



Belastingdienst

BIJLAGE A. Specificatie van de opdracht

Behorende bij : Beschrijvend document Gegevensstromen

Versie : 1.0 Definitief

Kenmerk : IUC21-051

Datum : 20 mei 2022

Inhoudsopgave

Inhoudsopgave	2
Hoofdstuk 1.	Doel van dit document4
Hoofdstuk 2.	Algemene eisen5
2.1.	Verplichtingen belastingen, milieubescherming, arbeidsvoorwaarden ..5
2.2.	Verzekering5
2.3.	Business Etiquette5
2.4.	Continuïteitsregeling.....6
2.5.	Juridische kaders6
Hoofdstuk 3.	Functionaliteiten7
3.1.	Opbouw van de dienst7
3.2.	Technische functionaliteiten8
Hoofdstuk 4.	Communicatie en offerteproces9
Hoofdstuk 5.	Implementatie fase..... 12
5.1.	Eisen aan de Voortbrenging..... 12
5.2.	Projectmanagement 14
5.3.	Gebruikers-acceptatietest 16
Hoofdstuk 6.	Operationele fase..... 18
6.1.	Technisch Beheer & Onderhoud Gegevensstromen 18
6.1.1.	Beschikbaarheid..... 18
6.1.2.	Performance..... 19
6.1.3.	Helpdesk en Service window 19
6.1.4.	Incident management..... 20
6.1.5.	Security management 21
6.1.6.	Business Continuity management..... 22
6.1.7.	Availability management 23
6.1.8.	Releasemanagement 23
6.2.	Service niveaus..... 23
Hoofdstuk 7.	Retransitie..... 25
Hoofdstuk 8.	IV kaders..... 26
8.1.	Toe te passen standaarden 26
8.2.	ISO 25010..... 27
8.3.	Wet- en regelgeving 27
8.4.	Beveiliging..... 27
8.4.1.	Logisch Toegangsbeheer..... 33
8.4.2.	Identity Management..... 34
8.5.	Gegevens..... 34
8.5.1.	Gegevens in rust..... 34
8.5.2.	Gegevens in transitie 35
8.5.3.	Schonen van Gegevens 35
8.5.4.	Verwerken van Gegevens 36
8.5.5.	Beveiligen van Gegevens 36
8.6.	Aansluitvoorwaarden..... 37

	8.7.	Bewaken van de Oplossing.....	38
Hoofdstuk 9.		Financiële afspraken.....	39
	9.1.	Tariefherziening	39
	9.2.	Facturatievoorwaarden	39
	9.3.	Elektronisch factureren (EBF) – e-factureren.....	40

Hoofdstuk 1. Doel van dit document

Dit document beschrijft de eisen en wensen die de Aanbestedende dienst stelt in het kader van de Europese aanbesteding Gegevensportalen met kenmerk IUC21-051. Dit document maakt integraal onderdeel uit van het Beschrijvend Document.

Hoofdstuk 2. Algemene eisen

In dit hoofdstuk zijn algemene Uitvoeringseisen opgenomen. De bepalingen in dit hoofdstuk hebben allemaal specifiek betrekking op de uitvoeringsperiode van de aanbestede opdracht, echter ook in de andere hoofdstukken komen Uitvoeringseisen voor.

2.1. Verplichtingen belastingen, milieubescherming, arbeidsvoorwaarden

UE 1	Opdrachtnemer dient bij de uitvoering van de Overeenkomst 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. Kennis omtrent die belastingen en milieubescherming, arbeidsvoorwaarden en arbeidsbescherming kunnen Opdrachtnemers, voor zover het gaat om uitvoering in Nederland, verkrijgen bij: • de Belastingdienst, www.belastingdienst.nl • het Ministerie van Infrastructuur en Milieu, www.rijksoverheid.nl/ministeries/ienm • het Ministerie van Sociale Zaken en Werkgelegenheid www.rijksoverheid.nl/ministeries/szw
------	--

2.2. Verzekering

UE 2	Gezien de aard van de werkzaamheden acht de Opdrachtgever het noodzakelijk dat Inschrijver verzekerd is tegen bedrijfsaansprakelijkheid, dan wel bereid en in staat te zijn om bij gunning zich voor bedrijfsaansprakelijkheid te verzekeren met een minimale dekking van €2.500.000 per jaar en een dekking van €1.000.000 per aanspraak, gedurende tenminste de looptijd van de Raamovereenkomst en de Nadere overeenkomsten. Op daartoe strekkend verzoek verstrekt de winnende Inschrijver bewijs van adequate verzekering.
------	--

2.3. Business Etiquette

Specifiek voor het zakendoen met marktpartijen heeft de Opdrachtgever de [Business Etiquette](#) (Bijlage 3) opgesteld. Hierin kunnen de externe partijen lezen wat wel en niet toegestaan is in de contacten met medewerkers van de Aanbestedende dienst.

UE 3	Opdrachtnemer conformeert zich aan de Business Etiquette zoals opgenomen in Bijlage 3.
------	---

2.4. Continuïteitsregeling

Opdrachtgever hecht groot belang aan het waarborgen van het continu en ongestoord gebruik van de Gegevensstromen door Opdrachtgever. De belangrijkste zorg van Opdrachtgever in deze is dat de Continuïteit van de dienstverlening aan de burgers en ondernemers te allen tijde gewaarborgd blijft. Om deze reden dient Opdrachtnemer na de definitieve gunning mee te werken aan het uitwerken van een regeling om dit te waarborgen. Deze regeling kan het afsluiten van een driepartijen overeenkomst in de vorm van een escrow overeenkomst zijn, maar ook andere uitwerkingen zijn denkbaar.

UE 4	Na definitieve gunning werkt u mee aan het uitwerken van een regeling om de Continuïteit en het ongestoorde gebruik van de Diensten te allen tijde te waarborgen, bijvoorbeeld door het afsluiten van een driepartijen overeenkomst in de vorm van een escrow.
------	--

2.5. Juridische kaders

De Concept Raamovereenkomst, inclusief Bijlagen (Bijlage 2) kan, alvorens deze door Partijen worden ondertekend, door de Opdrachtgever worden gewijzigd en nader uitgewerkt, mede naar aanleiding van de gedane opmerkingen en tekstsuggesties. Deze wijzigingen zullen per Nota van Inlichtingen kenbaar worden gemaakt.

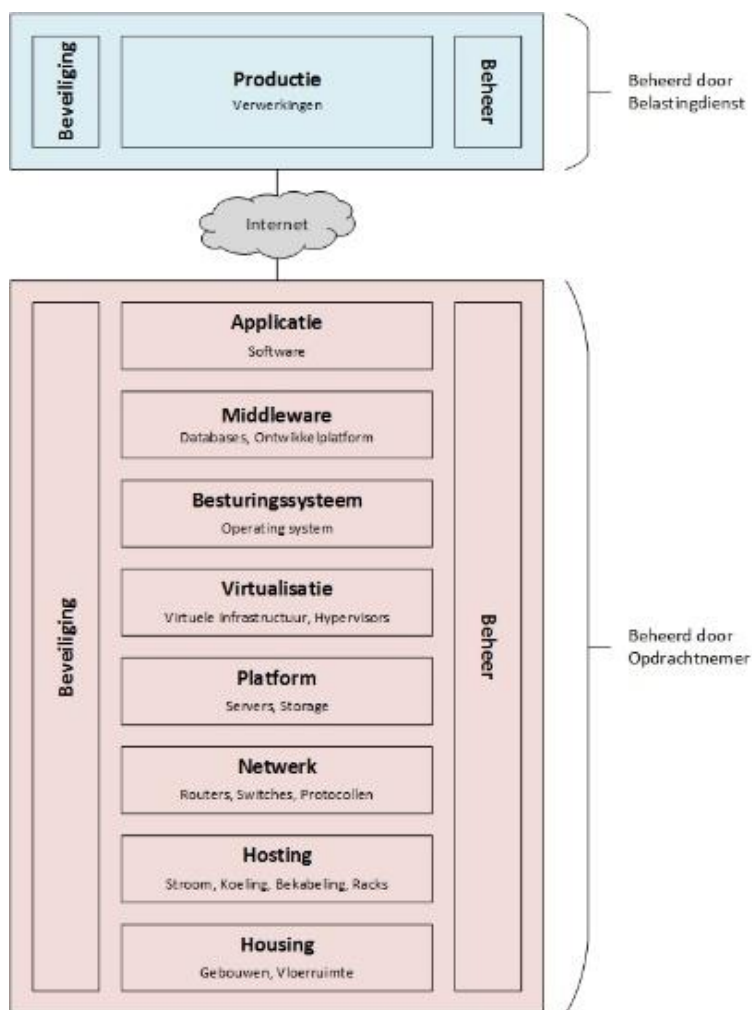
UE 5	Inschrijver gaat akkoord met de bijgevoegde Concept Raamovereenkomst, inclusief Bijlagen (Bijlage 2) met inbegrip van de eventuele per Nota van Inlichtingen kenbaar gemaakte wijzigingen.
UE 6	Inschrijver gaat akkoord met de volledige inhoud van Nadere overeenkomst, inclusief de bijbehorende Bijlagen.

Hoofdstuk 3. Functionaliteiten

De Belastingdienst wenst een Oplossing voor de gegevensuitwisseling met haar Gegevenspartners. Hierbij wordt gebruik gemaakt van Gegevensstromen. In de volgende paragraaf is de samenhang tussen de Gegevensstromen, Gegevensportalen, het gemeenschappelijk raamwerk en de (virtuele) machines beschreven en vereenvoudigd weergegeven.

3.1. Opbouw van de dienst

De Oplossing wordt als een SAAS-dienst aanbesteed. Ten aanzien van de SAAS-dienst is de verdeling in verantwoordelijkheidsgebieden tussen Opdrachtnemer en Belastingdienst opgenomen in de onderstaande Figuur 1.



Figuur 1. Opbouw van de dienst

De Oplossing dient uit één logisch geheel te bestaan. Hosting van de oplossing dient plaats te vinden binnen de Rijksoverheid, hiervoor is ODC-Noord geselecteerd. De Opdrachtgever sluit voor de hosting een contract af met ODC-Noord. Van de Opdrachtnemer wordt verwacht dat hij zo veel als mogelijk als aanspreekpunt voor de gehele oplossing fungeert. De Opdrachtgever zal de opdrachtnemer mandateren om, binnen afgesproken kaders, namens hen op te treden richting ODC-Noord. De Opdrachtnemer zal vooraf toestemming vragen aan de Opdrachtgever als acties implicaties op het service level kunnen hebben. Voor acties die financiële gevolgen kunnen hebben, ook voor het contract tussen ODC-Noord en de Opdrachtgever, vraagt de Opdrachtnemer expliciete toestemming van de Opdrachtgever.

UE 7	De Opdrachtnemer levert de Oplossing als één integraal werkend systeem dat bij ODC-Noord gehost moet worden. De Opdrachtgever garandeert dat de hostingpartij, ODC-Noord, een hostingoplossing levert die het voor de Opdrachtnemer mogelijk maakt om aan de in de Aanbestedingsstukken gestelde eisen te voldoen. Als de Oplossing bestaat uit deeloplossingen dan is de integratie van deze oplossingen de verantwoordelijkheid van de Opdrachtnemer. De Opdrachtnemer garandeert dat, bij gebruik van (deel)oplossingen van eventuele onderaannemers, ook deze partijen en hun (deel)oplossingen aan de in de Aanbestedingsstukken gestelde eisen voldoen. Opdrachtnemer verplicht zich er hierbij toe deze verplichtingen met de onderaannemer(s) vooraf schriftelijk overeen te komen en de naleving ervan te controleren. De Opdrachtnemer meldt bij de Opdrachtgever wanneer er sprake is van onderaannemerschap.
------	---

3.2. Technische functionaliteiten

UE 8	De Gegevensstromen worden ondersteund op de volgende browsers en browserversies: Chrome 97 (en hoger), Firefox 96 (en hoger), Microsoft Edge (alle versies), Safari 14 (en hoger).
------	--

In Bijlage B (Ontwerp Gegevensstromen) staan alle overige generieke technische eisen aangaande de Gegevensstromen omschreven. Deze Bijlage zal na de gunning onlosmakelijk onderdeel van de Raamovereenkomst zijn en als leidraad gelden bij elke offerteaanvraag en de Nadere overeenkomst. In verband met de leesbaarheid van dit document is ervoor gekozen om in onderstaande eisen te verwijzen naar Bijlage B (Ontwerp Gegevensstromen).

In Bijlage C. (Menukaart) is een voorbeeld van de menukaart opgenomen. Deze wordt in elke Nadere Overeenkomst gebruikt om van de diverse standaard onderdelen van een Gegevensstroom, die staan beschreven in Bijlage B, aan te geven of deze worden afgenomen in die overeenkomst.

