



Belastingdienst

BIJLAGE A – Specificatie van de opdracht

Behorende bij : Aanbesteding Uitwijk Print & mail

Versie : 1.0
Kenmerk : IUC21-008
Datum : 23-7-2021

Template versie: 4.3

INHOUDSOPGAVE

Hoofdstuk 1. Doel van dit document	3
1.1. <i>Eisen en wensen</i>	3
Hoofdstuk 2. Algemene Uitvoeringseisen	4
2.1. <i>Verplichtingen belastingen, milieubescherming, arbeidsvoorwaarden</i>	4
2.2. <i>Verzekering.....</i>	4
2.3. <i>Business Etiquette.....</i>	4
2.4. <i>Integriteit.....</i>	4
Hoofdstuk 3. Beleid gerelateerde eisen en wensen.....	5
3.1. <i>Maatschappelijk Verantwoord Inkopen</i>	5
3.2. <i>Milieu</i>	5
Hoofdstuk 4. Juridische kaders	6
Hoofdstuk 5. Financiële afspraken	7
5.1. <i>Prijsstelling.....</i>	7
5.2. <i>Indexering prijs</i>	7
5.3. <i>Elektronisch factureren (EBF) – e-factureren.....</i>	8
Hoofdstuk 6. Kwaliteit	9
6.1. <i>Locatie</i>	9
6.1.1. <i>Normen en standaards</i>	9
6.2. <i>Productie kaders.....</i>	10
6.3. <i>Personele kaders.....</i>	10
6.4. <i>Productie proces.....</i>	10
6.5. <i>Implementatie</i>	11
6.6. <i>Calamiteitenplan</i>	13
6.7. <i>Documentatie.....</i>	14
Hoofdstuk 7. Technische omgeving	15
7.1. <i>Beveiligingskaders (BIO)</i>	15

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 IUC21-008 Uitwijk Print & mail. Dit document maakt integraal onderdeel uit van het Beschrijvend Document.

1.1. Eisen en wensen

Voor het indienen van de inschrijving zal onderhavige bijlage van het beschrijvend document integraal als word document ter beschikking worden gesteld zodat Inschrijvers op eenvoudige wijze de tabellen kunnen invullen waarin de eisen en wensen zijn opgenomen.

De Aanbestedende dienst heeft geen voorkeur voor bepaalde Inschrijvers, noch voor bepaalde merken, types, fabricaten, herkomst e.d. Als er wordt gerefereerd aan bepaalde fabricaten, merken, typen, specifieke standaarden en dergelijke, dan dient dit te worden gelezen met de toevoeging “of daaraan gelijkwaardig”.

Aan eisen moet worden voldaan. Het niet voldoen aan een eis betekent uitsluiting van verdere beoordeling en wordt de inschrijving terzijde gelegd (knock-out criterium).

De wensen worden inhoudelijk beoordeeld door een beoordelingscommissie.

Inschrijvers dienen te voldoen aan alle opgenomen eisen en wensen die de Aanbestedende dienst heeft geformuleerd ten aanzien van de te leveren prestatie. Eisen en wensen worden als volgt weergegeven:

EIS 1	Gunningseisen zijn eisen waar u reeds ten tijde van de Inschrijving aan moet voldoen. Het niet voldoen aan een Gunningseis leidt tot uitsluiting van de aanbestedingsprocedure en is dus een knock-out criterium.
W 1	Wensen Wensen maken onderdeel uit van gunningscriteria. De scores op de Wensen bepalen de hoogte van het onderdeel Kwaliteit in de prijs/kwaliteit verhouding per Inschrijving
UE 1.	Uitvoeringseisen Uitvoeringseisen zijn eisen waar de Opdrachtnemer zich bij de uitvoering van de opdracht aan dient te houden. Door het indienen van een Inschrijving gaat u onvoorwaardelijk akkoord met het voldoen aan de Uitvoeringseisen gedurende de uitvoering van de Overeenkomst.

Hoofdstuk 2. Algemene Uitvoeringseisen

In dit hoofdstuk zijn specifieke uitvoeringseisen opgenomen. De bepalingen in dit hoofdstuk hebben allemaal specifiek betrekking op de uitvoeringsperiode van de aanbestedde opdracht, echter ook in andere hoofdstukken, waaronder Hoofdstuk 6 “Kwaliteit”, komen uitvoeringseisen voor.

