Algemene informatie

Aanbesteding:	Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Aanbestedende Dienst:	gemeente Sittard-Geleen
Referentie:	Z/23/486936

Toelichting:
Let op: er is een nieuw Prijzenblad toegevoegd (versie 3). De oude versies vervallen.

Vraag en antwoord

Ref.nr.	**Onderwerp:**
167	Vraag 98 - NvI

Vraag:
Vraag 98 Nota van Inlichtingen

In uw antwoord geeft u aan dat de pentestovereenkomst dient ter verificatie van de gestelde security eisen. Wij kunnen er niet mee instemmen dat u een pentest uitvoert op onze systemen, te meer nu wij ISO27001 gecertificeerd zijn, waarmee deugdelijkheid van het informatiebeveiligingsniveau afdoende wordt aangetoond. Het uitvoeren van pentesten op onze systemen door klanten is vanwege de grote hoeveelheid klanten die wij bedienen praktisch gezien niet uitvoerbaar. Bovendien vraagt u in onderhavige aanbesteding dienstverlening uit met betrekking tot uw informatiebeveiligingsniveau. Het is niet passend dat u in dit verband door een derde een pentest laat uitvoeren op systemen van opdrachtnemer, zeker niet nu niet bekend is op welke systemen u dit wenst te laten doen en opdrachtnemer daarvoor een vrijwaring dient af te geven. Het verstrekken van een vrijwaring in het kader van pentestdienstverlening is gebruikelijk omdat normaliter de partij waarbij de pentest wordt uitgevoerd ook degene is die de pentest wenst uit te laten voeren.

Gelet op de verhoudingen tussen partijen en het aantonen van een voldoende informatiebeveiligingsniveau door middel van het ISO27001 certificaat verzoeken wij u de pentestovereenkomst voor deze opdracht buiten toepassing te verklaren. Kunt u daarmee instemmen? Zo niet, waarom acht u het noodzakelijk (en passend) dat u ervoor kunt kiezen een pentest uit te (laten) voeren op de systemen van uw opdrachtnemer?

Antwoord:
Er wordt niet afgeweken van het uitvoeren van de pentest. De pentest heeft echter betrekking op representatieve omgeving en niet op de productieomgeving.

Percelen: P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op: 3 okt. 2024

Ref.nr.
168

Onderwerp:
Vraag 103 - NvI

Vraag:
Vraag 103 Nota van Inlichtingen

In uw antwoord op vraag 103 geeft u aan niet akkoord te gaan. U geeft aan dat het optionele verificatieverslag en de opdrachtbrief geen afwijkingen zullen bevatten. Echter prevaleren bepaalde documenten (waaronder de overeenkomst) nu boven de Nota's van Inlichtingen, terwijl de Nota's van Inlichtingen bedoeld zijn om aanpassingen op de contractvoorwaarden door te voeren. Wij wensen derhalve de overeengekomen afspraken uit de NvI hoger in rang op te nemen dan de reeds bestaande documenten (waaronder de overeenkomst), zodat de afspraken uit de NvI's zullen prevaleren. Indien dit niet zo wordt opgenomen, hebben de afwijkingen in de NvI feitelijk geen nut. Wij verzoeken u gelet hierop uw antwoord op vraag 103 te heroverwegen en alsnog akkoord te gaan met ons verzoek de NvI's het hoogste in rang te plaatsen, zodat de overeengekomen afwijkingen prevaleren. Kunt u hiermee instemmen?

Antwoord:
Nee, er is geen sprake van een separate overeenkomst. Zoals opgenomen in de leidraad bestaat de overeenkomst uit de
opdrachtbrief en alle documenten die horen bij deze aanbesteding, te weten:
1. Verificatieverslag (OPTIONEEL)
2. (eventuele) Nota(s) van inlichtingen (*);
3. Verwerkersovereenkomst;
4. Programma van eisen;
5. Aanbestedingsleidraad, inclusief alle bijlagen die niet separaat benoemd zijn;
6. Algemene Inkoopvoorwaarden gemeente Sittard-Geleen
7. Uw inschrijving.

