Bijlage: Nonfunctional requirements (Eisen niet functioneel)

ROCvA-F stelt de volgende (onvoorwaardelijke) eisen aan de S2P-applicatie:
Bij de WENSEN dient u uw antwoord in te vullen. Deze worden niet meegenomen als gunningscriterium.

Vragen over aanpassingen van deze set eisen kunt u stellen middels het formulier notavragen (als bijlage bij een bericht in Tenderned)

Algemeen

Nummer	Eis	Keyword
Algemeen		
AL1	Inschrijver heeft een aangetoond ecosysteem van innovatie met gebruikersbijeenkomsten, een actieve gebruikersgemeenschap, een actieve partnergemeenschap en andere programma's waarmee we technische en zakelijke problemen kunnen oplossen.	Ecosysteem
AL2	Opdrachtnemer informeert Opdrachtgever terstond over alle zaken en onregelmatigheden die van belang zijn voor de continuïteit van de uitvoering van de opdracht of een bedreiging vormen voor de continuïteit van de bedrijfsprocessen van Opdrachtgever.	Continuïteit
AL3	De Servicedesk van Opdrachtnemer is op werkdagen telefonisch bereikbaar van 08:00-18:00	Servicedesk
ICT functionaliteit		
IE1	De oplossing dient gebaseerd te zijn op een SaaS oplossing dat wil zeggen dat de leverancier verantwoordelijk is voor het beheer, het hosten van de oplossing en het realiseren van koppelingen. Er is geen sprake van maatwerk, wel van configureren. De software hoeft niet meer (af)gemaakt te worden op het moment van aanbieden.	ondersteuning van browsers
IE2	Alle functionaliteiten van de oplossing zijn gedurende de gehele contractperiode voor Opdrachtgever benaderbaar via gangbare browsers. Onder gangbare browsers verstaan we die browsers die gemeld worden op http://www.netmarketshare.com/ We eisen 100% functionaliteit in deze top 5 meest gebruikte browsers	ondersteuning van browsers
IE3	De applicatie moet te 100% te gebruiken zijn op alle gebruikelijke devices (zoals iPad, iPhone, Android telefoons en tablets, met minimaal besturingssysteem N-2. Dit betekent de laatste versie én de twee vorige versies van het besturingsysteem.	Mobile devices
IE4	Het is mogelijk dat alle rollen (medewerker, leidinggevende en functioneel beheerder) op elk device zonder additionele plugins of andere software, gebruik kunnen maken van de applicatie. De SaaS applicatie is voor deze rollen een "Zero Footprint" web-applicatie: er is geen clientsoftware nodig voor het kunnen gebruiken van de functionaliteiten.	
IE5	Er zijn geen applicatiespecifieke plugins en/ of add-ons benodigd om de SaaS-oplossing te benaderen via de webinterface.	
IE6	Er zijn geen applicatiespecifieke plugins en/ of add-ons benodigd om de SaaS-oplossing te benaderen via de webinterface. Een plug-in (ook wel invoegtoepassing) is een aanvulling op een computerprogramma; in dit geval de webbrowser. Plug-	

	ins worden over het algemeen gemaakt om een programma uit te breiden of meer mogelijkheden te geven. Een plug-in heeft de host-applicatie (i.c. de webbrowser) nodig om te kunnen werken en kan niet standalone draaien. SAAS: Leverancier garandeert dat data ontsluiten via een webservice zonder onderbrekingen van de webservice gebeurt (geen corrupte data) ongeacht de dataomvang	
WENS	De gebruikersinterface voldoet aan de webrichtlijnen niveau 2 (zie https://www.digitoegankelijk.nl/). Het betreft zowel de gebruikersinterface van de applicatie als de output die daaruit gegenereerd wordt. De leverancier moet desgevraagd via certificering of auditing kunnen aantonen dat wordt voldaan aan de WCAG. Wordt niet beoordeeld.	Uw reactie
IE7	Alle componenten van de oplossing bieden een intuïtieve, marktconforme gebruikersinterface in tenminste de Nederlandse taal.	
WENS	Het moet mogelijk zijn om een voorkeurstaal in te stellen, waarbij minimaal Nederlands en Engels wordt ondersteund.	Uw reactie
IE9	De gebruikersinterface moet voldoen aan de huisstijl van de Opdrachtgever. Zo moet het minimaal mogelijk zijn om het logo van de opdrachtgever in te richten in de applicatie frontend.	
IE10	Een te printen of gmeaakt document kan met een preview op het scherm getoond worden. In deze preview kunnen door de gebruiker geen wijzigingen worden doorgevoerd.	
IE11	Het Aanbestedende Dienst kiest één samenwerkingsplatform binnen de organisatie: M365.	
IE12	Documentatie is in het nederlands en wordt opgeleverd in bewerkbaar Office365 formaat	
IE13	Een medewerker moet volgens het single sign on principe via het portaal naar de applicatie kunnen gaan. Ons principe is Surfconext tenzij..	
IE14	De applicatie dient het gebruik van M365 client applicatie op het device van de door de medewerker te ondersteunen. Van toepassing wanneer documenten met de standaard werkplek software geopend of bewerkt moeten worden.	
IE15	Het is mogelijk om vanuit de SaaS oplossing, mail te sturen naar medewerkers van de Opdrachtgever via het publieke mail adres van de betreffende medewerker (bijvoorbeeld: "voornaam.achternaam@opdrachtgever.nl"): Richting: van de SaaS oplossing naar het MX record van het domain "opdrachtgever.nl". Batch/Realtime: Realtime, Transport/Bestandsformaat: SMTP	
IE16	Bij het versturen van e-mail namens de opdrachtgever moet gebruik worden gemaakt van DNS gebaseerde beveiligingsmethodes SPF, DKIM, DMARC en DANE. Dit is bedoeld om SPAM en spoofing tegen te gaan. SPF – Sender Policy Framework. Doel: verminderen van SPAM en fraude. DKIM – DomainKeys Identified Mail. Doel: verminderen van SPAM DMARC – Domain-based Message Authentication, Reporting and Conformance. Doel: spoofing van e-mail mitigeren. DANE – DNS-based Authentication of Named Entities. Doel: het afdwingen van cryptografische oplossingen (STARTTLS). https://jarnobaselier.nl/e-mailbeveiligingsprotocollen-dkim-dmarc-en-dane/	

Beveiliging		
BE1	De Oplossing voldoet gedurende de gehele looptijd van de Overeenkomst aan de algemene vigerende wet- en regelgeving van de Nederlandse overheid, waaronder de Algemene Verordening Gegevensbescherming, en de meest recente standaard security protocollen en algoritmen, waaronder de ICT-Beveiligingsrichtlijnen voor Webapplicaties van het NCSC*. Toelichting: De ICT-beveiligingsrichtlijnen voor webapplicaties geven een leidraad voor veiliger ontwikkelen, beheren en aanbieden van webapplicaties en bijbehorende infrastructuur. Deze beveiligingsrichtlijnen zijn breed toepasbaar voor ICT-voorzieningen die gebruikmaken van webapplicaties. https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html	AVG
BE2	De Inschrijver is minimaal tot uiterste datum van de inschrijving ISO27001 gecertificeerd met betrekking op de te leveren dienstverlening, voldoet aan de norm ISO 27001, SOC II of een minstens gelijkwaardige norm en toont dit periodiek aan door middel van een audit dat door een onafhankelijk en algemeen erkend bureau wordt uitgevoerd. De resultaten van de audits worden gedeeld met de Security Officer van de Opdrachtgever. De organisatie(s) die de ICT-voorzieningen van de Oplossing levert en beheert, de datacentra, zijn ISO 27001, SOC II of gelijkwaardig gecertificeerd. ZIE OOK Kerncompetentie 3 in de Leidraad	ISO27001
BE3	Leverancier toont de Opdrachtgever periodiek een ISAE3402 type II of ISAE3000 verklaring van een onafhankelijk derde waaruit blijkt dat de informatiebeveiliging van de organisatie conform gestelde eisen van de Opdrachtgever is en alle maatregelen gedurende een periode goed heeft gefunctioneerd. Opdrachtgever krijgt op eerste verzoek inzage in de rapportage. ZIE OOK kerncompetentie 2 in de Leidraad	ISAE3402
BE4	Indien de leverancier niet ISO 27001 gecertificeerd is kan een kwaliteitshandboek voldoen. Hiervan zijn alle onderdelen van de ISO 27001 uitgewerkt en heeft een externe auditor vastgesteld dat de opgenomen PDCA cyclus gelijkwaardig is van opzet als de ISO 27001 voorschrijft. Alternatieven voor een ISO27001 certificering is een ISAE3402 type II of ISAE3000 verklaring: Oplevertermijn: Binnen vijftien (15) kalenderdagen na voorlopige gunning dient de Inschrijver aan wie de Opdrachtgever voornemens is de opdracht te gunnen, het bij deze eis behorende bewijs in te dienen, met name de beoordeling van de externe auditor omtrent de opzet en bestaan van het kwaliteitshandboek. Voor het certificaat geldt dat Inschrijver middels een alternatieve methode kan aantonen dat zijn inrichting en beheer voor informatiebeveiliging vergelijkbaar is aan het kwaliteitsniveau van een ISO27001 certificaat. Inschrijver moet een kwaliteitsmanagementsysteem moet kunnen overleggen dat voldoet aan de onderwerpen van de gestelde ISO/IEC 27001 norm. De beschrijving mag maximaal 20 A4-pagina's te zijn. Het kwaliteitshandboek is door een externe auditor getoetst (in opzet en bestaan). Het kwaliteitsmanagementsysteem van de Inschrijver zal, in geval van gunning, onderdeel gaan	ISAE3402

