



BIJLAGE A. SPECIFICATIE VAN DE OPDRACHT

Europese aanbesteding

“Low-code Oplossing”

Versie : 1.0 Definitief
Kenmerk : IUC25-011
Datum : 16-04-2026

Inhoud

Hoofdstuk 1.	Inleiding.....	4
Hoofdstuk 2.	Functionals	5
2.1	Generieke eisen en Wensen	5
2.1.1	Huistijl	5
2.1.2	Zoeken.....	5
2.1.3	Tenants.....	5
2.1.4	Ontwikkeldaders en waarborgen	6
2.1.5	Continuous Integration & Continuous Delivery	7
2.1.6	(Private) Marketplace	7
2.1.7	Migratie en importmogelijkheden	9
2.1.8	Versiebeheer	10
2.2	Specifieke eisen en Wensen aan de Low-code Oplossing op basis van DevOps fases	10
2.2.1	Plan.....	11
2.2.2	Model	11
2.2.3	Build.....	13
2.2.4	Test	13
2.2.5	Deploy	14
2.2.6	Release	14
2.2.7	Operate.....	14
2.2.8	Logging en monitoren.....	15
Hoofdstuk 3.	IV kaders	16
3.1	Integraliteit.....	16
3.2	Gebruikersinterface	16
3.3	RBAC – Rechtenstructuur	16
3.4	Hosting: On-premises containerplatform	16
3.4.1	Kubernetes/OpenShift compatible	17
3.4.2	Container security / Security Context Constraints	17
3.4.3	Cluster-admin rechten	17
3.4.4	Cluster Resource Quota.....	17
3.4.5	Air-gapped	17
3.4.6	Storage reclaim.....	18
3.4.7	NodePorts	18
3.4.8	Installeerbaarheid.....	18
3.4.9	Logging.....	18
3.4.10	Onderhoud platform (containerhostingplatform).....	18
3.5	Transitie Clouddienst	19
3.6	Connectiviteit	19
Hoofdstuk 4.	Beveiliging	20
4.1	Algemene eisen beveiligingsperspectief	20
4.2	Informatiebeveiligingsbeleid	20
4.3	Wet- en regelgeving	21
4.4	Data	21
4.5	Data encryptie	21
4.6	Specifieke eisen Beveiligingsbeleid.....	21
4.6.1	Overheids- en Belastingdienstbeleid: Standaarden	22
4.6.2	Design & Runtime	23
4.6.3	Quantumveilige cryptografie.....	23

	4.6.4	Richtlijnen rond Beveiligingsincidenten en ontdekken Kwetsbaarheden	26
	4.6.5	Coördinated Vulnerability Disclose	27
	4.7	Beveiligingstesten	28
	4.8	Autorisatie en Autenticatie	28
Hoofdstuk 5.		Documentatie	30
Hoofdstuk 6.		Realisatie fase	31
	6.1	Inleiding	31
	6.2	Concept Plan van Aanpak Realisatie	31
	6.3	Mijlpalen	33
	6.3.1	Mijlpaal: Plan van Aanpak Realisatie	34
	6.3.2	Mijlpaal: Minimum Viable Product	35
	6.3.3	Mijlpaal Productiewaardige Oplossing	36
	6.3.4	Mijlpaal: Inrichten Low-code Center of Excellence	38
	6.3.5	Mijlpaal: Opleidingen en trainingen	41
	6.3.6	Mijlpaal: SLA en DAP definitief maken	43
Hoofdstuk 7.		Operationele fase	44
	7.1	Inleiding	44
	7.2	Onderhoud en Support	44
	7.2.1	Incidentmanagement	45
	7.2.2	Service Level Agreement (SLA)	46
	7.2.3	Dossier Afspraken en Procedures (DAP)	47
	7.3	Rapporteren / Dashboard	47
	7.4	Keuze-elementen	48
	7.4.1	Consultancy	48
	7.4.2	Opleidingen en trainingen	49
	7.4.3	Componenten Private Marketplace	49
Hoofdstuk 8.		Retransitie & Exit-strategie	50
	8.1	Retransitie	50
	8.2	Exit strategie	51
Hoofdstuk 9.		Integriteit	52
Hoofdstuk 10.		Maatschappelijk Verantwoord Opdrachtgeven en Inkopen (MVOI)	53
	10.1	Milieu	53
	10.2	Ketenverantwoordelijkheid (ISV)	53
Hoofdstuk 11.		Juridische kaders	55
Hoofdstuk 12.		Prijsstelling	56
	12.1	Algemene eisen ten aanzien van Prijzen	56
	12.2	Toelichting ten aanzien van de Prijzen	56
	12.3	Afrekenmethodiek	58
	12.4	Indexering Prijs	59
	12.5	Factureren en bestellen	60

Hoofdstuk 1. Inleiding

Dit document beschrijft de eisen (UE en GUE) en Wensen die de Opdrachtgever stelt in het kader van de Europese Aanbesteding met kenmerk IUC25-011 (Low-code Oplossing). Dit document maakt integraal onderdeel uit van het Beschrijvend Document.

Hoofdstuk 2. Functionals

2.1 Generieke eisen en Wensen

2.1.1 Huisstijl

Het is de bedoeling dat verschillende huisstijlen van Opdrachtgever (van bijvoorbeeld de Belastingdienst, Toeslagen en Douane) opgenomen kunnen worden in de Front-end van een Low-code Applicatie.

De huisstijl dient als een CSS-Stylesheet gecreëerd en /of aan te passen zijn en te kunnen worden hergebruikt bij het modeleren van Low-code Applicaties.

De Opdrachtgever ziet de volgende meerwaarde van Stylesheets in Low-code Ontwikkeling:

- Snelle Aanpassingen: DevOps-medewerkers kunnen snel visuele aanpassingen maken zonder diepgaande kennis van Cascading Style Sheets (CSS).
- Consistentie: Stylesheets zorgen voor een consistente visuele presentatie door de hele Low-code Applicatie.
- Efficiëntie: Door gebruik te maken van vooraf gebouwde thema's en sjablonen, kunnen DevOps-medewerkers tijd besparen en zich concentreren op de functionaliteit van de Low-code Applicatie.

GUE 1.	De Low-code Oplossing ondersteunt het kunnen creëren en/of aanpassen van CSS-Stylesheets tijdens het modelleren van de Low-code Applicatie.
GUE 2.	Alle Front-end (UI)-elementen van de Low-code Applicatie dienen met behulp van de CSS-Stylesheets volledig te kunnen worden aangepast.
GUE 3.	De CSS-Stylesheets moeten herbruikbaar zijn.

2.1.2 Zoeken

GUE 4.	De Low-code Oplossing dient te beschikken over een ingebouwde zoekfunctionaliteit, waarmee DevOps-medewerkers ten minste: <ul style="list-style-type: none"> • Visueel en tekstueel kunnen zoeken naar beschikbare Componenten en databronnen; • Filters kunnen toepassen op type Component, functionaliteit of categorie; • Eigenschappen, instellingen en Documentatie van Componenten kunnen vinden.
--------	--

2.1.3 Tenants

De Low-code Oplossing zal binnen de IV-organisatie van de Opdrachtgever als dienst worden aangeboden aan de IV medewerkers van de Directoraat-generaal (DG) Belastingdienst, DG Douane en DG Toeslagen. Daarom wil de Opdrachtgever dat de Low-code Oplossing een multi-tenant structuur ondersteunt.

GUE 5.	De Low-code Oplossing ondersteunt een tenant architectuur inrichting (multi-tenant).
GUE 6.	Elke tenant moet onafhankelijk Low-code Applicaties kunnen aanmaken, ontwikkelen, testen, opleveren en beheren. Hierin mogen zij niet afhankelijk zijn van centraal beheer op de Low-code Oplossing.

GUE 7.	De Low-code Oplossing ondersteunt, ten behoeve van Opdrachtgever, minimaal een OTAP (Ontwikkel, Test, Acceptatie, Productie) omgeving per tenant.
--------	---

2.1.4 Ontwikkelkaders en waarborgen

Het is de bedoeling dat de Low-code Oplossing zogenaamde 'Guardrails' biedt om binnen het ontwikkelproces van Low-code Applicaties de Kwaliteit, veiligheid en efficiëntie te borgen.

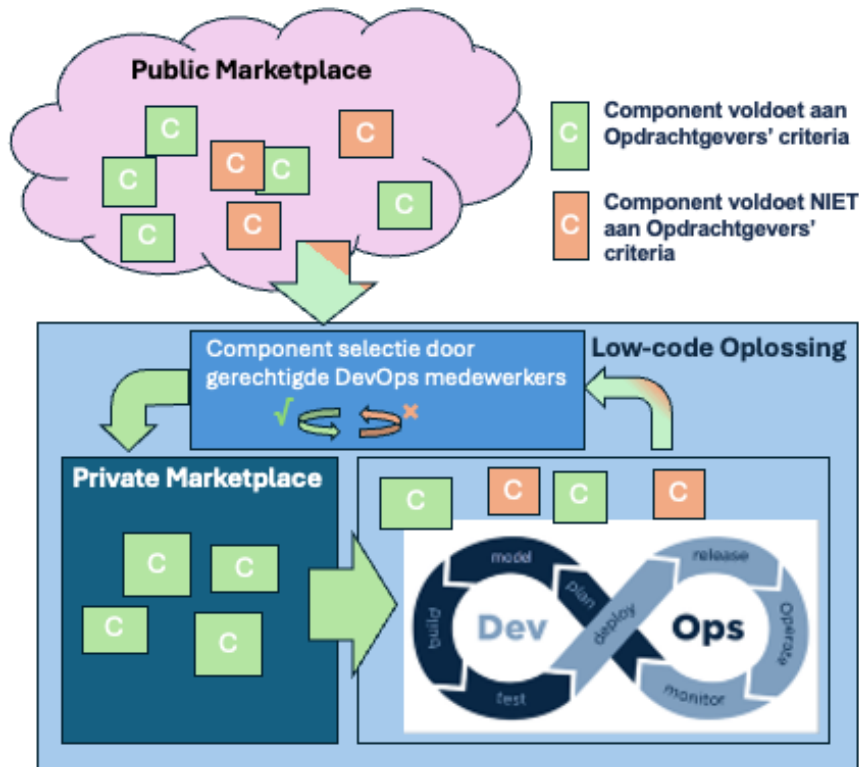
GUE 8.	De Low-code Oplossing biedt Guardrail functionaliteit om het modelleren van de te ontwikkelen Low-code Applicaties te stroomlijnen.
GUE 9.	De Low-code Oplossing biedt kant-en-klare codeobjecten en drag-and-drop tools om visuele modellen van Low-code Applicatie logica, integraties en interface van een Low-code Applicatie te maken.
GUE 10.	Binnen de Low-code Oplossing moeten Dependencies minimaal beheerd kunnen worden middels: <ul style="list-style-type: none"> • Het voorzien in een overzicht van binnen Low-code Oplossing aanwezige Dependencies die door een Low-code Applicatie kunnen worden gebruikt; • Het expliciet kunnen aangeven welke binnen de Low-code Oplossing ontwikkelde Componenten als Dependencies aan andere Low-code Applicaties opengesteld worden binnen de Low-code Oplossing; • Het voorzien in versiebeheer van de aanwezige Dependencies binnen de Low-code Oplossing.
GUE 11.	De Low-code Oplossing ondersteunt configureerbare security componenten (in ieder geval tot het voorkomen van SQL injecties, het kunnen ophalen van een token in relatie tot authenticatie en autorisatie) en dataconnectors die in een Low-code Applicatie gemodelleerd kunnen worden.
GUE 12.	De Low-code Oplossing biedt configureerbare componenten zodat Low-code Applicaties kunnen koppelen met: <ul style="list-style-type: none"> • Databases; en • Andere systemen.
GUE 13.	De Low-code Oplossing biedt inzicht in ten minste het aantal: <ul style="list-style-type: none"> • Low-code Applicaties per omgeving (OTAP) van Opdrachtgever; • Eindgebruikers per Low-code Applicatie; • DevOps-medewerkers die gebruik maken van de Low-code Oplossing.
GUE 14.	De met de Low-code Oplossing gebouwde Low-code Applicaties moeten meetbaar zijn met de meetapplicatie Sigrid van Software Improvement Group (SIG).

2.1.5 Continuous Integration & Continuous Delivery

Om een snelle, betrouwbare en geautomatiseerde levering van Low-code Applicaties te waarborgen, moet de Low-code Oplossing de "Continuous Integration / Continuous Delivery (CI/ CD) principes" ondersteunen.

GUE 15.	<p>De Low-code Oplossing biedt CI/CD functionaliteit op één van de volgende manieren:</p> <ol style="list-style-type: none"> 1. Integraal in de Low-code Oplossing; of 2. Gekoppeld met een extern CI/CD systeem. <p>In het geval de Low-code Oplossing de ondersteuning van een CI/CD systeem extern koppelt, dan dient minimaal met één van de volgende CI/CD systemen van de Opdrachtgever gekoppeld te kunnen worden:</p> <ul style="list-style-type: none"> • Tekton (OpenShift Pipelines); • ArgoCD; • Bitbucket.
GUE 16.	<p>In het geval CI/CD integraal onderdeel uitmaakt van de Low-code Oplossing, biedt de Low-code Oplossing de functionaliteit dat er expliciet handmatige goedkeuring kan worden verleend door een daartoe gerechtigde DevOps-medewerkers minimaal voordat een gemodelleerde Low-code Applicatie naar Productie wordt gebracht.</p>

2.1.6 (Private) Marketplace



Afbeelding 1. Samenhang

DevOps-medewerkers kunnen sneller Low-code Applicaties modelleren als zij gebruik kunnen maken van herbruikbare Componenten.

GUE 17.	De Low-code Oplossing biedt toegang tot een Public Marketplace met Componenten.
GUE 18.	Minimaal de volgende Componenten zijn beschikbaar in de Public Marketplace: <ul style="list-style-type: none"> • Componenten van de Fabrikant zelf, • Door de Fabrikant gecontroleerde Componenten, • Componenten van de door de Fabrikant vertrouwde Derde partijen.
GUE 19.	Van elk Component in de Public Marketplace zijn de Licentievoorwaarden inzichtelijk.

Het aanbieden van deze Componenten aan daartoe gerechtigde DevOps-medewerkers is alleen via een Private Marketplace mogelijk. Ook door Opdrachtgever zelf ontwikkelde Componenten moeten in deze Private Marketplace kunnen worden opgenomen. Het realiseren van de Private Marketplace is onderdeel van de Opdracht.

UE 1.	Tijdens de Realisatiefase van de Low-code Oplossing Realiseert Opdrachtnemer een Air-gapped Private Marketplace als onderdeel van de Low-code Oplossing. Hierin worden zowel door de Opdrachtgever geselecteerde Componenten uit de Public Marketplace alsook vanuit de Opdrachtgever zelf ontwikkelde Componenten aangeboden aan de DevOps-medewerkers.
GUE 20.	Het al dan niet kunnen afnemen van Componenten van deze Private Marketplace moet per DevOps-medewerker instelbaar / configureerbaar zijn / gereguleerd kunnen worden.
GUE 21.	De Low-code Oplossing ondersteunt dat alleen daartoe gerechtigde DevOps-medewerkers de Private Marketplace met Componenten kunnen vullen. Componenten, afkomstig uit de Public Marketplace of gemodelleerd zijn door DevOps-medewerkers van Opdrachtgever, kunnen alleen in de Private Marketplace worden opgenomen als zij voldoen aan de door het CoE gestelde toetsingskader. De controle op basis van het toetsingskader wordt gedaan door daartoe gerechtigde DevOps-medewerkers.
GUE 22.	De Low-code Oplossing ondersteunt om binnen de Private Marketplace een tenantstructuur aan te brengen, waarbij: <ol style="list-style-type: none"> 1. Multi-tenant beheer mogelijk is (zodat Componenten per tenant (bijvoorbeeld per organisatieonderdeel, afdeling of project) zichtbaar en beschikbaar gemaakt kunnen worden). 2. Toegangs- en publicatierechten per tenant configureerbaar zijn, inclusief rolgebaseerde toegang (RBAC). 3. Versiebeheer van Componenten per tenant wordt ondersteund (zodat verschillende tenants verschillende versies van dezelfde Component kunnen gebruiken). 4. Isolatie van resources wordt geborgd (zodat Componenten, Data en configuraties van de ene tenant niet toegankelijk zijn voor andere tenants, tenzij expliciet gedeeld). <p>Beheerfunctionaliteit aanwezig is om tenants centraal te administreren, inclusief rapportages over gebruik, Updates en afhankelijkheden.</p>

2.1.7 Migratie en importmogelijkheden

W 1.	<p>Migratie-/Importmogelijkheden</p> <p>In het verleden zijn twee Low-code platformen geselecteerd Opdrachtgever. De Low-code Applicaties die met behulp van deze twee geselecteerde platformen gerealiseerd zijn, wil Opdrachtgever graag kunnen continueren binnen het te verwerven platform.</p> <p>Vraag</p> <p>Geef aan in welke mate en op welke wijze uw Oplossing de mogelijkheid biedt om Low-code Applicaties te migreren naar uw Oplossing van:</p> <ul style="list-style-type: none"> • Mendix en/of • OutSystems (versie 11) <p>Indien uw Oplossing de mogelijkheid biedt om bestaande low-code applicaties te migreren, beschrijft u op welke wijze u een dergelijke Migratie voor zich ziet. In uw antwoord gaat u in op uw voorgestelde aanpak, gehanteerde methodieken, beschikbare best practices en eventuele randvoorwaarden die volgens u van toepassing zijn</p> <p>Uw uitwerking bestaat uit <u>maximaal 5 pagina's A4</u> (lettertype Arial, lettergrootte 10, regelafstand 1,0) mag geen verwijzingen en hyperlinks bevatten. Extra pagina's worden niet beoordeeld. Voor deze Wens kunt u <u>maximaal 25 punten</u> verdienen.</p> <p>Beoordelingskader</p> <p>De beoordeling van de beantwoording van deze Wens vindt plaats op basis van onderstaand scoretabel.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #0056b3; color: white;"> <th style="text-align: left;">Beoordeling / aantal punten</th> <th style="text-align: left;">Toelichting</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">Niet beantwoord 0 punten</td> <td>Er is geen inhoudelijk antwoord gegeven op de migratiemogelijkheden, of expliciet aangegeven dat Migratie niet mogelijk is.</td> </tr> <tr> <td style="text-align: center;">Onvoldoende 5 punten</td> <td>Alleen conceptueel Het antwoord bevat uitsluitend een hoog-over voorstel. Er is geen concreet, stapsgewijs migratieplan en geen benoeming van concrete deliverables. Daarnaast blijkt uit het antwoord geen of onvoldoende aantoonbare ervaring met de genoemde platformen.</td> </tr> <tr> <td style="text-align: center;">Matig 10 punten</td> <td>Gestructureerd maar theoretisch Het antwoord bevat een generieke, gestructureerde aanpak met een beschreven fase-indeling en benoemde activiteiten. Eén of meerdere van de volgende elementen ontbreken: <ul style="list-style-type: none"> • Concrete templates of voorbeeld-deliverables • (Technische) tooling • Specifieke of gekwantificeerde activiteiten • Praktijkvoorbeelden of referenties Specifieke uitwerking voor de context van de Opdrachtgever </td> </tr> <tr> <td style="text-align: center;">Voldoende 15 punten</td> <td>Gestructureerde methode met documentatie Het antwoord bevat een gefaseerd migratieplan met voorbeeld-deliverables (bijv. een assessment-template). De randvoorwaarden worden expliciet benoemd. Er is documentatie beschikbaar over de uitvoering van de methode. Risico's worden geïdentificeerd en beschreven. Het antwoord is intern consistent en bevat geen tegenstrijdigheden tussen aanpak, planning en risico-inschatting.</td> </tr> </tbody> </table>	Beoordeling / aantal punten	Toelichting	Niet beantwoord 0 punten	Er is geen inhoudelijk antwoord gegeven op de migratiemogelijkheden, of expliciet aangegeven dat Migratie niet mogelijk is.	Onvoldoende 5 punten	Alleen conceptueel Het antwoord bevat uitsluitend een hoog-over voorstel. Er is geen concreet, stapsgewijs migratieplan en geen benoeming van concrete deliverables. Daarnaast blijkt uit het antwoord geen of onvoldoende aantoonbare ervaring met de genoemde platformen.	Matig 10 punten	Gestructureerd maar theoretisch Het antwoord bevat een generieke, gestructureerde aanpak met een beschreven fase-indeling en benoemde activiteiten. Eén of meerdere van de volgende elementen ontbreken: <ul style="list-style-type: none"> • Concrete templates of voorbeeld-deliverables • (Technische) tooling • Specifieke of gekwantificeerde activiteiten • Praktijkvoorbeelden of referenties Specifieke uitwerking voor de context van de Opdrachtgever	Voldoende 15 punten	Gestructureerde methode met documentatie Het antwoord bevat een gefaseerd migratieplan met voorbeeld-deliverables (bijv. een assessment-template). De randvoorwaarden worden expliciet benoemd. Er is documentatie beschikbaar over de uitvoering van de methode. Risico's worden geïdentificeerd en beschreven. Het antwoord is intern consistent en bevat geen tegenstrijdigheden tussen aanpak, planning en risico-inschatting.
Beoordeling / aantal punten	Toelichting										
Niet beantwoord 0 punten	Er is geen inhoudelijk antwoord gegeven op de migratiemogelijkheden, of expliciet aangegeven dat Migratie niet mogelijk is.										
Onvoldoende 5 punten	Alleen conceptueel Het antwoord bevat uitsluitend een hoog-over voorstel. Er is geen concreet, stapsgewijs migratieplan en geen benoeming van concrete deliverables. Daarnaast blijkt uit het antwoord geen of onvoldoende aantoonbare ervaring met de genoemde platformen.										
Matig 10 punten	Gestructureerd maar theoretisch Het antwoord bevat een generieke, gestructureerde aanpak met een beschreven fase-indeling en benoemde activiteiten. Eén of meerdere van de volgende elementen ontbreken: <ul style="list-style-type: none"> • Concrete templates of voorbeeld-deliverables • (Technische) tooling • Specifieke of gekwantificeerde activiteiten • Praktijkvoorbeelden of referenties Specifieke uitwerking voor de context van de Opdrachtgever										
Voldoende 15 punten	Gestructureerde methode met documentatie Het antwoord bevat een gefaseerd migratieplan met voorbeeld-deliverables (bijv. een assessment-template). De randvoorwaarden worden expliciet benoemd. Er is documentatie beschikbaar over de uitvoering van de methode. Risico's worden geïdentificeerd en beschreven. Het antwoord is intern consistent en bevat geen tegenstrijdigheden tussen aanpak, planning en risico-inschatting.										

