



BIJLAGE A SPECIFICATIE VAN DE OPDRACHT

Europese aanbesteding

“Inbound & Outbound Telefonie”

Versie : 1.0
Kenmerk : IUC23-019
Datum : 15-11-2023

INHOUDSOPGAVE

Hoofdstuk 1.	Inleiding.....	3
Hoofdstuk 2.	Functionals	4
2.1.	Netwerk-IVR	4
2.2.	Portal	6
2.3.	Blacklisting.....	7
2.4.	Enquete functionaliteit.....	8
2.5.	Performance eisen	9
2.6.	Leveringsgebied.....	10
2.7.	Koppelvlakken.....	10
2.8.	Extra hoge beschikbaarheid	11
2.9.	Afhandeling ingaand Telefoonverkeer.....	11
2.10.	Servicenummers	12
2.11.	Uitgaand Telefoonverkeer	13
2.12.	Gegevenslevering	13
Hoofdstuk 3.	IV kaders.....	15
3.1.	Algemene Beveiligingseisen	15
3.2.	Informatiebeveiligingseisen	16
3.3.	Specifieke eisen van de Opdrachtgever.....	17
Hoofdstuk 4.	Integriteit	26
4.1.	Business Etiquette	26
4.2.	Verzekering.....	26
Hoofdstuk 5.	Maatschappelijk Verantwoord Inkopen (MVI)	27
5.1.	Energie verbruik.....	27
5.2.	Ketenverantwoordelijkheid (ISV).....	27
Hoofdstuk 6.	Juridische kaders	29
Hoofdstuk 7.	Prijsstelling	30
7.1.	Algemene eisen ten aanzien van Prijzen	30
7.2.	Toelichting Prijscomponenten in Bijlage VII "Prijzenformulier"	30
7.3.	Indexering Prijs	31
Hoofdstuk 8.	Documentatie en Opleiding.....	32
8.1.	Documentatie	32
8.2.	Opleiding	32
Hoofdstuk 9.	Voorbereiding- en Migratieperiode	33
9.1.	Voorbereiding	33
9.2.	Migratieperiode	33
9.3.	Acceptatietest en -procedure.....	33
Hoofdstuk 10.	Operationele fase.....	35
10.1.	Service Levels	35
10.2.	Toekomstige ontwikkeling	40
10.3.	Factureren en bestellen.....	41
10.4.	Kaders voor (re)transitie.....	42

Hoofdstuk 1. Inleiding

Dit document beschrijft de eisen en wensen die de Aanbestedende dienst stelt in het kader van de Europese aanbesteding Inbound & Outbound Telefonie met kenmerk IUC23-019. Dit document maakt integraal onderdeel uit van het Beschrijvend Document.

Hoofdstuk 2. Functionals

In hoofdstuk 2 'Functionals' worden de functionaliteiten beschreven waaraan de Oplossing dient te voldoen. Bestaande uit de volgende paragrafen: Netwerk-IVR, Portal, blacklisting, enquête functionaliteit, Performance eisen, Leveringsgebied, extra hoge beschikbaarheid, afhandeling ingaand Telefoonverkeer, Servicenummers, uitgaand Telefoonverkeer en Gegevenslevering.

2.1. Netwerk-IVR

Er dient een Netwerk-IVR (Interactive Voice Response) aan de Opdrachtgever beschikbaar te worden gesteld. Dit biedt de Opdrachtgever de mogelijkheid het ingaande Telefoonverkeer op te splitsen in werkstromen die op het Contactcenter platform van de Opdrachtgever verder verfijnd kunnen worden.

GUE 1.	De Opdrachtnemer levert een Netwerk-IVR functionaliteit welke door de Opdrachtgever vanuit de Portal ingericht kan worden.
GUE 2.	De Opdrachtnemer levert een Netwerk-IVR functionaliteit, waarbij de Beller een Getrapt keuzemenu te horen krijgt en uit verschillende opties een keuze kan maken door het intoetsen van het bijhorende cijfer (* of #). Een Getrapt keuzemenu dient minimaal uit 3 lagen te bestaan: - Laag 1: 5 keuzemogelijkheden; - Laag 2: 3 keuzemogelijkheden; - Laag 3: 3 keuzemogelijkheden.
Het moet mogelijk zijn een afwijkend keuzemenu af te spelen op basis van een combinatie van tijdcriteria. Zie de onderstaande voorbeelden: - Buiten openingstijden wordt een afwijkend keuzemenu afgespeeld (tijdstip gedurende de dag); - Openingstijden variëren, afhankelijk van de dag van de week (dag van de week); - Op bepaalde dagen wordt gedurende openingstijden een afwijkend keuzemenu afgespeeld, bijvoorbeeld feestdagen of betaaldagen van de Toeslagen (dag van het jaar); - Onderhoud volgens planning buiten openingstijden; - Extra menukeuze tijdens de belastingaangifte campagnetijd.	
GUE 3.	Het keuzemenu dat beschikbaar wordt gesteld door de Opdrachtgever aan de Beller kan afhankelijk zijn van 5 verschillende tijdcriteria (bijvoorbeeld: tijdstip, dag van de week en dag van jaar).
GUE 4.	De Beller kan in het keuzemenu terugkeren naar het hoofdkeuzemenu door het intoetsen van het bijbehorende cijfer (* of #) en krijgt daarna weer het keuzemenu te horen.
GUE 5.	De Netwerk-IVR ondersteunt dat de Beller kan Vooruittypen. De Beller kan aaneengesloten een aantal menukeuze (nummers) intypen, voordat Spraakfragmenten zijn gepresenteerd: - Vooruittypen kan worden ingesteld via Portal.
GUE 6.	De Beller heeft de mogelijkheid van Interrumpen van het keuzemenu: - Interrumpen kan worden ingesteld via Portal.
GUE 7.	De Opdrachtnemer biedt een geheime keuzemenu functionaliteit, dit ten behoeve van specifieke doelgroepen van de Opdrachtgever. De doelgroep ontvangt een meercijferige code die toegang geeft tot een ingang in het keuzemenu, zonder dat er een Spraakfragment wordt gepresenteerd.

	- De geheime code dient te kunnen worden gemanaged vanuit de Portal; - Geheime menukeuzes dienen overal in het keuzemenu te kunnen worden gezet; - Meerdere geheime menukeuzes kunnen actief zijn in een keuzemenu; - Meerdere geheime menukeuzes kunnen verwijzen naar dezelfde Eindbestemming.
GUE 8.	De Opdrachtnemer biedt aan de Opdrachtgever de mogelijkheid de te gebruiken Spraakfragmenten ten behoeve van de Netwerk-IVR in de Portal toe te voegen, verwijderen, activeren en deactiveren. - De lengte van Spraakfragmenten zijn minimaal: - o Welkomstekst: 15 seconden; - o Subkeuzemenu: 30 seconden; - o Hoofdkeuzemenu 50 seconden.
GUE 9.	Het dient mogelijk te zijn in het Netwerk-IVR door de Opdrachtgever om een bibliotheek van Spraakfragmenten vast te leggen. Deze dient op ieder willekeurig tijdstip te kunnen worden ingezet voor een keuzemenu.
GUE 10.	Binnen de Netwerk-IVR is het mogelijk een keuzemenu te bouwen met één enkel Spraakfragment waarbij het gesprek na het afspelen van het Spraakfragment automatisch verbroken wordt.
W1.	In de praktijk kan de situatie zich voordoen dat de Opdrachtnemer telefoongesprekken als gevolg van een storing niet bij Opdrachtgever kan afleveren. De Opdrachtgever wil in dit geval vanuit de Netwerk-IVR een bericht afspelen waarin wordt gemeld dat het telefoongesprek vanwege een storing niet kan worden doorverbonden. De Opdrachtgever zou de de Beller dan de mogelijkheid willen geven dat de Beller een menukeuze kan maken om een melding te ontvangen zodra de storing is verholpen. Voor het mogelijk maken van deze functionaliteit is het noodzakelijk dat Opdrachtnemer dan de onderstaande functionaliteit(en) kan bieden. Geef aan of Opdrachtnemer onderstaande functionaliteit(en) kan leveren: 1) De telefoonnummers van de betreffende Bellers worden door Opdrachtnemer in telefoonlijsten opgeslagen; 2) De telefoonlijsten moeten door Opdrachtnemer ontdubbeld worden zodat iedere Beller maar éénmaal het herstelbericht ontvangt. Daarnaast hanteert de Opdrachtnemer gescheiden lijsten voor Bellers vanaf een mobiele telefoon en Bellers vanaf een vaste telefoonlijn. De Opdrachtnemer maakt de ontdubbelde lijsten met telefoonnummers van mobiele Bellers voor de Opdrachtgever beschikbaar in de Portal. 3) De Opdrachtnemer informeert Bellers die via een vaste telefoonlijn hadden gebeld via een Uitgaand telefoongesprek met een tekstmelding wanneer de Opdrachtgever weer beschikbaar is. De telefoonlijsten met uitgaande telefoongesprekken worden door Opdrachtnemer gefaseerd uitgebeld om piekbelasting te voorkomen. Ter informatie: Voor het informeren van mobiele Bellers middels een SMS-bericht is de Opdrachtgever contractueel gehouden aan het contract met haar SMS-dienstverleners. Via dit kanaal zullen de mobiele Bellers middels de door Opdrachtnemer aangeleverde telefoonlijst in de Portal worden geïnformeerd. Beoordelingscriteria: - De Inschrijver levert functionaliteiten: 1, 2 en 3: 15 punten; - De Inschrijver levert functionaliteiten 1 en 2: 10 punten; - De Inschrijver levert functionaliteit: 1: 5 punten; - De Inschrijver levert geen extra functionaliteiten: 0 punten.

2.2. Portal

Voor het uitvoeren van dagelijkse werkzaamheden dient er een Portal beschikbaar te worden gesteld. Deze Portal is webbased en dient als toegangspoort voor alle door de Opdrachtnemer te leveren functionaliteiten. Met behulp van de Portal geeft de Opdrachtnemer ondersteuning aan functioneel beheer- en administratieve processen maar ook aan het incident-, rapportage en change managementproces.

