



Bijlage 2
Non functionele eisen

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Kwaliteit				
1.1	De kwaliteit van de Oplossing wordt bepaald op basis van de ISO25010-norm. De hierin genoemde kwaliteitsnormen zijn gerangschikt naar de daarin genoemde kwaliteitskenmerken. Vanuit de kwaliteitskenmerken zijn eisen en wensen geformuleerd. De norm is aangevuld met specifieke eisen en wensen die voor de Belastingdienst, of rijksoverheden in het algemeen, gelden. Er is voor gekozen om alleen de meest relevante kwaliteitseigenschappen te formuleren. Uitgangspunt hierbij is dat van de Oplossing minimaal een marktconforme kwaliteit wordt verwacht. Zo begrijpt iedereen dat de Responsetijd van een gebruikersactie niet in een ordegrootte van tientallen seconden ligt. De Belastingdienst wil dat de Oplossing logisch uit één geheel bestaat en dat te allen tijde de Inschrijver verantwoordelijk is voor alle functionele en non-functionele gedragingen van de Oplossing. Dit laat onverlet dat de Inschrijver delen van de Oplossing kan en mag onder-uitbesteden naar derden.	De Inschrijver levert de Oplossing als één integraal werkend systeem. Als de Oplossing bestaat uit deeloplossingen dan is de integratie van deze oplossingen de verantwoordelijkheid van de Inschrijver. De Inschrijver garandeert dat, bij gebruik van (deel)oplossingen van eventuele onderaannemers, ook deze partijen en hun (deel)oplossingen aan de in de Aanbestedingsstukken gestelde Kwaliteitsnormen en (Security)eisen voldoen.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Gebruik				
1.2	Onder Gebruik verstaan we de kwaliteit van de prestatie (performance), presentatie en interactie van de Oplossing. Voor wat betreft de prestatie wordt van de Inschrijver gevraagd aan te geven hoe objectief kan worden gemeten dat de prestatie van de Oplossing constant blijft gedurende de looptijd van de Overeenkomst.	De Oplossing kent minimaal 2 normwaarden (bijvoorbeeld Responsetijd van een specifieke veelgebruikte actie) waaraan de prestatie van de Oplossing wordt gemeten. Deze normwaarden worden opgenomen in de concept SLA van de Inschrijver, zijn gebaseerd op de normale en maximale werklast en dienen mede als referentie voor de prestatie van de Oplossing bij vermoedelijke toekomstige problemen omtrent de prestatie van de Oplossing. Over de actuele waarden wordt minimaal eens per kwartaal gerapporteerd. Invoervelden zijn voorzien van controles om gebruikersfouten te voorkomen.		
1.3	De Oplossing zal gebruikt worden door personen met een functiebeperking. De Belastingdienst is verplicht om hier rekening mee te houden. De Oplossing moet hier in zekere mate op ingesteld zijn.	De Oplossing biedt een intuïtieve, marktconforme gebruikersinterface in tenminste de Nederlandse taal.		
1.4	De Oplossing zal gebruikt worden door personen met een functiebeperking. De Belastingdienst is verplicht om hier rekening mee te houden. De Oplossing moet hier in zekere mate op ingesteld zijn.	De gebruikersinterface voldoet aan de EN 301 549* standaard en biedt hiermee oplossingen voor Gebruikers met een functiebeperking.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Gebruik				
1.5	De Belastingdienst hecht waarde aan een gelijke presentatie van alle applicaties die door de gebruikers van de Belastingdienst worden gebruikt. De Rijkshuisstijl geldt hierbij als leidraad.	De presentatie aan de Gebruikers is conform de Nederlandse Rijkshuisstijl ingericht (zie www.rijkshuisstijl.nl).		
1.6	Om de Oplossing te kunnen gebruiken is het wenselijk dat er zo min mogelijk aanpassingen op het gebruikersapparaat nodig zijn. De gebruikersapplicatie heeft bij voorkeur een 'zero-client footprint', waarbij de volledige toegang via een standaard browser verloopt, zonder het gebruik van applicatie-specifieke toevoegingen (bijv. plug-ins en/of dongles).	De oplossing dient een 'zero-client footprint' te hebben. D.w.z. er is, naast een webbrowser, geen additionele software, browser-plugin of additionele hardware nodig op de gebruikersapparaten om alle gevraagde functionaliteit van de Oplossing te kunnen benaderen.		