Ten aanzien van de actuele Gegevensstromen zijn de Specificaties uitgewerkt in Bijlage D (Specificaties actuele Gegevensstromen)

UE 9	U gaat akkoord met Bijlage B (Ontwerp Gegevensstromen) en Bijlage C (Menukaart).
UE 10	U gaat akkoord met de uitgewerkte Specificaties van de actuele Gegevensstromen (Bijlage D).

Hoofdstuk 4. Communicatie en offerteproces

De Opdrachtgever hecht waarde aan duidelijke communicatielijnen. De Opdrachtgever is een grote organisatie en derhalve is het van belang dat juiste informatie op de juiste plekken terechtkomt.

UE 11	Opdrachtnemer stelt één Contactpersoon aan voor de Opdrachtgever die kennis neemt van de juiste communicatielijnen en deze naleeft.
-------	---

B/CFD IUC Belastingdienst is als enige partij binnen de Opdrachtgever gerechtigd overeenkomsten met de Opdrachtnemer aan te gaan. Indien er behoefte is aan een nieuwe Gegevensstroom of een Change op een of meerdere bestaande Gegevensstro(o)m(en) wordt door B/CFD IUC Belastingdienst een offerteaanvraag naar de Opdrachtnemer verstuurd. Bij alle offerteaanvragen, zowel op basis van een Menukaart als RFC-formulier, wordt een termijn meegegeven waarbinnen Opdrachtnemer zijn Offerte moet aanleveren bij B/CFD IUC Belastingdienst.

UE 12	Indien B/CFD IUC Belastingdienst daar door middel van een offerteaanvraag om verzoekt is de Opdrachtnemer verplicht tot het uitbrengen van een Offerte. Opdrachtnemer dient binnen twee weken of, indien anders vooraf is overeengekomen, conform de overeengekomen termijn een passende Offerte uit te brengen.
UE 13	De Opdrachtnemer zal de Offertes aanbieden in het Nederlands en/of Engels en de bedragen worden in Euro's excl. BTW weergegeven.

De Prijs voor de Realisatie en het Beheer en Onderhoud van nieuwe Gegevensstromen en Changes wordt bepaald op basis het aantal functiepunten vermenigvuldigd met de Prijs (voor Realisatie en Beheer en Onderhoud) per functiepunt. Bij de berekening van de kosten wordt onderscheid gemaakt tussen de functiepunten vanuit het raamwerk welke eenmalig worden gefactureerd voor alle gerealiseerde Gegevensstromen en de functiepunten die per Gegevensstroom worden gefactureerd.

In de offerte maakt de Opdrachtnemer, op basis van de Menukaart of het RFC-formulier, een calculatie van het aantal functiepunten, onderscheiden naar generiek (Raamwerk) en specifiek (per Gegevensstroom). Daarin wordt de omvang van Gegevensstromen en Changes vastgesteld op basis van de functiepuntenmethodiek en telrichtlijnen zoals beschreven in de Nesma Functiepuntenanalyse voor software onderhoud richtlijnen Versie 2.3 NL (Bijlage F). De Opdrachtgever zal deze daarna (steekproefsgewijs) controleren en bij verschil (groter dan 10% of structureel) zal er overleg plaatsvinden om gezamenlijk het juiste aantal functiepunten te bepalen. Mochten Partijen er gezamenlijk niet uitkomen dan heeft de Opdrachtgever het recht om de functiepuntentelling door een onafhankelijke derde partij uit te laten voeren waarvan het resultaat leidend zal zijn voor de uiteindelijke Offerte.

UE 14	De Opdrachtnemer zal de Offertes aanbieden op basis van de conform de functiepuntenmethodiek en telrichtlijnen zoals beschreven in de Nesma Functiepuntenanalyse voor software onderhoud richtlijnen Versie 2.3 NL (Bijlage F).
UE 15	De Opdrachtnemer gaat ermee akkoord dat de Opdrachtgever, op eigen kosten, een derde onafhankelijke partij kan inschakelen indien: 1. het aantal functiepunten in de uitgebrachte Offerte meer dan 10% afwijkt van de functiepuntentelling van de Opdrachtgever; 2. of wanneer er sprake is van een structurele afwijking in de telling van functiepunten. De functiepuntentelling van deze derde partij is dan leidend voor de Offerte van Opdrachtnemer.

UE 16	Na oplevering van de Gegevensstroom of Change levert Opdrachtnemer een functiepuntanalyse op van hetgeen daadwerkelijk is opgeleverd. Opdrachtgever controleert de functiepuntanalyse van hetgeen is opgeleverd. Opdrachtgever en Opdrachtnemer stemmen de nieuwe productomvang af zodat de basis voor volgende projecttellingen helder is.
-------	---

In voorkomende gevallen kunnen Partijen tot inzicht komen dat de functiepuntanalyse bij bepaalde werkzaamheden en/of Changes een aantoonbaar onredelijk nadeel voor Opdrachtnemer of Opdrachtgever oplevert (zoals mogelijk bij het verwijderen van (meerdere) functionaliteiten).

UE 17	Partijen kunnen overeenkomen dat bepaalde werkzaamheden of Changes op basis van een Prijs per uur wordt geoffreerd en uitgevoerd. Ook voor het Beheer en onderhoud kunnen in dat geval specifieke afspraken worden gemaakt.
UE 18	Indien hier sprake van is geldt een maximaal uurtarief per uur (excl. BTW) zoals in Bijlage vi (Prijsmodel) opgenomen. De werkzaamheden worden uitgevoerd op basis van een open boek calculatie. De Opdrachtnemer geeft hierbij inzicht in het aantal uren dat wordt en is besteed, welke werkzaamheden per uur zijn uitgevoerd en welke personen met welke functies de werkzaamheden hebben uitgevoerd inclusief een berekening van de totstandkoming van de prijs op persoonsniveau.

In (toekomstige) Nadere overeenkomsten worden de Gegevensstromen gespecificeerd door middel van een Menukaart (Bijlage C) met generieke bouwblokken gebaseerd op het hoofddocument Ontwerp Gegevensstromen, Bijlage B, en eventuele aanvullende specifieke eigenschappen, of afwijkingen ten opzicht van de generieke opzet.

Voor toekomstige nieuwe Gegevensstromen zal deze Menukaart, Bijlage C, met eventuele aanvullende eigenschappen of afwijkingen, het basisdocument zijn om tezamen met de offerteaanvraag richting Opdrachtnemer te sturen. Na acceptatie van de Offerte zal deze als Bijlage bij de daaruit voortvloeiende Nadere overeenkomst worden gevoegd.

UE 19	Bij een offerteaanvraag wordt gebruik gemaakt van de Menukaart (Bijlage C), eventueel aangevuld met specifieke eigenschappen of afwijkingen, welke na de acceptatie als Bijlage aan de Nadere overeenkomst van de betreffende Gegevensstroom wordt gevoegd.
-------	---

Een Request For Change wordt gedaan door middel van een offerteaanvraag waar het RFC-formulier (Bijlage E), bij wordt gebruikt. Een Request For Change wordt altijd gedaan onder een bestaande Nadere overeenkomst.

De Opdrachtnemer doet de Opdrachtgever een aanbieding door middel van het invullen en retourneren van het RFC-formulier. Acceptatie van deze Offerte vindt plaats door ondertekening van het RFC-formulier door beide Partijen aangevuld met een Inkoopopdracht. Het RFC-formulier wordt als addendum bij de betreffende Nadere overeenkomst toegevoegd.

Eventueel meer- en minderwerk zal tevens via een Change-procedure verlopen.

UE 20	Bij een Request voor Change maakt Opdrachtnemer gebruik van het daarvoor bestemde RFC-formulier (Bijlage E), welke na acceptatie als addendum aan de Nadere overeenkomst van de betreffende Gegevensstroom wordt toegevoegd.
-------	--

De acceptatie van een Offerte, het sluiten van een Nadere overeenkomst en overeenkomen van een Change wordt gedaan door B/CFD IUC van de Opdrachtgever. Acceptatie van een Offerte door een ander bedrijfsonderdeel van de Opdrachtgever is niet mogelijk. De acceptatie van een Offerte gaat altijd tezamen met het verstrekken van een Inkoopopdracht inclusief Bestelnummer voor de facturatie.

Let op: dit staat los van Acceptatie door middel van een Acceptatietest van de nieuw te leveren Diensten welke toeziet op het testen van de Gegevensstroom op basis van de gestelde Specificaties.

UE 21	Opdrachtnemer start met de uitvoering van de Diensten nadat Opdrachtnemer per e-mail een getekende acceptatie van de Offerte van B/CFD IUC van de Opdrachtgever heeft ontvangen vergezeld van een Inkoopopdracht met Bestelnummer.
-------	--

Hoofdstuk 5. Implementatie fase

5.1. Eisen aan de Voortbrenging

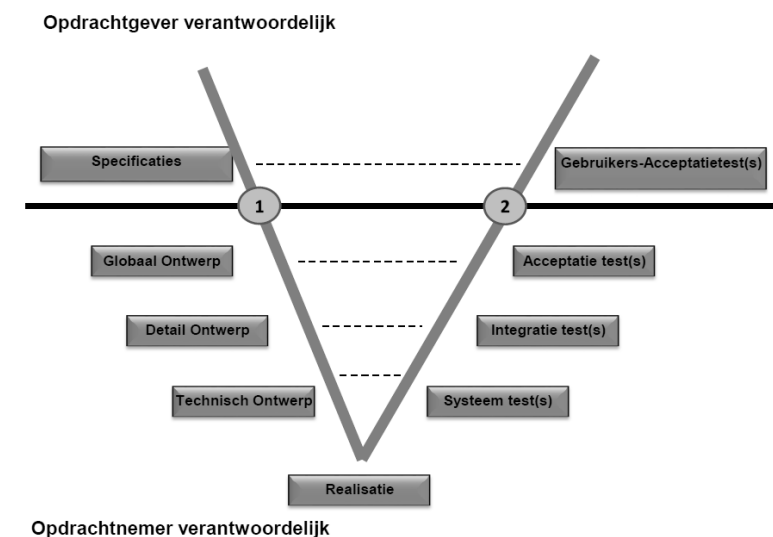
De Opdrachtnemer en Opdrachtgever zorgen gezamenlijk voor een goede aansluiting van elkaars ketens zodat er een logisch Voortbrengingsproces ontstaat, de Opdrachtnemer dient hierin het voortouw te nemen. Deze invulling en afstemming dient als een van de eerste projectactiviteiten te worden opgepakt, zodat er tijdens de uitvoering van het Voortbrengingsproces voor beide Partijen geen onduidelijkheid is. In alle gevallen geldt dat Partijen elkaar hierbij, zonder additionele kosten, ondersteunen waar dat nodig en/of gewenst is.

UE 22 Bij de start van de Raamovereenkomst zorgen Partijen voor een goede aansluiting van elkaars ketens zodat er een logisch Voortbrengingsproces ontstaat. Pas nadat er akkoord is tussen Partijen zal worden gestart met het uitvoeren van het Voortbrengingsproces.

Het gezamenlijke Voortbrengingsproces is weergegeven in figuur 2 door middel van een vereenvoudigd V-model.

Er zijn veel manieren om het V-model weer te geven en in te richten, in een scrum of agile omgeving wordt bijvoorbeeld vaak gesproken over een W-model. Omwille van de eenvoud is hier gekozen voor de weergave als V-model. Het figuur schrijft niet voor hoe Opdrachtnemer geacht wordt voor te brengen, noch geeft het in detail weer welke Gebruikers-acceptatietest(s) door de Opdrachtgever wordt uitgevoerd. Het doel is te visualiseren voor welk deel de Opdrachtgever en voor welk deel de Opdrachtnemer verantwoordelijk is. Het deel boven de dik weergegeven streep is de verantwoordelijkheid van de Opdrachtgever, de activiteiten daaronder zijn de verantwoordelijkheid van de Opdrachtnemer.

De cijfers 1 en 2 in figuur 2 geven het moment van overdracht van de verantwoordelijkheid weer, dit zijn Overdrachtmoment 1 en Overdrachtmoment 2.



Figuur 2. Voortbrenging V-model

Het opstellen van Specificaties is de verantwoordelijkheid van de Opdrachtgever. Na de acceptatie van een Offerte, Change en/of het sluiten van een Nadere overeenkomst vindt Overdrachtmoment 1 uit figuur 2 plaats, daarna is de Opdrachtnemer verantwoordelijk voor de Voortbrenging. Voor de initiële Gegevensstromen die in deze Aanbestedingsstukken al zijn gespecificeerd geldt dat de eerste stap in dit Voortbrengingsproces al reeds is uitgevoerd door de Opdrachtgever.

UE 23	U gaat akkoord met het overnemen van de verantwoordelijkheid in het Voortbrengingsproces bij Overdrachtsmoment 1, na het opleveren van Specificaties door de Opdrachtgever en de acceptatie van een Offerte, Change en/of het sluiten van een Nadere overeenkomst.
UE 24	In de periode na Overdrachtsmoment 1 voert de Opdrachtnemer alle werkzaamheden uit die benodigd zijn voor het opleveren van een Gegevensstroom of Change conform de Specificaties op Overdrachtsmoment 2.