UE 1.	De Opdrachtnemer stelt een Portal beschikbaar aan de Opdrachtgever. Deze Portal stelt de Opdrachtgever in staat om minimaal de volgende functionaliteiten uit te voeren: - Beheer van de omgeving (Zoals IVR-beheer, enquêtes en blacklisting); - Monitoring; - Inzicht facturatie en verbruik; - SLA afspraken; - Incidentdesk.
UE 2.	De Portal is door de Opdrachtgever benaderbaar met de gangbare versies van minimaal de volgende browsers: Chrome, Edge, Firefox en Safari.
UE 3.	De Portal is door Opdrachtgever bruikbaar en leesbaar op een 10.1 inch tablet (Android, iOS of Windows).
UE 4.	De Portal dient door Opdrachtgever 24 x 7 bereikbaar te zijn, met een beschikbaarheid van 99,8% zoals beschreven in Bijlage 9 'SLA & SLA parameters'.
UE 5.	De performance van de Portal is voor de Opdrachtgever zodanig dat responstijden korter zijn dan 1 seconde.
UE 6.	De Gebruikers hebben toegang tot de role-based Portal en uitsluitend toegang tot de Gegevens die behoren bij de door hen toegekende rollen. De volgende rollen worden minimaal ondersteund: - Functioneel beheerder voor menu's en routing; - Incident beheerder; - Enquete beheerder; - Blacklist beheerder; - SLA beheerder; - Rapportage beheerder.
UE 7.	De Gebruikers met dezelfde rollen kunnen gelijktijdig actief zijn in de Portal.
UE 8.	De Portal is voor Gebruikers van de Opdrachtgever alleen toegankelijk middels 2-factor authenticatie.
UE 9.	De Gebruikers worden gedwongen bij 1e aanmelding zelf hun wachtwoord te wijzigen.
UE 10.	De Opdrachtgever kan in de Portal zelfstandig het gebruikersbeheer (user management) inrichten, aanpassen en onderhouden.
UE 11.	De Opdrachtnemer biedt een voorziening waarbij Gebruikers van de Opdrachtgever zonder tussenkomst van de Opdrachtnemer het eigen wachtwoord kunnen resetten.
UE 12.	Als onderdeel van het te leveren support door Opdrachtnemer, levert de Opdrachtnemer op verzoek van de Opdrachtgever ondersteuning bij het uitvoeren van beheersopdrachten in de Portal.

2.2.1. Monitoring

UE 13.	De Opdrachtnemer stelt in de Portal een monitoring functionaliteit beschikbaar. De Opdrachtgever wordt in staat gesteld minimaal de volgende zaken real-time te monitoren: - Beschikbaarheid van het koppelvlak; - Spraakkwaliteit / verstaanbaarheid; - Real-time inzicht in de procentuele capaciteitsbenutting van de afgenomen aansluitingen; - Bereikbaarheid per telefoonnummer te monitoren: - o Aantal bij Opdrachtnemer aangeboden Calls; - o Aantal door Opdrachtnemer aangeboden Calls; - o Aantal door Opdrachtgever aangenomen Calls; - o Aantal door Opdrachtgever aangeboden Calls (uitgaand Telefoonverkeer); - o Aantal doorverbindingen per Eindbestemming; - o Aantal niet aangeboden Calls vanwege een call limit; - o Aantal niet afgeleverde Calls.
UE 14.	Weergave van real-time Telefoonverkeer van één Servicenummer in één grafiek, gecombineerd met dezelfde Gegevens van maximaal 1 jaar in het verleden. De monitoring functionaliteit dient de Gegevens hiervoor minimaal 1 jaar te bewaren.
UE 15.	De Opdrachtnemer voorziet in een real-time monitoring mogelijkheid waarin het totaaloverzicht van het huidige Telefoonverkeer inclusief de belasting / het gebruik per Servicenummer gedurende de dag is te volgen.
UE 16.	De informatie over de status van de te monitoren items wordt in de Portal weergegeven in dashboards en/of diagrammen zodat het voor de Gebruiker in één oogopslag duidelijk is wat de huidige status is.

2.3. Blacklisting

Op verzoek van de Opdrachtgever dient het mogelijk te zijn om Bellers te laten plaatsen op een Blacklist, zodat de telefoonnummers van deze Beller worden geblokkeerd. Het gaat hier om zogenaamde plaagbellers of frauduleuze Bellers. Deze Bellers zorgen voor onnodige kostenstijging en claimen onterecht resources.

GUE 11.	De Opdrachtnemer is in staat specifieke Bellers op basis van telefoonnummer op verzoek van de Opdrachtgever te blokkeren.
GUE 12.	De geblokkeerde Beller hoort een tekstmelding waarin diegene wordt geïnformeerd over de redenen van de blokkade en op welke wijze deze ongedaan gemaakt kan worden. De tekstmelding is via de Portal in te stellen.
GUE 13.	De Opdrachtnemer onderzoekt op verzoek van de Opdrachtgever vanaf welk telefoonnummer ongewenste gesprekken plaatsvinden en voegt het betreffende telefoonnummer toe aan de Blacklist.
GUE 14.	Indien het geblokkeerde telefoonnummer een telefoonnummer betreft waarbij telefoonnummergegevens is uitgeschakeld, dan blijft dit telefoonnummer geheim voor de Opdrachtgever.
GUE 15.	Blokkade dient ingesteld te worden door de Opdrachtnemer voor het telefoonnummer waar naartoe gebeld werd, maar ook voor alle andere Servicenummers die door Opdrachtgever bij Opdrachtnemer worden afgenomen.

GUE 16.	De Opdrachtnemer houdt een Blacklist bij van de telefoonnummers, die zijn geblokkeerd. Op deze Blacklist staan minimaal de volgende Gegevens: - Telefoonnummer van geblokkeerde Beller. Behalve indien telefoonnummerweergave is uitgeschakeld; - Tijdstip van ingaan blokkering; - Intern referentienummer van de Opdrachtgever; - In de Portal is de Blacklist met geblokkeerde telefoonnummers in de vorm van een (standaard) rapportage zichtbaar.
----------------	--

2.4. Enquete functionaliteit

Er dient een enquête functionaliteit beschikbaar te zijn om geselecteerde Bellers aan het einde van het telefoongesprek deel te laten nemen aan een geautomatiseerde telefonische enquête. Middels de telefonische enquêtes kan de Opdrachtgever tevredenheidsonderzoek doen hoe de Beller de gesprekken ervaart en beoordeelt.

GUE 17.	Het is mogelijk door de Opdrachtgever om enquêtes te starten na het afronden van een telefoongesprek.
----------------	---

GUE 18.	De Opdrachtgever kan de enquête functionaliteit instellen voor zowel ingaand als uitgaand telefoongesprek. Bij een uitgaand telefoongesprek zorgt de Opdrachtgever voor de selectie en het doorverbinden van het telefoongesprek naar de enquête functionaliteit van de Opdrachtnemer. De Opdrachtnemer biedt per enquête de mogelijkheid voor een separaat telefoonnummer waarnaar de Opdrachtgever het telefoongesprek kan doorverbinden.
----------------	---

GUE 19.	De enquête functionaliteit kan volledig via de Portal worden beheerd. De beheerwerkzaamheden omvatten minimaal de volgende functionaliteiten: - Activeren van enquête; - Selectiecriteria voor welke Bellers enquête krijgen te horen na afloop gesprek; - Aanmaken van gesproken boodschappen (o.a. voor introductie en afsluiting); - Aanmaken van de vragen voor de enquête; - Instellen van beoordelingsopties voor de Beller.
----------------	---

GUE 20.	Op basis van gedefinieerde selectiecriteria krijgt de Beller een enquête te horen. Minimaal de volgende selectiecriteria zijn definieerbaar: - Percentage van het aantal ingaande telefoongesprekken per telefoonnummer; - Telefoonnummer van de Opdrachtgever wat van toepassing is.
----------------	---

GUE 21.	Meerdere enquêtes kunnen tegelijkertijd actief zijn, elk met eigen selectiecriteria.
----------------	--

GUE 22.	Tijdspanne (start- en einddatum) waarop een enquête wordt aangeboden aan de Beller is instelbaar.
----------------	---

GUE 23.	De Beller krijgt voor de start van een telefoongesprek een keuzemenu-mogelijkheid om aan te geven of de Beller wel of niet wil deelnemen aan de enquête.
----------------	--

GUE 24.	Indien Beller heeft aangegeven te willen deelnemen aan de enquête, dan krijgt de Beller na het afronden van zijn gesprek met de Opdrachtgever een vooraf ingesproken boodschap te horen, voordat de daadwerkelijke enquête start.
----------------	---

GUE 25.	Er kunnen minimaal 15 vragen in de enquête door Opdrachtgever aan de Beller worden gepresenteerd.
----------------	---

GUE 26.	De minimale beantwoordingscapaciteit voor de enquête is 150 gelijktijdige enquêtes aan 150 gelijktijdige Bellers.
GUE 27.	De enquêtevragen kunnen door de Beller op de volgende wijze worden beantwoord: - Door middel van DTMF (Dual Tone Multifrequency).
GUE 28.	Aan het einde van de enquête krijgt de Beller een afsluitende tekst te horen en wordt daarna het telefoongesprek automatisch verbroken.
GUE 29.	Alle door de Beller gegeven antwoorden worden gelogd voor rapportagedoeleinden. De antwoorden die door middel van DTMF (Dual Tone Multi Frequency) worden gegeven dienen in CSV-formaat te kunnen worden geëxporteerd.
GUE 30.	De Opdrachtnemer biedt de mogelijkheid het unieke telefoongesprekskenmerk van het telefoongesprek op te slaan samen met de gegeven antwoorden uit de enquêtes.
W 2.	De Opdrachtnemer biedt de mogelijkheid bij minimaal 2 vragen in de enquête functionaliteit via de Portal instelbaar, dat er door de Beller een antwoord kan worden ingesproken: - Ja: 10 punten; - Nee: 0 punten.
W 3.	De Opdrachtnemer biedt de mogelijkheid om de mondelinge beantwoording uit de enquêtes te exporteren naar MP3-formaat: - Ja: 10 punten; - Nee: 0 punten.
W 4.	De Opdrachtnemer biedt de mogelijkheid om de mondelinge beantwoording uit de enquête om te zetten naar een bewerkbaar tekstbestand (Speech-to-Text): - Ja: 10 punten; - Nee: 0 punten.

2.5. Performance eisen

Voor de continuïteit en de klanttevredenheid van de Contactcenters van de Opdrachtgever is het belangrijk dat de Operator een betrouwbare partner is die kan voldoen aan de performance eisen van de Opdrachtgever.

UE 17.	De Opdrachtnemer verzorgt voldoende capaciteit om het Telefoonverkeer van de Opdrachtgever foutloos te kunnen afleveren.
UE 18.	De Spraakkwaliteit dient door Opdrachtnemer aantoonbaar te voldoen aan een minimale MOS-waarde van 4 conform ITU-T P.800 of de overeenkomstige minimale R-Factor waarde van 80 conform ITU-T G.107.
UE 19.	Voor 99% van de Calls per maand treedt er geen merkbare vertraging in het Spraakverkeer. Dat houdt in dat de vertragingstijd op het telecommunicatienetwerk van de Opdrachtnemer maximaal 50 milliseconde end-to-end mag bedragen.
UE 20.	De blokkeringkans voor de Beller per aansluiting (indien niet alle kanalen bezet zijn, dus in het telecommunicatienetwerk van de Opdrachtnemer) mag niet hoger zijn dan 0,1% van alle opgebouwde telefoongesprekken tezamen gemeten per maand.

UE 21.	De performance dient gegarandeerd te zijn voor minimaal 11 Calls per seconde waarbij alle functionaliteit en overige prestatieparameters zoals Spraakkwaliteit, vertraging en blokkeringskans, behouden blijven.
UE 22.	De performance dient gegarandeerd te worden tot pieken van 20 Calls per seconde met een lengte van 15 minuten met behoud van alle functionaliteit en overige prestatieparameters zoals Spraakkwaliteit, vertraging en blokkeringskans.
UE 23.	De Opdrachtnemer levert aansluitingen die een capaciteit van 3000 gelijktijdige Calls kunnen verwerken.
UE 24.	De Opdrachtgever heeft het recht om Derden in te schakelen om de geleverde performance te laten onderzoeken en beoordelen. De Opdrachtnemer verleent medewerking aan onderzoeken door de Opdrachtgever ingeschakelde Derden naar de geleverde performance en de resultaten hiervan direct en ongewijzigd aan Opdrachtgever op te leveren.