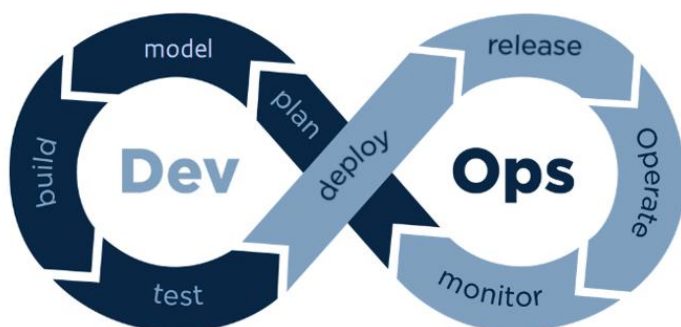
<p>Goed 20 punten</p>	<p>Gespecificeerd en contextgericht Alles van “Voldoende”, plus:</p> <ul style="list-style-type: none"> • De migratieaanpak is deels specifiek uitgewerkt voor de context van de Opdrachtgever. • Inschrijver toont specifieke en aantoonbare technische kennis van zowel het bron- als doelplatform, waarbij verschillen in architectuur, modellering, integratie en LifeCycle Management (LCM) expliciet worden benoemd. • Naast risico’s worden concrete mitigerende maatregelen benoemd. • Er wordt een globale, onderbouwde inspanningsinschatting gegeven (bijv. per type Low-code Applicatie of complexiteitscategorie). • De voorgestelde aanpak en inspanningsinschatting zijn aantoonbaar onderbouwd en proportioneel in verhouding tot de beschreven migratiecomplexiteit. <p>Er wordt expliciet aandacht besteed aan teststrategie, datamigratie-aanpak en migratiescenario’s (bijvoorbeeld gefaseerde Migratie of parallelle overgang).</p>
<p>Uitstekend 25 punten</p>	<p>Bewezen en aantoonbaar toegepast Alles van “Goed”, plus:</p> <ul style="list-style-type: none"> • De migratieaanpak is volledig uitgewerkt inclusief stappen, rollen, risico’s en mitigaties. • De methodiek is aantoonbaar toegepast in eerdere, vergelijkbare migraties en wordt onderbouwd met referenties of case studies. • Best practices zijn concreet, toepasbaar en aantoonbaar effectief. • Randvoorwaarden zijn volledig, consistent en passend binnen de context van de Aanbesteding. De aanpak bevat een expliciete strategie voor borging van continuïteit en beheersing van operationele risico’s tijdens de migratieperiode. • Beschikbare technische migratietooling wordt concreet toegelicht, inclusief toepassingsgebied, beperkingen en aantoonbare inzet in vergelijkbare trajecten.

2.1.8 Versiebeheer

<p>GUE 23.</p>	<p>De Low-code Oplossing biedt ondersteuning voor geïntegreerd versiebeheer, inclusief de visuele weergave van 'merging' en 'Conflict Resolvment' mogelijkheden.</p>
----------------	--

2.2 Specifieke eisen en Wensen aan de Low-code Oplossing op basis van DevOps fases

Aan de hand van het volgende figuur met DevOps capabilities worden de meer specifieke eisen en Wensen aan de Low-code Oplossing uiteengezet.



Afbeelding 2. DevOps Capabilities Lemniscaat.

GUE 24.	<p>De Low-code Oplossing ondersteunt ten minste de volgende DevOps capabilities:</p> <ul style="list-style-type: none"> • Plan • Model • Build • Test • Deploy • Release • Operate • Monitor
GUE 25.	<p>Minimaal de volgende DevOps capabilities dienen met een CI/CD pipeline geautomatiseerd te worden ondersteund:</p> <ul style="list-style-type: none"> • Build • Test • Deploy • Release

2.2.1 Plan

Binnen het DevOps-lemniscaat verwijst de fase 'plan' naar het proces van het definiëren van doelen, vereisten en prioriteiten voor softwareontwikkeling. Het omvat het opstellen van een Roadmap, het identificeren van gebruikersbehoeften en het plannen van iteraties. Deze fase legt de basis voor een gestroomlijnde samenwerking tussen teams en zorgt ervoor dat iedereen dezelfde visie deelt voordat de daadwerkelijke ontwikkeling begint.

GUE 26.	De Low-code Oplossing ondersteunt het kunnen aanmaken, bijhouden en beheren van een Backlog.
---------	--

2.2.2 Model

'Model' verwijst naar meer dan alleen de broncode van een applicatie. Het omvat alle aspecten van softwareontwikkeling die bijdragen aan het creëren van waarde, zoals scripts, configuratiebestanden, infrastructuurcode (infrastructure as code), en zelfs testcode. Het idee is dat alles wat nodig is om een Low-code Applicatie te bouwen, te testen, te implementeren en te onderhouden, als 'code' wordt behandeld. Dit maakt automatisering en samenwerking tussen teams eenvoudiger en efficiënter.

GUE 27.	Met de Low-code Oplossing dient op basis van Visual Coding coherent een Applicatie gemodelleerd te kunnen worden.
GUE 28.	Met Visual Coding kunnen ten minste de volgende Applicatielagen worden gemodelleerd: <ul style="list-style-type: none"> • Data; • Logica; • User interface (UI).
GUE 29.	Alle configuratie kenmerken en instellingen van een Low-Code Applicatie zijn visueel op te vragen, te inspecteren en te wijzigen.
GUE 30.	Tijdens het modelleren van een Low-code Applicatie ondersteunt de Low-code Oplossing geautomatiseerde controles op basis van Consistency Checks.
GUE 31.	De Low-code Oplossing dwingt af dat indien er tijdens het modelleren blokkerende inconsistenties en/of kritieke fouten ('Errors') worden geconstateerd door de geautomatiseerde Consistency Check, de te ontwikkelen Low-code Applicatie niet deployed kan worden én de DevOps-medewerker een melding met een omschrijving van de inconsistentie of fout krijgt.
GUE 32.	De modelleeromgeving van de Low-code Oplossing geeft modelleersuggesties aan de DevOps-medewerker en conflicterende en/of blokkerende inconsistenties en/of kritieke fouten ('Errors') worden aan de DevOps-medewerkers getoond.
GUE 33.	De Low-code Oplossing ondersteunt het tonen van context-gerelateerde documentatie via een hulpfunctie tijdens het modelleren.
GUE 34.	De Low-code Oplossing ondersteunt het uitbreiden van het Low-code Applicatiemodel met maatwerk (custom-code) op basis van zelfbouw (High-code). Dit moet minimaal kunnen voor de: <ul style="list-style-type: none"> • Back-end met C# of Java; • Front-end met Javascript, CSS 3, HTML 5.
UE 2.	Ten aanzien van het toepassen van Artificial Intelligence(AI)-functionaliteiten in de Low-code Oplossing committeert Opdrachtnemer zich gedurende de looptijd van de Overeenkomst tot het minimaal jaarlijks of vaker indien Opdrachtgever dit wenst, aanleveren van een toelichting op de beschikbare AI-functionaliteiten binnen de Oplossing en ten aanzien van de volgende onderdelen: <ol style="list-style-type: none"> 1. De mate waarin de Low-code Oplossing AI-functionaliteiten ondersteunt die bijdragen aan efficiëntie, Kwaliteit en toekomstbestendigheid van de ontwikkel- en beheerprocessen. De Opdrachtnemer geeft een toelichting op de beschikbare AI-functionaliteiten binnen de Oplossing. <ol style="list-style-type: none"> a. AI-ondersteuning tijdens softwareontwikkeling (bijv. suggesties, code-generatie, kwaliteitscontrole). b. AI-functionaliteiten voor beheer, monitoring of optimalisatie van Low-code Applicaties. c. Mogelijkheden om AI-modellen of generatieve AI te integreren in Low-code Applicaties. d. Beschikbare standaardcomponenten, connectors of frameworks voor AI-toepassingen. e. Roadmap en visie op toekomstige AI-ontwikkelingen binnen de Oplossing. 2. In hoeverre de AI-functionaliteit, zonder tussenkomst van de Fabrikant of Opdrachtnemer, aan- of uitgezet kan worden. Hierbij wordt onderscheid gemaakt in a. Platform, b. Tenant, c. Applicatie(ontwikkeling) en 4. Gebruikersrol. 3. De mate waarin de Opdrachtgever, zonder tussenkomst van de Fabrikant of Opdrachtnemer, een eigen keuze kan maken in LLM's. Hierbij wordt in ieder geval ingegaan op de volgende mogelijkheden: <ol style="list-style-type: none"> a. Alleen het model van Fabrikant of Opdrachtnemer is toegestaan. b. Inzet van externe modellen alleen via API. c. Volledige BYOM en model-routing mogelijk. d. Volledige BYOM, model-routing en on-prem modellen mogelijk. 4. In hoeverre de Low-code Oplossing volledig bruikbaar blijft zonder AI, dus zonder degradatie van kernfunctionaliteit. Waarbij er een keuze wordt gemaakt uit de volgende mogelijkheden:

	<ul style="list-style-type: none"> a. Platform verliest essentiële functionele zonder AI. b. Enkele functies vallen weg, maar de kern blijft bruikbaar. c. AI is volledig optioneel maar sommige UX-flows zijn minder efficiënt. d. Volledige functionaliteit blijft behouden. e. Anders, namelijk... <p>5. In hoeverre de inzet van AI binnen de Low-code Oplossing uitlegbaar, controleerbaar en veilig binnen de normen van de publieke sector is. Hierbij wordt in ieder geval ingegaan op in hoeverre:</p> <ul style="list-style-type: none"> a. Keuzes, risico's en output-herkomst uitlegbaar zijn. b. Prompts centraal te beheren, blokkeren of whitelisten zijn. c. Modeltraining op klantdata alleen met expliciete toestemming mogelijk is. d. De Opdrachtnemer AI-risicoanalyse conform EU AI Act levert en op welke wijze.
--	--

2.2.3 Build

'Build' verwijst naar het proces waarin de Broncode van een applicatie wordt omgezet in een uitvoerbaar bestand of een werkend systeem. Dit omvat het compileren van code, het integreren van verschillende componenten, en het uitvoeren van geautomatiseerde tests om ervoor te zorgen dat de software correct functioneert. Het doel is om een stabiele versie van de software te creëren die klaar is voor verdere testen of implementatie. Binnen een Low-code Oplossing zijn dit geïntegreerde stappen die door het platform worden uitgevoerd.

Het 'build'-proces is vaak geautomatiseerd en geïntegreerd in CI/CD-pipelines (Continuous Integration/Continuous Deployment), zodat DevOps-medewerkers snel en efficiënt nieuwe versies kunnen leveren.

In de DevOps fase "Build" zijn geen specifieke eisen en of Wensen aan de Low-code Oplossing.

2.2.4 Test

'Test' verwijst naar het proces van het valideren van de Kwaliteit en functionaliteit van software. Dit omvat verschillende soorten testen, zoals Unit Tests, integratietests, systeemtests en Acceptatietests. Het doel is om fouten vroegtijdig te identificeren en te corrigeren, zodat de software betrouwbaar en gebruiksklaar is. In een DevOps-context wordt testen vaak geautomatiseerd en geïntegreerd in de CI/CD-pipeline (Continuous Integration/Continuous Deployment). Dit zorgt ervoor dat elke wijziging in de code direct wordt getest, wat de snelheid en Kwaliteit van softwarelevering verhoogt. Testen is een continu proces en een gedeelde verantwoordelijkheid binnen het team, waarbij iedereen bijdraagt aan de Kwaliteit van het eindproduct. Noot: Binnen het conglomeraat van kwaliteitseisen wordt een aantal van deze eisen geconcretiseerd en vertaald naar specifieke testsoorten en eventueel testtechnieken om inzicht te krijgen in het kwaliteitsniveau.

Bij deze fase gaat het om het kunnen schrijven van testgevallen op basis van het Low-code Applicatie ontwerp.

GUE 35.	De Low-code Oplossing biedt integrale testtools waarmee Unit Tests direct binnen de Low-code Oplossing kunnen worden aangemaakt en uitgevoerd ten einde logica of bouwstenen van de Low-code Applicatie te isoleren en te testen zonder handmatige codering.
GUE 36.	De binnen de Low-code Oplossing gemaakte Unit Tests dienen vanuit een CI/CD pipeline uitgevoerd te kunnen worden waarbij het resultaat teruggekoppeld wordt.

2.2.5 Deploy

Binnen het DevOps-lemniscaat verwijst 'deploy' naar het proces van het implementeren van software in een specifieke omgeving, zoals Productie, test of staging. Het doel is om de software beschikbaar te maken voor gebruik, of dat nu door Eindgebruikers is of door andere systemen. Dit proces omvat vaak geautomatiseerde stappen om consistentie en betrouwbaarheid te garanderen.

In een DevOps-context wordt 'deploy' vaak uitgevoerd via Continuous Deployment (CD), waarbij nieuwe versies van software automatisch worden uitgerold zodra ze voldoen aan de kwaliteitsnormen. Dit minimaliseert handmatige interventie en versnelt de levering van waarde aan Eindgebruikers.

GUE 37. De Low-code Oplossing ondersteunt dat alle deployment-activiteiten worden gelogd.

2.2.6 Release

Binnen het DevOps-lemniscaat verwijst 'release' naar het proces van het beschikbaar stellen van een nieuwe versie van software aan gebruikers of Productie omgevingen. Dit omvat het plannen, voorbereiden en implementeren van de software, vaak met behulp van geautomatiseerde tools en processen. Het doel is om software snel, betrouwbaar en met minimale risico's te leveren.

In een DevOps-context is 'release' een continu proces dat nauw verbonden is met CI/CD (Continuous Integration/Continuous Deployment). Het stelt teams in staat om frequente en kleine updates uit te brengen, wat helpt om sneller waarde te leveren en eventuele Problemen snel op te lossen.

In de DevOps fase "Release" zijn geen specifieke eisen en of Wensen aan de Low-code Oplossing. Er zijn hierboven eisen gesteld aan de CI/CD die op deze fase betrekking hebben.

2.2.7 Operate

Binnen het DevOps-lemniscaat verwijst 'operate' naar het beheren en onderhouden van software en infrastructuur in Productie omgevingen. Het doel is om ervoor te zorgen dat systemen betrouwbaar, veilig en efficiënt blijven functioneren. Dit omvat taken zoals monitoring, incidentbeheer, probleemoplossing, prestatieoptimalisatie en het implementeren van beveiligingsupdates.

In een DevOps-context wordt 'operate' vaak ondersteund door geautomatiseerde monitoring- en beheeroplossingen, zodat teams proactief Problemen kunnen identificeren en oplossen. Het benadrukt ook samenwerking tussen ontwikkelings- en operationele teams om een continue stroom van verbeteringen en stabiliteit te waarborgen.

GUE 38. De Low-code Oplossing ondersteunt het modelleren van Low-code Applicaties die benaderbaar zijn met een standaard webbrowser. De volgende standaard webbrowsers dienen minimaal te worden ondersteund:

- Google Chrome;
- Microsoft Edge.

2.2.8 Logging en monitoren

Binnen het DevOps-lemniscaat verwijst 'monitor' naar het proces van het continu bewaken van systemen, applicaties en infrastructuur om prestaties, beschikbaarheid en veiligheid te waarborgen. Monitoring omvat het verzamelen van Data zoals logs, metrics en traces, en het analyseren van deze Data om Problemen vroegtijdig te detecteren en op te lossen. Het doel is om een stabiele en betrouwbare omgeving te behouden, terwijl teams proactief kunnen reageren op afwijkingen of Incidenten.

In een DevOps-context wordt monitoring vaak gecombineerd met observability, wat een diepgaander inzicht biedt in de interne werking van systemen. Tools zoals Prometheus, Grafana en ELK Stack wordt in de wereld van softwareontwikkeling vaak gebruikt om monitoring en visualisatie te ondersteunen.

GUE 39.	De Low-code Oplossing ondersteunt ten minste volgende twee typen logging: <ul style="list-style-type: none"> • Low-code Applicatie Logging; en • Audit Logging.
GUE 40.	De Low-code Oplossing ondersteunt dat logging als volgt configureerbaar zijn: <ul style="list-style-type: none"> • welke gebeurtenissen en of acties; • op welk detailniveau gebeurtenissen en of acties worden gelogd; • de retentie van logging.
GUE 41.	De Low-code Oplossing voldoet aan de OpenTelemetry standaard met betrekking tot Applicatie Logging.
GUE 42.	De Low-code Oplossing ondersteunt volcontinue monitoring en dat excepties worden gelogd op: <ul style="list-style-type: none"> • Datum en tijd; • IP-adres of hostnaam van het device dat de informatie logt; • IP-adres van het remote systeem (indien met een ander systeem wordt gecommuniceerd); • identificatie van de gebruiker of het proces; • beschrijving van de activiteit of gebeurtenis; • het resultaat van de activiteit of gebeurtenis. Gebeurtenissen die minimaal gelogd moeten worden: <ul style="list-style-type: none"> • authenticatie/autorisatie pogingen, inloggen en uitloggen; • acties die betrekking hebben op gebruikersprofielen, bestanden en databases of systeemservices; • transacties tussen systemen; • activatie en/of de-activatie van beveiligingsfunctionaliteit; • niet gespecificeerd gedrag van systemen en Low-code Applicaties (uitzonderingen, fouten en storingen); • Beveiligingsincidenten.
GUE 43.	De Low-code Oplossing biedt inzage in logs.
GUE 44.	De Low-code Oplossing biedt de mogelijkheid om logs te downloaden in minimaal .txt of .csv formaat.

Hoofdstuk 3. IV kaders

3.1 Integraliteit

GUE 45.	<p>De Opdrachtnemer levert de Low-code Oplossing als één integraal coherent werkend systeem. De deelcomponenten van de Low-code Oplossing werken als één integraal coherent systeem.</p> <p>De Low-code Oplossing voldoet (out-of-the-box) aan alle Specificaties. De Oplossing kan door middel van configuratie worden afgestemd op de processen van Opdrachtgever, maar vereist geen aanvullende ontwikkelactiviteiten om aan de gestelde Specificaties te voldoen.</p> <p>Als de Low-code Oplossing bestaat uit deeloplossingen dan is de integratie en werking van deze oplossingen de verantwoordelijkheid van de Opdrachtnemer.</p>
---------	---

3.2 Gebruikersinterface

GUE 46.	De Low-code Oplossing biedt een rol gebaseerde gebruikersinterface (hierna: GUI), waarmee DevOps-medewerkers direct toegang hebben tot projecten, informatie en functionaliteiten die voor de betreffende DevOps-medewerkers relevant zijn.
GUE 47.	<p>De Low-code Oplossing biedt minimaal de volgende interfaces:</p> <ul style="list-style-type: none"> • Een IDE geïnstalleerd op de werkplek van de DevOps-medewerkers of een webcliënt; • Webcliënt t.b.v. beheeractiviteiten.
GUE 48.	De IDE moet werken op laptops van minimaal de volgende specificatie: Windows 11 met 16 GB RAM en 256 GB opslag.

3.3 RBAC – Rechtenstructuur

Het is de bedoeling dat de Low-code Oplossing een fijnmazige rollen- en rechtenstructuur ondersteunt. Zo dient bijvoorbeeld één of meerdere centrale "super administrator" rollen aangemaakt te kunnen worden, die op hun beurt weer permissies kunnen delegeren aan andere type gebruikers (rollen).

GUE 49.	De Low-code Oplossing ondersteunt een configureerbare rol gebaseerde toegangscontrole om toegangsrechten in de Low-code Oplossing te beheren door machtigingen toe te wijzen op basis van rollen.
---------	---

3.4 Hosting: On-premises containerplatform

De containerhostingeisen zijn van toepassing op de On-premises situatie.

3.4.1 Kubernetes/OpenShift compatible

GUE 50.	<p>De Low-code Oplossing moet werken op het On-premises Red Hat OpenShift versie 4.18 (Kubernetes) containerplatform en diens opvolgende versies.</p> <p>Met werken wordt bedoeld dat ten minste Installeren, Productiewaardig functioneren van de Low-code Oplossing en het kunnen deployen van Low-code Applicaties met de Low-code Oplossing.</p>
---------	--

3.4.2 Container security / Security Context Constraints

GUE 51.	De Low-code Oplossing moet kunnen draaien op de Securitycontextconstraint: restricted-v2 en diens logische opvolgers. Deze instelling is default op het het doel cluster (containerplatform) ingesteld.
GUE 52.	De aangeleverde containerimages moeten kunnen omgaan met willekeurig ingestelde user id's.

3.4.3 Cluster-admin rechten

GUE 53.	De Low-code Oplossing moet voor het normale gebruik zonder cluster-admin rechten op OpenShift kunnen draaien. Indien er initieel verhoogde rechten nodig zijn dan kunnen deze gedurende het installatieproces worden toegestaan door de Opdrachtgever.
GUE 54.	De Installatie van de Low-code Oplossing wordt uitgevoerd met een account met standaard rechten in plaats van een account met verhoogde rechten zoals cluster admin. Mocht dit toch noodzakelijk zijn, dan is dit slechts eenmalig tijdens de Installatie.