De Opdrachtnemer dient de leiding te nemen bij de Implementatie van de Oplossing. Om inzicht te krijgen op welke wijze de Opdrachtnemer de Implementatie uit gaat voeren, wordt een Plan van Aanpak gevraagd dat door de Belastingdienst wordt beoordeeld. De Belastingdienst stelt een projectmanager aan die namens de Belastingdienst verantwoordelijk is voor de Implementatie. De projectmanager van de Opdrachtnemer dient de Implementatie uit te voeren conform het Plan van Aanpak in samenwerking met de projectmanager van de Belastingdienst. Het gecombineerde projectmanagement zal rapporteren aan een stuurgroep.

UE 25	Opdrachtnemer heeft een resultaatverplichting voor het tijdig (conform vooraf overeengekomen planning) productiegereed Opleveren van de Gegevensstromen. Het in Gebruik nemen van de Oplossing vindt plaats na Acceptatie van de Oplossing door de Belastingdienst. In UE 38 zijn de data opgenomen wanneer de initiël te realiseren Gegevensstromen in gebruik moeten zijn genomen.
UE 26	Opdrachtnemer levert bij Inschrijving een Plan van Aanpak voor de Implementatie van de Oplossing.
UE 27	Het door Opdrachtnemer in te dienen Plan van Aanpak, vormt de basis voor de wijze waarop de Oplossing wordt geïmplementeerd. Het Plan van Aanpak zal na het tekenen van de Overeenkomst tussen Opdrachtnemer en de Belastingdienst worden besproken. Pas nadat er akkoord is tussen Partijen over het Plan van Aanpak zal worden gestart met het uitvoeren van de Implementatie.
W 1	Plan van aanpak Om inzicht te krijgen in de wijze waarop de Opdrachtnemer de Implementatie uit gaat voeren, dient Opdrachtnemer een Plan van Aanpak voor de Implementatie in te dienen. In dit Plan van Aanpak dient u in ieder geval de volgende aspecten uit te werken: • Projectmanagementmethode en projectaanpak om tot de gewenste functionaliteit, inclusief “look and feel”, van de Oplossing te komen; • De aanpak om koppelvlakken en gegevensuitwisselingen met derden te realiseren; • Projectorganisatie en governance incl. escalatieprocedure en interactie met Belastingdienst (welke rollen worden wanneer betrokken en geïnformeerd); • Beschrijving van de (5 belangrijkste) beheersmaatregelen van risico's om de in productie name van de Oplossing te borgen; • De randvoorwaarden waar de Belastingdienst aan moet voldoen om de in productie name van de Oplossing te borgen; • De aanpak voor het instrueren, begeleiden en ondersteunen van Gebruikers; • Test- en Acceptatieproces;

	De Belastingdienst wil in ieder geval kunnen vaststellen of de Oplossing voldoet aan de gevraagde eisen en wensen uit de aanbestedingsdocumenten. Vraag: Beschrijf het concept Plan van Aanpak in maximaal zeven (7) pagina's A4 en één (1) pagina A3 ten behoeve van een planning. De Belastingdienst verwacht van het antwoord van de Opdrachtnemer dat: • De beantwoording volledig is conform de hierboven genoemde aspecten. • Het antwoord overtuigend, samenhangend en logisch is. Beoordeling: Het Plan van Aanpak wordt integraal op bovenstaande aspecten beoordeeld op de mate van haalbaarheid om tot het gewenste eindresultaat te komen binnen de gewenste doorlooptijd. Voor deze Wens zijn in totaal maximaal 75 punten te behalen.
--	---

5.2. Projectmanagement

Van Opdrachtnemer wordt verwacht het projectmanagement te voeren ten aanzien van het gehele Voortbrengingsproces. Opdrachtnemer werkt daarbij samen met de Opdrachtgever, waarbij de Opdrachtgever verwacht zoveel mogelijk ontzorgd te worden. De Opdrachtgever is gewend aan de Prince II methodiek voor projectmanagement maar tevens bekend met methodieken als waterval, Scrum en Agile.

UE 28	Het door u, ten beantwoording van wens 1 aangeleverde Plan van Aanpak, vormt de basis voor de wijze waarop de Diensten (project ten behoeve van de initiële Gegevensstromen, toekomstige Gegevensstromen en Changes) worden gemanaged en uitgevoerd. Bij de start van de Raamovereenkomst zal Opdrachtnemer het Plan van Aanpak in overleg met Opdrachtgever nader afstemmen in invullen. Pas nadat er akkoord is tussen Partijen over de inhoud van het Plan van Aanpak zal worden gestart met het uitvoeren van het Voortbrengingsproces ten behoeve van de Gegevensstromen.
-------	---

Van de Opdrachtnemer wordt verwacht dat de Kwaliteit van de op te leveren Gegevensstromen en Changes zodanig hoog is dat er bij Overdrachtmoment 2 geen Blokkerende of Ernstige Bevindingen open staan. Eventuele Storende Bevindingen dienen bij een volgende Release opgelost te worden.

UE 29	Bij Overdrachtmoment 2 van een op te leveren Gegevensstroom of Change staa(t)(n) er geen Blokkerende of Ernstige Bevindingen (meer) open op de betreffende Gegevensstroom, Change, of de Gegevensstroom waar de Change op van toepassing is. Storende Bevindingen worden bij een volgende Release opgelost.
-------	--

Bij Overdrachtmoment 2 toont de Opdrachtnemer aan dat de opgeleverde Gegevensstroom of Change voldoet aan de Specificaties. Pas nadat de Opdrachtgever de overdracht heeft beoordeeld én goedgekeurd zal de Gebruikers-acceptatietest worden uitgevoerd.

UE 30	Bij Overdrachtmoment 2 toont de Opdrachtnemer aan dat de opgeleverde Gegevensstroom of Change voldoet aan de Specificaties en levert daarvoor ter goedkeuring door de Opdrachtgever een testplan op, met logische en fysieke testgevallen, alsmede testrapportages inclusief een traceability tabel, Known errors en vrijgaveadvies.
-------	---

UE 31	De Opdrachtnemer levert bij Overdrachtmoment 2 Documentatie in de vorm van handleidingen voor de Beheerders van de Gegevensstroom. Deze handleiding bevat ten minste een beschrijving van de functionaliteiten van de Gegevensstroom en de wijze van het gebruik.
UE 32	Ten behoeve van de Gebruikers-acceptatietest dienen de op te leveren Gegevensstromen en Changes voor de Opdrachtgever beschikbaar te zijn binnen een Testomgeving van Opdrachtnemer waarbij het mogelijk is de testwerkzaamheden uit te voeren door middel van webtoegang op een locatie van de Opdrachtgever.

Voor het bepalen van de omvang van de Gegevensstromen en Changes hanteert de Opdrachtgever de functiepuntenmethodiek en telrichtlijnen zoals beschreven in de Nesma Functiepuntenanalyse voor software onderhoud richtlijnen Versie 2.3 NL (Bijlage F). Opdrachtgever is zich ervan bewust dat de op te leveren Gegevensstromen en Changes fouten kunnen bevatten.

UE 33	Opdrachtnemer gaat akkoord met het toepassen van de functiepuntenmethodiek en telrichtlijnen zoals bechreven in de Nesma Functiepuntenanalyse voor software onderhoud richtlijnen Versie 2.3 NL (Bijlage F) voor het bepalen van de omvang van Gegevensstromen en Changes.
UE 34	Opdrachtnemer gaat akkoord met de volgende normen voor monitoren en beoordelen van de Kwaliteit van de op te leveren Gegevensstromen en Changes: 1. Minimaal 95% van de fouten wordt gevonden en opgelost voorafgaand of tijdens de Gebruikers-acceptatietest van de op te leveren Gegevensstromen en Changes. 2. De overige fouten (maximaal 5%) dienen in de eerste maand na ingebruikname van de opgeleverde Gegevensstromen en Changes te worden gevonden en opgelost. 3. Er worden in de eerste maand na ingebruikname van de opgeleverde Gegevensstromen en Changes maximaal 1,5 bevindingen per 100 functiepunten gevonden en opgelost. Omdat de complexiteit van op te leveren Gegevensstromen en Changes kan verschillen kunnen Opdrachtnemer en Opdrachtgever in onderling overleg andere normen afspreken voor specifieke Gegevensstromen en Changes

Zodra er door middel van het goed doorlopen van de Gebruikers-acceptatietest invulling is gegeven aan de Specificaties zal de Opdrachtgever deze formeel Accepteren. Vervolgens start de Operationele fase.

Ten aanzien van de Bevindingen gelden de volgende eisen om de Gebruikers-acceptatietest te kunnen beëindigen:

UE 35	Om de Gebruikers-acceptatietest te kunnen beëindigen en de Gegevensstroom of Change te Accepteren geldt het volgende ten aanzien van de Bevindingen: 1. Er staan geen Blokkerende Bevindingen open. 2. Er staan geen Ernstige Bevindingen open.
UE 36	Bevindingen ten gevolge van de Gebruikers-acceptatietest, of Incidenten tijdens de productie of Operationele fase, worden door de Opdrachtnemer geanalyseerd en, conform afspraken en/of vastgestelde Prioriteit, Opgelost, of er wordt aangetoond dat er geen Oplossing nodig is, bijvoorbeeld bij gebruikersfouten.

Het is productie nemen van de Gegevensstroom of Change gaat in onderlinge afstemming tussen Opdrachtnemer en de Opdrachtgever. Let op: het moment van in productie name kan op een later moment zijn dan de start van de Operationele fase. Gedurende de Implementatie en het in productie nemen van de Gegevensstroom of Change is de Opdrachtnemer bereikbaar voor de Opdrachtgever.

UE 37	De Implementatie en het in productie nemen van de Gegevensstroom of Change gaat in onderlinge afstemming tussen Opdrachtnemer en de Opdrachtgever. De Opdrachtnemer is goed bereikbaar voor de Opdrachtgever gedurende het in productie nemen van een Gegevensstroom of Change.			
UE 38	De initiële Gegevensstromen dienen, uiterlijk op de volgende data door Opdrachtgever Geaccepteerd en in productie te zijn genomen. Gegevensstroom A t/m J uiterlijk per 01-02-2024 met uitzondering van de optionele Gegevensstroom G welke op 01-02-2023 in productie genomen dient te worden.			
	De Specificaties waaraan de Gegevensstromen moeten voldoen zijn opgenomen in Bijlage D.			
	Inwinstromen: Hierbij leveren Gebruikers gegevens aan bij de Belastingdienst			
	ID	Portaal	Gegevensstroom	Datum
	I01	Portaal Internationale Gegevensuitwisseling	A. Bank- en beleggingsproducten	01-02-2024
			B. CbC Notificaties	01-02-2024
	I03	Portaal Verzekeringsproducten	C. Verzekerings-producten	01-02-2024
	I05	Portaal Kinderopvang organisaties	D. Verleende kinderopvang	01-02-2024
			Gastouder bureaus	01-02-2024
	I08	Portaal OV verklaringen	F. OV-verklaringen	01-02-2024
I09	Portaal Eigenwoning en Lijfrentesparen	G. Eigenwoning- en Lijfrentesparen	01-02-2023 (optioneel)	
I10a	Gegevensportaal Belastingdienst	H. 'Ad-hoc'	01-02-2024	
Verstrekstromen: Hierbij worden Gegevens worden vanuit de Belastingdienst verstrekt aan Gegevenspartners, vaak op basis van een vraagbestand dat wordt aangevuld met gegevens tot een antwoordbestand.				
ID	Portaal	Gegevensstroom	Datum	
V01	Portaal Inkomensafhankelijke Huurverhoging	I. Inkomensafhankelijke huurverhoging	01-02-2024	
V02	Portaal Gemeenten en Waterschappen	J. Dwanginvordering lokale overheden	01-02-2024	

5.3. Gebruikers-acceptatietest

Voor in productie name van de Oplossing, inclusief nieuw op te leveren gegevensstromen, changes en documentatie, wordt een Acceptatietest door de Belastingdienst uitgevoerd. Er kan worden getest op alle specificaties. De Gebruikers-acceptatietest vindt plaats in de Acceptatie-omgeving van Opdrachtnemer en is een voorwaarde voor Acceptatie van de Resultaten van de Diensten alvorens deze operationeel door de Opdrachtgever in gebruik worden genomen.

Tijdens de Acceptatietest kan de Opdrachtgever de door de Opdrachtnemer opgeleverde Dienst en/of Change testen op de volgende onderdelen:

1. Functionaliteit. Dat wil zeggen alle aspecten van gedrag en resultaten zoals beschreven in de overeengekomen specificaties.
2. Robuustheid. Dat wil zeggen, de mate waarin de gegevensstroom zinvol reageert op foute invoer, technische foutsituaties en gebruikersfouten.
3. Koppelingen met andere informatiesystemen.

