Bijlage A. Specificatie van de opdracht

Openbare Europese aanbesteding

Beheer, Onderhoud & support Oracle Exadata-omgeving

Versie: 1.0
Kenmerk: IUC25-008
Datum: maandag 12 januari 2026

Inhoudsopgave

Dit document beschrijft de eisen die de Aanbestedende dienst stelt in het kader van de Europese aanbesteding Beheer, Onderhoud & Support Oracle Exadata omgeving met kenmerk IUC25-008. Dit document maakt integraal onderdeel uit van het Beschrijvend Document.

Hoofdstuk 1. Functionals

1.1. Onderhoud & Suppport

UE 1.	Opdrachtnemer voert Onderhoud & Support uit op basis van Oracle premier support op de Exadata-stack (Installed base) conform Oracle supportvoorwaarden: • Apparatuur: Oracle hardware and system support (Bijlage 3.); • Programmatuur: Oracle software technical support (Bijlage 4.).
UE 2.	Opdrachtnemer voert conform de overeengekomen planning het Onderhoud & Support uit.
UE 3.	Het Onderhoud & Support wordt uitgevoerd door Personeel dat gecertificeerd is door de Vendor voor werkzaamheden op de Exadata-omgeving. De dienstverlening vindt plaats in overeenstemming met de richtlijnen, procedures en best practices zoals voorgeschreven door de Vendor. Er wordt aantoonbaar gebruik gemaakt van door de Vendor goedgekeurde tools, Updates, Upgrades, Patches ed.
UE 4.	Opdrachtnemer gaat er mee akkoord dat aan de hand van een Customer Support Identifier (CSI nummer), toegekend door Vendor, Opdrachtgever rechtstreeks technisch support kan aanvragen bij de helpdesk van de Vendor.
UE 5.	Opdrachtnemer zorgt ervoor dat Opdrachtgever tijdens de looptijd van de Overeenkomst recht heeft op (het gebruik van): • installatieproducten; • installatiehandleidingen en overige Documentatie.
UE 6.	Opdrachtnemer draagt zorg voor het tijdig en proactief beschikbaar stellen van actuele, volledige en relevante Documentatie met betrekking tot de Exadata-omgeving. Deze Documentatie wordt digitaal aangeleverd en is opgesteld in de Nederlandse en/of Engelse taal. De Documentatie bevat een duidelijke, gedetailleerde en begrijpelijke beschrijving van de geleverde Componenten, inclusief de functionaliteiten, configuraties en gebruiksmogelijkheden, zodat gebruikers binnen de organisatie van Opdrachtgever zelfstandig en effectief gebruik kunnen maken van de omgeving. Opdrachtgever heeft het recht om de Documentatie binnen de eigen organisatie te reproduceren en waar nodig aan te passen. Opdrachtnemer is verantwoordelijk voor het actueel houden van de Documentatie gedurende de looptijd van de Overeenkomst. Indien blijkt dat de Documentatie onjuist, onvolledig, onduidelijk of verouderd is, zal Opdrachtnemer deze onverwijld corrigeren en opnieuw beschikbaar stellen. Bij iedere Update en/of Upgrade of wijziging wordt de bijbehorende geactualiseerde Documentatie digitaal aangeleverd/beschikbaar gesteld. In deze Documentatie worden de wijzigingen ten opzichte van eerdere versies duidelijk en overzichtelijk weergegeven

1.2. Updates en Upgrades

UE 7.	Opdrachtnemer stelt een kalender beschikbaar waarin de toekomstige Updates en Upgrades zijn opgenomen.
UE 8.	Met de Opdrachtgever wordt voortijdig afgestemd over aankomende Updates en Upgrades en de eventuele Impact op het gebruik van de Exadata-omgeving. Het doorvoeren wordt in overleg ingepland.
UE 9.	Updates en Upgrades zijn grondig en in samenhang getest door de Opdrachtnemer of Vendor voor ze worden geïnstalleerd.
UE 10.	Updates en Upgrades mogen de Beschikbaarheid van de Exadata-omgeving niet negatief beïnvloeden.
UE 11.	Opdrachtnemer levert voorafgaand aan Updates en Upgrades releasenotes. In de releasenotes zijn overzichtelijk de voor de Exadata-omgeving relevante wijzigingen, verbeteringen en nieuwe functionaliteiten die in de nieuwe versie van de Programmatuur doorgevoerd zijn opgenomen.
UE 12.	Opdrachtnemer draagt zorg voor het beschikbaar stellen en installeren van actuele Programmatuur (Updates en Upgrades).
UE 13.	Om de veiligheid van Programmatuur te borgen dient voor het beschikbaar stellen van Updates en Upgrades op een veilige manier te gebeuren. Hiervoor kan gebruik worden gemaakt van filetransfer. Opdrachtgever maakt gebruik van filetransfer om (grote) bestanden te verzenden en te ontvangen.
UE 14.	Installatie en configuratie van Updates en Upgrades vindt op locatie van Opdrachtgever plaats.
UE 15.	Het installeren van Updates en Upgrades dient in overleg met Opdrachtgever ingepland te worden.
UE 16.	Opdrachtnemer is verantwoordelijk dat Documentatie na een Update en/of Upgrade actueel blijft. Na oplevering van een nieuwe Update en/of Upgrade wordt de geactualiseerde Documentatie digitaal beschikbaar gesteld.