3.4.4 Cluster Resource Quota

GUE 55.	De Low-code Oplossing moet kunnen omgaan met Namespaces waarin het instellen van resource requests en limits verplicht is.
---------	--

3.4.5 Air-gapped

GUE 56.	De Low-code Oplossing moet in staat zijn om Air-gapped te kunnen functioneren. De Low-code Oplossing moet kunnen omgaan met een private registry en repository van de Opdrachtgever voor Kubernetes.
GUE 57.	De Low-code Oplossing biedt Support voor een Air-gapped omgeving. Benodigde images dienen via een 'bastion server' intern opgeslagen in Harbor (incl. Vulnerability Scanning).

3.4.6 Storage reclaim

GUE 58.	Er mag geen reclaim policy van een persistent volume worden ingesteld op 'retain'.
---------	--

3.4.7 NodePorts

GUE 59.	De Low-code Oplossing maakt geen gebruik van de nodeports op het Red Hat OpenShift container platform cluster van de Opdrachtgever.
---------	---

3.4.8 Installeerbaarheid

GUE 60.	De Low-code Oplossing kan op basis van operators of helm charts worden uitgerold.
GUE 61.	De Low-code Oplossing moet seamless Upgrades ondersteunen.
GUE 62.	Indien de Low-code Oplossing geïnstalleerd wordt met een operator, is uit de beschrijving van de operator duidelijk welke aanpassingen de operator op cluster-niveau aanbrengt.
GUE 63.	De Low-code Oplossing is geschikt om in een Red Hat OpenShift container op een On-premises hostingplatform van de Opdrachtgever te draaien en is onafhankelijk van de onderliggende hardware met uitzondering van processor architectuur. De Opdrachtgever moet Life Cycle Management (LCM) kunnen uitvoeren op haar X86 gebaseerde hardware, zonder dat dit impact heeft op de Low-code Oplossing.
GUE 64.	De 'ReclaimPolicy' van 'StorageClasses' en 'PersistentVolumes' op het containerplatform staat standaard op 'Delete'. De Low-code Oplossing mag niet eisen dat deze instelling gewijzigd wordt.

3.4.9 Logging

GUE 65.	Het gebruik van de Low-code Oplossing kan worden gelogd naar de console van het containerplatform van de Opdrachtgever.
---------	---

3.4.10 Onderhoud platform (containerhostingplatform)

GUE 66.	De correcte werking van de Low-code Oplossing wordt niet beïnvloed doordat de container met de Low-code Oplossing door het containerplatform wordt gestopt en op een andere worker node (container) wordt gestart.
GUE 67.	De Low-code Oplossing reageert op het stopsignaal en geeft aan hoe lang er maximaal gewacht mag worden tot Red Hat OpenShift de container uitzet.
GUE 68.	Platform versies (van Red Hat OpenShift) worden blijvend ondersteund door Opdrachtnemer, totdat deze End of Support zijn.
GUE 69.	De Low-code Oplossing mag niet verhinderen dat altijd de laatste security patches worden geïnstalleerd.

3.5 Transitie Clouddienst

UE 3.	<p>Op het moment dat de Opdrachtgever de Low-code Oplossing en de daarmee gerealiseerde Low-code Applicaties als Clouddienst wenst af te nemen, dient ten behoeve van de transitie de Opdrachtnemer een concept Plan van Aanpak Transitie op te leveren die met Opdrachtgever op uitvoerbaarheid wordt afgestemd.</p> <p>In het concept Plan van Aanpak Transitie komen in ieder geval de volgende onderwerpen terug:</p> <ul style="list-style-type: none"> • De technische en functionele aanpak voor het Migreren van bestaande Low-code Applicaties en onderliggende datamodellen, inclusief eventuele conversietools, migratiescripts of methodieken. • Een strategie voor het waarborgen van datakwaliteit, Beveiliging en continuïteit tijdens de Migratie, met speciale aandacht voor auditability en compliance (bijv. AVG). • Maatregelen om downtime van bedrijfskritische processen te beperken en fallback-mechanismen in te richten; • De wijze waarop bestaande functionaliteiten worden behouden, vervangen of geoptimaliseerd binnen de Clouddienst; • Afhankelijk van de ervaring van Opdrachtnemer met vergelijkbare transities: een overzicht van lessons-learned en referentiecasses op basis van vergelijkbare migratietrajecten van de aangeboden Oplossing. • Een kostenraming: <ul style="list-style-type: none"> ○ van de te verrichten werkzaamheden, taken en verantwoordelijkheden van de Opdrachtgever en Opdrachtnemer ○ voor het gebruik de Clouddienst.
-------	---

3.6 Connectiviteit

GUE 70.	<p>De Low-code Oplossing dient minimaal met de volgende courante Relational Database Management Systemen (RDBMS) te kunnen koppelen:</p> <ul style="list-style-type: none"> • PostgreSQL.
GUE 71.	<p>De Low-code Oplossing biedt functionaliteit waarmee API's gedefinieerd, aangeboden en geconsumeerd kunnen worden op basis van minimaal de volgende courante API-protocollen:</p> <ul style="list-style-type: none"> • REST; • OData; • SOAP.
GUE 72.	<p>De Low-code Oplossing ondersteunt minimaal de volgende mogelijkheden voor het beveiligen van API's en/of webservices:</p> <ul style="list-style-type: none"> • TLS 1.3; • OAuth, SAML, OIDC (ondersteunt of mogelijkheid om in te bouwen); • Encryptie (door het Low-code Oplossing).
GUE 73.	<p>De Low-code Oplossing biedt de integratie met een On-premises Active Directory service op basis van LDAP (Lightweight Directory Access Protocol).</p>

Hoofdstuk 4. Beveiliging

4.1 Algemene eisen beveiligingsperspectief

Opdrachtgever vindt het van belang dat zijn Data en Processen veilig zijn. Data moeten beschikbaar zijn, maar ook betrouwbaar (niet onbevoegd gewijzigd) en alleen toegankelijk voor de personen die die Data daadwerkelijk nodig hebben.

UE 4.	Opdrachtnemer conformeert zich aan Geheimhoudingsplicht (artikel 3.13.8 Reglement Personeelsvoorschriften Belastingdienst), Huisregels kritische ruimten en richtlijnen Fotograferen en Filmen. Personeel van Opdrachtnemer die het datacenter betreden dienen bijgevoegde verklaring (Bijlage 7. Algemene verklaring kritische ruimten en na ondertekening van de Overeenkomst, Bijlage C van de Overeenkomst) te ondertekenen
-------	---

Data dient verwerkt (onder andere: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen) te worden in de Economische Europese Ruimte (EER) en landen waarvan de Europese Commissie bepaald heeft dat in deze landen een passend beveiligingsniveau is. Voor Processen geldt iets gelijksoortigs: het gaat erom dat Processen niet negatief beïnvloed mogen worden: van totale onbeschikbaarheid tot en met het kunnen aanpassen van flows binnen de Processen.

4.2 Informatiebeveiligingsbeleid

De Opdrachtgever is gehouden op in Nederland van toepassing zijnde wet- en regelgeving en specifiek aan de **Baseline Informatiebeveiliging Overheid (BIO)** (Bijlage 8. BIO2 – versie 1.3). Deze regelgeving is gebaseerd op de NEN/ISO 27001:2017 en de NEN/ISO 27002:2022, en bevat daarnaast aanvullende beveiligingseisen. Vanwege de eigen technische inrichting, stelt de Opdrachtgever zelf ook specifieke beveiligingseisen. De opzet, bestaan en werking kunnen worden gecontroleerd middels Audits en beveiligings- en continuïteitstesten. Dit is geborgd via de contractdocumenten van de Opdrachtgever.

De Opdrachtnemer dient minimaal hetzelfde beveiligingsniveau te leveren als de Opdrachtgever. Opdrachtnemer heeft een informatiebeveiligingsbeleid. De Opdrachtgever neemt richting de markt ISO27001/2 als uitgangspunt. Opzet, bestaan en werking van het informatiebeveiligingsbeleid met betrekking tot datgene dat geleverd gaat worden moet worden aangetoond voor Gunning én gedurende de looptijd van de Overeenkomst.

Opdrachtgever accepteert, onder voorwaarden, ook borging van het informatiebeveiligingsbeleid gelijkwaardig aan ISO27001/2. Deze gelijkwaardigheid dient aangetoond te worden door Opdrachtnemer.

De Opdrachtgever zelf is gehouden aan de Baseline Informatiebeveiliging Overheid (BIO). Als Opdrachtgever zal de Opdrachtgever relevante maatregelen in eisen verwoorden, zodat hij zijn verantwoordelijkheid ook kan nemen. Dit onderdeel is samengevoegd met de Opdrachtgever specifieke eisen.

4.3 Wet- en regelgeving

De Opdrachtnemer dient alle passende en nodige maatregelen te hebben getroffen en te treffen om de Opdrachtgever in staat te stellen deze taak uit te voeren en haar verantwoordelijkheid te kunnen nemen. Een belangrijk kader in de te nemen Beveiligings(maatregelen) zijn de vigerende wetgeving en standaarden ten aanzien van ICT-Beveiliging en privacy.

Opdrachtgever hecht veel belang aan de Beveiliging van Data. De Opdrachtgever heeft een taak en verantwoordelijkheid om ervoor te zorgen dat Data nooit in onbevoegde handen vallen of kunnen vallen. De Opdrachtnemer dient alle passende en nodige maatregelen te hebben getroffen en te treffen om de Opdrachtgever in staat te stellen deze taak uit te voeren en haar verantwoordelijkheid te kunnen nemen. Een belangrijk kader in de te nemen beveiligingsmaatregelen zijn de vigerende wetgeving en standaarden ten aanzien van ICT-Beveiliging en privacy.

GUE 74.	De Opdrachtnemer en de Low-code Oplossing voldoen aan de vigerende Nederlandse Wet- en Regelgeving.
---------	---

4.4 Data

Data van de Opdrachtgever worden gescheiden verwerkt (waaronder opgeslagen) van andere klanten van Opdrachtnemer: de Opdrachtgever heeft geen zicht in Data van andere klanten, andere klanten hebben geen zicht in de Data van de Opdrachtgever.

Personeel van Opdrachtnemer hebben alleen toegang tot de Data van de Opdrachtgever voor zover dat noodzakelijk is voor het uitvoeren van de Overeenkomst.

UE 5.	Data van de Opdrachtgever worden gescheiden opgeslagen van de Data van andere klanten van Opdrachtnemer. Toegang tot deze Data is beperkt tot de Opdrachtgever en –voor zover noodzakelijk voor het uitvoeren van de Overeenkomst- Opdrachtnemer.
-------	--

4.5 Data encryptie

In de context van een Low-code Oplossing is data-encryptie essentieel om gevoelige informatie te beschermen.

GUE 75.	De Low-code Oplossing biedt ondersteuning voor data-encryptie 'in rest' en 'in transition'.
---------	---

4.6 Specifieke eisen Beveiligingsbeleid

In deze paragraaf stelt de Opdrachtgever eisen die specifiek zijn voor de Opdrachtgever. Hier zijn ook eisen opgenomen om te borgen dat de Opdrachtgever aan het overheidsinformatiebeveiligingsbeleid (Baseline Informatiebeveiliging Overheid (BIO)) kan voldoen. De hier opgenomen eisen zijn dus aanvullend op wat reeds via certificering en de auditcyclus wordt uitgevraagd.

Het legt dus aan de ene kant accenten op onderdelen die reeds onderdeel uitmaken van een op 27001-gebaseerd informatiebeveiligingsbeleid, aangevuld met overheids- en Belastingdienst specifieke zaken.

4.6.1 Overheids- en Belastingdienstbeleid: Standaarden

Opdrachtgever is als overheidspartij gehouden aan de standaarden, zoals vastgesteld door het Forum Standaardisatie. De verplichte standaarden worden toegepast conform het Pas-toe-of-leg-uit-principe (Comply-or-Explain). Van een aantal standaarden heeft Opdrachtgever overigens vastgesteld dat Opdrachtnemer deze standaarden moet toepassen (dus zonder “Leg-uit”-mogelijkheid). Dit zijn de streefbeeldafspraken informatieveiligheid.

Dit is ook van toepassing gedurende de looptijd van de Overeenkomst. Als deze lijst met standaarden of de standaarden zelf inhoudelijk wijzigen zullen tussentijds afspraken gemaakt worden ter implementatie.

Forum Standaardisatie:

- Verplichte standaarden: <https://www.forumstandaardisatie.nl/open-standaarden/verplicht>
- Beslisboom Open standaarden: De Beslisboom Open Standaarden: <https://www.forumstandaardisatie.nl/beslisboom/beslisboom-open-standaarden>
- Streefbeeldafspraken informatieveiligheid: <https://www.forumstandaardisatie.nl/onderwerpen/veilig-internet/streefbeeldafspraken#:~:text=Wat%20is%20een%20streefbeeldafpraak%3F,van%20bestaan%20moeten%20worden%20toegepast>

UE 6.	<p>Opdrachtgever committeert zich aan het gebruik van de van toepassing zijnde en de verplichte standaarden van het Forum Standaardisatie in relatie tot de Low-code Oplossing. Het betreft de volgende streefbeeldafspraken informatieveiligheid conform https://www.forumstandaardisatie.nl/onderwerpen/veilig-internet/streefbeeldafspraken:</p> <ul style="list-style-type: none"> • Ades Baseline Profiles De ‘AdES Baseline Profiles’ moeten worden toegepast op de ondertekening van XML-, CMS-, PDF- en ZIP-bestanden met geavanceerde en/of gekwalificeerde elektronische handtekeningen, zegels of tijdstempels. • Digikoppeling Digikoppeling moet worden toegepast bij digitale gegevensuitwisseling die plaatsvindt met voorzieningen die onderdeel zijn van de GDI, waaronder de basisregistraties, of die sector overstijgend is. De verplichting geldt voor gegevensuitwisseling tussen systemen waarbij er noodzaak is voor tweezijdige authenticatie. Geautomatiseerde gegevensuitwisseling tussen informatiesystemen op basis van NEN3610 is uitgesloten van het functioneel toepassingsgebied. • Digitoegankelijk (EN 301 549 met WCAG 2.1) Digitoegankelijk (EN 301 549 met WCAG 2.1) moet worden toegepast op het aanbieden van webgebaseerde informatie-, interactie-, transactie- en participatiediensten. • HTTPS en HSTS HTTPS en HSTS moeten worden toegepast op de communicatie tussen clients (zoals webbrowsers) en servers voor alle websites en webservices. • IPv6 IPv6 moet op digitale diensten en op netwerken en apparaten worden toegepast. Dit betekent ten eerste dat digitale diensten, zoals websites en e-mail servers, bereikbaar moeten zijn via IPv6. Ten tweede betekent dit dat netwerken IPv6 moeten aanbieden en dat apparaten zo moeten worden geconfigureerd dat IPv6 wordt gebruikt indien aangeboden. In veel gevallen zal het vanwege interoperabiliteit noodzakelijk blijven om naast IPv6 ook IPv4 toe te passen. • NL GOV Assurance Profile for OAuth 2.0 NL GOV Assurance Profile for OAuth 2.0 moet worden toegepast bij applicaties waarbij gebruikers of ‘resource owners’ impliciet of expliciet toestemming geven aan een dienst van een derde om namens deze toegang te krijgen tot Data via een REST API waarvoor ze recht van toegang hebben. • Open API Specification OAS moet worden toegepast op het beschrijven/specificeren van een REST API.
-------	--

	<ul style="list-style-type: none"> • REST-API ‘Design Rules’ De standaard REST-API ‘Design Rules’ moet worden toegepast bij het aanbieden van REST API’s ten behoeve van het ontsluiten van overheidsinformatie en/of functionaliteit. • TLS TLS moet worden toegepast op de uitwisseling van Data tussen clients en servers, inclusief machine-to-machine communicatie.
GUE 76.	De Low-code Oplossing moet OAS3.x in alle onderdelen en gebruik ondersteunen.
GUE 77.	De Low-code Oplossing ondersteunt Single Sign On (SSO) via Security Assertion Markup Language (SAML) en OIDC.

4.6.2 Design & Runtime

Binnen een Low-code Oplossing dienen de OWASP-risico's op zowel designniveau als runtime-niveau te worden afgevangen.

GUE 78.	De Low-code Oplossing ondersteunt geïntegreerde beveiligingsmaatregelen tegen veel voorkomende Beveiligingsincidenten zoals, maar niet gelimiteerd tot de actuele OWASP top 10 en OWASP Top 10 Low-code / no-code.
---------	--

4.6.3 Quantumveilige cryptografie

Door quantumtechnologie (QT) kan binnen afzienbare termijn een situatie ontstaan dat de bepaalde mate en sterkte van de van toepassing zijnde versleuteling ontoereikend is om de beschikbaarheid, integriteit en vertrouwelijkheid van informatiesystemen, processen en Data van Opdrachtgever in de toekomst te waarborgen. Ook vandaag is er al sprake van dreiging, vanwege het zogeheten 'steal now, decrypt later'-scenario en moeten extra beveiligingsmaatregelen getroffen worden, bijvoorbeeld door het gebruik van TLS1.3 met hybride configuratie van Post-Quantum Cryptografie voor quantumveilige verbindingen.

Opdrachtgever bereidt zich voor op mogelijke QT-risico's door te bewegen richting 'crypto agility' en quantumveilige cryptografie, conform richtlijnen van de AIVD en het NCSC en anticiperend op in ontwikkeling zijnde wet- en regelgeving rondom quantumveiligheid. In het verlengde daarvan dienen ook de betrokken marktpartijen van gecontracteerde en te contracteren oplossingen, producten en/of diensten stappen te zetten in die richting, ten aanzien van door hen geleverde c.q. te leveren oplossingen, producten en/of diensten, alsmede ten aanzien van hun bedrijfsvoering daaromtrent. Voor meer informatie, zie: <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/quantumveilige-cryptografie> en publicaties van de AIVD en NCSC.

Het ligt voor de hand dat ten aanzien van de Low-code Oplossing, risico's met betrekking tot de (toegang tot) Data, zijn of worden gemitigeerd door middel van adequate versleuteling. Dat geldt ook voor de bij Opdrachtnemer en/of Fabrikant zelf in gebruik zijnde informatiesystemen, bedrijfsprocessen en Data voor zover deze van invloed (kunnen) zijn op de Low-code Oplossing (hieronder samengevat als de bedrijfsvoering).

In dat kader heeft Opdrachtgever onderstaande Specificaties opgesteld met betrekking tot de onderhavige verwerving.

Opdrachtnemer is zich bewust van mogelijke QT-risico's die zich nu en in de toekomst bij Opdrachtgever kunnen manifesteren door het gebruik van de Low-code Oplossing of via de bedrijfsvoering.