Voor zover bovengenoemde documenten met elkaar in tegenspraak zijn, geldt dat het hoger genoemde document prevaleert boven het lager genoemde.

Enkel het optionele verificatieverslag heeft een hogere randorde dan de Nota's van Inlichtingen. Hiervoor is gekozen aangezien een optionele verificatie pas plaatsvindt na het publiceren van de Nota's van Inlichtingen en in overleg met de voorgenomen gegunde inschrijver.

Percelen: P1 Instrumenten bewustwordingscampagne

Informatieveiligheid en Privacy

Beantwoord op: 3 okt. 2024

Ref.nr.
169

Onderwerp:
Vraag 101 - NvI

Vraag:
Vraag 101 Nota van Inlichtingen

In uw antwoord op onze vraag 101 geeft u aan dat opdrachtnemer persoonsgegevens verwerkt van medewerkers van opdrachtgever, bijvoorbeeld om hen toegang tot de e-learning omgeving te verstrekken en daarnaast verwerkt opdrachtnemer persoonsgegevens ten behoeve van het genereren van rapportages.

Dat opdrachtnemer persoonsgegevens verwerkt staat niet ter discussie. Daarover zijn partijen het eens. Echter is voor het kwalificeren van verwerker dan wel verwerkingsverantwoordelijke niet van belang of persoonsgegevens worden verwerkt. In beide rollen verwerkt men persoonsgegevens. Van belang is echter welke partij bepaalt wat voor soort persoonsgegevens worden verwerkt, wat het doel van die verwerking is en op welke wijze die verwerking plaatsvindt. De opdracht heeft niet als primair doel het verwerken van persoonsgegevens. De opdracht bestaat uit een verscheidenheid van zakelijke dienstverlening, zoals het verzorgen van trainingen, een e-learning applicatie ter beschikking stellen, voortgangsmetingen doen, meedenken over beleid in het kader van informatiebeveiliging etc. Aangezien onze opdracht niet primair betrekking heeft op het verwerken van persoonsgegevens, dienen wij te worden aangemerkt als zelfstandig verwerkingsverantwoordelijke, hetgeen in overeenstemming met de wet is. Wij verwijzen u in dit kader ook graag naar hoofdstuk 3.5.1, tweede alinea van de Handleiding Algemene verordening gegevensbescherming (Handleiding Algemene verordening gegevensbescherming (AVG) | Rapport | Rijksoverheid.nl).

Van belang is om te vermelden dat opdrachtnemer de gegevens enkel voor de overeengekomen diensten zal verwerken. Dat opdrachtnemer de gegevens alleen verwerkt binnen het kader van de opdracht, maakt niet dat sprake is van een verwerkersrelatie. Dan zou immers elke dienstverlener als verwerker kwalificeren hetgeen onjuist is. Wij zijn bereid met u aanvullende afspraken te maken betreffende gegevensverwerking (voor zover dit mogelijk is in het kader van onze dienstverlening en na onderling overleg over de eventuele voorwaarden tussen partijen) in een zelfstandig verwerkingsverantwoordelijken overeenkomst. In deze

verwerkingsverantwoordelijken overeenkomst kan worden opgenomen dat wij de gegevens enkel verwerken in het kader van de opdracht, hetgeen in lijn is met de juridische grondslag welke wij hebben conform AVG. Wij zijn echter niet bereid om met u een verwerkersovereenkomst te sluiten aangezien wij geen verwerker zijn bij de uitvoering van deze diensten. Het is daarom niet uit te leggen aan een toezichthouder (AP in dit geval) dat wij contractueel een rol aannemen welke niet in lijn is met onze wettelijke kwalificatie. Dit kan tot problemen met de toezichthouder.

Bent u gelet op bovenstaande bereid uw antwoord op vraag 101 te herzien en de verwerkersovereenkomst alsnog buiten toepassing te verklaren?