1.3. Beheer

UE 17.	Opdrachtnemer is verantwoordelijk voor het up-to-date houden van de Engineered Systems conform de richtlijnen van Vendor (Oracle). Hiervoor voert Opdrachtnemer periodiek per Engineered system ten minste 2 x per jaar werkzaamheden voor Beheer uit, waaronder: • Patches; • Updates en –Upgrades • coördinatie en uitvoering van geplande Beheer werkzaamheden Indien noodzakelijk (bijvoorbeeld in het geval zich beveiligingsincidenten voordoen), voert Opdrachtnemer aanvullende Beheerwerkzaamheden uit, zodat kritieke (beveiligings)patches binnen de overeengekomen termijnen na beschikbaarheid worden geïmplementeerd.
UE 18.	Opdrachtnemer voert, onder regie van Opdrachtgever, Beheer op de gehele Exadata omgeving uit, inclusief de Oracle database software laag en (minor) Patches.
UE 19.	Opdrachtnemer voert het Beheer uit op locatie van Opdrachtgever.
UE 20.	Beheerwerkzaamheden worden in overleg met Opdrachtgever ingepland.
UE 21.	Opdrachtnemer voert conform de overeengekomen planning het Beheer uit.

1.4. Technical Account Management (TAM)

UE 22.	Opdrachtnemer stelt een Technical Account Manager (TAM) beschikbaar voor: • proactieve ondersteuning; • advies over optimalisatie van de Exadata-omgeving; • coördinatie van supportcases; • planning en coördinatie van de Diensten (conform de rechtlijnen van de Vendor); • periodieke evaluaties.
UE 23.	Opdrachtnemer adviseert de Opdrachtgever over marktontwikkelingen en kennis van de Exadata-omgeving ten aanzien van strategische ontwikkelingen en innovatieve keuzes voor het ontwikkelen en onderhouden van informatiesystemen in het applicatielandschap.
UE 24.	Indien Opdrachtgever behoefte heeft aan specifieke kennis dan kunnen er onder de dagen die beschikbaar zijn voor de Technical Accountmanager specialisten ingezet worden. Indien de TAM-dagen niet voldoen (qua tarief of qua omvang) wordt er een separate opdracht verstrekt (adhoc of projectmatig).

1.5. Consultancy

UE 25.	Opdrachtnemer dient op verzoek van de Opdrachtgever Consultants beschikbaar te stellen voor ondersteuning en service op de Exadata-omgeving. Deze inzet kan plaatsvinden op basis van: • Ad-hoc inzet op uurbasis: Voor kortdurende, niet-projectmatige werkzaamheden kunnen Consultants worden ingezet op basis van een uurtarief, waarbij de inzet per geval wordt afgestemd. • projectmatige inzet: Consultants kunnen worden ingezet voor vooraf gedefinieerde projecten met een duidelijke scope, planning en deliverables. De Consultants dienen aantoonbare relevante kennis en ervaring te hebben met (vergelijkbare) Exadata-omgevingen en in staat te zijn om zelfstandig en effectief ondersteuning te bieden binnen de complexe IT-infrastructuren van de Opdrachtgever.

1.6. Dossier Afspraken en Procedures (DAP)

UE 26.	Partijen stellen een Dossier Afspraken en Procssen (DAP) op. In dit document zijn de operationele afspraken en de daarbij behorende overleggen opgenomen. Het DAP zal als Bijlage B aan de Overeenkomst worden toegevoegd.
UE 27.	Opdracthnemer stelt na gunning het DAP op. Opdrachtnemer is ervoor verantwoordleijk dat het DAP uiterlijk binnen drie maanden na ondertekening van de Overeenkomst afgerond is.
UE 28.	Het DAP zal jaarlijks, of indien noodzakelijk vaker, door Partijen gereviewd worden en waar nodig door Opdrachtnemer geactualiseerd en/of aangepast.

1.7. Rapportage en communicatie

UE 29.	Opdrachtnemer stelt op zowel op strategisch, tactisch en operationeel niveau een Single Point of Contact (SPoC) tijdens de looptijd van de Overeenkomst aan.