2.6. Leveringsgebied

GUE 31.	Het Leveringsgebied waarop Opdrachtgever de Oplossing levert aan de Opdrachtgever beslaat Nederlands grondgebied in Europa. De Opdrachtnemer is gemachtigd en in staat om de Oplossing te kunnen leveren in dit gehele geografische gebied.
GUE 32.	Het fysieke en logische pad van de Oplossing van de Opdrachtnemer en de (eventuele) onderaannemers loopt alleen over Nederlands grondgebied in Europa. Dit ook in geval van routing. Bij afleveren van het Telefoonverkeer bij (de hostingpartij van) een CCAAS-aanbieder is het traject van de infrastructuur van Opdrachtnemer naar de infrastructuur van de CCAAS-aanbieder hiervan uitgezonderd.

2.7. Koppelvlakken

De Koppelvlakken gelden voor zowel ingaand als uitgaand Telefoonverkeer, tenzij het anders is gespecificeerd.

UE 25.	De Opdrachtnemer dient het Telefoonverkeer door middel van SIP (Session Initiation Protocol) trunks op de 2 datacenter locaties van de Opdrachtgever in Apeldoorn en indien van toepassing op de locatie van de nieuwe CCAAS-aanbieder af te leveren.
UE 26.	De Opdrachtnemer levert zijn SIP-trunks af op de 2 datacenter locaties van de Opdrachtgever in Apeldoorn: - Indien de Opdrachtnemer nog geen infrastructuurkoppeling naar de 2 datacenter locaties van de Opdrachtgever in Apeldoorn heeft, dan dient de Opdrachtnemer deze binnen 2 maanden na de ondertekening van de Overeenkomst werkend opgeleverd te hebben; - Bij het aanleggen van infrastructuurkoppelingen naar de 2 datacenter locaties van de Opdrachtgever gelden specifieke eisen. Deze worden op verzoek door de Opdrachtgever toegestuurd.
UE 27.	Bij de koppeling aan het netwerk van de Opdrachtgever dient de Opdrachtnemer te voldoen aan de voorwaarden zoals benoemd in Bijlage 10 'Aansluitvoorwaarden Netwerk aansluitdiensten Datacenter'.

UE 28.	De SIP-trunks (netwerk van Opdrachtnemer naar Opdrachtgever en vice versa die gebruikt worden voor het afleveren van Telefoonverkeer met behulp van het SIP-protocol) dienen minimaal te ondersteunen: - G.711 codec; - SIP-option ping; - Diversion header.
UE 29.	De Opdrachtnemer dient op basis van het SIP-protocol te kunnen koppelen met Session Border Controllers (SBC's) van de Opdrachtnemer. De Opdrachtgever gebruikt Audiocodes Mediant 4000 SBC's. De Opdrachtgever gebruikt per datacenter locatie 2 Mediant 4000 SBC's. De Opdrachtnemer dient het af te leveren Telefoonverkeer evenredig te kunnen verdelen over de beschikbare SBC's van Opdrachtgever.
UE 30.	De Opdrachtnemer is in staat op aanvraag (storing, onderhoud) van Opdrachtgever het Telefoonverkeer naar 1 of 2 SBC's van de Opdrachtgever tijdelijk te blokkeren zonder merkbare gevolgen voor de Bellers.

De Opdrachtgever wenst het aanwijzen van gesprekken voor Blacklisting, het controleren van de maandelijkse rekening en het onderzoek van storingen te vereenvoudigen door telefoongesprekken eenduidig te kunnen identificeren, zowel binnen de systemen van de Opdrachtnemer als binnen de systemen van de Opdrachtgever.

UE 31.	De Opdrachtnemer levert bij de eerste SIP-Invite van een nieuw ingaand Telefoongesprek een extra X-header mee met een Uniek telefoongesprekskenmerk. Dit Unieke telefoongesprekskenmerk wordt door de Opdrachtnemer ook vermeld in de Call Detail Records omtrent de Gegevenslevering.
W 5.	De Opdrachtnemer levert bij de eerste SIP-Invite van een nieuw ingaand telefoongesprek een extra X-header mee met de starttijd van dat gesprek. Het is toegestaan deze waarde toe te voegen aan de X-header met het Unieke telefoongesprekskenmerk: - In Unix Epoch: 20 punten; - Mogelijk (Niet in Unix Epoch formaat) : 10 punten; - Niet mogelijk 0 punten.

2.8. Extra hoge beschikbaarheid

W 6.	Welke extra hoge beschikbaarheid kan de Opdrachtnemer leveren tegen een maximale tariefsvergoeding van niet meer dan € 0,01 per telefoongesprek: - Hoger dan 99,95%: 20 punten; - Vanaf 99,9% t/m 99,95%: 10 punten; - Vanaf 99,8% tot 99,9%: 0 punten.
-------------	---

2.9. Afhandeling ingaand Telefoonverkeer

Het afhandelen van het ingaand Telefoonverkeer is de belangrijkste en primaire dienst die de Operator aan de Opdrachtgever levert.

GUE 33.	De Opdrachtnemer garandeert dat de door Opdrachtgever gebruikte Servicenummers bereikbaar zijn voor alle vaste en mobiele telefoonaansluitingen met telefoonnummers uit het Nationale nummerplan.
GUE 34.	De Opdrachtnemer kan routeren op basis van round-robin over zelf te definiëren Eindbestemmingen van aansluitingen (evenredige verdeling).

GUE 35.	De Opdrachtnemer kan Telefoonverkeer routeren minimaal op basis van de volgende (vrij instelbare) variabelen: - Routeren op basis van netnummer van de oproeper, inclusief het onderscheid tussen vaste telefoonaansluitingen en mobiele telefoonnummers; - Routeren op basis van (tot op de minuut vrij instelbare) tijdvakken, er moeten minimaal 5 vrij instelbare tijdvakken mogelijk zijn; - Combinatie van netnummer routing met tijdrouting moet mogelijk zijn; - Routeren op basis van instelbare belintensiteit naar andere door de Opdrachtgever op te geven locaties (overflow naar andere locaties of andere Eindbestemmingen); - Routeren op basis van procentuele verdeling over zelf te definiëren groep van Eindbestemmingen van aansluitingen.
----------------	--

2.10. Servicenummers

In Bijlage 14 'Overzicht Servicenummers' is een overzicht van de huidige Servicenummers van de Opdrachtgever weergegeven.

2.10.1. 0800-nummers

GUE 36.	De Opdrachtnemer kan de Diensten voor Telefoonverkeer van 0800-nummers.
----------------	---

2.10.2. 088-nummers

GUE 37.	De Opdrachtnemer kan de Dienst inzetten voor Telefoonverkeer van 088-nummers.
----------------	---

2.10.3. 0900-nummers

GUE 38.	De Opdrachtnemer kan de Dienst inzetten voor Telefoonverkeer van 0900-nummers met afwijkende gesprekskosten waarbij de Opdrachtgever zelf de hoogte van het tarief (inclusief nul-tarief) voor de geboden informatie bepaalt.
----------------	---

2.10.4. 14xx-nummers

De Opdrachtgever wil ook de mogelijkheid hebben gebruik te kunnen maken van 14xx-nummers. De Operator dient deze beschikbaar te stellen op verzoek van de Opdrachtgever.

GUE 39.	De Opdrachtgever kan de Dienst zonder beperkingen inzetten voor Telefoonverkeer afkomstig van 14xx-nummers.
----------------	---

GUE 40.	De Opdrachtnemer kan telefoonnummers uit de 14xx-nummerreeks leveren, die bedoeld zijn voor overheidsinstanties en -instellingen.
----------------	---

2.10.5. Internationale 0800-nummers

Ook buiten de landsgrenzen van Nederland zijn Belastingplichtige woonachtig. Specifiek voor deze Belastingplichtigen dienen er telefoonnummers beschikbaar gesteld te worden waarmee de Beller naar de Opdrachtgever vanuit het Buitenland gratis kan bellen.

GUE 41.	De Opdrachtgever maakt gebruik van internationale 0800-nummers. De Opdrachtgever kan de Dienst zonder beperkingen inzetten voor verkeer afkomstig van internationale 0800-nummers.
----------------	--

2.10.6. Lokale Servicenummers

Het is mogelijk om lokale Servicenummers af te nemen. Lokale Servicenummers zijn (kleine) nummerblokken uit het Nationale nummerplan waarop 0800-nummers kunnen worden geleverd. De Beller betaalt het tarief, behorend bij het bellen van een geografisch telefoonnummer.

GUE 42.	De Opdrachtgever kan de Dienst zonder beperkingen inzetten voor Telefoonverkeer afkomstig van lokale Servicenummers.
----------------	--

2.11. Uitgaand Telefoonverkeer

De Opdrachtnemer is verantwoordelijk voor het leveren van de Oplossing die noodzakelijk zijn om te garanderen dat de Opdrachtgever uitgaand Telefoonverkeer kan verrichten. Daarnaast dat de Oplossing voldoet aan de kwaliteit en eisen die de Opdrachtgever hieraan stelt. De Oplossing die de Opdrachtnemer aanbiedt voor het uitgaande Telefoonverkeer dient naadloos te functioneren in combinatie met de infrastructuur van de Opdrachtgever.