Antwoord:
Nee.

Percelen: P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op: 3 okt. 2024

Ref.nr.
170

Onderwerp:
Vraag 99 - NvI

Vraag:
Vraag 99 Nota van Inlichtingen

In uw antwoord op onze vraag 99 geeft u aan dat het soort audits dat wordt uitgevoerd afhankelijk is van de aanleiding. Mogelijk betreft dit audits in het kader van security incidenten.

Wij beschikken over een Informatie Privacy Management Systeem (hierna: IPMS) dat voorziet in een plan-do-check-act cyclus, waardoor continu aandacht bestaat voor informatiebeveiliging en privacy in de producten en diensten die wij onze klanten leveren. Dit systeem is gebaseerd op de ISO-27001-norm. Het IPMS wordt jaarlijks zowel intern (door onze eigen afdeling ICT) als extern beoordeeld door middel van audits. Dit zorgt ervoor dat wij inzicht hebben in de risico’s en kwetsbaarheden van onze IT-beveiliging en dat onze organisatie blijft voldoen aan de ISO-27001-normering. Door het overleggen van de ISO-verklaring kunnen wij aantonen dat wij onze IT-beveiliging op orde hebben. Dit neemt ons inziens het belang voor het uitvoeren van een audit weg. Wij verzoeken u daarom eis IS27 PvE te schrappen.

Indien u hiertoe niet bereid bent wensen wij dit artikel zo aan te passen dat daarmee uw auditrecht deels wordt beperkt. Wij stellen voor dat, indien u voornemens bent een audit uit te voeren, voorafgaand overleg plaatsvindt tussen partijen. Wij achten het daarnaast redelijk dat u slechts de mogelijkheid krijgt een audit uit te voeren als daarvoor gegronde redenen bestaan. Verder dient u de kosten van een dergelijke audit te dragen, aangezien u de audit wil (laten) uitvoeren.

Bent u gelet op het voorgaande bereid eis IS27 PvE te schrappen? Zo nee, bent u dan bereid om eis IS27 PvE als volgt op te nemen:

“ De aanbesteder heeft het recht een onafhankelijke externe auditor of haar interne auditafdeling een onderzoek te laten doen naar de naleving van de Overeenkomst, doch uitsluitend indien de aanbestder gegronde redenen heeft te vermoeden dat Opdrachtnemer in de nakoming van zijn verplichtingen tekortschiet. Een audit zal minimaal twee (2) weken vooraf aangekondigd worden voor zover dat redelijkerwijs mogelijk is. De kosten van de audit worden door de aanbesteder gedragen. Daarnaast vinden audits plaats tijdens normale kantooruren en tracht de aanbesteder de impact van audits op de bedrijfsvoering van Opdrachtnemer zoveel mogelijk te beperken.

Audits zijn daarnaast vertrouwelijk en worden uitgevoerd door een (externe) onafhankelijke auditor, niet zijnde een concurrent van Opdrachtnemer. Opdrachtnemer behoudt het recht voor de benoeming van een auditor of externe vertegenwoordiger te weigeren, die wordt beschouwd als een directe concurrent van Opdrachtnemer.

Opdrachtnemer verleent medewerking aan audits genoemd in deze bepaling door aan de auditor redelijke en noodzakelijke middelen ter beschikking te stellen. De audit wordt uitgevoerd in de vorm van het beantwoorden van schriftelijke vragen (verstrekt door de aanbesteder of een externe autoriteit), een interview met een lid van informatiebeveiligingspersoneel van Opdrachtnemer en/of een inspectie van beleidsdocumentatie op een geschikt kantoor. Ter voorkoming van onduidelijkheid; een dergelijke audit neemt niet de vorm aan van een analyse, test of op instructieve wijze toegang proberen te krijgen tot systemen, netwerken, lokalen of vertrouwelijke informatie van Opdrachtnemer .”

