



Belastingdienst

BIJLAGE A. Specificatie van de opdracht

Behorende bij : Beschrijvend document Online security awareness game

Versie : 1.0 Definitief
Kenmerk : IUC21-004
Datum : 21 mei 2021

INHOUDSOPGAVE

Hoofdstuk 1.	Doel van dit document	3
Hoofdstuk 2.	Algemene eisen	4
2.1.	Verplichtingen belastingen, milieubescherming, arbeidsvoorwaarden	4
2.2.	Business Etiquette.....	4
2.3.	Juridische kaders	4
Hoofdstuk 3.	De OSAG Dienst.....	5
3.1.	Opbouw van de OSAG dienst.....	5
3.1.1.	Kennisoverdracht en spelelement.....	6
3.1.2.	Vorbereiding van een OSAG.....	8
3.1.3.	Uitvoering van een OSAG	10
3.1.4.	Rapportage	11
3.1.5.	Additionele diensten	12
3.2.	Implementatie fase	12
3.2.1.	Initiële Release	12
3.2.2.	Instructie	13
3.2.3.	Plan van Aanpak	14
3.3.	Operationele fase	16
3.3.1.	Hosting, Beheer en Onderhoud	16
3.3.2.	Support	16
3.3.3.	Releasemanagement	18
3.4.	Retransitie	18
3.5.	IV kaders	19
3.5.1.	Logisch Toegangsbeheer	23
3.5.2.	Identity Management	24
3.5.3.	Koppelingen	25
Hoofdstuk 4.	Financiële afspraken	26
4.1.	Tariefherziening	26
4.2.	Facturatievoorwaarden	26
4.3.	Elektronisch factureren (EBF) – e-factureren	27

Hoofdstuk 1. Doel van dit document

Dit document beschrijft de Specificaties (bestaande uit Gunningeisen, Uitvoeringseisen en Wensen) ten aanzien van de Prestatie die de Opdrachtgever stelt in het kader van de Europese Aanbesteding Online security awareness game IUC21-004 Dit document maakt integraal onderdeel uit van het Beschrijvend Document.

De Opdrachtgever heeft geen voorkeur voor bepaalde ondernemingen, noch voor bepaalde merken, types, fabricaten, herkomst en dergelijke. Als er wordt gerefereerd aan bepaalde fabricaten, merken, typen, specifieke standaarden en dergelijke, dan dient dit te worden gelezen met de toevoeging "of daaraan gelijkwaardig".

Aan alle eisen (Gunningeisen en Uitvoeringseisen) moet worden voldaan. Het niet voldoen aan een eis betekent uitsluiting van verdere beoordeling en wordt de Inschrijving terzijde gelegd (knock-out criterium).

Voor alle eisen geldt dat deze tijdens de looptijd van de Overeenkomst door de Opdrachtgever beoordeeld kunnen worden op hun conformiteit. Ingeval de opdracht niet, niet geheel of ten dele wordt uitgevoerd volgens de eisen, wordt voor de mogelijke gevolgen hiervan verwezen naar wat hierover gesteld wordt in Bijlage 2. Concept Overeenkomst.

De Wensen worden inhoudelijk beoordeeld door de beoordelingscommissie.

Uitvoeringseisen, Gunningeisen en Wensen worden als volgt weergegeven in dit document Bijlage A. Specificatie van de opdracht.

GUE	Gunningeisen Aan een Gunningseis moet reeds ten tijde van de Inschrijving worden voldaan. Het niet voldoen aan een Gunningseis leidt tot uitsluiting van deze aanbestedingsprocedure, en is dus een knock-out criterium.
UE	Uitvoeringseisen Voorwaarden waar de Opdrachtnemer zich bij de uitvoering van de opdracht aan dient te houden zijn Uitvoeringseisen. Door het indienen van een Inschrijving gaat u onvoorwaardelijk akkoord met het voldoen aan de Uitvoeringseisen gedurende de uitvoering van de Overeenkomst.
W	Wensen Wensen maken onderdeel uit van gunningscriteria op basis waarvan de Economisch Meest voordelige Inschrijving (EMVI) wordt bepaald. De scores op de Wensen bepalen de hoogte van het onderdeel kwaliteit in de prijs/kwaliteitverhouding van de Inschrijving.

Hoofdstuk 2. Algemene eisen

In dit hoofdstuk zijn algemene Uitvoeringseisen opgenomen. De bepalingen in dit hoofdstuk hebben allemaal specifiek betrekking op de uitvoeringsperiode van de aanbestede opdracht, echter ook in de andere hoofdstukken komen Uitvoeringseisen voor.

2.1. Verplichtingen belastingen, milieubescherming, arbeidsvoorwaarden

UE 1	Opdrachtnemer dient bij de uitvoering van de Overeenkomst rekening te houden met de verplichtingen uit hoofde van de bepalingen inzake de arbeidsbescherming en de arbeidsvoorwaarden die gelden in het land waar de opdracht wordt uitgevoerd, zoals bedoeld in artikel 2.81 lid 2 Aw2012. Kennis omtrent die belastingen en milieubescherming, arbeidsvoorwaarden en arbeidsbescherming kunnen Opdrachtnemers, voor zover het gaat om uitvoering in Nederland, verkrijgen bij: • de Belastingdienst, www.belastingdienst.nl • het Ministerie van Infrastructuur en Milieu, www.rijksoverheid.nl/ministeries/ienm • het Ministerie van Sociale Zaken en Werkgelegenheid www.rijksoverheid.nl/ministeries/szw
------	--

2.2. Business Etiquette

Specifiek voor het zakendoen met marktpartijen heeft de Opdrachtgever de [Business Etiquette](#) (Bijlage 3) opgesteld. Hierin kunnen de externe partijen lezen wat wel en niet toegestaan is in de contacten met medewerkers van de Aanbestedende dienst.

UE 2	Opdrachtnemer conformeert zich aan de Business Etiquette zoals opgenomen in Bijlage 3.
------	--

2.3. Juridische kaders

De Concept Overeenkomst (Bijlage 2), inclusief Bijlagen kan, alvorens deze door Partijen worden ondertekend, door de Opdrachtgever worden gewijzigd en nader uitgewerkt, mede naar aanleiding van de gedane opmerkingen en tekstsuggesties. Deze wijzigingen zullen per Nota van Inlichtingen kenbaar worden gemaakt.

UE 3	Inschrijver gaat akkoord met de bijgevoegde Concept Overeenkomst (Bijlage 2), inclusief Bijlagen met inbegrip van de eventuele per Nota van Inlichtingen kenbaar gemaakte wijzigingen.
------	--

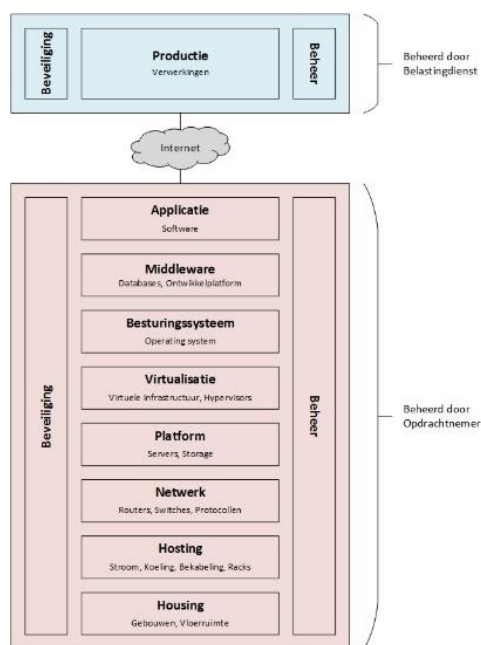
Hoofdstuk 3. De OSAG Dienst

In de volgende paragrafen worden de Specificaties met betrekking tot de OSAG Dienst beschreven. De OSAG Dienst is hierbij op een manier geconfigureerd/ingericht waarmee (gelijktijdig) aan alle eisen voldaan wordt. Bij de beantwoording dient er consequent van één en dezelfde configuratie/inrichting te worden uitgegaan.

GUE 1	Bij de beantwoording van de Gunningeisen, Uitvoeringseisen en Wensen wordt er door de Inschrijver consequent van één en dezelfde configuratie/inrichting van de OSAG Dienst uitgegaan.
-------	--

3.1. Opbouw van de OSAG dienst

De Online security awareness game wordt aanbesteed als een SaaS-dienst (Software-as-a-Service dienst). Ten aanzien van de SaaS-dienst is de verdeling in verantwoordelijkheidsgebieden tussen Opdrachtnemer en Opdrachtgever opgenomen in de onderstaande figuur:



De OSAG Dienst dient logisch uit één geheel te bestaan en te allen tijde is de Opdrachtnemer verantwoordelijk voor alle Specificaties. Dit laat onverlet dat de Opdrachtnemer delen van de OSAG Dienst kan en mag uitbesteden aan Derden.