GUE 79.	Opdrachtnemer heeft zich verdiept, en zal zich in de toekomst blijvend verdiepen, in initiatieven, kaders, wet- en regelgeving, best practices en dergelijke publicaties ten aanzien van QT-risico's die betrekking (kunnen) hebben op de Low-code Oplossing, of op de bedrijfsvoering. Relevante informatie uit de genoemde publicaties is of wordt verwerkt in de Low-code Oplossing en in de bedrijfsvoering, zodat risico's op het gebied van QT in toekomstige ontwikkelingen adequaat worden gemitigeerd.
GUE 80.	De Low-code Oplossing is ten tijde van aanvang van de Realisatie fase compatibel met OpenShift versie 4.18 (Kubernetes). Hierdoor kan door de Low-code Oplossing gebruik gemaakt worden van door OpenShift geleverde ondersteuning van quantumveilige cryptografie.
UE 7.	<p>Opdrachtnemer levert binnen 3 maanden na ingangsdatum van de Overeenkomst een Roadmap quantumveiligheid op voor de Low-code Oplossing. Deze Roadmap zal vervolgens halfjaarlijks worden geactualiseerd. Hierin zijn minimaal de volgende onderwerpen uitgewerkt:</p> <ul style="list-style-type: none"> • De aanwezigheid van een actuele inventaris van de Cryptografische Assets die deel uitmaken van de Low-code Oplossing, tot welke datum deze inventaris is bijgewerkt, en indien deze inventaris niet aanwezig is, via welke stappen en binnen welk tijdsbestek Opdrachtnemer voornemens is een dergelijke inventaris aan te leggen; • De beschikbaarheid van Cryptographic Bill Of Materials (hierna: CBOM) informatie voor de Low-code Oplossing, en of deze in zijn geheel of specifieke onderdelen hiervan gedeeld kunnen worden met de Opdrachtgever. Indien een CBOM niet beschikbaar is voor de Low-code Oplossing, geeft Opdrachtnemer aan of Opdrachtnemer voornemens is CBOM te genereren voor de Low-code Oplossing, via welke stappen en binnen welk tijdsbestek. • De concrete stappen die Opdrachtnemer op korte en middellange termijn zet om in de Low-code Oplossing gebruikte cryptografie quantumveilig te maken, waarbij minimaal de volgende onderwerpen benoemd worden: <ul style="list-style-type: none"> ○ TLS ○ SSH ○ IPSEC ○ Certificaten ○ Cryptografische libraries ○ Cryptografische configuraties ○ Cryptografisch sleutelbeheer • De actuele Certificate Lifespan die binnen en voor gebruik van de Low-code Oplossing wordt toegepast (voor zo ver niet in beheer bij de Opdrachtgever). Indien er verschillende Certificate Lifespans worden toegepast, wordt de geldigheidstermijn per toepassingsgebied gespecificeerd. • Relevante ontwikkelingen ten aanzien van quantumveiligheid en cryptografie in de bedrijfsvoering van Opdrachtnemer. <p>De omvang van de Roadmap quantumveiligheid is beperkt, bij voorkeur maximaal 3 vel A4, inclusief illustraties/figuren.</p> <p>De Roadmap dient daarbij te zijn gebaseerd op de volgende bronnen of diens opvolgende versies:</p> <ul style="list-style-type: none"> • PQC Migratiehandboek van de AIVD: https://www.aivd.nl/documenten/2024/12/3/het-pqc-migratie-handboek • NCSC Richtlijn TLS mei 2025: https://www.ncsc.nl/wat-kun-je-zelf-doen/documenten/publicaties/2025/juni/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2025-05 • NIST PQC project: https://csrc.nist.gov/projects/post-quantum-cryptography • Vigerende wet- en regelgeving rondom quantumveiligheid en cryptografie (zoals bijvoorbeeld NIS2 en het Rijksbrede beleidskader)

	<p>cryptografie: https://www.digitaleoverheid.nl/document/rijksbreed-beleidskader-cryptografie/)</p> <p>Opdrachtgever is bereid om hiervoor een zogenaamd non-disclosure agreement (NDA) te tekenen, zodat eventuele (commerciële) vertrouwelijkheid rond informatie gewaarborgd is.</p>
UE 8.	<p>Indien gedurende de looptijd van de Overeenkomst via Nederlandse of Europese wet- en regelgeving een Cryptographic Bill of Materials (CBOM) vereist wordt voor de Opdrachtgever, draagt Opdrachtnemer zorg dat met de Low-code Oplossing een CBOM automatisch gegenereerd kan worden voor de met de Low-code Oplossing te ontwikkelen Low-code Applicaties.</p>
UE 9.	<p>Indien aan de hand van een CBOM cryptografische Kwetsbaarheden worden gevonden in een met de Low-code Oplossing te ontwikkelen Low-code Applicatie, welke direct terug te leiden zijn tot de Low-code Oplossing, is de Opdrachtnemer verantwoordelijk -op zijn eigen kosten- deze Kwetsbaarheden op te lossen.</p> <p>Als er geen veilige versie van de kwetsbare cryptografische toepassing beschikbaar is, dan wordt dit gemeld als Beveiligingsincident.</p>
W 2.	<p>Quantumveiligheid</p> <p>Met de doorontwikkeling van quantumtechnologie ontstaat een nieuw type computersystemen dat ongekende mogelijkheden geeft. Naast veelbelovende kansen dient zich de dreiging aan dat cryptografische versleutelingen niet meer veilig zullen zijn. Daarbij komt dat met het zogeheten ‘steal now, decrypt later’-scenario ook vandaag al sprake is van dreiging. opdrachtgever vindt het belangrijk om te bewegen richting ‘crypto agility’ en de implementatie van quantumveilige cryptografie. ‘Crypto agility’ betekent dat een organisatie gemakkelijk geïmplementeerde cryptografische primitieven kan aanpassen of vervangen zonder dat dit tot Incidenten leidt. Voor meer informatie, zie: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/quantumveilige-cryptografie.</p> <p>Vraag</p> <p>Inschrijver wordt verzocht aan te geven op welke wijze er voorbereidingen getroffen worden om de risico's en dreiging die uitgaan van quantumtechnologie te mitigeren. Daarbij dient ook beschreven te worden wat de impact daarvan is op de te leveren Diensten en producten. In uw antwoord dienen in ieder geval de volgende onderdelen terug te komen:</p> <ol style="list-style-type: none"> 1. Op welke wijze u inzicht heeft in de cryptografische technieken en algoritmes die deel uitmaken van (de systemen die deel uitmaken van) de door u geleverde Diensten en producten. 2. Wat op hoofdlijnen de impact is van doorontwikkelde quantum computers op de cryptografische technieken en algoritmes die deel uitmaken van (de systemen die deel uitmaken van) de door u geleverde Diensten en producten. 3. Of u beschikt over een migratieplan voor de migratie naar quantumveilige cryptografie en zo ja, de status daarvan. 4. Welke verschillende stappen en mijlpalen u ziet in het migratieproces die de door u geleverde Diensten en producten raken. 5. De wijze waarop u ‘crypto agility’, of stappen in die richting, realiseert in de door u geleverde Diensten en producten. 6. Op welke wijze uw organisatie samen met Opdrachtgever kan verifiëren dat Updates en aanpassingen leiden tot correcte werking en inzetbaarheid van de door u geleverde Diensten en producten. Achtergrond is dat het voor sommige cryptografische implementaties van belang is dat beide partijen eenzelfde of complementaire implementatie hebben toegepast voor een correcte werking. Beschrijf ook hoe eventuele knelpunten kunnen worden verholpen. <p>In uw uitwerking dient u de bovenstaande 6 onderwerpen puntsgewijs uit te werken. U dient hierbij rekening te houden met hetgeen in de Aanbestedingsdocumenten verwoord is.</p> <p>Uw uitwerking bestaat uit maximaal <u>6 pagina's A4</u> (lettertype Arial, lettergrootte 10, regelafstand 1,0) mag geen verwijzingen en hyperlinks bevatten. Extra pagina's worden niet beoordeeld. U dient bij de uitwerking de structuur van de Wens aan te houden (1 t/m 6).</p>

	<p>Voor deze Wens kunt u <u>maximaal 10 punten</u> verdienen.</p> <p>De beoordelingscriteria per uitgewerkt onderdeel (1 t/m 6) van deze Wens zijn:</p> <ol style="list-style-type: none"> Voor de onderdelen 1 t/m 5: de mate waarin de beantwoording van onderdelen 1 t/m 5 Opdrachtgever concreet en volledig is en overtuigt dat uw organisatie gestructureerd toe werkt naar implementatie van 'crypto agility' en quantumveilige cryptografie in de door u geleverde Diensten en producten (en de systemen die daarvan deel uitmaken); Voor onderdeel 6: De manier waarop de beantwoording concreet en volledig uitwerking geeft aan gezamenlijke verantwoordelijkheid van uw organisatie en Opdrachtgever rondom de inzet van quantumveilige cryptografie. <p>Beoordelingskader</p> <p>De uitwerking van de Wens wordt hierbij als geheel beoordeeld. Het is niet zo dat er per onderdeel een score wordt gegeven.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #0056b3; color: white;"> <th style="text-align: left;">Beoordeling / aantal punten</th> <th style="text-align: left;">Toelichting</th> </tr> </thead> <tbody> <tr> <td>Niet beantwoord 0 punten</td> <td>De Wens is in zijn geheel niet beantwoord. Indien wel een uitwerking is gegeven aan het gevraagde en deze uitwerking aantoonbaar geen betrekking heeft op de betreffende Wens en/of de wens in zijn geheel niet beoordeeld kan worden, wordt ook 0 punten toegekend.</td> </tr> <tr> <td>Onvoldoende 2 punten</td> <td>Een deel van de Wens is niet beantwoord en/of de beantwoording sluit niet of nauwelijks aan bij de betreffende Wens en/of de Wens kan slechts gedeeltelijk beoordeeld worden.</td> </tr> <tr> <td>Matig 4 punten</td> <td>De Wens wordt niet volledig beantwoord en wordt niet volledig en onvoldoende onderbouwd.</td> </tr> <tr> <td>Voldoende 6 punten</td> <td>De Wens wordt volledig beantwoord, maar niet volledig en voldoende onderbouwd.</td> </tr> <tr> <td>Goed 8 punten</td> <td>De Wens wordt volledig beantwoord en volledig en voldoende onderbouwd.</td> </tr> <tr> <td>Uitstekend 10 punten</td> <td>De Wens wordt volledig beantwoord en onderbouwd, daarnaast bestaat het antwoord uit positieve, verrassende en vernieuwende elementen waardoor de Wens wordt beoordeeld als uitstekend.</td> </tr> </tbody> </table>	Beoordeling / aantal punten	Toelichting	Niet beantwoord 0 punten	De Wens is in zijn geheel niet beantwoord. Indien wel een uitwerking is gegeven aan het gevraagde en deze uitwerking aantoonbaar geen betrekking heeft op de betreffende Wens en/of de wens in zijn geheel niet beoordeeld kan worden, wordt ook 0 punten toegekend.	Onvoldoende 2 punten	Een deel van de Wens is niet beantwoord en/of de beantwoording sluit niet of nauwelijks aan bij de betreffende Wens en/of de Wens kan slechts gedeeltelijk beoordeeld worden.	Matig 4 punten	De Wens wordt niet volledig beantwoord en wordt niet volledig en onvoldoende onderbouwd.	Voldoende 6 punten	De Wens wordt volledig beantwoord, maar niet volledig en voldoende onderbouwd.	Goed 8 punten	De Wens wordt volledig beantwoord en volledig en voldoende onderbouwd.	Uitstekend 10 punten	De Wens wordt volledig beantwoord en onderbouwd, daarnaast bestaat het antwoord uit positieve, verrassende en vernieuwende elementen waardoor de Wens wordt beoordeeld als uitstekend.
Beoordeling / aantal punten	Toelichting														
Niet beantwoord 0 punten	De Wens is in zijn geheel niet beantwoord. Indien wel een uitwerking is gegeven aan het gevraagde en deze uitwerking aantoonbaar geen betrekking heeft op de betreffende Wens en/of de wens in zijn geheel niet beoordeeld kan worden, wordt ook 0 punten toegekend.														
Onvoldoende 2 punten	Een deel van de Wens is niet beantwoord en/of de beantwoording sluit niet of nauwelijks aan bij de betreffende Wens en/of de Wens kan slechts gedeeltelijk beoordeeld worden.														
Matig 4 punten	De Wens wordt niet volledig beantwoord en wordt niet volledig en onvoldoende onderbouwd.														
Voldoende 6 punten	De Wens wordt volledig beantwoord, maar niet volledig en voldoende onderbouwd.														
Goed 8 punten	De Wens wordt volledig beantwoord en volledig en voldoende onderbouwd.														
Uitstekend 10 punten	De Wens wordt volledig beantwoord en onderbouwd, daarnaast bestaat het antwoord uit positieve, verrassende en vernieuwende elementen waardoor de Wens wordt beoordeeld als uitstekend.														

4.6.4 Richtlijnen rond Beveiligingsincidenten en ontdekken Kwetsbaarheden

Voor Beveiligingsincidenten geldt dat bij ontdekking/melding zowel de Impact als Urgentie als Hoog worden gekwalificeerd, wat resulteert in een Prioriteit 1 Incident. Een Beveiligingsincident wordt altijd per direct opgevolgd met een actie van de Opdrachtnemer. Na een eerste evaluatie kan onderbouwd besloten worden de Prioriteit te verlagen. De Opdrachtgever heeft hierbij het laatste woord. Er worden vier typen Beveiligingsincident onderkend:

- (Cyber)hack, of een poging daartoe. Dit is inclusief malware.
- Coordinated Vulnerability Disclosure (CVD, voorheen: Responsible disclosure).
- Kwetsbaarheid via CVE-database of Security Note van leverancier van ICT-component of beveiligingsberichten van CERTs (NCSC, Digital Trust Center, bedrijfstak- of sectorgerichte CERT).
- Kwetsbaarheid vanuit beveiligingstest (A&P-test of Vulnerability Scan).

Als waarderingsmethodiek voor Kwetsbaarheden wordt gebruik gemaakt van de meest recente versie van marktstandaard Common Vulnerability Score System (CVSS, momenteel versie 4.0). Oplostermijnen die hieraan gekoppeld zijn, zijn:

- Kritisch risico (Critical risk, score 9.0 – 10.0): per direct (voor in Productie gaan van een nieuwe Low-code Oplossing is dit belemmerend). Voor de Opdrachtgever is dit een Incident.
- Hoog risico (high risk, score 7.0 – 8.9): per direct, na afstemming maximaal 1 maand (voor in Productie gaan van een nieuwe Low-code Oplossing is dit belemmerend). Voor de Opdrachtgever is dit een Incident.
- Gemiddeld risico (Medium risk, score 4.0 – 6.9): 3 maanden. Voor de Opdrachtgever is dit een Probleem.
- Laag risico (Low risk, 0.1 – 3.9): 6 maanden. Voor de Opdrachtgever is dit een Probleem.

De Opdrachtgever heeft geen Low-code Oplossingen in Productie staan waarin zich Kwetsbaarheden bevinden die als kritisch of hoog risico zijn gekwalificeerd. Bij kritische- en hoge risico's kan een Leg-uit alleen gebruikt worden om de Oplostijd (beperkt) op te rekken. Dit kan alleen met nadrukkelijke instemming van de Opdrachtgever. De Opdrachtgever kan besluiten dat Data onbeschikbaar gemaakt moeten worden en dat de Low-code Oplossing geheel dan wel gedeeltelijk onbeschikbaar gemaakt moet worden. Staat de Low-code Oplossing nog niet in Productie dan zal inproductienaam niet mogen totdat de kritische- en hoge risicobevindingen zijn weggenomen. Bekende Kwetsbaarheden worden onverwijld gemeld. Gemiddeld- en laag risicobevindingen worden afgehandeld conform het "Pas-toe-of-Leg-uitprincipe". Dit laatste, een Leg uit (explain), betekent dat er besloten is dat de Kwetsbaarheid niet weggenomen wordt of dat adresseren ervan meer tijd gaat kosten dan de standaard Oplostijd. Opdrachtnemer onderbouwt zijn besluit (bijvoorbeeld: er zijn afdoende mitigerende maatregelen getroffen waardoor de Kwetsbaarheid niet uitgevoerd hoeft te worden of dat de impact nihil is). Het is aan de Opdrachtgever om akkoord te gaan met een "Leg-uit".

UE 10.	Opdrachtnemer conformeert zich aan de door de Opdrachtgever gebruikte methode (CVSS 4.0) om Beveiligingsincidenten te kwalificeren en heeft zijn organisatie zodanig ingericht dat de door de Opdrachtgever onderkende typen Beveiligingsincidenten voor (onderdelen) van de Low-code Oplossing binnen gestelde termijnen opgepakt en opgelost (patchmanagement) worden: <ul style="list-style-type: none"> • Kritisch risico (critical risk): per direct (belemmerend voor in Productie gaan); • Hoog risico (high risk): 1 maand (belemmerend voor in Productie gaan); • Gemiddeld risico (medium risk): 3 maanden; • Laag risico (low risk): 6 maanden.
UE 11.	Opdrachtnemer conformeert zich aan onderstaande: <ul style="list-style-type: none"> • Indien er gegronde redenen zijn om een Kwetsbaarheid die als 'gemiddeld' of 'laag' is geclassificeerd, niet te verhelpen, dan bespreekt Opdrachtnemer dit met Opdrachtgever. • Zolang Opdrachtnemer geen contact opneemt met Opdrachtgever blijft de Oplostijd conform CVSS doorlopen.
UE 12.	In de Low-code Oplossing gebruikte Open Source-code en libraries van andere leveranciers bevatten geen bekende Kwetsbaarheden. Er wordt gebruik gemaakt van de meest recente veilige versies. Als er geen veilige versie beschikbaar is dan wordt dit gemeld als Beveiligingsincident.
UE 13.	Indien gedurende de looptijd van de Overeenkomst via Nederlandse of Europese wet- en regelgeving een Software Bill of Materials (SBOM) vereist wordt voor de Opdrachtgever, draagt Opdrachtnemer zorg dat met de Low-code Oplossing een SBOM automatisch gegenereerd kan worden voor de met de Low-code Oplossing te ontwikkelen Low-code Applicaties.
UE 14.	Indien aan de hand van een Software Bill of Materials (SBOM) Kwetsbaarheden worden gevonden in een met de Low-code Oplossing te ontwikkelen Low-code Applicatie, welke direct terug te leiden zijn tot de Low-code Oplossing, is de Opdrachtnemer verantwoordelijk -op zijn eigen kosten- deze Kwetsbaarheden op te lossen. Als er geen veilige versie van de kwetsbare Open Source-code of Library beschikbaar is, dan wordt dit gemeld als Beveiligingsincident.

4.6.5 Coördinated Vulnerability Disclose

De Opdrachtgever heeft een Coördinated Vulnerability Disclosure-procedure (CVD-procedure). Goedwillende beveiligingsonderzoekers kunnen via een vastgesteld proces Kwetsbaarheden, mits er geen wetten worden

overtreden, melden. Het CVD-proces is op deze pagina beschreven:

https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/standaard_functies/prive/contact/fraude_misd_aad_en_misstanden_melden/datalek-beveiligingslek-misbruik-computersystemen/datalek-beveiligingslek-misbruik-computersystemen#coordinated-vulnerability-disclosure

UE 15.	Opdrachtnemer handelt via de Opdrachtgever gemelde CVD-meldingen af conform het CVD-beleid van de Opdrachtgever. Dit proces zal door Opdrachtnemer beschreven worden in de DAP.
--------	---

4.7 Beveiligingstesten

UE 16.	<p>Opdrachtnemer levert een veilige Low-code Oplossing. Dit wordt aangetoond middels uit te voeren beveiligings- en/of Acceptatietesten vóór in gebruikname en periodiek gedurende de levensduur van de Low-code Oplossing.</p> <p>A&P-testen worden minimaal jaarlijks of na een significante wijziging van de Low-code Oplossing uitgevoerd door Opdrachtnemer.</p> <p>Vulnerability Scans worden minimaal maandelijks uitgevoerd. Er wordt gebruik gemaakt van de meest recente marktinzichten, tooling en definitiebestanden.</p>
UE 17.	<p>Opdrachtgever kan (op basis van een risico-inschatting) het noodzakelijk achten een A&P-test uit te laten voeren op de Low-code Oplossing. De precieze invulling van de A&P-test is afhankelijk van de situatie. Het organiseren van deze A&P-test gebeurt door de Opdrachtgever en de kosten van het uitvoeren van de A&P-test zelf zijn voor rekening van de Opdrachtgever.</p> <p>Eventuele Kwetsbaarheden worden conform de paragraaf 4.6.4 "Richtlijnen rond Beveiligingsincidenten en ontdekken Kwetsbaarheden" van de Opdrachtgever opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan.</p>

4.8 Autorisatie en Authenticatie

De Low-code Oplossing en Data mogen alleen gebruikt worden door bevoegde personen. Dit gebeurt door middel van identificatie, authenticatie en autorisatie. Aanvullend kan gekozen worden voor een vorm van multi-factor authentication

Bij authenticatie kan het nodig zijn aanvullend bewijs te leveren. Dit kan door een aanvullende verificatiecode te vragen. Dit gebeurt middels two-factor authentication.

Een gebruikersaccount is altijd te herleiden naar een Natuurlijk Persoon. Uitzondering zijn gedocumenteerde en geregistreerde systeemaccounts (bijvoorbeeld voor koppelingen).

Identificatie, autorisatie en authenticatie heeft alleen betrekking op Eindgebruikers en niet op bezoekers van een publieke website. Bezoekers kunnen zonder identificatie toegang krijgen tot het openbare gedeelte van de Low-code Oplossing. Een Low-code Oplossing heeft alleen een openbaar gedeelte als dit nadrukkelijk geëist is door de Opdrachtgever.

UE 18.	Het beheer van toegangsrechten voor de Low-code Oplossing, inclusief de bewaking van functiescheiding en het gebruik van groepsrollen, geschiedt vanuit één door de Opdrachtnemer geboden (logisch) Identity Managementsysteem (IMS).
UE 19.	Indien de Low-code Oplossing gebruik maakt van een gebruikersidentificatie (gebruikersaccount), is deze altijd één op één herleidbaar naar een Natuurlijk Persoon.

De Opdrachtgever stelt de volgende algemene eisen aan authenticatie. Zo is het gebruik van intern gebruikte userIDs niet toegestaan (mailadres van werk mag wel). Voor de Opdrachtgever zijn ook minimale vereisten voor wachtwoorden van toepassing.

UE 20.	Als identificatie is het gebruik van het user ID van de Opdrachtgever niet toegestaan.
UE 21.	<p>Wachtwoorden voldoen minimaal aan de eisen zoals gesteld in de BIO (zie Bijlage 8.):</p> <p>Algemeen (technisch afdwingen):</p> <ul style="list-style-type: none"> • Gebruik van wachtwoorden wordt geautomatiseerd afgedwongen; • Initiële wachtwoorden (inclusief de gereset zijn) zijn een Werkdag geldig en worden bij eerste gebruik gewijzigd; • Eisen aan wachtwoorden worden geautomatiseerd afgedwongen; • Minimaal 12 posities, complex (nummers, klein, groot); • Aantal foutieve inlogpogingen: 10. In dat geval: blokkering account; • Minimaal jaarlijks vernieuwen. <p>Indien het authenticatieproces is gekoppeld aan dat van de Opdrachtgever dan zijn de richtlijnen van de Opdrachtgever leidend.</p>
GUE 81.	<p>De Low-code Oplossing biedt out of the box functionaliteit voor het integreren van de externe identity-manager Microsoft Active Directory ten behoeve van autorisatie en authenticatie op basis van:</p> <ul style="list-style-type: none"> • OIDC en • SAML.

Hoofdstuk 5. Documentatie

UE 22.	Opdrachtnemer zal Opdrachtgever tijdig voorzien van actuele en volledige Documentatie in elektronische vorm, ten behoeve van de Low-code Oplossing. Hierbij is de Documentatie over de eigenschappen en gebruiksmogelijkheden van de Low-code Oplossing in de Nederlandse en/of Engelse taal.
UE 23.	De Documentatie dient zodanig te zijn dat zij een juiste, volledige en gedetailleerde beschrijving geeft van de door Opdrachtnemer te leveren Low-code Oplossing en de functies daarvan, zodat DevOps-medewerkers op eenvoudige wijze van alle mogelijkheden van de Low-code Oplossing gebruik kunnen maken.
UE 24.	Opdrachtgever mag de Documentatie voor gebruik binnen de eigen organisatie zonder bijkomende kosten verspreiden.
UE 25.	Opdrachtnemer zal de door hem geleverde Documentatie zo spoedig mogelijk vervangen, wijzigen of aanpassen indien op enig tijdstip tijdens het gebruik door Opdrachtgever van de Low-code Oplossing, blijkt dat de Documentatie onjuiste informatie bevat of anderszins onvolledig, onvoldoende, onduidelijk en/of verouderd is.
UE 26.	Opdrachtnemer is verantwoordelijk dat Documentatie na een nieuwe Release van de Low-code Oplossing actueel blijft. Bij Oplevering van een nieuwe Release van de Low-code Oplossing wordt de geactualiseerde Documentatie digitaal beschikbaar gesteld.

