



BIJLAGE A SPECIFICATIE VAN DE OPDRACHT

Europese aanbesteding

“API Management Oplossing”

Versie : 1.1
Kenmerk : IUC24-019
Datum : 22-05-2025

INHOUDSOPGAVE

Hoofdstuk 1. Inleiding	3
Hoofdstuk 2. Functionals	4
Hoofdstuk 3. IV kaders	19
Hoofdstuk 4. Business Etiquette	42
Hoofdstuk 5. Maatschappelijk Verantwoord Inkopen (MVI)	43
5.1. Milieu	43
5.2. Ketenverantwoordelijkheid (ISV)	43
Hoofdstuk 6. Juridische kaders	45
Hoofdstuk 7. Prijsstelling	46
7.1. Algemene eisen ten aanzien van Prijzen	46
7.2. Toelichting Prijscomponenten in Bijlage VII "Prijzenformulier"	46
7.3. Specifieke eisen ten aanzien van Prijzen	48
7.4. Indexering Prijs	49
Hoofdstuk 8. Documentatie, Opleiding en Consultancy	51
8.1. Documentatie	51
8.2. Opleiding	51
8.3. Consultancy	53
Hoofdstuk 9. Voorbereiding- en Implementatiefase	54
9.1. Voorbereiding	54
9.2. Implementatie	54
9.3. Documentatie, Opleiding en Consultancy	54
Hoofdstuk 10. Operationele fase	55
10.1. Onderhoud en Support	55
10.2. Documentatie, Opleiding en Consultancy	66
10.3. Factureren en bestellen	66
10.4. Kaders voor (re)transitie	67

Hoofdstuk 1. Inleiding

Dit document beschrijft de eisen en wensen die de Aanbestedende dienst stelt in het kader van de Europese aanbesteding met kenmerk IUC24-019 “API Management”. Dit document maakt integraal onderdeel uit van het Beschrijvend Document.

Hoofdstuk 2. Functionals

2.1 Functionele Eisen

Taal

GUE 1.	De Inschrijving en alle overige informatie dient volledig in het Nederlands en/of Engels taal te zijn geformuleerd.
--------	---

Generiek Interface

GUE 2.	De Oplossing ondersteunt een Graphical User Interface (hierna: GUI) waarin in real time, validatiemeldingen en gebruikersfouten worden getoond bij het maken en aanpassen van een API.
--------	--

GUE 3.	De Oplossing biedt een rol gebaseerde gebruikersinterface, waarmee Gebruikers vanuit de Opdrachtgever en (externe) API-Consumers direct toegang hebben tot taken en informatie die voor de betreffende Gebruikers relevant zijn.
--------	--

W1	GUI en gebruiksvriendelijkheid Gebruikersgemak is een belangrijke pijler voor het dagelijks (goed) gebruik van de Oplossing. Daar ondersteund de GUI van de Oplossing in en daarom wenst de Opdrachtgever een GUI die intuïtief werkt. Vraag Geef van alle handelingen, doormiddel van screenshots, beschrijvingen en invoervalidaties in de GUI aan, dat deze intuïtief werkt. Doe dit op basis van het creëren van een API-product conform Open API Specificatie 3 (OAS3). We beoordelen of een GUI intuïtief werkt als blijkt dat uit de aangeleverde screenshots en omschrijvingen: 1. <u>De bediening van de GUI consequent is.</u> - Termen, menu's, pictogrammen en knoppen komen overeen met de functie die een Gebruiker ervan verwacht (wat logisch is, dus de synchronisatie knop is synchroniseren) en hebben in alle gevallen een gelijke betekenis = 2 punten. Indien niet of slechts gedeeltelijk dan krijgt u geen (o) punten. 2. <u>Uit de screenshots en omschrijving blijkt dat de Navigatie door het systeem en de werkvolgorde logisch in elkaar zit.</u> Hiermee bedoelen we dat de Gebruiker moet kunnen zien waar deze zich bevindt. Allerlei omwegen en noodgedwongen “trucs” moeten niet nodig zijn. <i>Bijvoorbeeld:</i> als een gebruiker in een bepaalde module zit, dan moet de gebruiker ook op een intuïtieve en logische wijze weer terug kunnen d.m.v. bijvoorbeeld een knop “terug”, zodat de gebruiker weer in het hoofdmenu terugkomt= 2 punten. Indien niet of slechts gedeeltelijk dan krijgt u geen (o) punten. 3. <u>Invoer validatie wordt per invoerveld of per schermovergang verwerkt.</u> In het geval van validatiefouten vinden er meldingen plaats= 3 punten. Indien niet of slechts gedeeltelijk dan krijgt u geen (o) punten.
----	--

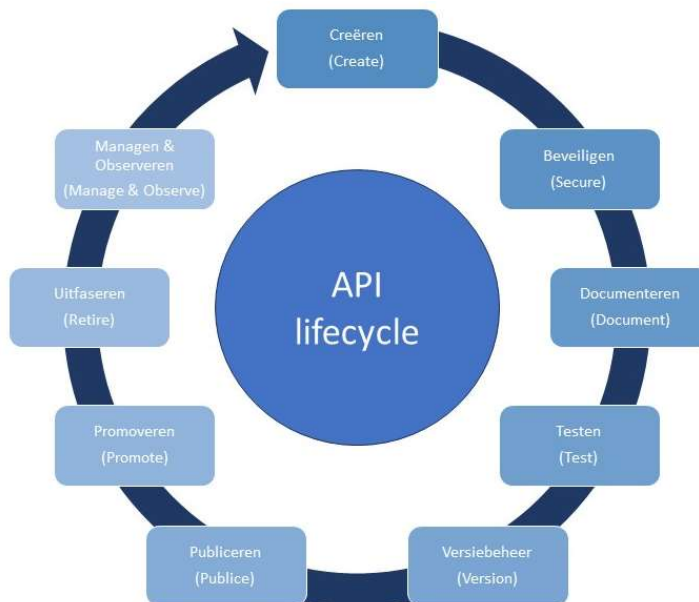
	U krijgt per bovenstaand genoemde mogelijkheid het benoemde aantal punten. Blijkt uit de beantwoording dat de GUI alle drie de bovengenoemde intuïtieve mogelijkheden bezit (of zelfs meer), dan krijgt u 2+2+3=7 punten, blijkt uit het antwoord dat de GUI geen één van bovenstaande intuïtieve mogelijkheden heeft dan krijgt u 0 punten. Uw uitwerking inclusief leesbare screenshot (hyperlinks worden niet beoordeeld en minimaal 800x600 pixels) is maximaal 5 pagina's A4 (Lettertype Arial, lettergrootte 10 en regelafstand 1,0), dient u de bovenstaande onderwerpen per punt uit te werken. Het maximum aantal te behalen punten voor deze Wens is 7 punten
--	---

Zoeken

GUE 4.	De Oplossing biedt de mogelijkheid om API-Gegevens te zoeken in alle beschikbare zoekvelden (query), waarbij het mogelijk is om selectiefilters gecombineerd in te stellen.
GUE 5.	De Oplossing biedt de mogelijkheid om op basis van reguliere expressies te zoeken in API-Gegevens. Gebruikers kunnen zoektermen gebruiken. De functie doorzoekt vervolgens op basis van filtering op alle API-Gegevens op het betreffende woord, deel van het woord of combinatie van woorden.

API lifecycle

Als "kapstok" voor de andere functionele eisen en wensen heeft de Opdrachtgever er voor gekozen om de processtappen van de volgende API lifecycle cirkel te gebruiken:



Figuur 1

GUE 6.	De Oplossing ondersteunt het managen van een API lifecycle door ten minste de volgende functionaliteiten te ondersteunen: - creëren; - beveiligen;
--------	--

	- documenteren; - testen; - versiebeheer; - publiceren; - promoveren; - uitfasen; - managen en observeren.
--	--

W 2	Connectiviteit De Opdrachtgever wenst een Oplossing die past binnen haar Informatie Voorziening (IV) voortbrengingsketen en de automatisering van IV processen ondersteund. Het is de bedoeling dat met de Oplossing, op een gestandaardiseerde en efficiënte manier, veilige API's worden gecreëerd en het Lifecyclemanagement hierop wordt uitgevoerd. Vraag De Opdrachtgever wenst op vijf (5) technisch beheer aspecten puntsgewijs een omschrijving en toelichting in hoeverre de Beheer API voorziet in de ondersteuning van: 1. het deployment proces; (het kunnen publiceren en/ of stagen van een API) 2. het Lifecycle Management (LCM) proces; (paragraaf 2.5.1 Beschrijvend document) 3. Koppelbaarheid; 4. Gebruiksgemak; 5. Documentatie. Beoordelingscriteria 1. Deployment. Uit de beantwoording blijkt dat de Oplossing: ▪ het deployment proces via de Beheer API ondersteund; (1 punt) ▪ Security constraints kan aanpassen; (1 punt) ▪ API testen ondersteund; (1 punt) ▪ mogelijkheden heeft voor updates, fixes en herstel; (1 punt) Indien alle bovengenoemde technisch beheer aspecten door de Oplossing worden ondersteund dan krijgt u 2 punten extra (6 punten in totaal). 2. LCM Proces. Uit de beantwoording blijkt dat de Oplossing: ▪ alle LCM proces stappen (conform figuur 1) ondersteund; (1 punt) ▪ CRUD (Create, Read, Update, Delete) + backwards/forwards capabilities heeft; (1 punt) ▪ Retirement/notification ondersteund; (1 punt) ▪ Het toekennen van rechten ondersteund op een (versie van) specifieke API; (1 punt) Indien alle bovengenoemde aspecten door de Oplossing worden ondersteund dan krijgt u 2 punten extra (6 punten in totaal).
------------	--

	3. Koppelbaarheid. Uit de beantwoording blijkt dat de Oplossing als volgt kan koppelen met andere systemen: a. Aansluiten. (4 punten), kan dit niet is, 0 punten b. Ontsluiten. (4 punten), kan dit niet is, 0 punten 4. Gebruikersgemak. Uit de beantwoording blijkt of gebruikersgemak van API's voldoet aan standaarden en logische indeling: ▪ geen standaard RESTful API's. (0 punten) ▪ standaard RESTful API's. (2 punten) 5. De kwaliteitstandaard van de API Documentatie. Uit de beantwoording blijkt dat: ▪ Deze niet conform OAS3.x opgemaakt is (0 punten) ▪ Conform OAS3.X is opgemaakt (2 punten) In uw uitwerking, maximaal 2 pagina's A4 (Lettertype Arial, lettergrootte 10 en regelafstand 1,0), dient u de bovenstaande onderwerpen per punt uit te werken. Het maximum aantal te behalen punten voor deze Wens is 24 (6 + 6 + 8 + 2 + 2)..
--	---

API Creëren (Create)

Het is de bedoeling dat met de Oplossing APIs kunnen worden gecreëerd.

GUE 7.	De Oplossing ondersteunt dat daartoe gerechtigde Gebruikers hun API's kunnen creëren en onderhouden.
GUE 8.	De Oplossing ondersteunt het Consumeren van externe aangeboden API's van buiten de organisatie, door aanbieden van interne gerichte API's binnen de organisatie.
GUE 9.	De Oplossing ondersteunt het transformeren van API-berichten van JSON naar XML, voordat het verkeer naar backend systemen wordt doorgestuurd.
GUE 10.	Een daartoe gerechtigde Gebruiker dient in de API ten minste het volgende te kunnen configureren: - Rate Limiting, - Throttling en - Caching.
GUE 11.	De Oplossing ondersteunt minimaal de onderstaande communicatievormen: - REST - SOAP - GraphQL - WebSocket - gRPC
W 3	Traffic management vormen Throttling, caching en rate limiting zijn capabilities die vereist zijn. Er zijn Oplossingen in de markt die hierin meer of minder configuratie mogelijkheden bieden. Hoe fijnmaziger de configuratie kan worden toegepast, hoe beter een Oplossing past bij de behoefte vanuit de Opdrachtgever.

Zo zijn er bijvoorbeeld technieken zoals Rate Limiting, Throttling, Caching, Quota Management, Load Balancing, IP Whitelisting/Blacklisting, Spike Arrest, Traffic Shaping, Burst limiting en circuit breaker. Voor de Opdrachtgever zijn de verschillende vormen en/of de fijnmazigheid van configuratie mogelijkheden van deze technieken, per API, per API Consumer, of API Consumer groep van belang.

De Opdrachtgever ziet de volgende vormen van traffic management voor zich:

- **Rate Limiting:** Hiermee kun je het aantal verzoeken beperken dat een client binnen een bepaalde tijdsperiode kan doen. Dit helpt om overbelasting van de API te voorkomen.
- **Throttling:** Dit is vergelijkbaar met rate limiting, maar in plaats van verzoeken te blokkeren, worden ze vertraagd. Dit kan nuttig zijn om pieken in het verkeer te beheeren zonder verzoeken volledig af te wijzen.
- **Caching:** Door antwoorden op veelvoorkomende verzoeken tijdelijk op te slaan, kan caching helpen om de belasting op de backend servers te verminderen en de responstijd te verbeteren.
- **Quota Management:** Hiermee kunnen limieten ingesteld worden op het totale aantal verzoeken dat een client gedurende een bepaalde periode kan doen. Dit kan op dagelijkse, maandelijkse of jaarlijkse basis zijn.
- **Load Balancing:** Dit verdeelt het inkomende verkeer gelijkmatig over meerdere servers om ervoor te zorgen dat geen enkele server overbelast raakt.
- **IP Whitelisting/Blacklisting:** Hiermee kan de toegang tot de API worden beperkt tot bepaalde IP-adressen of IP-adressen blokkeren die verdacht verkeer genereren.
- **Spike Arrest:** Dit helpt om plotselinge pieken in het verkeer te beheersen door een maximum aantal verzoeken per seconde in te stellen.
- **Traffic Shaping:** Hiermee kun je het verkeer sturen op basis van bepaalde criteria, zoals het type client of de geografische locatie.
- **Burst Limiting:** Dit stelt een API in staat om een korte periode van verhoogd verkeer te verwerken door tijdelijk hogere limieten toe te staan. Na deze burst periode wordt het verkeer weer beperkt tot de normale limieten. Dit helpt om tijdelijke pieken in het verkeer te beheeren zonder dat gebruikers direct worden geblokkeerd.
- **Circuit breaker:** Grijpt in bij aanhoudende problemen bij verkeer naar backend systemen, op basis van ingestelde configuratiewaarden, om onnodig verkeer en daarmee belasting te voorkomen. Gebruikt informatie over het verkeer om te controleren wanneer berichten weer correct verwerkt kunnen worden, of geeft direct een exceptie wanneer er nog fouten optreden.

Vraag

1. Geef aan in hoeverre uw aangeboden Oplossing deze vormen van traffic management ondersteund;

	2. Omschrijf en toon de mate van schaalbaarheid aan van de door u aangegeven traffic management vormen die uw Oplossing ondersteunen. Bijvoorbeeld over meerdere fysieke locaties heen, met hoge load (mimimaal 1600 API Calls per seconde). 3. Geef aan op welke niveaus uw Oplossing (fijnmazige) configuratie mogelijkheden van de verschillende vormen van traffic management ondersteund per API, Gateway instantie en/of Consumer. Beoordeling 1. De traffic management vormen die de aangeboden Oplossing ondersteund zijn omschreven: ▪ <5 traffic management vormen = 0 punten; ▪ >= 5 traffic management vormen = 2 punten. 2. De mate van schaalbaarheid van de door u aangegeven traffic management vormen die uw Oplossing ondersteunen zijn omschreven: ▪ 1 gateway instantie = 0 punten; ▪ >1 gateway instantie, met hoge load (mimimaal 1600 API Calls per seconde) = 4 punten. 3. Omschreven is op welke niveaus (mate van fijnmazigheid) de Oplossing configuratie mogelijkheden van de verschillende vormen van traffic management ondersteund per API, Gateway instantie en/of Consumer. ▪ De Oplossing kan niet per API, Gateway instantie en/of Consumer (Fijnmazige) configuratie mogelijkheden van de verschillende vormen ondersteunen = 0 punten ▪ De Oplossing kan per API, Gateway instantie en/of Consumer (Fijnmazige) configuratie mogelijkheden van de verschillende vormen ondersteunen = 4 punten In uw uitwerking, maximaal 1 pagina's A4 (Lettertype Arial, lettergrootte 10 en regelafstand 1,0), dient u de bovenstaande onderwerpen per punt uit te werken. Het maximum aantal te behalen punten voor deze Wens is 10 punten (2+4+4).
--	--

API Beveiligen (Secure)

Om API's te beschermen en veilig te kunnen beheren dient de Oplossing diverse beveiligingsfunctionaliteiten te hebben.

Het is de bedoeling dat autorisaties zo fijnmazig mogelijk kunnen worden ingeregeld.

GUE 12.	De Oplossing voorziet in Role Based Access (RBAC).
GUE 13.	De Oplossing biedt de mogelijkheid (voor functiescheiding en datascheiding) om door middel van autorisaties rechtendifferentieatie in te richten op basis van autorisatiegroepen en rollen. Voor datascheiding is daarbij mogelijk om in ieder geval onderscheid te maken tussen de volgende rechten: - lees-,

	- maak-, - wijzig- en - verwijderrechten.
GUE 14.	De Opdrachtgever kan zonder tussenkomst van de Opdrachtnemer autorisatiegroepen en rollen in de Oplossing toevoegen, wijzigen of verwijderen via een daartoe geautoriseerde Gebruiker.
GUE 15.	Daartoe geautoriseerde Gebruikers dienen Gebruikers te kunnen bundelen tot groepen Gebruikers (teams).
GUE 16.	Afhankelijk van de autorisatie heeft de Gebruiker inzage tot alle of een deel van de informatie in de Oplossing.
GUE 17.	De Oplossing moet de mogelijkheid hebben om opties te verbergen die Gebruikers niet mogen of moeten gebruiken op basis van hun rol of op basis van configuratie van de gebruikers portalen.
GUE 18.	De Oplossing ondersteunt het beheer van toegangsrechten en autorisaties voor het gebruik van API's door Consumer-applicaties.
GUE 19.	De Oplossing ondersteunt ten minste OAuth2.0.
GUE 20.	De Oplossing ondersteunt OpenID Connect.
GUE 21.	De Oplossing ondersteunt het proces van rechten aanvragen, verstrekken én intrekken aan API Consumers.
GUE 22.	De Oplossing voorziet in het geautomatiseerd valideren van APIs én API verkeer (payload) op basis van OpenAPI Specificaties (OAS).
GUE 23.	De Oplossing moet aansluiten bij een mechanisme voor Identity Propagation en token kunnen doorgeven aan back-end systemen.
GUE 24.	Oplossing garandeert dat ongeautoriseerde wijzigingen niet kunnen plaatsvinden.
W 4	Configureerbaarheid van logische scheiding De Opdrachtnemer wenst de workload van de API Gateway's logisch te kunnen scheiden door de juiste inrichting met betrekking tot rechten en isolatie. De mate van logische scheiding en het gemak van het beheren van meerdere omgevingen is hierbij onderscheidend (dit staat los van GUE 13). De Opdrachtnemer wenst op de volgende punten fijnmazigheid van de configuratie mogelijkheden: 1. indelingen en bijbehorende configuraties/opties; 2. configuratie van API provider groepen;

	3. configuratie voor het opdelen van API gateways. Vraag Beschrijf in hoeverre en op welke wijze de Oplossing configuratie mogelijkheden biedt op basis van bovenstaande drie punten. Hoe meer configuratie mogelijkheden er zijn per punt, hoe meer punten worden toegekend. Beoordeling Uit de beantwoording blijkt hoeveel configuratiemogelijkheden dit per genoemd punt kan. 1) Configuratiemogelijkheden van indelingen en bijbehorende configuraties/opties in relatie tot workload: a) Tot en met 3 configuratie mogelijkheden/ opties omschreven en toegelicht: 0 punten b) Meer dan 3, maar minder dan 6 configuratie mogelijkheden omschreven en toegelicht: 2 punten c) Meer dan 5 configuratie mogelijkheden omschreven en toegelicht: 5 punten 2) De hoeveelheid aan mogelijke hoofdgroepen van configuratie van API-provider groepen: a) Geen hoofdgroep configuratie omschreven en toegelicht: 0 punten b) Hoofdgroep configuratie omschreven en toegelicht: 2 punten c) Subhoofdgroepen configuratie omschreven en toegelicht: 3 punten d) Uw antwoordt verrast ons positief op basis van configuratiemogelijkheden van API-provider groepen anders hierboven genoemde <u>ad b</u> en <u>ad c</u> die voor de Opdrachtgever van toegevoegde waarde zijn: 5 punten 3) De hoeveelheid aan mogelijkheden van configuratie voor het opdelen van verschillende API-Gateway instanties: a) Geen runtime aanpassingen van de configuratie van meerdere API-Gateways mogelijk omschreven en toegelicht: 0 punten. b) Het runtime (zonder downtime) configureren van meerdere API-Gateways met verschillende instellingen omschreven en toegelicht: 3 punten. c) Het runtime (zonder downtime) configureren van meerdere API-Gateways met verschillende instellingen, en het dynamisch (als vanzelf) reageren op wijzigingen omschreven en toegelicht: 5 punten. In uw uitwerking, maximaal 1 pagina's A4 (Lettertype Arial, lettergrootte 10 en regelafstand 1,0), dient u de bovenstaande 3 onderwerpen puntsgewijs uit te werken. Het maximum aantal te behalen punten voor deze Wens is 15 punten (5+5+5)

API Documenteren (Document)

- | | |
|---------|--|
| GUE 25. | In de Oplossing dienen specifiek de documentatie elementen van de OAS 3.x specificatie te kunnen worden beheerd. |
|---------|--|

API Testen (Test)

Het is de bedoeling dat daartoe gerechtigde gebruikers in staat zijn om de kwaliteit, prestaties en betrouwbaarheid van API's te testen in een geïsoleerde omgeving met de oplossing.