1.7	De Oplossing zal worden gebruikt op een diversiteit van apparaten, besturingssystemen en browsers. Een brede ondersteuning voor de toegang via deze gebruikersapparaten is nodig.	De Oplossing is apparaat-onafhankelijk te gebruiken op gangbare gebruikersapparaten die over een webbrowser beschikken. De Oplossing ondersteunt minimaal de huidige en de voorgaande versie van het Besturingssysteem welke nog actief wordt ondersteund door de leverancier van het Besturingssysteem. De Oplossing ondersteunt de vijf meest gangbare web browsers: Google Chrome, Microsoft Internet Explorer/Edge, Mozilla Firefox en Apple Safari. De versies die ondersteund worden zijn gelijk aan de versies die nog actief ondersteund worden door de leverancier van de web browser.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Gebruik				
1.8		Indien Opdrachtnemer gebruik maakt van Derde partijen voor Diensten of het leveren/gebruik laten maken van niet zelf voortgebrachte (programma)code dan wordt de Belastingdienst voor ingebruikname hiervan op de hoogte gebracht zodat hiervoor expliciete toestemming gegeven kan worden.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Beveiliging				
Normering /audit 1.9	Door ISO 27001 certificering kunt u aantonen dat uw informatiebeveiliging managementsysteem voldoet aan alle normen op het gebied van informatiebeveiliging.	De gevraagde oplossing van de Inschrijver is ISO 27001, SOC II gecertificeerd of een minstens gelijkwaardige norm en toont dit jaarlijks aan door middel van een audit dat door een onafhankelijk en algemeen erkend bureau wordt uitgevoerd. De resultaten van de audits (Certificaat /SOA) worden gedeeld met een door de Belastingdienst aangewezen Contractmanager.		
2.0		De organisatie(s) die de ICT-voorzieningen van de Oplossing levert en beheert, de datacentra, zijn ISO 27001, SOC II of gelijkwaardig gecertificeerd en blijven dit voor ten minste de duur van de Raamovereenkomst. Opdrachtnemer levert hiervan bewijs telkens terstond op eerste verzoek van de Belastingdienst.		
2.1		De Opdrachtnemer beschikt over een Informatiebeveiligingsbeleid conform de BIR2017 en een Verbeterplan Beveiliging (Security Roadmap). Documenten worden in het Engels of het Nederlands op verzoek van de Belastingdienst ter inzage gegeven.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Beveiliging				
2.2	De Oplossing van de Inschrijver zal ten aanzien van het beveiligingscertificaat en de configuratie ervan aan een QuickScan worden onderworpen. Deze QuickScan wordt uitgevoerd via de website van Qualsys SSL Labs. Een status van minimaal 'A' wordt door de Belastingdienst gezien als een aanvaardbaar veilige Oplossing.	De Oplossing behaalt een A-status (A-, A, A+) bij de SSL/TLS-test van Qualsys SSL Labs, op basis van TLS versie 1.2 of hoger. Deze status wordt periodiek, minimaal eens per kwartaal, bevestigd gedurende de Levensduur van de Oplossing.		
2.3		De Oplossing voldoet aan minimaal de ICT-beveiligingsrichtlijnen voor web-applicaties van het National Cyber Security Centre (NCSC).		
2.4	De Inschrijver zal er op toezien dat maatregelen worden genomen om ononderbroken de beveiliging van de Gegevens te kunnen waarborgen. Hiertoe zal regelmatig worden getoetst of de Oplossing veilig genoeg is en zullen, wanneer de beveiliging moet worden verbeterd, de nodige maatregelen ter verbetering worden uitgevoerd.	Elke medewerker van Opdrachtnemer die al dan niet direct toegang heeft tot (privacy)gevoelige Gegevens van de Belastingdienst, is in het bezit van een Verklaring Omtrent Gedrag (VOG, Certificate of Conduct).		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Beveiliging				
2.5		De Belastingdienst heeft het recht om minimaal 1 keer per jaar een audit (waaronder 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 resultaten van de audits worden, in de vorm van een Third Party Memorandum, gedeeld met een door de Inschrijver aangewezen Security Officer.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Beveiliging				
Kwetsbaarheden 2.6	Een grote bedreiging voor beveiliging van de Gegevens komt van derden, die ongeautoriseerd en ongewenst toegang krijgen tot de Oplossing en/of de Gegevens in deze Oplossing. Door regelmatig een Attack en Penetration test uit te voeren, kan tijdig worden onderkend of de Oplossing voldoende beschermd is tegen deze ongewenste toegang. Daarnaast zal bij elke wijziging een risicoanalyse op het gebied van informatiebeveiliging moeten plaatsvinden. Op basis van de uitkomsten van deze analyse wordt bepaald of naar aanleiding van de wijziging een extra Attack en Penetration moet worden uitgevoerd.	Conform beleid van de Belastingdienst is het niet toegestaan dat er kwetsbaarheden, gekwalificeerd door het bureau dat een <i>Attack and Penetration Test</i> (A&P-test) voor de Opdrachtnemer of de Belastingdienst, als Kritisch (Critical) of Hoog (High risk) in Productie staan. Kwetsbaarheden worden gekwalificeerd doormiddel van het Common Vulnerability Scoring System (CVSS 3.0). Kritische bevindingen dienen per direct te worden weggenomen door de Opdrachtnemer. Voor hoge risicobevindingen 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.		
