonder expliciete goedkeuring van Opdrachtgever: - Gebruik maken van een back-up dienst (al dan niet van derden) waarbij niet 100% zeker is dat de data binnen de Europese Economische Ruimte (EER) blijft. - Gebruik maken van beheerdiensten van partijen gevestigd buiten de EER. - Hergebruik van gemeentelijke data voor test- en acceptatiedoelen, zonder expliciete schriftelijke toestemming van Opdrachtgever. - Opslag van gemeentelijke data buiten de beveiligde omgeving, bijvoorbeeld op laptops van medewerkers om 'even' wat te testen, fouten te zoeken etc. Op voorhand zal Opdrachtgever geen toestemming geven voor deze situaties. Indien Leverancier aan één van bovenstaande risico's niet voldoet, dient hij dit kenbaar te maken via de Nota van inlichtingen.	
E4-5	De fysieke locaties van waar de ict oplossing wordt gehost is beveiligd tegen toegang door onbevoegden. De locatie is adequaat - minimaal naar marktstandaarden - beveiligd tegen onheil van buitenaf, waaronder in ieder geval weersomstandigheden en vandalisme.	
E4-6	De ict oplossing ondersteunt Roll Based Access Control (RBAC). Rechten hangen aan rollen en gebruikers worden gekoppeld aan rollen.	
E4-7	Gebruikers dienen alleen de gebruikersinterfaces/-menu's en onderliggende gegevens te zien waarvoor zij zijn geautoriseerd. Denk hierbij aan het principe 'need to know /least privileged'.	
E4-8	Er dient een totaaloverzicht (op elk moment en direct) beschikbaar te zijn van autorisaties van zowel Leverancier als Opdrachtgever verdeeld naar gebruikers per rol en autorisaties per rol (in het kader van de audittrail).	
E4-9	De ict oplossing en daarmee samenhangende diensten van Leverancier stellen Opdrachtgever in staat om te voldoen aan de dan geldende Baseline Informatiebeveiliging Overheid (BIO2).	
E4-10	Leverancier zal een geldend ISO 27001 certificaat inclusief Verklaring van Toepasselijkheid of een ISAE 3402 SOC type II certificaat moeten overleggen.	
E4-11	De infrastructuur en organisatie van Leverancier zijn adequaat beveiligd volgens ISO/IEC 27001 en ISO/IEC 27002 of vergelijkbaar. Leverancier is bereid op verzoek een verklaring van getrouwheid (of vergelijkbaar) te verkrijgen via een onafhankelijke derde partij (TPM).	
E4-12	Alle software (front-end en backend) behorend tot de (cloud)dienst is volgens relevante standaarden beveiligd, conformeert zich telkens aan de laatste bekende beveiligingsinzichten en is blijvend van voldoende kwaliteit. Richtlijnen van de Autoriteit Persoonsgegevens (AP), Nationaal Cyber Security Centrum (NCSC), Informatiebeveiligingsdienst voor gemeenten (IBD), Forum Standaardisatie en Open Web Application Security Project (OWASP) zijn hierbij normstellend.	
E4-13	De ict oplossing ondersteunt Domain Name System Security Extensions (DNSSEC) voor de webservices.	
E4-14	Er dient altijd gebruik gemaakt te worden van beveiligde internetverbindingen waarbij de richtlijnen van het NCSC worden toegepast.	
E4-15	De logging biedt voldoende inzicht in het bijhouden, uitwisseling van-, en selecties van gegevens om het gebruik van een gegeven door een applicatie te kunnen achterhalen en hierop te signaleren of acteren. Logregels mogen op geen enkele wijze kunnen worden bewerkt / gemanipuleerd. Onderdelen die minimaal in de logging opgenomen dienen te zijn: - Gebruikerslogging - Datum/tijd van actie - Gebruikersnaam of gebruiker ID - Uitgevoerde handeling - Object waarop de handeling werd uitgevoerd - Handelingen van gebruikers met speciale bevoegdheden - Systeemlogging - Opgetreden fouten (error log) - (Poging tot) ongeautoriseerde toegang - (Poging tot) wijziging van beveiligingsinstellingen In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, etc.). In de logregel mogen ook geen persoonsgegevens worden opgenomen uit systemen van Opdrachtgever zelf (dus wel gebruikersnamen of inlog accounts).	