Eisen aan de OSAG Dienst:

GUE 2	De OSAG Dienst bestaat uit één integraal werkende oplossing Deze integrale werkende oplossing kan uit meerdere (deel)oplossingen bestaan. Als de OSAG Dienst bestaat uit (deel)oplossingen dan is de integratie van deze (deel)oplossingen de verantwoordelijkheid van de Opdrachtnemer.
-------	--

	De Opdrachtnemer garandeert dat, bij gebruik van (deel)oplossingen van eventuele onderaannemers, ook deze partijen en hun (deel)oplossingen aan Specificaties (blijven) voldoen.
GUE 3	De OSAG Dienst dient een 'zero-client footprint' te hebben. Dat wil zeggen er is, naast een webbrowser, geen additionele software, browser-plug-in of additionele hardware nodig op de gebruikersapparaten om alle functionaliteiten van de OSAG Dienst te kunnen benaderen.
GUE 4	De OSAG Dienst is apparaat-onafhankelijk te gebruiken op alle gangbare gebruikersapparaten die over een webbrowser beschikken. De volledige functionaliteit van de OSAG Dienst wordt ondersteund door de meest gangbare webbrowsers. Op het moment van publicatie zijn dat: Google Chrome, Microsoft Edge, Mozilla Firefox en Apple Safari. De OSAG Dienst ondersteunt minimaal de huidige versie en de voorgaande versie van de webbrowsers welke nog actief worden ondersteund door de leverancier van de webbrowser.

Het is noodzakelijk om zicht te hebben op de Gebruikers. Opdrachtnemer is gedurende de opdracht verantwoordelijk voor alle user accounts en bijbehorende rechten.

De opdrachtgever levert het organisatiemodel van de Belastingdienst op aan de opdrachtnemer. Wanneer de Deelnemer zich registreert in de Online security awareness game, kiest de Deelnemer het organisatieonderdeel waar hij/zij werkzaam is.

GUE 5	De OSAG Dienst moet Gegevens kunnen importeren vanuit de administratie van de Opdrachtgever t.b.v. het gebruikersbeheer en rapportages in de OSAG Dienst. Afhankelijk van de door Opdrachtgever gekozen importvorm schrijft Opdrachtgever daarbij voor: - op welke wijze de gegevensuitwisseling plaatsvindt; - middels handmatig importfunctie binnen de OSAG Dienst die vanuit een Belastingdienstwerkplek door een Belastingdienstmedewerker kan worden uitgevoerd; - middels het opnemen van de Gegevens in een tabel in de OSAG Dienst (welke gevuld wordt zonder import functie). - wanneer de gegevensimport plaatsvindt.
-------	---

3.1.1. Kennisoverdracht en spelelement

De OSAG Dienst dient kennis over te brengen naar de Deelnemers. Om een serieus spel leuk en onderhoudend te maken moet het ten minste:

1. aansluiten bij de beleavingswereld van de Deelnemers;
2. gebruiksvriendelijk zijn;

3. uitdagend zijn waarbij de inhoud (in de vorm van Content) vertaald wordt naar een inspirerende omgeving;
4. voorzien in een spelelement doormiddel van bijvoorbeeld een vraag-antwoord-actie omgeving.

GUE 6	De OSAG Dienst dient aantoonbaar kennis over te brengen naar de Deelnemers en tegelijkertijd te voorzien in een of meerdere spelelementen.
W 1	Spelbeleving: Om een serieus spel leuk en onderhoudend te maken vindt de Opdrachtgever het belangrijk dat de OSAG Dienst uitnodigt tot gebruik en dat de spelbeleving optimaal is. Hierbij dient de OSAG Dienst: 1. gebruiksvriendelijk te zijn, waarbij ten minste aandacht is voor - o logische opbouw van de schermen (overzichtelijk, alle benodigde informatie op een scherm, waarbij gebruik gemaakt is van bijvoorbeeld adaptive of responsive design); - o de OSAG Dienst intuïtief is, en schermen eenduidig zijn; - o doelgericht en behulpzaam (zoals beperkt aantal invoervelden en muisklikken, geen onnodige pop-ups en acceptabele performance/snelheid). 2. De inhoud te vertalen naar een omgeving met spelelementen welke aansluit bij de Deelnemers, waarbij: - o de OSAG plaats vindt in een inspirerende omgeving (bijvoorbeeld een spannend verhaal) welke aansluit bij de belevingswereld van de Deelnemers, - o de Deelnemers in deze omgeving opdrachten moeten uitvoeren (bijvoorbeeld vraag-antwoord-actie opdracht). - o de Deelnemers hierbij op basis van de behaalde score beloningen kunnen verdienen (bijvoorbeeld niveau één, twee, drie, vier of rang in termen van bijvoorbeeld rookie, practitioner, jedi, master of bijvoorbeeld brons, zilver, goud en platina). - o de Deelnemers in een flow komen waardoor de OSAG uitdagend is, maar ook weer niet zo moeilijk dat Deelnemers het opgeven (bijvoorbeeld met hintkaartjes, aanwijzingen of een nieuw deel van de theorie). 3. uitdagend te zijn voor de Deelnemers, waarbij de betrokkenheid en motivatie van de Deelnemers wordt vergroot (bijvoorbeeld door structuur of extra beloningen te bieden wat tot gevolg heeft dat de leerprestaties worden verbeterd). Vraag: Geef aan op welke manier uw OSAG Dienst voorziet in bovenstaande behoefte.

U dient via schermafbeeldingen en bijbehorende toelichtingen de OSAG Dienst hieromtrent te presenteren (max. 10 pag. A4). Aanvullend mag dit met een korte video impressie (in een voor Windows Media Player leesbaar bestandsformaat) van maximaal 15 minuten worden ondersteund. Houd u hierbij rekening met de met voorwaarden welke TenderNed stelt ten aanzien van de up te loaden bestanden. Een mediabestand kan middels een Zip file in TenderNed geüpload te worden (de maximale grote van het bestand bedraagt 2 GB).

Beoordeling:

De spelbeleving wordt beoordeeld op de volgende aspecten:

1. Gebruiksvriendelijkheid;
2. Omgeving met spelelementen welke aansluiten bij de Deelnemers;
3. Uitdagend voor de Deelnemers,

Deze Wens wordt beoordeeld op basis van de mate waarin het antwoord voldoet aan de verwachtingen van de Opdrachtgever.

Voor deze Wens zijn in totaal maximaal 55 punten te behalen.

Ten aanzien van deze Wens geldt dat er een minimale score van 44 punten (beoordeling "Ruim voldoende" 80% van 55 punten) behaald moet worden. Deze minimale score geldt derhalve als een minimale eis/knock-out criterium. Bij het niet behalen van deze score zal de Inschrijving terzijde worden gelegd.

3.1.2. Voorbereiding van een OSAG

De OSAG Dienst wordt als SaaS-dienst aangeboden door de Opdrachtnemer. Opdrachtgever stelt (in overleg met de Opdrachtnemer) de kennisthema's en leerdoelen vast. De Opdrachtnemer is verantwoordelijk voor het samenstellen van de spelrondes met kennisthema's en het creëren van de Content alsmede het publiceren (plaatsen/beschikbaar stellen/inladen) van de Content in de OSAG Dienst.

De Content dient te allen tijde in lijn te zijn met geldende wet- en regelgeving. Hierbij wordt ook rekening gehouden met de Baseline Informatiebeveiliging Overheid (BIO). Alvorens Content daadwerkelijk door de Opdrachtnemer aan de Deelnemers beschikbaar wordt gesteld dient deze geaccordeerd te worden door de Opdrachtgever. Aannee is dat gemiddeld per kennisthema en/of spelronde 80% van de Content organisatieonafhankelijk en daarmee dus generiek is, en 20% organisatie specifiek voor de Opdrachtgever (aan deze aannames kunnen geen rechten worden ontleend).