2.7		Kwetsbaarheden in de Oplossing worden, zodra deze kwetsbaarheden bekend zijn, door Opdrachtnemer verholpen door een patch uit te voeren, direct na het beschikbaar komen van deze patch.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Beveiliging				
2.8		Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie-verwerkende systemen, behoren zo snel mogelijk (binnen 72 klokuren) al dan niet geautomatiseerd te worden gemeld aan het SOC van Belastingdienst.		
2.9		Opdrachtnemer heeft een medewerker in de rol van Security Officer die de Engelse of Nederlandse taal machtig is. Dit zowel in spraak al schriftelijk. Opdrachtnemer heeft een medewerker in de rol van contactpersoon voor privacyvraagstukken en –meldingen die de Engelse of Nederlandse taal machtig is. Dit zowel in spraak al schriftelijk.		
3.0	De Belastingdienst wil voorkomen dat er enkel op basis van de A&P test van de leverancier een kwetsbare Oplossing naar productie wordt gebracht.	De Belastingdienst behoudt zich het recht voor om een A&P-test uit te voeren als onderdeel van de Acceptatietest vóór in Productie name van de Oplossing. Opdrachtnemer dient hieraan kosteloos mee te werken. De bevindingen van de A&P-test worden door de Opdrachtnemer opgelost voordat door de Belastingdienst overgegaan kan worden tot het in productienemen van de Oplossing.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Beveiliging				
3.1		Opdrachtnemer laat minimaal één keer per jaar én bij iedere risicovolle wijziging van de Oplossing op het gebied van informatiebeveiliging een A&P-test uitvoeren op de Oplossing door een onafhankelijk en algemeen erkend bureau om de beveiliging te testen. Opdrachtnemer en de Belastingdienst besluiten gezamenlijk de scope van de A&P test. De resultaten van de testen worden gedeeld met een door de Belastingdienst aangewezen Security Officer. Bij het bespreken van de bevindingen worden afspraken gemaakt over de oplostijden en de aansluitende hertest. Opdrachtnemer draagt zorg voor het oplossen van de bevindingen binnen de afgesproken Oplostijden.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Beveiliging				
3.2	De Belastingdienst wil de risico's inperken dat onbevoegden gebruik kunnen maken van kwetsbaarheden in de Oplossing.	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. De kosten van de uitvoering van deze test zijn voor rekening van de Belastingdienst. Opdrachtnemer en de Belastingdienst besluiten gezamenlijk de scope van de A&P test. Mochten partijen er niet gezamenlijk uit komen, dan neemt de Belastingdienst de uiteindelijke beslissing hierover. De resultaten van de testen worden gedeeld met Opdrachtnemer. Bij het bespreken van de bevindingen worden afspraken gemaakt over de oplostijden en de aansluitende hertest. Opdrachtnemer werkt kosteloos mee aan A&P testen. Bevindingen uit A&P testen dienen op kosten van Opdrachtnemer opgelost te worden. Mochten er na een hertest nog onopgeloste bevindingen met de classificatie Medium of hoger open staan, dan worden er nieuwe afspraken gemaakt over de oplostijden voor de nog onopgeloste bevindingen. De aansluitende hertest hierna is op kosten Opdrachtnemer.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Beveiliging				
3.3		De Security Officer van de Belastingdienst heeft de bevoegdheid om toegang tot (relevante delen van) de oplossing te blokkeren. Dit wordt het Stekkermanndaat genoemd. Dit mandaat bestaat uit twee door Opdrachtnemer binnen 24 Klokuren uit te voeren acties: • Het onbeschikbaar maken van de oplossing; • 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. Opdrachtnemer werkt mee aan het implementeren van een Alternatieve werkstroom om het uit te voeren proces zoveel als mogelijk doorgang te laten vinden. Het deblokkeren van (delen van) de Oplossing mag alleen na toestemming van de Security Officer van de Belastingdienst. Bij de herstelacties werkt de Opdrachtnemer mee aan het weer in Productie nemen van de Oplossing, inclusief integratie van Gegevens die ontstaan is door de noodgedwongen uitwijk naar een Alternatieve werkstroom.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Beveiliging				