GUE 43.	Het moet mogelijk zijn dat de Opdrachtgever bij uitgaande telefoongesprekken de geografische telefoonnummers weergeeft behorend bij de SIP-trunk en 088-nummers uit het nummerplan van de Opdrachtgever zie Bijlage 11 'Nummerplan en overzicht aansluitingen'. Het betreffende telefoonnummer wordt weergegeven in het display van de ontvanger van het gesprek.
----------------	---

GUE 44.	De levering van de geografische telefoonnummerblokken is noodzakelijk om bij het uitgaande Telefoonverkeer geografische CLI's (Call Line Identification) mee te kunnen sturen. Het betreft hier de volgende reeds aanwezig telefoonnummerblokken: - 055-53853xx (waarvan 10 stuks als lokaal Servicenummer); - 055-54347xx; - 055-54348xx; - 055-54349xx.
----------------	--

GUE 45.	Voor Telefoonverkeer bij ontwikkel, test en acceptatie werkzaamheden is het noodzakelijk te kunnen testen op geografische telefoonnummers. In Bijlage 11 'Nummerplan en overzicht aansluitingen' benoemde geografische telefoonblokken dienen ook voor ingaande Telefoonverkeer geschikt te zijn.
----------------	---

2.12. Gegevenslevering

UE 32.	De Opdrachtnemer voorziet in een geautomatiseerde Gegevenslevering in CSV-formaat door middel van SFTP op een daarvoor door de Opdrachtgever beschikbaar gestelde locatie en de afgesproken tijd. De Gegevenslevering dient te voldoen aan de specificaties zoals weergegeven in de Bijlage 12 'Specificatie gegevenslevering'
---------------	--

UE 33.	De Opdrachtnemer dient de dagelijkse geautomatiseerde Gegevenslevering ook op de volgende manier aan te leveren: - Gegevensleveringen zijn ook als rapportage in de Portal beschikbaar.
---------------	---

UE 34.	De Opdrachtgever kan in de Portal rapportages genereren. In de Portal zijn standaard templates aanwezig, en is er de mogelijkheid om zelfstandig templates te kunnen ontwikkelen.
UE 35.	Alle Gegevensleveringen moeten tussen 00:00 en 02:30 plaatsvinden. Dit geldt voor de dagelijkse rapportages. Wat betreft de maandelijkse rapportages op de eerste werkdag van de volgende maand.
UE 36.	Indien er behoefte bestaat aan afwijkende rapportage, rapportagefrequenties of aanvullende rapportage items, dan is het mogelijk dat de Opdrachtnemer deze laat ontwikkelen. Dit valt onder de Additionele dienstverlening.
UE 37.	De Opdrachtnemer dient alle rapportages en bijbehorende Brongegevens gedurende de Overeenkomst vermeerderd met 1 jaar te bewaren. Gedurende deze periode dienen de rapportages en Brongegevens direct beschikbaar te zijn.
UE 38.	De Opdrachtnemer dient alle rapportages en bijbehorende Brongegevens gedurende de Overeenkomst vermeerderd met 1 jaar te bewaren. Na afloop van deze periode dienen deze Gegevens definitief te worden verwijderd.
UE 39.	Bij storingen of onjuiste leveringen, wordt een nieuwe Gegevenslevering gedaan. Deze nieuwe Gegevenslevering wordt uiterlijk binnen 1 Werkdag geleverd (bij voorkeur nog eerder). Vanuit de Opdrachtgever wordt een pro-actieve signalering verwacht, zodat storing en onjuiste Gegevensleveringen pro-actief worden gesignaleerd en hersteld. Het is herkenbaar dat deze Gegevenslevering nieuw is (ander id).
UE 40.	Wanneer nieuwe enquêtes worden gemaakt dienen de Gegevens van de nieuwe enquêtes vanaf de eerst volgende Gegevenslevering meegeleverd te worden.
UE 41.	Van alle Gegevensleveringen stelt de Opdrachtnemer Documentatie beschikbaar in de vorm van datamodellen, definities en bedrijfsregels (business rules).
UE 42.	De Opdrachtnemer levert Gegevens aan, waarmee Opdrachtgever in staat wordt gesteld te kunnen voldoen aan de eisen die zijn gedefinieerd in de Archiefwet. Nadere uitwerking zal verder worden gedefinieerd in de DAP.

Hoofdstuk 3. IV kaders

In hoofdstuk 3 'IV kaders' worden de algemene beveiliging en Informatiebeveiliging beschreven waaraan de Oplossing dient te voldoen. Bestaande uit de volgende paragrafen: algemene Beveiligingseisen, Informatiebeveiligingseisen en specifieke eisen van de Opdrachtgever.

3.1. Algemene Beveiligingseisen

UE 43.	De Opdrachtnemer garandeert Opdrachtgever de integriteit en vertrouwelijkheid van de aangeboden Oplossing.
UE 44.	De Opdrachtnemer maakt op aanvraag van de Opdrachtgever inzichtelijk welke maatregelen er zijn genomen om de integriteit en vertrouwelijkheid aan de Opdrachtgever aangeboden Oplossing te waarborgen.
UE 45.	De Opdrachtgever heeft het recht om Derden in te schakelen om de geleverde beveiliging te laten onderzoeken en beoordelen. De Opdrachtnemer verleent kosteloos medewerking aan onderzoeken op dit gebied door de Opdrachtgever ingeschakelde Derden.
UE 46.	De Opdrachtnemer informeert de Opdrachtgever binnen 4 uur indien er sprake is van een Securityincident en neemt passende maatregelen.
UE 47.	De Opdrachtnemer is te allen tijde verantwoordelijk voor de geleverde Oplossing aan de Opdrachtgever. Dit geldt zowel voor Oplossing die geleverd worden via het eigen telecommunicatienetwerk van Opdrachtnemer als voor Oplossing die geleverd worden via andere (gehuurde) telecommunicatienetwerken.
UE 48.	Voorafgaand aan alle door de Opdrachtnemer uit te voeren werkzaamheden - zowel op locatie als op afstand – met betrekking tot de te leveren Oplossing bij de Opdrachtgever wordt altijd de geautoriseerde contactpersoon van de betreffende locatie geïnformeerd.
UE 49.	De SIP-trunks (telecommunicatienetwerk van Opdrachtnemer naar Opdrachtgever en vice versa die gebruikt worden voor het transport van Telefoonverkeer met behulp van het SIP-protocol) dienen minimaal te kunnen ondersteunen: - TLS; - Secure SIP; - Secure RTP.
UE 50.	De Gegevens worden verwerkt in lidstaten van de EU of een land met een door de EU goedgekeurd beveiligingsniveau. De Gegevens van de Opdrachtgever verlaten deze landen niet.

Indien de Opdrachtnemer of één van haar Onderaannemers onder wetgeving valt waardoor Gegevens op wettelijke basis wel gedeeld moeten worden met Derden dan maakt Opdrachtgever dat bij Inschrijving bekend. Hierbij wordt duidelijkheid gegeven om welke partijen het gaat en hoe dergelijke verzoeken afgehandeld worden. Het betreft Onderaannemers die betrokken zijn bij de Opdrachtgever afgenomen Oplossing.

UE 51.	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.
--------	---

De Opdrachtgever wil de 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.

UE 52.	De Opdrachtnemer geeft inzicht in de Onderaannemers en in welke landen deze Onderaannemers geregistreerd zijn.
--------	--

3.1.1. Levering in CCAAS-omgeving (Contact Center as a Service)

De verwachting is dat mede door de ontwikkelingen in de markt, de Opdrachtnemer de Oplossing dient af te leveren aan de CCAAS-omgeving waar de Opdrachtgever gebruik van maakt.

UE 53.	Indien de Opdrachtgever gebruik gaat maken van CCAAS dan levert de Opdrachtnemer het Telefoonverkeer via redundante verbindingen naar het datacenter waarvan de CCAAS-aanbieder gebruik van maakt.
--------	--

3.2. Informatiebeveiligingseisen

De Oplossing die door de Opdrachtnemer wordt geleverd, voldoet aan alle in Nederland toepasselijke wettelijke bepalingen.

UE 54.	Opzet, bestaan en werking van het informatiebeveiligingsbeleid kan periodiek worden aangetoond door Opdrachtnemer. Er wordt ook aangetoond dat dit informatiebeveiligingsbeleid onderhevig is aan een PDCA-cyclus. De Opdrachtnemer verstrekt ter beoordeling een door een geaccrediteerde partij verstrekt ISO27001-certificaat, compleet met bijbehorend Statement of Applicability. Uit het geleverde blijken opzet, bestaan en werking van geïmplementeerd informatiebeveiligingsbeleid.
--------	---

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 Oplossing.

UE 55.	De Opdrachtgever heeft het recht om zelf (een deel van) de Oplossing aan een Audit te onderwerpen. Basis van de Audit is deze Specificatie van de Opdracht.
--------	---

3.2.1. Gegevens

UE 56.	Gegevens van de Opdrachtgever worden logisch gescheiden opgeslagen van de Gegevens van andere klanten. Toegang tot deze Gegevens is beperkt tot de Opdrachtgever en voor zover noodzakelijk voor het uitvoeren van de Overeenkomst door Opdrachtnemer.
--------	--

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 Derden. Gegevens worden door Opdrachtnemer alleen verwerkt voor de doelen waarover afspraken gemaakt zijn.

UE 57.	De 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 Opdrachtgever maakt bij voorkeur gebruik van versleutelde Gegevens bij opslag (encryption-at-rest). Eén van de voordelen is dat als de Gegevens op ongecontroleerde wijze buiten de Oplossing terecht komen, Derden geen gebruik kunnen maken van deze Gegevens.

UE 58.	Op de Gegevens wordt door Opdrachtnemer de encryption-at-rest toegepast.
---------------	--

Als de Opdrachtgever dat nodig acht dan kan de Opdrachtgever de Opdrachtnemer verzoeken zijn Gegevens of een deel van zijn Gegevens te verstrekken voor verdere verwerking. Aanleveren van de Gegevens gebeurt via een beveiligd kanaal van de Opdrachtgever in een door de Opdrachtgever bruikbaar digitaal formaat.

UE 59.	De Opdrachtnemer levert op aanvraag en conform afspraken een voor de Opdrachtgever bruikbare digitale kopie van de meest actuele Gegevens en de structuur. Vertrouwelijkheid en integriteit blijven geborgd.
---------------	--

3.2.2. Proces

Beschikbaarheid, integriteit en vertrouwelijkheid van Gegevens van de Opdrachtgever mogen op geen enkele manier gecompromitteerd raken. Van medewerkers van Opdrachtnemer met toegang tot Gegevens en de Oplossing is de achtergrond gecontroleerd. Voor Nederlandse ingezetenen wordt gebruik gemaakt van de VOG. Voor niet-ingezetenen kan een gelijkwaardige verklaring worden overlegd. De Opdrachtgever oordeelt over de bruikbaarheid hiervan.

UE 60.	De Opdrachtnemer heeft van alle medewerkers met toegang tot de Gegevens de achtergrond geverifieerd conform relevante wet- en regelgeving. Voor Nederlandse ingezetenen wordt gebruik gemaakt van de VOG. Voor niet-ingezetenen kan een gelijkwaardige verklaring worden overlegd.
---------------	--

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 hij dit noodzakelijk wordt geacht. 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 61.	De 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.
---------------	---

UE 62.	Als er Broncodeonderzoek uitgevoerd moet worden dan kan Opdrachtnemer een (aanvullende) 'Non-disclosure agreement Broncodeonderzoek' afsluiten met de A&P- testpartij.
---------------	--

3.3. Specifieke eisen van de Opdrachtgever

De Opdrachtgever stelt eisen die specifiek zijn voor de Opdrachtgever. Hier zijn ook eisen opgenomen om te borgen dat de Opdrachtgever aan het overheidsinformatiebeveiligingsbeleid (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 Opdrachtgever specifieke zaken.

3.3.1. Forum Standaardisatie

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 standaarden moet toepassen (dus zonder Leg-uit-mogelijkheid).

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.