Hoofdstuk 6. Realisatie fase

6.1 Inleiding

De scope van de opdracht bestaat uit twee fases:

1. Realisatie fase
2. Operationele fase

Na definitieve gunning en ondertekening van de Overeenkomst start de eerste fase, de Realisatie fase. De Operationele fase is in het volgende hoofdstuk uitgewerkt. De Realisatie bestaat uit de geïnstalleerde, geïmplementeerde en geconfigureerde Low-code Oplossing. Opdrachtnemer verzorgt een complete inrichting van een Productiewaardige Low-code Oplossing. Voor de beschikbaarheid van het On-premises Red Hat OpenShift containerplatform zorgt de Opdrachtgever. Het team IV GV/GOS/LIV van de Opdrachtgever is het aanspreekpunt richting de interne organisatie. De Opdrachtnemer dient de Realisatie uit te voeren conform het definitief te maken Plan van Aanpak Realisatie in samenwerking met de Opdrachtgever. Aansluitend op de contractondertekening wordt het concept Plan van Aanpak Realisatie nader besproken en uitgelijnd met de omgeving van de Opdrachtgever.

6.2 Concept Plan van Aanpak Realisatie

Om inzicht te krijgen op welke wijze de Opdrachtnemer de Realisatie uit gaat voeren, wordt aan de Opdrachtnemer gevraagd bij haar Inschrijving, ten behoeve van Wens 3, een concept Plan van Aanpak (PvA) Realisatie fase mee te sturen. Het concept PvA heeft betrekking op Realisatie en het in gebruik nemen van de Productiewaardige Low-code Oplossing. Het heeft de voorkeur dat de Realisatie van de Low-code Oplossing conform 'best practices' wordt aangeboden, ingericht en nader geconfigureerd wordt ten einde passend te zijn voor de Opdrachtgever.

GUE 82.	De Opdrachtnemer levert bij Inschrijving een concept PvA voor de Realisatie van de Low-code Oplossing bij de Opdrachtgever aan en behandelt daarin de 6 onderwerpen zoals deze in Wens 3. "Concept Plan van Aanpak Realisatie" zijn omschreven. Het concept PvA is onderdeel van het aanbod door de Opdrachtnemer en zal tijdens de beoordelingsprocedure door de Opdrachtgever worden beoordeeld. In het concept PvA dient rekening te worden gehouden dat de Low-code Oplossing, vanaf ingangsdatum Overeenkomst, uiterlijk binnen 3 maanden is gerealiseerd, Geaccepteerd is en daarmee in Productie staat (Productiewaardige Low-code Oplossing).
UE 27.	De Low-Code Oplossing dient binnen 3 maanden na ingangsdatum van de Overeenkomst Productiewaardig te zijn en in gebruik genomen te kunnen worden door de Opdrachtgever
W 3.	<p>Concept Plan van Aanpak Realisatie Opdrachtgever wenst een beheerste Realisatie van de door Opdrachtnemer aangeboden Oplossing. De Realisatie dient als onlosmakelijk onderdeel van de aanbieding gezien te worden en projectmatig te worden uitgevoerd binnen de gestelde kaders.</p> <p>Het concept Plan van Aanpak (PvA) heeft betrekking op de Realisatie van de Oplossing. In de tijd vanaf het moment van ondertekening contract tot en met het moment waarop de laatste Acceptatietest(en) zijn uitgevoerd en positief zijn afgerond. De Acceptatietesten worden uitgevoerd door de Opdrachtgever. Opdrachtnemer dient ondersteuning te leveren bij de Acceptatietesten en eventuele Bevindingen op te lossen.</p> <p>Vraag Inschrijver wordt gevraagd om een concept Plan van Aanpak uit te werken waarin wordt beschreven op welke wijze Opdrachtnemer de Oplossing gaat realiseren. Opdrachtgever verwacht</p>

een uitwerking van de Opdrachtnemer op de volgende 6 onderwerpen en onderliggende sub-onderwerpen:

1. Beschrijving in hoeverre de voorgenomen Realisatie door Opdrachtgever matcht met de eigen ervaring van Opdrachtnemer en inzichten rondom implementaties van de Oplossing inclusief de inrichting en bemensing (fit for purpose) van een Center of Excellence: eventuele aanvullingen hierop of een tegenvoorstel inclusief een Definition of Done en bijbehorende acceptatiecriteria;
2. Omschrijving en toelichting op de projectorganisatie o.b.v. in te zetten expertise (inclusief noodzakelijke senioriteit);
 - a. uit de toelichting blijkt hoe de Opdrachtnemer de eigen en de verwachte kennis/expertise bij Opdrachtgever ziet o.b.v. ervaringen uit eerdere trajecten en hoe precies de verhouding tussen de inzet van rollen van de Opdrachtgever en die van Opdrachtnemer is;
 - b. best practices en 'lessons learned' bij vergelijkbare opdrachten;
 - c. rollen en verantwoordelijkheden vanuit zowel Opdrachtnemer als Opdrachtgever;
 - d. samenwerking- en communicatie: zoals overlegstructuren, locatie (fysiek en digitaal, voorgestelde Kantoortijden);
 - e. (overige) randvoorwaarden; zoals toegang tot de infrastructuur van Opdrachtgever.
3. Planning inclusief toelichting en doorlooptijden, waarbij het van belang is dat hierbij geconformeerd wordt aan de mijlpalen uit paragraaf 6.3 van de Specificatie van de Opdracht en alle punten van de Definition of Done onder de mijlpalen uitgewerkt zijn;
4. Risicomanagement: inzicht in mogelijke risico's inclusief een bijbehorende/voorgestelde aanpak.
5. De Opdrachtgever onderkend een aantal typen DevOps-medewerkers zoals opgenomen in de Mijlpaal "Opleidingen en trainingen", paragraaf 6.3 de Specificatie van de Opdracht. Opdrachtgever heeft behoefte aan inzicht in de opleidingspaden per type DevOps-medewerker van de Oplossing die de Opdrachtnemer biedt.
6. Omschrijf het test- en acceptatieproces om te komen tot een Productiewaardige Oplossing waarbij geconformeerd wordt aan artikel 10 (Oplevering en Acceptatietest(en) van de concept Overeenkomst (Bijlage 2.).

In uw uitwerking dient u de bovenstaande 6 onderwerpen en onderliggende sub-onderwerpen puntsgewijs uit te werken. U dient hierbij rekening te houden met hetgeen in de Aanbestedingsdocumenten verwoord is.

Uw uitwerking bestaat uit maximaal 18 pagina's A4 (lettertype Arial, lettergrootte 10, regelafstand 1,0) mag geen verwijzingen en hyperlinks bevatten. Extra pagina's worden niet beoordeeld. U dient bij de uitwerking de structuur van de Wens aan te houden (1 t/m 6).

Voor deze wens kunt u maximaal 65 punten verdienen.

Beoordelingskader

De beantwoording van deze Wens wordt beoordeeld op de volgende beoordelingscriteria:

- **Compleetheid** De mate waarin het ingediende antwoord volledig ingaat op alle onderdelen van de Wens.
- **Consistentie** De interne samenhang van het antwoord: verschillende onderdelen van het voorstel spreken elkaar niet tegen en sluiten logisch op elkaar aan.
- **Concreetheid** De mate waarin de Inschrijver specifiek, meetbaar en duidelijk maakt hoe de Wens wordt ingevuld (in plaats van algemene of vage bewoordingen).
- **Realistisch** De mate waarin de beschrijving van de aanpak en resultaten geloofwaardig, uitvoerbaar en haalbaar is binnen de gegeven context.

De uitwerking van de Wens wordt hierbij als geheel beoordeeld. Het is niet zo dat er per onderdeel een score wordt gegeven.	
Beoordeling / aantal punten	Toelichting
Niet beantwoord 0 punten	De Wens is in zijn geheel niet beantwoord. Indien wel een uitwerking is gegeven aan het gevraagde en deze uitwerking aantoonbaar geen betrekking heeft op de betreffende Wens en/of de Wens in zijn geheel niet beoordeeld kan worden, wordt ook 0 punten toegekend.
Onvoldoende 13 punten	Een deel van de Wens is niet beantwoord en/of de beantwoording sluit niet of nauwelijks aan bij de betreffende Wens en/of de Wens kan slechts gedeeltelijk beoordeeld worden.
Matig 26 punten	De Wens wordt niet volledig beantwoord en wordt niet volledig en onvoldoende onderbouwd.
Voldoende 39 punten	De Wens wordt volledig beantwoord, maar niet volledig en voldoende onderbouwd.
Goed 52 punten	De Wens wordt volledig beantwoord en volledig en voldoende onderbouwd.
Uitstekend 65 punten	De Wens wordt volledig beantwoord en onderbouwd, daarnaast bestaat het antwoord uit positieve, verrassende en vernieuwende elementen, welke voor Opdrachtgever relevant (verminderen van de doorlooptijd en/of vergroten van de kwaliteit en/of verhogen van de klanttevredenheid) zijn, waardoor de Wens wordt beoordeeld als uitstekend.

6.3 Mijlpalen

Opdrachtgever heeft ten aanzien van de Realisatie fase mijlpalen vastgesteld. Per mijlpaal is in dit hoofdstuk uitgewerkt wat van de Opdrachtnemer wordt verwacht op basis van Doorlooptijd, doel, supportbehoefte en Definition of Done. Van de Opdrachtnemer wordt gedurende de Realisatie fase verwacht dat op basis van haar opgedane kennis en kunde mee wordt gedacht in de haalbaarheid van de verwachte Doorlooptijd, doel, supportbehoefte en Definition of Done.

Hieronder een schematische weergave van de onderkende mijlpalen uitgezet in de tijd.

Mijlpaal	Doorlooptijd	Weken													
		1	2	3	4	5	6	7	8	9	10	11	12	13	
Plan van Aanpak Realisatie	1,5 weken	■	■												
MVP	5 weken		■	■	■	■	■	■	■						
Productiewaardig product	6 weken			■	■	■	■	■	■	■	■	■	■	■	■
Inrichten CoE	12 weken		■	■	■	■	■	■	■	■	■	■	■	■	■
Opleidingen/Trainingen	12 weken		■	■	■	■	■	■	■	■	■	■	■	■	■
Finaliseren SLA en DAP	12 weken		■	■	■	■	■	■	■	■	■	■	■	■	■

Opdrachtgever definieert in de Realisatie fase 6 mijlpalen. Per mijlpaal is in dit hoofdstuk uitgewerkt wat van de Opdrachtnemer wordt verwacht op basis van Doorlooptijd, doel, supportbehoefte en Definition of Done. Van de Opdrachtnemer wordt verwacht dat op basis van haar opgedane kennis en kunde mee wordt gedacht in de haalbaarheid van de verwachte Doorlooptijd, doel, supportbehoefte en Definition of Done, zolang de Realisatie fase binnen 3 maanden na ondertekenen van de Overeenkomst is afgerond. De genoemde Doorlooptijd van 12 weken voor de mijlpalen “Inrichten CoE”, “Opleidingen/Trainingen” en “Finaliseren SLA/DAP” zijn indicatief. Dit betekent dat deze zaken binnen de gestelde termijn afgerond moeten zijn, dit betekent niet dat de Doorlooptijd ook per definitief zo lang is.

GUE 83.	Opdrachtnemer conformeert zich voor wat betreft de Realisatie fase aan onderstaande 6 mijlpalen met bijbehorende doelen, supportbehoefte en Definitions of Done.
---------	--

6.3.1 Mijlpaal: Plan van Aanpak Realisatie

Doorlooptijd: 1,5 week (7 Werkdagen).

Doel:

- Het definitief maken van het concept PvA samen met de Opdrachtgever.
- Praktische details voor de mijlpalen worden nader uitgewerkt.

Supportbehoefte:

- De Opdrachtnemer levert bij Inschrijving een concept PvA aan.
- Tijdens dit proces wordt van de Opdrachtnemer verwacht om samen met de Opdrachtgever een gedragen PvA vast te stellen op basis van best practices van de Opdrachtnemer.

Definition of Done:

- Geaccordeerd PVA:
 - Plan van aanpak Realisatie is formeel goedgekeurd door alle relevante stakeholders.
 - Scope, planning, rollen en verantwoordelijkheden zijn vastgelegd en gecommuniceerd.
 - Governance-structuur is ingericht (stuurgroep, CoE, product owner, etc.).
- Realisatie & CoE-inrichting:
 - Er is een duidelijke vergelijking gemaakt tussen de voorgenomen realisatie door de Opdrachtgever en de ervaring van de Opdrachtnemer.
 - Eventuele aanvullingen of tegenvoorstellen zijn expliciet en onderbouwd met praktijkervaring, best practices of lessons learned.
 - Een voorstel voor inrichting van een Center of Excellence (CoE) is opgenomen, inclusief een bijbehorende Definition of Done voor CoE-activatie.
- Projectorganisatie & Communicatie:
 - De projectstructuur is beschreven, inclusief rollen, verantwoordelijkheden en communicatielijnen.
 - Ingezette expertise is gespecificeerd, inclusief vereiste senioriteit per rol.
 - Er is een reflectie opgenomen op de eigen en verwachte kennis/expertise, gebaseerd op eerdere trajecten.
 - Devicegebruik door Opdrachtnemer is benoemd, inclusief technische specificaties en beveiligingsvoorwaarden.
 - Locatie van werkzaamheden (fysiek en digitaal) en voorgestelde Kantoortijden zijn expliciet vermeld.
- Mijlpalenplanning:
 - Een overzichtelijke planning met concrete mijlpalen is opgenomen.
 - Elke mijlpaal is voorzien van een toelichting op doel, afhankelijkheden en verwachte output.
 - De planning is afgestemd op de realisatiefase en bevat ruimte voor toetsmomenten.

- Opleidingsmogelijkheden
 - Er is een overzicht van verschillende typen gebruikers (beheerder, ontwikkelaar, etc.).
 - Per type gebruiker zijn relevante opleidingsvormen beschreven (klassikaal, e-learning, coaching).
 - Opleidingspaden zijn uitgewerkt en afgestemd op de realisatiefase.
 - Er is een voorstel voor timing, beschikbaarheid en eventuele certificering.
- Risicomanagement:
 - Minimaal vijf relevante risico's zijn benoemd, inclusief impact en waarschijnlijkheid.
 - Voor elk risico is een mitigerende maatregel of aanpak voorgesteld.
 - Risico's zijn gekoppeld aan specifieke onderdelen van het PvA (techniek, organisatie, planning, adoptie).
- Test- en acceptatieproces:
 - Het testproces is beschreven, inclusief testsoorten (unit, integratie, gebruikersacceptatie).
 - Acceptatiecriteria zijn geformuleerd per fase of component.
 - Rollen en verantwoordelijkheden binnen het testproces zijn benoemd.
 - Er is een voorstel voor documentatie en rapportage van testresultaten.

UE 28.	<p>Het concept PvA van de Opdrachtnemer wordt uiterlijk binnen 7 Werkdagen na ingangsdatum van de Overeenkomst tussen Opdrachtnemer en de Opdrachtgever afgestemd en gefinaliseerd.</p> <p>Het omvat minimaal uitwerking van de 6 onderwerpen inclusief sub-onderwerpen zoals deze in de Wens concept Plan van Aanpak Realisatie zijn omschreven.</p> <p>Pas nadat er akkoord is tussen Partijen over het definitieve Plan van Aanpak Realisatie zal worden gestart met het verder uitvoeren van de Realisatie fase.</p>
--------	--

6.3.2 Mijlpaal: Minimum Viable Product

Geschatte Doorlooptijd: 5 weken.

Doel:

- Initiële uitrol van de Low-code Oplossing. Dit bestaat uit:
 - een client (IDE, web) die werkt op werkplek van Opdrachtgever;
 - het deel van de Low-code Oplossing dat draait op Red Hat OpenShift;
 - koppelingen met benodigde/vereiste resources van de Fabrikant;
 - koppelingen met benodigde/vereiste resources van de Opdrachtgever.
- Het uitbreiden en "eigen maken" van de Low-code Oplossing met de DevOps capabilities en overige beschikbare componenten.
- Beheren van de Low-code Oplossing m.b.t. de beschikbare en relevante componenten.

Supportbehoefte:

- Tijdens dit proces wordt van de Opdrachtnemer verwacht om samen met de Opdrachtgever uitvoering aan het PvA te geven teneinde de Low-code Oplossing te Installeren en initieel werkend te krijgen. Dat houdt in:
 - De client-software is benaderbaar door medewerkers van Opdrachtgever met de onderkende rollen.
 - De benodigde/vereiste resources van de Fabrikant zijn beschikbaar en benaderbaar.
 - De benodigde/vereiste resources van de Opdrachtgever zijn beschikbaar en benaderbaar. Dat houdt onder andere in dat:
 - Low-code Applicaties ontwikkeld kunnen worden (beschikbaarheid O-omgeving);
 - Low-code Applicaties gedeployed kunnen worden naar tenminste de T-omgeving.
- Opdrachtnemer levert inhoudelijke expertise (engineers) ten behoeve van het kunnen beheren van de Low-code Oplossing.
- De Opdrachtnemer levert Opleidingen aan de medewerkers van Opdrachtgever conform het PvA.

Definition of Done:

- Initiële uitrol van de Low-code Oplossing:
 - Clientcomponent (IDE of webinterface) is geïnstalleerd en functioneert op ten minste Windows 11 en MacOS Tahoe (inclusief eventuele dependencies).
 - Werkende koppeling met de AD/PingFederate op basis van OIDC (config en keys door de Belastingdienst).
 - Backendcomponent is succesvol uitgerold op Red Hat OpenShift met werkende container(s).
 - Werkende koppeling met database omgeving, Postgresql op OpenShift (database wordt door de Belastingdienst geleverd).
 - Werkende koppeling met storage omgeving, Huawei Oceanstor Pacific buiten OpenShift (S3 buckets worden door de Belastingdienst geleverd).
 - Werkende koppeling met de Portal omgeving t.b.v. de applicatie bouw, beheer en deployments vanaf de belastingdienst werkplek.
 - Werkende koppeling om images via bastion server On-premises naar binnen te halen (bastion server wordt door de Belastingdienst geleverd).
 - Werkende koppeling met Harbor registry intern (Harbor registry wordt door de Belastingdienst geleverd).
 - Toegang tot beide componenten is getest en gevalideerd door ten minste één ontwikkelaar en één beheerder.
 - Basisfunctionaliteit (app bouwen, deployen, testen) is aantoonbaar werkend.
 - Inrichten en aantonen van de werking van de interne Private Marketplace.
- Koppelingen met resources van de Fabrikant:
 - Authenticatie met fabrikantservices (licentiebeheer, supportportaal, Private Marketplace) is succesvol getest.
 - API's, SDK's of connectors van de fabrikant zijn beschikbaar en bruikbaar binnen het platform.
 - Documentatie en supportkanalen van de fabrikant zijn toegankelijk voor het CoE.
- Uitbreiden en eigen maken met DevOps capabilities:
 - Fabrikant eigen CI/CD-pipeline is opgezet en integratie met een extern CI/CD-pipeline-mechanisme of deploymentproces is gedocumenteerd en getest.
 - Versiebeheer (bijv. Git-integratie) is operationeel en gekoppeld aan het platform.
 - Minimaal één testapplicatie is gebouwd, gedeployed en geversioneerd via DevOps flow.
 - Rollen en rechten voor DevOps-activiteiten zijn ingericht en getest.
- Beheer van de Low-code Oplossing:
 - Beheerdersconsole of dashboard is toegankelijk en functioneel.
 - Monitoring, logging en alerting zijn geconfigureerd en getest.
 - Documentatie voor beheer en Onderhoud is beschikbaar en gedeeld met het CoE.
 - Backup- en recoveryprocedures zijn ingericht en getest (of gepland met datum).
 - Minimaal één beheerder heeft toegang en is getraind in het gebruik van de beheermogelijkheden.
 - Mogelijke alternatieven in versiebeheer zijn inzichtelijk gemaakt.

UE 29.	Opdrachtnemer realiseert On Premises bij de Opdrachtgever op het Red Hat OpenShift containerplatform een Minimum Viable Product versie van de Low-code Oplossing.
--------	---

6.3.3 Mijlpaal Productiewaardige Oplossing

Geschatte Doorlooptijd: 6 weken

Doel:

- Volledige functionaliteit conform de Specificaties, waarbij de Low-code Oplossing gebruiksklaar in Productie, beschikbaar en toepasbaar is.

Supportbehoefte:

- Opdrachtnemer levert inhoudelijke expertise (engineers) t.b.v. het ontwikkelen en deployen van applicatie.
- Medewerkers van Opdrachtgever kunnen Opleidingen volgen conform de geadviseerde Opleidingen uit van het PVA.
- De Opdrachtnemer levert volledig Support en Onderhoud conform het bestek.

Applicaties die binnen de Belastingdienst ontwikkeld worden hebben vaak koppelingen met andere softwaresystemen. Een voorbeeld daarvan is de koppeling met het systeem waarin alle Data is opgeslagen (BVR). Deze koppeling loopt via een webservice. Om inzicht te krijgen in het maken/inrichten van zo'n koppeling, wil de Opdrachtgever graag weten hoe zo'n functionele koppeling m.b.v. verschillende protocollen tot stand gebracht kan worden.