E4-16	De ict oplossing moet bovenstaande systeem logging beschikbaar stellen aan de SIEM oplossing van Opdrachtgever. Denk hierbij aan het uitlezen van de logging van de ict oplossing via een API. Het is mogelijk om logregels direct te versturen naar een door Opdrachtnemer aangewezen systeem waar ze verzameld en geanalyseerd kunnen worden (log collector, SIEM/SOC) (BIO 12.4.1.3 / BIO2 8.15; BBN2).	
E4-17	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald op tenminste 6 maanden (BIO 9.4.4.2 / BIO2 8.15). Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd. Indien een beveiligingsincident is opgetreden, is de bewaartermijn 5 jaar (conform resultaat 15.1). Daaronder vallen dan ook de monitoringsgegevens die horen bij de informatie waar het incident betrekking op heeft.	
E4-18	De logging dient alleen beschikbaar te zijn voor daartoe geautoriseerde medewerkers. Deze autorisaties zijn via de Oplossing inregelbaar door Opdrachtgever.	
E4-19	Binnen een instelbare periode is het ongewijzigd beschikbaar blijven van loginformatie gewaarborgd. Na deze periode wordt loginformatie conform geldende archiefwet en -regelgeving vernietigd (BIO 12.4.2.2 / BIO2 8.15).	
E4-20	De functioneel beheerder kan bovengenoemde logging zelfstandig raadplegen.	

	Privacy-by-design Systeemeisen	
E4-21	De infrastructuur, de geleverde dienst en organisatie van Leverancier voldoen aan de voorwaarden genoemd in de Algemene verordening Gegevensbescherming (AVG) en de uitvoeringswet algemene verordening gegevensbescherming (UAVG).	
E4-22	In de ict oplossing zijn functionaliteiten opgenomen voor Opdrachtgever, om aan drie AVG taken invulling te geven: 1) transparantie van gegevens, 2) recht op inzage en 3) gegevensminimalisatie.	
E4-23	Op verzoek van Opdrachtgever dient Leverancier een Data Protection Impact Assessment (DPIA) aan te leveren aan Opdrachtgever en indien die niet beschikbaar is mee te werken aan het uitvoeren hiervan op de ict oplossing. Dit moet gebeuren voordat de applicatie echte persoonsgegevens bevat.	
E4-24	De leverancier draagt zorg voor transparantie, third party assurance en continuïteitsborging.	
E4-25	De leverancier kan zorgdragen dat een derde partij de dienst over kan nemen bij uitval van de aanbieder of beëindiging van het contract, op basis van de beschikbare documentatie en ontwerp.	
	privacy / derde landen / AVG-documentatie	
E4-26	De leverancier dient te borgen dat opslag en primaire verwerking van persoonsgegevens uitsluitend binnen de EU/EER plaatsvinden. Doorgifte van persoonsgegevens buiten de EU/EER is alleen toegestaan indien dit juridisch is toegestaan, volledig transparant wordt gemaakt en is voorzien van passende waarborgen conform geldende wet- en regelgeving.	
E4-27	De leverancier dient inzichtelijk te maken en aantoonbaar vast te leggen welke groepsmaatschappijen, subverwerkers en supportlocaties toegang hebben tot persoonsgegevens. Tevens moet de leverancier expliciet aangeven op basis van welke juridische grondslag eventuele doorgifte van persoonsgegevens buiten de EU/EER plaatsvindt, conform de geldende wet- en regelgeving.	