- | | |
|---------|---|
| GUE 26. | De Oplossing biedt de mogelijkheid om de API en bijbehorende configuratie met de Oplossing te testen. |
|---------|---|

API Versiebeheer (Version)

Met versiebeheer functionaliteit binnen de Oplossing dient meerdere versies van een API naast elkaar te kunnen worden beheert en aangeboden.

Zodoende kan de Opdrachtgever haar API's laten evolueren, zonder dat bestaande Consumers worden verstoord.

- | | |
|---------|---|
| GUE 27. | Om API versies bij te houden dient de Oplossing semantic versioning (SemVer standaard) te ondersteunen. |
|---------|---|

- | | |
|---------|---|
| GUE 28. | Om de compatibiliteit te waarborgen terwijl de API evolueert dient de Oplossing: <ul style="list-style-type: none">- het beheren van verschillende versies van een API te ondersteunen;- minimaal de voorgaande versie en de huidige versie van de API aan te kunnen bieden. |
|---------|---|

API Publiceren (Publish)

Met publicatie functionaliteit van de Oplossing dient de Opdrachtgever haar API's effectief beschikbaar te kunnen stellen aan haar Consumers, terwijl zij de controle behoudt over toegang en gebruik van de API's.

- | | |
|---------|--|
| GUE 29. | De Oplossing ondersteunt dat daartoe gerechtigde Gebruikers API's kunnen publiceren. |
|---------|--|

- | | |
|---------|--|
| GUE 30. | De Oplossing ondersteunt het kunnen instellen en configureren van een API publicatie met een Beheer-API. |
|---------|--|

Toegang tot API Discovery

- | | |
|---------|--|
| GUE 31. | De Oplossing ondersteunt API Discovery voor API-Consumers. |
|---------|--|

- | | |
|---------|---|
| GUE 32. | De Oplossing ondersteunt de mogelijkheid om de API als private of als public te publiceren. |
|---------|---|

- | | |
|---------|---|
| GUE 33. | De Consumer vereisten voor toegang tot inzage in API's moeten configureerbaar en instelbaar zijn. |
|---------|---|

- | | |
|---------|---|
| GUE 34. | De Oplossing ondersteunt een publicatieomgeving voor API's waarin het mogelijk is de stijl van de user interface aan te passen. |
|---------|---|

API Promoveren (Promote)

Met de promoveer functionaliteit dient de Opdrachtgever API's gestructureerd en gecontroleerd API's te kunnen migreren tussen verschillende omgevingen in een ontwikkelcyclus. Bijvoorbeeld van een ontwikkel- naar een test- naar een productieomgeving of binnen een omgeving an sich.

GUE 35.	De Oplossing heeft een geïntegreerde ontwikkelaarsportaal (developersportal). Daartoe geautoriseerde Gebruikers dienen ten minste: - API-specificaties te kunnen raadplegen (lezen, sorteren, zoeken); - API-toegangssleutels te kunnen verkrijgen; - API's te kunnen uitproberen en testen.
GUE 36.	De Oplossing ondersteunt dat tijdens het promoveren alle relevante configuratieinstellingen, policies en documentatie worden meegenomen naar de, hierboven genoemde (nieuwe) omgeving
GUE 37.	De Oplossing geeft inzicht en overzicht aan daartoe gerechtigde Gebruikers welke API-versies in welke omgevingen actief zijn.

API Uitfaseren (Retirement)

Met de API uitfaseer functionaliteit dient de Oplossing op een gecontroleerde en gestructureerde manier een API uit gebruik te nemen.

GUE 38.	De Oplossing ondersteunt het geleidelijk en/of gefaseerd buitengebruik stellen van API's.
GUE 39.	De Oplossing moet kunnen notificeren over ten minste: - API deprecation; - API termination.

API Managen & Observeren (Manage & Observe)

De API managen & observeren functionaliteit gaat om de managen van het de gehele levenscyclus van een API en om het monitoren, analyseren, loggen en kunnen auditen daarvan.

GUE 40.	De Oplossing ondersteunt het real time kunnen monitoren van het API verkeer en de API prestatie ten minste op: - aantal calls; - snelheid; - foutmeldingen.
GUE 41.	De Oplossing ondersteunt het kunnen loggen van het API verkeer en de API prestatie ten minste op: - aantal calls; - snelheid; - foutmeldingen.
GUE 42.	De Oplossing voorziet in een configureerbaar Dashboard van API statistieken waarin ten minste: - aantal calls;

	- snelheid; - foutmeldingen over een instelbare periode van tijd worden weergegeven.
--	--

GUE 43.	Het is mogelijk om op basis van autorisaties onderscheid te maken in het niveau van de informatie die in het Dashboard wordt gepresenteerd, bijvoorbeeld op het niveau van afdeling, gebruikersgroepen en individuele gebruikers.
---------	---

GUE 44.	In het geval dat er fouten optreden in de API's ondersteunt de Oplossing bij foutafhandeling gericht op het identificeren, beheren en reageren op fouten.
---------	---

GUE 45.	De Oplossing ondersteunt de open standaard OpenTelemetry.
---------	---

W 5	Governance via een totaaloverzicht en inzicht van alle API's Ten behoeve van governance van de Opdracht is het belangrijk om overzicht en inzicht te hebben in het geheel van alle API's. Het is van meerwaarde dat de Oplossing voorziet in een API overzicht via een GUI of via een Beheer-API. Vraag Uit uw beantwoording blijkt dat de aangeboden Oplossing de volgende mogelijkheden biedt: • Totaal inzicht van alle API's van het gehele APIM landschap • Totaal overzicht gebruik en gebruikers van het gehele APIM landschap Beoordeling In het antwoordt blijkt dat: • geen van beide mogelijkheden door de Oplossing wordt ondersteund = 0 punten • het totaal inzicht van de API's van het gehele APIM landschap kan worden weergegeven = 3 punten • het totaal overzicht van het gebruik en de gebruikers van het gehele APIM landschap = 4 punten In uw uitwerking, maximaal halve (0,5) pagina's A4 (Lettertype Arial, lettergrootte 10 en regelafstand 1,0), dient u de bovenstaande mogelijkheden puntsgewijs uit te werken. Het maximum aantal te behalen punten voor deze Wens is 7 punten
------------	---

2.2 Realisatie fase, Operationele fase, Afrekenmethode

2.2.1 Omgevingen

De Realisatie bestaat uit een hybride oplossing met twee hosting omgevingen, namelijk: on-premises en off-premises.

Verschillende componenten landen op de ene of de andere hosting omgeving. Voor de off-premises componenten zorgt de Opdrachtnemer voor een complete inrichting conform de eisen uit de aanbesteding, deze onderdelen worden hieronder verder aangeduid met de term SaaS onderdelen. Voor de on-premises componenten zorgt de Opdrachtgever voor een hosting omgeving met connectie tot het internet waarop de componenten kunnen worden uitgerold.

Om inzicht te krijgen op welke wijze de Opdrachtnemer de Realisatie uit gaat voeren, wordt een Plan van Aanpak (PvA) gevraagd aan de Opdrachtnemer. Het PvA heeft betrekking op Realisatie, livegang en het in beheer nemen van de Oplossing. Dit PvA wordt door Opdrachtgever beoordeeld. In het PvA dient rekening te worden gehouden dat de Oplossing uiterlijk op **01-10-2026** is gerealiseerd, in productie staat en is geaccepteerd.

Het heeft de voorkeur dat de processen conform 'best practice' worden aangeboden en nader geconfigureerd worden ten einde passend te zijn voor de Opdrachtgever. Met de Oplossing dient de continuïteit en kwaliteit van de dienstverlening van de Opdrachtgever gewaarborgd te zijn.

GUE 46.	De Opdrachtnemer levert bij Inschrijving een Plan van Aanpak voor de Realisatie van de Oplossing bij de Opdrachtgever aan en behandelt daarin de 12 onderwerpen zoals deze in de Wens 6 Implementatieplan en ondersteuning zijn omschreven.
---------	---

UE.1	De datum voor het in gebruik nemen van de Oplossing is uiterlijk 01-10-2026.
------	--

W 6	Implementatieplan en ondersteuning Opdrachtgever wenst een beheerste Realisatie van de door Opdrachtnemer aangeboden Oplossing. De Realisatie dient als onlosmakelijk onderdeel van de aanbidding gezien te worden en projectmatig te worden uitgevoerd binnen de gestelde kaders. Opdrachtnemer wordt gevraagd een concept Plan van Aanpak (PvA) (ook wel implementatieplan) in te dienen bij haar inschrijving met betrekking tot de Realisatie fase. Het betreft een planmatige omschrijving op basis vanaf contractingang tot en met het moment waarop de laatste acceptatietest(en) worden uitgevoerd en positief zijn afgerond. Gevraagde uitwerking Opdrachtnemer wordt gevraagd om een PvA uit te werken waarin wordt beschreven op welke wijze Opdrachtnemer de Oplossing gaat realiseren. Opdrachtgever verwacht een uitwerking van de Opdrachtnemer op ten minste de volgende 12 onderwerpen:
------------	--

	1) De wijze waarop de voorgenomen Realisatie van Opdrachtnemer bijdraagt aan de scope en doelstellingen van deze Aanbesteding; 2) De projectaanpak voor de Realisatie (inclusief acceptatie) van de Oplossing; 3) Mijlpalenplanning inclusief deliverables plus verwachte inzet per rol van de Opdrachtgever; 4) Een toelichting en aanbevelingen op de Mijlpalenplanning en projectaanpak met best practices en lessons learned bij soortgelijke opdrachten en opdrachtgevers; 5) Omschrijving en toelichting op de projectorganisatie inclusief communicatie o.b.v. in te zetten medewerkers, rollen en noodzakelijke senioriteit met de voorgestelde Oplossing; Beschikbare rollen vanuit de Opdrachtgever. De volgende rollen worden onderkend binnen het projectteam Opdrachtgever: a) Projectmanager b) Solution Engineer c) Solution Architect 6) Omschrijf hoe we gaan samenwerken, betrek in uw antwoord te minste: a) locatie (fysiek en digitaal) b) manier van communiceren c) kantoortijden in overeenstemming met die van de Opdrachtgever 7) Aanpak Risicomanagement; 8) Voorgestelde maatregelen om continuïteit van dienstverlening (beschikbaarheid) te borgen tijdens de realisatiefase; Geef hierbij minimaal een RASCI-overzicht van de verantwoordelijkheden aan tussen Opdrachtgever en Opdrachtgever. 9) Randvoorwaarden/uitgangspunten ten behoeve van een succesvolle realisatie; Geef hierbij minimaal aan: a) Hoe de hoog beschikbare inrichting on-premises en off-premises eruit komt te zien. b) wat benodigd is aan resources voor de on-premises componenten. 10) Welke opleidingen (trainingen) Gebruikers van de Opdrachtgever tijdens de Realisatie dient te volgen (geef daarbij aan: waarom en hoe lang. Een duidelijke aanpak rondom het opleiden van medewerkers van de opdrachtgever); 11) Advies over welke opleidingen (trainingen) Opdrachtnemer voor Opdrachtgever noodzakelijk acht en waarom Opdrachtnemer dit vindt tijdens de Operationele fase; 12) Test- en acceptatieproces (waaronder performance en A&P testen). U dient hierbij rekening te houden met hetgeen in het beschrijvend document en haar bijlagen verwoord is. In uw uitwerking dient u de bovenstaande 12 onderwerpen puntsgewijs uit te werken.
--	---

Voorschriften uitwerking

Wij vragen uw uitwerking in maximaal **15 pagina's A4** (lettertype Arial, lettergrootte 10 en regelafstand 1,0) te verwoorden. Extra pagina's en/of hyperlinks worden niet in de beoordeling meegenomen.

De beoordelingscriteria voor deze Wens zijn:

1. Alle 12 onderwerpen zijn volledig uitgewerkt;
2. De mate waarin de 12 beschreven onderwerpen vertrouwen geeft dat:
 - a. de Realisatie soepel verloopt;
 - b. en dat de testen in het kader van de acceptatie met succes worden doorlopen.
3. De mate waarin en wijze waarop het tijdsplan van de Realisatie (duidelijke implementatie stappen en tijdslijnen) is beschreven en dat een Productiewaardig Oplossing uiterlijk 1 oktober 2026 is opgeleverd vanaf het moment dat het PvA gezamenlijk is vastgesteld tot en met de Acceptatie van de gewenste criteria conform Bijlage XII Realisatiefase
4. De mate waarin benodigde rollen en bijbehorende taken en verantwoordelijkheden van Partijen terugkomen in het PvA;
5. De mate waarin en wijze waarop wordt beschreven op welke wijze Opdrachtgever door Opdrachtnemer ontzorgd (werkverdeling tussen Opdrachtnemer en Opdrachtgever wordt duidelijk) wordt;
6. De mate waarin het antwoord inhoudelijk overtuigend en relevant is en met 'best practices' wordt ondersteund (hoe wordt het meeste uit de Oplossing wordt gehaald).

Alle bovenstaande zes beoordelingscriteria worden individueel beoordeeld op basis van onderstaande waardering. Het gemiddelde bepaald het aantal punten voor deze Wens, dat wordt afgerond naar een heel punt:

Zeer slecht

Het beoordelingscriterium is in zijn geheel niet beantwoord. Indien wel een uitwerking is gegeven aan het gevraagde en deze uitwerking aantoonbaar geen betrekking heeft op de betreffende beoordelingscriterium en/of het beoordelingscriterium is in zijn geheel niet beoordeeld kan worden, wordt ook **0 punten** toegekend

Matig;

Een deel van het beoordelingscriterium is niet beantwoord en/of de beantwoording sluit niet of nauwelijks aan bij de betreffende beoordelingscriterium en/of indien het beoordelingscriterium slechts gedeeltelijk beoordeeld kan worden, wordt ook **3 punten** toegekend.

Voldoende;

Het beoordelingscriterium wordt volledig beantwoord echter wordt de beantwoording voldoende onderbouwd en/of de beantwoording wordt beoordeeld als voldoende. U ontvangt **6 punten**

Goed;

Het beoordelingscriterium wordt volledig beantwoord en onderbouwd en de beantwoording

	wordt beoordeeld als goed. U ontvang 11 punten. Uitstekend; Het beoordelingscriterium wordt volledig beantwoord en onderbouwd, daarnaast bestaat het antwoord uit positieve, verrassende en vernieuwende elementen waardoor het beoordelingscriterium wordt beoordeeld als uitstekend. U ontvangt 17 punten. Het maximum aantal te behalen punten voor deze Wens is 17
--	--

Het organisatie onderdeel van de Opdrachtgever, IV GV Bouwblokken ICC team, is het aanspreekpunt voor naar de interne organisatie toe. De projectmanager van de Opdrachtnemer dient de Realisatie uit te voeren conform het PvA in samenwerking met de Opdrachtgever. Tijdens de gunningsfase wordt het Plan van Aanpak nader besproken en uitgelijnd met de omgeving van de Opdrachtgever.

2.2.2 Deel 1 Realisatie fase

Een overzicht van de planning, mijlpalen en acceptatie van de realisatiefase staat beschreven in Bijlage XII Realisatiefase.

UE.2	Het Plan van Aanpak van de Opdrachtnemer wordt na tekenen van de Overeenkomst uiterlijk binnen twee weken tussen Opdrachtnemer en de Opdrachtgever afgestemd en gefinaliseerd. Het omvat minimaal de 12 onderwerpen zoals deze in Wens 6 Implementatieplan en ondersteuning zijn omschreven. Pas nadat er akkoord is tussen Partijen over het Plan van Aanpak zal worden gestart met het uitvoeren van de Realisatie.
------	---

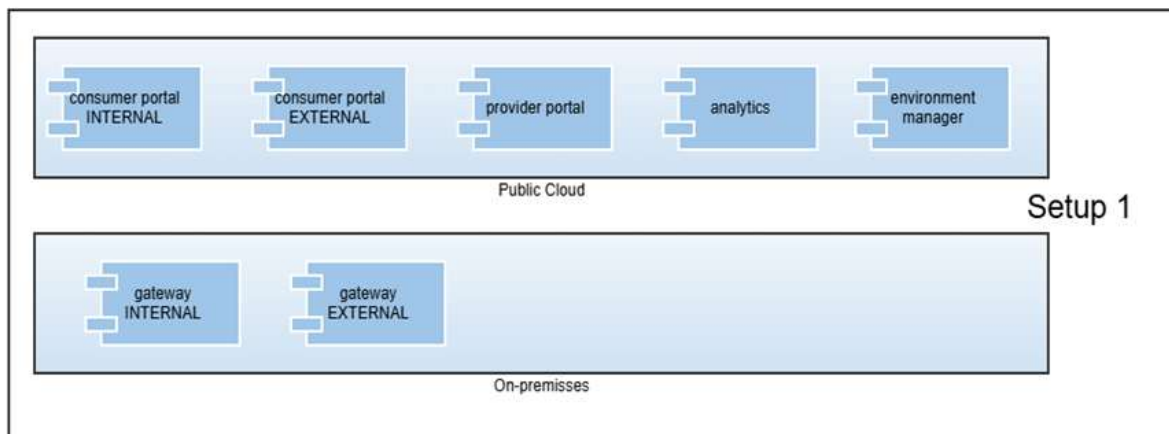
Met de Inschrijver die de economisch meest voordelige Inschrijving wordt een Gunningstest doorlopen (zie ook Paragraaf 6.2 in het Beschrijvend Document)

GUE 47.	In het kader van de Gunningstest wordt geëist dat wordt aangetoond dat de Offerte, voor zover dit praktisch gezien mogelijk is om te testen, voldoet aan de in deze Offerteaanvraag gestelde bovengenoemde eisen. De Opdrachtnemer stelt de noodzakelijke technische en personele ondersteuning en de benodigde middelen voor de uitvoering van deze Gunningstest kosteloos ter beschikking. In Bijlage XI Gunningstest staan de onderwerpen waarop getest wordt beschreven.
---------	---

Hoofdstuk 3. IV kaders

3.1 Hybride hosting

Het is de bedoeling dat de Oplossing hybride wordt gehost.



Figuur 2: hybride hosting setup.

Deze setup illustratie (zie figuur 2) schrijft voor welke Oplossing componenten precies in de control plane of data plane zitten. Alhoewel de exacte setup aan de markt zelf is, **moeten** de gateway componenten on-premises staan. De andere componenten staan off-premises in de public cloud. Dit zodat het API-verkeer afhandelingen on-premises plaatsvindt.

- GUE 48. De Oplossing dient hybride te kunnen worden gehost:
- Control Plane off premises als SaaS (in de EER);
 - Data Plane on premises op een Red Hat OpenShift container platform van de Opdrachtgever.

- GUE 49. De gateway componenten van de Oplossing moeten on-premises staan op een Red Hat Openshift container platform van de Opdrachtgever.

Gedurende de maximale looptijd van de Overeenkomst, dient de hybride hosting opzet een doorontwikkeling naar een off premises omgeving als SaaS binnen de dan toegestane geografische omgeving (nu de EER) eenvoudig mogelijk te maken.

3.1.1 Provisioning

Staging omgevingen

Gebruikers (in de rol API Provider of API Virtualizer) willen hun API's kunnen testen en geautomatiseerd kunnen doorzetten naar andere stages binnen de API LCM om fouten te voorkomen.

- GUE 50. De Oplossing ondersteunt meerdere omgevingen t.b.v. staging van API's en performance testen.
- Op basis van projects/namespaces kunnen geïsoleerde omgevingen worden uitgerold t.b.v. de voortbrengingsprocessen van de gebruikers.