2.1. Verplichtingen belastingen, milieubescherming, arbeidsvoorwaarden

- | | |
|-------|--|
| UE 1. | <p>Inschrijvers dienen bij het opstellen van hun Inschrijving rekening te hebben gehouden 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"> • 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. | <p>Gezien de aard van de werkzaamheden acht de Aanbestedende dienst 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 dekking van € 1.250.000 of equivalente tegenwaarde, gedurende tenminste de looptijd van de opdracht. Op daartoe strekkend verzoek verstrekt de winnende Inschrijver bewijs van adequate verzekering dan wel een verklaring waaruit blijkt dat deze hiertoe bereid en in staat is de bij gunning af te sluiten.</p> |
|-------|---|

2.3. Business Etiquette

- | | |
|-------|--|
| UE 3. | <p>Inschrijver conformeert zich aan de business etiquette zoals opgenomen in Bijlage 13.</p> |
|-------|--|

2.4. Integriteit

- | | |
|-------|---|
| UE 4. | <p>Inschrijver handelt conform de integriteitsregels als zijn opgenomen in Bijlage 7.</p> |
|-------|---|

Hoofdstuk 3. Beleid gerelateerde eisen en wensen

3.1. Maatschappelijk Verantwoord Inkopen

Het Inkoopuitvoeringscentrum (IUC) van de Belastingdienst heeft ambitie op het gebied van duurzaamheid. Zij wil klanten, behoeftestellers 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 Inkopen (MVI) 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 transitie, inschakelen van kwetsbare groepen en om innovatief in te kopen.

3.2. Milieu

EIS 1	Voor digitaal printwerk geldt dat de toegepaste inkt, toners, lijm, reinigingsmiddelen of andere chemicaliën bij het vervaardigen van het in het kader van deze aanbesteding te leveren printwerk niet mogen bevatten: alkylfenolethoxylaten (APEO); halogenen, met uitzondering van biocides met halogenen, met één of meerdere van de H-zinnen: H300 H301 H304 H310 H311 H330 H331 H340 H341 H350 H350i H351 H360F H360FD H360Fd H360Df H361f H361d H361fd H362 H370 H371 H372 H373 H400 H410 H411 H412 H413 EUH059 EUH029 EUH031 EUH032 EUH070; ftalaten met de H-zinnen: H360F, H360D, H361f; biocides, inclusief biocides met halogenen, met een log Pow (octanol/waterverdelingscoëfficiënt) $\geq 3,0$ of een experimenteel bepaalde bioconcentratiefactor (BCF) > 100 .
EIS 2	Voor digitaal printwerk geldt dat voor de vervaardiging van het in het kader van deze aanbesteding te leveren printwerk geen inkt, verf, verfstoffen, vernis, toevoegingen, reinigingsmiddelen of oplosmiddelen mogen worden gebruikt die geclassificeerd zijn met één of meerdere van de H-zinnen: H300 H301 H310 H311 H330 H331 H340 H341 H350 H350i H351 H360F H360FD H360Fd H360Df H361f H361d H361fd H362 H370 H371 H372 H373 H400 H410 H411 H412 H413 EUH059 EUH029 EUH031 EUH032 EUH070. Als uitzondering op deze eis geldt dat UV-inkten en UV-vernissen geclassificeerd mogen zijn met H412.

Hoofdstuk 4. Juridische kaders

De in bijlage 2 van het Beschrijvend Document opgenomen Overeenkomst kan - alvorens deze door Inschrijver(s) wordt ondertekend - door de Aanbestedende dienst worden gewijzigd en nader uitgewerkt, mede naar aanleiding van de door de Inschrijver gedane opmerkingen en tekstsuggesties als bedoeld in paragraaf 3.3. (nadere inlichtingen of vragen over de aanbestedingsstukken) De wijzigingen en/of de aangepaste Overeenkomst zullen/zal de Inschrijvers per nota van inlichtingen kenbaar worden gemaakt.

UE 5.	Inschrijver gaat akkoord met de eisen en verplichtingen zoals vastgelegd in de Aanbestedingsstukken, met inbegrip van Bijlage 2 Overeenkomst. Voor zover per Nota van Inlichtingen wijzigingen doorgevoerd worden aan de Aanbestedingsstukken, zullen deze integraal onderdeel uitmaken van het bestek en gaat Inschrijver eveneens akkoord met deze wijzigingen.
-------	---

UE 6.	Bij een situatie zoals bedoeld in Artikel 9 van de Overeenkomst worden Persoonsgegevens verwerkt. Teneinde de verplichtingen uit Artikel 21 te kunnen waarborgen, zullen Partijen een verwerkersovereenkomst conform Bijlage 15 overeenkomen binnen 20 werkdagen na ondertekening van de Overeenkomst sluiten.
-------	--

UE 7.	Inschrijver gaat akkoord met de volledige inhoud en alle voorwaarden uit Bijlage 3 – Wachtkamerovereenkomst, met inbegrip van de eventuele per Nota van inlichtingen kenbaar gemaakte wijzigingen.
-------	--

UE 8.	Inschrijver gaat akkoord met de SLA zoals opgenomen in Bijlage 4 van deze aanbesteding.
-------	---

Hoofdstuk 5. Financiële afspraken

5.1. Prijsstelling

De volgende Prijzen worden onderscheiden:

- a. Prijs Implementatie (eenmalig)
- b. Prijs Standby per jaar
- c. Prijs per test
- d. Prijs Consultancy per uur