Antwoord:

Akkoord. Eis IS 27 wordt alsvolgd aangepast:

De aanbesteder heeft het recht een onafhankelijke externe auditor of haar interne auditafdeling een onderzoek te laten doen naar de naleving van de Overeenkomst, doch uitsluitend indien de aanbesteder gegronde redenen heeft te vermoeden dat Opdrachtnemer in de nakoming van zijn verplichtingen tekortschiet. Een audit zal minimaal twee (2) weken vooraf aangekondigd worden voor zover dat redelijkerwijs mogelijk is.

De kosten van de audit worden door de aanbesteder gedragen. Indien er sprake is van een toekenbare tekortkoming zijn de kosten voor de opdrachtnemer.

Daarnaast vinden audits plaats tijdens normale kantooruren en tracht de aanbesteder de impact van audits op de bedrijfsvoering van Opdrachtnemer zoveel mogelijk te beperken.

Audits zijn daarnaast vertrouwelijk en worden uitgevoerd door een (externe) onafhankelijke auditor, niet zijnde een concurrent van Opdrachtnemer. Opdrachtnemer behoudt het recht voor de benoeming van een auditor of externe vertegenwoordiger te weigeren, die wordt beschouwd als een directe concurrent van Opdrachtnemer.

Percelen: P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op: 3 okt. 2024

Ref.nr.
171

Onderwerp:
Vraag 83 - NvI

Vraag:
Vraag 83 Nota van Inlichtingen

In uw antwoord op vraag 83 geeft u aan dat er geen overzicht van een applicatielandschap is opgenomen. De reden dat opdrachtnemer deze vraag stelt, is omdat artikel 6.5 GIBIT 2023 ons verplicht tot het aanpassen van het applicatielandschap op onze kosten. Dit artikel is niet passend bij de soort dienstverlening die u uitvraagt. U vraag geen hardcore ICT prestatie uit, maar zakelijke dienstverlening, waarbij gebruik wordt gemaakt van een ICT prestatie. Gelet op uw antwoord gaan wij er vanuit dat er geen sprake is van aanpassingen aan uw applicatielandschap en artikel 6.5 GIBIT 2023 derhalve buiten toepassing kan worden verklaard. Kunt u dit bevestigen?

Antwoord:
Ja.

Percelen: P1 Instrumenten bewustwordingscampagne

Informatieveiligheid en Privacy

Beantwoord op: 3 okt. 2024

Ref.nr.
172

Onderwerp:
Vraag 80 - NvI

Vraag:
Vraag 80 Nota van Inlichtingen

In uw antwoord op vraag 80 geeft u aan niet akkoord te gaan met ons voorstel om persoons- en zaakschade te beperken aan de hand van een veelvoud van de opdrachtwaarde. U geeft daarbij aan dat het tekortschieten van leverancier tot grote schade bij de gemeente kan leiden. Onzes inziens wordt dan voorbij gegaan aan de soort schade zoals opgenomen in artikel 16.3 GIBIT 2023. Deze bepaling heeft immers enkel betrekking op persoons- en zaakschade. Daar zal niet snel sprake van zijn bij het uitvoeren van consultancydiensten (zeker niet aangezien grote delen van de opdracht mogelijk ook buiten locaties van opdrachtgever zullen worden verricht). Een dusdanig hoge beperking voor dergelijke schade achten wij derhalve niet passend. Indien sprake is van schade ten gevolge van dood en/of lichamelijk letsel is opdrachtnemer daarvoor, op grond van artikel 16.5, reeds onbeperkt aansprakelijk. Dan resteert enkel nog zaakschade. Wij voorzien niet dat een dergelijk hoge beperking vereist is voor enkel deze schade.

Wij stellen dan ook voor om de specifieke schade uit lid 3 samen te voegen met de ‘algemene’ schade en één aansprakelijkheidsbeperking daarvoor op te nemen. Dit zorgt ervoor dat e.e.a. overzichtelijk blijft en dat risico’s in het kader van de uitvoering van de opdracht evenwichtig verdeeld worden.