UE 30.	De Opdrachtnemer levert periodieke (ten minste eens per kwartaal) en op verzoek rapportages over: • uitgevoerde werkzaamheden; • Incidenten en hun afhandeling; • status van de Exadata-omgeving en aanbevelingen. • overzicht verwachte EOS-datum Tevens levert Opdrachtnemer op ad-hoc basis specifieke rapportages aan.
UE 31.	Binnen 30 dagen na signalering van een (naderende) EOS-status stelt Opdrachtnemer een vervangingsvoorstel op. Het voorstel bevat ten minste: • Technische specificaties van de vervangende component; • Planning van de vervanging; • Kostenraming; • Eventuele impact op dienstverlening.
UE 32.	De Opdrachtgever beoordeelt het vervangingsvoorstel binnen een redelijke termijn. Bij akkoord wordt er door Opdrachtnemer (op basis van een Offertetraject zoals hieronder beschreven) een Offerte opgesteld. Na akkoord van de Offerte zal de vervanging ingepland en door Opdrachtnemer uitgevoerd worden.
UE 33.	Indien de Opdrachtgever gedudende de looptijd van de Overeenkomst behoefte heeft aan Keuze-elementen, herzieningsclausules en/of Wijzigingen wordt een Offertetraject gestart conform artikel 12 van de Overeenkomst. De werkwijze van een Offertetraject is in grote lijnen als volgt: 1. het IUC Belastingdienst stuurt een aanvraag naar de Opdrachtnemer; 2. de Opdrachtnemer stuurt, binnen maximaal tien (10) Werkdagen, de Offerte, inclusief de originele door de Vendor afgegeven aanbieding retour aan het IUC Belastingdienst. De Offerte heeft een geldigheidsduur van tenminste 60 dagen; 3. na goedkeuring van de Opdrachtgever op de Offerte accepteert het IUC Belastingdienst de Offerte door middel van een Inkoopopdracht. Standaard wordt er een termijn van tien (10) Werkdagen gehanteerd voor het uitbrengen van een Offerte. In specifieke gevallen kunnen hierover aangepaste termijnen worden gehanteerd. Opdrachtnemer conformeert zich aan de werkwijze van een Offertetraject zoals hierboven beschreven.
UE 34.	Indien door Opdrachtgever gewenst wordt Apparatuur (Engineered systems en Componenten) welke door de Opdrachtnemer worden geleverd door de Opdrachtnemer met een (configuratie)nummer gelabeld. Het configuratienummer wordt door de Opdrachtgever aangeleverd. De Opdrachtnemer registreert de combinatie van configuratienummer en serienummer van het Engineered System.
UE 35.	De Opdrachtnemer houdt te allen tijde een complete actuele administratie bij van alle bij Opdrachtgever in gebruik zijnde Engineered Systems met daarin minimaal de volgende items: • Artikelnummer; • Aantal; • serienummer; • omschrijving; • configuratienummer (wordt door Opdrachtgever aangeleverd); • configuratie van het Engineered System (incl. overzicht van (relevante) Componenten) • ingangs- en einddatum Onderhoud & Support; • Contract- en CSI-nummer van de Vendor. Deze administratie dient te allen tijde up to date te zijn, en bij vervanging, uitbreiding of updates dient deze door de Opdrachtnemer geactualiseerd te worden. Deze administratie dient op verzoek van de Opdrachtgever overlegd te worden door Opdrachtnemer.

UE 36.	Opdrachtnemer is verantwoordelijk voor het houden van een administratie van in door Opdrachtgever op de Exadata-stack in gebruik zijnde Programmatuur, met daarin minimaal de volgende items: • serienummer; • artikelnummer • omschrijving; • aantal; • ingangs- en einddatum Onderhoud & Support; • Contract- en CSI-nummer van de Vendor. Deze administratie dient te allen tijde up to date te zijn, en bij vervanging, uitbreiding of updates dient deze door de Opdrachtnemer geactualiseerd te worden. Deze administratie dient op verzoek van de Opdrachtgever overlegd te worden door Opdrachtnemer. Opdrachtnemer stelt op verzoek informatie beschikbaar teneinde Opdrachtgever in staat te stellen een verzoek tot controle van bijvoorbeeld Licentierecht, Gebruiksrecht, rechtmatigheid van gebruik van Programmatuur door de Vendor, te kunnen beantwoorden.

1.8. Herstelplan

UE 37.	Indien de Diensten voor een periode van drie (3) maanden niet voldoet aan één of meerdere Service Levels levert Opdrachtnemer hiervoor een herstelplan, inclusief een bijbehorend implementatievoorstel, aan bij de Opdrachtgever. Het herstelplan moet leiden tot een situatie waarbij de Service Levels wel worden gerealiseerd. Het herstelplan wordt binnen vijftien (15) Werkdagen na verzoek van de Opdrachtgever opgeleverd. Toepassing van het herstelplan laat de overige rechten van Opdrachtgever onverlet, waaronder die op schadevergoeding.