	uitmaken van de Overeenkomst . Inschrijver verplicht zich er dan toe om zijn geoffreerde kwaliteitssysteem in stand te houden gedurende de duur van de Overeenkomst .	
WENS	Inschrijver toont één keer per jaar in de vorm van een recente formele audit-verklaring van een onafhankelijke partij aan, de opzet, het bestaan en de werking van een passend stelsel van beveiligingsmaatregelen ten aanzien van de Oplossing. De resultaten van de audits worden gedeeld met de Security Officer van de Opdrachtgever. De Opdrachtgever 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 Opdrachtgever kiest hierbij, in consensus met de Inschrijver, 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 de Security Officer.	Uw reactie
BE6	Zolang de Opdrachtnemer/Verwerker niet beschikt over een geldige certificering als bedoeld in artikel 4.2.van de Verwerkersovereenkomst rapporteert Opdrachtnemer/Verwerker jaarlijks over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van het bepaalde in de Verwerkersovereenkomst. Deze rapportage betreft ook, indien van toepassing, de werkzaamheden van door hem ingeschakelde derden. Opdrachtnemer/Verwerker zal na een verzoek daartoe van Verwerkingsverantwoordelijke minimaal eens per jaar kosteloos een Third Party Memorandum (TPM) c.q. een verklaring van een onafhankelijke externe deskundige aan Verwerkingsverantwoordelijke verstrekken over de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen. Zie voor details de Addendum bij de Verwerkersovereenkomst, Bijlage 3, artikel 4.5.	Audit verklaring
BE7	Inschrijver laat minimaal één keer per jaar én bij iedere risicovolle wijziging van de Oplossing op het gebied van informatiebeveiliging een penetratie-test uitvoeren door een onafhankelijk en algemeen erkend bureau om de beveiliging te testen. De resultaten van de testen worden gedeeld met de Security Officer van de Opdrachtgever. De Opdrachtgever heeft het recht om een penetratie test uit te laten voeren om de beveiliging te testen. De Opdrachtgever kiest hierbij zelf, in consensus met de Inschrijver, een onafhankelijk en algemeen erkend bureau dat de testen uitvoert. De resultaten van de testen worden, in de vorm van een Third Party Memorandum, gedeeld met de Security Officer van de Opdrachtgever. Opdrachtgever heeft de bevoegdheid om opdracht te geven de toegang tot de Oplossing per direct (tijdelijk) te blokkeren. Het weer toegankelijk maken van de Oplossing mag alleen na toestemming van de Security Officer van de Deelnemende Organisaties. Inschrijver beschrijft in de SLA van de Inschrijver hoe hier invulling aan wordt gegeven.	Third Party Memorandum
BE8	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT componenten van de webapplicatie (scope) gevolgd door een follow up van noodzakelijke verbeteringen.	Vulnerability assessment
BE9	Toegang tot de SaaS oplossing via een Internet Browser vindt versleuteld plaats ("https") met TLS1.2 of hoger.	Toegang tot browser

BE10	De applicatie voldoet aan de meest actuele OWASP richtlijnen: https://owasp.org/www-project-top-ten/ Uitleg De OWASP top tien is een ranglijst met de 10 gevaarlijkste beveiligingsrisico's. Op basis van de OWASP Risk Rating Methodology wordt voor elk punt in de top 10 beoordeeld wat de zwakte, detecteerbaarheid en de exploiteerbaarheid is. En ook wat de ernst van de gevolgen is, als je er niet goed mee omgaat in je applicatie.	Beveiligingsrichtlijnen
BE11	Het systeem voorziet in validatiecontroles in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken. Er zijn geschikte beheersmaatregelen geïmplementeerd voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.	Validatiecontroles
BE12	Alle betrokken systeemcomponenten worden (gelijk aan het scannen op kwetsbaarheden) frequent gepatcht volgens marktconforme 'best practices'. Kritische security patches moeten direct worden aangebracht. Er is een schriftelijk vastgelegd proces voor patching en wijzigingsbeheer van toepassing.	Wachtwoord
BE13	Opdrachtnemer beveiligt alle gegevens van Opdrachtgever op adequate wijze zodanig dat bescherming wordt geboden tegen gegevensverlies als wel toegang tot gegevens door onbevoegden. Met "alle gegevens" wordt bedoeld zowel "data in use" als "data in motion" en "data at rest". Opdrachtnemer informeert Opdrachtgever direct bij een (vermoeden van) toegang door onbevoegden.	Wachtwoord
BE14	Gevoelige (vertrouwelijke) gegevens worden beschermd door gebruik te maken van cryptografische technieken in de database, bestanden en/of communicatie.	Geautoriseerd gebruik
BE15	Alle betrokken systeemcomponenten zijn ontworpen om en getest op het voorkomen van gegevensverlies, het lekken van gegevens en systeemproblemen. Systeemcomponenten dienen veilig te worden geconfigureerd conform best practice hardening guidelines. Er is een schriftelijk vastgelegd proces voor hardening van alle systeemcomponenten.	Patching
BE16	De architectuur van de dienst bevat een scheiding tussen: - gebruikersschermen, technische interfaces en web services; - proceslogica en informatieverwerking; - gegevensopslag en databases. Tussen deze onderdelen zijn beveiligingsmaatregelen geïmplementeerd waarmee oneigenlijk gebruik wordt voorkomen.	Gegevens
BE17	Opdrachtnemer dient voor zowel de applicatie als de onderliggende technische infrastructuur doorlopend maatregelen te nemen om bedreigingen en aanvallen zoals onder meer side channel, guest-hopping, hyperjacking en SQL-injection te voorkomen.	Cryptografie
BE18	De inschrijver heeft een uitgewerkt protocol om cyberaanvallen te weren of de eventueel geleden schade op een gestructureerde en adequate manier op te lossen.	Encryptie
BE19	Bij koppelingen wordt de inkomende en uitgaande data gecontroleerd op malafide code/Virussen/Trojans/Spam door middel van een Intrusion Detection System (Inbraakdetectiesysteem, IDS) en Intrusion Prevention System (inbraakpreventiesysteem, IPS), waarbij de de eventueel geleden schade op een gestructureerde en adequate manier wordt opgelost.	Hardening