Kunt u gelet op bovenstaande instemmen met het opnemen van artikel 16.3 als volgt (ter vervanging van artikel 16.3 en 16.4 GIBIT 2023):

“ De in lid 1 bedoelde aansprakelijkheid voor schade (uit welke grond dan ook voortvloeiend), is beperkt tot drie maal de hoogte van de Jaarvergoeding per gebeurtenis voor het onderdeel van de ICT-prestatie waarin de oorzaak van de schade is gelegen. De totale aansprakelijkheid per jaar bedraagt evenwel nooit meer dan zes maal de Jaarvergoeding (ongeacht het aantal gebeurtenissen). Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.”

Hierin wordt reeds een uitbreiding van aansprakelijkheid per jaar

voorgesteld ten opzichte van het bestaande artikel 16.4. Kunt u instemmen met bovengenoemd tekstvoorstel?

Indien u hiermee niet kunt instemmen, dan verzoeken wij u de aansprakelijkheidsbeperking uit artikel 16.3 te verlagen naar een bedrag van € 500.000,-- per gebeurtenis en artikel 16.4 te vervangen voor het volgende:

“ De in lid 1 bedoelde aansprakelijkheid voor overige schade is beperkt tot vier maal de hoogte van de Jaarvergoeding per gebeurtenis voor het onderdeel van de ICT-prestatie waarin de oorzaak van de schade is gelegen. De totale aansprakelijkheid per jaar bedraagt evenwel nooit meer dan zes maal de Jaarvergoeding (ongeacht het aantal gebeurtenissen). Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.”

Kunt u hiermee instemmen?

Antwoord:
Nee.

Percelen:	P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op:	3 okt. 2024

Ref.nr.
173

Onderwerp:
Vraag 79 en vraag 100 NvI

Vraag:
Vraag 79 en vraag 100 (met betrekking tot Programma van Eisen D3) Nota van Inlichtingen

In uw antwoorden op vraag 79 en 100 geeft u aan niet akkoord te gaan met ons voorstel om een dossier aan te mogen houden. Ons is niet helder waarom u dat opdrachtnemer niet toestaat.

Zoals aangegeven is het verplicht op grond van (o.a.) wet en (beroeps) regelgeving verplicht voor opdrachtnemer om een dossier aan te houden van opdrachten die zijn uitgevoerd. Ons interne bewaarbeleid is gebaseerd op artikel 2:10 BW en wij houden onze dossiers aan in lijn met hetgeen de wet

daarover bepaalt. Daarnaast zijn er collega's welke zijn aangesloten bij bepaalde beroepsverenigingen, welke beroepsverenigingen op bepaalde dossiers kwaliteitsreviews moeten uitvoeren. Ook voeren wij intern kwaliteitsreviews uit op onze dossiers, zodat de dienstverlening doorlopend wordt beoordeeld en verbeterd.

Het is voor ons gelet op bovenstaande niet mogelijk om geen dossier aan te houden. Wij zijn hiertoe immers gehouden op grond van wet- en beroepsregelgeving. Wij verzoeken u daarom uw antwoord op vraag 79 en 100 te heroverwegen en ons alsnog toe te staan een dossier aan te houden, met daarin kopieën van relevante stukken. Uiteraard blijft dergelijke informatie onderworpen aan de geheimhoudingsverplichting. Kunt u hiermee instemmen? Zo nee, waarom niet?

Antwoord:
Opdrachtnemer mag een dossier aanhouden op grond van wet en (beroeps) regelgeving. Wij gaan ervan uit dat deze gegevens geen persoonsgegevens van de opdrachtgever bevatten.