UE 30.	<p>Opdrachtnemer realiseert minimaal één (voorbeeld) Low-code Applicatie die koppelt met interne/bestaande voorzieningen, gebruikmakend van de volgende protocollen:</p> <ul style="list-style-type: none"> • Webservice (SOAP/REST); • MQ; • Kafka. <p>Opdrachtgever levert de informatie aan die nodig is voor het realiseren van de koppelingen. Denk hierbij aan o.a. end-points en credentials.</p>
--------	---

Definition of Done:

- Volledige functionaliteit beschikbaar:
 - Alle functionaliteiten van de Low-code Oplossing zijn conform de Specificaties van de Aanbestedingsstukken geïnstalleerd en operationeel (app-ontwikkeling, workflowbeheer, integratiecomponenten, gebruikersbeheer).
 - Functionaliteiten zijn getest op beschikbaarheid en stabiliteit (in de Productie omgeving).
 - Documentatie van beschikbare functionaliteiten is compleet en toegankelijk voor Opdrachtgever.
 - Alle benodigde componenten (runtime, database, integratie-interfaces) zijn operationeel.
 - Netwerk- en firewallinstellingen zijn afgestemd en getest.
 - De Low-code Oplossing is succesvol geïnstalleerd in de On-premises Red Hat OpenShift omgeving van de Opdrachtgever.
 - Authenticatie en autorisatie zijn ingericht conform CoE-beleid (AD, SSO).
 - Tenminste 2 tenants zijn ingericht inclusief bijbehorende huisstijl (Belastingdienst en Douane).
- Functionele toepasbaarheid gevalideerd:
 - Minimaal één voorbeeld Low-code Applicatie, conform Uitvoeringseis (UE) 35 is succesvol gemodelleerd, gebouwd, getest en gedeployed via de Low-code Oplossing.
 - Geëiste functionaliteiten zijn toepasbaar binnen de context van de Opdrachtgever (bijv. security policies, data-integriteit, governance).
 - Opgeleide DevOps-medewerkers kunnen zonder tussenkomst van de Opdrachtnemer een Low-code Applicatie bouwen en publiceren.
 - Gebruikersrollen en rechten zijn gedefinieerd en geïmplementeerd (bijvoorbeeld: ontwikkelaar, beheerder, tester).
 - Minimaal één (test)gebruiker per rol is aangemaakt en gevalideerd.
- Security en compliance:
 - Authenticatie en autorisatie werken conform het securitybeleid van de opdrachtgever.
 - Logging, monitoring en audit-trails zijn actief en functioneel.
 - De Low-code Oplossing voldoet aan interne security policies en relevante wet- en regelgeving
 - Penetratietest en/ of securityscan is uitgevoerd. Mogelijke Bevindingen die te herleiden zijn naar de Fabrikant dienen onder verantwoordelijkheid van de Opdrachtnemer te zijn opgelost.

- Gebruikersacceptatie en bruikbaarheid:
 - Minimaal één gebruikersgroep van DevOps-medewerkers heeft de Low-code Oplossing getest en feedback geleverd. Testbevindingen en/of functionele feedback zijn opgelost.
 - Met de Low-code Oplossing kunnen Low-code Applicaties gerealiseerd worden die WCAG2.1-compliant zijn. Dit is aangetoond binnen één testapplicatie.
 - Opleidingsmateriaal en supportkanalen zijn beschikbaar gesteld aan de Opdrachtgever.
- Release- en deploymechanisme:
 - Low-code Applicaties kunnen via een gestandaardiseerd proces worden gedeployed naar Productie.
 - CI/CD-pijplijn is gedocumenteerd (deploymentproces), getest en functioneert conform de gestelde eisen in de Aanbesteding.
- Ondersteuning en beheer:
 - Beheerfunctionaliteiten zijn operationeel (bijv. gebruikersbeheer, versiebeheer, monitoring).
 - Gebruikers zijnde beheerders hebben toegang tot relevante dashboards en configuratieopties binnen de Low-code Oplossing.
 - Onderhoudsprocedures zijn gedocumenteerd en afgestemd met de Opdrachtgever.
 - Logging en monitoring zijn geactiveerd en toegankelijk voor de CoE.
 - Van alle alerts en foutmeldingen die gegenereerd en gelogd worden is duidelijk wat deze betekenen én dat deze in relatie staan met de bron van de alert of fout.
 - Technische documentatie voor Installatie, configuratie en beheer is aan de Opdrachtgever digitaal beschikbaar gesteld.

UE 31.	Opdrachtnemer Realiseert On-premises bij de Opdrachtgever op het Red Hat OpenShift containerplatform een gebruiksklare Productiewaardige Low-code Oplossing conform de Specificaties.
UE 32.	Als onderdeel van de Productiewaardige Low-code Oplossing Oplevering wordt relevante Documentatie (zoals technische Documentatie voor Installatie, configuratie en beheer, Release notes en relevant instructiemateriaal) digitaal beschikbaar gesteld.

6.3.4 Mijlpaal: Inrichten Low-code Center of Excellence

Geschatte Doorlooptijd: 12 weken

De Low-code Oplossing zal als een ontwikkelstraat binnen de IV-organisatie als dienst worden ingezet. Om de ontwikkeling van Low-code Applicaties veilig en gestandaardiseerd via de Low-code Oplossing te laten plaatvinden, dient een CoE te worden opgericht en ingericht. Het CoE zorgt voor ondersteuning, beheer, en begeleiding bij de uitrol en adoptie van de Low-code Oplossing én bewaakt de Kwaliteit van de ontwikkeling van Low-code Applicaties. Het CoE (onder)kent 6 doelstellingen en taken, waarbij we ondersteund willen worden door de Opdrachtnemer met:

1. Standaardisatie & hergebruik:
 - templates in de huisstijl van ten minste de DGs Belastingdienst, Douane en Toeslagen.
 - gratis Componenten vullen van de interne Private Marketplace vanaf de door Opdrachtnemer beschikbaar gestelde Public Marketplace.
 - opstellen intern beleid/instructies voor het gebruik van de Componenten in de Private Marketplace.
 - harvesten van Componenten gemodelleerd door DevOps-medewerkers (het plaatsen van componenten in de Private Marketplace is voorbehouden aan de medewerkers van het CoE).
 - best practices voor applicatie-ontwikkeling aanbieden (Opdrachtnemer draagt haar best practises over door middel van documentatie, demonstratie (voor doen) en/of het actief te laten integreren in de Low-code Oplossing of werkproces van CoE.

2. Governance & compliance:
 - inrichten van role-based access control (RBAC).
 - inrichten van audit- & aanvullende logging: Houd bij wie wat doet in het platform (inclusief de admintrator rollen), actieve apps, flows en DevOps-medewerkers.
 - Security policies opstellen: stel eisen aan authenticatie (bijv. SSO, MFA) en versleuteling.
 - Inrichten tenantstructuur.
3. Development & Educatie:
 - Onboarding proces / trainingsprogramma opstellen voor ten minste de volgende gebruikers rollen/ DevOps-medewerkers: 1. ontwikkelaars, 2. beheerders 3. administrator.
4. Monitoring en LifeCicle Management:
 - App LifeCicle policies: opstellen beleid hoe en wanneer Low-code Applicaties (Data, etc) worden gearchiveerd, geüpdatet of verwijderd.
 - Best practises over platform LifeCiclemanagement.
 - Versiebeheer: best practises versiebeheermechanisme.
5. Experimenteren en innoveren:
 - In het kader van LifeCicle management t.a.v. de Low-code Oplossing en in het verlengde daarvan.
 - Een veilige omgeving (“sandbox”) creëren voor proof-of-concepts en pilots, zodat nieuwe ideeën snel getest kunnen worden zonder risico voor Productie omgevingen.
6. Opstellen best practises voor integratie met bestaande systemen:
 - Generieke werking van koppelingen o.b.v. MQ, Kafka en webservices.

Initieel ziet Opdrachtgever dat het Center of Excellence bemensd moet worden met de volgende (gecombineerde) rollen:

1. CoE Lead / Product owner; stuurt het CoE aan, bewaakt visie, Roadmap, budget, prioriteert Backlog en zorgt voor alignment met de bedrijfsstrategie.
2. Governance & Compliance Officer / Low-code Architect; stelt richtlijnen op voor security, privacy, architectuur en kwaliteitsstandaarden, en ziet toe op naleving.
3. Platform administrator; beheert de Low-code Oplossing, gebruikersrechten, Performance, gebruik etcetera.
4. Community manager / Enablement specialist; stimuleert kennisdeling, verzorgt documentatie en onboarding en organiseert events en onderhoudt de interne low-code community.

UE 33.	De Opdrachtnemer dient samen met de Opdrachtgever een Low-code CoE in te richten tijdens de Realisatie fase, op dusdanige wijze dat er invulling kan worden gegeven aan de 6 doelstellingen en de taken zoals omschreven in de Definition of Done behorende bij deze mijlpaal. De Opdrachtnemer dient hierbij een onderbouwd advies op te leveren in hoeverre de genoemde bemensing in relatie tot de CoE, met gecombineerde rollen fit for purpose is voor de onderkende doelstellingen en taken.
UE 34.	De CoE medewerkers zijn opgeleid en in staat om zelfstandig het CoE uit te baten.

Definition of Done

1. Standaardisatie & hergebruik:
 - Templates: Alle standaard templates (UI, huisstijl, documentatie) zijn beschikbaar in de Low-code Oplossing, getest en voldoen aan de huisstijlrichtlijnen van ten minste de DGs Belastingdienst, Douane en Toeslagen.
 - Private Marketplace: Ingericht en gevuld met minimaal goedgekeurde gratis Componenten*, inclusief Documentatie, gebruiksbeleid en instructies.
 - Harvesting: Proces en criteria voor het identificeren en opnemen van generieke componenten in de CoE marketplace zijn gedocumenteerd en getest.
 - Integratie: Koppelingen met kernsystemen (bijv. Belastingdienst) zijn gerealiseerd, getest en voldoen aan dataconsistentie en beveiligingseisen.
 - Generieke koppelingen: Mechanismen voor MQ, Kafka en webservices zijn generiek opgezet, gedocumenteerd en getest.

2. Governance & compliance:
 - RBAC: Rollen en rechten zijn ingericht, getest en gedocumenteerd, inclusief beheerproces.
 - Audit & logging: Logging is actief voor alle relevante acties (incl. admin acties), voldoet aan compliance eisen en is toegankelijk voor Audits.
 - Overzicht actieve assets: Dashboard of rapportage beschikbaar met actuele lijst van actieve apps, flows en gebruikers.
 - Authenticatie: SSO en koppeling AD zijn geïmplementeerd en getest volgens afgesproken security standaarden.
 - Encryptie: Data-in-transit en data-at-rest zijn versleuteld conform beleid.
 - Tenantstructuur: Documentatie en inrichting van tenant en omgevingsstructuur zijn afgerond en afgestemd met security & compliance, zodanig dat de Opdrachtgever zelfstandig een tenantstructuur kan toevoegen, inrichten, wijzigen en onderhouden.
3. Development & educatie:
 - Onboardingprogramma: Trainingsmateriaal, handleidingen en toegang tot best practices zijn beschikbaar voor tenminste de volgende gebruikersrollen/DevOps-medewerkers: ontwikkelaars, beheerders en administrators.
 - Training gegeven: Minimaal één opleidingssessie/workshop is uitgevoerd voor relevante stakeholders.
4. Monitoring en LCM:
 - App LifeCycle policies: Beleidsdocument en technische inrichting voor archiveren, updaten en verwijderen van Low-code Applicaties zijn gereed en getest.
 - Platform LifeCycle: Proces en infrastructuur voor deployment naar verschillende platformversies zijn ingericht en getest.
 - Versiebeheer: Mechanisme voor versiebeheer (code, configuraties, componenten) is operationeel en gedocumenteerd.
5. Experimenteren & innoveren:
 - Sandboxomgeving: Veilige, gescheiden omgeving voor PoC's en pilots is ingericht en getest.
 - Innovatieproces: Richtlijnen voor het testen en doorvoeren van nieuwe ideeën zonder risico voor Productie zijn beschikbaar.
6. Opstellen Best Practices:

Beschikbaarstellen van alle best practices in een centrale kennisbank, inclusief voorbeelden en richtlijnen. Naast de onderwerpen die hierboven beschreven zijn, hieronder een overzicht van aanvullende zaken die ook hieronder vallen:

 - Ontwikkelstandaarden: Naamgevingsconventies voor flows, componenten, datamodellen, variabelen et cetera.
 - Componenthergebruik: Richtlijnen m.b.t. UI, logica en datamodellen.
 - Error handling: Generieke wijze om te komen tot een logische en sluitende foutafhandeling.
 - Test management: Betreft richtlijnen voor verschillende testsoorten, testdatamanagement.
 - Platform LifeCycleLCM: gestructureerd beheren van de LifeCycle van het platform in samenhang met de Componenten/Low-code Applicaties die er binnen de Oplossing ontwikkeld zijn.

Voor elk onderdeel geldt aanvullend:

1. **Kennisoverdracht:** Alle onderdelen zijn toegelicht in een overdrachtsessie aan het interne CoE-team, inclusief Q&A.
2. **Documentatie:** Volledige en actuele Documentatie is opgeleverd in afgesproken formaat (bijv. wiki, SharePoint, Confluence).
3. **Acceptatie:** Alle onderdelen zijn formeel getest en geaccepteerd door de Opdrachtgever.
4. **Self-service:** Het interne team kan zelfstandig de ingerichte processen en omgevingen beheren zonder afhankelijkheid van de Opdrachtnemer.

6.3.5 Mijlpaal: Opleidingen en trainingen

Doorlooptijd: 12 weken

Doel

- Medewerkers van Opdrachtgever in de relevante rollen voorbereiden op hun toekomstige werkzaamheden, zodat zij aansluitend op de Realisatie aan de slag kunnen binnen het Center of Excellence.

Supportbehoefte

- | | |
|-----------------------------------|--|
| • CoE Lead | Governance & operating model voor Low-Code: change management en adoptionstrategie |
| • Product Owner | Agile productontwikkeling in Low-code: requirements mapping en backlogbeheer |
| • Governance & Compliance Officer | Security & compliance in Low-code: auditing en riskmanagement workflows |
| • Low-code Architect | Solution design & architecture: integratiepatronen en schaalbaarheid |
| • Platform administrator | Platformbeheer & configuratie: monitoring, logging en incidentmanagement |
| • Data & Analytics specialist | Data-integratie in Low-code: visualisatie en rapportagecomponenten |
| • Community manager | Community building & supportstructuur: feedbackloops en kennisdeling |
| • Enablement specialist | Opleidingspaden en onboarding: coaching en adoptieprogramma's |
| • Developer | App-ontwikkeling in Low-code: CI/CD, versiebeheer en testautomatisering |

Opleiding:

Doelgroep:

Doel:

Opleidingsvorm:

Taal:

Aantal deelnemers:

Platformbeheer

Technisch platform beheerders

Opleiding om IV-medewerkers een vliegende start te geven met het beheren van de Low-code Oplossing. Het gaat om een samenwerking tussen de Opdrachtnemer en de Opdrachtgever.

De Opdrachtnemer brengt de best practices met zich mee ten aanzien van de Low-code Oplossing en de Opdrachtgever brengt de kennis van de Belastingdienst omgeving in.

On-site bij de Belastingdienst – Support, op de werkplek van de Belastingdienst.

Nederlands of Engels

4, bestaande uit:

- 1 x CoE Lead;
- 1 x Product Owner;
- 1 x Governance & Compliance Officer;
- 1 x Low-code Architect.

Opleiding:

Doelgroep:

Doel:

Opleidingsvorm:

Taal:

Expert

Belastingdienst Experts

Gebruik Low-Code Oplossing uitgebreid. Opleiding bedoeld voor een aantal specialisten gericht op security, transformaties die de basiskennis ontstijgen. Het is de bedoeling dat de Belastingdienst medewerkers experts worden van de Low-code Oplossing.

Klassikaal

Nederlands of Engels

Aantal deelnemers:	4, bestaande uit: <ul style="list-style-type: none"> • 1 x Platform administrator • 1 x Data & Analytics specialist • 1 x Community manager • 1 x Enablement specialist
Opleiding:	Developer
Doelgroep:	Developer (junior-, medior- en senior niveau)
Doel:	Gebruik Low-Code Oplossing voor Applicatieontwikkeling: Een opleiding voor (nieuwe) gebruikers om kennis mee te krijgen hoe Low-code Applicaties gemaakt en beheerd worden vanuit Developers perspectief. Methodiek ‘voor doen’, ‘samen doen’ en ‘zelf doen’.
Opleidingsvorm:	Klassikaal of op basis van instructievideo's.
Taal:	Nederlands of Engels
Aantal deelnemers:	20, bestaande uit: <ul style="list-style-type: none"> • 10 x Developer (jr.) • 6 x Developer (mr.) • 4 x Developer (sr.)

Definition of Done

- Inhoudelijke dekking:
 - De opleiding dekt de kerncompetenties en verantwoordelijkheden van de rol.
 - De Opleiding wordt op verschillende kennisniveaus aangeboden,
 - Er is een duidelijke koppeling met de Low-code Oplossing en de specifieke implementatiecontext.
- Praktische toepasbaarheid:
 - De Opleiding biedt minimaal één praktijkopdracht die aansluit bij de rol van de deelnemer.
 - De opgedane kennis is toepasbaar in het eigen werkdomein (bijv. via een demo, prototype of procesontwerp).
- Evaluatie en toetsing:
 - Er is een toetsmoment of evaluatie (quiz, opdracht, peer review) om kennisniveau vast te stellen.
 - De Opleiding biedt een mogelijkheid om op basis van objectieve criteria het kennisniveau van de deelnemer vast te stellen.
- Toegang tot materiaal:
 - Deelnemer heeft toegang tot naslagwerken, documentatie en supportkanalen.
 - Opleidingsmateriaal is afgestemd op het kennisniveau van de doelgroep.
- Registratie en bewijs:
 - De Opleiding biedt voor deelnemers een document als bewijs van afronding met goed gevolg aan.
- Feedback en verbetering:
 - Opdrachtnemer heeft een proces voor continue verbetering van de Opleiding op basis van feedback.

UE 35.	Opdrachtnemer geeft de Opleiding tijdens de Realisatie fase aan medewerkers van de Opdrachtgever afgestemd op de doelgroep en in de Opleidingsvorm zoals aangegeven in paragraaf 6.3.5 van de Specificatie van de opdracht.
--------	---

6.3.6 Mijlpaal: SLA en DAP definitief maken

Doorlooptijd: 12 weken

UE 36.	De Opdrachtnemer maakt binnen de Realisatie fase in samenspraak met de Opdrachtgever de SLA en DAP definitief op basis van de gestelde Specificaties.
--------	---

Hoofdstuk 7. Operationele fase

7.1 Inleiding

De scope van de opdracht bestaat uit twee fases:

- Realisatie fase;
- Operationele fase.

Er is een gebruiksklaar Productiewaardige Low-code Oplossing Opgeleverd en na Acceptatie door Opdrachtgever start het 1e gebruiksjaar van de Low-code Oplossing. Daarmee start het Onderhoud en Support. Verder kunnen Keuze-elementen onder de Overeenkomst worden afgenomen. In dit hoofdstuk zijn op deze onderwerpen de bijbehorende Gunnings-, Uitvoeringseisen en Wensen nader uitgewerkt.

UE 37.	Functionaliteiten die nieuw zijn en beschikbaar worden gesteld, al dan niet via Nieuwe versies dienen na activering van de Nieuwe versie, als integraal onderdeel van de Low-code Oplossing aangeboden te worden.
--------	---

7.2 Onderhoud en Support

Het leveren van Onderhoud en Support en dit alles met inbegrip van:

- de (eventuele) nieuwe functionaliteiten, gericht op het in operationele staat brengen en houden van de Low-code Oplossing;
- de Service Desk activiteiten in de vorm van Support;
- Request for Changes (RFC) proces in relatie tot de Low-code Oplossing en of de Hosting daarvan;
- Uitvoering geven aan de SLA, DAP en Verbeterplan afspraken, waaronder contractgovernance en opleveren van de daarin afgesproken rapportages en documentatie. Inclusief het organiseren van Rrpooadmap sessies, waarin o.a. meegedacht wordt over de volgende generatie software en op- en afschaal mogelijkheden.

Opdrachtnemer is gehouden tot het leveren van Onderhoud en Support ten behoeve van de Low-code Oplossing. Dit betekent onder andere dat Opdrachtnemer Onderhoud en Support levert bij Incidenten aangaande de Low-code Oplossing.

UE 38.	Opdrachtgever eist dat op de door u aangeboden Low-code Oplossing Onderhoud en Support) geleverd wordt door de Opdrachtnemer.
UE 39.	De Opdrachtnemer levert per Nieuwe versie en/of Release van de Low-code Oplossing een overzicht van opgeloste bugs en uitgerolde features.
UE 40.	De LifeCycle van de Low-code Oplossing wordt actief bewaakt waarbij de status actief wordt gecommuniceerd met de Opdrachtgever.
UE 41.	(Nieuwe) versies van de Low-code Oplossing worden minimaal voor een periode van drie (3) jaar ondersteund.

7.2.1 Incidentmanagement

Incidenten kunnen met drie verschillende Prioriteiten aangemeld worden. Aan elk Incident, ongeacht de vermoedelijke oorzaak van een Incident, wordt een Prioriteit toegekend op basis van Impact en Urgentie.