En indien daadwerkelijk gebruik wordt gemaakt van de Uitwijk, gelden de volgende Tarieven:

- e. Tarief per A4 tijdens calamiteit
- f. Tarief personeel per uur tijdens calamiteit

EIS 3	In de in Bijlage 10 “Prijzmodel” en “Bijlage 11 Bonus-Malus voor wens 3 & 4” geoffreerde Prijzen dienen alle kosten voor de Prestatie verdisconteerd te zijn. Hierbij kan (en niet limitatief) worden gedacht aan: • (periodieke) rapportages, • (periodiek) overleg, • inspecties, • evaluaties, • toekomstverkenningen, • deelname aan begeleidings- en stuurgroepen, • reis- en verblijfkosten • het verstrekken van de benodigde toegangscode voor gebruik van de Oplossing, • Materialen en Documentatie vereist voor het gebruik van de Oplossing.
-------	---

UE 9.	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 Oplossing 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.
-------	--

EIS 4	De facturering dient voor de Standby fee jaarlijks voorafgaande aan de nieuwe periode plaats te vinden. Voor facturering van test en daadwerkelijke uitwijk, geldt facturatie per maand na levering van de dienstverlening.
-------	--

5.2. Indexering prijs

De door Inschrijver geoffreerde Prijzen : de ‘Standby fee’ en ‘Tarief testen’ en ‘Tarief Consultancy’, zoals opgegeven in het spreadsheet Prijzenformulier, Bijlage 10 end e Tarieven in Bijlage 11, mogen vanaf 2022 jaarlijks en steeds per 1 november geïndexeerd worden op basis van de CBS-tabel Dienstenprijzen (DPI); commerciële dienstverlening en transport; indexcijfers 2015 = 100 (CPA2008, kwartaalindex).

<https://opendata.cbs.nl/#/CBS/nl/dataset/83760NED/table?dl=55206>

Prijsaanpassingen dienen uiterlijk voor 1 september van enig jaar aan de contractmanager ter goedkeuring te worden aangeboden, waarbij het op dat moment – door het CBS - beschikbare en gepresenteerde indexcijfer, Jaarmutatatie 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 1-1-2021 geïndexeerd had mogen worden, was de prijsindexatie 1,3% geweest (jaarmutatatie DPI 3e kwartaal 2020, op dat moment laatst beschikbaar indexcijfer).

EIS 5	Inschrijver is akkoord met de indexering voor jaarlijkse standby fee en additionele Prijzen conform de geoffreerde Prijzen in Bijlage 10 – Prijzenformulier en Bijlage 11, en dient voor 1 september, voorafgaande aan de genoemde momenten van tarief indexering, een schriftelijk verzoek in met bijbehorende onderbouwing om voor de indexering in aanmerking te komen.
-------	--

5.3. 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 Inschrijver
- het KvK-nummer van de Inschrijver
- het btw-nummer van de Inschrijver
- het bankrekeningnummer (en indien van toepassing de BIC- en IBAN-code) van de Inschrijver
- 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

EIS 6	Inschrijver verzendt de factuur elektronisch zodat deze met inachtneming van de door de Aanbestedende dienst gegeven specificaties elektronisch kan worden ontvangen en verwerkt.
-------	---

EIS 7	Inschrijver start direct na de gunning het aansluitproces op e-factureren via één van de door de Aanbestedende dienstvoorgeschreven manieren voor e-factureren en informeert de Opdrachtgever over de door Inschrijver gekozen wijze van aansluiten op e-factureren.
-------	--

EIS 8	De Rijksoverheid berekent geen kosten aan opdrachtnemers voor aansluiting op en communicatie met DigiPoort. Bij een directe aansluiting op de Digipoort komen alle kosten vanaf het koppelvlak aan opdrachtnemerszijde voor rekening van de Inschrijver. De kosten die Inschrijver in dit verband nu (en in de toekomst) maakt, zijn voor eigen rekening.
-------	---

Aansluiten op het factuurportaal van de Rijksoverheid kan de Inschrijver 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 Inschrijver 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 (offerte) impliceert dat voornoemde voorwaarden door de Inschrijver 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 via : helpdesk-efactureren.nl

Hoofdstuk 6. Kwaliteit

6.1. Locatie

De uitwijk locatie die middels deze aanbesteding dient binnen de Nederlandse landsgrenzen te staan. Dit vanwege het feit dat vanuit beveiliging de benodigde productgegevens niet buiten de landgrenzen mogen komen. Daarnaast zijn er praktische belemmeringen indien er tijdens een Calamiteit voor zorgen dat een locatie buiten de Nederlandse landsgrenzen zorgt voor belemmeringen in de continuïteit. Dit vanwege contractuele afspraken met andere partijen in de productieketen zoals het post bedrijf en leveranciers van papier en enveloppen.