BE20	Bij koppelingen (in- en uitgaand) biedt de applicatie een mechanisme dat datamutaties tijdens transport detecteert en logt.	
BE21	Bij koppelingen (in- en uitgaand) biedt de applicatie een mechanisme om de data ("payload") te versleutelen.	
BE22	De (web-)applicatie heeft een A status bij de certificaat- en configuratie-test van “Qualsys SSL Labs” op https://www.ssllabs.com/ssltest/.	Beveiliging
BE23	Verbindingen tussen cliënt (webbrowser/app) en de (SAAS) server dienen versleuteld (minimaal SSL) plaats te vinden op basis van een Extended Validation SSL certificaat (zowel intern als extern). Bij verwerking van bijzondere persoonsgegevens dienen deze gegevens aanvullend versleuteld via de bestaande SSL verbinding dan wel via een versleutelde tunnel plaats te vinden (SSH/VPN/SFTP).	Koppelingen
BE24	Bij systeemkoppelingen (in- en uitgaand) van data vindt er wederzijds systeemauthenticatie plaats door middel van certificaten ("Two Way SSL").	Koppelingen
BE25	Verkeer tussen de verschillende segmenten wordt gefilterd (minimaal op IP) en verkeer wordt alleen toegestaan in overeenstemming met applicatie benodigdheden	Filteren
BE26	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van protectie- en detectiemechanismen.	Netwerkverkeer
BE27	Het netwerk van de opdrachtnemer is gescheiden in logische en fysieke domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.	Netwerksegmentatie, DMZ
BE28	Er wordt (logische) netwerksegmentatie toegepast waarbij productie, acceptatie en test omgevingen met verschillende beveiligingsniveaus van elkaar gescheiden worden.	Netwerksegmentatie
BE29	Data van de Opdrachtgever mag niet voor andere dan de beoogde gebruikers beschikbaar komen. In geval van “multi-tenancy” oplossingen mogen API-services en netwerk-services shared zijn, maar data opslag niet. De data is alleen per tenant toegankelijk en opgeslagen.	Mult-tenancy
BE30	In het geval van multi-tenancy, moeten virtuele servers of applicaties geïsoleerd zijn van andere virtuele servers en applicaties van de andere tenants	Mult-tenancy
BE31	Opdrachtnemer zal Opdrachtgever onmiddellijk informeren nadat zij bekend is geworden met een vermoedelijk(e) of daadwerkelijk(e) onbevoegde kennisneming, wijziging of verstrekking van gegevens; verlies van gegevens; of schending van de beveiligingsmaatregelen. Opdrachtnemer zal op eigen kosten alle benodigde maatregelen nemen om de gegevens veilig te stellen, de tekortkomingen in de beveiligingsmaatregelen te herstellen om verdere onbevoegde kennisneming, wijziging, en verstrekking te voorkomen, onverminderd enig recht van Opdrachtgever op schadevergoeding of andere maatregelen. Opdrachtnemer zal op verzoek van Opdrachtgever meewerken aan het informeren van de bevoegde autoriteiten en betrokkene.	Beveiligingsincidenten
BE32	Opdrachtnemer heeft alle relevante beveiligingseisen waaronder geheimhouding opgenomen in overeenkomsten met eigen medewerkers en derden waarbij sprake is van toegang tot, het verwerken van, communicatie van of beheer van informatie of IT-voorzieningen van de organisatie. Dit geldt ook wanneer er sprake is van toegang in verband met toevoeging van producten of diensten aan IT voorzieningen.	Geheimhoudings verklaring

Koppelingen			
KE1	De applicatie voldoet aantoonbaar aan de onderstaande richtlijnen: 1. Het koppelvlak zorgt ervoor dat de applicaties volledig zijn ontkoppeld en onafhankelijk van elkaar zijn. 2. Het koppelvlak is volledig stateless ten opzichte van de applicatie. 3. Het gekozen protocol dat via het koppelvlak loopt is duidelijk vastgelegd en wordt volledig ondersteund. 4. Bij elke koppeling dient de gegevensverantwoordelijke akkoord te zijn met de levering. 5. Het koppelvlak dient getest te kunnen worden van en naar de applicatie. (ketentest) 6. Het gegevens model en de opdrachten wat via het koppelvlak loopt dient volledig gemodelleerd en bepaald te zijn.	Richtlijnen	
KE2	De applicatie mag geen interactie met overige applicaties van de Opdrachtgever hebben behalve wanneer deze voor het internet geschikte API's hanteren.	Interactie met overige applicaties	
KE3	Data uitwisseling via koppelingen vindt plaats via REST / SOAP over HTTPS. De ondersteunde bestandformaten zijn XLSx, JSON, of XML.	Transportformaat	
KE4	Voor koppelingen, integratie, imports en export vindt data uitwisseling plaats via bestanden en protocollen die voorkomen in de lijst van open standaarden (https://www.forumstandaardisatie.nl/open-standaarden).	Open standaarden	
KE5	Opdrachtnemer dient voor de API's gebruik te maken van een API-gateway, waarbinnen de vereiste beveiliging geregeld wordt, DDOS bescherming geboden wordt (bijvoorbeeld via whitelists), het gebruik van de API wordt gelogd en gemanaged kan worden en throttling geregeld kan worden, zodat er bijvoorbeeld een limiet ingesteld kan worden aan het aantal API requests per tijdseenheid.	API-gateway	
KE6	Binnen de API dient het versiebeheer vastgelegd te worden.	Versiebeheer	
KE7	Op het moment dat er een nieuwe versie van de API beschikbaar is en nadat de Opdrachtnemer schriftelijk aan Opdrachtgever en alle toepassende instanties van de API heeft aangegeven dat de oude API niet meer ondersteund gaat worden, moet de oude API nog minimaal 1 jaar ondersteund worden. Opdrachtnemer blijft verantwoordelijk om bij bijvoorbeeld constatering van een beveiligingslek in de oude API direct adequate actie te ondernemen.	Versiebeheer	
KE8	Opdrachtnemer levert een beschrijving aan van de functionaliteit van de API als onderdeel van de documentatie van de API. Ook levert Opdrachtnemer aan hoe de foutafhandeling in de response van de API is ingericht, welke duidelijke en consistente foutcodes en foutmeldingen worden toegepast. Opdrachtnemer geeft aan hoe het versiebeheer is ingeregeld.	Documentatie	
KE9	Opdrachtnemer levert een (bij voorkeur geautomatiseerd) testplan voor de API aan bij Opdrachtgever ter goedkeuring. Alle mogelijke use cases dienen in het testplan uitgewerkt te zijn, waardoor per toepassing of actie getest kan worden of deze voldoet.	Testplan	
KE10	Voor oplevering levert Opdrachtnemer de resultaten van een pen- en hacktest aan welke is uitgevoerd op de op te leveren API.	Testplan	
KE11	De API wordt door Opdrachtnemer bij initiële oplevering en bij oplevering van nieuwe versies middels het door	Testplan	

	Opdrachtnemer eventueel bijgewerkte en door Opdrachtgever goedgekeurde testplan getest binnen de door Opdrachtnemer beschikbaar gestelde Acceptatieomgeving.	
KE12	Tijdens de test wordt door Opdrachtnemer de resultaten van de test vastgelegd in het testplan. Opdrachtgever ontvangt dit testplan binnen een week na uitvoering van de test en reageert formeel binnen vijf werkdagen op de resultaten.	Testplan
KE13	Eventuele restpunten worden binnen een week na reactie van Opdrachtgever op de resultaten van het testplan opgelost. Na controle hiervan door Opdrachtgever wordt het testplan definitief opgesteld en door Opdrachtgever en Opdrachtnemer schriftelijk geaccordeerd en is er sprake van Acceptatie van de API.	Testplan
Implementatie		
AE1	Inschrijver zal in de eerste week na bekendmaking van de voorlopige gunning een startoverleg voeren met de contactpersonen van de deelnemende organisaties. Alle werkzaamheden zijn onder voorbehoud tot aan de definitieve gunning. In het geval de gunning na de stand-still periode wordt ingetrokken zal de inschrijver de gemaakte kosten in rekening kunnen brengen.	Implementatieplan
AE2	Op verzoek van een deelnemende organisatie dient de inschrijver binnen 30 dagen in samenspraak met de deelnemende organisatie te komen tot een definitief implementatieplan voor de betreffende deelnemende organisatie. Het uitgangspunt voor dit plan in het bij de inschrijving ingestuurde implementatieplan.	Implementatieplan
AE3	De Inschrijver verzorgt de migratie van alle, door de Opdrachtgever gewenste, informatie van het oude naar het nieuwe systeem.	migratie
AE4	Tijdens de migratie wordt door Inschrijver zorg gedragen voor de continuïteit in dienstverlening.	migratie
AE5	De Inschrijver dient tijdens de migratie aandacht te besteden aan de communicatie intern bij Inschrijver, tussen Opdrachtgever en Inschrijver en communicatie tussen huidige Opdrachtnemer en Inschrijver.	migratie
AE6	De leverancier zorgt voor de complete implementatie (technisch en functioneel) van koppelingen met andere SaaS leveranciers.	koppelingen
AE7	In het implementatieplan staat helder beschreven welke processen en systemen geraakt gaan worden tijdens de inplementatie. Hiervoor wordt een design gemaakt door opdrachtnemer wat wordt voorgelegd aan de opdrachtgever ter goedkeuring.	Implementieplan
AE8	Indien tijdens de implementatie onvoorziene zaken worden geconstateerd wordt dit vroegtijdig voorgelegd aan opdrachtgever. Mogelijke aanpassingen aan implementatieplan zijn voor rekening opdrachtnemer	Implementieplan
AE9	In het implementatieplan wordt duidelijk aangegeven wat de eisen vanuit opdrachtgever zijn. Hierin wordt tevens aangegeven wat de rollen van zowel opdrachtnemer als -gever zijn	Implementieplan
AE10	De aangeboden applicaties zijn in acceptatie fase aan een veiligheidstest onderworpen en bevindingen zijn aantoonbaar verholpen voordat deze in productie gaat. Alvorens de toepassing door ROCvA-F in gebruik genomen wordt, wordt/is een zgn. Pen- en Hacktest uitgevoerd. De uitvoering van de Pen- en Hacktest vindt plaats, of heeft aantoonbaar plaatsgevonden, door een onafhankelijke partij. Inschrijver draagt de kosten voor de Pen- en Hacktest.	Pen- en hacktest