Opdrachtgever heeft op dit moment het beeld dat een Online security awareness game uit ten minste vier verschillende spelrondes bestaat. De eerste spelronde moet de Deelnemer voorzien in een basis kennisniveau rondom het doordacht omgaan met informatie(veiligheid). Streven is dat de maximale duur van de eerste spelronde rond de 45 minuten ligt. Spelronde twee bouwt voort op het geleerde in spelronde één en is daarmee een verdieplings- en verbredingslag. Op basis van voortschrijdend inzicht zal spelronde twee focussen op privacy en AVG. Het streven voor de maximale spelduur van ronde twee is circa 30 minuten. Spelrondes één en

twee hebben een statisch karakter. De verwachting is dat jaarlijks kleine aanpassingen op bestaande inhoud noodzakelijk zijn. De daaropvolgende spelrondes (drie en vier) zijn kennisthema en/of periode afhankelijk. Dit wil zeggen dat de inhoud over het jaar kan variëren op basis van risico's, maatregelen of bijvoorbeeld wet- en regelgeving. Het streven voor de maximale speluur van ronde drie en vier is maximaal 15 minuten per speelronde.

GUE 7	De OSAG Dienst ondersteunt minimaal vier spelrondes.
UE 4	De overdracht van kennis wordt ondersteund door spelrondes, waarbij een spelronde kan bestaan uit één of meerdere kennisthema's.
UE 5	Spelronde één behandelt minimaal, maar is niet gelimiteerd tot de volgende kennisthema's: • alles over bewust en veilig werken binnen de kantooromuren; • alles over verantwoord thuis en onderweg werken; • alles over digitale bedreigingen herkennen en vermijden; • verantwoord omgaan met persoonsgegevens; • verantwoord werken in de cloud, omgaan met sociale media en andere tools.
UE 6	Spelronde twee bouwt voort op het geleerde in spelronde één en is daarmee een verdieplings- en verbredingslag. Op basis van voortschrijdend inzicht zal spelronde twee focussen op privacy en AVG.
UE 7	Spelrondes drie en vier hebben een flexibel karakter. De opdrachtnemer moet rekening houden dat spelrondes drie en vier jaarlijks inhoudelijk compleet wijzigen op basis van actuele kennisthema's.
UE 8	Alle Content in de OSAG Dienst, inclusief bijvoorbeeld menu-items of hulp velden, zijn in het Nederlands op taalniveau B1 beschikbaar.
UE 9	Bestaand standaard Kennismateriaal kan binnen de OSAG Dienst worden aangepast naar de situatie/inzicht van de Opdrachtgever.
UE 10	Opdrachtnemer is ervoor verantwoordelijk dat de Content te allen tijde in lijn is met geldende wet- en regelgeving. Hierbij wordt ook rekening gehouden met de vigerende Baseline Informatiebeveiliging Overheid (BIO).
UE 11	De Opdrachtnemer is verantwoordelijke voor het creëren, samenstellen en in de OSAG Dienst publiceren/beschikbaar stellen van de Content op basis van de door Opdrachtgever vastgestelde kennisthema's en leerdoelen. Opdrachtgever kan, indien gewenst, zelf input ten behoeve van (nieuwe) Content aanleveren.
UE 12	Content kan zowel tekstueel als visueel zijn en kan zowel audio als (hyper)links bevatten.
UE 13	Content aanpassingen i.v.m. onjuistheden of spelfouten worden binnen één (1) Werkdag door de Opdrachtnemer opgelost.
UE 14	Aanpassen of toevoegen van één of enkele items binnen de Content worden binnen twee (2) Werkdagen door de Opdrachtnemer gerealiseerd.

UE 15	Beschikbaar stellen van een geheel nieuwe spelronde, nadat de kennisthema's en alle Content is goedgekeurd door de Opdrachtgever, is door de Opdrachtnemer binnen zes (6) Werkdagen gerealiseerd.
-------	---

3.1.3. Uitvoering van een OSAG

Opdrachtgever verwacht dat de OSAG Dienst gebruiksvriendelijk is waarbij een beperkte, efficiënte ondersteuning van Spelondersteuners noodzakelijk is.

Opdrachtgever verwacht echter wel dat, gelet op de omvang van het deelnemersveld, er enige ondersteuning van Spelondersteuners nodig is.

Opdrachtgever ziet de programma-organisatie als volgt voor zich:

- op centraal niveau wordt een interne spelleider (van Opdrachtgever) aangewezen;
- per organisatieonderdeel kunnen vervolgens een spelcoördinatoren worden aangewezen waarbij afhankelijk van de omvang van het organisatieonderdeel ook per afdeling een (sub)spelcoördinator kan worden aangewezen.

Onderdeel van de opdracht is het instrueren van de Spelondersteuners.

Opdrachtgever beschikt over een eigen supportdesk voor technische storingen. Voor ondersteuning kan een Deelnemer terecht bij de aangewezen Spelondersteuner. Dit betekent dat de Opdrachtnemer geen direct contact heeft met de Deelnemer maar dat dit verloopt via de supportorganisatie en/of de aangewezen Spelondersteuner van Opdrachtgever.

GUE 8	De OSAG Dienst beschikt over een programma-organisatie waarbij ten minste op centraal niveau een interne Spelondersteuner (spelleider) kan worden aangewezen.
UE 16	De Opdrachtnemer verzorgt voor de Spelondersteuners de instructies en het benodigde instructiemateriaal zodat zij voldoende kennis hebben om in de OSAG Dienst zelfstandig hun werkzaamheden kunnen uitvoeren.
W 2	Programma-organisatie: De OSAG dienst beschikt over een programma-organisatie waarbij op een efficiënte wijze op meerdere niveaus ondersteuning kan worden geboden door Spelondersteuners. Vraag: Beschrijf in maximaal twee (2) pagina's A4 welke programma-organisatie, welke aansluit bij bovenstaande, u voorstelt. Beoordeling: De programma-organisatie wordt beoordeeld op de volgende aspecten: 1. Aantal ondersteunde organisatieniveaus; 2. Mogelijkheden om rollen, verantwoordelijkheden en informatie-/rapportagemogelijkheden per organisatieniveau in te stellen.

	3. Verwachte benodigde inzet van de Spelondersteuners (incl. instructie); Deze Wens wordt beoordeeld op basis van de mate waarin het antwoord voldoet aan de verwachtingen van de Opdrachtgever. Voor deze Wens zijn in totaal maximaal 25 punten te behalen.
GUE 9	Binnen de OSAG Dienst wordt een score gedurende een spelronde opgebouwd. De minimale te behalen score is per spelronde te definiëren.
GUE 10	Een spelronde kan vergeleken worden met een bepaald kennisniveau. Na het behalen van een spelronde kan hier een termijn aan gekoppeld worden (of over gerapporteerd worden) zodat de Deelnemer verzocht kan worden deze spelrondes na bijvoorbeeld één, twee, of drie jaar te herhalen.
GUE 11	Indien een Deelnemer een kennisthema of specifieke vraag onvoldoende, onvolledig of "fout" heeft beantwoord moet de Deelnemer worden voorzien van extra informatie waarom zijn antwoord onjuist is.
UE 17	Na het succesvol afronden (op basis van score) van een spelronde wordt de Deelnemer voorzien van een (digitaal) certificaat van deelname (in, bij voorkeur, Pdf-formaat) welke hij kan downloaden of (elektronisch) krijgt toegezonden.

3.1.4. Rapportage

De groei van het kennisniveau van Deelnemers (niet per individuele Deelnemer) wordt meerjarig gevolgd door middel van de (management)informatie en rapportages over de diverse spelrondes. De OSAG Dienst voorziet in de benodigde (management)informatie en rapportage. Opdrachtnemer is verantwoordelijk voor het inrichten/configureren van de door Opdrachtgever gewenste standaard rapportages zodat deze op elk gewenst moment door de geautoriseerde Gebruikers (online) kunnen worden opgevraagd c.q. ingezien.

Op basis van de in de OSAG Dienst ingerichte organisatie structuur wordt verwacht van de Opdrachtgever dat op organisatie en -onderdeelniveau gerapporteerd kan worden. Denk aan rapportages zoals:

- aantal geregistreerde Deelnemers
- behaalde scores
- aantal en percentage gestarte, lopende en afgeronde spelrondes

Nadere uitwerking zal in nauwe samenwerking met de opdrachtnemer plaats vinden.