EIS 9	De Uitwijklocatie dient binnen de Nederlandse landsgrenzen (in Europa) te staan, alwaar de Print & mail productie kan plaatsvinden.
-------	---

EIS 10	Productiebestanden mogen de landsgrenzen fysiek en digitaal niet verlaten.
--------	--

UE 10.	Dataverbinding is op basis van koppeling via Internet beveiligd door gebruik van IPSec of inzet van SFTP.
--------	---

UE 11.	De dataverbinding is beschikbaar in een productie-omgeving en tevens in een acceptatie/test-omgeving.
--------	---

6.1.1. Normen en standaards

EIS 11	Opdrachtgever en Opdrachtnemer voeren Periodieke testen (tenminste twee maal per jaar) uit om na te gaan of de Uitwijklocatie voldoet aan de gestelde eisen zoals beschreven in de Specificatie van de opdracht
--------	---

UE 12.	De Inschrijver kan de op de Uitwijklocatie in het geval van een Calamiteit op locatie Quintax: • Binnen 48 uur na melding bij Opdrachtnemer, 7% van het totale Postaanbod verwerken; • Na maximaal één week na melding bij Opdrachtnemer 50% van het totale Postaanbod verwerken; • Na maximaal twee weken na melding bij opdrachtnemer 100% van het totale Postaanbod verwerken; Indien een Calamiteit zich voordoet, dient Opdrachtnemer de werken conform de bovenstaande tijdslijnen.
--------	---

UE 13.	Inschrijver biedt de mogelijkheid om tijdens reguliere productie tijden (07:00 – 24:00 uur) de Uitwijk te laten plaatsvinden.
--------	---

UE 14.	De Inschrijver is in staat om de Capaciteit zoals bescheven in het Beschrijvend document te kunnen verwerken.
--------	---

6.2. Productie kaders

UE 15.	Voor de Productie tijdens een Calamiteit, dient gebruik gemaakt te worden van Canon Red Label 90 grams , rol 450 mm * 1380 mm Papier.
UE 16.	Opdrachtgever levert zelf Papier zoals opgenomen in UE13 en enveloppen (diverse formaten) ten behoeve van de Productie op de Uitwijk locatie.
UE 17.	In het geval van Productie op de Uitwijk locatie, dient Post van de Belastingdienst op het Post-NL klantnummer van de Belastingdienst te worden aangeboden ter verzending.
UE 18.	Opdrachtnemer werkt mee aan de realisatie van een netwerkverbinding tussen Belastingdienst en Opdrachtnemer met 99.99% beschikbaarheid.

6.3. Personele kaders

UE 19.	De inschrijver is akkoord met het inzetten van personeel van Opdrachtgever op de Uitwijk locatie in het geval van een Calamiteit.
UE 20.	Op verzoek kan Opdrachtnemer Personeel leveren voor de uitvoering van de Productie op de Uitwijk locatie.
UE 21.	In te zetten Personeel heeft ten alle tijden een geldige VOG (verstrekt voor de uitvoering van de activiteiten bij regulier productieproces (bij Opdrachtnemer)) en dient een geheimhoudingsverklaring zoals opgenomen in de Overeenkomst te ondertekenen.
UE 22.	Op verzoek kan Opdrachtnemer Consultancy leveren als Additionele dienst. Consultancy is enkel van toepassing als werkzaamheden of adviezen buiten de Implementatie, Periodieke testen of andere reeds gecontracteerde onderdeel

6.4. Productie proces

De voorkeur gaat uit naar een partij die op dezelfde manier kan werken als de Belastingdienst. Dit is om, in geval van Calamiteit, de Productie op de Uitwijklocatie te starten zonder dat er aanpassingen hoeven te worden gemaakt in de formulieren (opmaak, kleur etc.) en printmethode (printvolgorde A-Z/Z-A, foot-first/head-first, face-up/face-down etc.). Er wordt volledig gebruik gemaakt van blanco papier. Voor een beschrijving van de massaal print omgeving van de belastingdienst wordt verwezen naar Bijlage 17.

EIS 12	De Print-faciliteiten maken gebruik van blanco rollen papier (white paper factory).
EIS 13	De Print-faciliteiten moeten voorzien in Full-Color CMYK printing en bieden ondersteuning voor gebruik van "spotkleuren".
EIS 14	Inschrijver kan omgaan met colormanagement en het gebruik van spotkleuren,
EIS 15	De Print-faciliteiten ondersteunen diverse vormen van printerconfiguraties (2-up/A4-dynamisch, foot-first/head-first, face-up/face-down).
EIS 16	Aanlevering van print-data is in AFP formaat, Inschrijver kan deze printdata verwerken.

6.5. Implementatie

De Opdrachtnemer dient de leiding te nemen bij de Implementatie van de uitwijk voorziening Print & mail. Om inzicht te krijgen op welke wijze de Opdrachtnemer de Implementatie uit gaat voeren, dient de Opdrachtnemer een Implementatie plan voor de in deze Aanbesteding beschreven Uitwijk op te leveren.