Impact	
Hoog	Een Incident heeft of kan ernstige gevolgen hebben voor <ul style="list-style-type: none"> • één of meer bedrijfsprocessen die de burger en/of het bedrijf direct raken, en/of • één of meer fabriekstaken voor (massale) gegevensverwerking en/of • de Informatiebeveiliging en/of • het imago van de Opdrachtgever en/of • onacceptabele hoge kosten.
Laag	Overige situaties
Urgentie	
Hoog	Een Incident: <ul style="list-style-type: none"> • beïnvloedt Kwaliteit van functies/beschikbaarheid/Beveiliging en/of • brengt integriteit van de Data in het geding (o.a. (potentiële) Datalekken) en/of • treedt op tijdens piektijd/-periode van het bedrijfsproces en/of • brengt uiterste verzenddatum van klantbescheiden in gevaar en/of • verstoort de communicatie met de klanten van de Opdrachtgever en/of • er geen Workaround mogelijk is en/of • de verwerking kan niet worden uitgesteld en/of • de schade is al een feit of zal dat zijn binnen 24 uur.
Laag	Overige situaties
Prioriteit	
Prio 1	<ul style="list-style-type: none"> • Impact Hoog / Urgentie Hoog
Prio 2	<ul style="list-style-type: none"> • Impact Hoog / Urgentie Laag • Impact Laag / Urgentie Hoog
Prio 3	<ul style="list-style-type: none"> • Impact Laag / Urgentie Laag

Tabel 1. Impact, Urgentie en Prioriteit

Prioriteit	Reactietijd		Oplostijd		Streef Hersteltijd (inspanning)	
Prio. 1	30 minuten	100%	8 uur	100%	2 Werkdagen	98%
Prio. 2	60 minuten	100%	1 Werkdag	100%	5 Werkdagen	95%
Prio. 3	8 uur	100%	5+ Werkdagen	100%	10 Werkdagen	90%
Service request	1 Werkdag	100%				

Tabel 2. Service Levels Service Desk en Incidentmanagement.

Omschrijving	Indicator	KPI
Openstelling Service Desk	Reguliere openingstijd Service Desk	Op Werkdagen Maandag t/m Vrijdag: 08:00 – 18:00 Nederlandse tijd (GMT +1)
	Openingstijd Service Desk voor melden van Prio. 1 Incidenten	7*24 uur, 365 dagen per jaar*
Service uren	Reguliere Service uren waarin ondersteuning wordt geleverd.	Op Werkdagen Maandag t/m Vrijdag: 08:00 – 18:00 Nederlandse tijd (GMT +1)
Monitoring en alerting	Opdrachtnemer heeft een monitoring en alerting proces ingericht om direct te kunnen handelen in geval van (security) Incidenten en (dreigende) Verstoringen van de beschikbaarheid van de Low-code Oplossing.	7*24 uur, 365 dagen per jaar*
Prio 1. Incident en/of kritisch Beveiligingsincident oplossen	Oplossen conform Tabel X: Service Levels Service Desk en Incidentmanagement.	Werkt ook buiten service uren door.

Tabel 3. Service Window (Nota Bene: in het geval van een schrikkeljaar geldt 366 dagen).

UE 42.	<p>Incidenten (incl service requests) worden afgehandeld conform:</p> <ul style="list-style-type: none"> • Tabel 1: Impact, Urgentie en Prioriteit; • Tabel 2: Service Levels Service Desk en Incidentmanagement; • Tabel 3: Service Window. <p>Ten aanzien van de afhandeling van Incidenten en service requests wordt ten minste voldaan aan de Service Levels zoals opgenomen in de tabel 2. Service Levels Service Desk en Incidentmanagement in combinatie met Tabel 1. Impact, Urgentie en Prioriteit.</p> <p>Ten aanzien van de Openstelling van de Service Desk wordt ten minste voldaan aan de Service Levels zoals opgenomen in de table 3. Service Levels Service Desk en Incidentmanagement</p>
UE 43.	<p>Activiteiten die om redenen niet binnen de afgesproken termijn kunnen worden opgelost worden opgenomen in een Verbeterplan.</p>

7.2.2 Service Level Agreement (SLA)

De Opdrachtgever sluit met de Opdrachtnemer een Service Level Agreement (SLA) af aangaande het te leveren Onderhoud en Support. De SLA bevat een beschrijving van de vastgestelde normen in de vorm van Service Levels.

UE 44.	<p>Opdrachtnemer levert binnen tien (10) Kalenderdagen na Mededeling van de gunningsbeslissing (zie paragraaf 6.2.1 van het Beschrijvend document) conform de Specificaties, een concept SLA op. De concept SLA beschrijft in elk geval de wijze waarop door Opdrachtnemer invulling wordt gegeven voor Onderhoud en Support. De concept SLA bevat minimaal de volgende onderdelen:</p> <ul style="list-style-type: none"> • Doel en scope van de concept SLA en de dienstverlening. • Benoeming partijen, verantwoordelijkheden en werkingsgebied. • Aanvang, looptijd, wijzigingsbeleid, vaststelling en ondertekening.
--------	--

	<ul style="list-style-type: none"> • Gerelateerde documenten. • In het kader van Informatiebeveiliging: <ul style="list-style-type: none"> ○ Service Desk (melding en oppakken Prio 1-security incidenten, Datalekken); ○ Change-en releasemanagement (waaronder security patches); ○ Securitymanagement: <ul style="list-style-type: none"> - Incident- en problemmanagement; - Audits, beveiligingstesten (A&P-testen, Vulnerability Scans) en continuïteitstesten (backup & restore, calamiteitentests); - Monitoring, alerting en logging. ○ Rapportage. <p>Deze concept SLA vormt mede de basis voor de nog overeen te komen DAP (Dossier Afspraken Procedures) tussen Opdrachtnemer en Opdrachtgever.</p>
UE 45.	<p>Gedurende de Realisatie fase wordt de door de Opdrachtnemer aangeleverde concept SLA in overeenstemming met de Opdrachtgever definitief gemaakt conform de Specificaties. Na vaststelling van de definitieve versie zal deze jaarlijks worden onderhouden als er wijzigingen in de SLA optreden. De versienummering geeft aan welke SLA de laatste versie is. De SLA en maakt onlosmakelijk deel uit van de Overeenkomst.</p>

7.2.3 Dossier Afspraken en Procedures (DAP)

UE 46.	<p>Gedurende de Realisatie fase wordt door Opdrachtnemer een DAP in overeenstemming met de Opdrachtgever opgesteld, afgestemd en definitief gemaakt. Het DAP bevat minimaal de volgende onderdelen:</p> <ul style="list-style-type: none"> • Leveranciersmanagement (o.a. overlegstructuren en interval); • Werkafspraken serviceverlening processen (o.a. Release management); • Change management afspraken (Procedure aanvraag RFC); • Audits en beveiligingstesten (planning); • Afspraken en Procedures (Beveiligings- en privacy Incidenten); • Financiële afspraken zoals facturatiemomenten; • Contactgegevens partijen; • Escalatieprocedure bij onderlinge geschillen. <p>Na vaststelling van de versie 1.0 zal deze jaarlijks worden onderhouden als er wijzigingen in de DAP optreden. De versienummering geeft aan welke DAP de laatste versie is. De DAP maakt onlosmakelijk deel uit van de Overeenkomst.</p>
--------	--

7.3 Rapporteren / Dashboard

Opdrachtgever wil periodiek een actueel inzicht in de geleverde prestaties van de Low-code Oplossing en hetgeen geëist in dit bestek. Het gevraagde inzicht kan bijvoorbeeld middels een maandelijkse rapportage toegestuurd worden vóór de 10e van de maand, maar een Dashboard met actuele informatie is ook mogelijk. Het is Opdrachtnemer vrij hier een keuze in te maken, zolang het inzicht in een rapportagevorm maar gegeven wordt.

UE 47.	<p>Opdrachtnemer levert inzicht in de geleverde prestaties ten opzichte van de in dit document overeengekomen prestaties. Dit inzicht dient minimaal maandelijks actueel te zijn. Met name wil Opdrachtgever inzicht in:</p> <ul style="list-style-type: none"> • KPI opgeloste Incidenten binnen en buiten Service Levels; • KPI opgeloste Beveiligingsincidenten binnen en buiten Service Levels;
--------	---

	<ul style="list-style-type: none"> • Status, voortgang en afhandeling van openstaande en opgeloste vragen, Incidenten, Problems en verbetervoorstellen. Hierbij wordt aangegeven: datum ontvangst, datum in behandeling, verwachte Opleverdatum en datum afgevoerd; • Een cumulatieve rapportage over alle vragen, Incidenten en Problems. De gecumuleerde rapportage laat de historie over een periode van minimaal 14 maanden zien, zodat trends kunnen worden geanalyseerd; • Datum laatste en volgende A&P testen; • Statement of Applicability: <ul style="list-style-type: none"> ○ Vervaldatum certificaten zoals ISO27001-certificering (of gelijkwaardig), TLS-certificaat. ○ Bij Wijziging van de Statement of Applicability en/of ISO27001-certificering (of gelijkwaardig) wordt inzage gegeven in de datum en het resultaat van de wijziging. • Tevens worden volgende onderdelen verwacht indien deze van toepassing zijn in relatie tot Keuze-elementen: <ul style="list-style-type: none"> ○ Consultancy. ○ Opleidingen en trainingen. Hierbij wordt minimaal aangegeven: <ul style="list-style-type: none"> - datum - opdrachtverstrekking, - startdatum, (verwachte) Opleverdatum indien relevant, - (verwachte) acceptatiedatum, - kosten / uitnutting budget. ○ Componenten in de Private Marketplace. <p>Het proces en de vorm wordt vastgelegd in de DAP. In overleg kunnen onderwerpen worden toegevoegd of verwijderd.</p>
--	--

7.4 Keuze-elementen

Tijdens de Operationele fase voor de duur van de Overeenkomst heeft de Opdrachtgever de volgende eisen voor wat betreft de Keuze-elementen.

7.4.1 Consultancy

Het kunnen afnemen van Consultancy voor de duur van de Overeenkomst.

UE 48.	<p>De Opdrachtnemer en/of een door de Opdrachtnemer geselecteerde partij levert Consultancy in het gebruik van de Low-code Oplossing. Consultancy betreft ondersteuning door de Opdrachtnemer voor werkzaamheden waarvoor aanvullende specialistische kennis of expertise vereist is. Deze ondersteuning kan onder meer worden ingezet voor:</p> <ul style="list-style-type: none"> • Technische inrichting en configuratie van de Low-code Oplossing, waaronder het aanpassen of integreren van externe versiebeheertools, CI/CD-mechanismen en andere componenten in de ontwikkelketen waarvoor specifieke kennis noodzakelijk is. • Ondersteuning bij de ontwikkeling van Low-code Applicaties, waaronder het oplossen van functionele of technische ontwikkelvraagstukken die specifieke expertise vereisen. • Het verstrekken van advies of aanvullende inzichten, bijvoorbeeld bij optimalisatie van het platform, het oplossen van complexe issues of het inrichten van best practices. • Uitvoering van hands-on werkzaamheden, indien dit nodig is om vraagstukken op te lossen of gewenste functionaliteiten te realiseren. • Consultancy kan daarmee uiteenlopen van adviserend tot uitvoerend van aard, afhankelijk van de benodigde diepgang en expertise.
--------	--

UE 49.	Communicatie met de consultants dient plaats te vinden in het Nederlands of Engels.
--------	---

7.4.2 Opleidingen en trainingen

Tijdens de Operationele fase van de Overeenkomst wil de Opdrachtgever optioneel Opleidingen in relatie tot de Low-code Oplossing (inclusief leveren van Documentatie) kunnen afnemen.

UE 50.	<p>Opdrachtnemer levert relevante Opleidingen, inclusief Documentatie, over</p> <ul style="list-style-type: none"> • Het modelleren en beheren van Low-code Applicaties met de Low-code Oplossing op het kennisniveau van een: <ul style="list-style-type: none"> ○ Junior ontwikkelaar (Developer); ○ Medior ontwikkelaar (Developer); ○ Senior ontwikkelaar (Developer). • Het beheren van de Low-code Oplossing op het kennisniveau van: <ul style="list-style-type: none"> ○ Platformbeheer (Platformbeheer); ○ Governance & Compliance (Expert); ○ Data & Analytics (Expert); ○ Community- & Enablement management (Expert). <p>De Opleidingen en/of trainingen worden aangeboden in de volgende vormen:</p> <ul style="list-style-type: none"> • Onsite (op locatie); • Online. <p>Instructievorm:</p> <ul style="list-style-type: none"> • Met docent; • E-learning. <p>Taal:</p> <ul style="list-style-type: none"> • Nederlands en/of Engels.
UE 51.	Opdrachtnemer stelt voor de DevOps-medewerkers de goedgekeurde gebruikersinstructie online beschikbaar gedurende de looptijd inclusief verlengingsopties van de Overeenkomst en houdt deze actueel.
UE 52.	Opleiding en ondersteuning dient door deskundigen, die daartoe bekwaam en geschikt zijn, te worden gegeven.

7.4.3 Componenten Private Marketplace

Het via een door de Fabrikant beheerde Public Marketplace leveren van Componenten.

UE 53.	Opdrachtnemer faciliteert het proces van offerteaanvragen in relatie tot het afnemen van betaalde Componenten.
--------	--

Hoofdstuk 8. Retransitie & Exit-strategie

In geval van (tussentijdse) beëindiging of afloop van de Overeenkomst, dient de Opdrachtnemer ten allen tijde medewerking te verlenen aan een gecontroleerde en projectmatige overdracht aan de Opdrachtgever (en mogelijk een opvolgend Opdrachtnemer). Alle Documentatie, Data en informatie in relatie tot de Low-code Oplossing dient door Opdrachtnemer te worden verstrekt die nodig zijn voor zo'n overdracht. De termijn waarbinnen de Retransitie dient te worden afgerond zal tussen Opdrachtnemer en Opdrachtgever worden overeengekomen en is afhankelijk van de omvang van de Low-code Oplossing en gemodelleerde Low-code Applicaties. Aanlevering van de Documentatie gebeurt via een beveiligde verbinding. Opdrachtgever draagt zorg voor deze verbinding.

Om te waarborgen dat de Retransitie op een efficiënte en ongestoorde wijze plaatsvindt, zal de Opdrachtnemer in ieder geval voldoen aan de volgende uitvoeringseisen:

UE 54.	Zodra Partijen bekend zijn met het feit dat de Overeenkomst om welke reden dan ook eindigt of wordt beëindigd, waaronder begrepen opzegging en ontbinding, inventariseren Partijen gezamenlijk welke assistentie van Opdrachtnemer, tegen de reeds overeengekomen Consultancy tarieven, noodzakelijk is voor een succesvolle Retransitie waarbij de continuïteit van de Prestatie gewaarborgd blijft. Hierbij wordt, indien noodzakelijk, een Retransitieplan opgesteld door de Partijen.
UE 55.	In het geval van een Retransitie dient Opdrachtnemer gekwalificeerd Personeel beschikbaar te stellen voor de ontmanteling van de Low-code Oplossing en het 'overhevelen' van relevante Data.
UE 56.	Op eerste verzoek van Opdrachtgever overlegt Opdrachtnemer een door een onafhankelijk IT-auditor of accountant gecertificeerde verklaring van vernietiging waaruit blijkt dat alle Data in verband met deze Overeenkomst zijn gewist.
UE 57.	Naar de Opdrachtgever herleidbare domeinnamen en URL's worden onbeschikbaar gemaakt op het internet en domeinnamen worden –zo mogelijk- overgedragen aan de Opdrachtgever. Hergebruik van deze domeinnamen en URL's is niet toegestaan zonder nadrukkelijke toestemming van de Opdrachtgever. Indien overdracht niet mogelijk is dan overlegt Opdrachtnemer een verklaring waaruit blijkt dat hergebruik niet zal plaatsvinden.

8.1 Retransitie

UE 58.	Opdrachtnemer dient onder meer de verbindingen te verbreken, eventueel aan Opdrachtgever ter beschikking gestelde apparatuur terug te nemen, eventuele licenties te verstrekken ten aanzien van Oplossing die noodzakelijk is om de omgeving in stand te houden/te blijven beheren; en elektronische sleutels aan Opdrachtgever ter beschikking te stellen.
UE 59.	De Opdrachtnemer is gehouden om bij beëindiging van de Overeenkomst, dan wel bij overgang naar een opvolgende Low-code Oplossing geleverd door een andere Opdrachtnemer/Fabrikant, volledige medewerking te verlenen aan een ordentelijke Retransitie. Deze medewerking omvat alle noodzakelijke handelingen om de continuïteit van de Low-code Applicaties en bijbehorende Data te waarborgen.
UE 60.	De Opdrachtnemer verleent gedurende de retransitieperiode technische ondersteuning aan de Opdrachtgever en/of opvolgende Opdrachtnemer/Fabrikant, waaronder: Ondersteuning bij het opnieuw deployen van de Low-code Applicaties

UE 61.	De Opdrachtnemer levert bij Retransitie: <ul style="list-style-type: none"> • De code van de Low-code Applicaties en bijbehorende artefacten; • De Data en metadata; • De Documentatie en deployment-instructies.
UE 62.	Opdrachtnemer verleent medewerking aan een Audit betreffende de inhoud en de Kwaliteit van de informatie die Opdrachtnemer in het kader van Retransitie beheerd.

8.2 Exit strategie

UE 63.	De Opdrachtnemer faciliteert de volledige overdracht aan Opdrachtgever van alle informatie (waaronder Data) die zijn gegenereerd of opgeslagen binnen de Low-code Applicaties, waaronder begrepen: <ul style="list-style-type: none"> • Gebruikersdata, metadata, audit-trails en logginginformatie; • export in een open en gestandaardiseerd formaat, zoals CSV, JSON, XML of relationele database-dumps; • een beschrijving van de datamodellen en relaties tussen entiteiten.
UE 64.	De Opdrachtnemer garandeert dat de Low-code Applicatie(s) en bijbehorende Data na beëindiging van de Overeenkomst functioneel zijn zonder afhankelijkheid van: <ul style="list-style-type: none"> • Cloudgebaseerde diensten van de leverancier; • Licentiecomponenten die niet overdraagbaar zijn aan de Opdrachtgever.
UE 65.	De Opdrachtnemer voert, voorafgaand aan de beëindiging van de Overeenkomst, een exit-validatie uit waarin wordt aangetoond dat: <ul style="list-style-type: none"> • de Low-code Applicatie(s) correct functioneren buiten de Low-code Oplossing; • de Data van Low-code Applicaties volledig en correct zijn gemigreerd; • de redeployment van Low-code Applicaties is succesvol uitgevoerd binnen de infrastructuur van de Opdrachtgever.

Hoofdstuk 9. Integriteit

Opdrachtgever maakt graag gebruik van de kennis en innovatieve kracht uit de markt. Daarvoor werkt de Opdrachtgever samen met leveranciers. In deze samenwerking speelt u dus een essentiële rol. Opdrachtgever vindt onpartijdigheid en transparantie belangrijk. Daarom maken we afspraken hierover: onze Business Etiquette.

GUE 84.	Opdrachtnemer conformeert zich aan de Business etiquette zoals opgenomen in Bijlage 5. van het Beschrijvend Document.
---------	---

Hoofdstuk 10. Maatschappelijk Verantwoord Opdrachtgeven en Inkopen (MVOI)

Het Inkoopuitvoeringscentrum (IUC) van Opdrachtgever heeft ambitie op het gebied van duurzaamheid. Zij wil klanten, behoeftezoekers en leveranciers begeleiden in het vormgeven van de duurzaamheidsaspecten in producten en diensten op het vlak van bedrijfsvoering, bij aanbestedingen en gedurende de looptijd van de contracten (maatschappelijk verantwoord inkopen).

Maatschappelijk Verantwoord Opdrachtgeven en Inkopen (MVOI) binnen de overheid is een uitvloeisel van een politiek besluit. Sinds 2010 is de rijksoverheid verplicht 100% duurzaam in te kopen. Door gelijktijdig milieu-, sociale- en economische afwegingen in alle aankopen mee te nemen leidt dit tot winst voor de belastingbetaler, de overheidsorganisatie en de samenleving.

Het nieuwe regeerakkoord stelt dat de overheid zijn inkoopkracht beter gaat benutten voor het versnellen van duurzame transities, inschakelen van kwetsbare groepen en om innovatief in te kopen.

Hoe de Opdrachtgever MVOI wil toepassen op deze opdracht vindt u in de volgende paragrafen. Hierin zijn de toepasselijke MVOI-thema's beschreven.

10.1 Milieu

GUE 85.	Om het energieverbruik te beperken dient de te leveren Low-code Oplossing te functioneren als een zero footprint client. Dit betekent dat de oplossing minimaal gebruikmaakt van cookies en vergelijkbare opslagmechanismen. Het aantal en de omvang van cookies moeten worden beperkt tot uitsluitend strikt noodzakelijke functionele cookies.
---------	--

10.2 Ketenverantwoordelijkheid (ISV)

Internationale verdragen bevatten morele normen over mensenrechten, arbeidsomstandigheden en beloningen. Het voldoen aan sociale aspecten van duurzaam inkopen betekent dat leveranciers zich moeten inspannen dat deze normen in de hele keten van het productieproces worden nagestreefd. De systematiek die hiervoor is ontworpen, noemen we 'sociale voorwaarden'. De fundamentele normen in de verdragen van Internationale Arbeidsorganisatie en de normen in de Universele Verklaring van de Rechten van de Mens, noemen we generieke normen. Zij gelden voor de inkoop van alle producten. Voor sommige productgroepen heeft de Rijksoverheid aanvullende normen gesteld. Met aanvullende normen streven we in die producten een nog grotere verbetering na van arbeidsomstandigheden en beloningen.