4. Gebruikersinterface (incl. performance en gebruikersvriendelijkheid).
5. De mate waarin de gegevensstroom voldoet aan de overeengekomen kwaliteitsniveaus.
6. Documentatie voor beheerders en gebruikers.
7. Procedures voor handmatige werkzaamheden (zo die er zijn).
8. Een A&P test bij een nieuwe gegevensstroom of change
9. Een performancetest kan onderdeel zijn van de gebruikers-acceptatietest.

UE 39	De Belastingdienst behoudt zich het recht voor om vóór in productionname de overeengekomen Specificaties te testen in een Acceptatietest. De Acceptatietest vindt plaats in de Acceptatie-omgeving. Opdrachtnemer dient hieraan kosteloos mee te werken. De bevindingen van de Acceptatietest worden door de Opdrachtnemer opgelost. Na een succesvolle afronding van de Acceptatietest zal de datum, moment en wijze van In Productie name tussen Partijen worden afgestemd en overeengekomen. De beheerfase gaat in ná succesvolle afronding van de Acceptatietest.
-------	---

De Belastingdienst wil voorkomen dat er enkel op basis van de A&P test van de leverancier een kwetsbare Oplossing naar productie wordt gebracht.

UE 40	Opdrachtgever behoudt zich het recht voor om een A&P-test uit te voeren als onderdeel van de Acceptatietest vóór in Productionname van de Oplossing. Opdrachtnemer dient hieraan kosteloos mee te werken. Kwetsbaarheden met de classificatie critical of high (conform CVSS 3.1) worden door de Opdrachtnemer opgelost voordat door Opdrachtgever overgegaan kan worden tot het in productionnemen van de Oplossing.
UE 41	Bij het testen van de Oplossing mag geen gebruik worden gemaakt van naar Natuurlijke Personen herleidbare gegevens. Indien het voor het testen van de Oplossing noodzakelijk is om gegevens te gebruiken die herleidbaar zijn naar individuen dienen afdoende beveiligingsmaatregelen te zijn getroffen en dient er een door Opdrachtgever ondertekende Waiver overlegd te kunnen worden.
UE 42	Infrastructurele en functionele wijzigingen ten aanzien van de Oplossing worden door de Opdrachtnemer minimaal twee maanden voor geplande implementatiedatum aangekondigd. Dit zodat Opdrachtgever in afstemming met de Opdrachtnemer in de gelegenheid wordt gesteld een Acceptatietest te organiseren en uit te voeren voor de wijzigingen die impact kunnen hebben op koppelvlakken en gegevensuitwisselingen met andere dan door de Opdrachtnemer geboden Oplossingen. Wijzigingen die impact kunnen hebben op koppelvlakken en gegevensuitwisselingen dienen voor in productionname geaccepteerd te worden door de Belastingdienst.

Hoofdstuk 6. Operationele fase

De operationele fase vangt aan na integrale Acceptatie van een Gegevensstroom waarin Opdrachtnemer de Oplossing operationeel houdt, innoveert en verbetert tot het moment van Retransitie. In onderstaande paragrafen is deze fase verder beschreven.

6.1. Technisch Beheer & Onderhoud Gegevensstromen

Technisch beheer en Onderhoud van de Gegevensstromen richt zich op het 'in stand houden' en onderhouden van de applicatie-infrastructuur. Aangezien deze opdracht een SaaS-dienst betreft, zal Technisch beheer en Onderhoud in zijn geheel bij de Opdrachtnemer liggen. De opdrachtgever is verantwoordelijk voor Hosting bij ODC-Noord. Opdrachtnemer is verantwoordelijk voor de volledige regie hierop.

UE 43	Opdrachtnemer levert per Gegevensstroom vanaf het moment dat de Operationele fase begint Technisch beheer en Onderhoud conform de duur van de bijbehorende Nadere overeenkomst. De Operationele fase bedraagt maximaal zes (6) jaar.
UE 44	Hosting wordt uitgevoerd door ODC-Noord. De Opdrachtgever sluit hiervoor een contract af. Opdrachtnemer is verantwoordelijk voor de regievoering op de Hosting. De Opdrachtgever zal de opdrachtnemer hiervoor de benodigde mandaten en kaders verstrekken.
UE 45	Opdrachtnemer is volledig verantwoordelijk voor het Technisch beheer en Onderhoud op de Gegevensstromen. Een en ander binnen de kaders en mandaten zoals overeengekomen met betrekking tot de Hosting bij ODC-Noord

6.1.1. Beschikbaarheid

UE 46	De Oplossing voldoet minimaal aan het volgende Service Levels m.b.t. de beschikbaarheid van de Oplossing: • 7*24 openstelling van de gehele Oplossing voor gebruik door de Opdrachtnemer; • Norm: beschikbaarheid van 99,8% per maand (= maximaal 1,5 uur downtime per maand); • Beschikbaarheid is exclusief downtime bij implementaties van wijzigingen ten aanzien van de Oplossing op verzoek van de Opdrachtnemer. Berekening van Beschikbaarheid: • Berekening Beschikbaarheid: $(\text{gerealiseerd aantal uren} / \text{Beschikbaarheid/overeengekomen uren}) \times 100$; • Overeengekomen aantal uren Beschikbaarheid = aantal uren Openstellingstijden – (aantal uren gepland Technisch beheer en onderhoud en/of maintenance tijdens Openstelling); • Gerealiseerd aantal uren Beschikbaarheid = overeengekomen aantal uren Beschikbaarheid – som van de Oplostijden van prio 1 Incidenten.
-------	--

6.1.2. Performance

UE 47	De Opdrachtnemer voldoet minimaal aan de volgende performancenormen en kan dit op basis van monitoring aantonen:	
	Uitwerking	Te behalen KPI
	Reactietijd schermopbouw	bij 95% onder 1 seconde (maximaal 3 seconden) per maand
	Time outs tijdens uploaden	30 minuten (maximaal) per maand
UE 48	Gemiddelde downloadsnelheid	14,2 Mbit/s Voor minimaal 75% van het aantal downloads per maand dient deze snelheid behaald te worden
	De Opdrachtnemer voldoet minimaal aan de volgende norm ten aanzien van het aantal gelijktijdige gebruikers	
	- Tot een maximum van 10.000 gebruikers 100% van de gebruikers per Gegevensstroom; - Vanaf 10.000 gebruikers tenminste 25% van de totale doelgroep van de Gegevensstroom.	

6.1.3. Helpdesk en Service window

UE 49	De Opdrachtnemer voldoet minimaal aan de volgende normen:		
	Omschrijving	Indicator	Norm
	Openstelling Helpdesk Opdrachtnemer	Reguliere Openingstijd	Maandag t/m Vrijdag 09:00 – 17:00 Nederlandse tijd
		Stand-by Openingstijd service desk voor melden Prio 1 Incidenten	7*24 uur*365 dagen
	Service window	Reguliere service uren waarin ondersteuning wordt geleverd	Maandag t/m Vrijdag: 08:00 – 17:00 Nederlandse tijd
		Stand-by service uren waarin voor Prio 1 verstoringen ondersteuning wordt geleverd	7*24 uur
	Stand-by	Extra (stand-by) openstelling service desk en/of ondersteuning t.b.v. speciale situaties (b.v. implementaties).	Wordt aangevraagd uiterlijk 5 Werkdagen voor aanvang. Opdrachtnemer mag hiervoor vooraf overeengekomen additionele kosten berekenen)
	Monitoring en alerting	Opdrachtnemer heeft een monitoring en alerting proces ingericht om direct (binnen 2 klokuren, conform reactietijd Prio1) te kunnen handelen in geval van Incidenten en (dreigende) verstoring van de beschikbaarheid van de oplossing	7*24 uur*365 dagen
Indien nodig zal Opdrachtnemer doorwerken buiten het service window om een Incident op te lossen (doorwerk garantie).			

UE 50	Opdrachtnemer beschikt over een online ticket omgeving voor het kunnen aanmelden en volgen van Incidenten en vragen.
UE 51	Een ongelimiteerd aantal Calls kan via website (of e-mail) en telefonisch worden aangemeld.

6.1.4. Incident management

Met betrekking tot het bepalen van de prioriteit van Bevindingen gebruikt de Opdrachtgever een standaard model. Afhankelijk van de Impact en de Urgentie wordt de Prioriteit bepaald van opgetreden Incidenten. Bij verschil van inzicht bepaald de Opdrachtgever uiteindelijk de Prioriteit.

Impact	
Hoog	Een Incident heeft of kan ernstige gevolgen hebben voor • 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 Opdrachtgever en/of • onacceptabele hoge kosten.
Laag	• Overige situaties.
Urgentie	
Hoog	Een Incident • beïnvloedt Kwaliteit van functies/Beschikbaarheid/Beveiliging sterk en/of • brengt integriteit van de Gegevens in het geding en/of • treedt op tijdens peiktijd/-periode van het bedrijfsproces en/of • brengt uiterste verzenddatum van klantbescheiden in gevaar en/of • verstoort de communicatie met de klanten van 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	
Prioriteit 1	• Impact hoog / Urgentie hoog
Prioriteit 2	• Impact hoog / Urgentie laag • Impact laag / Urgentie hoog
Prioriteit 3	• Impact laag / Urgentie laag

UE 52

Op basis van bovenstaande tabel worden de prioriteiten van de Incidenten bepaald. De Oplossing voldoet minimaal aan de volgende Serviceniveaus ten aanzien van de afhandeling van Incidenten (Oplostijd):

Prestatie- indicator	Doel
Oplostijd Incident prio 1	Ma. 00:00 – Zo. 24:00 uur Nederlandse tijd: 4 klokuren
Oplostijd Incident prio 2	Ma t/m vr 08:00 – 17:00 Nederlandse tijd: 24 klokuren
Oplostijd Incident prio 3	Ma t/m vr 08:00 – 17:00 Nederlandse tijd: 72 klokuren

Toelichting op oplostijden

De beoogd hostingpartner, ODC-Noord, hanteert voor prio 2 16 werkuren en voor prio 3 incidenten 24 werkuren (op maandag t/m vrijdag tussen 8:00 en 17:00 uur) als oplostijd. Daarmee wijkt ODC-Noord af van de hierboven genoemde criteria. De door ODC-Noord gehanteerde oplostijden voor prio 2 en prio 3 incidenten blijven echter ruim binnen de hierboven gestelde kaders.

Het beheer van applicaties wordt binnen de Belastingdienst uitgevoerd met een IT Service Management functionaliteit (IBM Control Desk).

6.1.5. Security management

UE 53	Beveiligingsincidenten zijn incidenten die een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van de data in informatieverwerkende systemen hebben.
	Beveiligingsincidenten dienen door de Opdrachtnemer altijd als volgt te worden geclassificeerd: • Impact: Hoog • Urgentie: Hoog Onder Beveiligingsincidenten worden o.a. de onderstaande incidenten bedoeld: • (Poging tot) Cyberinbraak; • Responsible Disclosure; • Common Vulnerability en Exposures (CVE) en Security Notes en NCSC kennisgevingen; • Bevindingen A&P-test conform (classificatie) paragraaf 8.4 Beveiliging.
	UE 54
	Opdrachtnemer informeert de Belastingdienst onmiddellijk wanneer er een beveiligingsincident wordt geconstateerd of redelijkerwijs verwacht, ten aanzien van de data en/of persoonsgegevens van de Belastingdienst. Opdrachtnemer zal in dat geval tevens de omvang van het incident aangeven alsmede de reeds getroffen en te treffen maatregelen om de gevolgen te beperken. Dit onverminderd de wettelijke verplichting van Opdrachtnemer, als verwerkingsverantwoordelijke, om datalekken te melden bij de Autoriteit persoonsgegevens.
UE 55	Een Beveiligingsincident wordt altijd per direct na constatering (24 uur per dag, 7 dagen per week en 365 dagen per jaar) opgevolgd met een actie van de Opdrachtnemer. Beveiligingsincidenten moeten derhalve ook altijd (24 uur per dag, 7 dagen per week en 365 dagen per jaar) aangemeld kunnen worden.