EIS 17	Inschrijver levert bij Inschrijving een (concept) Implementatieplan op, uitgaande van gebruiksklare Oplevering van de uitwijk voorziening Print en mail op 1 maart 2022.
--------	--

UE 23.	Het door Opdrachtnemer definitief opgeleverde Implementatieplan dient eerst door Opdrachtgever zoals omschreven in de Overeenkomst te zijn goedgekeurd. Pas na schriftelijke goedkeuring kan worden aangevangen met de Implementatie.
--------	---

UE 24.	De Uitwijklocatie wordt tijdens de Implementatie onderworpen aan diverse testen ten behoeve van de Acceptatie, zoals technische en functionele acceptatietesten, maar ook testen met betrekking tot de performance en beveiliging (bijvoorbeeld een Attack and Penetration (A&P) test).
--------	---

UE 25.	Implementatie dient door Opdrachtnemer uiterlijk 30 april 2022 te zijn afgerond.
--------	--

W 1

(concept) Implementatieplan

Om inzicht te krijgen in de wijze waarop de Opdrachtnemer de Implementatie uit gaat voeren, dient Opdrachtnemer een Concept Implementatieplan in te dienen. De projectmanagement methode van de Belastingdienst is Prince 2. Daarnaast zal er vanuit de Belastingdienst een projectleider vanuit de interne organisatie worden aangesteld ten behoeve van het begeleiden van het implementatietraject aan de kant van de Belastingdienst.

In dit (concept) Implementatieplan dient u in ieder geval de volgende aspecten uit te werken:

- De veronderstelde uitgangspunten voor implementatiefase
- Projectmanagementmethode en projectaanpak;
- Projectorganisatie en governance incl. escalatieprocedure en interactie met Belastingdienst (welke verantwoordelijken worden wanneer betrokken en geïnformeerd); (Opdrachtgever levert een projectleider vanuit de interne organisatie)
- Borging van (Productie) inhoudelijke kennis;
- Planning, met mijlpalen, binnen de gestelde tijdslijnen in deze Specificatie van de opdracht.
- Voortgangsrappportage;
- Beschrijving van de (5 belangrijkste) risico's en beheersmaatregelen om de start van de Operationele fase te borgen;
- Beveiliging van gegevens, technische & fysiek;
- Test- en Acceptatieproces;
 - Opdrachtgever wil in ieder geval kunnen vaststellen of de Prestatie voldoet aan de gevraagde functionaliteit, koppelvlakken, Beveiliging en overige non-functional eisen;
 - De door Opdrachtnemer vastgestelde en voor Opdrachtgever benodigde acceptatiecriteria (deze moeten Opdrachtgever overtuigen dat de Prestatie voldoet).

Voorschriften uitwerking

Wij vragen uw uitwerking in maximaal 6 pagina's A4 (lettertype Arial, lettergrootte 10 en regelafstand 1,0) te verwoorden. Extra pagina's worden niet in de beoordeling meegenomen.

Beoordelingsmethode

Het (concept) Implementatieplan wordt beoordeeld op onderstaande aspecten:

- De mate waarin de beantwoording volledig is en ingaat op alle hierboven genoemde aspecten;
- De mate waarin de verantwoordelijkheden van partijen op heldere wijze terugkomen in het (concept) Implementatieplan;
- De mate waarin het beschreven (concept) Implementatieplan vertrouwen geeft dat de realisatie soepel verloopt, dat Uitwijklocatie zal voldoen aan alle specificaties en dat de testen in het kader van de acceptatie met succes worden doorlopen;
- De voorgestelde planning concreet, haalbaar en S.M.A.R.T. geformuleerd is;
- Of de aangegeven risico's in relatie staan tot de Prestatie;
- Hoe de voorgestelde mitigerende maatregelen de risico's afdekken;
- De mate waarin en wijze waarop wordt beschreven op welke wijze de Aanbestedende dienst door Opdrachtnemer ontzorgt wordt;
- De mate waarin het antwoord inhoudelijk overtuigend en relevant is.

Voor het scoreverloop wordt verwezen naar paragraaf 4.2 in het Beschrijvend Document

6.6. Calamiteitenplan

Opdrachtgever verwacht een (Concept) Calamiteitenplan bij Inschrijving. Tijdens de Implementatie zullen opdrachtgever en Opdrachtnemer gezamenlijk tot een definitief Calamiteitenplan komen, wat als draaiboek wordt gebruikt in het geval van een Calamiteit.