Meerwerk		
MW1	Opdrachtgever is vrij om te beslissen of Leverancier opdracht krijgt tot het uitvoeren van Meerwerk.	Meerwerk
MW2	Leverancier zal niet eerder met het Meerwerk aanvangen nadat hij daartoe schriftelijk en uitdrukkelijk opdracht van Opdrachtgever heeft gekregen. Indien Leverancier Meerwerk verricht zonder zodanige schriftelijke opdracht is hij met betrekking tot die werkzaamheden niet gerechtigd tot enige vergoeding.	Meerwerk
MW3	Mondelinge afspraken of mondelinge opdrachten tot het verrichten van Meerwerk binden Opdrachtgever niet, ongeacht de persoon door wie ze zijn gemaakt of gegeven. Partijen doen afstand van de mogelijkheid zich ter zake van mondelinge afspraken of mondelinge (opdrachten op artikel 3:61 lid 2 BW dan wel artikelen 3:35 en 36 BW te beroepen.	Meerwerk
MW4	Indien Opdrachtgever het wenselijk acht om vanwege doorontwikkeling, aanpassingen van processen en/of procedures wijzigen in de ICT Dienstverlening aan te brengen, zal er hiervoor een RFC t.b.v. Meerwerk worden ingediend bij Leverancier. In deze RFC staat opgegeven wat er gewenst is, welke randvoorwaarden daarvoor gesteld zijn/ worden en de gewenste doorlooptijd.	Request for Change
MW5	Leverancier stuurt uiterlijk binnen twee (2) werkdagen nadat de RFC van de Opdrachtgever is binnengekomen een digitale ontvangstbevestiging met een referentienummer.	Request for Change
MW6	Uiterlijk binnen twee (2) weken na binnenkomst van de RFC zal Leverancier een voorstel bij Opdrachtgever neerleggen van de gewenste werkzaamheden/functionaliteiten. Hierin staat ondermeer: · dat de offerte opgesteld is op basis van de voorwaarden / condities komende vanuit de (hoofd) overeenkomst; · het referentienummer van de Leverancier en de Opdrachtgever; · een omschrijving van de gewenste werkzaamheden/functionaliteiten op detail niveau. D.w.z. dat de Opdrachtgever duidelijk kan herleiden welke Dienst/Producten er (functioneel) worden geleverd, tegen hoeveel uren per expertise, de onderlinge rolverdeling, eventuele randvoorwaarden en risico's, de eenmalige kosten, de terugkerende kosten (beheer/onderhoud)en de planning.	Request for Change
MW7	Opdrachtgever zal de offerte binnen vijf (5) werkdagen inhoudelijk beoordelen, en de Leverancier hierover informeren.	Meerwerk
MW8	Indien de Opdrachtgever zich niet kan vinden in de prijs, kan er besloten worden op deze te controleren op marktconformiteit (zie Benchmarkprocedure)	Meerwerk
MW9	Een offerte wordt uitsluitend goedgekeurd nadat beide partijen hebben ondertekend voor akkoord.	Meerwerk
Beheer		
BR1	De opdrachtgever kan zelf autorisaties inrichten op basis van rollen en/of hiërarchie waarbij de autorisatiestructuur is gebaseerd op gebruikersgroepen.	Aurorisaties
BR2	Opdrachtgever kan zelf gebruikers aanmaken en autoriseren, rechten wijzigen en intrekken zonder tussenkomst van de Inschrijver.	Gebruikersaccount
BR3	Elke Gebruiker van de Oplossing krijgt een unieke gebruikersidentificatie (gebruikersaccount). Een gebruikersaccount is altijd herleidbaar naar een Natuurlijk Persoon. De Opdrachtgever beheert de gebruikersaccounts en bepaalt welke accounts opgevoerd of verwijderd moeten	Gebruikersaccount

	worden. De Oplossing biedt uitsluitend toegang tot Gegevens aan Gebruikers, die daarvoor expliciet geautoriseerd zijn door de Opdrachtgever.	
BR4	De applicatie faciliteert authenticatie door middel van de combinatie gebruikersnaam/wachtwoord + Token, voor situaties waarbij niet via SSO ingelogd wordt, bijv. vanuit BYOD.	Wachtwoord
BR5	Wachtwoorden voldoen aan de complexiteitseisen en lengte van de aanbestedende dienst (beleid opvraagbaar bij Aanbestedende Dienst)	Wachtwoord
BR6	Indien de gebruiker zijn wachtwoord moet wijzigen, kan hij dit (in geval van Single Sign On) middels een email-procedure zelf regelen zonder tussenkomst van enige servicedesk.	Inloggen
BR7	Alle inlogpogingen (inclusief mislukte) van gebruikers en systemen worden gelogd. Minimaal wordt in de log vastgelegd de accountnaam, de locatie, het tijdstip, en het resultaat van de inlogpoging.	Wijzigen wachtwoord
BR8	Ingeregeld moet kunnen worden wat de maximale gebruikerssessietijd is voor gebruikers. Daarna wordt de sessie automatisch verbroken.	Inloggen
BR9	Het is mogelijk om een account te blokkeren na een ingesteld aantal foutieve inlogpogingen.	Inloggen
BR10	Het account van een gebruiker die 3 maanden niet heeft ingelogd, wordt bevroren. Als dit 6 maanden is, dan wordt zijn recht(en) ingetrokken of on hold gezet. Hij/zij moet dan opnieuw de rechten aanvragen via de gebruikelijke procedure voor het aanvragen van een nieuw gebruikersaccount .	
BR11	Authenticatie van medewerkers vindt plaats op basis van de Identity Access Management (IAM) oplossing van de Opdrachtgever.	IAM
BR12	Het Identity Managementsysteem (IMS) van de Oplossing ondersteunt federatieve authenticatie op basis van SAML 2.0 of het OAUTH2 protocol	IAM
BR13	De gebruiker authentiseert conform de Identity Access Management (IAM) oplossing van de Opdrachtgever. De gebruiker kan hiermee inloggen met de netwerk inlognaam en wachtwoord en token van de Opdrachtgever.	IAM
BR14	Van uitgegeven autorisaties aan gebruikers kunnen op eenvoudige wijze door Opdrachtgever rapportages/selecties gemaakt worden.	Overzicht autorisaties
BR15	Er moet in ieder geval 1 persoon van de Opdrachtgever de rol van “site administrator” of 'super user' hebben die het benodigde beheer kan uitvoeren.	System administrator
BR16	De functioneel beheerder dient, indien nodig, extra rechten (raadplegen, mutatie- en beheerrechten, etc.) aan rollen en profielen te kunnen toewijzen, zodat er verschillende rollen ondersteund kunnen worden.	System administrator
BR17	Afhankelijk van de gekozen autorisatiemodule: a. De functioneel beheerder dient gebruikers aan te kunnen maken, wijzigen en ‘verwijderen’ in de applicatie, of, b. De functioneel beheerder dient rollen te kunnen definiëren die gekoppeld zijn aan het Active Directory van de Opdrachtgever, zodat deze automatisch gekoppeld kunnen worden, zodra er een nieuwe medewerker in dienst komt.	System administrator
BR18	De Applicatie beschikt over functionaliteit om beheeractiviteiten uit te voeren door Opdrachtgever, zonder tussenkomst van de leverancier, zoals het kunnen opstarten en monitoren van batches.	Beheeractiviteiten