UE 63.	De Opdrachtnemer committeert zich aan het gebruik van de Verplichte standaarden van het Forum Standaardisatie in relatie tot de Oplossing. Het betreft de volgende standaarden: 1. De Opdrachtnemer is in staat voor alle webverbindingen van de Oplossing HTTPS en HSTS toe te passen conform de richtlijnen van het NCSC. Er wordt alleen gebruik gemaakt van standaarden en instellingen die door het NCSC als 'Goed' zijn gekwalificeerd ("ICT-beveiligingsrichtlijnen voor Transport Layer Security"). Met de 'Qualys SSL Labs SSL Server Test'¹ wordt minimaal een A-behaald. 2. De Opdrachtnemer is in staat voor e-mailverbindingen met de Opdrachtgever en/of burgers en/of bedrijven TLS, STARTTLS, DANE, SPF en DMARC toe te passen. De IP-adressen van verzendende systemen zijn geregistreerd als SPF-record in de DNS van de verzendende domeinnaam. Van inkomende e-mailberichten wordt de geldigheid van het verzendend IP-adres gecontroleerd tegen het IP-adres van de verzendende server. De policies voor SPF en DMARC zijn strikt geconfigureerd (SPF: "~all" en "-all", DMARC: "p=quarantine" en "p=reject"). STARTTLS is zodanig geconfigureerd dat alleen e-mailverkeer over TLS mogelijk is. TLS is geconfigureerd conform de richtlijnen van het NCSC ("ICT-beveiligingsrichtlijnen voor Transport Layer Security", er wordt alleen gebruik gemaakt van standaarden en instellingen die door het NCSC als 'Goed' zijn gekwalificeerd.). 3. De Opdrachtnemer is in staat web- en maildomeinen waar de Oplossing gebruik van maakt beschikbaar te maken via zowel IPv4 als IPv6 (dual stack). In het gebruik, in de breedste zin van het woord, tussen IPv4 en IPv6 is geen verschil. 4. De Opdrachtnemer is in staat voor elke domeinnaam van de Oplossing voor communicatie met burgers en/of bedrijven gebruik te maken van DNSSEC. De domeininformatie, zoals bijbehorende IP-adressen, is met een geldige DNSSEC-handtekening ondertekend. 5. De Opdrachtnemer is in staat voor elke domeinnaam van de Oplossing gebruik te maken van SPF, DKIM en DMARC. Alleen met nadrukkelijke toestemming van de Opdrachtgever kan hier van worden afgeweken. De Opdrachtnemer gaat akkoord met het toepassen van wijzigingen op basis van wijzigingen bij het Forum van Standaardisatie
--------	--

3.3.2. Richtlijnen beveiligingsincidenten

3.3.2.1. Standaard afhandeling

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. De 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 46.	De 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 aangeven, de verwachte consequenties voor de Opdrachtgever alsmede de reeds getroffen en te treffen maatregelen om de gevolgen te beperken.
----------------	--

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 47.	De Opdrachtnemer heeft zijn bedrijfsvoering zodanig ingericht dat technische kwetsbaarheden adequaat worden ontdekt, geëvalueerd en geadresseerd. Daarnaast is het patchmanagement is ingericht. Opdrachtnemer werkt kosteloos mee aan analyse en afhandeling van het Beveiligingsincident of de (mogelijke) inbreuk op persoonsgegevens..
----------------	---

De Opdrachtgever houdt er rekening mee dat Opdrachtnemer zijn Oplossing ook levert of gaat leveren aan Derden. Indien in dergelijk geval inbreuken op beveiliging en/of persoonsgegevens gebeuren, die ook kunnen gebeuren in de geleverde Oplossing, dan wordt de Opdrachtgever daarvan op de hoogte gebracht om zonodig mitigerende maatregelen te kunnen treffen. De Opdrachtgever monitort dit actief. 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 een zero-day exploit. Het gaat de Opdrachtgever om het (technisch) inhoudelijke Incident om dit te kunnen analyseren en –zonodig- mitigerende maatregelen te treffen. Er worden nadrukkelijk geen bedrijfsgegevens van getroffen partijen gedeeld.

UE 64.	De 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. De 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.
---------------	---

3.3.2.2. Datalek afhandeling

De Verwerkingsverantwoordelijke (in dit geval Opdrachtgever) 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 65.	De 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.
---------------	---

3.3.2.3. Coördinated Vulnerability Disclosure

De Opdrachtgever heeft een Coördinated Vulnerability 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: <https://www.belastingdienst.nl/security#coordinated-vulnerability-disclosure>.

UE 66.	De Opdrachtnemer handelt via de Opdrachtgever gemelde CVD-meldingen af conform het CVD-beleid van de Opdrachtgever. Gemelde kwetsbaarheden worden conform het CVD-beleid afgehandeld.
---------------	--

3.3.3. 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 continu). De partij waar 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 beveiligingstesten 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 uit de Functionals security de beveiligingstest behoort uit te voeren. De andere partij werkt op verzoek kosteloos mee aan dergelijke testen met 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 beveiligingsmaatregelen (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:
 - o managementsamenvatting met een definitie van de opdracht, relevante kenmerken van de A&P-test, een conclusie en aanbevelingen;
 - o 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:

- wordt getest in de Acceptatieomgeving, die 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 67.	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.
UE 68.	Indien de Opdrachtgever het noodzakelijk acht (op basis van een risico-inschatting) een Vulnerability scan uit te laten voeren op de Oplossing dan staat Opdrachtnemer dat toe. Kosten van het uitvoeren van de Vulnerability scan worden gedragen door de Opdrachtgever. Eventuele Kwetsbaarheden worden conform de richtlijnen van de Opdrachtgever opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan.
UE 69.	De Opdrachtnemer heeft een beveiligingstestbeleid en voert ook beveiligingstesten conform dit beleid uit.
UE 70.	De Opdrachtnemer geeft inzage in het beveiligingstestbeleid en levert een rapportage dan wel verslag betreffende de volgende testen: - Rapport A&P-test - Rapport Vulnerability scan

3.3.4. Continuïteit- en continuïteitstesten

Van belang is om te weten welke maatregelen getroffen zijn om eventuele onbeschikbaarheid te voorkomen én hoe snel 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 de Opdrachtnemer wordt verwacht dat de Oplossing bij onbeschikbaarheid binnen bepaalde termijnen weer beschikbaar is zonder verlies van integriteit en vertrouwelijkheid.

UE 71.	De Oplossing voldoet aan onderstaande eisen betreffende de operationele continuïteit in geval van een Calamiteit (crisis): - Recovery Time Objective (RTO): De Oplossing is binnen 2 dagen weer volledig functioneel beschikbaar; - Recovery Point Objective (RPO): Er is maximaal 3 klokuren verlies van Gegevens toegestaan. Beleid en procedures om bovenstaande te borgen zijn vastgesteld.
--------	--

UE 72.	De Opdrachtnemer voert periodiek een Backup & Restoretest uit. De 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.
--------	--

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. Opdrachtnemer 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 73.	Na afloop 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.
--------	---

3.3.5. Voortbrenging (onderdelen) Oplossing

Bij het ontwerpen en ontwikkelen van Oplossing wordt gewerkt vanuit de principes dat de Oplossing voldoet aan informatiebeveiligingsstandaarden, voldoet aan de privacywetgeving en de gedachte dat beschikbaarheid zowel operationeel als bij uitzonderingssituaties geborgd is. Deze principes zijn cyclisch in het ontwerp geborgd, op een correcte manier geïmplementeerd en geëvalueerd. In de markt wordt dit wel aangeduid met Naast 'Security by Design', 'Privacy by Design' en 'Continuity by Design'.

UE 74.	De gangbare principes rondom 'Security by Design', 'Privacy By Design' (samen met 'Privacy by Default') en 'Continuity by Design' voor het ontwerp en de ontwikkeling van software en systemen toegepast.
--------	--

UE 75.	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.
--------	--

3.3.6. Logging

De systemen die door Opdrachtnemer gebruikt worden voor het leveren van Oplossing aan Opdrachtgever, dienen te voldoen aan onderstaande eisen betreffende logging.

UE 76.	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. Logbestanden zijn beveiligd tegen ongeautoriseerde toegang/wijziging en zijn geschikt om forensisch onderzoek te verrichten. Logbestanden in het kader van technische beveiligingslogging worden minimaal 18 maanden bewaard. Logbestanden die onderdeel uitmaken van forensisch onderzoek naar een beveiligingsincident worden bewaard, zolang het onderzoek niet afgesloten is. 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 sluiten aan op die van de Opdrachtgever. Eventuele nadere afspraken worden beschreven in de DAP.
----------------------	---

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

De Oplossing en bijbehorende functies en Gegevens mogen alleen gebruikt worden door bevoegde personen van Partijen. 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. De Oplossing heeft alleen een openbaar gedeelte als dit nadrukkelijk geëist is door de Opdrachtgever.

UE 78.	Een gebruikersidentificatie (gebruikersaccount) is altijd 1 op 1 herleidbaar naar een Natuurlijk Persoon of een gedocumenteerd en geregistreerd systeem account.
---------------	--

De Opdrachtgever stelt de volgende algemene eisen aan authenticatie. Zo is het gebruik van intern gebruikte user ID's niet toegestaan (e-mailadres van de Opdrachtgever mag wel). Voor de Opdrachtgever zijn ook minimale vereisten voor wachtwoorden van toepassing.

UE 79.	Als identificatie is het gebruik van het user ID van de Opdrachtgever niet toegestaan.
---------------	--

UE 80.	De wachtwoorden voldoen minimaal aan de eisen zoals gesteld in de BIO. a) Algemeen (technisch afdwingen) - Gebruik van wachtwoorden wordt geautomatiseerd afgedwongen - Initiële wachtwoorden (inclusief die gereset zijn) zijn een werkdag geldig en worden bij eerste gebruik gewijzigd; - Eisen aan wachtwoorden worden geautomatiseerd afgedwongen. b) Geen MFA: - Minimaal 12 posities, complex (nummers, klein, groot); - Aantal foutieve inlogpogingen: 10. In dat geval: blokkering account; - Minimaal jaarlijks vernieuwen. Indien het authenticatieproces is gekoppeld aan dat van de Opdrachtgever dan zijn de richtlijnen van de Opdrachtgever leidend.
---------------	---

Gebruikers van Opdrachtnemer en Opdrachtgever met speciale (beheer)rechten binnen de Oplossing of met uitgebreide toegang en mogelijkheden tot de Gegevens, maken gebruik van multi-factor authentication (MFA). Voor andere gebruikers bestaat de mogelijkheid dit aan te zetten.

UE 81.	De Oplossing heeft een multi-factor authenticationmechanisme. Voor alle Gebruikers met verhoogde rechten (bijvoorbeeld: beheerrechten) is het gebruik verplicht. Voor andere Gebruikers kan de Opdrachtgever dit mechanisme op basis van rol (laten) activeren.
---------------	---

3.3.8. Koppelingen

De Oplossing is vaak met andere ICT-systemen binnen de Opdrachtgever gekoppeld. In alle gevallen zullen er Aansluitvoorwaarden van toepassing zijn. De Opdrachtgever stelt een aantal specifieke eisen die er op gericht zijn organisatorisch en technisch aan te sluiten op de Opdrachtgever.

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 client.

UE 82.	De Oplossing maakt gebruik van een zero-footprint client en maakt gebruik van een standaard webbrowser.
UE 83.	De Webrowsers om de Oplossing te benaderen worden door de maker van de webbrowser nog ondersteund middels beveiligingsupdates. De webrowsers zijn voorzien van de meest recente security Patches.

Hoofdstuk 4. Integriteit

4.1. Business Etiquette

De 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.