3.4	De Belastingdienst wil de mogelijkheid hebben om nieuwe kwetsbaarheden te detecteren en vaststellen dat bestaande kwetsbaarheden zijn opgelost. Dit is aanvullend op de eisen t.a.v. de Attack and Penetration tests.	De Belastingdienst heeft het recht om minimaal één keer per kwartaal een Kwetsbaarhedenscan op de Oplossing uit te laten voeren door het Security Operation Center (SOC) van de Belastingdienst. De Bevindingen worden indien nodig gedeeld en besproken met Opdrachtnemer. Opdrachtnemer werkt kosteloos mee aan de Kwetsbaarhedenscans die namens de Belastingdienst worden uitgevoerd en gevonden Kwetsbaarheden worden kosteloos opgelost.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
(Persoons-) Gegevens				
3.5	De Belastingdienst hecht veel belang aan de beveiliging van de (persoons-) Gegevens. De Belastingdienst heeft een taak en verantwoordelijkheid om er voor te zorgen dat (persoons-) Gegevens nooit in onbevoegde handen valt of kan 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.	De Oplossing voldoet aan de algemene vigerende Nederlandse Wet- en regelgeving, waaronder de Algemene verordening gegevensbescherming (AVG).		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
(Persoons-) Gegevens				
3.6	Op basis van een dataclassificatie BIR2017, en een Business Impactanalyse (BIA), zijn eisen geformuleerd ten aanzien van de inrichting, levering en het gebruik van de Oplossing	De Opdrachtnemer dient t.a.v. de Oplossing het mede mogelijk te maken dat de Belastingdienst aan de Baseline Informatiebeveiliging Rijksdienst (BIR) met dataclassificatie Basis Beveiligingsniveau 1 en 2 voldoet. Van de Opdrachtnemer worden de controls en rijksmaatregelen geëist die in de BIR2017 gekoppeld zijn aan het begrip “Dienstenleverancier”. Zie hiervoor de hoofdstukken 5 t/m 18 van de BIR2017: http://www.cip-overheid.nl/media/1151/20180210-bir2017-definitief.pdf Van de Opdrachtnemer wordt niet geëist dat wordt voldaan aan de onderstaande controles/rijksmaatregelen uit de BIR2017: 13.2.3.3. Maak gebruik van PKI-Overheid certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn o.a. digitale documenten binnen de Rijksdienst waar gebruikers rechten aan kunnen ontleen. 16.1.4.1. Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie-verwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC door of namens het department security contact (DSC, operationele contactpersoon voor het NCSC) of de Chief Information Security Officer (CISO).		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
(Persoons-) Gegevens				
3.7		De Oplossing moet voldoen aan relevante onderdelen uit de "Pas-toe-of-leg-uit-lijst" van het Forum Standaardisatie.		
Opslag 3.8	Het Rijksbeleid kent voorschriften t.a.v. locatie waar de gegevens worden opslagen.	Gegevens van de Belastingdienst worden binnen de Europese Economische Ruimte (EER) opgeslagen. Gedurende de levenscyclus van de Gegevens, blijven deze Gegevens binnen de EER.		
3.9	Voldoen aan Rijksbeleid.	Gegevens van de Belastingdienst zijn logisch gescheiden van Gegevens van andere klanten van Opdrachtnemer opgeslagen.		
4.0	De Gegevens zijn onder andere onderhevig aan de AVG en Archiefwet. Technische mogelijkheden in de Oplossing kunnen het eenvoudiger maken om aan deze Wetten te conformeren.	De Oplossing biedt de mogelijkheid om het archiveren en verwijderen van geclassificeerde Gegevens, bij voorkeur automatisch, uit te voeren.		
4.1	Het anonimiseren en/of pseudonimiseren van deze informatie heeft een positief effect op de zwaarte van de beveiligingseisen, die gesteld worden aan de koppelingen. De Belastingdienst hecht daarom veel waarde aan het kunnen anonimiseren en/of pseudonimiseren van persoonsgegevens.	De Oplossing kan (persoons)Gegevens bij verzending & opslag anonimiseren en/of pseudonimiseren.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
(Persoons-) Gegevens				
4.2		Op verzoek van de Belastingdienst worden de Gegevens binnen <24> Klokuren ter beschikking gesteld in een voor de Belastingdienst bruikbaar van te voren afgesproken digitaal formaat. Aanlevering gebeurt via een beveiligde verbinding.		
4.3		De Opdrachtnemer heeft een procedure voor het melden van datalekken aan de Belastingdienst op basis van de AVG zodat de Belastingdienst tijdig een melding kan doen bij de Autoriteit Persoonsgegevens. (Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra sprake is van een Datalek waarbij persoonsgegevens in het geding zijn).		