W 2	Afhandeling van Beveiligingsincidenten Om inzicht te krijgen in de wijze waarop de Beveiligingsincidenten door de Opdrachtnemer adequaat, effectief en efficiënt worden afgehandeld, dient Opdrachtnemer een beschrijving te geven van de relevante procedures. In deze beschrijving dient u in ieder geval de volgende aspecten uit te werken: • Reactietijd • Oplostijd • Rollen en verantwoordelijkheden • Contactmomenten met Opdrachtgever. Vraag: Beschrijf in maximaal drie (3) pagina's A4 de relevante procedures waarmee de Beveiligingsincidenten adequaat, effectief en efficiënt door de Opdrachtnemer worden afgehandeld. De Belastingdienst verwacht van het antwoord dat: • De beantwoording volledig is conform de hierboven genoemde aspecten. • Het antwoord overtuigend, samenhangend en logisch is. Beoordeling: De beoordeling vindt plaats op basis van de hierboven beschreven verwachting en de mate waarin uw antwoord daaraan voldoet. Voor deze Wens zijn in totaal maximaal 45 punten te behalen.
-----	---

6.1.6. Business Continuity management

UE 56	De Oplossing voldoet aan onderstaande eisen betreffende de Operationele continuïteit in geval van een Calamiteit (crisis): Recovery Time Objective (RTO): • Gegevens ingevoerd tot maximaal 1 week terug Reproductie binnen 4 kantooruren per recovery • Gegevens ingevoerd in de periode tussen 1 week terug en 6 maanden terug Reproductie binnen 1 werkdag per recovery Recovery Point Objective (RPO): • Maximaal 1 seconde dataverlies per recovery.
W 3	Herstel bij Calamiteiten Opdrachtgever is gebaat bij een adequaat, effectief en efficiënt herstel bij Calamiteiten waarbij de Oplossing zo snel mogelijk weer operationeel is en er zo min mogelijk verlies van Gegevens plaatsvindt. Om inzicht te krijgen in hoeverre Opdrachtnemer in staat is de Oplossing te herstellen in geval van een Calamiteit, dient Opdrachtnemer een beschrijving te geven van de relevante procedures en maatregelen. In deze beschrijving dient u in ieder geval de volgende aspecten uit te werken: • Aanpak en snelheid van herstel • Technische maatregelen • Organisatorische maatregelen

	- Financiële impact van de maatregelen Vraag: Beschrijf in maximaal drie (3) pagina's A4 de relevante procedures en maatregelen waarmee de Oplossing in geval van een Calamiteit door de Opdrachtnemer wordt hersteld. De Belastingdienst verwacht van het antwoord dat: - De beantwoording volledig is conform de hierboven genoemde aspecten. - Het antwoord overtuigend, samenhangend en logisch is. Beoordeling: De beoordeling vindt plaats op basis van de hierboven beschreven verwachting en de mate waarin uw antwoord daaraan voldoet. Voor deze Wens zijn in totaal maximaal 45 punten te behalen.
--	--

6.1.7. Availability management

UE 57	De Oplossing heeft een Maintenance Mode (Sorry-pagina), waarmee de Gebruiker op de hoogte wordt gesteld van de onbeschikbaarheid. In geval van geplande onbeschikbaarheid wordt de Gebruiker geïnformeerd over de duur van de onbeschikbaarheid.
-------	--

6.1.8. Releasemanagement

UE 58	Wijzigingen ten aanzien van de Dienst worden door de Opdrachtnemer tijdig (minimaal 14 Kalenderdagen voor realisatie/in productie name ervan) aangekondigd.
UE 59	Opdrachtnemer spant zich in Releases op te leveren die foutvrij zijn en voldoen aan de gestelde (functionele en technische) Specificaties, zodat de kans dat Opdrachtgever nog Incidenten constateert minimaal is. Opdrachtgever wordt in de gelegenheid gesteld om een Acceptatietest te organiseren en uit te voeren voor de wijzigingen die impact kunnen hebben op koppelvlakken en gegevensuitwisseling met andere dan door de Opdrachtnemer geboden applicatie.
UE 60	Opdrachtnemer is verantwoordelijk dat Documentatie (inclusief instructiemateriaal) na een nieuwe Release actueel blijft. Na oplevering van een nieuwe Release wordt de geactualiseerde Documentatie digitaal beschikbaar gesteld.

6.2. Service niveaus

De overeengekomen Serviceniveaus zullen in een Service Level Agreement (SLA) worden vastgelegd. De Service Level Agreement (SLA) wordt door Opdrachtnemer opgesteld en aan Opdrachtgever opgeleverd met inachtneming van de in dit hoofdstuk opgenomen Serviceniveaus. De SLA maakt onderdeel uit van de Overeenkomst. De SLA bevat een beschrijving van de overeengekomen Serviceniveaus van de te leveren Diensten, de overeengekomen prestatiecriteria en de wijze waarop geacteerd wordt indien niet wordt voldaan aan de overeengekomen Serviceniveaus. Daarover wordt

door middel van een periodiek op te leveren rapportage en overleg verantwoording afgelegd aan de Opdrachtgever.

Indien door Opdrachtgever gewenst zal er aanvullend op de SLA een Dossier Afspraken en Procedures (DAP) opgesteld worden. De DAP beschrijft alle procedures en afspraken, inclusief namen en contactgegevens, die voor de Oplossing van toepassing zijn

UE 61	Na het tekenen van de Raamovereenkomst tussen Opdrachtnemer en Opdrachtgever levert Opdrachtnemer een passende Service Level Agreement (SLA) op. De SLA dient door de Opdrachtgever goedgekeurd te worden. Na vaststelling van definitieve versie zal deze door de Opdrachtnemer periodiek worden onderhouden.
UE 62	Opdrachtnemer levert maandelijks een Service level rapportage op aan de Contractmanager van Opdrachtgever, met ten minste de volgende inhoud: • Status nog openstaande incidenten • KPI overzicht Beschikbaarheid; • KPI opgeloste Incidenten; • KPI opgeloste Beveiligingsincidenten; • cumulatieve rapportage over incidenten/problem afgelopen 6 maanden • KPI Performance; • Status Additionele dienstverlening (changes). Hierbij wordt minimaal aangegeven: datum opdrachtverstrekking, startdatum, (verwachte) opleverdatum, (verwachte) acceptatiedatum, uitnutting budget; • Update ISO-certificering (of gelijkwaardige certificering).
UE 63	Operationele (werk)afspraken worden, indien door Opdrachtgever gewenst, in een DAP (Dossier Afspraken en Procedures) vastgelegd. Het DAP wordt door Opdrachtnemer opgesteld en dient door de Opdrachtgever goedgekeurd te worden. Na vaststelling van definitieve versie zal deze periodiek door de Opdrachtnemer worden onderhouden.

Hoofdstuk 7. Retransitie

Bij beëindiging van de Overeenkomst tussen Partijen is een gecontroleerd en projectmatig overgang van Opdrachtnemer naar de nieuwe opdrachtnemer gewenst om de continuïteit van de Diensten te borgen.

UE 64	De door Opdrachtnemer ten behoeve van de Belastingdienst gebruikte domeinnamen zijn eigendom van de Belastingdienst. De procedure voor de overdracht van de domeinnaam bij beëindiging van de Raamovereenkomst zal worden vastgelegd.
UE 65	Bij beëindiging van de Raamovereenkomst tussen de Belastingdienst en Opdrachtnemer is een ordentelijke overgang van Opdrachtnemer naar de nieuwe dienstverlener noodzakelijk om de continuïteit van de Diensten te borgen. Opdrachtnemer verleent haar volledige medewerking aan een zo soepel mogelijke overdracht
UE 66	Opdrachtnemer dient voldoende gekwalificeerd personeel beschikbaar te stellen voor de Retransitie.
UE 67	Opdrachtnemer geeft de volledige medewerking aan de Retransitie en overhandigt daarbij alle relevante Gegevens en Documentatie aan Opdrachtgever c.q. nieuwe dienstverlener.
UE 68	De Gegevens worden, indien door Opdrachtgever gewenst, zonder storing in de continuïteit van de Prestatie, gemigreerd naar een opvolgende applicatie.
UE 69	Op verzoek van de Opdrachtgever worden bij beëindiging van de Overeenkomst Gegevens van Opdrachtgever binnen een van te voren afgesproken aantal dagen ter beschikking gesteld, in een voor Opdrachtgever bruikbaar van te voren afgesproken digitaal formaat. Aanlevering gebeurt via een beveiligde verbinding. Opdrachtgever stelt hiervoor een beveiligde dienst beschikbaar. De ter beschikking gestelde Gegevens dienen te zijn voorzien van een zodanige functionele- en technische beschrijving dat in de toekomst een datamigratie naar een nieuwe Oplossing kan plaatsvinden zonder verdere tussenkomst van de Opdrachtnemer.
UE 70	Om bij beëindiging van de Raamovereenkomst invulling te kunnen geven aan een goede implementatie van een vervangende oplossing garandeert Opdrachtnemer het volgende: Opdrachtnemer levert gedurende minimaal drie maanden na het einde van de Raamovereenkomst op afroep Additionele Diensten in de vorm van Consultancy conform de in Bijlage vi. Prijsmodel aangegeven Prijzen.
UE 71	Opdrachtnemer zorgt er voor dat uiterlijk één (1) kalendermaand na het beëindigen van de Overeenkomst en/of na de migratie dat alle Gegevens (inclusief back-ups e.d.) van Opdrachtgever onherstelbaar zijn vernietigd. Hierbij wordt door de Opdrachtnemer aangetoond dat dit op een dusdanige wijze heeft plaatsgevonden dat de gegevens niet gereconstrueerd of anderszins hersteld kunnen worden. Voor de verwijdering dient er gebruik gemaakt te worden van een door de overheid gecertificeerd product, zie: www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducten/gevalueerde-producten
UE 72	Opdrachtnemer overhandigt een verklaring van vernietiging aan Opdrachtgever.

Hoofdstuk 8. IV kaders

8.1. Toe te passen standaarden

Van Opdrachtnemer wordt verwacht dat deze beschikt over een kwaliteitssysteem, conform onderstaande normen en standaarden, met het doel de Kwaliteit van de Diensten te borgen en fouten te voorkomen:

- ISO/IEC 12207:2008 (Systems and software engineering),
- ISO/IEC 25010:2011 (Software Product Quality),
- ISO 20000 (general requirements for service support and delivery processes),
- ISO 14764 (Maintenance processes of standard packages),
- Een test aanpak conform TMAP-next,
- ISO/IEC 24570 (Nesma globaal).

De Opdrachtgever verwacht dat Opdrachtnemer, voor zover dat de Kwaliteit van de Diensten raakt, voldoet aan de gestelde normen en standaarden. Er wordt niet verwacht dat de normen en standaarden in volle omvang worden toegevoegd of dat Opdrachtnemer daarvoor gecertificeerd is. De normen en standaarden gelden als referentie- en toets kader voor het maken van werkafspraken tussen Opdrachtgever en Opdrachtnemer. Mocht er verschil van mening zijn over de invulling van een bepaald aspect of blijken dat de geleverde Kwaliteit achterblijft bij het vereiste, dan geldt het daarover gestelde in de toepasselijke norm en/of standaard.

UE 73	Inschrijver beschikt over een kwaliteitssysteem waarmee, voor zover dat de Kwaliteit van de Diensten raakt, voldoen aan de volgende normen en standaarden: ISO/IEC 12207:2008 (Systems and software engineering), ISO/IEC 25010:2011 (Software Product Quality), ISO 20000 (general requirements for service support and delivery processes), ISO 14764 (Maintenance processes of standard packages), een test aanpak conform TMAP-next en ISO/IEC 24570 (Nesma globaal).
UE 74	Al het Personeel van Opdrachtnemer betrokken bij de uitvoering de te leveren Diensten is opgeleid in het werken met het kwaliteitssysteem en past dit toe in de uitvoering van de Diensten.

Bij de start van de Raamovereenkomst levert Opdrachtnemer een beschrijving van het kwaliteitssysteem aan bij de Opdrachtgever. In deze beschrijving wordt specifiek ingegaan op het Voortbrengingsproces en het proces van Technisch beheer en Onderhoud, waarbij de referentiekaders uit dit hoofdstuk in acht worden genomen. De Opdrachtgever zal dan een review uitvoeren op de geschiktheid van het kwaliteitssysteem en zal, indien het kwaliteitssysteem niet voldoet of naar inzicht van de Opdrachtgever onvoldoende waarborgt dat de Diensten op het juiste niveau worden geleverd, aanwijzingen geven welke aanpassingen nodig zijn om dit wel op het juiste niveau te krijgen. Dit laat onverlet dat na de Oplevering alle Specificaties van toepassing blijven.

UE 75	Opdrachtnemer levert bij de start van de Raamovereenkomst een beschrijving van het kwaliteitssysteem waarbij wordt ingegaan op zijn deel van het Voortbrengingsproces (vanaf Overdrachtmoment 1 tot en met Overdrachtmoment 2) en het proces van Technisch beheer en Onderhoud. Pas nadat er akkoord is tussen Partijen over de inhoud van het kwaliteitssysteem zal worden gestart met het Voortbrengingsproces.
UE 76	Indien relevant voert Opdrachtnemer de aanwijzingen van de Opdrachtgever door om het kwaliteitssysteem op het door de Opdrachtgever gewenste niveau te krijgen.

8.2. ISO 25010

De ISO25010 norm benoemt en beschrijft de aspecten van kwaliteit van software. Bij iedere Change zijn die aspecten een standaard onderdeel van de impact analyse die door de Opdrachtnemer dient te worden uitgevoerd, zie hiervoor ook het RFC-formulier (Bijlage E). Indien bij een Change is overeengekomen dat er geen impact aanwezig is (en dat dus niet door de Opdrachtnemer is aangegeven) en blijkt er toch een impact te zijn, dan is het herstel daarvan onderdeel van de Diensten van Opdrachtnemer.