1.9. Kaders voor (re)transitie

In geval van (tussentijdse) beëindiging of afloop van de Overeenkomst, 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.

1.9.1. Documentatie en Gegevens(overdracht)

UE 38.	Zodra partijen bekend zijn met het feit dat de Overeenkomst om welke reden dan ook eindigt of wordt beëindigd, waaronder begrepen opzegging en ontbinding, inventariseren Partijen gezamenlijk welke assistentie van Opdrachtnemer, tegen marktconforme tarieven, noodzakelijk is voor een succesvolle Retransitie 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 39.	Opdrachtnemer verleent volledige medewerking aan de Retransitie en verstrekt daarbij alle relevante Documentatie aan Opdrachtgever c.q. opvolgende opdrachtnemer verstrekken.

UE 40.	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 41.	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 42.	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 43.	De rapportage van de vernietigingshandelingen is in overeenstemming met wettelijke vereisten ter zake en wordt door Opdrachtnemer aan Opdrachtgever ter hand gesteld.
UE 44.	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.

1.9.2. (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 45.	Bij overgang naar een nieuwe opdrachtnemer moet de Prestatie voor een periode van zes (6) maanden tegen gelijkblijvende condities (naar rato), voor Opdrachtgever beschikbaar blijven.
UE 46.	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 47.	Opdrachtnemer houdt voldoende gekwalificeerd personeel beschikbaar voor de Retransitie.
UE 48.	Opdrachtnemer verleent medewerking aan een Audit betreffende de inhoud en de kwaliteit van de informatie die Opdrachtnemer in het kader van Retransitie beheerd.
UE 49.	Opdrachtnemer dient inzage te geven in de gebruikte middelen en processen tijdens de periode van Retransitie
UE 50.	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.

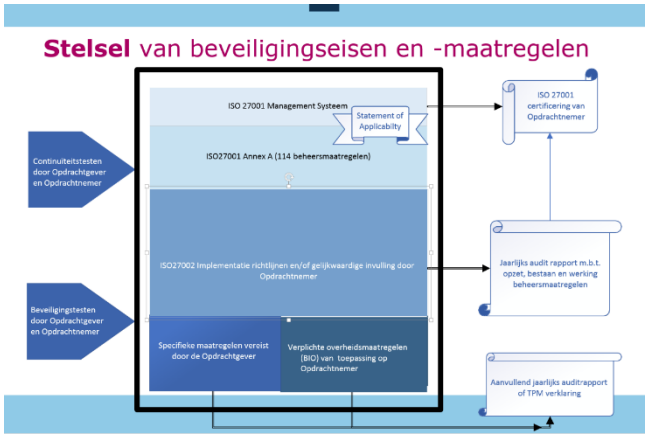
Hoofdstuk 2. IV kaders

2.1. Beveiligingseisen en -maatregelen

De omgang met 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 Opdrachtnemers. De Opdrachtnemer moet minimaal hetzelfde beveiligingsniveau leveren als de Opdrachtgever.

De Opdrachtgever is gehouden aan de algemene vigerende Nederlandse wet- en regelgeving en aan de Baseline Informatiebeveiliging Overheid (BIO). Dit document is als Bijlage B. Baseline Informatiebeveiliging Overheid beschikbaar gesteld. Deze regelgeving is gebaseerd op de ISO27001 en de ISO27002, en bevat daarnaast aanvullende beveiligingseisen, de zogenoemde overheidsmaatregelen. Vanwege de eigen technische inrichting, stelt de Opdrachtgever zelf ook specifieke beveiligingseisen.

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



De Opdrachtgever voert periodiek aanvullende Audits uit om de opzet, het bestaan en de werking van een passend stelsel van beveiligingsmaatregelen ten aanzien van Prestatie te toetsen. De Opdrachtgever kiest hierbij zelf welk onafhankelijk en algemeen erkend bureau de Audits uitvoert.

UE 51.	Ten aanzien van de ISO 27001, of gelijkwaardige certificering: • Toont de Opdrachtnemer jaarlijks de geldigheid van de certificering aan door het overleggen van een kopie van het kwaliteitscertificaat. • Laat Opdrachtnemer op verzoek van de Opdrachtgever Audits uitvoeren door een daartoe gecertificeerde partij, waarbij de Opdrachtgever inzage krijgt in de resultaten. • Wordt de Opdrachtgever door de Opdrachtnemer op de hoogte gehouden van de inrichting van de beheersmaatregelen van de ISO27001, conform de implementatierichtlijnen van de ISO27002, indien daar aanleiding voor is.
UE 52.	De Opdrachtgever voert regelmatig (ten minste jaarlijks) een risicoanalyse uit waaruit zal blijken of een A&P test en/of vulnerability (Kwetsbaarheids) scan moet worden uitgevoerd. Opdrachtnemer werkt mee aan de risicoanalyses en beveiligingstesten, zoals A&P testen en vulnerability (Kwetsbaarheids) scans, van de Opdrachtgever.