BR19	De opdrachtgever stelt minimaal een Acceptatie- en Productie-omgevingen beschikbaar. Hierbij dient er een fysieke scheiding te zijn tussen de Productieomgeving en de acceptatie- omgeving.	OTAP
BR20	Een (SAAS) oplossing/dienst of product heeft altijd minimaal een representatieve acceptatie omgeving met volledige functionaliteit.	OTAP
BR21	De Acceptatie omgeving moet om kunnen gaan met geanonimiseerde gegevens met volledig behoud van functionaliteit.	OTAP
BR22	Er dient 2 werkweken voor livegang eerst op een acceptatie omgeving een update van een (SAAS) oplossing/dienst/product beschikbaar worden gesteld.	OTAP
BR23	De SaaS oplossing is horizontaal en/of verticaal schaalbaar, zodat in de browser van de gebruiker een maximale beleving van de applicatie wordt gerealiseerd.	Schaalbaarheid
BR24	(Saas) oplossingen/dienst/product die aanvullende plugins vereisen krijgen de juiste plugin via leverancier gepushed, zodat juiste versie wordt gebruikt voor de applicatie.	Plugins
BR25	Leverancier ontwikkelt door aan de applicatie/product of dienst zodat de nieuwste plugin versie (N-1) wordt ondersteund	Plugins
BR26	Opdrachtnemer en/of diens SaaS-leverancier heeft netwerksegmentatie geïmplementeerd waarbij omgevingen met verschillende beveiligingsniveaus van elkaar gescheiden worden. Onder andere de eigen ontwikkel-, acceptatie-, en productie omgevingen.	Netwerk segmentatie
BR27	De beheerprocessen o.a. incident-, problem en releasemanagement van de Leverancier zijn op basis van de meest recente versies van ITIL en BISL ingericht.	ITIL
BR28	Alle data uitwisselactiviteiten via de systeemkoppelingen worden gelogd. Minimaal wordt in het log vastgelegd de accountnaam (welk systeem), het tijdstip, het soort data, het transportnummer en het resultaat van de uitwisseling.	Logging
BR29	Alle logbestanden worden minimaal 2 jaar bewaard, tenzij anders is afgesproken.	Logging
WENS	De logs voor authenticatie en transport worden op een andere locatie en een separaat systeem ("Security Information & Event Management" of "SIEM" oplossing) opgeslagen. Dus niet binnen de systeemoplossing.	Uw reactie
BR30	De toegang tot de logs voor authenticatie en transport zijn voorzien van separate accounts, toegangsrechten en rollen.	Logging
BR31	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.	Logging
BR32	Het is mogelijk om alerts op logging aan te maken. Opdrachtgever wordt hierover actief geinformeerd.	Logging
BR33	De applicatie beschikt over een niet-muteerbare audit-trail waarin automatisch registratie en opslag van de volgende gegevens plaats vindt: 1) alle handelingen (functionaliteiten) die door gebruikers met betrekking tot metagegevens, processen, documenten, dossiers of andere objecten worden verricht, 2) de gebruiker, datum en tijd van de uitvoering van de handeling	audit trail
BR34	De Applicatie moet de mogelijkheid bieden tot dagelijkse monitoring van de beveiligingsaspecten, capaciteit, performance en beschikbaarheid van alle componenten van de Applicatie door Opdrachtgever dan wel door een door Opdrachtgever aangewezen externe partij. Afwijkingen worden gerapporteerd aan de Opdrachtgever.	Monitoring

BR35	In de webapplicatieomgeving zijn signaleringsfuncties voor beveiligingsincidenten (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	Signalering beveiligings incidenten
BR36	De Leverancier richt een Service Desk in als enige contactpunt voor incidenten en wijzigingen met de Opdrachtgever	Service desk
BR37	De Service Desk communiceert met OG uitsluitend de Nederlandse taal.	Service desk
BR38	De Leverancier richt een proces in voor het opnemen van incidenten/meldingen en maakt hierbij gebruik van een webbased applicatie. Het systeem is toegankelijk voor de opdrachtgever en voldoet aan de ICT aansluitvoorwaarden. Met het systeem zijn zowel door de leverancier als de opdrachtgever rapportages te maken.	Incident management
BR39	Indien incidenten/meldingen niet adequaat worden opgevolgd wordt geëscaleerd conform door de Opdrachtgever en de Leverancier ingerichte escalatieprocedure op 3 niveaus (Strategisch/Tactisch/Operationeel).	Incidentmanagement
BR40	De Leverancier stelt een contactpersoon aan die aangesproken kan worden over de voortgang c.q. afhandeling van een incident of melding	Incident management
BR41	Opdrachtgever wordt actief geïnformeerd bij systeemfouten of onbeschikbaarheid van bepaalde functionaliteiten middels e-mailnotificatie of andere actieve foutenlog.	(On)beschikbaarheid
BR42	De Leverancier informeert de Opdrachtgever over de voortgang van het oplossen van een problem d.m.v. een problemrapport.	Problem management
BR43	In geval van contact met technisch applicatiebeheer is de voertaal Nederlands	Nederlands
BR44	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.	Patchmanagement
BR45	De leverancier stelt bij bekende 'bugs' bijbehorende workarounds beschikbaar.	Workarounds
BR46	De Leverancier voert alleen gepland onderhoud uit in het afgesproken Maintenance Window en stelt de Opdrachtgever minimaal een maand van tevoren daarvan op de hoogte. Leverancier stuurt een risico analyse van gepland onderhoud vergezeld van extra maatregelen om de stabiliteit te garanderen. De inschatting van de risico's is de verantwoordelijkheid van Opdrachtgever (op basis van implementatie plan of change voorstel). Na akkoord/geen bezwaar Opdrachtgever kan het onderhoud worden uitgevoerd.	Gepland onderhoud
BR47	Saas: Update, patches en ander onderhoud door leverancier worden tenminste 72 uur van tevoren aangekondigd op website en per mail aan contactpersoon Aanbestedende Dienst.	Gepland onderhoud

BR48	De leverancier stelt jaarlijks een update-beleid op voor hardware (indien van toepassing) en software. Dit beleid wordt vastgelegd en ter goedkeuring voorgelegd aan de beheerders van de Opdrachtgever	Gepland onderhoud
BR49	Het update-beleid moet zijn voorzien van een planning die is afgestemd met Opdrachtgever.	Gepland onderhoud
BR50	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Change management
BR51	Binnen het changeproces worden RFC's onderkend die geïnitieerd kunnen worden door de Leverancier en de Opdrachtgever, waarbij de wijzigingen niet worden uitgeleverd als maatwerk, maar als standaard functionaliteit.	Change management
BR52	De webserver is ingericht volgens een configuratie-baseline	Configuraties
WENS	Gegevens uit mutatietabellen kunnen ontsloten worden via een andere applicatie.	Release management
WENS	Opdrachtgever heeft de mogelijkheid om geen gebruik te maken van bepaalde releases of upgrades van het systeem	Release management
WENS	De Leverancier is verantwoordelijk voor de jaarlijkse test van de uitwijk en de disaster/recovery, indien noodzakelijk vanwege de BIV rating, de Opdrachtgever participeert in de uitwijktest. Deze test wordt in overleg met Opdrachtgever aan het begin van het jaar gepland.	Release management
WENS	De Leverancier stelt driemaandelijks een Service Managementrapport op ten behoeve van de Opdrachtgever.	Backup en recovery
WENS	Consequenties voor de (eind) gebruikers zijn tijdens de implementatie duidelijk gemaakt (instructies / handleidingen). Concreet: minimale extra workload na de implementatie van een applicatie/tool. Bij de Servicedesk dient documentatie beschikbaar te zijn voor het correct en tijdig kunnen afhandelen van eerste lijns meldingen	Overleg
BR53	Leverancier levert minimaal een kwartaal vooruit inzicht gegeven in geplande releases (met releasenotes), Life Cycle Management (LCM)-trajecten, upgrades en vergelijkbare changes en beschrijft de roadmap van de applicatie, product of dienst.	Rapportages
BR54	Bij een upgrade / nieuwe release van een SAAS-oplossing wordt altijd de documentatie up-to-date beschikbaar gesteld, ten tijde van het beschikbaar komen van de upgrade / nieuwe release op de acceptatie omgeving	Documentatie
BR55	Herstelmaatregelen, waaronder back-up en recovery procedures, zijn geïmplementeerd en worden periodiek getest.	SLA, DFA en DAP
BR56	De Leverancier levert actief een constructieve bijdrage aan het strategisch (1x per jaar), tactisch (1 keer per half jaar) en operationeel overleg (1x per half jaar)	Dossier Financiele Afspraken