Percelen:	P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op:	3 okt. 2024

Ref.nr.
174

Onderwerp:
Vraag 78 NvI

Vraag:
Vraag 78 Nota van Inlichtingen

In uw antwoord op vraag 78 geeft u aan niet akkoord te gaan met ons voorstel met betrekking tot artikel 18.6 GIBIT 2023. Wij kunnen ermee instemmen dat de boeteclausule in stand blijft, maar wij wensen de reeds verbeurde boete in mindering te brengen op de aanvullende schadevergoeding welke wij mogelijk nog verschuldigd zijn. Dat wil zeggen dat wanneer door de schending van de geheimhouding schade ontstaat bij opdrachtgever ter grootte van € 20.000,--, wij een boete verbeuren van € 10.000,-- en aanvullend schadevergoeding dienen te betalen van € 10.000,--. Dit is ook in lijn met hetgeen het Burgerlijk Wetboek daarover regelt. Deze regeling zorgt ervoor dat u te allen tijde uw schade vergoed zult krijgen in geval van schending van de geheimhouding.

Bent u bereid toe te staan dat opdrachtnemer de boete in mindering kan

brengen op een eventuele schadevergoeding? Zo nee, waarom niet?

Antwoord:
Nee, de boete en schadevergoeding hebben andere uitgangspositie.

Percelen: P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op: 3 okt. 2024

Ref.nr. 175
Onderwerp:
Vraag 77 - NvI

Vraag:
Vraag 77 Nota van Inlichtingen

In uw antwoord op vraag 77 geeft u aan niet akkoord te gaan met ons voorstel, omdat dit intellectuele eigendomsrechten van derden betreft en u dit derhalve niet kunt overzien. Wij kunnen ermee instemmen dat wij u zullen vrijwaren voor dergelijke schadeclaims, maar slechts voor zover deze schadeclaims aan ons toerekenbaar zijn. Kunt u bevestigen dat de vrijwaringsverplichting ingevolge artikel 20.5 GIBIT-2023 enkel geldt voor zover sprake is van een aan opdrachtnemer toerekenbare schending van intellectuele eigendomsrechten van derden. Kunt u dit bevestigen?

Antwoord:
Nee.

Percelen: P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op: 3 okt. 2024

Ref.nr. 176
Onderwerp:
Vraag 76 - NvI

Vraag:
Vraag 76 Nota van Inlichtingen

In uw antwoord op vraag 76 geeft u aan dat u niet akkoord gaat met het wederkerig maken van de opzeggingsmogelijkheid. Het is voor ons onduidelijk hoe de situatie er over vier jaar uitziet. Onze organisatie heeft te maken met diverse wet- en regelgeving waaraan moet worden voldaan. Wij wensen daarom de mogelijkheid te hebben de overeenkomst op te zeggen indien van ons niet in redelijkheid verwacht kan worden dat wij de overeenkomst langer voortzetten, bijvoorbeeld op grond van gedrags- en beroepsregels.

Wij stellen derhalve voor het volgende op te nemen in de overeenkomst:

" Het is partijen niet toegestaan de overeenkomst tussentijds door opzegging te beëindigen. Het is ieder der partijen echter toegestaan de overeenkomst te beëindigen in verband met toepasselijke wetgeving of gedrags- en beroepsregels, met inachtneming van een redelijke opzegtermijn."

Antwoord:
Nee.

Percelen: P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op: 3 okt. 2024

Ref.nr.
177

Onderwerp:
Vraag 75 - NvI

Vraag:
Vraag 75 Nota van Inlichtingen

Onder punt 75 NvI hebben wij gemotiveerd verzocht om het toevoegen van een artikel over de juistheid van informatie die u aan ons verstrekt. U geeft aan niet met ons voorstel akkoord te gaan, al is voor ons niet helder waarom u daarmee niet akkoord kunt gaan.

Voor ons is belangrijk dat wij ervan uit mogen gaan dat de informatie die we ontvangen hebben in het kader van de opdracht, juist is. Voor het correct kunnen uitvoeren van onze werkzaamheden is namelijk van belang dat de juiste, volledige en betrouwbare informatie is aangeleverd en wij daarvan uit mogen gaan. Dit leidt bovendien tot het beste resultaat – en de beste prijs - voor u, aangezien wij ons in dit geval volledig kunnen focussen op het uitvoeren van de overeenkomst, in plaats van dat wij extra uren aan het werk zijn om ook te controleren of alle ontvangen informatie correct is.