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
(Persoons-) Gegevens				
Versleuteling 4.4	In de ongewenste situatie dat onbevoegden toegang krijgen tot de Oplossing op een wijze, anders dan via de door de Belastingdienst toegekende identificatie en autorisatie, zullen de Gegevens in deze Oplossing ontoegankelijk moeten zijn. Hiertoe zullen alle Gegevens in alle toestanden, zijnde in ieder geval opslag en transport te allen tijde moeten worden geëncrypt met een door NIST of NCSC aanbevolen encryptie-algoritmes. Zie: http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html#ApprovedAlgorithms Een goede versleuteling van Gegevens verkleint het risico dat (persoons-)Gegevens ongewenst in handen komt van derden. Hierbij is het van belang dat: • de Gegevens versleuteld worden opgeslagen; • het transport van de Gegevens door middel van een versleutelde verbinding loopt; • de Gegevens zelf tijdens transport versleuteld zijn; • Sleutels op een correcte wijze worden beheerd (procedureel) en opgeslagen (technisch).	Gegevens waarmee in de Oplossing wordt gewerkt, worden versleuteld opgeslagen. Gegevens die tussen de Oplossing en andere ICT-services worden verzonden, waaronder die van Onderaannemers, dienen versleuteld te zijn. Versleuteling van de Gegevens geschiedt met een door NIST of NCSC aanbevolen encryptie-algoritmes van 256 bits of sterker. De Opdrachtnemer zorgt ervoor dat de versleuteling ook in de toekomst aangesloten blijft bij marktconforme encryptie-algoritmes.		