BR57	De Applicatie beschikt over een bibliotheek van rapportages en selecties/ queries, die gebruikt kunnen worden door eindgebruikers en / of functioneelbeheerders van de Opdrachtgever. Het gaat hier om operationele procesinformatie en managementinformatie over de processen. Het is mogelijkheid om op alle tabellen en velden: a. Nieuwe selecties/rapportages te maken, te wijzigen en uit te voeren b. Standaardselecties/rapportages uit te voeren.	Dossier Afspraken en Procedures
BR58	Documentatie van een product/dienst/applicatie is volledig vrij van copyrights en mag door de Aanbestedende Dienst worden gebruikt/gemodificeerd voor eigen gebruik	1e en 2e lijns onderhoud
BR59	Inschrijver draagt zorg voor de totstandkoming en het gedurende de looptijd van de overeenkomst/het contract actueel houden van de volgende documenten: • Service Level Agreement (SLA); • Dossier Afspraken en Procedures (DAP); • Dossier Financiële Afspraken (DFA).	SLA, DFA en DAP
BR60	Onderdeel van het contract is een aanvullend Dossier Financiele afspraken met de onderdelen: - Benoeming van de prijzen per onderdeel en totalen. - Interval van facturatie. - Toepassing van, en welke indexatie. - Kosten van uitbreidingen licenties en uren. - Aanvullende eisen inhoud facturen.	Dossier Financiele Afspraken
BR61	Onderdeel van het contract is een Dossier Afspraken en Procedures. De genoemde onderwerpen in het SLA worden hierin aangevuld met beschrijvingen van: - Werkwijze. - Communicatie.	Dossier Afspraken en Procedures
BR62	Het Onderhoud van de Apparatuur wordt door of namens Opdrachtnemer en door of namens Opdrachtgever verzorgd. Opdrachtgever zal het 1e lijns (Preventief en Correctief) Onderhoud (laten) verzorgen . Opdrachtnemer verzorgt al het overige (2e lijns) Preventief en (2e lijns) Correctief Onderhoud en vervanging (vervanging in het geval herstel niet langer mogelijk is, dan wel in het geval vervanging voordeliger is dan herstel).	1e en 2e lijns onderhoud
Gegevensbeheer		
GEG01	Alle binnen de Apparatuur verzamelde en vastgelegde data is en blijft eigendom van Opdrachtgever en dient te allen tijde op verzoek van Opdrachtnemer verstrekt te kunnen worden. Opdrachtnemer dient zich ten aanzien van alle verzamelde en vastgelegde data te houden aan de Algemene Verordening Gegevensbescherming (AVG) (let op: alle gegevens die	Eigenaarschap van gegevens, AVG

	informatie kunnen verschaffen over een identificeerbare natuurlijke persoon moeten als persoonsgegevens worden beschouwd). Opdrachtnemer behoudt geen rechten om de gegevens te gebruiken, te ontsluiten en/of publiek te maken. Opdrachtnemer verplicht zich om geen andere handelingen met de (persoons)gegevens te verrichten dan in de Overeenkomst is omschreven.	
GEG02	Bij een SAAS oplossing is de leverancier verantwoordelijk voor toepassing van de wettelijke bewaartermijnen van gebruikersgegevens conform de AVG (lifecycle management gegevens).	Bewaartermijn, AVG
GEG03	De bewaartermijn van de Persoonsgegevens wordt door Opdrachtgever vastgesteld. Opdrachtnemer/Verwerker vernietigt – na overleg met Opdrachtgever/Verwerkingsverantwoordelijke - gedurende de looptijd van de Overeenkomst en de Verwerkersovereenkomst de persoonsgegevens na ommekomst van de bewaartermijn. Zie voor details de Addendum bij de Verwerkersovereenkomst, Bijlage 3, artikel 1.	Bewaartermijn, AVG
GEG04	De applicatie ondersteunt Opdrachtgever in de naleving van de privacywetgeving (AVG), inzake de rechten van betrokkenen. Onder meer door het mogelijk te maken dat gedeelten van persoonsregistraties kunnen worden gewijzigd, gewist of beperkt toegankelijk kunnen worden gemaakt. Dit met het oog op het effectief opvolging kunnen gegeven aan een verzoek tot inzage, rectificatie en aanvulling, vernietiging of beperking van verwerking van Persoonsgegevens.	AVG
GEG05	Op verzoek van Opdrachtgever/ Verwerkingsverantwoordelijke werkt Opdrachtnemer/ Verwerker altijd mee aan een gegevensbeschermingseffectbeoordeling (DPIA) en een voorafgaande raadpleging als bedoeld in artikel 35 en 36 AVG. Zie de Verwerkersovereenkomst, Bijlage 3 artikel 4.7.	DPIA
GEG06	Opdrachtnemer/ Verwerker garandeert te allen tijde expliciet compliance van onderaannemers en gelieerde partners aan de overeengekomen regels met Opdrachtgever. Opdrachtnemer verifieert dit ook actief.	Onderaannemers
GEG07	Op een verifieerbaar authentiek schriftelijk verzoek van Opdrachtgever verwijdert Opdrachtnemer aantoonbaar en gegarandeerd alle betreffende gegevens, ook die op eventuele back-upmedia, volledig en onomkeerbaar, tenzij anders schriftelijk overeengekomen.	Verwijderen van gegevens
GEG08	Opdrachtnemer staat toe dat alle relevante data op verzoek als archief in een algemeen bruikbaar en bewerkbaar bestandsformaat gedownload kan worden door Opdrachtgever en dan wel naar een andere – door Opdrachtgever aan te wijzen - opdrachtnemer kan worden overgezet, in een algemeen	Archiveren

	bruikbaar en bewerkbaar bestandsformaat met inachtneming van vertrouwelijkheid en integriteit van de data.	
GEG09	De applicatie heeft een mechanisme om productiedata (of een subset) te anonimiseren of pseudonimiseren. Het is mogelijk de geanonimiseerde data te kopiëren naar een andere omgeving. De geanonimiseerde data mag niet herleidbaar zijn tot een natuurlijk persoon.	Anonimiseren van gegevens
WENS	Het moet mogelijk zijn om een export te maken van bestanden en bijbehorende metadata op basis van opgegeven zoekcriteria, zonder onacceptabel gegevensverlies, ten behoeve van bijvoorbeeld overdracht naar een andere omgeving, zoals bij het einde van de overeenkomst. De onderlinge samenhang tussen gegevens, indien van toepassing, kan worden blijven gelegd (bijv.: metadata en bestanden, relationele database) om informatieverlies te voorkomen (informatie blijft volledig interpreteerbaar).	Uw reactie
GEG11	Export van gegevens moet minimaal mogelijk zijn in csv of excel formaat.	Export van bestanden
GEG12	De applicatie kan gegevens en bestanden uitwisselen met andere systemen conform CMIS standaard.	
WENS	De applicatie kan gegevens en bestanden uitwisselen met andere systemen conform CMIS standaard.	
WENS	De oplossing biedt een gedetailleerde zoekfunctie op alle ingevoerde en automatisch gegenereerde metadata en combinaties hiervan.	
WENS	De zoekfunctie ondersteunt zoeken door alle tekstgegevens van van informatieobjecten (full tekst search).	
WENS	De zoekfunctie ondersteunt zoeken door specifieke metagegevens ('advanced search' of 'faceted search').	
GEG16	Opdrachtgeverspecifieke stuur- of stamtabellen zijn te onderhouden door Opdrachtgever zonder tussenkomst van de leverancier.	Beheer stamtabellen
GEG18	Data van de Opdrachtgever mag niet voor andere gebruikers beschikbaar komen. In geval van “multi-tenancy” oplossingen mogen API-services en netwerk-services shared zijn, maar de data niet. De data blijft alleen per tenant toegankelijk. In geval van toepassing van IT infrastructuur die gedeeld wordt met derde	Multi tenancy