GUE 48.	De Opdrachtnemer conformeert zich aan de Business Etiquette zoals opgenomen in Bijlage 4 van het Beschrijvend Document.
----------------	---

4.2. Verzekering

UE 84.	Gezien de aard van de werkzaamheden acht de Opdrachtgever het noodzakelijk dat Inschrijver verzekerd is tegen bedrijfsaansprakelijkheid, dan wel bereid en in staat te zijn om bij gunning zich voor bedrijfsaansprakelijkheid te verzekeren met een minimale dekking van €2.500.000 per jaar en een dekking van €1.000.000 per aanspraak, gedurende tenminste de looptijd van de Overeenkomst. Op daartoe strekkend verzoek verstrekt de winnende Inschrijver bewijs van adequate verzekering.
---------------	---

Hoofdstuk 5. Maatschappelijk Verantwoord Inkopen (MVI)

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

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

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

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

5.1. Energieverbruik

W7.	Geef aan in welke mate het datacenter waarop de Oplossing wordt gehost CO2 neutraal is. De Inschrijver toont met een bewijs aan waaruit blijkt dat in welke mate aan dit criterium is voldaan. De waardering voor deze Wens is: - Vanaf 96 % tot en met 100% 15 punten; - Vanaf 91 % t/m 95% 10 punten; - Vanaf 81 % t/m 90% 5 punten; - Vanaf 0 % t/m 80% 0 punten; - In geval er geen bewijs is aangeleverd 0 punten.
------------	--

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.

GUE 49.	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 85.	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 2Aw2012. Kennis omtrent die belastingen en milieubescherming, arbeidsvoorwaarden en arbeidsbescherming kunnen Inschrijvers, voor zover het gaat om uitvoering in Nederland, verkrijgen bij:

	- Opdrachtgever, www.belastingdienst.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 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). De wijzigingen en/of de aangepaste overeenkomst zullen/zal de Inschrijvers per nota van inlichtingen kenbaar worden gemaakt.

GUE 50.	Inschrijver gaat akkoord met de concept Overeenkomst met inbegrip van de eventuele per Nota van Inlichtingen kenbaar gemaakte wijzigingen zoals genoemd in Bijlage 2 'Beschrijvend document', paragraaf 3.2.1.
----------------	--

GUE 51.	Inschrijver gaat akkoord met de volledige inhoud en alle voorwaarden uit Bijlage 8 'Wachtkamerovereenkomst', met inbegrip van de eventuele per Nota van inlichtingen kenbaar gemaakte wijzigingen.
----------------	--

Hoofdstuk 7. Prijsstelling

7.1. Algemene eisen ten aanzien van Prijzen

In de in Bijlage VII “Prijzenformulier” geoffeerde Prijzen dienen alle kosten voor de Prestatie 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 86.	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 Prestatie conform de in de Aanbestedingsstukken gestelde eisen en de in de Inschrijving opgenomen beantwoording van de wensen, kan Opdrachtnemer niet in rekening brengen bij Opdrachtgever.
---------------	--

UE 87.	Eventuele valutarisico's zijn volledig voor rekening van Opdrachtnemer en worden geacht in de geoffeerde Prijzen te zijn verwerkt.
---------------	--

UE 88.	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”

In Bijlage VII ‘Prijzenformulier’ zijn een aantal tabbladen opgenomen welke door de Inschrijver ingevuld dient te worden.

Tabblad ‘Samenvatting’

Het betreft hier een samenvatting van de hieronder genoemde tabbladen. De vergelijkingswaarde wordt gebruikt om de Inschrijvingen met elkaar te vergelijken en de ‘Beste Prijs & Kwaliteit verhouding’ te bepalen.

De Inschrijver dient in alle genoemde tabbladen de geel gearceerde cellen in te vullen.

Tabblad ‘Functionals & Migratie’

De Inschrijver dient het tarief per functional op 2 verschillende manieren invullen:

- Migratie (fixed fee, jaar 1) of eenmalig;
- Servicekosten per maand.

Tabblad ‘Gesprekskosten inbound’

De Inschrijver dient het tarief voor vast, mobiel en internationaal op 2 verschillende manieren invullen:

- Starttarief;
- Tarief per minuut.

Tabblad 'Gesprekskosten Outbound'

De Inschrijver dient het tarief voor vast, mobiel en internationaal op 2 verschillende manieren invullen:

- Starttarief;
- Tarief per minuut.

Tabblad 'Additionele dienstverlening'

In het tabblad wordt er onderscheid gemaakt in 2 typen Additionele dienstverlening:

- Opleiding: De Inschrijver dient onder andere het tarief 'Opleidingskosten per dagdeel per groep', 'Groepsgroote' en 'Benodigd aantal dagdelen per groep' in te vullen;
- Consultancy: De Inschrijver dient het 'Uurtarief' in te vullen.

GUE 52.	De Inschrijver dient de Bijlage VII 'Prijzenformulier' volledig in te vullen. Het is, op straffe van uitsluiting van de aanbestedingsprocedure, niet toegestaan om de inhoud, opmaak en formules van de spreadsheet te wijzigen.
----------------	--

GUE 53.	De Inschrijver vermeld alle geldbedragen in Euro's en exclusief omzetbelasting (BTW).
----------------	---

7.3. Indexering Prijs

De door Inschrijver geoffreerde Prijzen en Tarieven, zoals opgegeven in Bijlage VII 'Prijzenformulier', mogen jaarlijks per 1 januari, maar niet eerder dan in 2025 worden geïndexeerd op basis van de CBS tabel 'Dienstenprijzen; commerciële dienstverlening en transport, indexcijfers (2015 = 100)' conform de volgende webpagina: <https://opendata.cbs.nl/#/CBS/nl/dataset/83760NED/table?dl=60A3F>

Prijsaanpassingen dienen uiterlijk 1 december 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 1 decimaal achter de komma. Inhaalslagen op niet doorgevoerde indexeringen worden niet geaccepteerd.

UE 89.	De opgegeven Tarieven staan vast voor het 1 ^e jaar. De Tarieven kunnen daarna jaarlijks per 1 januari worden herzien. De eerste tariefherziening kan derhalve plaatsvinden op 1 januari 2025.
---------------	--

UE 90.	De maximale tariefherzieningen zijn begrensd door het indexcijfer 'Dienstenprijzen (DPI); commerciële dienstverlening en transport; indexcijfers 2015 = 100', (CPA2008, kwartaalindex) conform de volgende webpagina: https://opendata.cbs.nl/#/CBS/nl/dataset/83760NED/table?dl=60A3F zoals gepubliceerd door het CBS. De Opdrachtnemer dient uiterlijk, per 1 december van enig jaar, een schriftelijk verzoek in bij de verantwoordelijk contractmanager van de Opdrachtgever, met bijbehorende onderbouwing en motivering om voor tariefherziening in aanmerking te komen.
---------------	---

UE 91.	Het is niet toegestaan om eventueel in een voorgaand jaar niet in rekening gebrachte tariefherzieningen later alsnog toe te passen.
---------------	---

Hoofdstuk 8. Documentatie en Opleiding

8.1. Documentatie

UE 92.	Opdrachtnemer zal Opdrachtgever tijdig voorzien van actuele en volledige Documentatie in elektronische vorm, ten behoeve van gebruik van de Oplossing in de Operationele fase. Hierbij is de Documentatie over de eigenschappen en gebruiksmogelijkheden van de Oplossing in de Nederlandse en/of Engelse taal.
UE 93.	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 94.	De Documentatie dient in een Docx-format aangeleverd te worden, zodat Opdrachtgever deze zelf kan aanpassen wanneer Opdrachtgever in de toekomst zaken wijzigt in de configuratie van de Oplossing.
UE 95.	Opdrachtgever mag de Documentatie voor gebruik binnen de eigen organisatie reproduceren en wijzigen.
UE 96.	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 Oplossing, blijkt dat de Documentatie onjuiste informatie bevat of anderszins onvolledig, onvoldoende, onduidelijk en/of verouderd is.

8.2. Opleiding

UE 97.	De Opdrachtnemer levert relevante Opleidingen, inclusief Documentatie, inzake het gebruik van de Oplossing, alsmede het functioneel, technisch en applicatief beheer van de Oplossing.
UE 98.	Opleidingen vinden plaats op locatie van de Opdrachtgever tenzij nadrukkelijk anders overeengekomen.
UE 99.	De Opleidingen vinden plaats in Nederland in de Nederlandse en/of Engelse taal.
UE 100.	Lesmateriaal voor Gebruikers is in de Nederlandse of Engelse Taal beschikbaar.

Hoofdstuk 9. Voorbereiding- en Migratieperiode

9.1. Voorbereiding

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

9.2. Migratieperiode

UE 101.	Outbound telefonie dient uiterlijk 23-07-2024 gebruiksklaar te zijn. Dan dient de Migratie voltooid te zijn.
UE 102.	Inbound telefonie inclusief de Portal dient uiterlijk 16-08-2024 gebruiksklaar te zijn. Dan dient de Migratie voltooid te zijn.
GUE 54.	De Opdrachtnemer committeert zich aan de Migratie zoals gedefinieerd in de Bijlage 13 'Migratie'.
UE 103.	De kosten voor de uitvoering van de Migratie zijn door de Opdrachtnemer geprijsd in Bijlage VII 'Prijzenformulier'.
UE 104.	De Opdrachtnemer stelt een Migratieplan op. Hierin is een planning met mijlpalen opgenomen. De Opdrachtnemer moet deze mijlpalen halen. Het niet halen van één of meerdere van de hieronder benoemde mijlpalen kan leiden tot diskwalificatie van de Opdrachtnemer, dit ter beoordeling van de Opdrachtgever: - Oplevering goedgekeurd Migratieplan: uiterlijk 30 Werkdagen na na ondertekening van de Overeenkomst; - Oplevering Koppelvlak voor de SIP-trunks: uiterlijk 3 maanden na ondertekening van de Overeenkomst; - Oplevering eerste versie van de Portal: uiterlijk 3 maanden na ondertekening van de Overeenkomst. (Hierbij zijn bevindingen van alle types toegestaan); - Oplevering van de Portal met volledige functionaliteit: uiterlijk 5 maanden na ondertekening van de Overeenkomst. (Alleen bevindingen van het type cosmetisch en hinderlijk toegestaan); - Proefmigratie van één 0800-nummer: uiterlijk 5 maanden na ondertekening van de Overeenkomst.

9.3. Acceptatietest en -procedure

UE 105.	Bij de oplevering van de Oplossing tijdens de migratieperiode wordt een Acceptatietest doorlopen. Doel van deze Acceptatietest is vaststellen dat de Oplossing voldoet aan relevante functionele Eisen en Wensen uit Bijlage A, hoofdstuk 2.
UE 106.	De Opdrachtnemer voert de Acceptatietest gedurende de migratieperiode uit. Uitvoering van de Acceptatietest in delen is toegestaan, bijvoorbeeld op basis van de op dat moment al opgeleverde Oplossing. In dat geval wordt een conformiteitenlijst bijgehouden door de projectmanager Migratie van Opdrachtnemer. In het projectoverleg Migratie wordt de conformiteitenlijst met de Opdrachtgever doorgenomen.
UE 107.	De Opdrachtnemer heeft een resultaatverplichting voor het tijdens de migratieperiode succesvol afronden van de Acceptatietest en zal daarvoor de benodigde kennis en expertise beschikbaar stellen. De Opdrachtgever zal ten behoeve van de Acceptatietest deskundigheid en infrastructuur ter beschikking stellen.