UE 18	De OSAG Dienst biedt (management)informatie en rapportage over spelgedrag en spelverloop uitgesplitst naar (1) gehele organisatie (2) organisatieonderdeel. Deze informatie bevat minimaal: • aantal geregistreerde Deelnemers; • behaalde scores; • aantal en percentage gestarte, lopende en afgeronde spelrondes.
-------	---

UE 19	Opdrachtnemer is verantwoordelijk voor het inrichten/configureren en beschikbaar stellen van de door Opdrachtgever gewenste standaard rapportages zodat deze, op elk gewenst moment, door de geautoriseerde Spelondersteuners (online) kunnen worden opgevraagd c.q. ingezien.
UE 20	Deelnemers moeten geïnformeerd worden over de status van de uitvoering van een spelronde (zoals start, voortgang en succesvol afronden van een spelronde).
UE 21	Individuele scores van een Deelnemer zijn alleen zichtbaar voor de Deelnemer. De privacy van de Deelnemer moet te allen tijde gewaarborgd zijn.

3.1.5. Additionele diensten

De Opdrachtnemer levert op verzoek van Opdrachtgever Additionele diensten in de vorm van Consultancy op senior niveau. De in te zetten consultant dient ervaring te hebben waarbij de consultant zelfstandig op een efficiënte wijze (complexe) vraagstukken met betrekking tot de OSAG Dienst kan behandelen.

Consultancy uren kunnen gevraagd worden voor onder andere het adviseren en realiseren over onder andere verbeteren van de inrichting, aanvullende koppelingen, mogelijkheden tot het vergroten van de kennisoverdracht, aanpassen/uitbreiden van rapportagemogelijkheden en uitbreiden van inzet van de OSAG Dienst.

Consultancy uren mogen niet ingezet worden voor het oplossen van Incidenten, Problemen met en/of vragen over het gebruik van de OSAG Dienst (dit valt binnen het Beheer en Onderhoud of Support). Ook het creëren en publiceren van de Content is onderdeel van de opdracht en geen consultancy.

UE 22	Opdrachtnemer levert op verzoek van Opdrachtgever Consultancy (op senior niveau). De verwachting is dat er gemiddeld circa 80 uur Consultancy er jaar zal worden afgenomen. Deze verwachte uren zijn indicatief en hier kunnen geen rechten aan worden ontleend.
-------	--

3.2. Implementatie fase

De OSAG Dienst dient bij de Opdrachtgever geïntroduceerd te worden en de Spelondersteuners moeten de OSAG Dienst leren gebruiken. In de volgende paragrafen worden de eisen omtrent de eenmalige werkzaamheden ten aanzien van de Implementatie (initiële inrichting, Test- en Acceptatie procedure, instructie en beschikbaar stellen van de OSAG Dienst) beschreven. Tot slot wordt deze paragraaf afgesloten met de beschrijving van Wens 3 Plan van Aanpak waarin een uitwerking wordt gevraagd van de voorgaande sub paragrafen.

3.2.1. Initiële Release

De OSAG Dienst dient binnen 6 weken na ondertekening van de Overeenkomst conform de in dit document beschreven Specificaties inclusief de eerste spelronde,

operationeel (opgeleverd en door Opdrachtgever geaccepteerd) te zijn. De tweede spelronde dient binnen 10 weken na ondertekening van de Overeenkomst operationeel te zijn. In overleg is het mogelijk om de OSAG Dienst beschikbaar te stellen en op een later moment managementinformatie beschikbaar te stellen.

De Opdrachtnemer is verantwoordelijk voor het daar waar nodig aanpassen van de Standaardprogrammatuur op de behoefte van de Opdrachtgever (inclusief de benodigde koppelingen en dergelijke).

UE 23	Opdrachtnemer stelt uiterlijk vier weken voor de start van de eerste spelronde communicatiemateriaal voor de promotie van de OSAG Dienst, in de vorm van bijvoorbeeld digitale posters, banners e.d. beschikbaar.
UE 24	Spelronde één, inclusief maar niet gelimiteerd tot de kennisthema's zoals genoemd bij UE 5, is binnen zes (6) weken na ingangsdatum van de Overeenkomst beschikbaar.
UE 25	Spelronde twee, welke zal focussen op privacy en AVG, is binnen tien (10) weken na ingangsdatum van de Overeenkomst beschikbaar.
UE 26	Opdrachtnemer spant zich in een initiële Releases op te leveren die foutvrij is en die voldoet aan de gestelde (functionele en technische) Specificaties, zodat de kans dat Opdrachtgever tijdens de Acceptatie nog Incidenten constateert minimaal is.
UE 27	Bij het testen van de OSAG Dienst mag geen gebruik worden gemaakt van naar natuurlijke personen herleidbare Gegevens.
UE 28	Als onderdeel van de Oplevering wordt de Documentatie (waaronder Releasenotes en instructiemateriaal) digitaal beschikbaar gesteld.
UE 29	De OSAG Dienst kan door de Opdrachtgever tijdens de Implementatie onderworpen worden aan diverse Testen ten behoeve van de Acceptatie, zoals technische, functionele en gebruikersacceptatietesten, maar ook testen met betrekking tot de Performance en Beveiliging (bijvoorbeeld een A&P test). De hieruit voortkomende Bevindingen en Kwetsbaarheden worden door de Opdrachtnemer opgelost, zonder extra kosten te rekenen voor bijvoorbeeld de inzet van medewerkers/productspecialisten en/of andere materialen en middelen.

3.2.2. Instructie

De OSAG Dienst zal gebruikt worden door alle interne en externe medewerkers van Opdrachtgever. De OSAG Dienst dient dusdanig intuïtief en gebruiksvriendelijk te zijn zodat een (potentiële) Deelnemers zich de OSAG Dienst, zonder extra instructie, snel en eenvoudig eigen kunnen maken.

De Opdrachtnemer verzorgt in maximaal één (1) dagdeel de instructie voor de Spelondersteuners. Dit kan in één of twee groepen op een door Opdrachtgever aan te geven locatie ergens centraal in het land of digitaal. Die locatie wordt door Opdrachtgever bekostigd. De Opdrachtnemer verzorgt een dusdanige instructie voor de Spelondersteuners zodat ze daarna zelfstandig in staat zijn om:

- ten behoeve van hun werkzaamheden zelfstandig met de OSAG Dienst kunnen werken en

- eerstelijns functionele vragen van de Deelnemers te kunnen beantwoorden.

De Opdrachtnemer stelt het benodigde instructiemateriaal digitaal beschikbaar. De benodigde instructies vinden kort voor de ingebruikname plaats.

GUE 12	De OSAG Dienst is intuïtief dat voor het gebruik door de Deelnemers geen instructie nodig is.
GUE 13	De OSAG Dienst beschikt over een relevante helpfunctie.
UE 30	Opdrachtnemer verzorgt op een door de Opdrachtgever aan te wijzen centrale plaats in Nederland (of digitaal) de benodigde instructie(s) voor de Spelondersteuners.
UE 31	Opdrachtnemer verzorgt in het Nederlands de benodigde Documentatie en instructiemateriaal.
UE 32	Documentatie en instructiemateriaal zal na de instructie elektronisch beschikbaar worden gesteld.

3.2.3. Plan van Aanpak

Om inzicht te krijgen op welke wijze de Inschrijver de Implementatie uit gaat voeren, wordt Inschrijver gevraagd daarvoor een concept Plan van Aanpak aan te leveren.

GUE 14	Het door Inschrijver, ten beantwoording van onderstaande Wens "Plan van Aanpak" aangeleverde concept Plan van Aanpak, vormt de basis voor de wijze waarop de Implementatie van de OSAG Dienst wordt gemanaged en uitgevoerd. Bij de start van de Overeenkomst zal Opdrachtnemer het concept Plan van Aanpak in overleg met Opdrachtgever nader afstemmen. Nadat er overeenstemming is tussen Partijen over de definitieve inhoud van het Plan van Aanpak wordt er met de uitvoering van de Implementatie gestart.
--------	---

Van de Opdrachtnemer wordt verwacht om met minimale belasting voor Opdrachtgever een test versie van de OSAG Dienst ten behoeve van de initiële Release op te leveren. Indien gewenst is de Opdrachtgever bereid om, op verzoek, (beperkt) specialisten beschikbaar te stellen. De Opdrachtnemer dient eventuele gewenste capaciteit tijdig aan te vragen. In verband hiermee beschikt Opdrachtgever onder andere over de volgende specialisten:

- een materiedeskundige (spelbegeleider of spelcoördinator) die bekend is met de functionele inhoud;
- een applicatiebeheerder die bekend is met de technische kant van de huidige software en is aanspreekpunt voor Beheer en Onderhoud;
- een projectmanager die fungeert als aanspreekpunt voor beide Partijen.