Figuur 3. ISO 25010

UE 77	Indien de Opdrachtnemer en de Opdrachtgever door middel van het RFC-formulier, (Bijlage E) zijn overeengekomen dat een betreffende Change geen impact heeft omdat de Opdrachtnemer dat niet heeft ingevuld, maar in de praktijk blijkt er wel een impact te zijn, dan zijn de gevolgen en het herstel daarvan de verantwoordelijkheid van Opdrachtnemer.
-------	--

8.3. Wet- en regelgeving

De Belastingdienst hecht veel belang aan de beveiliging van Gegevens. De Belastingdienst heeft een taak en verantwoordelijkheid om er voor te zorgen dat Gegevens nooit in onbevoegde handen vallen of kunnen vallen.

De Opdrachtnemer dient alle passende en nodige maatregelen te hebben getroffen en te treffen om de Belastingdienst in staat te stellen deze taak uit te voeren en haar verantwoordelijkheid te kunnen nemen.

Een belangrijk kader in de te nemen beveiligingsmaatregelen is de vigerende wetgeving en standaarden ten aanzien van ICT-beveiliging en privacy.

UE 78	De Oplossing voldoet aan de algemene vigerende Nederlandse Wet- en Regelgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG).
	Partijen zullen voldoen aan hun respectievelijke verplichtingen onder de van toepassing zijnde wet- en regelgeving ter bescherming van persoonsgegevens (zoals de Algemene Verordening Gegevensbescherming) met betrekking tot alle persoonsgegevens die bij de uitvoering van deze Overeenkomst worden verwerkt.

8.4. Beveiliging

Opdrachtgever is gehouden aan de vigerende **Baseline Informatiebeveiliging Overheid** (de actuele versie van de BIO is versie 1.04z, deze is opgenomen als Bijlage G). Dit overheidsbeleid is gebaseerd op de ISO27001 en de ISO27002 en bevat daarnaast aanvullende beveiligingseisen, de zogenoemde verplichte overheidsmaatregelen.

De Gegevensportalen dienen veilig te zijn. Dit betekent dat voldaan wordt aan BBN2 (Basis Beveiligingsniveau 2) zoals gesteld in de BIO.

Daarnaast stelt Opdrachtgever zelf ook beveiligingseisen, de zogenaamde Belastingdienst specifieke eisen. De eisen worden in deze paragraaf verder toegelicht.

De Opdrachtnemer is niet direct gehouden aan de Baseline Informatiebeveiliging Overheid omdat dit stelsel geldt voor overheidspartijen, zoals de Belastingdienst. Echter, de Opdrachtnemer dient Opdrachtgever in staat te stellen om haar verantwoordelijkheid te kunnen nemen.

Naast de ISO 27001 of gelijkwaardige certificering zijn een aantal aanvullende maatregelen naast de Baseline Informatiebeveiliging Overheid (BIO versie 1.04z) ook voor de Opdrachtnemer verplicht. Het betreft:

Par.	Maatregelen
8.3.2	Verwijderen van media
	1 Media die vertrouwelijke informatie bevatten zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden.
	3 Voor het wissen van alle data op het medium, wordt de data onherstelbaar verwijderd, bijvoorbeeld door minimaal twee keer te overschrijven met vaste data en één keer met random data. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is.
9.2.1	Registratie en afmelden van gebruikers Waar in 9.2.1.x gesproken wordt over identificaties worden daaronder tevens begrepen identificaties of accounts verstrekt door eHerkenning of DigiD.
	1 Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.
	2 Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de Belastingdienst.
9.2.2	Gebruikers toegang verlenen
	1 Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.
	2 Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.
	3 Er is een actueel mandaatregister waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten dan wel functieprofielen.
9.4.1	Beperking toegang tot informatie
	1 Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.
	2 Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.
9.4.3	Systeem voor wachtwoordbeheer Voor Gebruikers en Beheerders kan soms ook gebruik worden gemaakt van gebruikersnaam, wachtwoord en sms-verificatie (two factor authentication) gebruikt als login middel. Hierbij wordt twee factor authenticatie toegepast.
	1 Naast het gebruik van two factor authentication zijn de eisen aan het wachtwoord als volgt: - Bestaat uit minimaal 8 tekens en maximaal 32 tekens. - Bevat minimaal 1 kleine letter [a-z].

Par.	Maatregelen
	3. Bevat minimaal 1 hoofdletter [A-Z]. 4. Bevat minimaal 1 cijfer [0-9]. 5. Bevat minimaal 1 bijzonder teken: [- _ ! \$ % & . = / \ : < > ? @ [] { }]. 6. Mag niet de gebruikersnaam bevatten. Het aantal inlogpogingen is maximaal 5. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.
2	Minimaal halfjaarlijks moet het wachtwoord vernieuwd worden.
3	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.
4	Initiële wachtwoorden hebben een maximale geldigheidsduur van 30 dagen, die van een wachtwoordreset 3 dagen. Bij het eerste gebruik van het uitgegeven wachtwoord moet de gebruiker direct een eigen wachtwoord opgeven.
12.4.1	Gebeurtenissen registreren
1	Een logregel bevat minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een te identificeren organisatie of gebruikersaccount; het gebruikte apparaat; het resultaat van de handeling; datum en tijdstip van de gebeurtenis.
2	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.
12.4.2	Beschermen van informatie in logbestanden
2	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald op een periode van minimaal 14 maanden. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.
4	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident.
15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
4	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaardvoorwaarden voor inkoop gehanteerd.
15.1.3	Toelevingsketen van informatie- en communicatietechnologie
1	Leveranciers moeten hun keten van toeleveranciers bekend maken en transparant zijn over de maatregelen die zij genomen hebben om de aan hun opgelegde eisen ook door te vertalen naar hun toeleveranciers.
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen
1	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.
2	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.
3	Alle medewerkers en contractanten hebben aantoonbaar kennis genomen van de meldingsprocedure van incidenten.
4	Incidenten worden zo snel als mogelijk, maar in ieder geval binnen 24 uur na bekendwording, gemeld bij het meldloket.
5	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.
6	De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.

Par.	Maatregelen
	7 Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD) procedure is onderdeel van de incidentrapportage.
16.1.7	Verzamelen van bewijsmateriaal
	1 In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.

UE 79	Opdrachtnemer neemt de benodigde maatregelen om te garanderen dat Opdrachtgever kan voldoen aan de (beveiligings)eisen zoals gespecificeerd in de BIO en bovenstaande tabel.
UE 80	Inschrijver committeert zich aan het gebruik van de Verplichte standaarden van het Forum Standaardisatie. Het betreft de volgende standaarden: • Digitoegankelijk (EN 301 549 met WCAG 2.1) • DKIM • DMARC • DNSSEC • HTTPS en HSTS • IPv4 • NEN-ISO/IEC 27001 • OpenAPI Specification • PDF (NEN-ISO) • SAML • SPF • TLS Alleen met nadrukkelijke toestemming van de Belastingdienst kan hier van worden afgeweken. In de Service Level Agreement (SLA) en eventuele DAP staat beschreven wat de procedure is als er wijzigingen zijn bij het Forum Standaardisatie gedurende de Looptijd van de Overeenkomst.

Ontwikkel-, Test-, Acceptatie- en Productieomgevingen zijn van elkaar gescheiden (het is toegestaan Ontwikkel- en Testomgevingen met elkaar te integreren.). Programmacode wordt op een gecontroleerde manier tussen de omgevingen getransporteerd. In de Productieomgeving worden geen testen uitgevoerd. Acceptatie- en beveiligingstesten worden uitgevoerd in de Acceptatie-omgeving. De Acceptatieomgeving dient daartoe, op de Gegevensset na, in alle opzichten gelijk te zijn aan de Productieomgeving. Productiegegevens worden alleen in de Productieomgeving gebruikt. Idem Persoonsgegevens.

Alleen met expliciete toestemming van de Belastingdienst (dataeigenaar) kan hiervan worden afgeweken met toepassing van goedgekeurde (aanvullende) waarborgen.

UE 81	Inschrijver maakt gebruik van gescheiden Ontwikkel-, Test-, Acceptatie- en Productieomgevingen. In de Productieomgeving wordt niet getest. Productiegegevens worden alleen gebruikt in de Productieomgeving. Het niveau van beveiliging en technische inrichting van de Acceptatieomgeving is gelijk aan die van de Productieomgeving. Alleen met expliciete toestemming van de Belastingdienst (dataeigenaar) kan hiervan worden afgeweken met toepassing van goedgekeurde (aanvullende) waarborgen.
-------	---

Het gebruik van software van andere leveranciers (open source, libraries) is toegestaan conform de licentievooraarden. Gebruik altijd de meest recente (veilige) versie vanuit een betrouwbare bron. Er mogen geen bekende Kwetsbaarheden in aanwezig zijn. Hiertoe heeft een evaluatie van de broncode plaatsgevonden (onder andere code scanning). Ook na ingebruikname vinden dergelijke evaluaties periodiek plaats.

Mochten Kwetsbaarheden toch bestaan/ontstaan dan worden deze opgelost via de leverancier van de software of conform de van toepassing zijnde Open Source-licentie. Niet weg te nemen Kwetsbaarheden worden gemeld als beveiligingsincident.

UE 82	In de Oplossing gebruikte Open Source-code en libraries van andere leveranciers bevatten geen bekende Kwetsbaarheden. Er wordt gebruik gemaakt van de meest recente veilige versies uit betrouwbare bron. Als er geen veilige versie beschikbaar is dan wordt dit gemeld als beveiligingsincident conform de bestaande afspraken.
-------	--

Webheaders zijn regels die voor een webapplicatie ingesteld kunnen worden richting de web browser. Met de juiste instellingen worden maatregelen geïmplementeerd die een webapplicatie veiliger kunnen maken. Zie hiervoor bijvoorbeeld de OWASP Foundation.

Om te bepalen of de beveiliging via webheaders afdoende is geborgd, gebruikt de Belastingdienst de dienst 'Security Headers' (<https://securityheaders.com/>). Er dient minimaal een A-score behaald te worden. Zet 'Hide results' aan.

UE 83	Oplossingen met een webinterface richting het internet maken gebruik van door de markt aanbevolen instellingen. Bij het controleren van uw Oplossing via de website 'Security Headers' wordt minimaal een A behaald.
-------	---

Aanvullend op de gestelde norm omtrent de Informatiebeveiliging (conform Beschrijvend document GE 3.) en een aantal maatregelen uit de BIO dient de Opdrachtnemer aan een aantal specifieke eisen te voldoen.

UE 84	De Belastingdienst heeft het recht om een A&P test uit te laten voeren om de beveiliging te testen. De Belastingdienst contracteert hierbij zelf een onafhankelijk en algemeen erkend bureau dat de testen uitvoert. Opdrachtnemer en de Belastingdienst besluiten gezamenlijk over de scope van de A&P test. Mochten partijen er niet gezamenlijk uit komen, dan neemt de Belastingdienst de uiteindelijke beslissing hierover. A&P tests zijn enkel toetsend en vervangen niet de beveiligingsmaatregelen van de Opdrachtnemer. De kosten van de uitvoering van deze test zijn voor rekening van de Belastingdienst. Opdrachtnemer werkt kosteloos mee aan A&P testen. Bevindingen uit A&P testen worden op kosten van Opdrachtnemer opgelost. De resultaten van de testen worden gedeeld met Opdrachtnemer. Bij het bespreken van de bevindingen worden afspraken gemaakt over de oplostijden conform UE 87 en de aansluitende hertest. De aansluitende hertest is op kosten van de Opdrachtgever.
	UE 85 De Belastingdienst heeft de bevoegdheid om toegang tot (relevante delen van) de Oplossing te (laten) blokkeren. Dit wordt het Stekkermandaat genoemd. Dit mandaat bestaat uit twee acties, die door de Opdrachtnemer, binnen 24 klokuren, geëffectueerd moeten zijn: 1. Het onbeschikbaar maken van (relevante delen van) de oplossing; 2. Het ontoegankelijk maken van de Data.

	De Opdrachtnemer biedt de mogelijkheid om de gegevens van de Belastingdienst ontoegankelijk te maken voor onbevoegden en veilig te stellen. Dit zodat de vertrouwelijkheid en integriteit van de gegevens gewaarborgd blijven. Het deblokken van (delen van) de Oplossing mag alleen na toestemming van de Belastingdienst.
--	---

De Belastingdienst wil de mogelijkheid hebben om nieuwe kwetsbaarheden te detecteren en vast te stellen dat bestaande Kwetsbaarheden zijn opgelost. Dit is aanvullend op de eisen t.a.v. de andere A&P tests.