UE 66.	<p>De Opdrachtnemer past gedurende de looptijd van de Overeenkomst de Internationale Sociale Voorwaarden (ISV) toe zoals vastgesteld binnen het Rijk en gepubliceerd via Rijksoverheid.nl. https://www.pianoo.nl/nl/themas/maatschappelijk-verantwoord-inkopen/ketenverantwoordelijkheid/over-2</p> <p>1. Naleving fundamentele arbeidsnormen: De Opdrachtnemer borgt dat in de gehele keten van productie en levering van de Diensten en/of producten die onder deze opdracht vallen, wordt voldaan aan de volgende fundamentele arbeidsnormen van de International Labour Organization (ILO):</p> <ul style="list-style-type: none">• Verbod op kinderarbeid;• Verbod op dwangarbeid;• Verbod op discriminatie;• Vrijheid van vereniging en het recht op collectieve onderhandeling.
--------	--

	<p>2. Risicomanagement en due diligence: De Opdrachtnemer voert gedurende de opdracht passende due-diligence-maatregelen uit om risico's op schendingen van bovengenoemde arbeidsnormen te identificeren, te voorkomen en – indien van toepassing – te mitigeren. Indien de Opdrachtnemer risico's of daadwerkelijke schendingen in de keten constateert, stelt hij de Opdrachtgever hiervan onverwijld in kennis en treft hij aantoonbare corrigerende maatregelen.</p> <p>3. Leveranciers- en ketenverantwoordelijkheid: De Opdrachtnemer legt deze uitvoeringseis op aan alle relevante onderaannemers en leveranciers die bijdragen aan de uitvoering van deze Overeenkomst en ziet toe op de naleving daarvan. Op verzoek van de Opdrachtgever toont de Opdrachtnemer aan op welke wijze hij naleving door zijn ketenpartners heeft geborgd.</p> <p>4. Rapportageverplichting: De Opdrachtnemer rapporteert op verzoek van de Opdrachtgever over:</p> <ul style="list-style-type: none"> • geïdentificeerde risico's in de keten, • getroffen beheersmaatregelen, • verbeteracties en hun resultaten. <p>De rapportage dient in een vorm te worden aangeleverd die aansluit bij het ISV-format zoals gebruikt binnen de Rijksoverheid.</p> <p>5. Controle en Audit: De Opdrachtgever behoudt zich het recht voor om (laten) controleren of de Opdrachtnemer de ISV naleeft. De Opdrachtnemer verleent hiertoe alle redelijke medewerking, inclusief toegang tot relevante documentatie en (waar passend) ketenpartners.</p>
UE 67.	<p>Opdrachtnemer dient rekening te houden met de verplichtingen uit hoofde van de bepalingen inzake de arbeidsbescherming en de arbeidsvoorwaarden die gelden in het land waar de opdracht wordt uitgevoerd, zoals bedoeld in artikel 2.81 lid 2 Aw2012.</p> <p>Kennis omtrent die belastingen en milieubescherming, arbeidsvoorwaarden en arbeidsbescherming kunnen Inschrijvers, voor zover het gaat om uitvoering in Nederland, verkrijgen bij:</p> <ul style="list-style-type: none"> • Opdrachtgever, www.belastingdienst.nl; • het Ministerie van Infrastructuur en Waterstaat, https://www.rijksoverheid.nl/ministeries/ministerie-van-infrastructuur-en-waterstaat; • het Ministerie van Sociale Zaken en Werkgelegenheid, www.rijksoverheid.nl/ministeries/szw.

Hoofdstuk 11. Juridische kaders

De in het Beschrijvend Document opgenomen concept Overeenkomst (Bijlage 2.) en concept Wachtkamerovereenkomst (Bijlage 3.) kunnen (alvorens deze door Inschrijver(s) worden ondertekend) door de Opdrachtgever worden gewijzigd en nader uitgewerkt, mede naar aanleiding van de door de Inschrijver gedane opmerkingen en tekstsuggesties als bedoeld in paragraaf 3.2.1 van het Beschrijvend Document. De wijzigingen en/of de aangepaste Overeenkomst(en) zullen/zal de Inschrijvers per nota van inlichtingen kenbaar worden gemaakt.

GUE 86.	Inschrijver gaat akkoord met de concept Overeenkomst met inbegrip van de eventuele per Nota van Inlichtingen kenbaar gemaakte wijzigingen zoals genoemd in deze paragraaf.
GUE 87.	Inschrijver gaat akkoord met de concept Wachtkamerovereenkomst met inbegrip van de eventuele per Nota van Inlichtingen kenbaar gemaakte wijzigingen zoals genoemd in deze paragraaf.

Hoofdstuk 12. Prijsstelling

12.1 Algemene eisen ten aanzien van Prijzen

In de in Bijlage VI. (Prijzenformulier) geoffreerde Prijzen dienen alle kosten voor de Low-code Oplossing verdisconteerd te zijn. Deze kosten kunnen door Opdrachtnemer niet verbijzonderd worden verrekend aan Opdrachtgever. Hierbij kan (en niet limitatief) worden gedacht aan:

- periodieke rapportages;
- periodiek overleg;
- inspecties;
- evaluaties;
- toekomstverkenningen;
- deelname aan begeleidings- en stuurgroepen;
- reis- en verblijfkosten voor o.a. Consultancy, Opleidingen en/of (externe) bijeenkomsten;
- het verstrekken van de benodigde toegangscodes voor gebruik van de Low-code Oplossing;
- Materialen en Documentatie vereist voor het gebruik van de Low-code Oplossing.

UE 68.	Kosten die niet in de Inschrijving genoemd worden en niet verdisconteerd zijn in de Prijzen, maar toch noodzakelijk blijken te zijn voor een optimaal functioneren van de Low-code Oplossing en/of Prestatie conform de in de Aanbestedingsstukken gestelde eisen en de in de Inschrijving opgenomen beantwoording van de Wensen, kan Opdrachtnemer niet in rekening brengen bij Opdrachtgever.
GUE 88.	Prijzen zijn in Euro's, eventuele valutarisico's zijn volledig voor rekening van Opdrachtnemer en worden geacht in de geoffreerde Prijzen te zijn verwerkt.
UE 69.	Voor zover Opdrachtnemer gehouden is omzetbelasting in rekening te brengen, zullen de in het Prijzenformulier vermelde bedragen worden verhoogd met het geldende percentage omzetbelasting.

12.2 Toelichting ten aanzien van de Prijzen

In Bijlage VI. (Prijzenformulier) is een aantal tabbladen opgenomen die door Inschrijver dienen te worden ingevuld.

Tabblad 'Samenvatting'

Het betreft hier een samenvatting van de hieronder genoemde tabbladen. De Vergelijkingswaarde betreft het totaal van de geoffreerde Prijzen en per onderdeel vermenigvuldigt met een factor (zoals het aantal gebruiksjaren en de verwachte afname conform de dimensionering). De Vergelijkingswaarde wordt gebruikt om de Inschrijvingen met elkaar te vergelijken en de 'Economisch Meest Voordelige Inschrijving' te bepalen. In dit tabblad dient Inschrijver enkel de naam van de Inschrijver in te vullen.

Tabblad 'Dimensionering'

Het tabblad Dimensionering bevat een gestructureerd overzicht van de verwachte afname gedurende de initiële termijn van de Overeenkomst. De dimensionering dient uitsluitend ter indicatie en heeft als doel Inschrijvers in staat te stellen een realistische en vergelijkbare aanbieding op te stellen. In dit tabblad dient Inschrijver niets in te vullen.

Tabblad 'Realisatie'

Hier dient Inschrijver een Vaste Prijs te offeren voor de Realisatie van de Productiewaardige Oplossing zoals beschreven in de Aanbestedingsstukken met inbegrip van het (tijdelijke) Gebruiksrecht, Consultancy en Opleiding in de Realisatie fase. Tevens dient Inschrijver de Vaste Prijs te onderbouwen.

Tabblad 'Gebruiksrecht # Eindgebr.*'

Indien Inschrijver (mede) het Gebruiksrecht o.b.v. het aantal Eindgebruikers offreert, dient Inschrijver dit tabblad in te vullen.

Van de Inschrijver wordt verwacht een prijsopgave te doen voor onderstaande twee grondslagen:

- Gebruiksrecht per Interne Eindgebruiker;
- Gebruiksrecht per Externe Eindgebruiker.

In dit tabblad specificeert Inschrijver de onderdelen waaruit de Low-code Oplossing is opgebouwd. De volgende velden dienen te worden ingevuld:

- Productnaam: De commerciële benaming van het aangeboden product of component.
- Artikelnummer: Het unieke identificatienummer waaronder het product bij de Inschrijver of Fabrikant is geregistreerd.
- Versie: De aangeboden software- of productversie.
- Omschrijving: Een korte functionele beschrijving van het component, inclusief eventuele relevante specificaties.

Tabblad 'Gebruiksrecht Enterprise'*

Indien Inschrijver (mede) het Gebruiksrecht o.b.v. de Enterprise site licentie offreert, dient Inschrijver dit tabblad in te vullen.

De Inschrijver dient voor het Enterprise Gebruiksrecht een vaste Vergoeding per gebruiksjaar te offeren. Deze Vergoeding geldt voor elk afzonderlijk gebruiksjaar binnen de looptijd van de Overeenkomst. Daarnaast kan de Inschrijver optioneel per gebruiksjaar een korting offeren op de vaste Vergoeding per gebruiksjaar. Een dergelijke korting kan bijvoorbeeld worden aangeboden in verband met een opbouw naar volledig gebruik van de oplossing, oplopend nut gedurende de Overeenkomst, of om andere door de Inschrijver gemotiveerde redenen.

Indien een korting wordt aangeboden, dient deze deugdelijk en transparant te worden onderbouwd door de Inschrijver.

De Vergoeding per gebruiksjaar, alsmede de eventuele korting zoals toegepast in gebruiksjaar 6, vormen het uitgangspunt voor de prijsstelling gedurende een eventuele verlenging van de Overeenkomst, tenzij in de Overeenkomst uitdrukkelijk anders is bepaald.

In dit tabblad specificeert Inschrijver de onderdelen waaruit de Low-code Oplossing is opgebouwd. De volgende velden dienen te worden ingevuld:

- Productnaam: De commerciële benaming van het aangeboden product of component.
- Artikelnummer: Het unieke identificatienummer waaronder het product bij de Inschrijver of Fabrikant is geregistreerd.
- Versie: De aangeboden software- of productversie.
- Omschrijving: Een korte functionele beschrijving van het component, inclusief eventuele relevante specificaties.

* Voor de Vergelijkingswaarde in het gunningsmodel wordt de laagste waarde van het type Licentie (# Eindgebruikers of Enterprise) op basis van 6 gebruiksjaren meegenomen, conform het dimensioneringsscenario (geschatte ontwikkeling) van aantallen Eindgebruikers hierboven. Dit scenario kan afwijken van de praktijk.

Tabblad ‘Additionele dienstverlening’

In dit tabblad dient Inschrijver de Additionele diensten Consultancy (Keuze-element 1) en Opleiding (Keuze-element 2) te offrenen, bestaande uit:

- Uurtarief Consultancy.
- Prijs Opleiding per DevOps-medewerker voor de Opleidingen: Platformbeheerder, Expert en Developer (meerdere niveaus).

Tevens kan Inschrijver in dit tabblad zijn overige Opleidingen offrenen. Overige Opleidingen hebben geen impact op de Vergelijkingswaarde.

De gebruikte aantallen zijn indicatief en bedoeld ter vergelijking van de verschillende Inschrijvers. Hieraan kunnen geen rechten worden ontleend.

12.3 Afrekenmethodiek

Realisatie fase

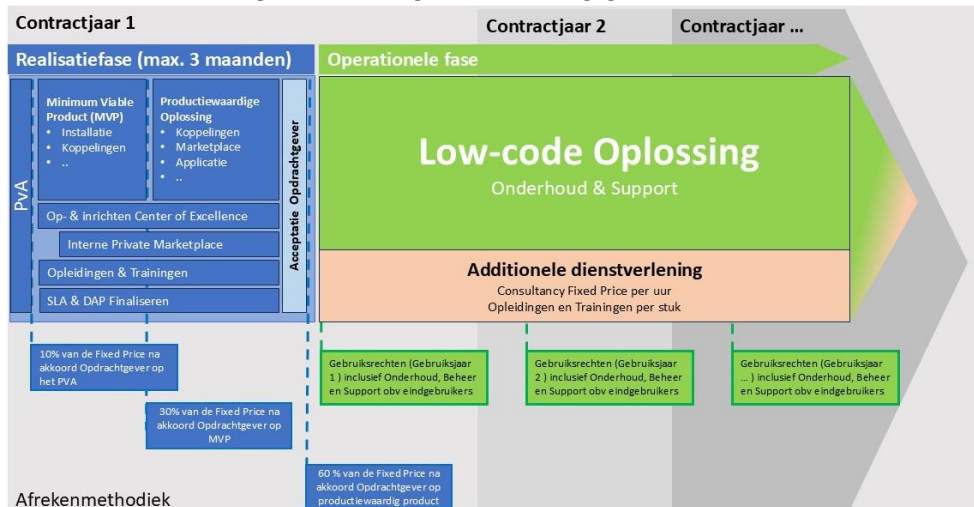
De Realisatie van de Low-code Oplossing is als fixed-price component opgenomen in het Prijzenformulier. Voorafgaand aan het in gebruik nemen dient de Low-code Oplossing door de Opdrachtgever geaccepteerd te worden.

UE 70.	De Opdrachtnemer heeft een Vaste Prijs (fixed-fee) met resultaatverplichting voor het Opleveren van een Productiewaardige Low-code Oplossing conform het geaccordeerde definitieve Plan van Aanpak Realisatie.
--------	--

De facturatiemomenten tijdens de Realisatie fase zijn als volgt:

- Facturatiemoment 1: Betaling 10% van de Vaste Prijs na Acceptatie van definitief Plan van Aanpak Realisatie;
- Facturatiemoment 2: Betaling 30% van de Vaste Prijs na Acceptatie van Minimum Viable Product (MVP);
- Facturatiemoment 3 t/m 6: Betaling 60% van de Vaste Prijs na Acceptatie van "Productwaardige Low-code Oplossing" inclusief levering Gebruiksrechten, Opleidingen, inrichting Center of Excellence en het beschikbaar stellen van een Private Marketplace (gevuld met geverifieerde gratis Componenten inclusief bijbehorende Gebruiksrechten).

Bovenaanstaande is in de volgende afbeelding illustratief weergegeven



Afbeelding 3. Afrekenmethodiek

UE 71.	De Vergoedingen voor Realisatie en de Low-code Oplossing, zijn pas verschuldigd na Acceptatie van de afgesproken mijlpalenplanning en facturatiemomenten.
--------	---

Operationele fase

UE 72.	Indien gebruik gemaakt wordt van het eerste licentiemodel (op basis van Gebruiksrecht aantal Eindgebruikers) uit het Bijlage VI. (Prijzenformulier) wordt de facturatie van Subscriptions jaarlijks vooraf gedaan op basis van een inschatting van het aantal unieke Eindgebruikers.
UE 73.	De Opdrachtnemer biedt de mogelijkheid om tijdens de looptijd van de Overeenkomst, tijdens de Operationele fase, periodiek unieke Eindgebruiker (Named User IDs) aantallen op- of af te schalen conform de Prijzen uit het Prijzenformulier. Hieraan zijn geen extra kosten verbonden.
UE 74.	Met ingang van de Operationele fase zal jaarlijks (voorafgaand aan het betreffende contractjaar) het gewenste aantal Licenties door Opdrachtgever vastgesteld en met Opdrachtnemer worden gecommuniceerd.
UE 75.	Opdrachtgever kan gedurende het contractjaar op elk gewenst moment aanvullende Licenties afnemen, zonder beperking in het aantal opschalingen per contractjaar. Opdrachtnemer brengt de bijbehorende kosten naar rato van de resterende looptijd van het betreffende contractjaar in rekening conform de Prijzen uit het Prijzenformulier.
UE 76.	Indien gebruik gemaakt wordt van het tweede licentiemodel (op basis van Gebruiksrecht enterprise) uit Bijlage VI. (Prijzenformulier) (vergoeding op basis van Onbeperkt gebruik (door Eindgebruikers)) wordt de facturatie van de Subscriptions vooraf en eenmaal per jaar gedaan.
UE 77.	De Vergoeding voor Gebruiksrechten biedt het recht om altijd gebruik te maken van de Nieuwe versies van de Low-code Oplossing zonder dat sprake is van een additionele kosten.
UE 78.	Alle deeloplossingen in de vorm van plug-ins en/of add-ons die door de Fabrikant worden geleverd of worden ontwikkeld ten behoeve van de Low-code Oplossing zijn onderdeel van de geoffreerde Prijs.
UE 79.	De Vergoeding van Opleidingen die op verzoek van Opdrachtgever worden geleverd gedurende de Operationele fase van de Overeenkomst worden vooraf verrekend conform de Prijzen 'Opleidingen', tabblad '3. Additionele diensten' Bijlage VI. (Prijzenformulier).
UE 80.	Consultancy die op verzoek van Opdrachtgever wordt geleverd gedurende de Operationele fase van de Overeenkomst wordt verrekend op basis van nacalculatie conform de Prijzen 'Consultancy', tabblad '3. Additionele diensten' Bijlage VI. (Prijzenformulier). Facturatie vindt maandelijks plaats.

12.4 Indexering Prijs

De door Inschrijver geoffreerde Prijzen 'Gebruiksrecht' en 'Additionele diensten', zoals opgegeven in Bijlage VI. (Prijzenformulier) mogen na de initiële Looptijd en vanaf 2032 jaarlijks en steeds per 1 januari worden geïndexeerd op basis van de CBS-tabel 'Dienstenprijzen (DPI); commerciële dienstverlening en transport; indexcijfers 2021 = 100', (CPA2008, kwartaalindex) conform de volgende webpagina: <https://opendata.cbs.nl/#/CBS/nl/dataset/85817NED/table?dl=AE1CF>

Prijsaanpassingen dienen uiterlijk voor 1 november van enig jaar aan de Contractmanager ter goedkeuring te worden aangeboden, waarbij het op dat moment (door het CBS) meest recent beschikbare en gepresenteerde indexcijfer, Jaarmutatie per kwartaal, gehanteerd wordt. Het percentage voor de tariefstijging wordt afgerond op één decimaal achter de komma. Inhaalslagen op niet doorgevoerde indexeringen worden niet geaccepteerd.

Voorbeeld: als de overeenkomst op 1 januari 2024 geïndexeerd had mogen worden, was de prijsindexatie 4,5% geweest (jaarmutatie DPI 3e kwartaal 2023, meest recent beschikbare indexcijfer).

UE 81.	De door de Opdrachtnemer in Bijlage VI. (Prijzenformulier) opgegeven Prijzen, mogen jaarlijks per contractjaar geïndexeerd worden conform paragraaf 12.4. De eerste indexering vindt plaats niet eerder dan na expiratie van de Initiële Looptijd van de Overeenkomst.
UE 82.	Opdrachtnemer dient ten minste twee maanden, voorafgaande aan de genoemde momenten van indexering, een schriftelijk verzoek in met bijbehorende onderbouwing om voor de indexering in aanmerking te komen.

12.5 Factureren en bestellen

Als leverancier bent u verplicht elektronisch te factureren

Wij zijn als overheid vanaf november 2018 verplicht om e-factureren te implementeren. Dit is vastgelegd in de EU-Richtlijn Elektronische facturering bij overheidsopdrachten (2014/55/EU). De Rijksoverheid werkt sinds 1 januari 2017 bij nieuwe overeenkomsten met e-facturering.

Manieren van e-factureren

Ondernemers die goederen of diensten aan de Rijksoverheid leveren en een e-factuur willen sturen, kunnen dat op verschillende manieren doen:

- via een DigiPoort aansluiting;
- via het netwerk Peppol;
- via het leveranciersportaal.

Bekijk de video op de website: [Home | Helpdesk e-factureren \(helpdesk-efactureren.nl\)](#).

DigiPoort

De DigiPoort is een technische voorziening die beheerd wordt door Logius en die het mogelijk maakt om diverse elektronische berichten (waaronder facturen) met de Rijksoverheid uit te wisselen. Meer informatie over berichtenuitwisseling via de DigiPoort vindt u op [Handleiding Aansluiten op DigiPoort voor Bedrijven | Logius](#)

Peppol

Peppol is een digitale infrastructuur gebaseerd op Open standaarden voor het eenvoudig en veilig uitwisselen van e-facturen en andere elektronische berichten. Met Peppol kunt u e-facturen rechtstreeks versturen vanuit uw boekhoudstelsel of e-facturen versturen via een (commercieel)Peppol-portaal. Peppol is de nieuwe EU standaard voor elektronisch berichtenverkeer met de overheid. Meer informatie over Peppol vindt u op www.peppolautoriteit.nl/

Leveranciersportaal

U kunt ook gebruik maken van het e-factuurportaal van de Rijksoverheid, het leveranciersportaal. Op dit portaal kunt u e-facturen versturen en inkooporders of tijdkaarten ontvangen indien het departement dit ondersteunt. Het Rijk bevindt zich in een transitiefase wat betreft het leveranciersportaal. Het huidige leveranciersportaal van DigiInkoop wordt vervangen. U wordt tijdig geïnformeerd over de overgang naar het nieuwe leveranciersportaal.

UE 83.	De Opdrachtnemer voldoet aan de vereisten van e-facturatie via het leveranciersportaal of een geautomatiseerde koppeling met de DigiPoort (toekomstig E-procurementpoort) of het Peppol netwerk met daarin de referentie naar de inkooporder en de inkooporderregel.
UE 84.	Kosten die voortkomen uit het realiseren van de koppeling voor elektronische berichten uitwisseling met de Rijksoverheid worden gedragen door de Opdrachtnemer.
UE 85.	Opdrachtnemer vermeldt het inkoopordernummer als referentie op elke pakbon en factuur aan Opdrachtgever. Zonder dit inkoopordernummer kan Opdrachtgever de levering of de factuur weigeren.

UE 86.	Opdrachtnemer is verantwoordelijk voor de implementatie aan haar zijde. Op verzoek van Opdrachtgever kunnen wijzigingen in het implementatieplan en/of implementatie worden aangebracht die invloed hebben op het bestelproces. Hieronder valt in ieder geval het inzetten van extra expertise.
UE 87.	Opdrachtnemer accepteert dat er gedurende de looptijd van de Overeenkomst nieuwe-/Verbeterde versies van de Programmatuur van het leveranciersportaal in gebruik genomen kunnen worden.