UE 53.	Opdrachtgever voert in geval van implementaties of aanpassingen op de Exadata-omgeving een hacktest (of ook wel meer formeel een pen(etratie)test genoemd) uit. Geconstateerde beveiligingsissues dienen kosteloos door Opdrachtnemer te worden opgelost.

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

Paragraaf	Beheersmaatregel
9.	Toegangsbeveiliging
9.4.4.1	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.
12.	Beveiliging bedrijfsvoering
12.6.1.1	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.
15.	Leveranciersrelaties
15.1.1.1	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, worden eisen ten aanzien van informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd. Deze eisen zijn gebaseerd op een expliciete risicoafweging.

UE 54.	Opdrachtnemer voldoet aan hierboven genoemde beheersmaatregelen uit de Baseline Informatiebeveiliging Overheid.
UE 55.	De Opdrachtnemer krijgt geen remote toegang en geen wachtwoorden/inlog credentials. Het Personeel van Opdrachtnemer krijgt toegang tot de Exadata-omgeving via een Belastingdienst-device. Onder begeleiding van een medewerker van de Opdrachtgever krijgt het Personeel toegang tot de Exadata-omgeving via een werkplek van de betreffende medewerker van de Opdrachtgever. Hiervoor is het vereist dat het betreffende Personeel fysiek aanwezig is op de locatie waar de Exadata-omgeving zich bevindt. Toegang tot gasten-wifi is mogelijk als het Personeel van de Opdrachtnemer via zijn eigen werkplek toegang nodig heeft tot informatie voor het uitvoeren van de werkzaamheden.
UE 56.	Alle Personeel van Opdrachtnemer en/of die worden ingezet via Opdrachtnemer, die werkzaamheden uitvoeren op locatie van de Opdrachtgever dienen zich altijd te kunnen legitimeren met een geldig legitimatiebewijs.
UE 57.	Alle Personeel van Opdrachtnemer die werkzaamheden uitvoeren op locatie van de Opdrachtgever dienen in het bezit te zijn van een geldige Verklaring Omtrent Gedrag Natuurlijke Personen VOG (algemeen screeningsprofiel, functie-aspecten: 11, 12, 13 en 41). Voor niet ingezeten kan een gelijkwaardige verklaring worden overlegd. De Opdrachtgever oordeelt over de bruikbaarheid hiervan. De verklaring dient op verzoek van Opdrachtgever te worden getoond.
UE 58.	Met de Opdrachtnemer worden de informatiebeveiligingseisen en een periodieke actualisering daarvan overeengekomen.
UE 59.	Ter bescherming van bedrijfs- en persoonlijke data, heeft Opdrachtnemer een beleid geformuleerd voor verwerking van data, tenminste voor: de vertrouwelijkheid en versleuteling van data, voor transformatie en aggregatie, voor toegang en privacy, classificatie en labelen en bescherming tegen verlies van gegevens.

UE 60.	Alle rollen en verantwoordelijkheden voor het installeren en onderhouden van middlewarefunctionaliteiten zijn gedefinieerd en toegewezen.
UE 61.	Het toewijzen en gebruik van speciale toegangsrechten tot de middlewarefunctionaliteiten en speciale systeemhulpmiddelen zijn beperkt en worden beheerst.

2.2. Algemene eisen vanuit beveiligingsperspectief

De Opdrachtgever stelt een aantal eisen aan maatregelen met betrekking tot vertrouwelijkheid en integriteit van informatie.

UE 62.	Opdrachtnemer stelt aan Opdrachtgever een medium (zoals een portal) beschikbaar waarop op een veilige manier documenten (zoals rapportages) en Gegevens uitgewisseld kunnen worden.
UE 63.	Opdrachtnemer conformeert zich aan Geheimhoudingsplicht (artikel 3.13.8 Reglement Personeelsvoorschriften Belastingdienst), Huisregels kritische ruimten en richtlijnen Fotograferen en Filmen. Personeel van Opdrachtnemer die het datacenter betreden dienen bijgevoegde verklaring (Bijlage 5. Algemene verklaring kritische ruimten en na ondertekening van de Overeenkomst, bijlage C van de Overeenkomst) te ondertekenen
UE 64.	Datadragers (zoals harddisks en SSD-s) die door de Opdrachtnemer vervangen worden, worden ter vernietiging ingenomen door Opdrachtgever.

2.3. Gegevens

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 zijn gemaakt.

UE 65.	Opdrachtnemer zal geen Gegevens voor eigen doeleinden delen dan wel verwerken, behalve na expliciete toestemming van de Opdrachtgever. De Opdrachtnemer openbaart welke Gegevens als strikt noodzakelijk worden beschouwd voor de uitvoering van de Overeenkomst.