UE 108.	Het Acceptatietestplan wordt door Opdrachtnemer opgesteld en ter goedkeuring aangeboden aan de Opdrachtgever. Met de uitvoering van de Acceptatietest bewijst de Opdrachtnemer aan de Opdrachtgever dat de aangeboden Oplossing te functioneren op de infrastructuur van de Opdrachtgever. Bij een positief resultaat van de Acceptatietest ondertekenen vertegenwoordigers van beide partijen een (deel)opleveringsdocument.
----------------	---

Hoofdstuk 10. Operationele fase

10.1. Service Levels

UE 109.	Alle informatie-uitwisseling met de Opdrachtnemer, zowel schriftelijk als mondeling, vindt plaats in de Nederlandse taal, tenzij de Opdrachtgever toestemming verleent om informatie-uitwisseling in een andere taal te laten plaatsvinden.
UE 110.	De Opdrachtnemer benoemt een vast contactpersoon. Deze contactpersoon is het vaste aanspreekpunt voor de Opdrachtgever voor alle vragen en adviezen gerelateerd gedurende de Overeenkomst.
UE 111.	De Opdrachtnemer stelt een medewerker beschikbaar voor migratie- en operationeel overleg
GUE 55.	De Opdrachtnemer gaat akkoord met de Bijlage 9 'SLA & SLA parameters' met inbegrip van de eventuele Nota van Inlichtingen kenbaar gemaakte wijzigingen.
UE 112.	Opdrachtnemer voert om het aantal Incidenten te beperken periodiek preventief Onderhoud uit en geeft, mede op basis van rapportages zie Bijlage 12 'Specificatie Gegevenslevering' gevraagd en ongevraagd minimaal de volgende adviezen: - Indien uit de rapportage blijkt dat de Oplossing te veel (grotere storingsgevoeligheid) of juist te weinig (een te dure Oplossing) gebruikt wordt zal Opdrachtnemer voorstellen om de betreffende Oplossing te vervangen door een andere Oplossing die beter gedimensioneerd is op het gebruik. Indien de Opdrachtgever instemt met het verzoek volgt een functionele conversie; - Indien uit de rapportage blijkt dat een bepaald (model) Oplossing teveel Incidenten veroorzaakt waardoor de Opdrachtnemer niet kan voldoen aan de overeengekomen SLA Parameters met betrekking tot beschikbaarheid dient de Opdrachtnemer voor de betreffende Oplossing een Technische Conversie uit te voeren; - Als uit de rapportage blijkt dat een Oplossing niet of nauwelijks wordt gebruikt, kan de Opdrachtgever verzoeken de Oplossing retour te nemen. Deze adviezen zijn niet van invloed op het in Bijlage 9 'SLA & SLA parameters' van de Overeenkomst gestelde over de gevolgen van het niet nakomen van de SLA Parameters.
UE 113.	Het onderhoud en de service worden door Opdrachtnemer uitgevoerd buiten Kantooruren. Incidenteel kan op verzoek hiervan worden afgeweken, in overleg met de Opdrachtgever.

10.1.1. 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.

UE 114.	Bij het constateren van Kwetsbaarheden met een niveau van kritisch (critical) of hoog (high), conform CVSS 3.0, wordt de Opdrachtgever daarover binnen 1 uur door Opdrachtnemer geïnformeerd.
UE 115.	Kwetsbaarheden die leiden tot een Incident worden gekwalificeerd door middel van CVSS 3.1. Op basis van de CVSS 3.1 kwalificaties gelden de volgende Oplostijden voor Opdrachtnemer:

- Kritisch (critical): per direct (binnen vier (4) uren) op te lossen.
- Hoog (high): binnen 1 maand.
- Gemiddeld (medium): binnen 3 maanden.
- Laag (low): binnen 6 maanden.

10.1.2. Beschikbaarheid

PI	Service Level
Beschikbaarheid 7 x 24 x 365	99,8 %

UE 116. De Oplossing voldoet ten minste aan de Beschikbaarheid zoals opgenomen in de tabel Service Level Beschikbaarheid.

10.1.3. 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.

UE 117. 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).

UE 118. Door de Opdrachtgever geautoriseerde contactpersonen dienen gedurende in de Bijlage 9 'SLA & SLA parameters' genoemde openingstijden telefonisch in contact te kunnen treden met de Incidentdesk.

UE 119. Van elk contact met de Incidentdesk, dat leidt tot verdere acties van de Opdrachtnemer, meldt de Opdrachtnemer aan het eind het referentienummer van dit contact per email. Ieder contact met het loket, ook als dit niet leidt tot verdere actie, dient geregistreerd te worden.

UE 120. Alle Incidenten die worden gemeld bij de Incidentdesk worden door Opdrachtnemer geregistreerd. Incidenten die tot verdere actie door Opdrachtnemer leiden worden voorzien van een referentienummer. Opdrachtnemer communiceert referentienummer aan Opdrachtgever.

UE 121. Alle gemelde Incidenten en alle relevante activiteiten, gebeurtenissen en contactmomenten, die tijdens het afhandelen van Incidenten plaatsvinden, worden door de Opdrachtnemer geregistreerd in een incidentregistratiesysteem. Deze informatie betreft onder andere:

- Het referentienummer van de Opdrachtnemer;
- Het referentienummer van de Opdrachtgever;
- De oplossing waarop het Incident betrekking heeft;
- De prioriteit (hoog, midden of laag);
- Een omschrijving van het Incident;
- Het tijdstip waarop het Incident is signaleerd;
- Het tijdstip waarop het Incident is opgelost;
- De status van het Incident;
- De oplossing van het Incident (indien afgesloten);
- De contacttijden:
 - o Datum/tijdstip signaleren of aanmelding (door de Opdrachtgever) en acceptatie (door Opdrachtnemer);
 - o Datum/tijdstip oplossing (door de Opdrachtnemer) en acceptatie (door de Opdrachtgever).

UE 122.	De Incidentdesk dient ook telefonisch bereikbaar te zijn vanuit het buitenland.
UE 123.	In geval van telefonische communicatie dient de Incidentdesk vanuit Nederland bereikbaar te zijn op telefoonnummers tegen binnenlands of gratis tarief (geen internationale nummers, geen betaalde Servicenummers).
UE 124.	Online of middels e-mail verzonden berichten met daarin (informatie)verzoeken of meldingen kunnen 7 x 24 uur naar de Opdrachtnemer worden verzonden. Gedurende openingstijden dient er op Werkdagen binnen 4 uur een terugkoppeling plaats te vinden met een indicatie wanneer antwoord kan worden verwacht. Aan de aan te leveren informatie en de opzet van dergelijke verzoeken en meldingen kan de Opdrachtnemer eisen en voorwaarden stellen.
UE 125.	Geautoriseerde contactpersonen van, of handelend namens de Opdrachtgever dienen 7 dagen per week, 24 uur per dag in contact te kunnen treden met de Incidentdesk.
UE 126.	Medewerkers van de Incidentdesk hebben technisch inhoudelijke kennis van de Oplossing die de Opdrachtnemer levert. De Opdrachtnemer beschikt over een skilled Incidentdesk. Een Helpdesk die inhoudelijke kennis heeft van de Oplossing en techniek.
UE 127.	Bij telefonische aanmelding van een Incident bij de Incidentdesk van de Opdrachtnemer, dient de aanmelder van de Opdrachtgever binnen 30 seconden een medewerker van de Opdrachtnemer aan de lijn te krijgen.
UE 128.	Opdrachtnemer biedt de mogelijkheid altijd (24x7 uur) online via de Portal / beheeromgeving een storing bij de Incidentdesk aan te melden.
UE 129.	Tijdens Kantooruren dienen Incidenten binnen 30 minuten in behandeling genomen te worden.
UE 130.	Opdrachtnemer, verstrekt Opdrachtnemer een transcript en meldt de Opdrachtnemer aan het eind (daarvan) het referentienummer van dit contact. Indien het contact via chat en/of e-mail verloopt zendt de Opdrachtnemer hiertoe een e-mail met het referentienummer in de onderwerp-regel van de e-mail aan de afzender.
UE 131.	Alle Incidenten worden door Opdrachtnemer op basis van de in Bijlage 9 'SLA & SLA parameters' gegeven omschrijving ingedeeld in 1 van de categorieën hoog, midden of laag.
UE 132.	Opdrachtnemer dient minimaal de SLA & SLA Parameters uit Bijlage 9 'SLA & SLA parameters' actief met een beheersysteem te bewaken, Incidenten te signaleren en per direct vast te leggen in het incidentregistratiesysteem.
UE 133.	Indien er geen Incident is gesignaleerd door middel van een beheersysteem, gaat de Oplostijd van een Incident in op het moment dat het Incident is aangemeld.
UE 134.	De Opdrachtgever kent aan elk Incident een prioriteit toe. Opdrachtnemer kent tevens een prioriteit toe. Beide prioriteiten worden in het incidentregistratiesysteem opgeslagen. Indien de toegekende prioriteit door Opdrachtnemer lager is dan de toegekende prioriteit door de Opdrachtgever wordt de contractmanager van de Opdrachtgever daar direct via e-mail van op de hoogte gesteld
UE 135.	Een Incident is pas afgesloten als de oplossing door de Opdrachtgever is geaccepteerd. De Opdrachtgever moet binnen 60 minuten na afmelding door de Opdrachtnemer

	aangeven of hij de afmelding accepteert. Indien de Opdrachtgever niet reageert binnen deze termijn, wordt het Incident als afgesloten beschouwd.
UE 136.	Indien de Opdrachtgever niet -tijdig- heeft gereageerd of het Incident is onterecht gesloten, heeft de Opdrachtgever 3 Werkdagen de tijd het betreffende Incident te heropenen.
UE 137.	Na een telefonische melding van een Incident bij de Opdrachtnemer vangt direct de Oplostijd voor afhandeling van Incidenten aan.
UE 138.	Na het verhelpen van het Incident kan er op verzoek van de Opdrachtgever, in het bijzijn van een medewerker van de Opdrachtgever een test worden uitgevoerd om vast te stellen dat de Oplossing goed werkt.
UE 139.	Bij vertrek nadat het Incident is verholpen dient de technicus van de Opdrachtnemer zich af te melden en desgewenst een afmeldformulier te tekenen bij de lokale C contactpersoon van de Opdrachtgever of diens plaatsvervanger.
UE 140.	Opdrachtnemer moet in staat zijn bij gemelde Incidenten binnen de gestelde reparatietijden de gemelde Incident fysiek te verhelpen. Opdrachtnemer wordt geacht binnen 30 minuten (reactietijd) aan te vangen met herstel door middel van instructie aan medewerkers van de Opdrachtgever, remote beheer, het plannen van een bezoek op locatie.
UE 141.	Incidenten die optreden bij de Opdrachtnemer en die een negatieve impact (kunnen) hebben op de Oplossing bij de Opdrachtgever dienen zo spoedig mogelijk aan de Opdrachtgever gemeld te worden.
UE 142.	Na aanmelden van een Incident dient de Opdrachtnemer binnen 30 minuten met een eerste reactie te komen. Bij deze terugkoppeling dient hij aan te geven of de Opdrachtgever nog aanvullende informatie moet aanleveren.
UE 143.	De meldperiode voor Incidenten moet 7 * 24 uur zijn voor hoge prioriteit Incidenten.
UE 144.	Voor midden Incidenten moet de Oplossing gedurende 7.00 tot 22.00 uitgevoerd worden.
UE 145.	Midden Incidenten moeten voor 90% van de Incidenten binnen 8 uur zijn opgelost en voor 100% van deze Incidenten moet de Oplostijd korter zijn dan 1 Werkdag.
UE 146.	Indien een midden Incident niet binnen 1 Werkdag is opgelost, dan dient deze de prioriteit 'hoog' te krijgen.
UE 147.	De Oplostijdtijd voor hoge prioriteit Incidenten moet in 90% van de Incidenten korter dan 4 uren zijn en binnen 100% van de Incidenten binnen 8 uur.
UE 148.	De Oplostijdtijd voor hoge prioriteit Incidenten moet in 90% van de Incidenten korter dan 4 uren zijn en binnen 100% van de Incidenten binnen 8 uur.
UE 149.	Tijdens afhandeling van een Incident verstrekt de Incidentdesk statusinformatie aan een door de Opdrachtgever aangewezen contactpersoon in de volgende frequenties: - Prioriteit hoog: 1 keer per 1 uur; - Prioriteit midden: 1 keer per 4 uur op werkdagen.
UE 150.	Alle gemelde Incidenten en alle relevante activiteiten, gebeurtenissen en contactmomenten, die tijdens het afhandelen van Incidenten plaatsvinden, worden door