Nr. E5	Eisen - Archief en archiefbeheereisen	Toelichting
E5-1	De ict oplossing voldoet aan de geldende Archiefwet en daaruit vloeiende regelingen (o.a. de NEN-ISO 16175)	Wij dienen als gemeente te voldoen aan de archiefwet, zo ook de ict oplossing
E5-2	De ict oplossing voldoet aan TMLO/MDTO	Noodzakelijk om informatie te kunnen overbrengen naar het E-depot
E5-3	Informatieobjecten (een verzameling aan elkaar gerelateerde gegevens die als eenheid wordt behandeld) kunnen worden beheerd in de context van een zaakdossier.	Noodzakelijk voor beheer van onze informatie
E5-4	Aan de informatieobjecten (een verzameling aan elkaar gerelateerde gegevens die als eenheid wordt behandeld) moeten metadata over de achtergronden van de waardering en/of hoogte van de bewaartermijn kunnen worden toegevoegd.	Conform archiefwet
E5-6	De datum voor het vernietigen of overbrengen (naar E-depot) van informatie moet automatisch berekend kunnen worden.	Conform archiefwet
E5-7	Van informatieobjecten die voor vernietiging of overbrenging in aanmerking komen, moeten op basis van het jaar van vernietiging of overbrenging overzichten kunnen worden gecreëerd.	Conform archiefwet
E5-8	Informatieobjecten en bijbehorende metadata (op verschillende aggregatieniveaus: dossier en onderliggende documenten, bestanden) moeten onherstelbaar kunnen worden vernietigd. Dit op basis van de als zoekcriteria (metadata) opgegeven waardering/vernietigtermijn.	Conform archiefwet
E5-9	Van de vernietiging dient een verklaring te kunnen worden opgeleverd. Hierin wordt minimaal vermeld welke informatie is vernietigd, op welke wijze de vernietiging plaatsvondt, de omvang van de data (in bytes) en de bevestiging dat de vernietiging volledig is uitgevoerd.	Conform archiefwet
E5-10	Leverancier garandeert dat bij een back-up-recovery geen gegevens terug in productie worden gezet die formeel al vernietigd zijn.	
Exporteerbaarheid / overdraagbaarheid		
E5-11	Het moet mogelijk zijn om een export te maken van informatieobjecten, bijbehorende metadata en gekoppelde bestanden op basis van opgegeven zoekcriteria, ten behoeve van bijvoorbeeld overbrenging naar een E-depot of een andere applicatie. Bij een export kan de metadata mee geëxporteerd worden op een manier dat het verband tussen bestanden en metadata intact blijft.	
E5-12	Bij een export kan de metadata in een gangbaar machinaal leesbaar bestandsformaat meegeleverd worden, zoals XML.	
E5-13	Bij het archiveren van zaakdossier worden alle documenten automatisch in PDF/A omgezet en dus bevoren voor verdere bewerking	
E5-14	De leverancier moet in het kader van exit strategie kunnen borgen dat archiefwaardige gegevens/metadata volledig en bruikbaar exporteerbaar zijn, mede met het oog op exit en overdraagbaarheid naar een opvolgende leverancier.	

Nr. E6	Eisen - Applicatie en functionele beheer eisen	Toelichting
E6-1	Alle functionele beheertaken kunnen worden uitgevoerd, zonder dat dit invloed heeft op de werking van de ict oplossing voor de overige gebruikers. Gebruikers kunnen ingelogd blijven en volledig gebruik maken van de ict oplossing tijdens deze functionele beheerstaken.	
E6-2	De autorisatie dient op een effectieve en efficiënte wijze te worden ingericht.	De situatie waar Opdrachtgever naartoe wil groeien is dat wanneer een nieuwe medewerker in dienst komt, wanneer een medewerker van functie verandert of wanneer een medewerker uit dienst gaat, dat dit een geautomatiseerd proces triggert. Als op basis van de functie (RBAC) blijkt dat de gebruiker toegang moet hebben tot de applicatie, dat deze gebruiker automatisch wordt aangemaakt in de applicatie en ook direct de juiste rechten krijgt binnen de applicatie.