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Autorisatie en Authenticatie				
4.5	Om te waarborgen dat alleen geautoriseerde Gebruikers gebruik maken van de Gegevens in de Oplossing, moet elke Gebruiker een eigen unieke gebruikersidentificatie krijgen. Door het gebruikersaccount te herleiden naar één en uitsluitend één natuurlijk persoon kan misbruik van een gebruikersaccount beter worden bestreden.	De Oplossing biedt uitsluitend en alleen toegang tot Gegevens aan Gebruikers, die daarvoor expliciet geautoriseerd zijn door de Belastingdienst. Elke Gebruiker van de Oplossing krijgt een unieke gebruikersidentificatie (gebruikersaccount). Het gebruikersaccount is altijd één op één herleidbaar naar een Natuurlijk Persoon. De Belastingdienst beheert de gebruikersaccounts en bepaalt welke accounts opgevoerd of verwijderd moeten worden.		
4.6	Gezien de vertrouwelijkheid van de Gegevens is het wenselijk dat de Oplossing two-factor authentication ondersteunt.	De Oplossing biedt een mechanisme voor Two-factor authentication aan. Voor beheerders van de Oplossing (Opdrachtgever en Inschrijver) is gebruik als verplicht in te richten.		
4.7	De Oplossing maakt gebruik van één Identity Management Systeem, 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.	De Gebruiker hoeft zich eenmalig 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 (logisch) Identity Managementsysteem (IMS).		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Autorisatie en Authenticatie				
4.8	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 Inschrijver 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.	Het Identity Managementsysteem (IMS) van de Oplossing ondersteunt federatieve authenticatie op basis van SAML 2.0		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Koppelingen				
4.9	De oplossing dient aan te sluiten op de standaard werkwijzen en techniek van het Datacenter van de Belastingdienst.	Bij koppeling van de Oplossing aan een systeem van de Belastingdienst wordt voldaan aan de aansluitvoorwaarden van het Datacentrum van de Belastingdienst.		
5.0	De Oplossing zal in meer of mindere mate in staat moeten zijn om te koppelen met Oplossingen van derden. Dit moet het mogelijk maken om in de toekomst gegevens tussen andere autonome systemen en de Oplossing uit te kunnen wisselen.	Alle relevante API's van de Oplossing ten aanzien van koppelingen en gegevensuitwisseling met andere autonome systemen van derden zijn gedocumenteerd. Deze informatie is actueel, correct en wordt beschikbaar gesteld aan de Contractmanager.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Logging en monitoring				
5.1	Voldoen aan Rijksbeleid (BIR).	Alle mutaties die leiden tot wijziging van (persoons)Gegevens moeten worden gelogd en zijn te raadplegen door een daartoe geautoriseerde medewerker van de Belastingdienst. De logging bevat per mutatie minimaal de volgende informatie: • de mutatie zelf, • het apparaat vanwaar de mutatie is uitgevoerd (!), • de Gebruiker die de mutatie uitvoert, en de datum en het tijdstip van de mutatie.		
5.2		Op het gebied van toegangsverlening wordt minimaal het volgende gelogd: • Inlogpogingen (gelukt, mislukt);		
5.3	Zicht krijgen op afwijkingen om herstelacties te kunnen formuleren.	De Oplossing wordt volcontinu gemonitord op beveiligingsaspecten, capaciteit, performance en beschikbaarheid. Afwijkingen worden gelogd en gerapporteerd aan de Contractmanager. Indien vooraf ingestelde grenswaarden worden overschreden, dient actieve signalering via berichten of e-mail ingesteld te kunnen worden, De beheerder heeft de beschikking over tools om de performance te kunnen monitoren.		