De Gegevens van de Opdrachtgever moeten gescheiden worden verwerkt (waaronder opgeslagen) van andere klanten van Opdrachtnemer; de Opdrachtgever wil geen zicht hebben in Gegevens van andere klanten van de Opdrachtnemer en andere klanten mogen geen zicht in de Gegevens van de Opdrachtgever hebben. Personeel van Opdrachtnemer mag alleen toegang hebben tot de Gegevens van de Opdrachtgever voor zover dat noodzakelijk is voor het uitvoeren van de Overeenkomst.

UE 66.	Gegevens van de Opdrachtgever worden gescheiden opgeslagen van de Gegevens van andere klanten van de Opdrachtnemer.
UE 67.	Toegang tot Gegevens van de Opdrachtgever is beperkt voor Personeel van de Opdrachtgever voor zover dit noodzakelijk is voor de uitvoering van de Overeenkomst.
UE 68.	Opdrachtnemer zal geen Gegevens voor eigen doeleinden delen dan wel verwerken, behalve na expliciete toestemming van de Opdrachtgever. De Opdrachtnemer openbaart welke Gegevens als strikt noodzakelijk worden beschouwd voor de uitvoering van de Overeenkomst.

2.4. Beveiligingsincidenten

Beveiligingsincidenten zijn Incidenten die een vermoedelijke of mogelijk opzettelijke inbreuk veroorzaken op de beschikbaarheid, vertrouwelijkheid of integriteit van de (persoons)Gegevens in informatieverwerkende systemen of inbreuk maken op deze systemen zelf. 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 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 CERTs (NCSC, Digital Trust Center, bedrijfstak- of sectorgerichte CERT).
4. Kwetsbaarheid vanuit beveiligingstest (zoals een 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 4.0x). Oplostermijnen die hier aan gekoppeld zijn, zijn:

- kritisch risico (critical risk, score 9.0 – 10.0): per direct. Voor de Opdrachtgever is dit een Incident.
- hoog risico (high risk, score 7.0 – 8.9): per direct, na afstemming maximaal 1 maand. Voor de Opdrachtgever is dit een Incident.
- gemiddeld risico (medium risk, score 4.0 – 6.9): 3 maanden. Voor de Opdrachtgever is dit een Probleem.
- laag risico (low risk, 0.1 – 3.9): 6 maanden. Voor de Opdrachtgever is dit een Probleem.

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-uitprincipe" alleen gebruikt worden om de oplostijd (beperkt) op te rekken. Dit kan alleen met nadrukkelijke instemming van de Opdrachtgever. De Opdrachtgever kan besluiten dat (persoons)Gegevens onbeschikbaar gemaakt moeten worden en dat de oplossing geheel dan wel gedeeltelijk onbeschikbaar gemaakt moet worden voor derden. Staat de oplossing nog niet in productie dan zal in productiename niet mogen totdat de kritische-en hoge risicobevindingen zijn weggenomen. Bekende Kwetsbaarheden worden onverwijld gemeld.

Gemiddeld- en laag risicobevindingen 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 oplostijd. 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 69.	Opdrachtnemer conformeert zich aan de door de Opdrachtgever gebruikte methode (CVSS4.x) om Incidenten 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. • hoog risico (high risk): 1 maand. • gemiddeld risico (medium risk): 3 maanden • laag risico (low risk): 6 maanden

UE 70.	Opdrachtnemer beschikt over een meldloket waar Beveiligingsincidenten en (potentiële) Datalekken per direct het hele jaar door 24/7 gemeld kunnen worden. De Opdrachtnemer zal de omvang van het Incident of Probleem aangeven, de verwachte consequenties voor de Opdrachtgever alsmede de reeds getroffen en te treffen maatregelen om de gevolgen te beperken.
UE 71.	De Opdrachtnemer is verplicht de Opdrachtgever onverwijld te informeren zodra een Kwetsbaarheid wordt vastgesteld of voorzien die betrekking heeft op de Gegevens van de Opdrachtgever, of wanneer bij een andere klant van de Opdrachtnemer een Kwetsbaarheid wordt geconstateerd in een Exadata-omgeving die vergelijkbaar is met de Exadata-omgeving van de Opdrachtgever. De melding dient ten minste de volgende informatie te bevatten: 1. Omschrijving en omvang van de Kwetsbaarheid; 2. Verwachte consequenties voor de Opdrachtgever; 3. Overzicht van reeds getroffen maatregelen en de nog te treffen maatregelen om de gevolgen te beperken.
UE 72.	Datalekken en/of beveilgingsrisico's worden onverwijld gemeld bij de Opdrachtgever. De Opdrachtnemer zal de omvang van het Incident aangeven alsmede de reeds getroffen en te treffen maatregelen om de gevolgen te adresseren.
UE 73.	De Opdrachtnemer meldt de Opdrachtgever onverwijld als er een (vermoeden) van een Datalek en/of beveiligingsrisico bestaat. Er zal indien nodig binnen de wettelijk gestelde termijnen een melding gedaan worden bij de Autoriteit Persoonsgegevens. De Opdrachtnemer analyseert het (potentiële) Datalek en neemt de wettelijke stappen om de (mogelijke) inbreuk van de (persoons)Gegevens af te handelen en de onderliggende problematiek te mitigeren. De Opdrachtnemer informeert de Opdrachtgever en blijft dit gedurende de duur van het Incident doen.
UE 74.	De Opdrachtgever kan op eigen kosten op een willekeurig moment een vulnerability scan uitvoeren op de Exadata-omgeving conform haar richtlijnen. Eventuele Kwetsbaarheden die binnen de verantwoordleijkhedne van de Opdrachtnemer vallen, worden conform de richtlijnen van de Opdrachtgever opgelost. In overleg worden relevante acties opgenomen in een herstelplan.