Inzicht in gebruik

- | | |
|---------|---|
| GUE 51. | Het runtime gebruik van de Oplossing in productie moet inzichtelijk zijn.
Minimaal het aantal request (load) en de omvang van de berichten (volume). |
|---------|---|

Rollback van provisioning

- | | |
|---------|---|
| GUE 52. | Bij aanpassingen in de configuraties van de Oplossing of het uitrollen van nieuwe versie van de Oplossing kan er iets onverwacht misgaan. Het is daarom noodzakelijk dat de voorgaande, werkende, versie van de Oplossing geautomatiseerd kan worden terug gezet door de Opdrachtgever. |
|---------|---|

3.1.2 Deployment

Geautomatiseerde deployments

- | | |
|---------|---|
| GUE 53. | Om fouten te voorkomen en een herhaalbaar proces te realiseren, dient de Oplossing geautomatiseerde deployment van API en bijbehorende configuraties te ondersteunen. |
|---------|---|

Deployment traceability

- | | |
|---------|---|
| GUE 54. | Ter verantwoording en om misbruik te detecteren, ondersteund de Oplossing observability/traceability functionaliteit waarmee te minste welke gebruiker, wanneer (tijdsregistratie), welke verandering heeft aangebracht wordt vastgelegd. |
|---------|---|

Meerdere functionele versies

Het hebben van meerdere functionele versies van een API naast elkaar is heel gebruikelijk in situaties waarbij een API provider meerdere consumers heeft.

- | | |
|---------|--|
| GUE 55. | Het moet mogelijk zijn om meerdere functionele versies van een API in een omgeving / stage actief te hebben. |
|---------|--|

3.1.3 LCM

Platform LCM

- | | |
|---------|---|
| GUE 56. | Om LCM (Life Cycle Management) taken uit te kunnen voeren moeten meerdere versies van de Oplossing naast elkaar kunnen draaien.
De Oplossing voorziet in het gelijktijdige gebruik van N-1, N en N+1 versies van de Oplossing. |
|---------|---|

Naadloze updates

Gebruikers willen geen verstoring van hun verwerking hebben. Een downtime van het systeem moet voorkomen worden.

- | | |
|---------|---|
| GUE 57. | De configuratie van API's, users, rechten, configuratie items moet automatisch overgezet kunnen worden naar de nieuwere versie. |
|---------|---|

Testen binnen de Oplossing

Na release van een nieuwe versie wenst de Opdrachtgever deze te kunnen testen in een separate omgeving van de Oplossing.

- | | |
|---------|---|
| GUE 58. | Na release van een nieuwe versie van de Oplossing moet het mogelijk zijn voor de Opdrachtgever deze te kunnen testen in een separate omgeving van de Oplossing. |
|---------|---|

Integriteit - Versleutelde communicatie

- | | |
|---------|---|
| GUE 59. | De Oplossing zorgt voor veilig verkeer tussen de componenten op het containerplatform. Het verkeer buiten het container platform moet versleuteld zijn. |
|---------|---|

Middenbeslag - Schaalbaarheid

De load op de Oplossing kan fluctueren door de aangroei van nieuwe API's en door het verwerken van bijvoorbeeld Gegevens van fiscale campagnes. De Oplossing moet dynamisch kunnen schalen, zonder downtime.

- | | |
|---------|--|
| GUE 60. | De Oplossing dient met de omgeving van de Opdrachtgever dynamisch te kunnen schalen zonder downtime. |
|---------|--|

Foutbestendigheid - Isolatie bij API Beheer

Het opvoeren van een API mag niet tot verstoringen van andere API's (al dan niet van anderen) leiden.

- | | |
|---------|---|
| GUE 61. | Design time en runtime mogen niet met elkaar interfereren.

De Oplossing moet (runtime) isolatie toepassen, zodat de performance én werking van API's niet door elkaar beïnvloed kunnen worden. |
|---------|---|

- | | |
|---------|---|
| GUE 62. | Het opvoeren van een API mag niet tot verstoringen van andere API's (al dan niet van anderen) leiden. |
|---------|---|

3.2 Aansluitvoorwaarden container hosting

Kubernetes/OpenShift compatible

- | | |
|---------|---|
| GUE 63. | De Oplossing moet in staat zijn om op het Kubernetes compatible container platform RedHat OpenShift te draaien. |
|---------|---|

Container security / Security Context Constraints

- | | |
|---------|--|
| GUE 64. | De geboden Oplossing moet kunnen draaien op de SecurityContextConstraint: restricted-v2. Deze instelling is default op het doel cluster (containerplatform) ingesteld.

De aangeleverde containerimages moeten daarnaast kunnen omgaan met willekeurig ingestelde user id's. |
|---------|--|

Cluster-admin rechten

GUE 65.	De Oplossing moet voor het normale gebruik zonder cluster-admin rechten op OpenShift kunnen draaien. Indien er initieel verhoogde rechten nodig zijn dan kunnen deze gedurende het installatieproces worden toegestaan door de Opdrachtgever. Dit mag niet leiden tot extra kosten voor Opdrachtgever.
GUE 66.	De installatie van de Oplossing wordt bij voorkeur uitgevoerd met een account met standaard rechten in plaats van een account met verhoogde rechten zoals cluster admin. Mocht dit toch noodzakelijk zijn, dan is dit slechts eenmalig tijdens de installatie.

Network Policies

GUE 67.	De Oplossing kan omgaan met een cluster waarin verkeer tussen namespaces binnen het Openshiftplatform van Opdrachtgever niet is toegestaan.
---------	---

Cluster Resource Quota

GUE 68.	De Oplossing moet kunnen omgaan met namespaces waarin het instellen van resource requests en limits verplicht is.
---------	---

Air-gapped

GUE 69.	De Oplossing moet in staat zijn om Air-gapped te kunnen functioneren. De Oplossing moet kunnen omgaan met een private registry en repository van de Opdrachtgever voor Kubernetes.
---------	--

Storage reclaim

GUE 70.	Er mag geen reclaim policy van een persistent volume worden ingesteld op Retain.
---------	---

NodePorts

GUE 71.	De Oplossing maakt geen gebruik van de nodePorts op het Redhat openshift container platform cluster van de Opdrachtgever.
---------	---

Installeerbaarheid

GUE 72.	De Oplossing moet automatisch geïnstalleerd kunnen worden op een actuele Kubernetes distributie waaronder minimaal op Red Hat OpenShift Container Platform versie 4 en diens logisch opvolgers.
GUE 73.	De Oplossing kan op basis van operators of helm charts worden uitgerold.
GUE 74.	De Oplossing moet seamless upgrades ondersteunen.
GUE 75.	Indien de Oplossing geïnstalleerd wordt met een operator, is uit de beschrijving van de operator duidelijk welke aanpassingen de operator op cluster-niveau aanbrengt.

GUE 76.	De Oplossing is geschikt om in een container op een on premises hosting platform van de Opdrachtgever te draaien en is onafhankelijk van de onderliggende hardware met uitzondering van processor architectuur. De Opdrachtgever moet Life Cycle Management (LCM) kunnen uitvoeren op haar X86 gebaseerde hardware, zonder dat dit impact heeft op de Oplossing.
GUE 77.	De Oplossing maakt voor voor het on-premise deel voor permanente opslag van gegevens gebruik van de persistent storage, zoals geleverd wordt door het container platform of maakt gebruik van opslag buiten het containerplatform.
GUE 78.	De ReclaimPolicy van StorageClasses en PersistentVolumes op het containerplatform staat standaard op 'Delete'. De Programmatuur mag niet eisen dat deze instelling gewijzigd wordt.

Licentie

GUE 79.	De Opdrachtnemer stelt de Opdrachtgever zonder extra aanvullende kosten in staat licentiegebruik en compliancy volgens het licentiemodel aan te tonen.
---------	--

Logging

GUE 80.	Het gebruik van de Oplossing kan worden gelogd naar de console van het containerplatform van de Opdrachtgever.
---------	--

Onderhoud platform

GUE 81.	De correcte werking van de Oplossing wordt niet beïnvloed doordat de worker node (container) met de Oplossing door het containerplatform wordt gestopt en op een andere worker node (container) wordt gestart.
GUE 82.	De Oplossing reageert op het stopsignaal en geeft aan hoe lang er maximaal gewacht mag worden tot OpenShift de container uitzet.

Platform upgrades

GUE 83.	Platform versies (van OpenShift) blijven ondersteund worden door Opdrachtnemer, totdat deze vanuit de leverancier van dat Platform (RedHat) end-of-support zijn.
GUE 84.	De Oplossing mag niet verhinderen dat altijd de laatste security patches worden geïnstalleerd.
GUE 85.	Bij het beschikbaar komen van een nieuwe versie het platform(OpenShift) levert de Opdrachtnemer, binnen 3 maanden na beschikbaar komen daarvan, een werkende versie van haar Oplossing voor die Platform (OpenShift) versie.

Snelheid – Latency

GUE 86.	De Oplossing mag in 95% van de gevallen maximaal een latency van 6 ms toevoegen aan het totaal.
---------	---

Het betreft de tijd die de API-manager gebruikt. Netwerktijd tussen externe partij en de Opdrachtgever en de aanroep vanuit APIM naar het back-end systeem (of systemen) staan hier buiten.

Snelheid – Response tijden Portaal

Gebruikers van de portalen willen niet wachten op antwoord, maar willen meteen verder kunnen werken. Het portal is een onderdeel dat aan afnemers wordt geboden om API's te ontdekken en om zich aan te melden als Gebruiker van een API. Het is geen onderdeel van de dataverwerking

GUE 87.	In 95% van de gevallen is de handeling in de API management portalen binnen 3 seconden afgerond. Met 1000 concurrent OLTP gebruikers.
---------	---

3.3 Non Functionals

Handelingen van Gebruikers van de Oplossing moeten inzichtelijk gemaakt kunnen worden door middel van logging. Registraties en subscriptions worden gelogd t.b.v. auditing.

GUE 88.	De Oplossing ondersteunt het loggen van gebruikershandelingen, zijnde API registraties en API subscriptions.
---------	--

Bij installatie of bij een upgrade van de Oplossing moet de werking geautomatiseerd geverifieerd kunnen worden.

GUE 89.	De oplossing ondersteunt het geautomatiseerd verifiëren van de werking van de Oplossing bij installatie of bij een upgrade.
---------	---

Gebruikers die een GUI gebruiken om toegang te krijgen, moeten niet beperkt zijn in keuze met welk device ze dat doen.

GUE 90.	De GUI van de Oplossing voor Gebruikers moet te gebruiken zijn.
---------	---

GUE 91.	De GUI van de Oplossing voor Gebruikers is browser based.
---------	---

Verschillende gebruikers krijgen te maken met de GUI van de oplossing. Denk hierbij aan interne developers/beheerders, incidenteel medewerkers van de business en gebruikers buiten de organisatie.

GUE 92.	De Oplossing moet ondersteuning bieden in de Nederlandse en/of Engels taal.
---------	---

GUE 93.	De Oplossing ondersteund direct in input validatie en meldingen waar nodig.
---------	---

Integriteit – platform

GUE 94.	Oplossing garandeert dat ongeautoriseerde wijzigingen niet kunnen plaatsvinden.
---------	---

3.3.1 Integraliteit

De Opdrachtgever wil dat de Oplossing logisch uit één geheel bestaat en dat te allen tijde de Opdrachtnemer verantwoordelijk is voor alle in de Aanbestedingsstukken gestelde eisen van de Oplossing. Dit laat onverlet dat de Opdrachtnemer delen van de Oplossing kan en mag uitbesteden aan derden.

GUE 95.	De Opdrachtnemer levert de Oplossing als één integraal coherent werkend systeem. De deelcomponenten van de Oplossing werken als één integraal coherent systeem. Er is functioneel geen maatwerk nodig om de Oplossing aan de functionele eisen en wensen te laten voldoen. Als de Oplossing bestaat uit deeloplossingen dan is de integratie en werking van deze oplossingen de verantwoordelijkheid van de Opdrachtnemer. Ook als gebruik wordt gemaakt van eventuele onderaannemers. Dit geldt bovendien voor omgevingen van Opdrachtnemer waarmee toegang wordt verkregen tot Gegevens of programma(code) van de Oplossing. Dit is van toepassing bij Gunning en gedurende de looptijd van de Overeenkomst.
GUE 96.	De Opdrachtnemer garandeert dat, bij gebruik van (deel)oplossingen van eventuele onderaannemers, ook deze partijen en hun (deel)oplossingen aan de in de Aanbestedingsstukken gestelde eisen voldoen. Opdrachtnemer verplicht zich er hierbij toe deze verplichtingen met de onderaannemer(s) vooraf schriftelijk overeen te komen en de naleving ervan te controleren.
GUE 97.	Alle deeloplossingen in de vorm van plugins en/of add-ons die door de Fabrikant worden geleverd of worden ontwikkeld ten behoeve van de Oplossing zijn onderdeel van de geoffreerde licentieprijs.
GUE 98.	De Opdrachtnemer is verantwoordelijk voor alle in de Aanbestedingsstukken gestelde (beveiligings)eisen van de totale Oplossing.

3.3.2 Plug-ins en add-ons

Binnen de Oplossing kunnen verrijkende functionaliteiten, die nu nog niet beschikbaar zijn, worden aangeboden middels plug-ins en/ of add- ons door de Opdrachtnemer. Deze verrijkende functionaliteiten moeten de scope van de Opdracht passen.

GUE 99.	Verrijkende functionaliteit in relatie tot de gestelde eisen in deze aanbesteding kan door middel van plug-ins en/of add-ons van de Fabrikant of van derde partijen, worden afgenomen via een door de Fabrikant beheerde marktplaats. In het geval het een plug-in/of add-on betreft waarvoor betaald moet worden, zal de Opdrachtgever een separaat offerte traject onder de Overeenkomst afroepen en wordt pas na accodering door Opdrachtgever hiervan worden aangeschaft.
GUE 100.	De Fabrikant beheert de marktplaats en valideert de door derde partijen aangeboden plug-ins en add-ons op geschiktheid tot integratie met de Oplossing.

GUE 101.	De Oplossing ondersteunt geautomatiseerde installatie van plug-ins en add-ons van de Fabrikant of derde partijen
GUE 102.	Functionaliteit zoals aangeboden dient gedurende de looptijd van de Overeenkomst tegen minimaal dezelfde contractuele condities te worden aangeboden. Producten die nieuw worden aangeboden dienen na activering tegen gelijke condities aangeboden te worden gedurende de resterende looptijd van de Overeenkomst. Dit is ook van toepassing op nieuwe versies van de aangeboden Oplossing.

3.3.3 Wet- en regelgeving

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

GUE 103.	De Oplossing voldoet aan de algemene vigerende Nederlandse Wet- en Regelgeving.
----------	---

Open Standaarden

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

Zie ook: <https://www.forumstandaardisatie.nl/open-standaarden/verplicht>.

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

GUE 104	Opdrachtgever committeert zich aan het gebruik van de van toepassing zijnde en de Verplichte standaarden van het Forum Standaardisatie in relatie tot de Oplossing. Het betreft de volgende streefbeeldafspraken informatieveiligheid conform https://www.forumstandaardisatie.nl/onderwerpen/veilig-internet/streefbeeldafspraken: DNSSEC DNSSEC zorgt voor de beveiliging van DNS door aan het DNS-record een digitale handtekening toe te voegen en deze bij uitwisseling te verifiëren. https://www.forumstandaardisatie.nl/open-standaarden/dnssec HTTPS en HSTS HTTPS en HSTS zorgen samen voor beveiligde verbindingen met websites, met als doel de veilige uitwisseling van gegevens tussen een webserver en client (vaak een webbrowser). Let op: per 1 juli 2023 zijn overheidsorganisaties wettelijk verplicht om HTTPS en HSTS te gebruiken voor beveiligen van publiek toegankelijke websites en webapplicaties. https://www.forumstandaardisatie.nl/open-standaarden/https-en-hsts IPv6 en IPv4
---------	--

	IPv6 en IPv4 standaardiseren communicatie op netwerkniveau over organisatiegrenzen heen tussen organisaties, individuele eindgebruikers, apparaten, diensten en sensoren. https://www.forumstandaardisatie.nl/open-standaarden/ipv6-en-ipv4 • RPKI Met Resource Public Key Infrastructure (RPKI) kan de rechtmatige houder van een blok IP-adressen een autoritatieve, digitaal getekende verklaring publiceren met betrekking tot de intenties van de routing vanaf haar netwerk. Deze verklaringen kunnen andere netwerkbeheerders cryptografisch valideren en vervolgens gebruiken om filters in te stellen die onrechtmatige routing negeren. https://www.forumstandaardisatie.nl/open-standaarden/rpki • TLS TLS beveiligt met behulp van certificaten de verbinding (op de transportlaag) tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie. https://www.forumstandaardisatie.nl/open-standaarden/tls
--	---

Koppelbaarheid – standaarden

GUE 105.	De Oplossing moet OAS3.x in alle onderdelen en gebruik ondersteunen.
----------	--

Digitoeigankelijk (EN 301 549 met WCAG 2.1)

GUE 106.	De Oplossing dient minimaal WCAG 2.1 A of soortgelijk compliant te zijn.
----------	--

Gegevens

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

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

UE.3	Gegevens van de Opdrachtgever worden gescheiden opgeslagen van de Gegevens van andere klanten.
------	--

UE.4	Toegang tot deze Gegevens is beperkt tot de Opdrachtgever en –voor zover noodzakelijk voor het uitvoeren van de Overeenkomst- Opdrachtnemer.
------	--

UE.5	Andere klanten van de Opdrachtnemer hebben geen toegang tot de Gegevens van de Opdrachtgever.
------	---

Gegevens van en over de Opdrachtgever zijn vertrouwelijk en niet zonder expliciete toestemming van de Opdrachtgever te gebruiken voor eigen gebruik of te delen met Derde partijen. Gegevens worden door Opdrachtnemer alleen verwerkt voor de doelen waarover afspraken gemaakt zijn.

UE.6	Opdrachtnemer zal geen Gegevens voor eigen doeleinden delen dan wel verwerken, behalve na expliciete toestemming van de Opdrachtgever. Opdrachtnemer openbaart welke Gegevens als strikt noodzakelijk worden beschouwd voor de uitvoering van de Overeenkomst.
------	--

Als de Opdrachtgever dat nodig acht dan kan de Opdrachtgever Opdrachtnemer verzoeken zijn Gegevens of een deel van zijn Gegevens te verstrekken voor verdere verwerking.

Aanleveren van de Gegevens gebeurt via een beveiligde verbinding van de Opdrachtgever in een door de Opdrachtgever bruikbaar digitaal formaat.

UE.7	Opdrachtnemer levert op aanvraag en conform afspraken een voor de Opdrachtgever bruikbare digitale kopie van de meest actuele Gegevens en haar structuur. Vertrouwelijkheid en integriteit blijven geborgd.
------	---

(Persoons)Gegevens en processen veiligstellen

In geval dat de (Persoons)Gegevens of Processen van de Opdrachtgever in gevaar komen, bijvoorbeeld door als Hoog of Kritisch gekwalificeerde Kwetsbaarheden kan de Opdrachtgever besluiten dat de (Persoons)Gegevens van de Opdrachtgever veiliggesteld moeten worden door:

- de Gegevens van de Opdrachtgever voor derden ontoegankelijk te maken en/of
- (relevante delen van) de Oplossing voor derden onbeschikbaar te maken.

Opdrachtnemer werkt, daar waar relevant, mee bij:

1. Export acties van (Persoons)Gegevens indien het proces via een andere Oplossing/procedure voortgezet dient te worden bij de Opdrachtgever.
2. De Oplossing wordt weer in productie (on-line) gebracht na toestemming van de Security Officer van de Opdrachtgever. (Persoons)Gegevens en processen zijn hierbij weer conform afspraken beschikbaar.

UE.8	Opdrachtnemer werkt onverwijld en kostenloos mee als de CISO (Chief Information Security Officer) van de Opdrachtgever besluit tot het uitvoeren van het veiligstellen van (Persoons)Gegevens en processen: - (Persoons)Gegevens van de Opdrachtgever worden ontoegankelijk gemaakt voor Derden. - De Oplossing, of een deel daarvan, wordt ontoegankelijk gemaakt voor Derden. Tussen het invoeren van de actie om (Persoons)Gegevens en processen veilig te stellen en het afronden van de uitvoering mag maximaal 4 uur verstrijken. De acties om de (Persoons)Gegevens en processen veilig te stellen worden direct na binnenkomst van het verzoek in gang gezet. (Persoons)Gegevens worden alleen via een beveiligd kanaal uitgewisseld. Zowel integriteit als vertrouwelijkheid zijn geborgd.
------	--

Het weer beschikbaar maken van de Oplossing (Reinstatement) houdt in dat de Oplossing weer in productie wordt gebracht met gebruikmaking van de meest actuele (Persoons)Gegevens. Dit is inclusief import acties van de (Persoons)Gegevens indien het proces via een andere oplossing/procedure voortgezet is geweest.

Speciale aandacht hierbij voor de situatie dat (Persoons)Gegevens van voor het stopzetten van de Oplossing samengevoegd moeten worden met de (Persoons)Gegevens die in de tussentijd mogelijk elders zijn gegenereerd. Integriteit en Vertrouwelijkheid van de (Persoons)Gegevens blijven te allen tijde geborgd.