Bijlage 2 - Non functionele eisen

5.4		Logfiles worden versleuteld opgeslagen op een daarvoor bestemde Log Server.		
5.5		Logfiles betreffende beveiligingsaspecten en incidenten & problemen worden dertien maanden bewaard en zijn geschikt om een root cause analysis (RCA) uit te voeren. Een RCA betreffende beveiligingsaspecten is verplicht en wordt gedeeld met een Security Officer van de Belastingdienst. De Opdrachtgever is verplicht om bij een prio 1 incidenten een RCA op te leveren en deze te delen met de Contractmanager van de Opdrachtgever.		
5.6		Bewaartijden van data (berichten, transacties, bestanden, databases, etc.) zijn vastgesteld en beschreven. Archivering en schoning van data (berichten, transacties, bestanden, databases, etc.) zijn beschreven en ingericht.		

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Herstelbaarheid				
5.7	De Oplossing dient voorbereid te zijn op een calamiteit, waarbij voldaan moet worden aan door de Belastingdienst gestelde eisen m.b.t. <i>Recovery Time Objective</i> .	De Oplossing dient in geval van een calamiteit binnen <24> klokuren weer volledig functioneel beschikbaar te zijn.		

Bijlage 2 - Non functionele eisen

5.8	De Oplossing dient voorbereid te zijn op een calamiteit, waarbij voldaan moet worden aan door de Belastingdienst gestelde eisen m.b.t. <i>Recovery Point Objective</i> .	In geval van een calamiteit is geen verlies van Gegevens toegestaan.		
5.9		De Oplossing heeft een Maintenance Mode (Sorry-pagina in te stellen door de beheerder). De Gebruiker wordt op de hoogte gesteld van de reden en de duur van de on-beschikbaarheid.		
6.0		Infrastructurele en functionele wijzigingen worden tijdig aangekondigd. Infrastructurele en functionele wijzigingen worden voor in productionenamen geaccepteerd door Opdrachtgever. Dit gebeurt in ieder geval als dit impact heeft voor de Gebruiker.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
SLA				
6.1	De Belastingdienst sluit met de Opdrachtnemer een Service Level Agreement (SLA) af aangaande de te leveren Diensten. De SLA bevat een beschrijving van de vastgestelde normen in de vorm van Service levels.	Opdrachtnemer levert bij inschrijving een SLA voor de oplossing dat in elk geval onderstaande aspecten bevat: • Wijze waarop invulling wordt gegeven aan 3e lijn ondersteuning; • Een aanpak die er voor zorgt dat de Belastingdienst altijd vrij kan beschikken over een op basis van open standaarden opgebouwde digitale recente (1 Kalenderdag) kopie van de Gegevens en de metadata van de Oplossing.		
6.2		Inschrijver heeft de procedures beschreven voor de afhandeling van (proces en afhandelingstermijnen) van beveiligingsincidenten op de aspecten: - (Poging tot) Cyberinbraak - Responsible disclosure - Common vulnerabilities en Exposures (CVE) en security notes - Bevindingen A&P-test.		