UE 86	De Belastingdienst heeft het recht om Vulnerability scans op de Oplossing uit te laten voeren door het Security Operation Center (SOC) van de Belastingdienst. Opdrachtnemer zorgt ervoor dat het SOC de benodigde toegang heeft om deze scan uit te voeren.
	De Bevindingen worden indien nodig gedeeld en besproken met de Opdrachtnemer. Gevonden kwetsbaarheden worden opgelost door Opdrachtnemer.
	Opdrachtnemer werkt kosteloos mee aan de Vulnerability scans die door de Belastingdienst worden uitgevoerd.
	Vulnerability scans vervangen niet de beveiligingsmaatregelen van de Opdrachtnemer.
UE 87	Kwetsbaarheden worden gekwalificeerd doormiddel van het Common Vulnerability Scoring System 3.1 (CVSS 3.1 rev.1).
	Kritische bevindingen (Critical) dienen per direct te worden weggenomen door de Opdrachtnemer.
	Voor hoge risicobevindingen (High risk) geldt dat deze binnen uiterlijk een maand zijn weggenomen door de Opdrachtnemer.
	Voor kwetsbaarheden die geclassificeerd zijn als Gemiddeld en Laag worden termijnen van respectievelijk drie en zes maanden gehanteerd (Comply).
	Indien er gegronde redenen zijn om een kwetsbaarheid geclassificeerd als Gemiddeld of Laag, niet te verhelpen dient de Opdrachtnemer hiervoor een motivatie op te leveren (Explain) aan de Belastingdienst en deze motivatie voor akkoord te laten verklaren door de Belastingdienst
	Bij het constateren van kwetsbaarheden met een niveau van kritisch (critical) of hoog (high), conform CVSS 3.1, wordt de Belastingdienst daarover binnen één (1) uur door Opdrachtnemer geïnformeerd.
UE 88	De Belastingdienst heeft het recht om minimaal 1 keer per jaar een Audit uit te laten voeren om de opzet, het bestaan en de werking van een passend stelsel van beveiligingsmaatregelen ten aanzien van de Oplossing te toetsen.
	De Belastingdienst kiest hierbij zelf welk onafhankelijk en algemeen erkend bureau de Audit uitvoert. De kosten van de uitvoering van deze audit zijn voor rekening van de Belastingdienst.
	De resultaten van de Audit worden, in de vorm van een Third Party Memorandum, gedeeld met Opdrachtnemer. Bij het bespreken van de bevindingen worden afspraken gemaakt over de te nemen vervolgstappen.

De Opdrachtnemer werkt kosteloos mee aan de te nemen vervolgstappen. De kosten van een eventueel benodigde her-audit zijn voor rekening voor de Opdrachtnemer.

8.4.1. Logisch Toegangsbeheer

Het proces van het beheer van medewerker autorisaties (verstrekken, intrekken en controleren) wordt binnen de Belastingdienst Logisch Toegangsbeheer genoemd, afgekort LTB. Een meer algemeen bekende term hiervoor is Identity & Access Management (IAM). Het LTB-proces omvat het autorisatieproces, identificatieproces en het authenticatieproces.

Voor een gecontroleerd LTB-proces is het noodzakelijk dat alle ICT-voorzieningen die autorisaties bevatten, de autorisatiebronnen, aangesloten zijn of worden op het LTB-proces.

Indien de applicatie een eigen autorisatiebron heeft, dient er middels het handmatige proces aangesloten te worden op het Identity Management Systeem van de Belastingdienst (IMS). In het handmatige proces dient wekelijks autorisatie informatie (IST) uit de autorisatiebron van de applicaties aangeleverd te worden aan IMS door middel van bestandsoverdracht. Het aanmaken en aanbieden van zo'n IST-bestand dient geborgd te zijn in de Oplossing.

UE 89

Indien de Oplossing een eigen autorisatiebron heeft dient deze tevens aan te sluiten op die van de Belastingdienst ten behoeve van de accounts die voor beheerders worden uitgegeven. Opdrachtnemer dient hiertoe te voldoen aan de standaard SAML of OIDC. Het portaal sluit aan via het federatieve authenticatieprotocol (SAML of OIDC) aan op de Belastingdienst component 'Identity Bridge'. Deze zorgt ervoor dat de beheerder naar de gewenste authenticatiedienst wordt gestuurd. Indien dit niet mogelijk is, worden de accountgegevens van beheerders als volgt aangeleverd:

De onderstaande gegevens te kunnen worden aangeleverd in een bestand aan de Belastingdienst:

- UserID (Account);
- Group.

Het bestand dient consistent te zijn:

- Alle leden van een Group dienen ook als account aangeleverd te worden in hetzelfde bestand;
- Als een Account wordt aangeleverd, dat geen lid is van een Group, dan zal dit Account automatisch worden gedisabled binnen IMS;
- Group dient ook aangeleverd te worden, als deze geen lidmaatschappen heeft.

Bestand informatie:

- 1 bestand van het formaat TXT of CSV, ; (punt-komma) als scheidingsteken;
- inhoud is ruwe onbewerkte data uit de Autorisatiebron;
- Een volledig extract, geen delta ten opzichte van vorige keer;
- Frequentie 1x per week;
- Er dienen geen quotes om waarden heen te staan. Tevens mogen er geen komma's, puntkomma's en diakrieten in de attributen staan.

De Belastingdienst wil waarborgen dat alleen geautoriseerde Gebruikers gebruik kunnen maken van de Gegevens in de Oplossing. Door het gebruikersaccount te herleiden naar één en uitsluitend één natuurlijk persoon kan misbruik van een gebruikersaccount beter worden bestreden.

UE 90	Indien de Oplossing gebruik maakt van een gebruikersidentificatie (gebruikersaccount), is deze altijd één op één herleidbaar naar een Natuurlijk Persoon.
	Indien binnen de Oplossing rollen onderkend worden, bepaalt de Belastingdienst welke medewerkers welke rol binnen de Oplossing verkrijgen.
UE 91	De Oplossing beschikt over een mechanisme voor Two-Factor Authenticatie.

8.4.2. Identity Management

De Oplossing maakt gebruik van één Identity Management Systeem (IMS), waardoor Gebruikers (ongeacht hun rol en autorisaties) maar één keer hoeven te authenticeren om alle aan hun toegewezen functionaliteiten van de Oplossing te kunnen gebruiken.

UE 92	De Gebruiker hoeft zich enkel één maal aan te melden om gebruik te maken van de integrale functionaliteit van de Oplossing.
	Het beheer van toegangsrechten voor de Oplossing, inclusief de bewaking van functiescheiding, geschiedt vanuit één door de Opdrachtnemer geboden (logisch) Identity Managementsysteem (IMS).

De Belastingdienst werkt aan een Identity Bridge waarmee SSO (Single Sign-on) met derde partijen mogelijk wordt. Voorwaarde is daarbij wel, dat authenticatie op basis van SAML 2.0 gebeurt. Van de Opdrachtnemer wordt gevraagd een Oplossing te leveren die SAML 2.0 ondersteunt, zodat SSO kan worden gerealiseerd wanneer de Identity Bridge van de Belastingdienst hiervoor geschikt is gemaakt.

UE 93	Het Identity Managementsysteem (IMS) van de Oplossing ondersteunt federatieve authenticatie op basis van SAML 2.0.
	Het inloggen door gebruikers verloopt via de middelen DigiD (burgers), eHerkenning (bedrijven) of in enkele gevallen gebruikersnaam/wachtwoord (met SMS verificatie). Het moet mogelijk zijn om meer middelen toe te voegen zoals eIDAS en IDIN.

8.5. Gegevens

8.5.1. Gegevens in rust

Het Rijksbeleid kent voorschriften t.a.v. locatie waar de gegevens worden opslagen.

UE 94	Opdrachtnemer zal geen persoonsgegevens doorgeven of laten doorgeven door diens aannemers of onderaannemers naar landen buiten de EU/EER zonder de uitdrukkelijke voorafgaande schriftelijke toestemming van de Belastingdienst. Zodra er nieuwe regelgeving is op het gebied van persoonsgegevens, zullen partijen in overleg treden en de overeenkomst op dit punt aanvullen zodat deze overeenkomst niet afwijkt van de geldende regelgeving.
UE 95	Gegevens (in rust) van de Belastingdienst zijn binnen het portaal versleuteld opgeslagen.

	Voor de versleuteling wordt gebruik gemaakt van een van de door NCSC voorgeschreven algoritmes met een naar de stand van de techniek afdoende sleutellengte (met kwalificatie 'goed').
W 4	Versleuteling van Gegevens Het is voor Opdrachtgever van belang dat Gegevens veilig zijn. Opdrachtgever wenst in dat kader dat Gegevens zoveel als mogelijk versleuteld worden Geef aan in hoeverre de Oplossing in staat is om Gegevens die in de Oplossing worden verwerkt versleuteld op te slaan. In uw beschrijving dient u in ieder geval de volgende aspecten uit te werken: • Op basis van welke encryptie-algoritmes Gegevens versleuteld worden; • Hoe de versleuteling ook in de toekomst aangesloten blijft bij marktconforme encryptie-algoritmes; • Of de Oplossing eigen sleutelbeheer door de Belastingdienst ondersteunt. Vraag: Beschrijf in maximaal drie (3) pagina's A4 de mogelijkheden welke uw Oplossing biedt in het kader van versleuteling van Gegevens De Belastingdienst verwacht van het antwoord dat: • De beantwoording volledig is conform de hierboven genoemde aspecten. • Het antwoord overtuigend, samenhangend en logisch is. Beoordeling: De beoordeling vindt plaats op basis van de hierboven beschreven verwachting en de mate waarin uw antwoord daaraan voldoet. Voor deze Wens zijn in totaal maximaal 75 punten te behalen.

8.5.2. Gegevens in transitie

UE 96	Opdrachtnemer dient gebruik te maken van versleuteling voor de uitwisseling van informatie tussen de Oplossing en andere partijen. Er dient gebruik te worden gemaakt van tweeweg TLS voor versleuteling van het Kanaal. Optioneel en in overleg kan versleuteling van de inhoud (de payload worden afgesproken). De gebruikte TLS-versie is conform de aanbeveling van NIST (www.nist.gov) of de NCSC (www.ncsc.nl), doch minimaal TLS 1.2.
-------	--

8.5.3. Schonen van Gegevens

UE 97	Gegevens dienen te allen tijde op verzoek van de Belastingdienst volledig verwijderd te kunnen worden. Hierbij wordt door de Opdrachtnemer aangetoond dat dit op een dusdanige wijze heeft plaatsgevonden dat de gegevens niet gereconstrueerd of anderszins hersteld kunnen worden.
-------	---

	Voor de verwijdering dient er gebruik gemaakt te worden van een door de overheid gecertificeerd product, zie: www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducten/gevalueerde-producten .
UE 98	Alle onderdelen van de Oplossing die gegevensdragers bevatten behoren na verwijdering te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software zijn verwijderd of betrouwbaar veilig zijn overschreven (gewist). Opdrachtnemer overhandigt daarvoor een door een IT-Auditor of accountant gecertificeerde verklaring van vernietiging aan de Belastingdienst.

8.5.4. Verwerken van Gegevens

UE 99	Opdrachtnemer zal slechts persoonsgegevens verwerken voor zover noodzakelijk is voor het uitvoeren van deze Overeenkomst. Opdrachtnemer zal geen persoonsgegevens verplaatsen of doorgeven aan bedrijven of bedrijfsonderdelen, gevestigd in territoria buiten de EU/EER, of in derde landen, zonder de uitdrukkelijke voorafgaande schriftelijke goedkeuring van de Belastingdienst. In het specifieke geval dat de Belastingdienst goedkeuring geeft aan verplaatsing van persoonsgegevens buiten de EU/EER, met inachtneming van het in de vorige volzin gestelde, zal Opdrachtnemer de daaraan verbonden verplichtingen uit de Algemene Verordening Gegevensbescherming nakomen, waaronder het aangaan van EU Model Clauses met de verwerkende identiteit buiten de EU.
UE 100	Opdrachtnemer garandeert dat alle data en persoonsgegevens die in verband met de uitvoering van de Overeenkomst door Opdrachtnemer ten behoeve van de Belastingdienst zijn verwerkt, zullen worden vernietigd na beëindiging van deze Overeenkomst.

8.5.5. Beveiligen van Gegevens

UE 101	Opdrachtnemer draagt zorg voor alle redelijke technische en organisatorische maatregelen om vernietiging van of schade aan data of persoonsgegevens te voorkomen, inclusief maar niet beperkt tot de betrouwbaarheid van werknemers die toegang hebben tot deze data of persoonsgegevens. Opdrachtnemer heeft tenminste de als normaal geldende standaardsystemen en procedures ingericht om de veiligheid en vertrouwelijkheid van data en persoonsgegevens te beschermen tegen bedreigingen en gevaren van deze data en persoonsgegevens en tegen niet geautoriseerde toegang tot of gebruik van deze data en persoonsgegevens.
UE 102	Behalve wanneer de Belastingdienst uitdrukkelijk anders bepaalt of voor zover Opdrachtnemer hiertoe wettelijk verplicht is, zal Opdrachtnemer geen data en of persoonsgegevens aan enige andere partij bekendmaken, anders dan aan medewerkers en betrokken onderaannemers voor wie een dergelijke bekendmaking noodzakelijk is om de gecontracteerde dienstverlening uit te voeren, en uitsluitend in de mate waarin het nodig is voor een daartoe bevoegde partij. Indien Opdrachtnemer ten gevolge van een wettelijke verplichting data en of persoonsgegevens aan een andere partij bekend moet maken, zal Opdrachtnemer dit (indien toegestaan) van tevoren met de Belastingdienst bespreken. Opdrachtnemer zal geen persoonsgegevens gebruiken voor eigen doeleinden anders dan noodzakelijk voor de uitvoering van de Overeenkomst.