EIS 18	Opdrachtnemer dient bij de Inschrijving een (concept) Calamiteitenplan in, waarin beknopt uiteen wordt gezet hoe in het geval van een Calamiteit, de Uitwijklocatie kan worden ingezet.
W 2	(Concept) Calamiteitenplan Om inzicht te krijgen in de wijze waarop de Opdrachtnemer in het geval van een Calamiteit gaat handelen, dient Opdrachtnemer een Calamiteitenplan in te dienen bij de Inschrijving. In dit (concept) Calamiteitenplan dient u in ieder geval de volgende aspecten uit te werken: • Voorstel activiteiten tot eerste Productie • Planning • Governance incl. escalatieprocedure en interactie met Belastingdienst; • Beschrijving van de (5 belangrijkste) risico's en bijbehorende beheersmaatregelen om de mogelijke uitnutting van de Uitwijk te waarborgen; • Inzet personeel van de Belastingdienst (Hoe verloopt het proces van inzet van personeel vanaf opstart Uitwijk); • Afbouw en afronding en evaluatie van de Calamiteit en het gebruik van de Uitwijklocatie. (data, en productiemiddelen (enveloppen papier etc) Voorschriften uitwerking Wij vragen uw uitwerking in maximaal 5 pagina's A4 (lettertype Arial, lettergrootte 10 en regelafstand 1,0) te verwoorden. Extra pagina's worden niet in de beoordeling meegenomen. Beoordelingsmethode Het (concept) Calamiteitenplan wordt beoordeeld op onderstaande aspecten: • De mate waarin de beantwoording volledig is en ingaat op alle hierboven genoemde aspecten; • De voorgestelde planning concreet, haalbaar en S.M.A.R.T. geformuleerd is; • De mate waarin de verantwoordelijkheden van partijen op heldere wijze terugkomen in het Calamiteitenplan; • Of de aangegeven risico's in relatie staan tot de Prestatie; • Hoe de voorgestelde mitigerende maatregelen de risico's afdekken; • De mate waarin het (concept) Calamiteitenplan vertrouwen geeft dat de overgang naar de Uitwijklocatie soepel verloopt, dat de Uitwijklocatie zal voldoen aan alle specificaties; • De mate waarin het antwoord inhoudelijk overtuigend en relevant is. Voor het scoreverloop wordt verwezen naar paragraaf 4.2 in het Beschrijvend document

Opdrachtgever wenst vooraf inzage in de Tarieven per A4 die betaald dient te worden tijdens het gebruik van de Uitwijk. De Tarieven zoals opgegevens bij Wens 3, zijn de Tarieven die gelden bij een Calamiteit. zie hiervoor ook hoofdstuk 5 van deze Specificatie van de opdracht.

W 3	Tarief A4 Indien Opdrachtgever besluit het Calamiteitenplan in werking te stellen en de Uitwijklocatie in te zetten, wordt afgerekend op basis van een Tarief per A4. Ook voor dit Tarief geldt dat kosten die niet in de inschrijving genoemd worden en niet verdisconteerd zijn in de prijsstelling, maar toch noodzakelijk blijken te zijn voor een goed functioneren van het product of de dienstverlening, conform de in de Aanbestedingsstukken gestelde eisen, voor rekening van Inschrijver zijn. Denk bij het opgeven van uw Tarief dus in elk geval aan de volgende componenten: Operationele kosten (Inkt, slijtage, onderhoud, energie), locatiekosten (toegang productie locatie, facilitaire
-----	---

	kosten), ondersteunend Personeel niet zijnde Personeel ten behoeve van de daadwerkelijke Productie en winst. U dient een ingevulde Bijlage 11 bij te voegen bij de beantwoording van deze wens. Voor het scoreverloop wordt verwezen naar Bijlage 11 en paragraaf 4.2 in het Beschrijvend document
--	--

Opdrachtgever wenst vooraf inzage in het Tarief van een medewerker, die betaald dient te worden tijdens het gebruik van de Uitwijk. De Tarieven zoals opgegevens bij Wens 4, zijn de Tarieven die gelden bij een Calamiteit. zie hiervoor ook hoofdstuk 5 van deze Specificatie van de opdracht.

W 4	Tarief Personeel Indien Opdrachtgever besluit het Calamiteitenplan in werking te stellen en de Uitwijklocatie in te zetten, wordt afgerekend op basis van een bleded uurtarief voor de inzet van Personeel ten behoeve van de Uitwijk. Het betreft Personeel ten behoeve van de Productie, zoals operators en ondersteuning van het Personeel (voorman, coördinatie en planning). Ook voor dit Tarief geldt dat kosten die niet in de inschrijving genoemd worden en niet verdisconteerd zijn in de prijsstelling, maar toch noodzakelijk blijken te zijn voor een goed functioneren van het product of de dienstverlening, conform de in de Aanbestedingsstukken gestelde eisen, voor rekening van Inschrijver zijn. U dient een ingevulde Bijlage 11 bij te voegen bij de beantwoording van deze wens. Voor het scoreverloop wordt verwezen Bijlage 11 en naar paragraaf 4.2 in het Beschrijvend document
------------	--