UE.9	Op aangeven van een Security Officer van de Opdrachtgever wordt de Oplossing weer ter beschikking gesteld, zodat (Persoons)Gegevens en Processen weer conform afspraken beschikbaar zijn. Opdrachtnemer werkt mee met het opnieuw in gebruik nemen van de Oplossing, waarbij vertrouwelijkheid en integriteit van de (Persoons)Gegevens gewaarborgd is. Ook als er integratie
------	---

van (Persoons)Gegevens van de Oplossing met (Persoons)Gegevens die tijdens de onbeschikbaarheid zijn gegenereerd, moet plaatsvinden.
--

3.3.4 (Informatie) Beveiliging van Gegevens

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

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

Gegevens dienen verwerkt (onder andere: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen) te worden in de EU en landen waarvan de Europese Commissie bepaald heeft dat in deze landen een passend beveiligingsniveau is (bron: <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal/doorgifte-binnen-en-buiten-de-eu#hoe-weet-ik-of-een-derde-land-een-passend-beschermingsniveau-heeft-1752>).

GUE 107.	Gegevens dienen te worden verwerkt in lidstaten van de EU of een land met een door de EU goed-gekeurd beveiligingsniveau (EER). Gegevens van de Opdrachtgever verlaten deze landen niet. Opdrachtnemer levert documenten die bewijzen dat verwerking in de in de hierboven genoemde landen plaatsvindt en deze landen nooit verlaat.
----------	---

Hoewel Gegevens in de EU verwerkt moeten worden, kan het mogelijk zijn dat een niet-EU mogendheid via eigen wetgeving toegang kan krijgen tot de Gegevens, waaronder Persoonsgegevens. Er dienen maatregelen getroffen te zijn om dit te voorkomen.

Indien Opdrachtnemer of één van haar Onderaannemers onder wetgeving valt waardoor Gegevens op wettelijke basis wel gedeeld moeten worden met Derden dan maakt Opdrachtnemer dat bij Inschrijving bekend. Er dient duidelijkheid te worden gegeven om welke Derde partijen het gaat, welke wettelijke grondslag het betreft en hoe dergelijke verzoeken worden afgehandeld.

GUE 108.	Indien de Opdrachtnemer of één van zijn Onderaannemers een eigenaar buiten de EU heeft dan zijn maatregelen getroffen zodat (Persoons)gegevens alleen conform de in de EU geldige wetgeving aan overheidspartijen in andere landen ter beschikking gesteld kunnen worden. Er wordt inzage gegeven in welke partijen inzage in de Gegevens kunnen eisen. Indien gegevens buiten de EU of EU goedgekeurde landen gedeeld moet worden, dan wordt gebruik gemaakt van Standard Contractual Clauses. Opdrachtnemer levert documenten die dit bewijzen.
----------	--

De Opdrachtgever wil haar gegevens binnen de grenzen van de EU houden. Daarom is het van belang dat de onderaannemers van de Opdrachtnemer dit ook doen. Hierover is inzicht nodig.

GUE 109.	Geef inzicht in uw Onderaannemers en in welke landen deze Onderaannemers geregistreerd zijn.
----------	--

(BIO Referentie 15.1.3.1)

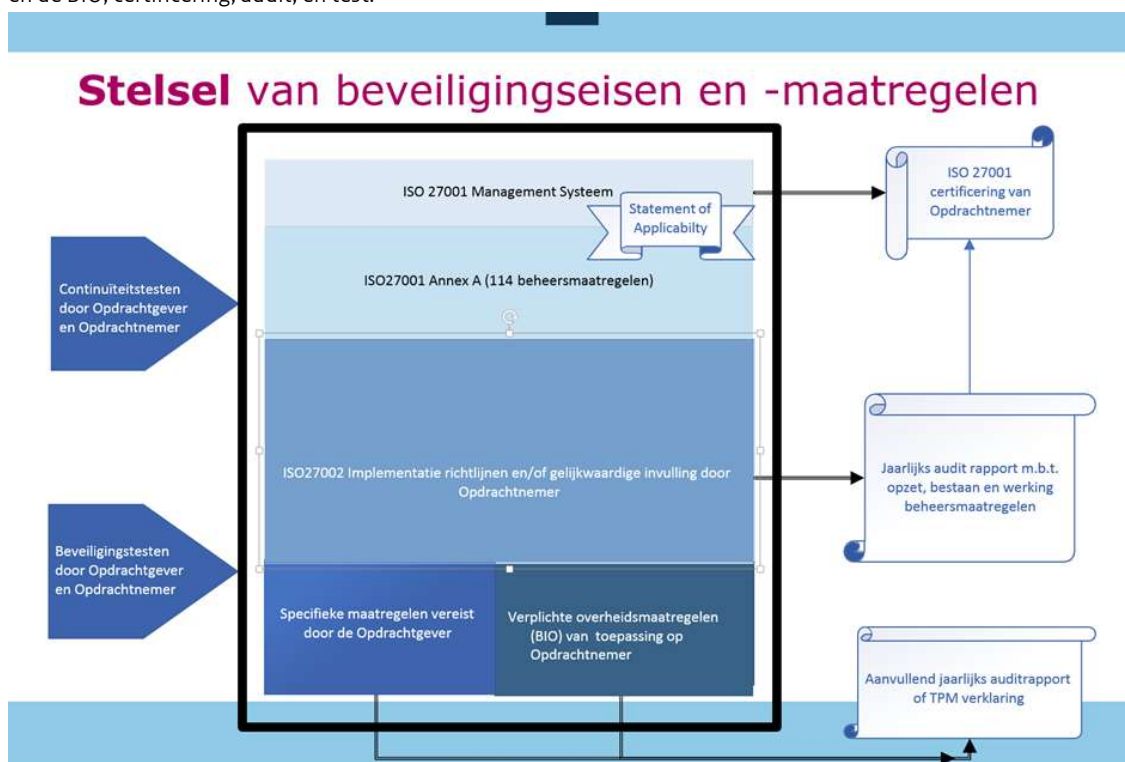
Informatiebeveiligingsbeleid

De Opdrachtgever verwerkt Fiscale en financiële gegevens van particulieren en ondernemingen, Persoonsgegevens van medewerkers en burger en andere mogelijkheden, zoals een mix eerder genoemde.

De omgang met deze gegevens vraagt van de Opdrachtgever een werkwijze die de vertrouwelijkheid en integriteit van deze gegevens waarborgt. Bij het betrekken van producten en diensten uit de markt dient een deel van de verantwoordelijkheden ingevuld te worden door de Opdrachtnemer. De Opdrachtnemer moet dus minimaal hetzelfde beveiligingsniveau leveren als de Opdrachtgever. De Opdrachtgever is gehouden aan de Baseline Informatiebeveiliging Overheid (BIO). Deze regelgeving is gebaseerd op de NEN/ISO 27001:2017 en de NEN/ISO 27002:2017, en bevat daarnaast aanvullende beveiligingseisen, de zogenoemde overheidsmaatregelen. Vanwege de eigen technische inrichting, stelt de Opdrachtgever zelf ook specifieke beveiligingseisen.

Opzet, bestaan en werking kunnen worden gecontroleerd middels audits en beveiligings- en continuïteitstesten.

In onderstaande figuur 3 is de samenhang weergegeven tussen beveiligingsmaatregelen, de kaders ISO 27001/2 en de BIO, certificering, audit, en test.



Figuur 3: samenhang beveiligingsmaatregelen, de kaders ISO 27001/2 en de BIO, certificering, audit, en test

GUE 110.	De Opdrachtnemer dient een informatiebeveiligingsbeleid te hebben met als uitgangspunt ISO27001/2 of beleid gelijkwaardig aan ISO27001/2. Opzet, bestaan en werking van het informatiebeveiligingsbeleid met betrekking tot de Oplossing moet worden aangetoond voor Gunning én gedurende de looptijd van de Overeenkomst. De Opdrachtgever accepteert ook borging van het informatiebeveiligingsbeleid gelijkwaardig aan ISO27001/2. In hoeverre het informatiebeveiligingsbeleid gelijkwaardig is aan de ISO27001/2 of niet, is ter beoordeling en acceptatie door de Opdrachtgever.
----------	---

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

GUE 111.	Opzet, bestaan, en werking van een actueel informatiebeveiligingsbeleid wordt periodiek (minimaal 1x per jaar) aangetoond door Opdrachtnemer. Op verzoek van Opdrachtgever verstrekt Opdrachtnemer ter beoordeling een door een geaccrediteerde partij verstrekt ISO27001/2- of gelijkwaardig certificaat, compleet met bijbehorend Statement of Applicability. Uit het geleverde blijken opzet, bestaan en werking van geïmplementeerd informatiebeveiligingsbeleid. Indien beoogde Oplossing en Opdrachtnemer niet voldoen aan de voorwaarden van de Opdrachtgever kan als alternatief een gelijkwaardige set documenten worden aangeleverd die bovenstaande vervangt. Dit kan alleen met toestemming van de Opdrachtgever. Deze set documenten bevat tenminste een mapping van het geleverde op de ISO27001/2 en wordt beoordeeld door de Opdrachtgever. Ook is duidelijk op welke onderdelen de bewijsvoering op de organisatie en welke op Oplossing van toepassing is.
----------	--

(BIO Referenties: 5.1.1.1, 5.1.2, 18.2.1.1)

Indien er aanleiding toe is dan kan de Opdrachtgever besluiten zelf een Audit (al dan niet op alle onderdelen) uit te laten voeren op de dienstverlening en/of Oplossing.

UE.10	De Opdrachtgever heeft het recht om zelf (een deel van) de dienstverlening en/of Oplossing aan een Audit te onderwerpen. De basis van de Audit is deze Bijlage A Specificatie van de Opdracht. De Opdrachtnemer werkt hier kosteloos aan mee.
-------	---

(BIO Referenties: 5.1.2, 15.1.2.6, 18.2.1.1)

3.3.5 Specifieke eisen van de Opdrachtgever

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

Het legt dus aan de ene kant accenten op onderdelen die reeds onderdeel uitmaken van een op 27001/2-gebaseerd Informatiebeveiligingsbeleid, aangevuld met overheids- en Opdrachtgeverspecifieke zaken.

Voortbrenging (onderdelen) Oplossing

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

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

UE.11	In de Oplossing gebruikte Open Source-code en libraries van andere leveranciers bevatten geen bekende Kwetsbaarheden. Er wordt gebruik gemaakt van de meest recente veilige versies uit betrouwbare bron. Als er geen veilige versie beschikbaar is dan wordt dit gemeld als beveiligingsincident conform de bestaande afspraken.
-------	--

W 7	Interoperabiliteit en cloud native Deze wens bestaat uit twee delen: 1. Deel I: Interoperabiliteit 2. Deel II Cloud Native <i>Deel I: Interoperabiliteit</i> Het Rijksbeleid is dat Open source software daar waar mogelijk gebruikt wordt, gepubliceerd en ondersteund, in lijn met het Open Tenzij beleid. Dit bevordert de interoperabiliteit, innovatie en duurzaamheid binnen applicaties en technologie, terwijl bijdragen aan open source projecten de samenwerking en kwaliteit verder versterken." Interoperabiliteit is belangrijk in de wereld van applicatie integratie, omdat juist op dit vlak veel technieken samenkomen en er nog volop ontwikkeld wordt. Vraag Beschrijf, bewijs en licht toe of de Oplossing is gebaseerd op Open source software én wat de footprint is van uw API-Gateway. Beoordeling Deel I Interoperabiliteit en footprint • Uit de beantwoording blijkt dat de Oplossing niet gebaseerd is op Open source software = 0 punten • Uit de beantwoording blijkt dat de Oplossing gebaseerd is op Open source software = 3 punten; • Een API-Gateway heeft een footprint > 500 MB RAM = 0 punten • Een API-Gateway heeft een footprint < 500 MB RAM = 3 punten ----- <i>Deel II Cloud Native</i> De Opdrachtnemer wenst een optimaal gebruik en inrichting van een Oplossing en denkt dat dit via een modulaire en cloud native Oplossing te verkrijgen. Voor de Opdrachtnemer is het belangrijk dat de Opdrachtnemer kan aantonen dat de Oplossing cloud native is opgezet en daarmee perfect past op een cloud platform. De Opdrachtgever wenst daarom inzicht in het feit of de aangeboden Oplossing een CNCF-certificering heeft (https://www.cncf.io) of niet. Vraag Beschrijf en geef aan of de Oplossing een CNCF-certificering heeft. Beoordeling Deel II Cloud Native • Uit de beantwoording blijkt Oplossing geen CNCF-certificering heeft = 0 punten. • Uit de beantwoording blijkt Oplossing een CNCF-certificering heeft = 6 punten.
------------	--

	In uw uitwerking, maximaal 1 pagina's A4 (Lettertype Arial, lettergrootte 10 en regelafstand 1,0), dient u de bovenstaande onderwerpen per punt uit te werken. Het maximum aantal te behalen punten voor deze Wens is 12
--	---

Beveiligings- en continuïteitstesten

Beveiligingstesten zijn een belangrijk onderdeel in het stelsel van beveiligingseisen-en maatregelen. De Opdrachtgever stelt eisen aan beveiligingstesten. Deze eisen betreffen de testmethode, waardering van de bevindingen, de testende partij, de rapportage en de afhandeling van de kwetsbaarheden.

Er worden periodiek of rond een omvangrijke release beveiligingstesten uitgevoerd op een internet-facing ICT-oplossing. Het betreffen zowel Attack & Penetration testen (jaarlijks) als Vulnerability scans (bij wijze van spreken continue). De partij waar primair de hosting plaatsvindt is de eerstverantwoordelijke om deze beveiligingstesten uit te voeren. Meestal is dat de Opdrachtnemer.

Beveiligingstesten die (aanvullend) uitgevoerd worden door de Opdrachtgever vervangen niet de beveiligings-testen van de Opdrachtnemer. Beveiligings- en continuïteitstesten zijn slechts momentopnamen. Herhaling is dus van belang. Net als het hertesten van geadresseerde bevindingen.

De kosten van uitvoering van dergelijke beveiligingstesten worden gedragen door de partij die conform de eisen de beveiligingstest behoort uit te voeren. De andere partij werkt op verzoek kosteloos mee aan dergelijke testen. Onder het kosteloos meewerken wordt - onder andere - bedoeld:

- beantwoorden van vragen in de verschillende fasen van voorbereiding en uitvoering van een beveiligingstest.
- het oplossen van bevindingen die uit de beveiligingstesten volgen. Dit is inclusief eventueel benodigd overleg hierover.

De partij die de A&P-test laat uitvoeren bepaalt zelf welke partij de A&P-test uitvoert en wat de inhoud van de A&P-test is. De Opdrachtgever stelt wel eisen aan de kwaliteit van zowel de A&P-test als de rapportage daarover.

Relevante bevindingen (kwalificatie Kritisch en Hoog) volgend uit de beveiligingstesten zullen tussen de Opdrachtgever en Opdrachtnemer worden gedeeld en zo nodig besproken. Hetzelfde geldt voor plannen van aanpak en Verbeterplannen. Om de A&P-test te kunnen beoordelen wordt het volgende tussen de partijen gedeeld:

- de scope van de test (infrastructuur, middleware, tooling en (API-)koppelingen) is beschreven. Het is duidelijk welke delen van de Oplossing binnen en buiten scope zijn geweest. Het is bekend welke beveiligings-maatregelen (tijdelijk) uitgeschakeld waren.
- welke testmethodieken (black-, grey- of crystal boxtesting, wel of niet inclusief broncodereview) zijn gebruikt, en welke normenkaders zijn gebruikt (bijvoorbeeld STRIDE, OWASP Top 10, SANS Top 25, OWASP Mobile Top 10, etc etc).
- hoe is getest: geautomatiseerd, handmatig (worden geautomatiseerd gevonden kwetsbaarheden handmatig geverifieerd?) en wordt er ook door pentesters zelf naar (combinaties van) kwetsbaarheden gezocht..
 - managementsamenvatting met een definitie van de opdracht, relevante kenmerken van de A&P-test, een conclusie en aanbevelingen.
 - alle gevonden Kwetsbaarheden zijn opgenomen in de rapportage met CVSS-waardering. Aangegeven welke versie van CVSS (vanaf 3.0) is gebruikt. Geef het volgende aan: de statusaanduiding, bijvoorbeeld "In behandeling" (met plandatum) of "Opgelost (en gehertest)".

Aanvullende uitgangspunten bij A&P-testen die door of namens de Opdrachtgever worden uitgevoerd. Er:

- wordt getest in de Acceptatieomgeving, welke technisch gelijk is aan en voorzien is van dezelfde beveiligingsmaatregelen als de Productie-omgeving. Voor afwijkingen is toestemming vereist van de eigenaar (of gemandateerde) van het te testen object

- wordt geen gebruik gemaakt van Productiegegevens. Voor afwijkingen is toestemming vereist van de Dataeigenaar (of gemandateerde).
- is sprake van een freeze-periode in de omgeving die wordt getest. Alleen in samenspraak met het A&P-testbedrijf, bijvoorbeeld om een patch uit te voeren om een Kwetsbaarheid weg te nemen, kan hier van worden afgeweken.
- kwetsbaarheden gekwalificeerd als Kritisch of Hoog risico worden zo mogelijk tijdens de A&P-test opgelost en gehertest.

UE.12	Opdrachtnemer voert voor in productiename en daarna minimaal jaarlijks, of na een significante release, een A&P-test uit over de gehele (of een deel van de Oplossing) conform de hierboven beschreven richtlijnen (uitvoering, afhandeling van Kwetsbaarheden, etc.) van de Opdrachtgever. Nadere afspraken over de uitvoerbaarheid worden vastgesteld in de DAP. Kwetsbaarheden met de kwalificaties Kritisch of Hoog risico worden bekendgemaakt aan de Opdrachtgever en na adressering gehertest. Ook de Managementsamenvatting wordt gedeeld. Eventuele Kwetsbaarheden worden conform de richtlijnen van de Opdrachtgever opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan. Kosten die hier eventueel aan verbonden zijn zijn voor rekening van Opdrachtnemer.
-------	--

(BIO Referenties 12.1.4.1, 18.2.3.1)

UE.13	Voor de (onderdelen van de) Oplossing die on premises worden gehost, voert Opdrachtgever voor in productiename, jaarlijks, of na een significante release, een A&P-test uit conform de hierboven beschreven richtlijnen van de Opdrachtgever. De precieze invulling van de A&P-test is afhankelijk van de situatie en wordt bepaald door de Opdrachtgever. Het kan een A&P-test zijn binnen de keten waar de Oplossing onderdeel van is. In het geval van er kwetsbaarheden worden gevonden die binnen de scope van de Opdrachtnemer vallen, lost de Opdrachtnemer conform de richtlijnen van de Opdrachtgever deze op. In overleg worden relevante acties opgenomen in het Verbeterplan. Opdrachtnemer werkt hier kosteloos aan mee.
-------	--

(BIO Referenties 12.1.4.1, 18.2.3.1)

UE.14	Indien de Opdrachtgever (op basis van een risico-inschatting) het noodzakelijk acht een A&P-test uit te laten voeren dan staat Opdrachtnemer dat toe en werkt daar conform afspraken kosteloos aan mee. De precieze invulling van de A&P-test is afhankelijk van de situatie. Het kan een A&P-test zijn binnen de keten waar de Oplossing onderdeel van is. Het organiseren van deze A&P-test gebeurt door de Opdrachtgever en het uitvoeren van de A&P-test zelf zijn voor rekening van de Opdrachtgever. Eventuele Kwetsbaarheden worden conform de richtlijnen van de Opdrachtgever opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan. Opdrachtnemer werkt hier kosteloos aan mee.
-------	---

(BIO Referenties 12.1.4.1, 18.2.3.1)

Vulnerability scans

Vulnerability scans zijn bedoeld om geautomatiseerd te scannen op bekende kwetsbaarheden. Een Vulnerability scan kan dus met een grote regelmaat worden uitgevoerd. De reden om dergelijke beveiligingstesten regelmatig uit te voeren is dat aan de ene kant de Oplossing (continu) ge-update wordt en aan de andere kant hackers en beveiligingsonderzoekers constant op zoek zijn naar nieuwe Kwetsbaarheden.

Aanvullend kan programmacode tijdens het ontwikkelproces on-the-fly worden getest met daarvoor geschikte hulpmiddelen.