8.6. Aansluitvoorwaarden

De oplossing dient aan te sluiten op de standaard werkwijzen en techniek van de Belastingdienst.

UE 103	Bij koppeling van de Oplossing aan een systeem van de Belastingdienst wordt voldaan aan de aansluitvoorwaarden van de Belastingdienst. • Koppeling met de Belastingdienst F5 proxyserver voor het ontsluiten van de Gegevensportalen via een URL op het Belastingdienst domein met Belastingdienst certificaat. Zie Bijlage H (Aansluitvoorwaarden_WSGW_v1.3_aanvraag_DataPower) • Uitwisselen van gegevens met de Belastingdienst via de 'Belastingdienst Poort' op basis van eBMS/AS4. Bestanden van en naar het Gegevensportaal. Zie Bijlage I (Aansluitvoorwaarden B2B v2.1) • Hosting bij ODC-Noord voor de Hosting van de Gegevensportalen. Zie Bijlage J (Aansluitvoorwaarden ODC-Noord) • Uitwisselen van gegevens met de Belastingdienst via Logius: het Gegevensportaal moet kunnen aansluiten bij Logius Digipoort op basis van FTP-s. Bestanden van en naar het portaal. Zie https://logius.nl/diensten/digipoort/koppelvlakken/documentatie-koppelvlak-bestandsuitwisseling-ftp-161
UE 104	Alle relevante API's van de Oplossing ten aanzien van koppelingen en gegevensuitwisseling met andere autonome systemen van derden (indien van toepassing) zijn gedocumenteerd. Deze API-documentatie is actueel, correct en wordt op verzoek beschikbaar gesteld aan de Contractmanager van de Belastingdienst.
W 5	Koppelbaarheid en gegevensuitwisseling Het is voor Opdrachtgever van belang dat eenvoudig met de Oplossing gekoppeld kan worden. Beschrijf de mate van koppelbaarheid van de Oplossing. In uw beschrijving dient u in ieder geval de volgende aspecten uit te werken: • De aanwezigheid van de hierboven genoemde koppelvlakken; • Gebruik van marktconforme standaarden voor gegevensuitwisseling; • De beveiligingsmaatregelen die onbedoelde en/of ongeautoriseerde toegang tot de Gegevens in transport, opslag en bewerking verhinderen; • De maatregelen die het anonimiseren of Pseudonimiseren van privacygevoelige Gegevens in transport, opslag en bewerking mogelijk maken; • De aanwezigheid van een testomgeving met koppelvlakken en representatieve testgegevens, zodat de koppeling getest kan worden met andere partijen. Vraag: Beschrijf in maximaal drie (3) pagina's A4 de mogelijkheden welke uw Oplossing biedt in het kader van versleuteling van Gegevens Opdrachtgever verwacht van het antwoord dat: • De beantwoording volledig is conform de hierboven genoemde aspecten. • Het antwoord overtuigend, samenhangend en logisch is. Beoordeling:

	De beoordeling vindt plaats op basis van de hierboven beschreven verwachting en de mate waarin uw antwoord daaraan voldoet.
	Voor deze Wens zijn in totaal maximaal 60 punten te behalen.

8.7. Bewaken van de Oplossing

De Belastingdienst wil zicht krijgen op afwijkingen om herstelacties te kunnen formuleren.

UE 105	De oplossing wordt door Opdrachtnemer continu gemonitord op beveiligingsaspecten, Capaciteit, Performance en Beschikbaarheid. De wijze van monitoring en rapportage en de waardes waarbij rapportage plaatsvindt worden beschreven in de Service Levels of DAP. Afwijkingen worden gerapporteerd in de Service Level Rapportage aan de Contractmanager van de Belastingdienst.
UE 106	Alle mutaties van (persoons)Gegevens moeten dusdanig door de Oplossing geregistreerd worden, dat het mogelijk is misbruik te detecteren en analyseren. De Oplossing wordt zodanig door de Opdrachtnemer bewaakt, dat het mogelijk is tot 14 maanden in het verleden forensisch onderzoek te verrichten.

Hoofdstuk 9. Financiële afspraken

9.1. Tariefherziening

De door Opdrachtnemer geoffreerde Tarieven, zoals opgegeven in Bijlage vi (Prijsmodel) staan voor de eerste twee (2) jaar vast en mogen niet worden herzien. Na deze periode kunnen de Tarieven jaarlijks per 01 januari worden herzien. De eerste tariefherziening kan derhalve plaatsvinden op 01 januari 2025.

Om voor tariefherziening in aanmerking te komen dient Opdrachtnemer uiterlijk voor 1 december van enig jaar, een schriftelijk verzoek voor een tariefherziening in bij de verantwoordelijk contractmanager van Opdrachtgever. Dit verzoek dient voorzien te zijn van een bijbehorende onderbouwing (ten aanzien van de gestegen kosten van uitvoering) en motivering.

De door Inschrijver geoffreerde Tarieven mogen (nadat de periode dat de Tarieven vast staan) jaarlijks steeds per 1 januari geïndexeerd worden. De maximale tariefherziening is vastgesteld op basis van de CBS index-tabel Dienstenprijzen (DPI); commerciële dienstverlening en transport; indexcijfers 2015 = 100 (CPA2008, kwartaalindex) conform de volgende webpagina: <https://opendata.cbs.nl/#/CBS/nl/dataset/83760NED/table?dl=25692>. Het percentage voor de tariefherziening wordt afgerond op één decimaal achter de komma. Inhaalslagen op niet doorgevoerde indexeringen worden niet geaccepteerd.

UE 107	De opgegeven Tarieven staan vast voor de eerste twee (2) jaar dat de Oplossing operationeel is. De Tarieven kunnen daarna jaarlijks per 01 januari worden herzien. De eerste tariefherziening kan derhalve plaatsvinden op 01 januari 2025.
UE 108	De maximale tariefherzieningen zijn begrensd door het indexcijfer 'Dienstenprijzen (DPI); commerciële dienstverlening en transport; indexcijfers 2015 = 100', (CPA2008, kwartaalindex) conform de volgende webpagina: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83760NED/table?ts=1594803086253 , zoals gepubliceerd door het CBS. Opdrachtnemer dient uiterlijk, per 1 december van enig jaar, een schriftelijk verzoek in bij de verantwoordelijk contractmanager van de Opdrachtgever, met bijbehorende onderbouwing en motivering om voor tariefherziening in aanmerking te komen.
UE 109	Het is niet toegestaan om eventueel in een voorgaand jaar niet in rekening gebrachte tariefherzieningen later alsnog toe te passen.

9.2. Facturatievoorwaarden

UE 110	Kosten die niet in de Inschrijving opgenomen zijn en niet verdisconteerd zijn in de prijsstelling, maar toch noodzakelijk blijken te zijn voor een goed functioneren van de Gegevensstromen of de Dienstverlening, conform de in het Beschrijvend Document (incl. Bijlagen) gestelde eisen, zijn voor rekening van Opdrachtgever.
UE 111	Facturatie van de kosten van Realisatie en Changes wordt gedaan na de Acceptatie op basis van het Inkooporder/bestelnummer die bij de formele acceptatie van de Offerte is gedeeld.
UE 112	Facturatie van het Technisch beheer & Onderhoud worden vooraf per kwartaal (1 januari, 1 april, 1 juli, 1 oktober) gefactureerd onder vermelding van de relevante Inkooporders/bestelnummers.
UE 113	Facturatie van de Variabele diensten (authenticatiemiddelen) worden achteraf per kwartaal (1 januari, 1 april, 1 juli, 1 oktober) op basis van werkelijke kosten (tegen kostprijs) gefactureerd onder vermelding van de relevante Inkooporders/bestelnummers.

UE 114	Additionele diensten worden achteraf na afronding en Acceptatie van de desbetreffende werkzaamheden in rekening gebracht.
UE 115	De uurtarieven ten behoeve van de inzet van consultants zijn all-in Tarieven. Er kunnen derhalve geen aanvullende kosten in rekening worden gebracht (bij on-site inzet zijn, reistijd, reis- en verblijfkosten in het uurtarief opgenomen). Reistijd kan nooit worden doorberekend, tenzij Partijen daar in uitzonderlijke gevallen voorafgaand schriftelijke afspraken over maken. Als er werk wordt uitgevoerd buiten kantooruren waarvoor bij Opdrachtnemer normaal gesproken een toeslag geldt dan is voorafgaande schriftelijke toestemming nodig van Opdrachtgever alvorens deze kunnen worden gefactureerd. Uitgangspunt is dat Opdrachtnemer zelf verantwoordelijk is wanneer werkzaamheden worden uitgevoerd zodat daar geen toeslag voor hoeft te worden berekend.
UE 116	Er wordt een betalingstermijn van 30 dagen na ontvangst van de factuur gehanteerd.

9.3. Elektronisch factureren (EBF) – e-factureren

Een e-factuur is een gestructureerd digitaal bestand (geen Pdf) waarbij de vereiste gegevens altijd op een vaste plek met specifieke codering in het bestand staan. Een e-factuur kan vanuit het ene geautomatiseerde systeem elektronisch worden aangemaakt en automatisch worden verwerkt in het andere systeem.

Voor het verzenden worden de volgende mogelijkheden geboden:

1. factuurportaal van de Rijksoverheid;
2. directe koppeling met DigiPoort;
3. e-factuur indienen vanuit uw (boekhoud)softwarepakket via Peppol;
4. e-factureren via een dienstverlener die een directe koppeling heeft met DigiPoort.

NB: Om elektronisch te kunnen factureren zijn ten minste de volgende gegevens nodig:

- naam en adres van de Opdrachtnemer;
- het KvK-nummer van de Opdrachtnemer;
- het btw-nummer van de Opdrachtnemer;
- de IBAN-code (en indien van toepassing de BIC) van de Opdrachtnemer;
- het Overheidsidentificatienummer (OIN) van de Rijksdienst waaraan de factuur wordt gestuurd. De lijst met OIN's wordt bijgehouden door Logius, zie www.logius.nl voor het actuele overzicht;
- het afleveradres (het adres waar de goederen of diensten zijn geleverd);
- het bestelnummer (bestaat uit totaal 10 cijfers (41xxxxxxx of 45xxxxxxx));
- contactpersoon (de persoon die de bestelling heeft geplaatst);
- artikelcode (indien van toepassing);
- de omschrijving van de bestelde/geleverde goederen of diensten;
- de bestelde/geleverde hoeveelheid;
- de prijs per eenheid.

UE 117	Opdrachtnemer verzendt de factuur elektronisch zodat deze met inachtneming van de door de Opdrachtgever gegeven Specificaties elektronisch kan worden ontvangen en verwerkt.
--------	--

Aansluiten op het factuurportaal van de Rijksoverheid kan de Opdrachtnemer regelen door middel van zelfregistratie via internet.

Aansluiting op DigiPoort voor geautomatiseerde uitwisseling van berichten wordt verzorgd door Logius, de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Voor aansluiting op DigiPoort neemt de Opdrachtnemer na gunning contact met hen op via telefoon 0900 - 555 4555, per e-mail servicecentrum@logius.nl of op www.logius.nl. Op het aansluiten op DigiPoort zijn

de algemene gebruiksvoorwaarden Digipoort en de algemene voorwaarden van Logius van toepassing. Deze voorwaarden treft u eveneens aan op voornoemde website. Het uitbrengen van een Inschrijving impliceert dat voornoemde voorwaarden door de Opdrachtnemer worden geaccepteerd.

Bij keuze voor Peppol of voor het inschakelen van een dienstverlener neemt de Inschrijver na gunning zelf contact op met de partij naar keuze.

Nadere informatie over e-factureren kunt u vinden in de brochure '[elektronisch factureren voor leveranciers](#)'. Meer informatie is ook verkrijgbaar bij de Rijks-brede helpdesk e-factureren, via www.helpdesk-efactureren.nl.

UE 118	Opdrachtnemer start direct na de gunning het aansluitproces op e-factureren via één van de door de Opdrachtgever voorgeschreven manieren voor e-factureren en informeert de Opdrachtgever over de door Opdrachtnemer gekozen wijze van aansluiten op e-factureren.
UE 119	De Opdrachtgever berekent geen kosten aan Opdrachtnemer voor aansluiting op en communicatie met DigiPoort. Bij een directe aansluiting op DigiPoort komen alle kosten vanaf het koppelvlak aan opdrachtnemerszijde voor rekening van de Opdrachtnemer. De kosten die Opdrachtnemer in dit verband nu (en in de toekomst) maakt, zijn voor eigen rekening.