	partijen (bijvoorbeeld SaaS) worden er door Opdrachtnemer afdoende maatregelen getroffen om te voorkomen dat gegevens van Opdrachtgever onbedoeld worden gedeeld met derden dan wel worden gecombineerd met gegevens van andere klanten door aggregatie of interferentie. Multi-tenancy	
SLA		
SLA1	Inhoud SLA De SLA zal in de periode tussen voorlopige gunning en tekenen van de overeenkomst tussen Inschrijver en Opdrachtgever worden besproken en vastgesteld, zodat deze door Inschrijver en Opdrachtgever gelijktijdig met de overeenkomst kan worden ondertekend. Na vaststelling van de Versie 1.0 zal deze jaarlijks worden onderhouden als er wijzigingen in de SLA optreden. De versienummering geeft aan welke SLA de laatste versie is. De SLA zal gebaseerd zijn op de Overeenkomst, het Beschrijvend Document en de Inschrijving. De SLA moet zorgdragen dat de geformuleerde beschikbaarheid en herstelbaarheid gehaald worden.	
SLA2	Onderdeel van het contract zijn aanvullende SLA's met prestatieindicatoren, onderdelen hierin: - Bereikbaarheid - Beschikbaarheid - Incidentmanagement - Security management - Change management - Releasemanagement - Servicerapportages - Servicegesprekken	
SLA3	In de SLA wordt opgenomen de wijze waarop de Opdrachtgever wordt geïnformeerd over: • Uitgevoerde beveiligingstesten en de bevindingen daaruit; • Gegevens vanuit IT-Service Continuity management; • KPI's; • De beschikbare SLA rapportages voor de verschillende rapportageniveau's.	
SLA4	In de SLA wordt informatie opgenomen ten aanzien van • Openstelling en Beschikbaarheid; • De gebruikte tool voor afhandelen van incidenten, issues, callls, enz; • Icident- en vraagafhandeling en daarbij behorende kwalificaties; • Verstrekken van informatie over de behandeling van een Incident of vraag; • Een afhandeling in streeftijden ten aanzien van het verstrekken van informatie over incidenten met een kwalificatie van de ernst van incidenten.	

SLA5	In de SLA wordt informatie opgenomen inzake • Hoe komen functionele wijzigingen tot stand; • Is er een gebruikersgroep, zo ja • Welke invloed heeft deze op de geboden functionaliteit van de oplossing; • Wie zitten er in deze groep.	
SLA6	Releases en releasemanagement In de SLA wordt opgenomen • Hoeveel versies van de Oplossing worden gelijktijdig ondersteund; • Hoeveel flexibiliteit wordt geboden met betrekking tot het moment waarop een nieuwe Release moet gaan gebruiken; • Kan bestaande functionaliteit vervallen. Zo ja, hoe en wanneer wordt dit gecommuniceerd; • Hoe lang wordt geboden functionaliteit minimaal ondersteund; Hoeveel Releases worden per jaar uitgebracht./ hoe is het releasemanagement ingericht?	
SLA7	Beschikbaarheid voor online verwerkingen/bedrijfskritische applicaties: • 7:00 -22:00 uur CET • Norm: 99,8% (38 minuten per maand niet beschikbaar) • Downtime op verzoek van Opdrachtgever wordt niet meegeteld bij het vaststellen van de beschikbaarheid.	
SLA8	Het oplossen van storingen dient minimaal te voldoen aan de volgende norm: - Hoge Prio -> 30 minuten responsetijd, 2 uur oplostijd - Medium Prio -> 60 minuten responsetijd , 5 uur oplostijd - Lage Prio -> 4 uur responsetijd, 2 werkdagen *Opdrachtgever bepaald de prioriteit*	
SLA9	De gebruiker dient verstoringen en hulpvragen per e-mail te kunnen melden 24 uur per dag / 7 dagen in de week. Prio 1 storingen dienen ook 24x7 telefonisch gemeld te kunnen worden.	
SLA10	Op werkdagen tussen **8.00** en **18.00** uur CET dienen verstoringen en hulpvragen ook telefonisch te kunnen worden gemeld.	Helpdesk
SLA11	Opdrachtgever zorgt voor performance monitoring en rapportage van transacties binnen de applicatie.	
SLA12	De opdrachtnemer is in staat in geval van een ernstige calamiteit de (corrupte) data te herstellen en beschrijft het proces hiervoor in de SLA.	
SLA13	Incidenten worden voorzien van een prioriteit: 1) Incidenten die leiden tot volledige uitval van één of meer bedrijfskritische procesonderdelen. Deze Incidenten komen in de Service Management rapportage tot uiting in een verlaagd beschikbaarheid percentage.	Prioriteit incidenten

	2) Incidenten die ernstig impact hebben op de dienstverlening en die leiden tot een uitval of verminderde dienstverlening voor een groot deel van de gebruikers 3) Incidenten die een beperkte impact hebben, die slechts voor enkele gebruikers merkbaar zijn, uitval van niet-bedrijf kritische applicatie.	
SLA14	In geval van fouten/verstoringen in de toepassing gelden de volgende normtijden 1. Prioriteit Hoog: De Oplossing vertoont ernstig verlies aan functionaliteit, maar kan- naar de mening van ROCvA-F - nog worden gebruikt; 2. Prioriteit Midden: De Oplossing vertoont hinderlijke tekortkomingen, maar kan normaal worden gebruikt); 3. Prioriteit Laag: overig. Zie Leidraad 1.2.10 en overeenkomst.	Prioriteit incidenten
SLA15	De Leverancier stelt een rootcause analyse op na elk Prio1 calamiteit. Dit rapport wordt binnen 5 werkdagen na het beëindigen van de escalatie door de Leverancier verzonden aan de Opdrachtgever en wordt besproken tijdens het eerstvolgende operationele overleg.	Escalaties
SLA16	Leverancier levert een (maandelijkse) servicerapportage op aan de opdrachtgever. De inhoud en exacte frequentie wordt beschreven in de SLA.	Servicerapportage
SLA17	Klachten worden ingediend bij de contactpersoon van leverancier en Opdrachtgever dient binnen twee werkdagen een terugkoppeling te hebben gekregen. De klacht dient binnen 5 werkdagen na terugkoppeling naar tevredenheid van Opdrachtgever te zijn afgehandeld.	Klachtafhandeling
SLA18	De leverancier garandeert dat het dataverlies bij een calamiteit maximaal vier (4) uur is.	
WENS	De leverancier heeft een backup retentie van minimaal dertig (30) dagen. Dus met andere woorden, we kunnen dertig (30) dagen terug in de tijd.	Uw antwoord
SLA19	Het maken van de back-ups vindt plaats zonder beperkingen voor het beschikbaarheidswindow.	Backup
Financieel		
FIN1	U dient het Tarievenblad/prijsformulier in te vullen. Onder de licentiekosten worden alle kosten ten behoeve van het leveren van de dienst verstaan, zoals bijvoorbeeld onderhoud, beheer, hosting, certificering, bereikbaarheid van de helpdesk, afstemming met opdrachtgever en alle overige bijkomende kosten. Alle vermelde prijzen en tarieven dienen gesteld te zijn **inclusief** BTW. Er mogen geen aanvullende kosten in rekening gebracht worden voor opdrachtgever. Het niet bekend zijn met de situatie bij de Opdrachtgever kan nimmer aanleiding zijn tot verrekening. De door u aangeboden prijzen en tarieven zijn	All inclusieve tarieven en bedragen

	tevens inclusief overige belastingen en/of heffingen. De prijzen dienen gesteld te zijn in euro's. Het indienen van irreële of manipulatieve prijzen, negatieve, prijzen van 0 euro zijn niet toegestaan.	
FIN2	Jaarlijks vindt (indicatieve) bijstelling plaats op basis van de verwachtingen aan de kant van de Opdrachtgever van de aantallen gebruikers die onderdeel uit zullen gaan maken van het gebruik van de dienstverlening. Deze vormt dan de grondslag voor de nieuwe maandelijkse termijn bedragen. Indien er op basis van een "fixed price", wordt aangeboden, dan is deze eis niet van toepassing.	Aantallen gebruikers
WENS	Maandelijks, achteraf, kan 1/12 van de jaarlijkse operationele kosten (lees beheer/onderhoud) voor de dienstverlening gefactureerd worden. Dit nadat de implementatefase is afgerond en de Opdrachtgever de ICT Prestatie heeft geaccepteerd.	Uw reactie
WENS	Verrekening van de initiële Meerwerk kosten vindt plaats nadat de desbetreffende ICT Prestatie door Opdrachtgever definitief is geaccepteerd. Beheer/onderhoudskosten welke naar aanleiding van Meerwerk ontstaan, worden pas aan het begin van het nieuwe jaar in rekening gebracht.	Uw reactie
FIN3	Aanpassingen, leveringen of installatiewerkzaamheden die niet uitgevraagd zijn en afgeprijsd zijn in het Prijzenblad zullen via de Projectopdracht op basis van een open kostencalculatie schriftelijk worden vastgelegd en afgesproken. In het Prijzenblad wordt een daartoe uurtarief uitgevraagd voor (software)enginering en Opdracht gerelateerde consultancy.	Aanpassingen
FIN4	Facturen dienen te voldoen aan de wettelijke vereisten (zie www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/btw/administratie_bijhouden/facturen_maken/factuureisen)	Facturatie
FIN5	Facturatie vindt plaats op basis van de in het prijzenblad opgenomen tarieven.	Facturatie
	De factuur dient minimaal de navolgende informatie te bevatten: a. Contact- en betalingsgegevens van Opdrachtnemer; b. Unieke factuurnummer en factuurdatum; c. Proq-nummer, referentie- en/of projectnummer; d. Omschrijving levering; e. Het betreffende bedrijfsonderdeel en contactpersoon; f. De locatie en kostenplaats (deze worden vooraf opgegeven door de Opdrachtgever); g. Overzicht bestelde/geleverde producten; h. Totaalbedrag met specificatie kosten van de geleverde producten; i. Datum van levering.	Facturatie