E6-3	Foutmeldingen in het systeem zijn eenduidig interpreteerbaar en herleidbaar	
E6-4	Ten behoeve van interne en externe audits dient elke wijziging te worden opgeslagen en gekoppeld te worden aan de desbetreffende gebruiker.	
E6-5	De aangeboden ICT oplossing moet het mogelijk maken dat nieuwe en bestaande zaaktypen én bijbehorende workflows volledig zelfstandig door functioneel beheer kunnen worden aangemaakt, ingericht en aangepast, uitsluitend via configuratie.	Showcase
E6-6	De ICT oplossing stelt de functioneel beheerder in staat om zelfstandig de legesverordening in te voeren, beheren en wijzigen, zonder afhankelijkheid van de leverancier. Deze functionaliteit moet standaard beschikbaar zijn binnen de applicatie.	
E6-7	De ICT oplossing stelt de gemeente in staat om op basis van vooraf configureerbare veldwaarden en/of acties binnen een zaak automatisch een nieuwe zaak van het juiste zaaktype aan te maken.	Showcase
E6-8	De functioneel beheerder dient zelf de logging en audittrail(rapportages) te kunnen raadplegen en exporteren.	
E6-9	Alle wijzigingen worden door Leverancier altijd eerst getest voordat deze in productie worden genomen.	
E6-10	Bij updates van de Programmatuur worden de doorgevoerde wijzigingen duidelijk omschreven in releasenotes. Deze worden tijdig, voorafgaand aan de update beschikbaar gesteld.	
E6-11	Het moet mogelijk dat de functioneel beheerder velden als verplicht invulveld aan kan merken. (in- en uitschakelbaar)	
E6-12	Het technisch beheer van de ict oplossing dient geheel verzorgd te worden door Leverancier.	Technisch applicatiebeheer betreft de werkzaamheden die nodig zijn voor het waarborgen van de ononderbroken goede werking van de SaaS-oplossing.
E6-13	Er dient op geen enkele wijze sprake te zijn van inlogmogelijkheden voor Leverancier of diens voor deze opdracht in te zetten derden (backdoor) waar Opdrachtgever niet van op de hoogte is. Toegang tot de omgeving gaat altijd na overleg vooraf.	
E6-14	Binnen de ict oplossing zijn de instellingen voor het automatisch publiceren flexibel in te richten (per zaaktype)	
E6-15	De ict oplossing bepaalt aan de hand van de inrichting welke dossiers automatisch moeten worden gepubliceerd	
E6-16	Binnen de ict oplossing zijn publicatiesjablonen vrij in te richten door de functioneel beheerder	
E6-17	Binnen de ict oplossing zijn publicaties die klaargezet zijn door het systeem door de gebruikers zelf te verwijderen	
E6-18	De ICT-oplossing biedt de gemeente volledig en actueel inzicht in alle verzoeken die via het Digitaal Stelsel Omgevingswet (DSO) zijn ingediend waarvoor de gemeente bevoegd gezag is. Dit geldt nadrukkelijk ook voor verzoeken waarvan de (gedeeltelijke) inhoudelijke behandeling is belegd bij externe behandeldiensten, zoals de omgevingsdienst. Indien een DSO verzoek niet automatisch is verwerkt tot een zaak, biedt de oplossing de mogelijkheid dat een functioneel beheerder dit verzoek handmatig kan verwerken tot een zaak binnen de gemeentelijke omgeving, zonder tussenkomst van de leverancier of koppelpartner en zonder aanvullende maatwerkactiviteiten.	Showcase

Nr. E7	Eisen- Service Level Agreement (SLA)	Toelichting
E7-1	De inschrijver dient bij inschrijving een concept-SLA of een SLA-respons aan te leveren. Deze dient aan te sluiten op de overeenkomst en te passen binnen de gemeentelijke contractkaders, waaronder de GIBIT 2025. De aangeleverde SLA mag geen afwijkingen bevatten ten opzichte van deze kaders.	