UE.15	Opdrachtnemer voert minimaal wekelijks een Vulnerability scan uit op de Oplossing. De gebruikte tooling, waar Opdrachtnemer zelf in dient te voorzien, maakt gebruik van up-to-date kwetsbaarheden- definitiebestanden. Op verzoek worden testresultaten, zeker als ze gekwalificeerd zijn als Kritisch of Hoog, gedeeld met de Opdrachtgever. Eventuele Kwetsbaarheden worden kosteloos opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan.
-------	--

(BIO Referentie 18.2.3.1)

UE.16	Voor de componenten van de Oplossing die on premises worden gehost, voert Opdrachtnemer op haar kosten periodiek maandelijks een Vulnerability scan uit op de Oplossing, conform haar richtlijnen. Eventuele Kwetsbaarheden die binnen de scope van de Opdrachtnemer vallen, worden opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan. Opdrachtnemer werkt hier kosteloos aan mee.
-------	---

UE.17	Voor de componenten van de Oplossing die off premises worden gehost én Opdrachtnemer het noodzakelijk acht (op basis van een risico-inschatting) een Vulnerability scan uit te laten voeren op de Oplossing dan staat de Opdrachtnemer dat toe. Kosten van het uitvoeren van de Vulnerability scan worden gedragen door Opdrachtgever. Eventuele Kwetsbaarheden worden opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan. Opdrachtnemer werkt hier kosteloos aan mee.
-------	--

(BIO Referentie 18.2.3.1)

UE.18	Voor de componenten van de Oplossing die off premises worden gehost én Opdrachtgever het noodzakelijk acht (op basis van een risico-inschatting) een Vulnerability scan uit te laten voeren op de Oplossing dan staat de Opdrachtnemer dat toe. Kosten van het uitvoeren van de Vulnerability scan worden gedragen door Opdrachtgever. Eventuele Kwetsbaarheden worden opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan. Opdrachtnemer werkt hier kosteloos aan mee.
-------	--

(BIO Referentie 18.2.3.1)

De Opdrachtgever wenst inzage in het beveiligingstestbeleid van de Opdrachtnemer. Het betreft opzet, bestaan en zo mogelijk werking van de A&P-testen en Vulnerability scans. Hiertoe worden documenten aangeleverd waarin het beveiligingstestbeleid wordt beschreven en hoe eventuele tekortkomingen worden afgehandeld. Ook moet blijken onder welke omstandigheden dergelijke beveiligingstesten worden uitgevoerd en dat deze worden uitgevoerd.

UE.19	Opdrachtnemer heeft een door haar directie goedgekeurd beveiligingstestbeleid en voert ook beveiligingstesten conform dit beleid uit. Indien gewenst door de Opdrachtgever, levert de Opdrachtnemer inzage in een rapportage dan wel verslagen betreffende de volgende testen: - Rapport A&P-test; - Rapport Vulnerability scan. In de rapportage / verslagen dienen ten minste de volgende aspecten uit te zijn gewerkt: - De aanwezigheid van een vastgesteld beveiligingsbeleid en de inhoud daarvan; - Aanwezigheid, opzet en informatieve waarde van een A&P-testrapport; - Aanwezigheid, opzet en informatieve waarde van een Vulnerability testrapport.
-------	--

Procedures hieromtrent worden vastgelegd en beschreven in de DAP.

Beveiligingstesten

Beveiligingstesten (A&P-test, Vulnerability scan) worden regelmatig uitgevoerd op de Oplossing. Normaal gesproken gebeurt dit door de Opdrachtnemer, maar de Opdrachtgever behoudt zich het recht voor ook beveiligingstesten uit te (laten) voeren als zij dit noodzakelijk acht. In het geval van A&P-testen maakt de Opdrachtgever gebruik van onafhankelijke A&P-testbedrijven. Er is dan een 'Vrijwaringsverklaring Pentesten' nodig. Als er ook Broncodeonderzoek uitgevoerd moet worden dan kan Opdrachtnemer een (aanvullende) 'Non-disclosure agreement Broncodeonderzoek' afsluiten met de A&P-testpartij.

UE.20	Opdrachtnemer gaat akkoord met de inzet door de Opdrachtgever van een onafhankelijk A&P-testbedrijf en sluit een Vrijwaringsverklaring af per A&P-testbedrijf, danwel A&P-test. Hetzelfde geldt voor een Non-disclosure Agreement voor inzage bij broncode-onderzoek.
-------	--

3.3.6 Continuïteit, Back-up & Recovery en continuïteitstesten

Van belang is om te weten welke maatregelen getroffen zijn om eventuele onbeschikbaarheid te voorkomen én hoe snel de de Gegevens beschikbaar zijn danwel de Oplossing weer volledig operationeel kan zijn, indien de onbeschikbaarheid toch groter mocht zijn dan gepland. Het gaat hierbij dus niet om de operationele beschikbaarheidseisen (waar het vooral draait om wanneer de Oplossing wel of niet te gebruiken is), maar om de excepties als het mis gaat (Calamiteiten en Back-up & Restore)

Van Opdrachtnemer wordt verwacht dat de Oplossing bij onbeschikbaarheid binnen bepaalde termijnen weer beschikbaar is zonder verlies van integriteit en vertrouwelijkheid.

Recovery Point Objective & Recovery Time Objective

UE.21	Voor de componenten van de Oplossing die on premisses worden gehost bij de Opdrachtgever, dient de Oplossing te voldoen aan onderstaande eisen betreffende de operationele continuïteit in geval van een Calamiteit (crisis): - Recovery Point Objective (RPO): Er dient een Recovery Point gemaakt te kunnen worden met maximaal 12 klokuren verlies van Gegevens. Voor de componenten van de Oplossing die door de Opdrachtnemer worden gehost, dient de Oplossing te voldoen aan onderstaande eisen betreffende de operationele continuïteit in geval van een Calamiteit (crisis): - Recovery Time Objective (RTO): De Oplossing is binnen 24 klokuren uren weer volledig functioneel beschikbaar; - Recovery Point Objective (RPO): Er is maximaal 12 klokuren verlies van Gegevens toegestaan.
-------	--

(BIO Referenties 11.1.4.2, 12.3.1.1, 12.3.1.3, 12.1.3.1.4, 17.1.3.3)

De Opdrachtgever wil de garantie dat het proces doorgang kan vinden met de afgesproken beschikbaarheid. Verstoringen en Calamiteiten zijn beheersbaar en mitigerende maatregelen worden periodiek getest. De scope is de Productie-omgeving en eventuele ondersteunende omgevingen/processen die de beschikbaarheid van de Productie-omgeving kunnen degraderen.

Er worden twee continuïteitstesten voorzien: Backup & Restore en Calamiteitentest.

Backups zijn bedoeld om Gegevens, Programmatuur en Configuratiegegevens periodiek veilig te stellen. Zodat deze gebruikt kunnen worden om Gegevens, Programmatuur of Configuratiegegevens bij onbeschikbaarheid binnen afgesproken termijnen al dan niet op hetzelfde systeem te herstellen.

Gegevens opgeslagen in back-ups zijn minimaal op het zelfde niveau beveiligd als Productiegegevens. Backups buiten de Oplossing zijn niet te gebruiken om de Gegevens te verwerken anders dan via het reguliere Restoreproces binnen de Oplossing te brengen.

Back-up & restore

UE.22	De Oplossing dient backup- en recovery-functionaliteit te bevatten. Data en configuratie van Gebruikers mogen niet verloren gaan. Om recovery uit te kunnen voeren dient automatisch een backup gemaakt worden. Een geautomatiseerde procedure moet de backups kunnen terugzetten.
-------	--

UE.23	Bestanden met Gegevens, de Oplossing én de Configuratiegegevens zijn veilig te stellen door de Back-upfunctionaliteit van de Oplossing.
-------	---

(BIO Referenties 12.3.1.4, 12.3.1.5)

UE.24	Voor de onderdelen van de Oplossing die door de Opdrachtnemer worden gehost, voert Opdrachtnemer periodiek een Backup & Restoretest uit. Afwijkingen worden aan de Opdrachtgever gemeld. Eventuele verbeterpunten worden geïdentificeerd, opgenomen in het Verbeterplan (en daarmee gedeeld met de Opdrachtgever) en van daar uit opgelost. Opdrachtnemer werkt kosteloos mee aan het implementeren van eventuele verbeterpunten die van toepassing zijn op de Oplossing zelf.
-------	---

(BIO Referenties 12.3.1.4, 12.3.1.5)

UE.25	De oplossing bevat geen klantdata, dat wil zeggen de oplossing transporteert de klantdata, maar houdt deze data niet vast. De data die wel gepersisteerd wordt is data over configuraties. Deze data moet na een calamiteit beschikbaar zijn.
-------	---

Een Calamiteit kan optreden als de Productie-omgeving, of de Gegevens daarop, volledig onbeschikbaar worden. In een dergelijke situatie mag er geen sprake zijn van inbreuk op Integriteit en Vertrouwelijkheid van de Gegevens. Men is hierop voorbereid door het opstellen van een Calamiteitenplan (Disaster Recovery Plan).

Een periodieke test om te controleren of de Oplossing naar aanleiding van gesimuleerde noodsituaties kan worden hersteld en daarna kan blijven functioneren zoals overeengekomen, is noodzakelijk.

UE.26	Opdrachtgever wenst in gezamenlijkheid met Opdrachtnemer een Calamiteitenplan op te stellen en uit te voeren. Opdrachtnemer dient aan het opstellen én uitvoeren van Calamiteitentesten kosteloos aan mee te werken. Na afloop van een Calamiteitentest wordt de managementsamenvatting van de testuitkomsten gedeeld. Eventuele verbeterpunten worden geïdentificeerd en opgenomen in het Verbeterplan (en daarmee gedeeld met de Opdrachtgever) en van daaruit opgelost. Afspraken hierover worden vastgelegd in de DAP.
-------	--

(BIO Referenties 11.1.4.2, 17.1.3.1)

3.3.7 Prestatie van de oplossing

Monitoring, Alerting en Logging

De Opdrachtgever heeft zicht in afwijkende/verdachte activiteiten binnen de Oplossing om herstelacties te kunnen formuleren en zo mogelijk in de toekomst te voorkomen. Denk aan (ongeautoriseerde) toegang tot de Oplossing, maar ook inzage, wijziging of verwijdering van Gegevens. Speciale aandacht voor gevoelige

Gegevens, zoals Persoonsgegevens. Bovendien, bijvoorbeeld, financiële Gegevens kunnen extra aandacht nodig hebben. Acties van gebruikers met veelomvattende rechten/privileges zijn inzichtelijk.

De Oplossing (inclusief raakvlaksystemen en tooling) wordt volcontinu gemonitord op beveiligingsinbreuken zodat er direct adequaat gereageerd kan worden op (beveiligings)incidenten. Er is een alertingproces ingericht om direct (Prio 1) te kunnen handelen in geval van incidenten en (dreigende) verstoringen en als de drempelwaarden voor de RTO (dreigen te) worden overschreden.

Excepties worden gelogd. Beveiligingsinbreuken worden daarnaast gelogd voor forensisch onderzoek.

Inbreuken worden vastgelegd en acties worden genomen de ontstane risico's te mitigeren.

UE.27	De Oplossing wordt volcontinu gemonitord en excepties worden gelogd. De logregel bevat minimaal: - Datum en tijd; - IP-adres of hostnaam van het device dat de informatie logt; - IP-adres van het remote systeem (indien met een ander systeem wordt gecommuniceerd); - Identificatie van de gebruiker of het proces; - Beschrijving van de activiteit of gebeurtenis; - Het resultaat van de activiteit of gebeurtenis. Gebeurtenissen die gelogd moeten worden: - Authenticatie/autorisatie pogingen, inloggen en uitloggen; - Acties die betrekking hebben op gebruikersprofielen, bestanden en databases of systeemservices; - Transacties tussen systemen; - Activatie en/of de-actieve van beveiligingsfunctionaliteit; - Niet gespecificeerd gedrag van systemen en applicaties (uitzonderingen, fouten en storingen); - Beveiligingsincidenten. De Oplossing dient Logbestanden te kunnen maken die beveiligd zijn tegen ongeautoriseerde toegang/wijziging en zijn geschikt om forensisch onderzoek te verrichten. Logregels bevatten geen informatie waarmee de beveiliging van de Oplossing gecompromitteerd kan worden. Via alerting wordt direct adequaat gereageerd op excepties om de situatie te onderzoeken en eventuele risico's te mitigeren. Onder excepties vallen ook incidenten rond ongeautoriseerde toegang en wijziging van logbestanden. Procedures voor kennisgeving en afhandeling worden afgestemd met die van de Opdrachtgever en in de DAP vastgelegd.
-------	--

(BIO referenties 9.4.4.2, 14.4.2.2, 16.1.7.1)

W 8	Configureerbaarheid van alerting Het dient mogelijk te zijn events te definiëren die leiden tot automatische signalering aandaartoe gerechtigde Gebruikers die de beheerorganisatie vormen. Dit zorgt erbijvoorbeeld voor dat , een beheerder, als gerechtigde Gebruiker, tijdig kan reageren op het signaal. De Opdrachtgever zou graag configuratie mogelijkheden hebben van de automatische signaleringsfunctionaliteit voor wat betreft limieten en thresholds. Vraag Beschrijf en geef aan of de Oplossing onderstaande mogelijkheden biedt:
-----	---

	- Mogelijkheden van het instellen van limieten en thresholds bij het signaleren van de volgende events: - platform problemen; - API-problemen. - Mogelijkheden van het instellen van specifieke bandbreedte van limieten en thresholds per API: Beoordeling - Uit de beantwoording blijkt dat de Oplossing niet de mogelijkheden heeft voor het instellen van limieten en thresholds bij het signaleren van: - Platform problemen = 0 punten. - API-problemen = 0 punten. - Uit de beantwoording blijkt dat de Oplossing de mogelijkheden heeft voor het van instellen van limieten en thresholds bij het signaleren van: - Platform problemen = 3 punten; - API-problemen = 3 punten. - Er zijn mogelijkheden omschreven van het instellen van specifieke bandbreedte van limieten en thresholds per API = 2 punten. In uw uitwerking, maximaal 1 pagina's A4 (Lettertype Arial, lettergrootte 10 en regelafstand 1,0), dient u de bovenstaande onderwerpen per punt uit te werken. Het maximum aantal te behalen punten voor deze Wens is 8 punten.
--	---

Autorisatie en Authenticatie

Toegang tot Oplossing en Gegevens van de Opdrachtgever gebeurt op basis van need-to-know en least privilege. Anders gezegd: gebruikers van zowel Opdrachtgever als Opdrachtnemer krijgen alleen die rechten die nodig zijn voor het uitoefenen van hun vastgestelde taken voor wat betreft Gegevens en functionaliteit van de Oplossing. Dit is overigens ook van toepassing op raakvlaksystemen (koppelende applicaties).

De Oplossing is zodanig ingericht dat deze principes zijn toe te passen.

UE.28	Toegang tot de Oplossing (inclusief raakvlaksystemen en tooling) en de Gegevens van de Opdrachtgever gebeurt op basis van de principes need-to-know, zero trust en least privilege. De Oplossing heeft de (technische) mogelijkheden om invulling te geven aan deze principes.
-------	--

(BIO referentie 6.1.2.1, 9.4.1.1, 9.4.1.2, 9.4.4.1)

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

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

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

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

UE.29	De Oplossing dient minimaal wachtwoorden te ondersteunen die aan de eisen zoals gesteld in de BIO voldoen: 1) Algemeen (technisch afdwingen) a. Gebruik van wachtwoorden wordt geautomatiseerd afgedwongen b. Initiële wachtwoorden (inclusief die gereset zijn) zijn een werkdag geldig en worden bij eerste gebruik gewijzigd c. Eisen aan wachtwoorden worden geautomatiseerd afgedwongen. d. Indien de Oplossing een multi-factor authenticationmechanisme ondersteund, dan dient dat deze te worden ingericht op basis van rollen indien de Oplossing een multi-factor authenticationmechanisme ondersteund, dan dient dat deze te worden ingericht op basis van rollen. 2) Indien de Oplossing geen Multi Factor Authenticatie (MFA) biedt, gelden de volgende aanvullende eisen: a. Minimaal 12 posities, complex (nummers, klein, groot) b. Aantal foutieve inlogpogingen: 10. Na 10 foutieve inlogpogingen dient de Oplossing automatisch het account te blokkeren. c. Minimaal jaarlijks vernieuwen.
-------	---

(BIO Referentie 9.4.3.1, 9.4.3.1-4)

3.4 Koppelingen

Een Oplossing staat zelden op zichzelf. Ook niet als het off-premise staat. De Oplossing zijn vaak met andere ICT-systemen binnen de Opdrachtgever gekoppeld. Denk ook aan de kantooromgeving van de Opdrachtgever. Of aan Gebruikers van buiten de Opdrachtgever die de Opdrachtgever toegang wil verlenen tot de Oplossing.

Hetzelfde geldt voor on-premise Oplossingen. In alle gevallen zullen er aansluitvoorwaarden van toepassing zijn.

De Opdrachtgever werkt met een standaard werkplek. Alleen goedgekeurde software kan vanuit een centraal punt geïnstalleerd worden. In de praktijk komt het erop neer dat naast een (standaard) webbrowser geen gebruik gemaakt kan worden van additionele software (zoals browser plug-ins) of additionele hardware (zoals dongles). Dit noemt de Opdrachtgever een zero-footprint cliënt.

In de praktijk betekent dat dat er gebruik wordt gemaakt van een web browser als cliëntprogramma. De Opdrachtgever ondersteunt op de eigen werkplek Google Chrome. Voor toegang door burgers en bedrijf moeten alle gangbare browsers ondersteund worden.

GUE 112.	De Oplossing maakt gebruik van een zero-footprint cliënt en maakt gebruik van een standaard (gangbare) web browser.
GUE 113.	De Oplossing is apparaat-onafhankelijk te gebruiken op gangbare gebruikersapparaten die over een webbrowser beschikken. De volledige functionaliteit van de Oplossing wordt ondersteund door de drie meest gangbare webbrowsers. Op het moment van publicatie zijn dat: Google Chrome, Microsoft Edge en Apple Safari. De Oplossing ondersteunt minimaal de huidige versie en de voorgaande versie van de webbrowsers welke nog actief worden ondersteund door de leverancier van de webbrowser.

In geval dat Derde partijen moeten koppelen aan de Oplossing van Opdrachtnemer dan is Opdrachtnemer verantwoordelijk voor de beveiliging van de koppeling. Indien een beveiligde koppeling niet gerealiseerd kan worden dan kan de koppeling niet in gebruik genomen worden.

UE.30	Opdrachtnemer is verantwoordelijk voor een beveiligde koppeling met Derden tenzij anders overeengekomen met de Opdrachtgever. Alle koppelingen zijn gedocumenteerd en nog relevante risico's zijn benoemd.
-------	---

De API's van de Oplossing zelf, zijn gedocumenteerd en de koppeling is beveiligd.

UE.31	De API-documentatie is actueel, correct voor wat betreft de laatste versie van de Oplossing en wordt op verzoek beschikbaar gesteld aan de Opdrachtgever.
-------	---

Koppelbaarheid - ontsluiten back-end systemen

UE.32	De Oplossing ondersteunt het ontsluiten van data van bestaande en nieuwe back-end systemen met een API in ieder geval volgens: - REST - SOAP - GraphQL - WebSocket - gRPC
-------	---

UE.33	De Oplossing moet te koppelen zijn aan de identity providers van de Opdrachtgever, minimaal op basis van OAuth2. Opdrachtnemer is verantwoordelijk om tijdens de Realisatie fase twee koppelingen te maken: 1. Productiewaardig Oplossing Extern met de identity providers van de Opdrachtgever; 2. Productiewaardig Oplossing Intern met de identity providers van de Opdrachtgever.
-------	--

Hoofdstuk 4. Business Etiquette

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

UE.34	Opdrachtnemer conformeert zich aan de Business Etiquette zoals opgenomen in Bijlage 4 Handreiking Due diligence ISV van het Beschrijvend Document.
-------	--

Hoofdstuk 5. Maatschappelijk Verantwoord Inkopen (MVI)

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

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

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

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

5.1. Milieu

GUE 114.	De Oplossing wordt met hybride hosting uitgevraagd met het off premises gedeelte (control plane) binnen de EER.
----------	---

5.2. Ketenverantwoordelijkheid (ISV)

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

Op deze opdracht zijn de generieke sociale voorwaarden van toepassing.

GUE 115.	De keten van leveranciers bevindt zich in de EER.
----------	---

GUE 116.	Inschrijver zal de sociale voorwaarden (Bijlage 3) op eerste verzoek van de Aanbestedende dienst, maar niet eerder dan na het mededelen van de gunningsbeslissing, invullen en ondertekend aanleveren.
----------	--

UE.35	Opdrachtnemer dient rekening te houden met de verplichtingen uit hoofde van de bepalingen inzake de arbeidsbescherming en de arbeidsvoorwaarden die gelden in het land waar de opdracht wordt uitgevoerd, zoals bedoeld in artikel 2.81 lid 2 Aw2012.
-------	---

	Kennis omtrent die belastingen en milieubescherming, arbeidsvoorwaarden en arbeidsbescherming kunnen Inschrijvers, voor zover het gaat om uitvoering in Nederland, verkrijgen bij: • Opdrachtgever, www.Opdrachtgever.nl; • het Ministerie van Infrastructuur en Waterstaat, https://www.rijksoverheid.nl/ministeries/ministerie-van-infrastructuur-en-waterstaat; • het Ministerie van Sociale Zaken en Werkgelegenheid, www.rijksoverheid.nl/ministeries/szw.
--	---

Hoofdstuk 6. Juridische kaders

De in Bijlage 2 Concept Overeenkomst van het Beschrijvend Document opgenomen concept Overeenkomst kan - alvorens deze door Inschrijver(s) wordt ondertekend - door de Aanbestedende dienst worden gewijzigd en nader uitgewerkt, mede naar aanleiding van de door de Inschrijver gedane opmerkingen en tekstsuggesties als bedoeld in paragraaf 3.2.1. (nadere inlichtingen of vragen over de aanbestedingsstukken) Beschrijvend Document. De wijzigingen en/of de aangepaste overeenkomst zullen/zal de Inschrijvers per nota van inlichtingen kenbaar worden gemaakt.