2.5. Coordinated Vulnerabilty Disclosure

Opdrachtgever heeft een Coördinated Vulnerabilty Disclosure-procedure (CVD-procedure). Goedwillende beveiligingsonderzoekers kunnen via een vastgesteld proces Kwetsbaarheden, mits er geen wetten worden overtreden, melden. Het CVD-proces is op deze pagina beschreven:
www.belastingdienst.nl/security#coordinated-vulnerability-disclosure.

UE 75.	Opdrachtnemer handelt via de Opdrachtgever gemelde CVD-meldingen af conform het CVD-beleid van de Opdrachtgever.

Hoofdstuk 3. Integriteit

3.1. 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 76.	Opdrachtnemer conformeert zich aan de Business Etiquette zoals opgenomen in Bijlage van het Beschrijvend Document.

Hoofdstuk 4. Maatschappelijk verantwoord inkopen (MVI)

Opdrachtgever heeft ambitie op het gebied van duurzaamheid. Zij wil klanten, behoeftestellers en leveranciers begeleiden in het vormgeven van de duurzaamheidsaspecten in producten en diensten op het vlak van bedrijfsvoering, bij aanbestedingen en gedurende de looptijd van de contracten (ook wel 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 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 Opdrachtgever MVI wil toepassen op deze opdracht vindt u in de volgende paragrafen. Hierin zijn de toepasselijke MVI thema's beschreven.

4.1. Energie & Klimaat

Nederland moet voor 2030 de helft minder CO_2 uitstoten ten opzichte van 1990, en in 2050 95% procent minder. In het klimaatakkoord staan de maatregelen die sectoren de komende 10 jaar nemen om de doelen voor CO_2-reductie te halen.

Het klimaatakkoord is een onderdeel van het Nederlandse klimaatbeleid. Het is een overeenkomst tussen veel organisaties en bedrijven in Nederland om de uitstoot van broeikasgassen tegen te gaan. Daarmee wordt de opwarming van de aarde beperkt. De Opdrachtnemer kan hier aanbijdragen door o.a. door de vrijgekomen CO_2 vanwege dienstreizen van Personeel van de Opdrachtnemer voor 100% te compenseren.

UE 77.	De Opdrachtnemer compenseert 100% van de vrijgekomen CO_2-uitstoot als gevolg van dienstreizen van haar Personeel die worden uitgevoerd ten behoeve van de uitvoering van de opdracht. Onder CO_2-compensatie wordt verstaan: het compenseren van vrijgekomen broeikasgassen (vertaald naar CO_2-equivalenten) door het vastleggen van CO_2 in biomassa (zoals bomen) of het voorkomen van CO_2-uitstoot door investeringen in duurzame energie en/of energiebesparing. Alleen CO_2-credits worden geaccepteerd waarvoor de CO_2-reductie is gerealiseerd conform de richtlijnen van de Clean Development Mechanism (CDM) methodologie. Deze methodologie is ook van toepassing op Verified Emission Reductions (VER's) en Emission Reduction Units (ERU's). Voor de berekening van CO_2-emissies bij buitenlandse dienstreizen gelden de emissiefactoren (well-to-wheel) zoals opgenomen op de website CO2emissiefactoren.nl. De vliegafstand wordt berekend op basis van de IATA-code tabel. De Opdracthnemer toont aan dat aan deze eis wordt voldaan door het overleggen van bewijsmiddelen, zoals: • Een Gold Standard certificaat; • Een gelijkwaardig certificaat; • Een gelijkwaardig bewijsmiddel dat aantoont dat de compensatie conform bovengenoemde methodologieën is gerealiseerd.