E7-2	De leverancier meldt de indexering voor het komende kalenderjaar uiterlijk vóór 1 augustus van het jaar voorafgaand aan het jaar waarin de indexering van kracht wordt. —Voor indexering geldt artikel 11.8 van de GIBIT 2025.	
E7-3	Leverancier verzorgt een door Nederlandstaligen bezette 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 Leverancier 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 17.30 uur. Voor ondersteuning door de helpdesk van Leverancier worden geen aanvullende kosten in rekening gebracht.	
E7-4	De helpdesk van Leverancier is verantwoordelijk voor de gehele behandeling van meldingen, incidenten m.b.t. de geboden oplossing volgens de procedure zoals vastgelegd in de Service Level Agreement (SLA). Opdrachtgever geeft bij het melden de prioriteit aan, Leverancier toetst deze. De prioriteit wordt door Leverancier aan Opdrachtgever gecommuniceerd. Bij verschil van de opgegeven Prioriteit informeert Leverancier Opdrachtgever hierover. Vervolgens wordt het incident met de vastgestelde Prioriteit behandeld. Indien geen overeenstemming wordt bereikt over de prioriteit treedt de escalatieprocedure in werking.	Daar waar Leverancier en Opdrachtgever van mening verschillen over de prioritering gaan deze hierover met elkaar in gesprek.
E7-5	De helpdesk zorgt voor relateren van incidenten aan reeds bekende problemen m.b.t. de geboden oplossing. Leverancier maakt voor Opdrachtgever inzichtelijk wanneer een incident in behandeling is genomen en wat de status van afhandeling is. Leverancier is eindverantwoordelijk voor het beheren van incidenten.	Bijvoorbeeld in de vorm van een online platform waarop functioneel beheer van Opdrachtgever op kan inloggen.
E7-6	Eventuele service windows, updates en releases zijn zoveel mogelijk buiten de reguliere kantoorwerk tijden (8:00 en 17:00) en indien afwijkend in overleg me de klant.	
E7-7	Op werkdagen van 07.00 - 22.00 uur wordt de beschikbaarheid van de geboden oplossing voor minimaal 99,5% per maand gegarandeerd, voor de overige uren van de werkweek en het weekend wordt dit voor minimaal 99,0% per maand gegarandeerd. Er wordt uitgegaan van een beschikbaarheid van de verbinding vanuit de gemeente van 99% waarbij gepland onderhoud niet wordt meegenomen. Leverancier levert 1 keer per kwartaal een rapportage aan betreffende de beschikbaarheid.	
E7-8	Diensten voor Onderhoud en ondersteuning, voor zover deze door Leverancier moeten worden geleverd, kunnen op afstand en op verzoek per direct worden uitgevoerd.	
E7-9	Leverancier is verantwoordelijk voor de gehele afhandeling van wijzigingsvoorstellen m.b.t. de ict oplossing. Leverancier is verantwoordelijk voor het inbrengen van wijzigingsvoorstellen ten behoeve van het oplossen van reeds geïdentificeerde problemen. Elk wijzigingsvoorstel ondergaat een intakeprocedure. De releasemomenten worden minimaal 2 weken van te voren vastgesteld. Bij vrijkomen van een release worden de releasenotes opgeleverd die ook voor de eindgebruiker bruikbaar zijn. Het streven is om zoveel mogelijk wijzigingen 'release gewijs' door te voeren. Voor het oplossen van urgente productieverstoringen kunnen ad-hoc crashreleases worden ingepland; dit gebeurt bij voorkeur in afstemming met Opdrachtgever.	