GUE 117.	Inschrijver gaat akkoord met de concept Overeenkomst met inbegrip van de eventuele per Nota van Inlichtingen kenbaar gemaakte wijzigingen zoals genoemd in deze paragraaf.
----------	--

Hoofdstuk 7. Prijsstelling

7.1. Algemene eisen ten aanzien van Prijzen

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

- periodieke rapportages,
- periodiek overleg,
- inspecties,
- evaluaties,
- toekomstverkenningen,
- deelname aan begeleidings- en stuurgroepen,
- reis- en verblijfkosten voor externe bijeenkomsten,
- het verstrekken van de benodigde toegangscode voor gebruik van de Oplossing,
- Materialen en Documentatie vereist voor het gebruik van de Oplossing..

UE.36	Kosten die niet in de Inschrijving genoemd worden en niet verdisconteerd zijn in de Prijzen, maar toch noodzakelijk blijken te zijn voor een optimaal functioneren van de Oplossing conform de in de Aanbestedingsstukken gestelde eisen en de in de Inschrijving opgenomen beantwoording van de Wensen, kan Opdrachtnemer niet in rekening brengen bij Opdrachtgever.
GUE 118.	Eventuele valutarisico's zijn volledig voor rekening van Opdrachtnemer en worden geacht in de geoffreerde Prijzen te zijn verwerkt.
UE.37	Voor zover Opdrachtnemer gehouden is omzetbelasting in rekening te brengen, zullen de in het Prijzenformulier vermelde bedragen worden verhoogd met het geldende percentage omzetbelasting.

7.2. Toelichting Prijscomponenten in Bijlage VII “Prijzenformulier”

De Aanbestedende dienst wenst een Inschrijver te contracteren die marktconforme Prijzen offreert ten aanzien van de Oplossing, Diensten en Additionele dienstverlening ten behoeve van de Aanbestedende dienst. In Bijlage VII ‘Prijzenformulier’ is een aantal tabbladen opgenomen die door Inschrijver dienen te worden ingevuld.

Tabblad ‘Samenvatting’

Het betreft hier een samenvatting van de hieronder genoemde tabbladen. De Vergelijkingswaarde betreft het totaal van de geoffreerde Prijzen. De Vergelijkingswaarde wordt gebruikt om de Inschrijvingen met elkaar te vergelijken en de ‘Economisch Meest Voordelige Inschrijving’ te bepalen. In dit tabblad dient Inschrijver enkel de naam van de Inschrijver in te vullen (cel D9).

Tabblad ‘o. Dimensionering’

Dit tabblad geeft een overzicht van de te verwachte dimensionering. Hierin hoeft de Inschrijver niets in te vullen.

Tabblad '1. Realisatie'

In dit tabblad vult de Inschrijver het bedrag in voor de Realisatie van de Oplossing zoals beschreven in Bijlage XII Realisatiefase en verwerkt in het Plan van Aanpak (PvA) als uitkomst van Wens 6

In het tabblad dient Inschrijver het geel gearceerde velden in te vullen, te weten:

1. 1a) Vaste Prijs. Hierin kan Inschrijver zijn vaste prijs invullen met betrekking tot Realisatie van de Oplossing (conform PvA uit Wens 6) inclusief een onderbouwing hiervan.
2. 1b) Tarief Opleiding per Gebruiker per dag evenals de dagdelen die hiervoor nodig zijn (zie ook UE 72) met betrekking tot Realisatie van de Oplossing (conform PvA uit Wens 6) inclusief een onderbouwing hiervan.

Tabblad '2. Gebruiksrecht'

Het Gebruiksrecht van de Oplossing kan door Inschrijvers op twee manieren worden aangeboden (zie hiervoor tabblad 2a en 2b). Beide zijn op basis van subscription onderscheidt zit hem in:

- a. Tabblad 2a Subscription gebaseerd API calls en op Staffel;
- b. Tabblad 2b Enterprise, gebaseerd op Subscription;

In het/ de tabblad(en) dient Inschrijver het geel gearceerde veld(en) in te vullen, te weten

Ad a. Het Gebruiksrecht van de Oplossing op basis van subscription heeft betrekking op een licentiemodel, waarbij de Opdrachtgever een eventuele vaste Vergoeding per jaar betaald van maximaal € 50.000- gecombineerd met een Vergoeding o.b.v. het aantal API Calls. Desgewenst met gebruikmaking van een staffelkorting (met inbegrip van Beheer en Onderhoud). Biedt u geen staffel dan kunt u in de cellen de waarde o (%) invullen.

Ad b. De Enterprise site licentie gebaseerd op subscription, heeft betrekking op een jaarlijks licentiemodel, waarbij de Opdrachtgever een Vergoeding per jaar betaald, ongeacht het aantal API Calls (met inbegrip van Support, Beheer en Onderhoud). Desgewenst met gebruikmaking van een staffelkorting.

Inschrijver dient ten minste één van de twee licentiemodellen te offeren. Indien Inschrijver meerdere licentiemodellen offreert, wordt de laagste waarde gebruikt om de Inschrijvingen met elkaar te vergelijken en de 'Economisch Meest Voordelige Inschrijving' te bepalen. Verrekening voor het gebruik van de Oplossing vindt altijd plaats op basis van het voor de Opdrachtgever meest gunstige licentiemodel.

Tabblad '2a. Gebruiksrecht – Staffel'

Indien Inschrijver (ook) dit licentiemodel aanbiedt dient Inschrijver in het tabblad de volgende geel gearceerde velden in te vullen:

1. Vaste vergoeding per jaar(max €50.000,-)
2. Vergoeding per API Call
3. De kortingspercentage per voorgeschreven staffel

Tabblad ‘2b. Gebruiksrecht – Enterprise’

Indien Inschrijver (ook) de Enterprise site licentie offreert, dient Inschrijver In het tabblad Gebruiksrecht de volgende geel gearceerde velden in te vullen:

1. Jaarlijkse Vergoeding Programmatuur incl. Beheer en Onderhoud ongeacht het aantal API's
2. De korting per jaar.

Tabblad ‘3. Additionele diensten’

Hier dient Inschrijver de Prijs voor de Additionele diensten Consultancy en Opleiding te offrenen, bestaande uit:

1. Consultancy uitgaande van:
 - a. 469 uur voor Consultancy gedurende de Overeenkomst (jaren 3 t/m 6), Maximum uurtarief);
 - b. 1232 uur voor Consultancy gedurende de Overeenkomst (jaren 7 t/m 20), Maximum uurtarief);
 - c. Consultancy uren (naar verwachting 320 uur) voor jaren 1 en 2 zitten in de realisatiefase en kunnen dus niet apart in rekening worden gebracht.
2. Opleidingen:
 - a. Opleiding Technisch en Applicatief beheer), Vergoeding per Gebruiker per dag uitgaande van 6 Gebruikers per jaar voor de jaren 2 t/m 11;
 - b. Opleiding Functioneel beheer Vergoeding per Gebruiker, per Dag uitgaande van 6 Gebruikers per jaar voor de jaren 2 t/m 11;
 - c. Opleiding Super user, Vergoeding per Gebruiker per dag uitgaande van 6 Gebruikers per dag per jaar voor de jaren 2 t/m 11;
 - d. Train-de-trainer (voor advanced training), Vergoeding per Gebruiker per dag uitgaande van 6 Gebruikers per jaar voor de jaren 2 t/m 11;

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

GUE 119.	Inschrijver gaat akkoord met het gestelde in paragraaf 7.2 met inbegrip van de eventuele per Nota van Inlichtingen kenbaar gemaakte wijzigingen.
----------	--

7.3. Specifieke eisen ten aanzien van Prijzen

GUE 120.	De aangeboden Oplossing is een productiewaardige Oplossing. Indien de Oplossing Programmatuur componenten nodig heeft op basis van virtualisatie, bijvoorbeeld OpenShift of VMware, dan dient u deze (inclusief benodigde Apparatuur, licenties en Beheer en Onderhoud) mee te leveren en dienen bij de Prijs inbegrepen te zijn.
----------	---

UE.38	De aangeboden Prijzen (uurtarieven) voor Consultancy zijn inclusief reis- en verblijfskosten.
-------	---

UE.39	De Vergoeding voor de Opleidingen die onderdeel uitmaken van de Realisatie dienen ingevuld te worden op tabblad '1. Realisatie' Bijlage VII 'Prijzenformulier'.
UE.40	Opleidingen die op verzoek van Opdrachtgever worden geleverd gedurende de Operationele fase van de Overeenkomst worden verrekend op basis van nacalculatie conform de Prijzen 'Opleidingen', tabblad '3. Additionele diensten' Bijlage VII 'Prijzenformulier'.
UE.41	De Vergoeding voor Beheer en Onderhoud biedt het recht om altijd gebruik te maken van de nieuwste versies van de geleverde Programmatuur zonder dat sprake is van een additionele licentievergoeding.
UE.42	Consultancy die op verzoek van Opdrachtgever wordt geleverd gedurende de Operationele fase van de Overeenkomst wordt verrekend op basis van nacalculatie conform de Prijzen 'Consultancy', tabblad '3. Additionele diensten' Bijlage VII 'Prijzenformulier'.
UE.43	De kosten voor Implementatie en de Oplossing, zijn pas verschuldigd na Acceptatie van de afgesproken mijlpalenplanning en facturatiemomenten conform UE 47.

7.4. Indexering Prijs

De door Inschrijver geoffreerde Prijzen van de 'Additionele diensten', zoals opgegeven in Bijlage VII "Prijzenformulier" mogen vanaf 2027 jaarlijks en steeds per 1 januari worden geïndexeerd op basis van de CBS-tabel 'Dienstenprijzen (DPI); commerciële dienstverlening en transport; indexcijfers 2021 = 100', (CPA2008, kwartaalindex) conform de volgende webpagina:

<https://opendata.cbs.nl/#/CBS/nl/dataset/85817NED/table?dl=AE1CF>

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

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

UE.44	De door de Opdrachtnemer geoffreerde Prijzen "Additionele diensten" mogen jaarlijks per 1 januari geïndexeerd worden conform paragraaf 7.4. De eerste indexering vindt plaats niet eerder dan 1 januari 2027.
-------	---

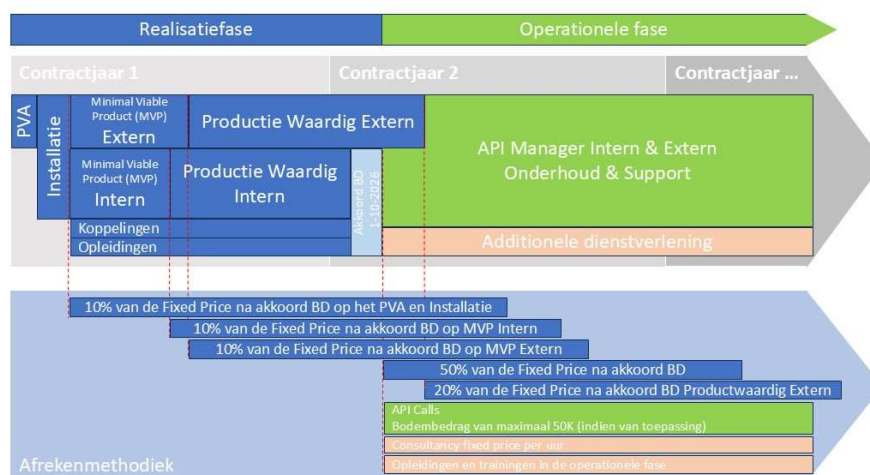
UE.45	Opdrachtnemer dient voor 1 november, voorafgaande aan de genoemde momenten van indexering, een schriftelijk verzoek in met bijbehorende onderbouwing om voor de indexering in aanmerking te komen.
-------	--

Afrekenmethode

De Realisatie van de Oplossing is als Fixed Price component opgenomen in het Prijzenformulier.

UE.46	De Opdrachtnemer heeft een resultaatverplichting voor het Productiewaardig opleveren van de Oplossing conform de mijlpalenplanning vanuit het gezamenlijk afgestemde Plan van Aanpak. Verrekening vindt plaats op basis van Fixed Price
	Het in Gebruik nemen van de Oplossing vindt plaats na Acceptatie van de Oplossing door de Opdrachtgever (zie onderstaande schema figuur 4: Afrekenmethodiek).

Onderstaande illustratie geeft aan in hoeverre de in Bijlage XII Realisatiefase uitgewerkte Realisatie fase en Operationele fase in mijlpalen, planning, en acceptatiecriteria in de tijd worden weggezet én wat de afrekenmethodiek is.



Figuur 4: Afrekenmethiek

Realisatie - Fixed Price - Factuur momenten

- Betaling 10% van de Fixed Price na Acceptatie van PvA en Installatie
- Betaling 10% van de Fixed Price na Acceptatie van Minimum Viable Product (MVP) Intern
- Betaling 10% van de Fixed Price na Acceptatie van MVP Extern
- Betaling 50% van de Fixed Price na Acceptatie van "Productwaardig maken" inclusief de API Gateway voor interne API's, Koppelingen en Opleidingen
- Betaling 20% van de Fixed Price na acceptatie van "Productie Waardig maken" inclusief de API Gateway voor externe API's.

Operationele Fase

- Afrekening per API Call per jaar achteraf, met in achtname van de vaste jaarlijkse vergoeding zoals beschreven in paragraaf 2.5.1. van het Beschrijvend Document indien het minimaal aantal API Call's niet wordt behaald.
- Consultancy op basis van een vast uurtarief, facturatie per maand achteraf.
- Opleiding Prijs per Opleiding per afgeronde opleiding, achteraf.

Hoofdstuk 8. Documentatie, Opleiding en Consultancy

8.1. Documentatie

UE.47	Opdrachtnemer zal Opdrachtgever tijdig voorzien van actuele en volledige Documentatie in elektronische vorm, ten behoeve van de Realisatie van de Oplossing en het gebruik van de Prestatie in de Operationele fase. Hierbij is de Documentatie over de eigenschappen en gebruiksmogelijkheden van de Oplossing in de Nederlandse en/of Engelse taal.
UE.48	De Documentatie dient zodanig te zijn dat zij een juiste, volledige en gedetailleerde beschrijving geeft van de door Opdrachtnemer te leveren Oplossing en de functies daarvan, zodat Gebruikers op eenvoudige wijze van alle mogelijkheden van de Oplossing gebruik kunnen maken.
UE.49	De Documentatie dient in een bewerkbaar format aangeleverd te worden, zodat Opdrachtgever deze zelf kan aanpassen wanneer Opdrachtgever in de toekomst zaken wijzigt in de configuratie van de Oplossing.
UE.50	Opdrachtgever mag de Documentatie voor gebruik binnen de eigen organisatie reproduceren en wijzigen.
UE.51	Opdrachtnemer zal de door hem geleverde Documentatie zo spoedig mogelijk vervangen, wijzigen of aanpassen indien op enig tijdstip tijdens het gebruik door Opdrachtgever van de Prestatie, blijkt dat de Documentatie onjuiste informatie bevat of anderszins onvolledig, onvoldoende, onduidelijk en/of verouderd is.
UE.52	Opdrachtnemer is verantwoordelijk dat Documentatie na een nieuwe Release actueel blijft. Na oplevering van een nieuwe Release wordt de geactualiseerde Documentatie digitaal beschikbaar gesteld.
UE.53	Opdrachtnemer geeft in de Documentatie de in de Release opgenomen aanpassingen duidelijk weer.

8.2. Opleiding

Tijdens de Realisatie fase dient Opdrachtnemer de volgende opleidingen te verzorgen:

UE.54	Soort Opleiding / Behoefte	Doelgroep	Opleidingsvorm	Aantal
	Een opleiding om ontwikkelaars/beheerders een vliegende start te geven met het installeren en technisch beheer rond API-Management product. Het gaat om een samenwerking tussen de Opdrachtnemer en de Opdrachtgever: De Opdrachtnemer brengt de best practises met zich mee ten aanzien van de Oplossing en de Opdrachtgever brengt de kennis van de Opdrachtgever omgeving in.	(Admin) / Technisch platform beheerders	On-site bij de Opdrachtgever - Support op de werkplek van de Opdrachtgever. Taal: Nederlands of Engels	6

	Gebruik API-Management uitgebreid: Opleiding bedoeld voor een aantal specialisten gericht op security, transformaties die de basiskennis ontstijgt. Het is de bedoeling dat de Opdrachtgever medewerkers experts worden van de Oplossing.	Opdrachtgever APIM Experts	Support van docent. Klassikaal op locatie van Opdrachtgever Taal: Nederlands of Engels	6
	Gebruikt API-Management basis: Een opleiding voor nieuwe gebruikers om basis kennis mee te krijgen hoe API gemaakt en beheert worden vanuit gebruikers perspectief. Methodiek 'voor doen', 'samen doen' en 'zelf doen'.	Developer	Train de trainer, op basis van training video's. Taal: Nederlands of Engels	6

UE.55	De Opdrachtnemer stelt kosteloos het opleidingsmateriaal (zoals bijvoorbeeld, maar niet gelimiteerd tot: documentatie, handboeken, powerpoints en video's) ter beschikking aan de Opdrachtgever voor (her)gebruik tijdens de uitvoering van de Overeenkomst.
-------	--

UE.56	De medewerkers van de Opdrachtgever dienen na acceptatie van de Productiewaardige Externe en Interne Oplossing zelfstandig het Technisch Beheer van de Oplossing uit te kunnen voeren.
-------	--

Tijdens de Operationele fase dient Opdrachtnemer minimaal de volgende opleidingen te verzorgen:

UE.57	Gebruikt API-Management basis: Een opleiding voor nieuwe gebruikers om basis kennis mee te krijgen hoe API gemaakt en beheert worden vanuit gebruikers perspectief.	Developer	Train de trainer, op basis van training video's	Fixed pay per use
-------	--	-----------	---	-------------------

Opdrachtgever kan andere opleidingen en of trainingen tijdens de operationele fase aangeven in het prijzenblad (Bijlage VII - Prijzenformulier).

UE.58	Opdrachtnemer levert relevante Opleidingen, inclusief Documentatie, inzake het gebruik van de Oplossing, alsmede het functioneel, technisch en applicatief beheer van de Oplossing.
-------	---

UE.59	Opleidingen vinden plaats op locatie van de Opdrachtgever tenzij nadrukkelijk anders overeengekomen .
-------	---

UE.60	Opdrachtnemer stelt voor de eindgebruikers de goedgekeurde gebruikersinstructie online beschikbaar gedurende de looptijd inclusief verlengingsopties van de Overeenkomst en houdt deze actueel.
-------	---

UE.61	Opleiding en ondersteuning dient door deskundigen, die daartoe bekwaam en geschikt zijn, te worden gegeven. In voorkomend geval kan Opdrachtgever voorafgaand aan de inzet van de betreffende deskundige(n), overlegging van, of inzage in, relevante diploma's en/of certificaten vorderen.
-------	--

UE.62	Lesmateriaal voor Gebruikers is in de Nederlandse of Engelse Taal beschikbaar.
-------	--

8.3. Consultancy

2.2.2 Consultancy

UE.63	De Opdrachtnemer biedt advies in de vorm van Consultancy in het gebruik van de Oplossing of voor maatwerk in relatie tot de Oplossing. Opdrachtnemer offreert hiervoor een All-in uurtarief, inclusief reiskosten en verblijf.
-------	--

Hoofdstuk 9. Voorbereiding- en Implementatiefase

9.1. Voorbereiding

De Opdrachtnemer dient de leiding te nemen bij de Implementatie van de Oplossing. Om inzicht te krijgen op welke wijze de Opdrachtnemer de Implementatie uit gaat voeren, dient de Opdrachtnemer een Implementatieplan van de Oplossing te leveren.