Licentiebeheer		
LIC1	De aangeboden oplossing bevat een flexibel en schaalbaar licentiemodel inzake het aantal gebruikers dat periodiek zowel naar boven als naar beneden bij te stellen is op basis van actuele behoefte. De aangeboden oplossing moet volledig blijven werken indien er niet voldoende licenties zijn geactiveerd of wanneer de aanwezige licenties zijn verlopen.	Licentiemodel
LIC2	Leverancier verplicht zich tot gedurende de gehele contractuele periode de Opdrachtgever te voorzien in ondersteuning, updates en upgrades. Ook na beëindiging is de applicatie ten behoeve van overdracht naar een ander pakket minimaal 6 maanden beschikbaar	Updates en upgradese
LIC3	Bij implementatie van nieuwe software, zal de subscriptie of support pas na implementatie en acceptatie door Opdrachtgever ingaan.	Ingangsdatum subscriptie
LIC4	Indien door opdrachtgever geaccepteerd: de oorspronkelijke Terms & Conditions van de benoemde software blijven ook van toepassing als Opdrachtgever gebruik maakt van upgrades naar hogere versies; het accepteren van (nieuwe) terms en condities is nimmer van toepassing.	Voorwaarden
LIC5	De Leverancier is verantwoordelijk voor de correcte en rechtmatige naleving van de licentieverplichtingen voor het gebruik van software van derden.	Software van derden
LIC6	Licenties zijn softwarematig (geen hardwaredongle via USB bv) ook niet in werkstations	Softwarematige licenties
WENS	Op eerste verzoek van Opdrachtgever zal Opdrachtnemer een escrow regeling voor de broncode van alle programmatuur afsluiten . Dit geldt ook voor toegepaste API's. Opdrachtgever is gerechtigd bij deze escrow regeling aan te sluiten. Dit geldt ook indien Opdrachtnemer voor haar Systeemprogrammatuur ten behoeve van een andere partij een escrow regeling afsluit, voor zover deze programmatuur ook aan Opdrachtgever is aangeboden. Opdrachtnemer verklaart deze escrow regeling naar behoren na te leven en de in escrow gegeven broncode up to date te houden.	Uw reactie
Exit		
EX1	Inschrijver dient als onderdeel van zijn aanbieding een Exit Plan op te leveren waarin onder meer wordt aangegeven dat Inschrijver op het einde van de opdracht medewerking verleent aan de overdracht aan de Opdrachtgever dan wel de door de Opdrachtgever aan te wijzen partij. De eventuele kosten van de exit dienen in het Prijzenblad vermeld te worden.	Exit plan

EX2	De Inschrijver draagt zorgt voor de overdracht van de gegevens in bruikbare formaten aan de Opdrachtgever, dan wel aan een nieuwe leverancier na opdracht hiervoor door de Opdrachtgever en levert een verklaring aan waarin de leveranciers aantoont dat alle data is vernietigd.	Vernietiging van data
EX3	De Leverancier is verantwoordelijk voor het opstellen van een Retransitieplan na het beëindigen van de overeenkomst	Retransitieplan
EX4	Opdrachtgever stelt in samenspraak met leverancier een decharge document op waarin wordt vastgelegd hoe de exit eruit ziet en wat er over en weer wordt gevraagd teneinde een goede afronding van het contract te bewerkstelligen	Decharge
Forum Standaardisatie		
WENS	De domeinnaam van het ICT-systeem biedt volledig werkende ondersteuning voor de Open Standaard DNSSEC – zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie – of daaraan gelijkwaardig. Dit betekent dat de domeinnaaminformatie, zoals bijbehorende IP-adressen, met een geldige DNSSEC handtekening is ondertekend.	Uw reactie
WENS	De opvragende DNS-software (resolver) biedt volledig werkende ondersteuning voor validatie c.q. verificatie van handtekeningen conform de Open Standaard DNSSEC -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent dat de DNSSEC-handtekeningen van opgevraagde domeinnamen worden gevalideerd.	Uw reactie
WENS	De e-mailvoorziening biedt volledig werkende ondersteuning voor DKIM versie 1 – zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie – of daaraan gelijkwaardig. Dit betekent dat: 1. op het systeem een publiek/privaat sleutelpaar is gegenereerd of kan worden gegenereerd; 2. de publieke DKIM-sleutel is gepubliceerd in de DNS van de e-maildomeinnaam; 3. alle uitgaand e-mailberichten worden ondertekend met de private DKIM-sleutel; 4. alle inkomende e-mailberichten worden gecontroleerd op de geldigheid van een eventuele DKIM-handtekening en het systeem hieraan mogelijke acties verbindt.	Uw reactie
WENS	De e-mailvoorziening biedt volledige ondersteuning voor de Open Standaard SPF versie 1 – zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie – of daaraan gelijkwaardig. Dit betekent dat: 1. de IP-adressen van de verzendende systemen als SPF-record worden geregistreerd in de DNS van de verzendende domeinnaam; 2. alle inkomende e-mailberichten worden gecontroleerd op de geldigheid van het verzendend IP-adres tegen het IP-adres dat in SPF-record staat van de verzendende domeinnaam.	Uw reactie

WENS	Het te leveren ICT-systeem (bijv. webapplicatie) kan documenten genereren/beheren/publiceren in een formaat conform de Open Standaard PDF/A – zoals opgenomen op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie – of daaraan gelijkwaardig. 2. Met het te leveren kantoorsoftwarepakket kan de gebruiker documenten bekijken en/of creëren in een formaat conform de Open Standaard PDF/A -zoals opgenomen op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. 3. Met de te leveren multi-functional kan de gebruiker scans maken en vastleggen in een formaat conform de Open Standaard PDF/A -zoals opgenomen op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie- of daaraan gelijkwaardig.	Uw reactie
WENS	Het te leveren ICT-systeem (bijv. webapplicatie) kan documenten genereren/tonen/beheren/publiceren in een formaat conform de Open Standaard PDF1.7 -zoals opgenomen op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. 2. Met het te leveren kantoorsoftwarepakket kan de gebruiker documenten bekijken en/of creëren in in een formaat conform de Open Standaard PDF1.7 – zoals opgenomen op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie – of daaraan gelijkwaardig. 4. Met de te leveren multi-functional kan de gebruiker scans maken en vastleggen in een formaat conform de Open Standaard PDF1.7 -zoals opgenomen op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie- of daaraan gelijkwaardig.	Uw reactie
WENS	Het te leveren ICT-systeem (bijv. webapplicatie) kan documenten genereren/tonen/beheren/publiceren in ODF versie 1.2 –zoals opgenomen op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. 2. Met het te leveren kantoorsoftwarepakket kan de gebruiker documenten bekijken en/of creëren in een formaat conform de Open Standaard ODF versie 1.2 – zoals opgenomen op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie – of daaraan gelijkwaardig. 3. Met de te leveren multi-functional kan de gebruiker scans maken en vastleggen in een formaat conform de Open Standaard ODF versie 1.2 – zoals opgenomen op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie – of daaraan gelijkwaardig.	Uw reactie
FOR1	Inschrijver conformeert zich aan de Open Standaarden van Forum Standaardisatie voor: - authenticatie, autorisatie en identificatie; - veilige verbindingen; - veilige berichten- en/ of bestandsuitwisseling; - metadatering; - digitale bestandsformaten. Zie: https://www.forumstandaardisatie.nl/	Forum
FOR2	De op te leveren website voldoet aantoonbaar aan alle A-, en AA- succescriteria van de Open Standaard Webrichtlijnen versie 2 – zoals opgenomen op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie – of daaraan gelijkwaardig.	