UE 33	Inschrijver dient in het concept Plan van Aanpak expliciet aan te geven welke inzet van specialisten van Opdrachtgever gewenst zijn (specialist, wanneer en hoeveel uur). Opdrachtnemer blijft te allen tijde verantwoordelijk voor de tijdige Oplevering van de OSAG Dienst.
UE 34	Indien Opdrachtnemer aanvullend (welke niet expliciet is opgenomen in het Plan van Aanpak) gebruik wenst te maken van specialisten van Opdrachtgever dan dient Opdrachtnemer dit tijdig (minimaal twee (2)

	weken voor aanvang) aan te vragen. Indien aanvullende inzet (welke niet expliciet is opgenomen in het Plan van Aanpak) gewenst is kan Opdrachtgever niet garanderen dat de benodigde specialisten tijdig voldoende capaciteit beschikbaar kan stellen voor Opdrachtnemer. Een tijdige oplevering van de OSAG dienst blijft dan alsnog de verantwoordelijkheid van Opdrachtnemer.
W 3	Plan van Aanpak Middels deze Wens wil de Opdrachtgever inzicht krijgen in het Plan van Aanpak van Inschrijver welke, indien u de opdracht gegund krijgt, de basis zal vormen voor de Implementatie van de initiële Release van de OSAG Dienst. Het Plan van Aanpak heeft betrekking op de Implementatie, vanaf het moment van gunning van de opdracht aan u door de Opdrachtgever tot en met in gebruik name van de OSAG Dienst ten behoeve van spelronde één en twee (hiervoor dient u Bijlage V. Toelichtingen en beantwoording Wensen te gebruiken). Vraag: Beschrijf uw concept Plan van Aanpak voor de Implementatie van de OSAG Dienst, met daarin ten minste: 1. Planning • Het door Inschrijver beoogde tijdspad voor de Implementatie (inclusief de oplevering van de eerste twee spelrondes) en de randvoorwaarden waar de Opdrachtgever aan moet voldoen om de OSAG Dienst te realiseren binnen het gestelde tijdspad. Het tijdspad dient realistisch te zijn. • Het tijdspad dient een duidelijke fasering en milestones te hebben. • De planning dient de periode vanaf definitieve gunning tot ingebruikname van de OSAG Dienst te bevatten. 2. Projectorganisatie • De projectmanagementmethode en projectaanpak voor de Implementatie (inclusief Acceptatie) van de OSAG Dienst. • Projectteam en door Inschrijver in te zetten medewerkers (inclusief een beschrijving van hun kennis en kunde). • De benodigde inzet van specialisten van de Opdrachtgever; • Verantwoordelijkheden (matrix). 3. Borging van de Kwaliteit • De aanpak voor het instrueren van de Spelondersteuners van de Opdrachtgever. • Een beschrijving van de (belangrijkste) beheersmaatregelen van risico's tijdens de Implementatie. Beschrijf het concept Plan van Aanpak in maximaal zeven (7) pagina's A4 en één (1) pagina A3 ten behoeve van een planning. Beoordeling:

	Het concept Plan van Aanpak wordt beoordeeld op de volgende aspecten: 1. Planning 2. Projectorganisatie 3. Borging van de Kwaliteit Deze Wens wordt beoordeeld op basis van de mate waarin het antwoord voldoet aan de verwachtingen van de Opdrachtgever. Voor deze Wens zijn in totaal maximaal 20 punten te behalen.
--	--

3.3. Operationele fase

De operationele fase vangt aan na integrale Acceptatie waarin Opdrachtnemer de OSAG Dienst operationeel houdt, innoveert en verbetert tot het moment van Retransitie. In onderstaande paragrafen is deze fase verder beschreven.

3.3.1. Hosting, Beheer en Onderhoud

De Hosting, Beheer en Onderhoud van de OSAG Dienst richt zich tot het 'in de lucht houden' en onderhouden van de applicatie-infrastructuur. Aangezien deze opdracht een SaaS dienst betreft, zal de Hosting, Beheer en Onderhoud in zijn geheel bij de Opdrachtnemer liggen.

GUE 15	Opdrachtnemer is volledig verantwoordelijk voor de Hosting, Beheer en Onderhoud van de OSAG Dienst.
--------	---

3.3.2. Support

De Service Level Agreement (SLA) wordt door Opdrachtnemer opgesteld en aan Opdrachtgever opgeleverd met inachtneming van onderstaande Service Levels. De SLA maakt onderdeel uit van de Overeenkomst. De SLA bevat een beschrijving van de overeengekomen Serviceniveaus van de geleverde Diensten, de overeengekomen prestatiecriteria en de wijze waarop geacteerd wordt indien niet wordt voldaan aan de overeengekomen Serviceniveaus. Daarover wordt door middel van rapportage en overleg verantwoording afgelegd aan de Opdrachtgever.

Met betrekking tot het bepalen van de prioriteit van Bevindingen gebruikt de Opdrachtgever een standaard model. Afhankelijk van de Impact en de Urgentie wordt de Prioriteit bepaald van opgetreden Incidenten.

Impact	
Hoog	Een Incident heeft of kan ernstige gevolgen hebben voor • één of meer bedrijfsprocessen die de burger en/of het bedrijf direct raken, en/of • één of meer fabriekstaken voor (massale) gegevensverwerking en/of • de Informatiebeveiliging en/of • het imago van Opdrachtgever en/of • onacceptabele hoge kosten.

Laag	Overige situaties.
------	--

Urgentie	
Hoog	Een Incident - beïnvloedt Kwaliteit van functies/Beschikbaarheid/(Informatie)Beveiliging en/of - brengt integriteit van de Gegevens in het geding en/of - treedt op tijdens piektijd/-periode van het bedrijfsproces en/of - brengt uiterste verzenddatum van klantbescheiden in gevaar en/of - verstoort de communicatie met de klanten van Opdrachtgever en/of - er geen workaround mogelijk is en/of - de verwerking kan niet worden uitgesteld en/of - de schade is al een feit of zal dat zijn binnen 24 uur.
Laag	Overige situaties.

Prioriteit	
Prioriteit 1	Impact hoog / Urgentie hoog
Prioriteit 2	- Impact hoog / Urgentie laag - Impact laag / Urgentie hoog
Prioriteit 3	Impact laag / Urgentie laag

UE 35	Op basis van bovenstaande tabel worden de prioriteiten van de Incidenten bepaald. De OSAG Dienst voldoet minimaal aan de volgende Serviceniveaus ten aanzien van de afhandeling van Incidenten (Oplostijd): - Oplostijd Incident prioriteit 1: binnen 1 Werkdag; - Oplostijd Incident prioriteit 2: binnen 3 Werkdagen; - Oplostijd Incident prioriteit 3: binnen 10 Werkdagen.
UE 36	De OSAG Dienst voldoet aan onderstaande eisen betreffende de operationele continuïteit in geval van een Calamiteit (crisis): - recovery time objective (RTO): De Oplossing is binnen 72 klokuren weer volledig functioneel beschikbaar; - recovery point objective (RPO): Er is maximaal 24 klokuren verlies van Gegevens toegestaan.
GUE 16	Een ongelimiteerd aantal Calls kunnen via website (of e-mail) en telefonisch worden aangemeld. De Servicedesk van de Opdrachtnemer is: 24 uur per dag 7 dagen per week voor meldingen via de website (of e-mail) bereikbaar en - tijdens Werkdagen van 09:00 tot 17:00 uur (Central European Time (CET)) telefonisch bereikbaar.
GUE 17	De OSAG dienst voldoet aan een Beschikbaarheid van minimaal 96% per maand. Hierbij geldt een Service window (openstelling van de OSAG Dienst) van 24 uur per dag, 7 dagen per week en 365 dagen per jaar

GUE 18	Een Beveiligingsincident wordt altijd per direct na constatering (24 uur per dag, 7 dagen per week en 365 dagen per jaar) opgevolgd met een actie van de Opdrachtnemer. Beveiligingsincidenten moeten derhalve ook altijd (24 uur per dag, 7 dagen per week en 365 dagen per jaar) aangemeld kunnen worden.
GUE 19	Op de OSAG Dienst wordt een passende Service Level Agreement toegepast welke voldoet aan de gestelde Serviceniveaus. De Service Level Agreement (SLA) wordt door Opdrachtnemer opgesteld en aan Opdrachtgever opgeleverd.
UE 37	Periodiek (minimaal per kwartaal) levert Opdrachtnemer een SLA-rapportage aan over bovenstaande Service levels.