E7-10	De inschrijver dient uiterlijk bij contractstart te beschikken over een passende continuïteitsregeling voor de aangeboden VTH-oplossing, zoals een escrowregeling of een aantoonbaar gelijkwaardige voorziening, passend bij het SaaS-karakter van de oplossing. De inschrijver dient deze regeling op verzoek van opdrachtgever te overleggen en toe te lichten. De continuïteitsregeling (escrow of gelijkwaardig) dient minimaal te borgen dat opdrachtgever bij verstoring van de continuïteit zelfstandig de dienstverlening kan voortzetten.	
E7-11	Indien de ICT-oplossing geheel of gedeeltelijk niet beschikbaar is, moet de leverancier voorzien in gedocumenteerde en toepasbare workarounds, waarmee kritische bedrijfsprocessen gedurende de uitval kunnen worden voortgezet.	
	Responsetijden	Impactcriteria
E7-12	De ict oplossing is volledig niet beschikbaar.	P1
E7-13	De ict oplossing is deels functioneel (bv. klantcontactfunctionaliteit) niet beschikbaar of deels niet beschikbaar voor meer dan 10% van de gebruikers.	P2
E7-14	Kleine verstoringen.	P3
E7-15	Gebruikers / beheerdersvraag.	P4

Nr. E8	Eisen - Business Intelligence (BI)	Toelichting
Algemene toelichting		
Opdrachtgever bedoelt met data alle data behorende bij een zaak / proces inclusief metadata. Rapporteren met alléén data uit de geboden oplossing wil Opdrachtgever bij voorkeur in de geboden oplossing kunnen doen. Voor analyses, rapportages en dashboards waarbij Opdrachtgever data uit de geboden oplossingen combineert met data uit andere bronnen dan de geboden oplossing, gebruikt Opdrachtgever een Azure Datawarehouse in combinatie met Power BI als presentatielaag. Het data team (data-analisten en gegevensbeheer) van Opdrachtgever is verantwoordelijk voor het verwerken van gecombineerde data.		
Toegankelijkheid en beschikbaarheid		
E8-1	Het moet mogelijk zijn om actuele, gestructureerde en bruikbare data uit de geboden oplossing te ontsluiten ten behoeve van het gemeentelijke data- en rapportagelandschap. De oplossing dient te voorzien in een passende en gestandaardiseerde mogelijkheid om deze data te integreren met de data- en analyseomgeving van opdrachtgever, waaronder Azure/Power BI.	
E8-2	Het meest actuele datamodel wordt actief gedeeld met Opdrachtgever, inclusief Primary Key en relaties tussen de tabellen.	
Reporting in de geboden oplossing		
Met "in de geboden oplossing" kan ook invulling gegeven worden door Leverancier met een rapportage module van een derde partij. Bij voorkeur geïntegreerd in de "hoofdapplicatie", zodat gebruikers niet het idee hebben in een andere applicatie aan te werk te zijn. Als gebruikt wordt gemaakt van derden programmatuur, dan dient dit ook een SaaS product te zijn. Hier zijn geen extra kosten aan verbonden.		
E8-3	Zelf rapporten kunnen bouwen en draaien in de ict oplossing	Bijvoorbeeld bij vraagstukken (ad-hoc, eenmalig en structureel terugkomende) vanuit de gebruikersorganisatie. Voorbeelden van rapportage zijn het aantal vergunningen verleend in een jaar, en hoeveel meldingen behandeld zijn.
E8-4	De ict oplossing biedt standaardrapportages vanuit de ict oplossing, direct beschikbaar voor gebruikers, voor ten minste de werkvoorraden, digitaal ingediende aanvragen, aanvragen per zaaktype, statussen, resultaten en doorlooptijden van processen. Deze rapportages kunnen op scherm worden gepresenteerd, en kunnen worden geëxporteerd naar .CSV of .xlsx en Pdf-formaat.	