UE 26.	Het Calamiteitenplan zal tijdens de implementatiefase verder worden uitgewerkt in samenspraak met Opdrachtgever.
---------------	--

6.7. Documentatie

UE 27.	Opdrachtnemer zal Opdrachtgever voorzien van Documentatie tijdens de implementatiefase in elektronische vorm in de Nederlandse taal. Technische documentatie mag ook in de Engelse taal worden verstrekt.
---------------	---

u

UE 28.	De documentatie die opgeleverd dient te worden door Opdrachtnemer bevat in elk geval een Implementatieplan en Calamiteitenplan.
---------------	---

UE 29.	De Documentatie dient in een bewerkbaar format aangeleverd te worden, zodat Opdrachtgever deze zelf kan aanpassen wanneer Opdrachtgever in de toekomst zaken wijzigen in de configuratie. Opdrachtnemer dient aangepaste Documentatie aan te leveren in het geval er hiertoe aanleiding is. (bijv. aanpassingen in configuraties)
---------------	---

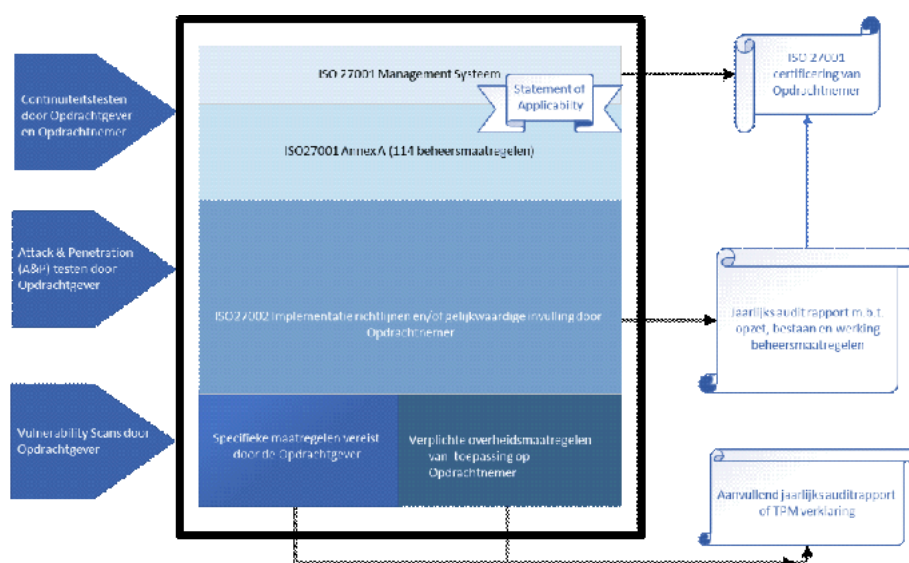
Hoofdstuk 7. Technische omgeving

7.1. Beveiligingskaders (BIO)

De omgang met Gegevens vraagt van de Aanbestedende dienst een werkwijze die de vertrouwelijkheid en integriteit van deze Gegevens waarborgt. Bij het betrekken van producten en diensten uit de markt dient een deel van de verantwoordelijkheden ingevuld te worden door de Opdrachtnemers. De Opdrachtnemer moet minimaal hetzelfde beveiligingsniveau leveren als de Aanbestedende dienst.

De Aanbestedende dienst is gehouden aan de algemene vigerende Nederlandse wet- en regelgeving en aan de Baseline Informatiebeveiliging Overheid (BIO). Dit document is als Bijlage B. Baseline Informatiebeveiliging Overheid beschikbaar gesteld. Deze regelgeving is gebaseerd op de ISO27002 en bevat daarnaast aanvullende beveiligingseisen, de zogenoemde overheidsmaatregelen. Vanwege de eigen technische inrichting, stelt de Aanbestedende dienst zelf ook specifieke beveiligingseisen.

In onderstaande figuur is de samenhang weergegeven tussen beveiligingsmaatregelen, de kaders ISO 27001/2 en de BIO, certificering, audits met betrekking tot opzet, bestaan en werking van de beheersmaatregelen, en continuïteits- en beveiligingstests.



UE 30.

Ten aanzien van de ISO 27001, of gelijkwaardige certificering:

- Toont de Opdrachtnemer jaarlijks de geldigheid van de certificering aan door het overleggen van een kopie van het kwaliteitscertificaat.
- Laat Opdrachtnemer op verzoek van de Aanbestedende dienst Audits uitvoeren door een daartoe gecertificeerde partij, waarbij de Aanbestedende dienst inzage krijgt in de resultaten.
- Wordt de Aanbestedende dienst door de Opdrachtnemer op de hoogte gehouden van de inrichting van de beheersmaatregelen van de ISO27001, conform de implementatierichtlijnen van de ISO27002, indien daar aanleiding voor is.