Bijlage 2 - Non functionele eisen

6.3		De Oplossing voldoet minimaal aan het volgende Service level m.b.t. de afhandeling van incidenten (Oplostijd): Impact/ Urgentie: Hoog/hoog Prestatie- indicator: Oplostijd Incident Prio 1 Doel: 4 klokuren Norm: 95% Impact/ Urgentie: Laag/hoog Prestatie- indicator: Oplostijd Incident Prio 2 Doel: Ma t/m vr: één dag (24 klokuren) Norm: 95% Impact/ Urgentie: Laag/laag Prestatie- indicator: Oplostijd Incident Prio 3 Doel: Ma t/m vr: drie dagen (72 klokuren) Norm: 85% Toelichting: <i>Impact Hoog</i> Een Incident heeft of kan ernstige gevolgen hebben voor • één of meer bedrijfsprocessen die burger en /of bedrijf direct raken, en/of • één of meer fabriekstaken voor (massale) gegevensverwerking en/of • de informatiebeveiliging en/of • het imago van de organisatie <i>Impact Laag</i> • Overige situaties <i>Urgentie Hoog</i> Een Incident • beïnvloedt Kwaliteit van functies/Beschikbaarheid/Beveiliging sterk en/of • brengt integriteit van de Gegevens in het geding en/of • treedt op tijdens piektijd/-periode van het bedrijfsproces en/of • uiterste verzenddatum van klantbescheiden in gevaar en/of • verstoort de communicatie met de klanten van Opdrachtgever <i>Urgentie Laag</i> • Overige situaties		
-----	--	---	--	--

Bijlage 2 - Non functionele eisen

6.4		De concept SLA zal in de periode tussen de mededeling van de gunningsbeslissing en de definitieve gunning door de winnende Opdrachtnemer en Opdrachtgever worden besproken en vastgesteld op een 1.0 versie. De 1.0 versie wordt Bijlage <X> – “Service Level Agreement” bij de Overeenkomst. De 1.0 versie wordt jaarlijks bijgewerkt wanneer er wijzigingen in de SLA optreden. De versienummering geeft aan welke SLA de laatste versie is.		
6.5		De Oplossing voldoet minimaal aan het volgende Service level m.b.t. de beschikbaarheid van de Oplossing: • 7x24 openstelling van de Oplossing; • Norm: beschikbaarheid van 99% per maand (= maximaal 7,20 uur downtijd per maand); • Downtime in verband met infrareserveringen in de changekalender of implementaties van IT-services op verzoek van deelnemende Organisaties wordt niet meegeteld bij het vaststellen van de Beschikbaarheid.		

Bijlage 2 - Non functionele eisen

Categorie	Doelstelling	Eis	Ik kan hier aan voldoen (Ja/Nee)	Opmerking leverancier
Algemeen				
6.6		De SAAS- oplossing wordt extern gehost, conform de aansluitvoorwaarden van de SAAS- broker Belastingdienst. De SAAS oplossing wordt gekoppeld aan Logius Digipoort. Hiervoor gelden de aansluitvoorwaarden van Logius: https://logius.nl/diensten/digipoort		
6.7	Beleid van Belastingdienst.	De door Opdrachtnemer ten behoeve van de Belastingdienst gebruikte domeinnamen zijn eigendom van de Belastingdienst.		
6.8	De Belastingdienst wil bij beëindiging van de overeenkomst invulling geven aan een goede implementatie van een vervangende oplossing.	Bij beëindiging van de overeenkomst tussen de Belastingdienst en Opdrachtnemer is een ordentelijke overgang van Opdrachtnemer naar de nieuwe dienstverlener gewenst om de continuïteit van de Diensten te borgen. Opdrachtnemer is verplicht haar volledige medewerking te verlenen aan een zo soepel mogelijke overdracht.		
6.9		Om bij beëindiging van de overeenkomst 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 overeenkomst op afroep Additionele Diensten conform de in Bijlage X "Financieel Model" aangegeven Prijzen. Deze Additionele diensten hebben in ieder geval betrekking op de migratie van Gegevens uit de Oplossing naar een vervangende oplossing.		

Bijlage 2 - Non functionele eisen

7.0		Opdrachtnemer zorgt er voor dat uiterlijk één (1) kalendermaand na het beëindigen van de overeenkomst en na ommekomst van een eventuele tijd voor migratie, dat alle Gegevens van de Belastingdienst onherstelbaar zijn vernietigd en overhandigt daarvoor een door een IT-Auditor of accountant gecertificeerde verklaring van vernietiging aan de Belastingdienst. Partijen zullen hierover gezamenlijk concrete werkafspraken maken.		
-----	--	---	--	--