E8-5	De ict oplossing biedt de mogelijkheid tot het door functioneel beheer maken van eigen rapportages vanuit de ict oplossing, waarbij het functioneel beheer alle selectie-, filter-, sorteer- en presentatiemogelijkheden van de aangeboden oplossing, zoals toegepast voor de levering van standaardrapportages, ook tot zijn / haar beschikking heeft. Deze rapportages zijn tevens direct beschikbaar te stellen voor gebruikers. Ook deze rapportages kunnen naar wens op scherm worden gepresenteerd en kunnen worden geëxporteerd naar .CSV of .xlsx en Pdf-formaat.	
Standaard rapportages		
E8-6	Leverancier zorgt dat tenminste een set aan werkende standaardrapportages beschikbaar is. · CBS · Bulkfactuur · Binnengekomen zaken · Verleende vergunningen per behandelaar · Afgehandelde zaken · Niet vastgestelde leges · Overzicht tijdelijke vergunningen · Overzicht bouwkosten per verleende vergunning · Doorlooptijd · Zaken met aanvrager In deze rapportages moet een periode (van t/m) gekozen kunnen worden.	Geef een overzicht van de standaard beschikbare rapportages.

Nr. E9	Omschrijving - Implementatie	Toelichting
	Ondersteuning rondom Conversie en livegang	
E9-1	Leverancier biedt een Implementatieplan waarin zijn opgenomen: * benodigde personele capaciteit aan de zijde van de gemeente (incl. verdeling in functies en rollen) * realistische tijdplanning * benodigde technische faciliteiten aan de zijde van de gemeente	
E9-2	Leverancier biedt een dusdanige gebruikersondersteuning tijdens livegang en de periode ná livegang dat gebruikers ná beëindiging van de gebruikersondersteuning zelfstandig kunnen werken.	Beschrijf maximaal in een A4 hoe u hierin voorziet
E9-3	Leverancier levert testscripts om processen, configuraties, documenten, sjablonen te testen	
E9-4	Handleidingen en andere documenten worden aangeboden in de Nederlandse taal, dit is ook van toepassing op geboden ondersteuning.	
E9-5	Leverancier verzorgt trainingen voor functioneel beheerders (2)	
E9-6	Leverancier verzorgt trainingen voor eindgebruikers. (50)	
	Conversie van data	
E9-7	Leverancier levert een migratieplan waarin is opgenomen welke data gemigreerd gaan worden. Hierin wordt onder andere opgenomen; de specificatie van het format voor de aan te leveren brongegevens voor de Conversie, en de voorwaarden waaraan Opdrachtgever aan moet voldoen.	Vooraf wordt in samenspraak met Opdrachtgever bepaald wat wordt verstaan onder "data" en welke gegevens worden opgenomen in het migratieplan. Er dienen gegevens van zowel Zaaksysteem (xllnc) als LEEF (Stadsbeheer) te worden geconverteerd.
E9-8	De leverancier is verantwoordelijk voor het migreren van de door opdrachtgever aangeleverde gegevens naar de ICT-oplossing. De leverancier dient zorg te dragen voor een volledige, controleerbare en gevalideerde migratie conform de overeengekomen migratiescope, inclusief proefconversie(s), validatie, foutlijsten en herstelrondes. De leverancier toont aantoonbaar aan dat de gemigreerde data correct en bruikbaar beschikbaar zijn in de oplossing.	
E9-9	Ten behoeve van de Conversie voert Leverancier binnen 3 maanden na start contract een proefconversie uit. Voor aanvang van de proefconversie levert Leverancier, in overleg met Opdrachtgever, een specifiek en op maat gemaakt plan van aanpak met daarin onder andere beschreven de mapping van metagegevens. Hierbij wordt benoemd welke activiteiten die door Leverancier en welke door Opdrachtgever uitgevoerd dienen te worden.	