4.2. Welzijn & Gezondheid

Opdrachtgever heeft het welzijn en gezondheid van eigen medewerkers hoog in het vaandel. Dit wordt dan ook van de Opdrachtnemer en, indien van toepassing, zijn toeleveranciers verwacht.

UE 78.	De Opdracthnemer beschikt over een aantoonbaar beleid dat gericht is op het bevorderen van het welzijn en de gezondheid van zijn Personeel. Dit beleid omvat ten minste geregelde medezeggenschap van Personeel, bijvoorbeeld via een ondernemingsraad, personeelsvertegenwoordiging of andere formele inspraakstructuren. Stimulerende maatregelen die bijdragen aan de fysieke en mentale gezondheid van Personeel, zoals: • preventieve gezondheidsprogramma's; • flexibele werktijden of hybride werkvormen; • toegang tot ergonomische werkplekken; • faciliteiten voor mentale ondersteuning (zoals coaching, counseling of mindfulness); • beleid gericht op duurzame inzetbaarheid.

Hoofdstuk 5. Prijsstelling en facturatie

5.1. Algemene eisen ten aanzien van Prijzen

UE 79.	In de in Bijlage IV (Prijsmodel) geoffreerde Prijzen dienen alle kosten voor het verrichten van de Prestatie verdisconteerd te zijn. Kosten die niet in de Bijlage, genoemd worden en niet verdisconteerd zijn in de Prijzen, maar toch noodzakelijk blijken te zijn voor een optimaal uitvoeren van de Prestatie conform de in de Aanbestedingsstukken gestelde eisen, kan Opdrachtnemer niet in rekening brengen bij Opdrachtgever.
UE 80.	Eventuele valutarisico's zijn volledig voor rekening van Opdrachtnemer en worden geacht in de geoffreerde Prijzen te zijn verwerkt.
UE 81.	Voor zover Opdrachtnemer gehouden is omzetbelasting in rekening te brengen, zullen de in het Prijzenformulier vermelde bedragen worden verhoogd met het geldende percentage omzetbelasting.

5.2. Indexering Prijs

UE 82.	De door Opdrachtnemer geoffreerde Prijzen, zoals opgegeven in het spreadsheet Prijsmodel (Bijlage IV), mogen na het tweede contractjaar jaarlijks geïndexeerd worden op basis van de CBS-index Dienstenprijzen; commerciële dienstverlening en transport, index 2021=100 - Informatie en Communicatie (categorie H).
UE 83.	Prijsaanpassingen dienen uiterlijk één (1) maand voorafgaand aan enig contractjaar (na het tweede contractjaar) aan de contractmanager ter goedkeuring te worden aangeboden, waarbij het op dat moment (door het CBS) meest recent beschikbare en gepresenteerde van toepassing zijnde CBS-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.

5.3. Facturatie

UE 84.	De facturatie van de Diensten geschiedt vooruit voor een periode van maximaal twaalf (12) maanden. Afwijkingen van deze termijn zijn in specifieke gevallen na overleg mogelijk.
UE 85.	De facturatie van Consultancy vindt als volgt plaats: • Ad-hoc inzet van Consultants: facturatie geschiedt achteraf (per maand) op basis van werkelijk gemaakte uren. • Projectmatige inzet van Consultants: wordt volledig achteraf gefactureerd tegen de vooraf overeengekomen vaste prijs. Bij langdurige projecten (> 2 maanden) is het mogelijk om meerdere factuurmomenten af te spreken, bijvoorbeeld gebaseerd op de projectfasering of de oplevering van deelresultaten.
UE 86.	Facturatie van Additionele Leveringen (voor uitbreiding en levering van nieuwe Programmatuur) vindt in principe na levering plaats.
UE 87.	Ten aanzien van de facturatie van leveringen in het kader van Life Cycle Management kunnen (passend bij de aard en omvang van de levering) aparte afspraken worden gemaakt in de Aanvullende Overeenkomst.

5.4. Electronisch factureren

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 leverancierssportaal.

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 is te vinden op de website www.peppolautoriteit.nl.

Leverancierssportaal
U kunt ook gebruik maken van het e-factuurportaal van de Rijksoverheid, het leverancierssportaal. 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 leverancierssportaal. Het huidige leverancierssportaal van DigiInkoop wordt vervangen. U wordt tijdig geïnformeerd over de overgang naar het nieuwe leverancierssportaal.

UE 88.	De Opdrachtnemer voldoet aan de vereisten van e-facturatie via het leverancierssportaal 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 89.	Kosten die voortkomen uit het realiseren van de koppeling voor elektronische berichten uitwisseling met de Rijksoverheid worden gedragen door de Opdrachtnemer.
UE 90.	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 91.	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 92.	Opdrachtnemer accepteert dat er gedurende de looptijd van de Overeenkomst nieuwe-/verbeterde versies van de programmatuur van het leverancierssportaal in gebruik genomen kunnen worden.