3.3.3. Releasemanagement

UE 38	Wijzigingen ten aanzien van de OSAG Dienst worden door de Opdrachtnemer tijdig (minimaal 14 Kalenderdagen voor realisatie/in productie name ervan) aangekondigd.
UE 39	Opdrachtnemer spant zich in Releases op te leveren die foutvrij zijn en voldoen aan de gestelde (functionele en technische) Specificaties, zodat de kans dat Opdrachtgever nog Incidenten constateert minimaal is. Opdrachtgever wordt in de gelegenheid gesteld om een Acceptatietest te organiseren en uit te voeren voor de wijzigingen die impact kunnen hebben op koppervlakken en gegevensuitwisseling met andere dan door de Opdrachtnemer geboden applicatie.
UE 40	Opdrachtnemer is verantwoordelijk dat Documentatie (inclusief instructiemateriaal) na een nieuwe Release actueel blijft. Na oplevering van een nieuwe Release wordt de geactualiseerde Documentatie digitaal beschikbaar gesteld.

3.4. Retransitie

Bij beëindiging van de Overeenkomst tussen Partijen is een gecontroleerd en projectmatig overgang van Opdrachtnemer naar de nieuwe opdrachtnemer gewenst om de continuïteit van de Diensten te borgen.

UE 41	Opdrachtnemer is verplicht haar medewerking te verlenen aan Retransitie zonder storing in de continuïteit van de Prestatie.
UE 42	Opdrachtnemer dient voldoende gekwalificeerd personeel beschikbaar te stellen voor de Retransitie.
UE 43	Opdrachtnemer geeft de volledige medewerking aan de Retransitie en overhandigt daarbij alle relevante Gegevens en Documentatie aan Opdrachtgever c.q. nieuwe dienstverlener.
UE 44	De Gegevens worden, indien door Opdrachtgever gewenst, zonder storing in de continuïteit van de Prestatie, gemigreerd naar een opvolgende applicatie.

UE 45	Op verzoek van de Opdrachtgever worden bij beëindiging van de Overeenkomst Gegevens van Opdrachtgever binnen een van te voren afgesproken aantal dagen ter beschikking gesteld, in een voor Opdrachtgever bruikbaar van te voren afgesproken digitaal formaat. Aanlevering gebeurt via een beveiligde verbinding. Opdrachtgever stelt hiervoor een beveiligde dienst beschikbaar. De ter beschikking gestelde Gegevens dienen te zijn voorzien van een zodanige functionele- en technische beschrijving dat in de toekomst een datamigratie naar een nieuwe OSAG Dienst kan plaatsvinden zonder verdere tussenkomst van de Opdrachtnemer.
UE 46	Bij overgang naar een nieuwe opdrachtnemer moet de OSAG Dienst (een beperkte, passende, vooraf overeengekomen periode), tegen gelijkblijvende condities (naar rato), voor Opdrachtgever beschikbaar blijven.
UE 47	Opdrachtnemer zorgt er voor dat uiterlijk één (1) kalendermaand na het beëindigen van de Overeenkomst en/of na de migratie dat alle Gegevens (inclusief back-ups e.d.) van Opdrachtgever onherstelbaar zijn vernietigd. Hierbij wordt door de Opdrachtnemer aangetoond dat dit op een dusdanige wijze heeft plaatsgevonden dat de gegevens niet gereconstrueerd of anderszins hersteld kunnen worden. Voor de verwijdering dient er gebruik gemaakt te worden van een door de overheid gecertificeerd product, zie: www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducten/geevalueerde-producten
UE 48	Opdrachtnemer overhandigt een verklaring van vernietiging aan Opdrachtgever.

3.5. IV kaders

Opdrachtgever hecht veel belang aan de Informatiebeveiliging van Gegevens. Opdrachtgever heeft een taak en verantwoordelijkheid om er voor te zorgen dat Gegevens nooit in onbevoegde handen vallen of kunnen vallen.

Opdrachtnemer dient alle passende en nodige maatregelen te hebben getroffen en te treffen om de Opdrachtgever in staat te stellen deze taak uit te voeren en haar verantwoordelijkheid te kunnen nemen.

Een belangrijk kader in de te nemen beveiligingsmaatregelen is de vigerende wetgeving en standaarden ten aanzien van ICT-beveiliging en privacy.

GUE 20	De OSAG Dienst voldoet aan de algemene vigerende Nederlandse Wet- en Regelgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG).
--------	--

Opdrachtgever is gehouden aan de vigerende **Baseline Informatiebeveiliging Overheid** (de actuele versie van de BIO is versie 1.04, deze is opgenomen als Bijlage B). Dit overheidsbeleid is gebaseerd op de ISO27001 en de ISO27002 en bevat daarnaast aanvullende beveiligingseisen, de zogenoemde verplichte overheidsmaatregelen.

De OSAG Dienst dient veilig te zijn. Dit betekent dat voldaan wordt aan BBN1 (Basis Beveiligingsniveau 1) zoals gesteld in de BIO.

Daarnaast stelt Opdrachtgever zelf ook beveiligingseisen, de zogenaamde Belastingdienst specifieke eisen.

De Opdrachtnemer is niet direct gehouden aan de Baseline Informatiebeveiliging Overheid omdat dit stelsel geldt voor overheidspartijen, zoals de Belastingdienst. Echter, de Opdrachtnemer dient Opdrachtgever in staat te stellen om haar verantwoordelijkheid te kunnen nemen.

Door ISO 27001 certificering kunt u deels aantonen dat u voldoet aan het overheidsbeleid op het gebied van informatiebeveiliging ten aanzien van de OSAG Dienst. Het stelt Opdrachtgever in staat om aan een deel van haar verplichten ten aanzien van de BIO te voldoen.

Ten minste de volgende verplichte overheidsmaatregelen vanuit de BIO zijn van toepassing:

Par.	Maatregelen
9.2.1	Registratie en afmelden van gebruikers
	1 Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.
	2 Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de Belastingdienst.
9.2.2	Gebruikers toegang verlenen
	1 Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.
	2 Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.
12.4.1	Gebeurtenissen registreren
	1 Een logregel bevat minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; datum en tijdstip van de gebeurtenis.
	2 Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.
12.4.2	Beschermen van informatie in logbestanden
	2 Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.
15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
	4 Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaardvoorwaarden voor inkoop gehanteerd.

Par.	Maatregelen
15.1.3	Toeleveringsketen van informatie- en communicatietechnologie
	1 Leveranciers moeten hun keten van toeleveranciers bekend maken en transparant zijn over de maatregelen die zij genomen hebben om de aan hun opgelegde eisen ook door te vertalen naar hun toeleveranciers.
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen
	1 Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.
	2 Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.
	3 Alle medewerkers en contractanten hebben aantoonbaar kennis genomen van de meldingsprocedure van incidenten.
	4 Incidenten worden zo snel als mogelijk, maar in ieder geval binnen 24 uur na bekendwording, gemeld bij het meldloket.
	5 De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.
	6 De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.
	7 Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD) procedure is onderdeel van de incidentrapportage.

UE 49	Opdrachtnemer neemt de benodigde maatregelen om te garanderen dat Opdrachtgever kan voldoen aan de (beveiligings)eisen zoals gespecificeerd in bovenstaande tabel.
-------	--

Aanvullend op de gestelde norm omtrent de Informatiebeveiliging (conform Beschrijvend document GE 2.) en een aantal maatregelen uit de BIO dient de Opdrachtnemer aan een aantal specifieke eisen te voldoen.

UE 50	Opdrachtgever heeft het recht om een A&P test uit te laten voeren om de beveiliging te testen. Opdrachtgever contracteert hierbij zelf een onafhankelijk en algemeen erkend bureau dat de testen uitvoert. A&P tests zijn enkel toetsend en vervangen niet de beveiligingsmaatregelen van de Opdrachtnemer. De kosten van de uitvoering van deze test zijn voor rekening van Opdrachtgever. Opdrachtnemer werkt kosteloos mee aan A&P testen. Bevindingen uit A&P testen dienen op kosten van Opdrachtnemer opgelost te worden.
UE 51	De resultaten van de testen worden gedeeld met Opdrachtgever. Deze procedure zal worden vastgelegd. Bij het bespreken van de Bevindingen worden afspraken gemaakt over de Oplostijden en de aansluitende hertest en, indien noodzakelijk, het moment dat een nieuwe A&P test wordt afgenomen.