Dit neemt niet weg dat wij onze verantwoordelijkheid nemen om niet uit te gaan van informatie die klaarblijkelijk onjuist is. Wij verzoeken u het volgende artikel op te nemen in de overeenkomst:

"X.X Opdrachtnemer mag uitgaan van de juistheid, volledigheid en

betrouwbaarheid van de aan haar verstrekte informatie, ook indien deze van derden afkomstig is, tenzij en voor zover Opdrachtnemer weet of redelijkerwijs behoort te weten dat de informatie onjuist, onvolledig of onbetrouwbaar is."

Gaat u akkoord met toevoeging van dit artikel?

Antwoord:
Ja, dit heeft echter enkel betrekking op de uitvoering van de opdracht.

Percelen: P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op: 3 okt. 2024

Ref.nr. 178

Onderwerp:
Nota van inlichtingen Ref.nr. 25 Onderwerp: PVE IN1

Vraag:
Uw antwoord:
De aan te bieden content voor e-learning modules moet geïmporteerd kunnen worden in het LMS van AFAS en moet derhalve voldoen aan het volgende bestandsformat SCORM.

Onze vraag:
Tegenwoordig worden koppelingen vaak op basis van LTI gemaakt ipv SCORM. Dit biedt diverse voordelen. Wordt LTI ondersteund door het AFAS LMS en mag de content ook op basis van LTI aangeboden worden?

Antwoord:
Ja.

Percelen: P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op: 3 okt. 2024

Ref.nr. 179

Onderwerp:
Nota van inlichtingen Ref.nr. 14 Onderwerp: Aanbestedingsleidraad pag 5, 1.1.3 Scope

Vraag:
Uw antwoord:
Bij aanvang opdracht hebben de gemeenten Sittard-Geleen, Heerlen en Maastricht AFAS. Gemeente Kerkrade en Stein maken momenteel geen gebruik van een LMS.

Onze vraag:
Dit zou betekenen dat Sittard-Geleen, Heerlen en Maastricht op het AFAS LMS gaan draaien en Kerkrade en Stein op ons LMS.

In het programma van eisen worden echter diverse eisen (D1-D10) gesteld aan de rapportage mogelijkheden. Bijvoorbeeld: “ Aanbestedingseisen IM&ICT Data, Stuurinformatie en rapportages (algemene info)”.

Bent u akkoord dat eisen gesteld aan het LMS ook van toepassing zijn op het LMS. En als het AFAS LMS gebruikt wordt dat de eisen van toepassing zijn op het AFAS LMS waar de opdrachtnemer geen invloed op heeft?

Antwoord:
Ja.

Percelen: P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op: 3 okt. 2024

Ref.nr. **Onderwerp:**
180 Nota van inlichtingen Ref.nr. 108 Onderwerp: Aanbestedingsleidraad bewustwording. 1.3.3. Scope

Vraag:
Uw antwoord:
Beide. Verwerkt in de leeromgeving (E-learning) en als aparte dienstverlening.

Onze vraag:
Hoeveel phishingtests wilt u per jaar per gemeente uitvoeren?

Antwoord:
Gemiddeld 1.

Ter verduidelijking: het betreft twee verschillende soorten dienstverlening.
1. Als training in de leeromgeving (E-learning)
2. Als Social engineering (scan)*

*Hiervoor is een nieuwe kostenpost toegevoegd op het prijzenblad.

Percelen: P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op: 3 okt. 2024

Ref.nr. **Onderwerp:**

181 Vervolgvraag NvI 1 ref 5:

Vraag:
Kunt u bevestigen dat deelnemers in het prijzenblad een prijsopgave doen voor 5 fysieke trainingen per jaar op locatie van minimaal 4 uur, voor 12 deelnemers?