9.1.1. Implementatieplan Oplossing

UE.64	Na ondertekening van de Overeenkomst zal Opdrachtnemer in goed overleg daartoe binnen 5 kalenderdagen een planning opstellen en na afstemming met Opdrachtgever binnen 14 kalenderdagen een definitief Implementatieplan opleveren. De vervolgbepalingen in de Overeenkomst gelden hierbij onverkort.
-------	---

UE.65	Het door Opdrachtnemer definitief opgeleverde Implementatieplan dient eerst door Opdrachtgever zoals omschreven in de Overeenkomst te zijn goedgekeurd. Pas na schriftelijke goedkeuring kan worden aangevangen met de Implementatie van de Oplossing.
-------	--

9.2. Implementatie

UE.66	De Oplossing dient uiterlijk op 01-10-2026 productiewaardig en geaccepteerd te zijn.
-------	--

UE.67	Opdrachtnemer is gedurende de fase van Implementatie bereid tot overleg en samenwerking met andere partijen van overige systemen.
-------	---

9.3. Documentatie, Opleiding en Consultancy

UE.68	Opdrachtnemer levert gedurende de voorbereidings- en implementatiefase van de Overeenkomst Documentatie, Opleiding en Consultancy conform de eisen zoals neergelegd in Hoofdstuk 8 'Documentatie, Opleiding en Consultancy'.
-------	--

9.3.1. Opleiding

UE.69	Opdrachtnemer geeft op aanvraag van Opdrachtgever aan iedere doelgroep, werkzaam in de organisatie van Opdrachtgever (een) passende Opleiding(en) bestaande uit concrete invulling, zoals opleiding, cursus, instructie, product sessies/seminars, etc.
-------	---

UE.70	In geval van uitstel of vertraging van de Implementatie van de Prestatie en/of in het geval de Aflevering van de Programmatuur wordt uitgesteld of vertraagd, is Opdrachtgever gerechtigd tot wijziging van de tijdstippen, dan wel wijziging van het aantal personeelsleden te verlangen dat aan de Opleiding deelneemt.
-------	---

Hoofdstuk 10. Operationele fase

10.1. Onderhoud en Support

Opdrachtnemer is gehouden tot het leveren van Onderhoud en Support ten behoeve van Oplossing. Dit betekent onder andere dat Opdrachtnemer derde lijns Onderhoud en Support levert bij Incidenten. Het Onderhoud en Support in de eerste en tweede lijn wordt namelijk door de Opdrachtgever zelf uitgevoerd.

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

GUE 121.	Inschrijver levert bij inschrijving, op basis van de in paragraaf 10.1.1 van Bijlage A 'Specificaties van de opdracht' gespecificeerde Service Levels, een SLA op. De SLA beschrijft in elk geval de wijze waarop door Opdrachtnemer invulling wordt gegeven aan derde lijns Onderhoud en Support. De SLA bevat minimaal de volgende onderdelen: - Doel en scope van het document - Benoeming partijen, verantwoordelijkheden en werkingsgebied - Aanvang, looptijd, wijzigingsbeleid, vaststelling en ondertekening - Gerelateerde documenten - Beschrijving en scope van de dienstverlening - In het kader van informatiebeveiliging: 1) Servicedesk (melding en oppakken prio 1-security incidenten, datalekken) 2) Change-en releasemanagement (waaronder security patches en significante juridische en infrastructurele wijzigingen) 3) Continuïteit (Business Continuity Management / BCM) 4) Securitymanagement: • Incident- en problemmanagement • Audits, beveiligingstesten (A&P-testen, vulnerability scans) en continuïteitstesten (backup & restore, Calamiteitentests) • Monitoring, alerting en logging 5) Rapportage Deze SLA vormt mede de basis voor de nog overeen te komen DAP (Dossier Afspraken Procedures) tussen Opdrachtnemer en Opdrachtgever.
UE.71	De SLA wordt binnen 4 weken na het tekenen van de Overeenkomst tussen Opdrachtnemer en Opdrachtgever vastgesteld. 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 na ondertekening door Partijen als bijlage aan de Overeenkomst worden toegevoegd.
UE.72	Opdrachtnemer voert het Onderhoud uit op locatie van Opdrachtgever ten behoeve van het on-premise gedeelte van de Oplossing, tenzij nadrukkelijk schriftelijk anders is overeengekomen.

UE.73	Gedurende de Realisatie fase wordt de door de Opdrachtnemer aangeleverde concept SLA in overeenstemming met de Opdrachtnemer definitief gemaakt conform de in het bestek gestelde eisen en wensen. 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 en maakt onlosmakelijk deel uit van de Overeenkomst.
-------	--

De gehanteerde begrippen en daarmee BIJLAGE 1 ICT Begrippenlijst zijn een integraal onderdeel van deze aanbesteding en zullen tevens tijdens de looptijd van de Overeenkomst van toepassing blijven.

UE.74	Tijdens de Realisatie fase zullen de begrippen in de SLA in overeenstemming met de Begrippenlijst van BIJLAGE 1 ICT Begrippenlijst worden gebracht. Daarbij is de uitleg van het begrip in de BIJLAGE 1 ICT Begrippenlijst leidend.
-------	---

UE.75	Opdrachtnemer verplicht zich om ten minste Onderhoud te verlenen op de voorlaatste (versie n-1) en nieuwste versie (versie n) van de Oplossing
-------	--

10.1.1. Service Levels

Omschrijving	Indicator	KPI
Openstelling service desk	Reguliere openingstijd service desk.	Op Werkdagen Maandag t/m Vrijdag: 08:00 – 18:00 Nederlandse tijd (GMT +1)
	Openingstijd service desk voor melden van prio 1 Incidenten	7*24 uur, 365 dagen per jaar*
Service uren	Reguliere service uren waarin ondersteuning wordt geleverd.	Op Werkdagen Maandag t/m Vrijdag: 08:00 – 18:00 Nederlandse tijd (GMT +1)
Monitoring en alerting	Opdrachtnemer heeft een monitoring en alerting proces ingericht om direct te kunnen handelen in geval van (security) Incidenten en (dreigende) verstoringen van de beschikbaarheid van de Oplossing.	7*24 uur, 365 dagen per jaar*
Prio 1 Incident en/of kritisch Beveiligingsincident oplossen	Oplossen conform Tabel 6: <i>Service Levels Servicedesk en Incidentmanagement</i> .	Werkt ook buiten service uren door.
3e Lijns ondersteuning	Opdrachtgever verzorgt zelf de 1e en 2e lijns ondersteuning.	Op Werkdagen Maandag t/m Vrijdag: 08:00 – 18:00 Nederlandse tijd (GMT +1) support.

Tabel 5: Service Window

Nota Bene: in het geval van een schrikkeljaar geldt 366 dagen.

REACTIETIJD			
Reactietijd	Prio 1	30 minuten	100%
Reactietijd	Prio 2	60 minuten	100%
Reactietijd	Prio 3	8 uur	100%
Reactietijd	Service request	1 Werkdag	100%
OPLOSTIJD			
Oplostijd	Prio 1	8 uur	100%
Oplostijd	Prio 2	1 Werkdag	100%
Oplostijd	Prio 3	5 Werkdagen	100%
STREEF HERSTELTIJD (INSPANNING)			
Hersteltijd	Prio 1	2 Werkdagen	98%
Hersteltijd	Prio 2	5 Werkdagen	95%
Hersteltijd	Prio 3	10 werkdagen	90%

Tabel 6: Service Levels Servicedesk en Incidentmanagement.

Incidenten kunnen met drie verschillende prioriteiten aangemeld worden. Aan elk Incident, ongeacht de vermoedelijke oorzaak van een Incident, wordt een prioriteit toegekend op basis van Impact en Urgentie. Naast de door de Opdrachtgever gemelde Incidenten aan de Servicedesk van de Opdrachtnemer worden tevens de meldingen die middels het automatisch uitbellen/signaleren van de Oplossing bij de Opdrachtnemer beschouwd als daadwerkelijke Incidenten.

Impact	
Hoog	Een Incident heeft of kan ernstige gevolgen hebben voor: - één of meer bedrijfsprocessen die de burger en/of het bedrijf direct raken, en/of - één of meer fabriekstaken voor (massale) gegevensverwerking en/of - de Informatiebeveiliging en/of - het imago van de Opdrachtgever en/of - onacceptabele hoge kosten
Laag	- Overige situaties
Urgentie	
Hoog	Een Incident - beïnvloedt kwaliteit van functies/Beschikbaarheid/beveiliging en/of - brengt integriteit van de Gegevens in het geding (o.a. (potentiële) Datalekken) en/of - treedt op tijdens piektijd/-periode van het bedrijfsproces en/of - brengt uiterste verzenddatum van klantbescheiden in gevaar en/of - verstoort de communicatie met de klanten van de Opdrachtgever en/of - er geen Workaround mogelijk is en/of

	- de verwerking kan niet worden uitgesteld en/of - de schade is al een feit of zal dat zijn binnen 24 uur
Laag	- Overige situaties
Prioriteit	
	- Impact Hoog / Urgentie Hoog geeft Prio 1 - Impact Hoog / Urgentie Laag geeft Prio 2 - Impact Laag / Urgentie Hoog geeft Prio 2 - Impact Laag / Urgentie Laag geeft Prio 3

Tabel 7: Impact, Urgentie en Prioriteit

UE.76	Indien een Incident niet binnen de Oplostijd wordt opgelost, wordt het Incident geëscaleerd naar de bovenliggende Prioriteit (Prio 3 wordt Prio 2 en Prio 2 wordt Prio 1).
UE.77	Opdrachtnemer conformeert zich aan bovenstaande tabellen: - Tabel 5: Service Window - Tabel 6: Service Levels Servicedesk en Incidentmanagement. - Tabel 7: Impact, Urgentie en Prioriteit

10.1.1.1. Kwetsbaarheden

Kwetsbaarheden kunnen onder andere ontdekt worden naar aanleiding van cyberhack, responsible disclosure, beveiligingstesten, berichten in de media, meldingen van leveranciers en op basis van informatie uit de CVE database.

Beveiligingsincidenten zijn incidenten die een vermoedelijke of mogelijk opzettelijke inbreuk veroorzaken op de beschikbaarheid, vertrouwelijkheid of integriteit van de Gegevens in informatieverwerkende systemen of inbreuk maken op deze systemen zelf. Kwetsbaarheden kunnen onder andere ontdekt worden naar aanleiding van cyberhack, responsible disclosure, beveiligingstesten, berichten in de media, meldingen van leveranciers en op basis van informatie uit de CVE database.

Voor beveiligingsincidenten geldt dat bij ontdekking/melding zowel de Impact als Urgentie als Hoog worden gekwalificeerd wat resulteert in een prioriteit 1 incident. Een beveiligingsincident wordt altijd per direct opgevolgd met een actie van de Opdrachtnemer. Na een eerste evaluatie kan onderbouwd besloten worden de prioriteit te verlagen. De Opdrachtgever heeft hierbij het laatste woord.

Er worden op dit moment vier typen beveiligingsincident onderkend:

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

Als waarderingsmethodiek voor kwetsbaarheden wordt gebruik gemaakt van de meest recente versie van marktstandaard Common Vulnerability Score System (CVSS, momenteel versie 3.0). Oplostermijnen die hier aan gekoppeld zijn, zijn:

- Kritisch risico (Critical risk, score 9.0 – 10.0): per direct (voor in productie gaan van een nieuwe Oplossing is dit belemmerend). Voor de Opdrachtgever is dit een incident.
- Hoog risico (High risk, score 7.0 – 8.9): per direct, na afstemming maximaal 1 maand (voor in productie gaan van een nieuwe Oplossing is dit belemmerend). Voor de Opdrachtgever is dit een incident.
- Gemiddeld risico (Medium risk, score 4.0 – 6.9): 3 maanden. Voor de Opdrachtgever is dit een problem.

- Laag risico (Low risk, 0.1 – 3.9): 6 maanden. Voor de Opdrachtgever is dit een problem.

De Opdrachtgever heeft geen Oplossingen in productie staan waarin zich Kwetsbaarheden bevinden die als Kritisch of Hoog risico zijn gekwalificeerd. Bij Kritische- en Hoge risico's kan een Leg-uit alleen gebruikt worden om de oplostermijn (beperkt) op te rekken. Dit kan alleen met nadrukkelijke instemming van de Opdrachtgever.

UE.78	Voordat de Oplossing in productie kan gaan is de beveiliging van de Oplossing getest en door Opdrachtgever geaccepteerd.
-------	--

Staat de ICT-oplossing nog niet in productie dan zal dat ook niet mogen totdat de Kritische-en Hoge risicobevindingen zijn weggenomen. Bekende kwetsbaarheden worden onverwijld gemeld.

Gemiddeld- en Laagrisicobevindingen worden afgehandeld conform het Pas-toe-of-Leg-uitprincipe. Dit laatste, een Leg uit (Explain), betekent dat er besloten is dat de kwetsbaarheid niet weggenomen wordt of dat adresseren ervan meer tijd gaat kosten dan de standaard Oplostermijn. Opdrachtnemer onderbouwt zijn besluit (bijvoorbeeld: er zijn afdoende mitigerende maatregelen getroffen waardoor de kwetsbaarheid niet uitgevoerd hoeft te worden of dat de impact nihil is). Het is aan de Opdrachtgever om akkoord te gaan met een Leg-uit.

UE.79	Bij het constateren van Kwetsbaarheden met een niveau van kritisch (critical) of hoog (high), conform de meest recente versie van CVSS, wordt de Opdrachtgever daarover binnen één (1) uur door Opdrachtnemer geïnformeerd. De rollen en contactpersonen die gecontacteerd dienen te worden, worden in DAP vastgelegd.
-------	--

(BIO Referentie 12.6.1.1)

UE.80	Opdrachtnemer conformeert zich aan de door de Opdrachtgever gebruikte methode (CVSS 3.0) om beveiligingsincidenten te kwalificeren en heeft zijn organisatie zodanig ingericht dat de door de Opdrachtgever onderkende typen beveiligingsincidenten voor (onderdelen) van de Oplossing binnen gestelde termijnen opgepakt en opgelost (patchmanagement) worden: - Kritisch risico (Critical risk): per direct (belemmerend voor in productie gaan). - Hoog risico (High risk): 1 maand (belemmerend voor in productie gaan). - Gemiddeld risico (Medium risk): 3 maanden - Laag risico (Low risk): 6 maanden
-------	--

UE.81	Opdrachtnemer conformeert zich aan onderstaande: Indien er gegronde redenen zijn om een Kwetsbaarheid die als 'Gemiddeld' of 'Laag' is geclassificeerd, niet te verhelpen, dan bespreekt Opdrachtnemer dit met Opdrachtgever. Zolang Opdrachtgever geen contact opneemt met Opdrachtnemer blijft de Oplostermijn conform CVSS doorlopen.
-------	---

UE.82	Bij het constateren van Kwetsbaarheden met een niveau van kritisch (critical) of hoog (high), conform CVSS 3.0, wordt de Opdrachtgever daarover binnen één (1) uur door Opdrachtnemer geïnformeerd.
-------	---

UE.83	Kwetsbaarheden die leiden tot een Incident worden gekwalificeerd door middel van CVSS 3.0. Op basis van de CVSS 3.0 kwalificaties gelden de volgende Oplostijden voor Opdrachtnemer: • Kritisch (critical): per direct (binnen vier (4) uren) op te lossen. • Hoog (high): binnen één (1) maand. • Gemiddeld (medium): binnen drie (3) maanden. • Laag (low): binnen zes (6) maanden.
-------	---

Beveiligingsincidenten

Beveiligingsincidenten moeten direct gemeld kunnen worden bij zowel Opdrachtnemer als de Opdrachtgever. Er is 24/7 een loket waar beveiligingsincidenten gemeld kunnen worden en van waar uit actie genomen kan worden om het incident verder af te handelen. Dit is ook van toepassing op meldingen voor wat betreft inbreuk op persoonsgegevens. Inschrijver heeft hier een proces voor ingericht.

Elk beveiligingsincident wordt in eerste instantie als prioriteit 1-incident beschouwd. De Opdrachtgever wordt hiervan per direct op de hoogte gesteld.

GUE 122.	Opdrachtnemer beschikt over een meldloket waar beveiligingsincidenten en (potentiële) Datalekken per direct het hele jaar door 24/7 gemeld kunnen worden. Opdrachtnemer zal de omvang van het incident aangeven, de verwachte consequenties voor de Opdrachtgever alsmede de reeds getroffen en te treffen maatregelen om de gevolgen te beperken. Procedures worden vastgelegd en beschreven in de DAP.
----------	---

Zodra technische kwetsbaarheden bekend worden bij Opdrachtnemer, dient hij ze te evalueren en er, indien nodig, zo snel mogelijk op te acteren. Bij Patchmanagement in het kader van het oplossen van beveiligingsmaatregelen wordt gebruik gemaakt van de termijnen zoals de Opdrachtgever deze hanteert.

GUE 123.	Opdrachtnemer heeft Patchmanagement ingericht, met als doel dat tenminste technische kwetsbaarheden kunnen worden ontdekt, geëvalueerd en geadresseerd. Opdrachtnemer draagt zorg voor een analyse en afhandeling van het beveiligingsincident of de (mogelijke) inbreuk op persoonsgegevens. De afhandelingswijze wordt geborgd in de DAP.
----------	--

(BIO Referenties 12.2.1.5, 12.6.1.1)

GUE 124.	Op het gebied van afhandeling van beveiligingsincidenten en privacymeldingen zijn er contactpersonen die vanuit die rollen de situatie kunnen beoordelen en er adequaat op kunnen (laten) acteren. Deze contactpersonen zijn 24/7 bereikbaar (buiten kantoor tijden evt. volgens een stand by-regeling). In de DAP worden de contactpersonen en rollen vastgelegd.
----------	--

(BIO Referentie 6.1.1.1)

GUE 125.	Opdrachtnemer heeft een gemandateerde contactpersoon specifiek voor het afhandelen van prioriteit 1 incidenten is deze contactpersoon 24/7 bereikbaar (buiten kantoor tijden evt. volgens een stand by-regeling). In de DAP worden de contactpersoon en rol vastgelegd. In de SLA worden nadere afspraken omtrent het afhandelingsproces van het incident vastgelegd.
----------	--

(BIO Referentie 6.1.1.1)

De Opdrachtgever houdt er rekening mee dat Opdrachtnemer zijn Oplossing ook levert of gaat leveren aan Derden. Indien op de Oplossing bij Derden zich inbreuken op beveiliging en/of persoonsgegevens voordoen, die zich ook kunnen voordoen in de aan de Opdrachtgever geleverde Oplossing, dan wordt de Opdrachtgever

daarvan op de hoogte gebracht om zo nodig mitigerende maatregelen te kunnen treffen. Het gaat niet alleen om opgetreden incidenten, maar ook om mogelijke toekomstige incidenten waar Opdrachtnemer van kan uitgaan dat deze in de (nabije) toekomst kunnen optreden. Denk aan bijvoorbeeld een kwetsbaarheid zoals een zero-day exploit.

Het gaat de Opdrachtgever om het (technisch) inhoudelijke incident om dit te kunnen analyseren en –zo nodig– mitigerende maatregelen te treffen. Er worden nadrukkelijk geen bedrijfsgegevens van getroffen partijen gedeeld.

UE.84	Opdrachtnemer informeert de Opdrachtgever onmiddellijk wanneer er een kwetsbaarheid wordt geconstateerd of verwacht, betreffende de Gegevens en/of de Oplossing waar de Opdrachtgever gebruik van maakt die ook in gebruik zijn bij andere klanten van Opdrachtnemer. Opdrachtnemer zal in dat geval tevens de omvang van de kwetsbaarheid aangeven, de verwachte consequenties voor de Opdrachtgever alsmede de reeds getroffen en te treffen maatregelen om de gevolgen te beperken. Procedures worden vastgelegd en beschreven in de DAP.
-------	---

Datalek afhandeling

De Verwerkingsverantwoordelijke is de partij die conform de wettelijke kaders als primaire partij Datalekincidenten afhandelt. De Verwerkingsverantwoordelijke is in bepaalde gevallen verplicht de Autoriteit Persoonsgegevens binnen 72 klokuren hiervan op de hoogte te stellen. In alle gevallen brengt de Opdrachtnemer de Opdrachtgever onverwijld op de hoogte van een vermoed Datalek (potentieel Datalek). Deze afspraken zijn vastgelegd in de verwerkersovereenkomst.

Aan een (potentieel) Datalek kan een beveiligingsincident ten grondslag liggen. De afhandeling van een (potentieel) Datalek en het onderliggende beveiligingsincident kunnen parallel worden afgehandeld.