	Opdrachtnemer draagt zorg voor het oplossen van de Bevindingen binnen de afgesproken Oplostijden.
UE 52	Opdrachtgever heeft de bevoegdheid om toegang tot (relevante delen van) de OSAG Dienst te blokkeren. Dit wordt het Stekkermandaat genoemd. Dit mandaat bestaat uit twee acties, die door de Opdrachtnemer, geëffectueerd moeten zijn: 1. het onbeschikbaar maken van (relevante delen van) de OSAG Dienst; 2. het ontoegankelijk maken van de Gegevens. De Opdrachtnemer biedt de mogelijkheid om de Gegevens van Opdrachtgever ontoegankelijk te maken voor onbevoegden en veilig te stellen. Dit zodat de vertrouwelijkheid en integriteit van de Gegevens gewaarborgd blijven. Het deblokken van (delen van) de OSAG Dienst mag alleen na expliciete toestemming van Opdrachtgever.
UE 53	Opdrachtgever heeft het recht om vulnerability (Kwetsbaarheden) scans op de OSAG Dienst uit te laten voeren door het Security Operation Center (SOC) Opdrachtgever. Opdrachtnemer zorgt ervoor dat het SOC de benodigde toegang heeft om deze scan uit te voeren. De Bevindingen worden indien nodig gedeeld en besproken met de Opdrachtnemer. Gevonden Kwetsbaarheden worden opgelost door Opdrachtnemer. Opdrachtnemer geeft toestemming voor de uitvoering door Opdrachtgever van de vulnerability scans en werkt hieraan kosteloos mee. Vulnerability scans vervangen niet de beveiligingsmaatregelen van de Opdrachtnemer.
UE 54	Kwetsbaarheden worden gekwalificeerd doormiddel van het common vulnerability scoring system 3.0 (CVSS 3.0). Kritische bevindingen (critical) dienen per direct te worden weggenomen door de Opdrachtnemer. Voor hoge risicobevindingen (high risk) geldt dat deze binnen uiterlijk 30 Kalenderdagen zijn weggenomen door de Opdrachtnemer. Voor Kwetsbaarheden die geclassificeerd zijn als "gemiddeld" en "laag" worden termijnen van respectievelijk drie en zes maanden gehanteerd (comply). Indien er gegronde redenen zijn om een Kwetsbaarheid geclassificeerd als "gemiddeld" of "laag", niet te verhelpen dient de Opdrachtnemer hiervoor een motivatie op te leveren (explain) aan Opdrachtgever en deze motivatie voor akkoord te laten verklaren door Opdrachtgever. Deze procedure zal worden vastgelegd.
UE 55	Opdrachtgever heeft het recht een Audit uit te laten voeren om de opzet, het bestaan en de werking van een passend stelsel van beveiligingsmaatregelen ten aanzien van de OSAG Dienst te toetsen. Opdrachtgever kiest hierbij zelf welk onafhankelijk en algemeen erkend bureau de Audit uitvoert. De resultaten van de Audit worden, in de vorm van een Third Party Mededeling (TPM), gedeeld met Opdrachtnemer. Bij het bespreken van de bevindingen worden

afspraken gemaakt over de te nemen vervolgstappen. Opdrachtnemer werkt kosteloos mee aan de te nemen vervolgstappen.

3.5.1. Logisch Toegangsbeheer

Het proces van het beheer van medewerker autorisaties (verstrekken, intrekken en controleren) wordt binnen Opdrachtgever Logisch Toegangsbeheer genoemd, afgekort LTB. Een meer algemeen bekende term hiervoor is Identity & Access Management (IAM). Het LTB-proces omvat het autorisatieproces, identificatieproces en het authenticatieproces.

Voor een gecontroleerd LTB-proces is het noodzakelijk dat alle ICT-voorzieningen die autorisaties bevatten, de autorisatiebronnen, aangesloten zijn of worden op het LTB-proces.

Indien de OSAG Dienst een eigen autorisatiebron heeft, dient er middels het handmatige proces aangesloten te worden op IMS (Identity Managementsysteem). In het handmatige proces dient wekelijks autorisatie informatie (IST) uit de autorisatiebron van de applicaties aangeleverd te worden aan IMS door middel van bestandsoverdracht. Het aanmaken en aanbieden van zo'n IST-bestand dient geborgd te zijn in de OSAG Dienst.

GUE 21	Indien de OSAG Dienst een eigen autorisatiebron heeft dienen de onderstaande gegevens te kunnen worden aangeleverd in een bestand aan Opdrachtgever: • UserID (Account); • Group. Het bestand dient consistent te zijn: • alle leden van een Group dienen ook als account aangeleverd te worden in hetzelfde bestand; • Als een Account wordt aangeleverd, dat geen lid is van een Group, dan zal dit Account automatisch worden gedisabled binnen IMS; • Group dient ook aangeleverd te worden, als deze geen lidmaatschappen heeft. Bestand informatie: • 1 bestand van het formaat TXT of CSV, ; (punt-komma) als scheidingsteken; • inhoud is ruwe onbewerkte data uit de autorisatiebron; • een volledig extract, geen delta ten opzichte van vorige keer; • frequentie 1x per week; • er dienen geen quotes om waarden heen te staan. Tevens mogen er geen komma's, puntkomma's en diakrieten in de attributen staan.
GUE 22	Indien de OSAG Dienst gebruik maakt van een gebruikersidentificatie (gebruikersaccount), is deze altijd één op één herleidbaar naar een natuurlijk persoon. Indien binnen de OSAG Dienst rollen onderkend worden, bepaalt

	Opdrachtgever welke medewerkers welke rol binnen de OSAG Dienst verkrijgen.
GUE 23	De OSAG Dienst biedt een mechanisme voor Two-factor authenticatie aan. Opdrachtgever bepaalt voor welke rollen gebruik van Two-Factor Authenticatie binnen de OSAG Dienst verplicht is. Opdrachtgever voorziet het gebruik van Two-factor authenticatie voor alle rollen met uitzondering van de Deelnemers aan de Online security awareness game. Dit betekent dat o.a. de volgende rollen gebruik maken van Two-factor authenticatie: • medewerkers van Opdrachtnemer welke verantwoordelijk zijn voor het publiceren (plaatsen/beschikbaar stellen/inladen) van de Content in de OSAG Dienst; • Spelondersteuners.

3.5.2. Identity Management

De OSAG Dienst maakt gebruik van één Identity Management Systeem (IMS), waardoor Gebruikers (ongeacht hun rol en autorisaties) maar één keer hoeven te authenticeren om alle aan hun toegewezen functionaliteiten van de OSAG Dienst te kunnen gebruiken.

GUE 24	De Gebruiker hoeft zich enkel één maal aan te melden om gebruik te maken van de integrale functionaliteit van de OSAG Dienst. Het beheer van toegangsrechten voor de OSAG Dienst, inclusief de bewaking van functiescheiding, geschiedt vanuit één door de Opdrachtnemer geboden (logisch) IMS.
GUE 25	Het IMS van de OSAG Dienst ondersteunt federatieve authenticatie op basis van SAML 2.0.

Het Rijksbeleid kent voorschriften t.a.v. locatie waar de Gegevens worden opslagen.

UE 56	Opdrachtnemer dient gebruik te maken van versleuteling voor de uitwisseling van informatie tussen de OSAG Dienst en andere partijen. Er dient gebruik te worden gemaakt van tweeweg TLS. De gebruikte TLS-versie is conform de aanbeveling van NIST (www.nist.gov) of de NCSC (www.ncsc.nl).
UE 57	Gegevens dienen te allen tijde op verzoek van Opdrachtgever volledig verwijderd te kunnen worden. Hierbij wordt door de Opdrachtnemer aangetoond dat dit op een dusdanige wijze heeft plaatsgevonden dat de gegevens niet gereconstrueerd of anderszins hersteld kunnen worden. Voor de verwijdering dient er gebruik gemaakt te worden van een door de overheid gecertificeerd product, zie: www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducten/geevalueerde-producten.

3.5.3. Koppelingen

De OSAG Dienst dient aan te sluiten op de standaard werkwijzen en techniek van Opdrachtgever.