	de Opdrachtnemer geregistreerd in een incidentregistratiesysteem. Minimaal moeten de volgende items geregistreerd worden: - Ticket-id (referentienummer van de Opdrachtnemer); - Ticket-id (referentienummer van de Opdrachtgever indien beschikbaar); - Identificatie van de Oplossing; - Prioriteit; - Naam van de melder/contactpersoon Opdrachtgever, incl. contactinformatie - Omschrijving; - Work-around; - Definitieve oplossing/actie; - Contacttijden: - o Datum/tijdstip aanmelding (door de Opdrachtgever) en acceptatie (door Opdrachtnemer); - o Datum/tijdstip oplossing (door Opdrachtnemer) en acceptatie (door de Opdrachtgever).
UE 151.	Indien een Incident is opgelost met een work-around (afwijkend van de standaarduitvoering van de Oplossing), dan dient de Opdrachtnemer daarna onverwijld het oorspronkelijke Incident te verhelpen met een structurele oplossing.
UE 152.	Repeterende Incidenten dienen als Probleem te worden geclassificeerd op basis van de volgende regels: - Als een Incident met prioriteit hoog ≥ 2 keer per jaar voorkomt; - Als een Incident met prioriteit midden ≥ 4 keer per kwartaal voorkomt. De Opdrachtnemer dient binnen een week een verbeterplan op te stellen en te laten accorderen door de Opdrachtgever. In het verbeterplan worden concrete acties en planningen (mensen en middelen) genoemd.
UE 153.	De Opdrachtgever ontvangt realtime status updates van Incidenten van de Oplossing middels e-mail.
UE 154.	De Opdrachtgever kan zelf de e-mailadressen instellen waarop de realtime incidentmeldingen worden ontvangen.
UE 155.	De Opdrachtgever kan zelf instellen van welke in de Oplossing er een Incident e-mailmeldingen worden verzonden per e-mail.
UE 156.	De Opdrachtgever kan zelf instellen van welke categorie Incident e-mailnotificaties worden verzonden.
GUE 56.	De Opdrachtnemer gaat akkoord met alle informatie die over beschikbaarheid is opgenomen in de Bijlage 9 'SLA & SLA parameters', waaronder de in die Bijlage opgenomen methode van berekening van de beschikbaarheidpercentages en de geëiste beschikbaarheidpercentages zelf.

10.1.4. Verbeterplan

UE 157.	Indien de Oplossing gedurende een periode van 3 maanden niet voldoet aan 1 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 10 Werkdagen na verzoek van de Opdrachtgever opgeleverd. Toepassing van het Verbeterplan laat de overige rechten van Opdrachtgever onverlet, waaronder die op schadevergoeding.
---------	---

10.1.5. Rapportage

UE 158.	Opdrachtnemer levert maandelijks een Service Level rapportage op aan de Opdrachtgever met minimaal de volgende inhoud: - Helpdesk: Reactietijden per Prio; - Beschikbaarheid; - KPI incidentmanagement; - KPI Helpdesk.
UE 159.	Geautoriseerde Gebruikers kunnen in het online rapportage-informatiesysteem door middel van queries zelf informatieoverzichten genereren.
UE 160.	Afwijkende frequentie en aanvullende rapportage-items kunnen afzonderlijk (tegen overeen te komen meerprijs) door de Opdrachtgever worden afgenomen.
UE 161.	Afwijkende rapportages, rapportagefrequenties, of aanvullende rapportage-items kunnen afzonderlijk (tegen nader te bepalen meerprijs) overeengekomen worden.
UE 162.	De Opdrachtnemer levert Gegevens aan in CSV-formaat en stelt deze beschikbaar via een SFTP-server op een nader te bepalen locatie.
UE 163.	De Opdrachtnemer dient de rapportages en Brongegevens gedurende de Overeenkomst vermeerderd met 1 jaar te bewaren. Gedurende deze periode dienen de rapportages en Brongegevens opvraagbaar te zijn.
UE 164.	De database waaruit de Opdrachtnemer de rapportages beschikbaar stelt wordt minimaal elke 4 uur geupdated.
UE 165.	De Opdrachtnemer stelt een rapportagetool beschikbaar in de Portal.
UE 166.	De Opdrachtgever kan zelf selecties en representaties van de rapportage-items realiseren en in een algemeen elektronisch formaat downloaden en opslaan voor verdere bewerking.
UE 167.	Brongegevens van de rapportages dienen door de Opdrachtnemer automatisch elektronisch aangeleverd te worden. Dit moet via push technologie kunnen op het koppelvlak in CSV- of Excel-formaat. De indeling van dit CSV- of Excel-formaat dient in onderling overleg met de Opdrachtgever overeengekomen te worden.
UE 168.	Elke inbound Call dient in de rapportages herleidbaar te zijn, inclusief de gemaakte keuzes van het moment van aanbieden aan de Opdrachtnemer tot aan de Eindbestemming.
UE 169.	De Rapportages betreffende 14xx-nummers worden geleverd door de Opdrachtnemer conform hetgeen bepaald is in Bijlage 12 'Specificatie gegevenslevering'.
UE 170.	De Opdrachtgever ontvangt gedurende de Overeenkomst elke Kalendermaand van de Opdrachtnemer een rapportage over de geleverde Prestatie van de Oplossing.

10.2. Toekomstige ontwikkeling

UE 171.	De toekomstige ontwikkelingen zoals de transitie van off-premise naar een cloudgebaseerde CCAAS-omgeving dient door de Opdrachtnemer te worden ondersteund.
---------	---

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 een Oplossing 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 boekhoudstelsel 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 172.	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 173.	Kosten die voortkomen uit het realiseren van de koppeling voor elektronische berichten uitwisseling met de Rijksoverheid worden gedragen door de Opdrachtnemer.
UE 174.	De Opdrachtnemer accepteert dat er gedurende de looptijd van de Overeenkomst nieuwe-/verbeterde versies van de programmatuur van het leveranciersportaal in gebruik genomen kunnen worden.
UE 175.	De Opdrachtnemer verstuurt maandelijks een factuur en vermeldt op de factuur minimaal de volgende Gegevens: - Inkoopordernummer (als referentie op elke pakbon en factuur aan Opdrachtgever) Zonder dit Inkoopordernummer kan Opdrachtgever de levering of de factuur weigeren. - Contractnummer; - Order/factuurnummer (Opdrachtnemer); - Identificatie; - Korte omschrijving; - Eenmalige kosten (indien van toepassing), inclusief en exclusief BTW; - Periodieke kosten (indien van toepassing), inclusief en exclusief BTW; - Factuurperiode;

	- Totale kosten exclusief BTW; - Totale kosten inclusief BTW; - Gehanteerde BTW-tarief; - Subtotalen per afdeling, kostenplaats en dergelijke (indien gewenst en van toepassing); - Overige wettelijke bepalingen die gelden voor een factuur
UE 176.	De Opdrachtnemer dient voorafgaand aan de 1e factuur eenmalig een pro forma factuur op te stellen, waarin alle geëiste factuurgegevens, en alle factureerbare items met bijbehorende beschrijving, inclusief de bijbehorende Prijzen, staan vermeld. Deze pro forma factuur dient ter goedkeuring te worden aangeboden aan Opdrachtgever. Pas na goedkeuring van de pro forma factuur kan de daadwerkelijke facturering van de geleverde Oplossing van start gaan.
UE 177.	De Opdrachtnemer brengt binnen 5 Werkdagen na ontvangst van een offerteaanvraag een offerte uit.
UE 178.	De uitgebrachte Offertes dienen een geldigheidsduur te hebben van minimaal 60 dagen na datum ontvangst.

10.4. Kaders voor (re)transitie

10.4.1. Inleiding

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

10.4.2. Documentatie en Gegevens(overdracht)

UE 179.	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, 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 dit hoofdstuk leidend zijn.
UE 180.	Opdrachtnemer verleent volledige medewerking aan de Retransitie en verstrekt daarbij alle relevante Documentatie en Gegevens aan Opdrachtgever c.q. opvolgende Opdrachtnemer verstrekken.
UE 181.	Aanlevering van de Documentatie en Gegevens gebeurt via een beveiligde verbinding. De Opdrachtgever draagt zorg voor deze verbinding.
UE 182.	Na ontvangst van bevestiging dat de Documentatie en Gegevens in goede orde zijn ontvangen, zal de Opdrachtnemer overgaan tot vernietiging van onder hem bevindende Gegevens, waarbij de vernietigingshandelingen gedocumenteerd zullen worden.

UE 183.	Opdrachtnemer zorgt dat binnen 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 184.	De rapportage van de vernietigingshandelingen is in overeenstemming met wettelijke vereisten ter zake en wordt door Opdrachtnemer aan Opdrachtgever ter hand gesteld.
UE 185.	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.
UE 186.	Naar de Opdrachtgever herleidbare domeinnamen en URL's worden onbeschikbaar gemaakt op het internet en domeinnamen worden –zo mogelijk- overgedragen aan de Opdrachtgever. 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.

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 187.	Bij overgang naar een nieuwe Opdrachtnemer moet de Prestatie gedurende de Retransitiefase (circa 6 maanden) tegen gelijkblijvende condities (naar rato), voor Opdrachtgever beschikbaar blijven.
UE 188.	Opdrachtnemer houdt voldoende gekwalificeerd personeel beschikbaar voor de Retransitie.
UE 189.	Opdrachtnemer verleent medewerking aan een Audit betreffende de inhoud en de kwaliteit van de informatie die Opdrachtnemer in het kader van Retransitie beheerd.
UE 190.	Opdrachtnemer dient inzage te geven in de gebruikte middelen en processen tijdens de periode van Retransitie