Opdrachtnemer is niet volledig gehouden aan de Baseline Informatiebeveiliging Overheid (BIO), Bijlage B, omdat dit stelsel geldt voor overheidspartijen. Er zijn desalniettemin een aantal verplichte implementatiemaatregelen waar ook de Opdrachtnemer invulling aan moet geven in het kader van de ISO27001 beheersmaatregelen. Dit betreffende volgende beheersmaatregelen:

Paragraaf	Beheersmaatregel
5.1	Aansturing door de directie van de informatiebeveiliging
5.1.1	Beleidsregels voor informatiebeveiliging Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
5.1.1.1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat ten minste de volgende punten: a. De strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid. b. De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden. c. De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers. d. De gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn. e. De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd. f. De bevordering van het beveiligingsbewustzijn.
5.1.2	Beoordeling van het informatiebeveiligingsbeleid Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
5.1.2.1	Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.
6.1.	Interne organisatie
6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.
6.1.1.1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.
6.1.1.2	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.
6.1.2	Scheiding van taken
6.1.2.1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.
6.2	Mobiele apparatuur en telewerken Rationale: procesondersteuning op gebied van voorgang, alerting, ... zou bij een externe partij ook zo maar via een mobile app gedaan kunnen worden.
6.2.1	Beleid voor mobiele apparatuur Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.
6.2.1.1	Mobiele apparatuur is zo ingericht dat bedrijfsinformatie niet onbewust wordt opgeslagen ('zero footprint'). Als zero footprint (nog)

Paragraaf	Beheersmaatregel
	niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, versleuteling van die gegevens. In het geval van opslag van vertrouwelijke informatie moet op deze mobiele apparatuur 'wissen op afstand' mogelijk zijn.
6.2.2	Telewerken Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen. Rationale: Op dit moment kunnen we niet overzien of straks activiteiten in het kader van b.v. werkvoorbereiding of rapportage vanuit huis kunnen worden uitgevoerd. Daarom is deze maatregel voor de zekerheid opgenomen.
7.1	Voorafgaand aan het dienstverband
7.1.1.1	Bij indiensttreding en bij functiewijziging wordt een Verklaring Omtrent het Gedrag (VOG) gevraagd.
7.1.2.1	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.
7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en – training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.
7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht.
8.	Beheer van bedrijfsmiddelen
8.3	Behandelen van media Rationale: opgenomen voor twee situaties: overdracht van gegevens wordt via fysieke media gedaan én de interne bedrijfsvoering van aanbieder is gebaseerd op informatie-overdracht met fysieke media
8.3.1	Beheer van verwijderbare media Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.
8.3.2	Verwijderen van media Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.
8.3.3	Media fysiek overdragen Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.
9.	Toegangsbeveiliging
9.1	Bedrijfseisen voor toegangsbeveiliging
9.1.1	Beleid voor toegangsbeveiliging Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.

Paragraaf	Beheersmaatregel
9.4.1	Beperking toegang tot informatie Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.
9.4.4	Speciale systeemhulpmiddelen gebruiken Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd. Rationale: met name bedoelt voor inperking van mogelijkheden om via 'tooltjes' aanvullend aan de eigenlijke bedrijfsmiddelen toegang verkregen kan worden tot afgeschermd informatie.
11.	Fysieke beveiliging en beveiliging van de omgeving Rationale: uitgangspunt is dat een externe locatie aan dezelfde beveiligingsnormen moet voldoen als onze eigen locatie, voor zover het de bescherming van onze gegevens (en evt. personeel) betreft.
11.1	Beveiligde gebieden
11.1.1	Fysieke beveiligingszone Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.
11.1.2	Fysieke toegangsbeveiliging Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.
11.1.4	Beschermen tegen bedreigingen van buitenaf Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.
11.2	Apparatuur Rationale: geen specifieke eisen, anders dan de eis dat dat output niet van buitenaf zichtbaar/leesbaar is.
13.	Communicatiebeveiliging
13.1	Beheer van netwerkbeveiliging Rationale: opgenomen omdat we nu nog niet weten welke rol (interne) netwerken bij de leverancier zullen spelen.
13.1.1	Beheersmaatregelen voor netwerken Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.
13.1.2	Beveiliging van netwerkdiensten Beveiligingsmechanismen, dienstverleningsniveaus en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.
13.1.3	Scheiding in netwerken Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.
13.2	Informatietransport
13.2.1	Beleid en procedures voor informatietransport Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.
13.2.2	Overeenkomsten over informatietransport Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.
13.2.3	Elektronische berichten Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.

Paragraaf	Beheersmaatregel
13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.
15.	Leveranciersrelaties
15.1.1.3	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.
15.1.3	Toeleveringsketen van informatie- en communicatietechnologie Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.
15.1.3.1	Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.
15.2.2	Beheer van veranderingen in dienstverlening van leveranciers Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.
16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen
16.1.5	Respons op informatiebeveiligingsincidenten Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.
UE 31.	Opdrachtnemer voldoet tenminste aan hierboven genoemde beheersmaatregelen uit de Baseline Informatiebeveiliging Overheid.