Antwoord:
Correct. Let op: het betreffen fictieve aantallen. Daadwerkelijke aantallen zijn afhankelijk van de behoefte van de opdrachtgever.

Percelen: P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op: 3 okt. 2024

Ref.nr. **Onderwerp:**
182 Vervolgvraag NvI 1, ref 124:

Vraag:
Kunt u bevestigen dat deelnemers in het prijzenblad een prijsopgave doen voor 2 maal een telefonische social engineering activiteit waarbij er 8 uur lang naar verschillende medewerkers gebeld gaat worden? Dus exclusief de inzet voor rapportage een aanbevelingen aan de kant van de leverancier? En dat dit dus om de twee jaar voorzien wordt?

Antwoord:
Dit is een fout in het prijzenblad. De fictieve afname is 1 scan per jaar.

Het betreft een volledige scan. Dat betekent: eventuele voorbereiding, het voeren van telefoongespreken en het opleveren van een rapportage met aanbevelingen.

Percelen: P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op: 3 okt. 2024

Ref.nr. **Onderwerp:**
183 Vervolgvraag NvI 1, ref 2:

Vraag:
Is aanbestedende dienst bereid om na gunning, in nader overleg met leverancier, afspraken te maken over het facturatieschema, aangezien er geen sprake is van een concept overeenkomst?

Antwoord:

Ja, in lijn met de GIBIT artikel 11.1 tot en met 11.12.

Percelen: P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op: 3 okt. 2024

Ref.nr. 184

Onderwerp:
Vervolgvraag Nvl 1, ref.nr 117

Vraag:
Er is sprake van 1 LMS per gemeente. Gemeente Kerkrade en Gemeente Stein hebben momenteel geen LMS.

Gaan gemeente Kerkrade en gemeente Stein nog het LMS van AFAS aanschaffen? Zo ja, per wanneer zal dit beschikbaar zijn?

Zo nee, is het de bedoeling dat de leverancier voor gemeente Kerkrade en gemeente Stein een LMS verzorgt en kan de aanbestedende dienst aangeven welk budget hiervoor beschikbaar is?

Antwoord:
Ad 1. Dit is onbekend.
Ad. 2 Ja, de opdrachtnemer moet een LMS verzorgen. De eventuele kosten moeten verwerkt zijn in de licentiekosten.

Ter verduidelijking: het moet mogelijk zijn om de E-learning applicatie te koppelen met de (AFAS) LMS van de opdrachtgever, maar een opdrachtgever kan er ook voor kiezen om deze koppeling niet te maken. In dat geval moet de LMS van de opdrachtnemer ingezet worden.

Percelen: P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op: 3 okt. 2024

Ref.nr. 185

Onderwerp:
vervolgvraag NvI 1, ref 25

Vraag:
Aanbestedende dienst vraagt een e-learning platform uit. Leverancier biedt een e-learning platform als SaaS oplossing inclusief de content en de volledige dienstverlening zoals uitgevraagd in uw scope.

Waarom wenst u de leerinhoud dan te importeren op het LMS van AFAS voor de 3 gemeenten die van AFAS LMS gebruik maken door middel van SCORM in plaats van LTI? Dit belemmert ons inziens ook de rapportagemogelijkheden? Wat is hier naar uw mening het voordeel van

SCORM?

Onze ervaring leert dat het importeren van deze specifieke content achterhaald is en de meeste gemeenten nu gebruik maken van een LTI koppeling, aangezien het ook een SaaS oplossing betreft waarbij u als gemeente volledig ontzorgd wil worden en dit meer betekent dan louter en alleen de contentleverancier te zijn.

Antwoord:
Het is toegestaan om, naast SCORM, gebruik te maken van een LTI koppeling.

Percelen:	P1 Instrumenten bewustwordingscampagne Informatieveiligheid en Privacy
Beantwoord op:	3 okt. 2024