UE 58	De OSAG Dienst moet Gegevens kunnen importeren vanuit de administratie van de Opdrachtgever middels een koppeling. Bij koppeling van de OSAG Dienst aan een systeem van Opdrachtgever wordt voldaan aan de door Opdrachtgever gestelde maatregelen (zoals bijvoorbeeld tweezijdig TLS).
UE 59	Alle relevante API's van de OSAG Dienst ten aanzien van koppelingen en gegevensuitwisseling met andere autonome systemen van Derde partijen (indien van toepassing) zijn gedocumenteerd. Deze API-documentatie is actueel, correct en wordt op verzoek beschikbaar gesteld aan de Contractmanager van Opdrachtgever.
UE 60	De OSAG Dienst wordt door Opdrachtnemer continu gemonitord op Beveiligingsaspecten, capaciteit, Performance en Beschikbaarheid. De wijze van monitoring en rapportage en de waardes waarbij rapportage plaatsvindt, zal worden vastgelegd. Afwijkingen worden gerapporteerd in de SLA-Rapportage aan de contractmanager van Opdrachtgever.
UE 61	Alle mutaties van (persoons)Gegevens moeten dusdanig door de OSAG Dienst geregistreerd worden, dat het mogelijk is misbruik te detecteren en analyseren. De OSAG Dienst wordt zodanig door de Opdrachtnemer bewaakt, dat het mogelijk is tot minimaal zes (6) maanden in het verleden (forensisch) onderzoek te verrichten.

Hoofdstuk 4. Financiële afspraken

4.1. Tariefherziening

De door Opdrachtnemer geoffeerde Tarieven, zoals opgegeven in Bijlage VI. Prijsmodel staan voor de eerste drie (3) jaar dat de OSAG Dienst operationeel is vast en mogen niet worden herzien. Na deze periode kunnen de Tarieven jaarlijks per 01 januari worden herzien. De eerste tariefherziening kan derhalve plaatsvinden op 01 januari 2026.

Om voor tariefherziening in aanmerking te komen dient Opdrachtnemer uiterlijk voor 1 december van enig jaar, een schriftelijk verzoek voor een tariefherziening in bij de verantwoordelijk contractmanager van Opdrachtgever. Dit verzoek dient voorzien te zijn van een bijbehorende onderbouwing (ten aanzien van de gestegen kosten van uitvoering) en motivering.

De door Inschrijver geoffeerde Tarieven mogen (nadat de periode dat de Tarieven vast staan) jaarlijks steeds per 1 januari geïndexeerd. De maximale tariefherziening is vastgesteld op basis van de CBS index-tabel 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=25692>. Het percentage voor de tariefherziening wordt afgerond op één decimaal achter de komma. Inhaalslagen op niet doorgevoerde indexeringen worden niet geaccepteerd.

UE 62	De opgegeven Tarieven staan vast voor de eerste drie (3) jaar dat de OSAG Dienst operationeel is. De Tarieven kunnen daarna jaarlijks per 01 januari worden herzien.
UE 63	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/statline/#/CBS/nl/dataset/83760NED/table?ts=1594803086253 , zoals gepubliceerd door het CBS. 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 64	Het is niet toegestaan om eventueel in een voorgaand jaar niet in rekening gebrachte tariefherzieningen later alsnog toe te passen.

4.2. Facturatievoorwaarden

UE 65	Kosten die niet in de Inschrijving opgenomen zijn en niet verdisconteerd zijn in de prijsstelling, maar toch noodzakelijk blijken te zijn voor een goed functioneren van de OSAG Dienst of de Dienstverlening, conform de in het Beschrijvend Document (incl. Bijlagen) gestelde eisen, zijn voor rekening van Inschrijver.
-------	---

UE 66	De implementatiekosten ten behoeve van de initiële Release van de OSAG Dienst (inclusief ten minste inrichting/configuratie van de Standaardprogrammatuur, realisatie van de koppelingen, creatie en publiceren/beschikbaar stellen van de Content ten behoeve van spelronde één en twee, instructie van de Spelondersteuners, oplevering van Documentatie en inrichten/beschikbaar stellen van (management)informatie en rapportages e.d.) mogen na volledige Acceptatie van de OSAG Dienst gefactureerd worden.
UE 67	De facturering van het gebruik van de OSAG Dienst incl. de Hosting, Beheer- , Onderhoud- en Supportkosten dienen jaarlijks vooraf aan het begin van elk gebruiksjaar (per 12 maanden) plaats te vinden. Het eerste gebruiksjaar mag na volledige Acceptatie van de OSAG dienst gefactureerd worden.
UE 68	Additionele diensten worden achteraf na afronding en Acceptatie van de desbetreffende werkzaamheden in rekening gebracht.
UE 69	De uurtarieven ten behoeve van de inzet van consultants zijn all-in Tarieven. Er kunnen derhalve geen aanvullende kosten in rekening worden gebracht (bij on-site inzet zijn, reistijd, reis- en verblijfkosten in het uurtarief opgenomen).
UE 70	Er wordt een betalingstermijn van 30 dagen na ontvangst van de factuur gehanteerd.

4.3. Elektronisch factureren (EBF) – e-factureren

Een e-factuur is een gestructureerd digitaal bestand (geen Pdf) waarbij de vereiste gegevens altijd op een vaste plek met specifieke codering in het bestand staan. Een e-factuur kan vanuit het ene geautomatiseerde systeem elektronisch worden aangemaakt en automatisch worden verwerkt in het andere systeem.

Voor het verzenden worden de volgende mogelijkheden geboden:

1. factuurportaal van de Rijksoverheid;
2. directe koppeling met DigiPoort;
3. e-factuur indienen vanuit uw (boekhoud)softwarepakket via Peppol;
4. e-factureren via een dienstverlener die een directe koppeling heeft met DigiPoort.

NB: Om elektronisch te kunnen factureren zijn ten minste de volgende gegevens nodig:

- naam en adres van de Opdrachtnemer;
- het KvK-nummer van de Opdrachtnemer;
- het btw-nummer van de Opdrachtnemer;
- de IBAN-code (en indien van toepassing de BIC) van de Opdrachtnemer;
- het Overheidsidentificatienummer (OIN) van de Rijksdienst waaraan de factuur wordt gestuurd. De lijst met OIN's wordt bijgehouden door Logius, zie www.logius.nl voor het actuele overzicht;
- het afleveradres (het adres waar de goederen of diensten zijn geleverd);
- het bestelnummer (bestaat uit totaal 10 cijfers (41xxxxxxxx of 45xxxxxxxx));
- contactpersoon (de persoon die de bestelling heeft geplaatst);
- artikelcode (indien van toepassing);
- de omschrijving van de bestelde/geleverde goederen of diensten;

- de bestelde/geleverde hoeveelheid;
- de prijs per eenheid.

UE 71	Opdrachtnemer verzendt de factuur elektronisch zodat deze met inachtneming van de door de Opdrachtgever gegeven Specificaties elektronisch kan worden ontvangen en verwerkt.
-------	--

Aansluiten op het factuurportaal van de Rijksoverheid kan de Opdrachtnemer regelen door middel van zelfregistratie via internet.

Aansluiting op DigiPoort voor geautomatiseerde uitwisseling van berichten wordt verzorgd door Logius, de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Voor aansluiting op DigiPoort neemt de Opdrachtnemer na gunning contact met hen op via telefoon 0900 - 555 4555, per e-mail servicecentrum@logius.nl of op www.logius.nl. Op het aansluiten op DigiPoort zijn de algemene gebruiksvoorwaarden Digipoort en de algemene voorwaarden van Logius van toepassing. Deze voorwaarden treft u eveneens aan op voornoemde website. Het uitbrengen van een Inschrijving impliceert dat voornoemde voorwaarden door de Opdrachtnemer worden geaccepteerd.

Bij keuze voor Peppol of voor het inschakelen van een dienstverlener neemt de Inschrijver na gunning zelf contact op met de partij naar keuze.

Nadere informatie over e-factureren kunt u vinden in de brochure '[elektronisch factureren voor leveranciers](#)'. Meer informatie is ook verkrijgbaar bij de Rijks-brede helpdesk e-factureren, via www.helpdesk-efactureren.nl.

UE 72	Opdrachtnemer start direct na de gunning het aansluitproces op e-factureren via één van de door de Opdrachtgever voorgeschreven manieren voor e-factureren en informeert de Opdrachtgever over de door Opdrachtnemer gekozen wijze van aansluiten op e-factureren.
UE 73	De Opdrachtgever berekent geen kosten aan Opdrachtnemer voor aansluiting op en communicatie met DigiPoort. Bij een directe aansluiting op DigiPoort komen alle kosten vanaf het koppelvlak aan opdrachtnemerszijde voor rekening van de Opdrachtnemer. De kosten die Opdrachtnemer in dit verband nu (en in de toekomst) maakt, zijn voor eigen rekening.