UE.85	Opdrachtnemer heeft gemandateerde contactpersonen specifiek voor het afhandelen van privacy gerelateerde zaken. In de DAP wordt de contactpersoon en rol vastgelegd.
-------	--

(BIO Referentie 6.1.1.1)

UE.86	Opdrachtnemer en Opdrachtgever zijn beide gedeeltelijk Verwerkingsverantwoordelijke. Beide partijen brengen elkaar onverwijld op de hoogte van een (potentieel) Datalek. In afstemming wordt bepaald welke partij de melding aan de Autoriteit Persoonsgegevens doet en welke partij primair analyse en afhandeling uitvoert. Procedures worden vastgelegd en beschreven in de DAP.
-------	--

10.1.1.2. Beschikbaarheid

UE.87	De Oplossing voldoet ten minste aan de Beschikbaarheid van de Oplossing zoals opgenomen in de tabel Service Level Beschikbaarheid en bovenstaande tekst onder Beveiligingsincidenten na te komen. De berekening van de Beschikbaarheid is als volgt: - Berekening beschikbaarheid percentage: (gerealiseerd aantal uren beschikbaarheid / overeengekomen uren beschikbaarheid) * 100%;
-------	--

	- Overeengekomen aantal uren beschikbaarheid = aantal uren openstellingstijden – (aantal uren gepland Technisch beheer en onderhoud en/of maintenance tijdens openstelling); - Gerealiseerd aantal uren beschikbaarheid = overeengekomen aantal uren beschikbaarheid – som van de oplostijden van incidenten, met invloed op de openstelling.
--	--

PI	Service Level
Beschikbaarheid per maand (Exclusief downtime bij Implementaties van wijzigingen ten aanzien van de Oplossing op verzoek van de Opdrachtnemer)	99,95% (maximale downtime 22 minuten en 44 seconden/maand)

Service Level Beschikbaarheid

10.1.1.3. Helpdesk en Incidentmanagement

Incidenten kunnen met drie verschillende prioriteiten aangemeld worden. Aan elk Incident, ongeacht de vermoedelijke oorzaak van een Incident, wordt een prioriteit toegekend op basis van Impact en Urgentie. Naast de door de Opdrachtgever gemelde Incidenten aan de Helpdesk van de Opdrachtnemer worden tevens de meldingen die middels het automatisch uitbellen/signaleren van de Oplossing bij de Opdrachtnemer beschouwd als daadwerkelijke Incidenten.

Impact	
Hoog	Een Incident heeft of kan ernstige gevolgen hebben voor • één of meer bedrijfsprocessen die de burger en/of het bedrijf direct raken, en/of • één of meer fabriekstaken voor (massale) gegevensverwerking en/of • de Informatiebeveiliging en/of • het imago van de Opdrachtgever en/of • onacceptabele hoge kosten.
Laag	• Overige situaties
Urgentie	
Hoog	Een Incident • beïnvloedt kwaliteit van functies/Beschikbaarheid/beveiliging en/of • brengt integriteit van de Gegevens in het geding en/of • treedt op tijdens piektijd/-periode van het bedrijfsproces en/of • brengt uiterste verzenddatum van klantbescheiden in gevaar en/of • verstoort de communicatie met de klanten van de Opdrachtgever en/of • er geen Workaround mogelijk is en/of • de verwerking kan niet worden uitgesteld en/of • de schade is al een feit of zal dat zijn binnen 24 uur.
Laag	• Overige situaties
Prioriteit	
	• Impact Hoog / Urgentie Hoog geeft Prio 1 • Impact Hoog / Urgentie Laag geeft Prio 2 • Impact Laag / Urgentie Hoog geeft Prio 2 • Impact Laag / Urgentie Laag geeft Prio 3

Tabel Impact, Urgentie en Prioriteit

PI	Prioriteit	Service Level	Norm
Openstelling Helpdesk	Incidenten	7 x 24 uur	100%
	Service requests	Werkdagen van 08:00 – 17:00 uur	100%
REACTIETIJD			
Reactietijd	Prio 1	30 minuten	100%
Reactietijd	Prio 2	60 minuten	100%
Reactietijd	Prio 3	8 uur	100%
Reactietijd	Service request	1 Werkdag	100%
OPLOSTIJD			
Oplostijd	Prio 1	8 uur	100%
Oplostijd	Prio 2	1 Werkdag	100%
Oplostijd	Prio 3	5 Werkdagen	100%
Streef HERSTELTIJD			
Hersteltijd	Prio 1	2 Werkdagen	98%
Hersteltijd	Prio 2	5 Werkdagen	95%
Hersteltijd	Prio 3	10 werkdagen	90%

Tabel Service Levels Helpdeks en Incidentmanagement

UE.88	Ten aanzien van de Openstelling van de Helpdesk wordt ten minste voldaan aan de Service Levels zoals opgenomen in de tabel Service Levels Helpdeks en Incidentmanagement.
UE.89	Ten aanzien van de afhandeling van Incidenten en Service requests wordt ten minste voldaan aan de Service Levels zoals opgenomen in de tabel Service Levels Helpdeks en Incidentmanagement.
UE.90	Indien een Incident niet binnen de Oplostijd wordt opgeslost, wordt het Incident geëscaleerd naar de bovenliggende Prioriteit (Prio 3 wordt Prio 2 en Prio 2 wordt Prio 1).

10.1.1.4. Release – en Patch management

UE.91	Opdrachtnemer informeert Opdrachtgever tijdig (x PERIODE) over nieuwe Releases en Patches ten behoeve van het optimaal gebruik van de Oplossing en de daarbij verwachte Impact voor Opdrachtgever.
UE.92	Het doorvoeren van Releases en Patches ten behoeve van het optimaal gebruik van de Oplossing wordt in overleg met Opdrachtgever ingepland.
UE.93	Opdrachtnemer levert voorafgaand aan de Release ten behoeve van het optimaal gebruik van de Oplossing de releasenotes ten behoeve van Acceptatie(test).
UE.94	Opdrachtnemer stelt Releases middels een beveiligde download beschikbaar.
UE.95	Gedurende de Overeenkomst is er voor Opdrachtgever een actuele Release kalender van de Oplossing beschikbaar.

10.1.1.5. Verbeterplan

UE.96	Indien de Oplossing voor een periode van drie (3) maanden niet voldoet aan één of meerdere Service Levels levert Opdrachtnemer hiervoor een Verbeterplan, inclusief een bijbehorend implementatievoorstel, aan bij de Opdrachtgever. Het verbeterplan moet leiden tot een situatie waarbij de Service Levels wel worden gerealiseerd. Het Verbeterplan wordt binnen tien (10) Werkdagen na verzoek van de Opdrachtgever opgeleverd. Toepassing van het Verbeterplan laat de overige rechten van Opdrachtgever onverlet, waaronder die op schadevergoeding.
-------	--

10.1.2. Remote support

Remote support biedt de mogelijkheid om, op ad hoc basis aan een Opdrachtnemer ondersteuning te vragen bij Incidenten, Problems of Changes. Met deze voorziening heeft Opdrachtgever de mogelijkheid Opdrachtnemer, op afstand mee te laten kijken binnen zijn/haar beheerapplicaties met aanvullend hierop het uit handen geven van toetsenbord en muis.

Opdrachtgever kan kiezen of Opdrachtnemer alleen bij een bepaalde applicatie mee kan kijken of dat deze de complete Desktop kan zien. Bij het uit handen geven van de regie krijgt Opdrachtnemer de mogelijkheid om de toetsenbord- en muisacties uit te voeren onder toezicht van de Opdrachtgever. Natuurlijk kan Opdrachtgever ten allen tijde de regie terugnemen.

Opdrachtnemers die gebruik willen maken van de Remote support functionaliteit, gaan vooraf akkoord met de huisregels in relatie tot het gebruik van Remote support. Door gebruik te maken van Remote support gaat u akkoord met onderstaande voorwaarden:

1. Door het gebruik van de aan u verstrekte URL krijgt u toegang tot vertrouwelijke gegevens van de Opdrachtgever. U mag hiervan uitsluitend zelf gebruik maken en alleen voor het doel waarvoor u uitgenodigd bent door de gastheer van de Opdrachtgever.
2. U mag verkregen informatie op geen enkele wijze overdragen, verveelvoudigen, bewerken of verspreiden dan uitsluitend voor de uitvoering van de overeengekomen werkzaamheden.
3. U bent verplicht om aanwijzingen van de Opdrachtgever omtrent het gebruik van de informatie en/of Remote support op te volgen.
4. Bij het inloggen dient u zich met uw volledige naam, voorletters en bedrijfsnaam bekend te **maken**.
5. De Opdrachtgever kan een lijst opleveren van ondersteunde besturingssystemen en browsers.
6. De Opdrachtgever is niet verantwoordelijk of aansprakelijk voor eventuele schade ten gevolge van het gebruiken van Remote support.
7. Ziet u iets afwijkends bij het gebruik van Remote support? Neem dan direct contact op met de gastheer van uw Remote support sessie.
8. Misbruik wordt bestraft.
9. Op het gebruik van Remote support is Nederlands recht van toepassing.

GUE 126.	Inschrijver conformeert zich aan bovenstaande voorwaarden indien gebruik gemaakt wordt van Remote support.
----------	--

10.1.3. Rapportage

Opdrachtgever wil periodiek een actueel inzicht in de geleverde prestaties van de Oplossing en hetgeen geëist in dit bestek.

Het gevraagde inzicht kan bijvoorbeeld middels een maandelijkse rapportage toegestuurd worden vóór de 10e van de maand, maar een Dashboard met actuele informatie is ook mogelijk.

Het is Opdrachtnemer vrij hier een keuze in te maken, zolang het inzicht in een rapportagevorm maar gegeven wordt.

UE.97	Gedurende de Realisatie fase wordt de door de Opdrachtnemer meegeleverde template, in overeenstemming met de Opdrachtnemer definitief gemaakt. Na vaststelling van de versie 1.0 zal deze jaarlijks worden onderhouden als er wijzigingen in de DAP optreden. De versienummering geeft aan welke DAP de laatste versie is. De DAP maakt onlosmakelijk deel uit van de Overeenkomst.
-------	---

UE.98	Opdrachtnemer levert middels een rapportage inzicht in de geleverde prestaties ten opzichte van de in dit document overeengekomen prestaties. Dit inzicht dient minimaal maandelijks actueel te zijn. Met name wil Opdrachtgever inzicht in: - KPI overzicht Beschikbaarheid; - KPI opgeloste Incidenten binnen en buiten Service Levels; - KPI opgeloste Beveiligingsincidenten binnen en buiten Service Levels; - Status, voortgang en afhandeling van openstaande en opgeloste vragen, Incidenten, Problems en verbetervoorstellen. Hierbij wordt aangegeven: datum ontvangst, datum in behandeling, verwachte opleverdatum en datum afgevoerd; - Een cumulatieve rapportage over alle vragen, Incidenten en Problems. De gecumuleerde rapportage laat de historie over een periode van minimaal 14 maanden zien, zodat trends kunnen worden geanalyseerd; - Datum laatste en volgende A&P testen; - Statement of Applicability • Vervaldatum certificaten zoals ISO27001-certificering (of gelijkwaardig), TLS-certificaat. • Bij Wijziging van de Statement of Applicability en/of ISO27001-certificering (of gelijkwaardig) wordt inzage gegeven in de datum en het resultaat van de wijziging. - Tevens worden volgende onderdelen verwacht indien deze van toepassing zijn: • Consultancy. Hierbij wordt minimaal aangegeven: 1) datum 2) opdrachtverstrekking, 3) startdatum, (verwachte) opleverdatum, 4) (verwachte) acceptatiedatum, 5) uitnutting budget; - API Calls en Gebruikers info (aantal API Calls, Gebruikers incl. autorisatieprofielen en Deelnemers); - Throughput en velocity; - API Subscriptions info. Het proces en de vorm van de rapportage wordt vastgelegd in de DAP. In overleg kunnen onderwerpen worden toegevoegd of verwijderd en wordt vastgelegd in de SLA.
-------	--

(BIO Referentie 15.2.1.1)

UE.99	Partijen geven minimaal jaarlijks inzicht in de planning (datum) van de eerstvolgende eigen relevante: - Audits; - Beveiligingstesten (A&P-testen, kwetsbaarheidscans) - Continuïteitstesten (Backup & Restore, Calamiteitentest). Proces en de vorm wordt vastgelegd in de DAP.
-------	--

(BIO Referentie 15.2.1.1)

UE.100	In het geval van beveiligingszaken waar conform de eisen en wensen in dit bestek een Verbeterplan wordt geëist, wordt minimaal het volgende opgenomen: - Naam van verbeterpunt; - Startdatum; - Geplande einddatum; - Beoogde aanpak; - Status; - Lessons learned.
--------	--

UE.101	Opdrachtnemer levert maandelijks een Service Level rapportage op aan de Opdrachtgever met minimaal de volgende inhoud: • Helpdesk: Reactietijden per Prio • Beschikbaarheid • KPI incident management • KPI Helpdesk
--------	--

10.2. Documentatie, Opleiding en Consultancy

UE.102	Opdrachtnemer levert gedurende de operationele fase van de Overeenkomst Documentatie, Opleiding en Consultancy conform de eisen zoals neergelegd in Hoofdstuk 8 'Documentatie, Opleiding en Consultancy'.
--------	--

10.3. Factureren en bestellen

Als leverancier bent u verplicht elektronisch te factureren

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

Manieren van e-factureren

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

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

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

DigiPoort

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

Peppol

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

Leveranciersportaal

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

UE.103	De Opdrachtnemer voldoet aan de vereisten van e-facturatie via het leveranciersportaal of een geautomatiseerde koppeling met de DigiPoort (toekomstig E-procurementpoort) of het Peppol netwerk met daarin de referentie naar de inkooporder en de inkooporderregel.
UE.104	Kosten die voortkomen uit het realiseren van de koppeling voor elektronische berichten uitwisseling met de Rijksoverheid worden gedragen door de Opdrachtnemer.
UE.105	Opdrachtnemer vermeldt het inkoopordernummer als referentie op elke pakbon en factuur aan Opdrachtgever. Zonder dit Inkoopordernummer kan Opdrachtgever de levering of de factuur weigeren.
UE.106	Opdrachtnemer is verantwoordelijk voor de implementatie aan haar zijde. Op verzoek van Opdrachtgever kunnen wijzigingen in het implementatieplan en/of implementatie worden aangebracht die invloed hebben op het bestelproces. Hieronder valt in ieder geval het inzetten van extra expertise.
UE.107	Opdrachtnemer accepteert dat er gedurende de looptijd van de Overeenkomst nieuwe-/verbeterde versies van de programmatuur van het leveranciersportaal in gebruik genomen kunnen worden.

10.4. Kaders voor (re)transitie

10.4.1. Inleiding

In geval van (tussentijdse) beëindiging of afloop van de Overeenkomst van de API Management, dient de Opdrachtnemer ten allen tijde alle medewerking te verlenen aan een gecontroleerde en projectmatige overdracht aan een opvolgende opdrachtnemer of Opdrachtgever en daarmee alle Documentatie, Gegevens en informatie te verstrekken die nodig zijn voor een goede overdracht.

De termijn waarbinnen de Retransitie dient te worden afgerond zal tussen Opdrachtnemer en Opdrachtgever worden overeengekomen. Deze zal worden vastgelegd in de DAP.

10.4.2. Documentatie en Gegevens(overdracht)

UE.108	Bij beëindiging van de Overeenkomst tussen Opdrachtgever en Opdrachtnemer is een ordentelijke overgang van Opdrachtnemer naar de nieuwe dienstverlener gewenst om de continuïteit van de Diensten te borgen. Opdrachtnemer (inclusief Fabrikant) is verplicht haar volledige medewerking te verlenen aan een zo soepel mogelijke overdracht waarbij de continuïteit van de Prestatie gewaarborgd blijft. Hierbij wordt, indien noodzakelijk, een Retransitieplan opgesteld door de Partijen, waarvoor de (Uitvoerings)eisen uit de hoofdstuk leidend zijn
UE.109	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 VII Prijzenformulier aangegeven Consultancy Prijzen. - Deze Additionele diensten hebben in ieder geval betrekking op de migratie of export van Gegevens uit de Oplossing naar een vervangende oplossing.
UE.110	Op verzoek van Opdrachtgever worden bij beëindiging van de Overeenkomst Gegevens van Opdrachtgever binnen een van te voren afgesproken aantal dagen ter beschikking gesteld, in een voor Opdrachtgever bruikbaar van te voren afgesproken digitaal formaat. De ter beschikking gestelde Gegevens dienen te zijn voorzien van een zodanige functionele- en technische beschrijving dat in de toekomst een datamigratie naar een nieuwe Oplossing kan plaatsvinden zonder verdere tussenkomst van de Opdrachtnemer.
UE.111	Opdrachtnemer verleent volledige medewerking aan de Retransitie en verstrekt daarbij alle relevante Documentatie aan Opdrachtgever c.q. opvolgende opdrachtnemer verstrekken.
UE.112	Aanlevering van de Documentatie gebeurt via een beveiligde verbinding. Opdrachtgever draagt zorg voor deze verbinding.
UE.113	De ter beschikking gestelde Gegevens dienen te zijn voorzien van een zodanige functionele - en technische beschrijving dat in de toekomst een datamigratie naar een nieuwe oplossing kan plaatsvinden zonder verdere tussenkomst van de Opdrachtnemer.
UE.114	Na ontvangst van bevestiging dat de Gegevens in goede orde zijn ontvangen, zal de Opdrachtnemer overgaan tot vernietiging van onder hem bevindende Gegevens, waarbij de vernietigingshandelingen gedocumenteerd zullen worden.
UE.115	Opdrachtnemer zorgt dat binnen één (1) maand na afloop van de Retransitie, alle Gegevens in verband met deze Overeenkomst van haar systemen zijn verwijderd, zodat de vertrouwelijkheid van deze Gegevens gewaarborgd blijft.
UE.116	De rapportage van de vernietigingshandelingen is in overeenstemming met wettelijke vereisten ter zake en wordt door Opdrachtnemer aan Opdrachtgever ter hand gesteld.
UE.117	Op eerste verzoek van Opdrachtgever overlegt Opdrachtnemer een door een onafhankelijk IT-auditor of accountant gecertificeerde verklaring van vernietiging waaruit blijkt dat alle Gegevens in verband met deze Overeenkomst zijn gewist.

10.4.3. (Proces)afspraken Retransitiefase

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

UE.118	Bij overgang naar een nieuwe opdrachtnemer moet de Prestatie voor een periode van 3 maanden tegen gelijkblijvende condities (naar rato), voor Opdrachtgever beschikbaar blijven.
UE.119	Opdrachtnemer verleent volledige medewerking aan de Retransitie en verstrekt daarbij alle relevante Documentatie en Gegevens aan Opdrachtgever in een nog met de Opdrachtgever af te stemmen formaat.

UE.120	Na ontvangst van bevestiging dat de Gegevens in goede orde zijn ontvangen, zal de Opdrachtnemer overgaan tot vernietiging van zich onder hem bevindende Gegevens, waarbij de vernietigingshandelingen gedocumenteerd zullen worden. Opdrachtnemer zorgt dat binnen één (1) maand na afloop van de Retransitie, alle Gegevens die verband houden met deze Overeenkomst van zijn systemen (inclusief back-ups, draagbare media) zijn verwijderd, zodat de vertrouwelijkheid van deze Gegevens gewaarborgd blijft. Opdrachtnemer overlegt een verklaring van vernietiging waaruit blijkt dat alle gegevens die verband houden met deze Overeenkomst zijn gewist.
--------	--

Van Oplossingen die toegankelijk zijn via het internet mogen domeinnamen en URL's die herleidbaar zijn naar de Opdrachtgever niet hergebruikt worden.

UE.121	Naar de Opdrachtgever herleidbare (sub)domeinnamen en URL's worden onbeschikbaar gemaakt op het internet. Als mogelijk worden de domeinnamen overgedragen aan de Opdrachtgever. In alle gevallen is hergebruik van deze domeinnamen en URL's is niet toegestaan zonder nadrukkelijke toestemming van de Opdrachtgever. Indien overdracht niet mogelijk is dan overlegt Opdrachtnemer een verklaring waaruit blijkt dat hergebruik niet zal plaatsvinden.
--------	---

UE.122	Opdrachtnemer stelt gedurende de periode van Retransitie de voor Opdrachtgever ontwikkelde methoden, technieken, Programmatuur en andere technische voorzieningen ter beschikking en laat deze ontwikkelde methoden, technieken, Programmatuur en andere technische voorzieningen gebruiken door Opdrachtgever en opvolgende Opdrachtnemer, met als doel een efficiënte Retransitie te bewerkstelligen. De opvolgende Opdrachtnemer wordt verplicht een geheimhoudingsverklaring te ondertekenen.
--------	---

UE.123	Opdrachtnemer houdt voldoende gekwalificeerd personeel beschikbaar voor de Retransitie.
--------	---

UE.124	Opdrachtnemer verleent medewerking aan een Audit betreffende de inhoud en de kwaliteit van de informatie die Opdrachtnemer in het kader van Retransitie beheerd.
--------	--

UE.125	Opdrachtnemer dient inzage te geven in de gebruikte middelen en processen tijdens de periode van Retransitie
--------	--

UE.126	Opdrachtnemer dient onder meer de verbindingen te verbreken, eventueel aan Opdrachtgever ter beschikking gestelde Apparatuur terug te geven, eventuele licenties te verstrekken ten aanzien van Oplossing die noodzakelijk is om de omgeving in stand te houden/te blijven beheren; en elektronische sleutels aan Opdrachtgever ter beschikking te stellen.
--------	---