

Nota van Inlichtingen 2 EU Aanbesteding Financieel systeem Gooi en Vechtstreek d.d. 14-01-2022

Tenderd kenmerk: 338617 ref.nr : 21.0007821

95	Individueel	In uw NV11 heeft u geantwoord:..... .	In verband met concurrentiegevoelige informatie heeft vraagsteller verzocht deze vraag individueel te beantwoorden. De vraag betreft een wedervraag op informatie die in de eerste nota van inlichtingen met iedere potentiële inschrijver is gedeeld. De vraagsteller moet gezien de antwoorden van de Regio in deze eerste nota van inlichtingen haar mogelijkheden tot het kunnen indienen van een regelmatige inschrijving heroverwegen. Dit in verband met een tekort aan functionaliteiten in de door haar aangeboden software oplossing. De Regio is daarom van mening dat de vraag en het antwoord geen informatie bevat waarmee het gelijkheidsbeginsel wordt overtreden. Overige potentiële inschrijvers worden niet benadeeld door het onthouden van deze vraag en het antwoord.
96	Verzoek tot aanpassen geplande data demonstraties	De experts die Inschrijver beoogt in te zetten bij het implementatietraject zijn vanwege geplande vakanties niet beschikbaar op de geplande data, te weten 07.02.2022 en 08.02.2022. Is Opdrachtgever bereid, indien Inschrijver de mogelijkheid krijgt om een presentatie en demonstratie te geven, om een datum en tijd te kiezen voor een demonstratiesessie op een later tijdstip, vanaf 17.02.2022? De voorkeur van Inschrijver gaat uit naar 17.02.2022 of 18.02.2022. Gezien het krappe planningsschema dat er vanaf de	Zoals u terecht constateert hebben wij in eis 29 duidelijk aangegeven dat de presentatie (mede) gehouden moet worden door de implementatieleider. Wij hechten daar groot belang aan. U geeft aan op de geplande data niet aan deze eis te kunnen voldoen. Omdat de Regio hecht aan maximale concurrentie is zij ondanks agenda technische problemen aan onze zijde (in zoverre) bereid op uw voorstel in te gaan, dat aan u alleen de mogelijkheid wordt geboden uw presentatie 's te mogen verzorgen op de ochtend van 17 februari 2022.

		publicatie van de NvI2 ligt, verzoekt Inschrijver Opdrachtgever om deze vraag zo spoedig mogelijk (tussendoor) te beantwoorden.	Voor de Regio is dit de enige agenda technische mogelijkheid om op een juiste wijze als geheel beoordelingsteam de totale beoordeling uiterlijk op maandag 21 februari 2022 af te kunnen ronden en daarmee de planning voor alle partijen gestand te kunnen doen.
97	PvE eis 4	Wat wordt bedoeld met 'workflow routes'? Heeft Opdrachtgever hiervan enkele voorbeelden of zelfs een uitputtende lijst?	De "workflow routes" zijn niet expliciet aan te duiden met een uitputtende lijst. Een voorbeeld hiervan zijn een verplichtingenadministratie die in veel gevallen over twee (boek)jaren verdeeld kan/moet worden. Denk hierbij ook aan de debiteuren- en crediteurenadministratie, activamodule of vlottende activa en passiva. Zie ook ons antwoord op vraag 14.
98	NvI1 vraag 82	Opdrachtgever suggereert een instelling waarmee kan worden voorkomen dat binnen de organisatie van Opdrachtgever medewerkers gebruikmaken van een outdated browser. De software van Inschrijver zal deze controle niet uitvoeren echter functioneert de oplossing dan niet/niet goed en zal de gebruiker dit in voorkomende gevallen merken. Inschrijver acht het logisch dat Opdrachtgever, indien het wenst dat niet naar de oplossing van Inschrijver mag worden gegaan binnen haar netwerk met een outdated browser, zelf zorgt draagt voor blokkade van deze browser. Kan Opdrachtgever instemmen met deze werkwijze?	De Opdrachtgever kan hiermee instemmen.
99	NvI1 vraag 79	Opdrachtgever beantwoordt dat historische gegevens inzichtelijk moeten blijven middels haar huidige financiële systeem. Bedoelt Opdrachtgever daarmee dat deze zelf zorgt draagt voor licenties en beheer voor een eventueel archief binnen haar eigen omgeving?	Ja, dat bedoelt Opdrachtgever hiermee. Zie verder ook de antwoorden op vraag 28 en 79.

100	NvI1 vraag 72	"Opdrachtgever beantwoordt dusdanig dat ze blijkbaar aangeeft dat het toevoegen van haar ISO 27001 en NEN 75100 certificeringen en de SofA niet voldoende is. Het antwoord suggereert eigenlijk dat er meer nodig is, maar het wordt niet concreet gemaakt wat er toegevoegd moet worden bij de inschrijving of aan welke specifieke eisen voldaan moet worden bij die inschrijving. Kan Opdrachtgever alsnog toelichten wat er extra nodig is bij de inschrijving?"	De ISO27001 en NEN7510 certificering en de SofA zijn de basis om aan de gestelde eis te voldoen. Aanvullende certificeringen (zoals bijvoorbeeld ISO27701) op dit gebied kunnen een meerwaarde zijn.
101	NvI1 vraag 67 punt 4	Kan Opdrachtgever op deze vraag concreter antwoord geven zodat inschrijver kan bepalen welke extra securityvoorzieningen benodigd zijn binnen de inschrijving?	De invulling van de periodieke pentest en kwetsbaarheidsscans is aan de opdrachtnemer. Dit kan dus een permanente oplossing zijn of een periodiek uitgevoerde scan. Zie ook ons antwoord op vraag 105 (meer specifiek het onderdeel vraag 65)
102	NvI1 vraag 67 punt 3	"Opdrachtgever kan voor ogen hebben voor eigen rekening pentesten en scans op het platform te laten uitvoeren van Inschrijver. Opdrachtgever kan ook bedoelen dat Inschrijver de kosten en technisch gezien de inrichting daarvan, overlaat aan Inschrijver. a) Bedoelt Opdrachtgever dat het zelf scan- en pentesten zal laten uitvoeren voor eigen rekening? b) Zo ja, hoe ziet Opdrachtgever dit voor zich? c) Bedoelt Opdrachtgever dat Inschrijver dit niet zelf faciliteert maar juist verwacht dat Inschrijver dit op haar platform specifiek voor RGV moeten laten uitvoeren en de kosten op nacalculatie in rekening kunnen worden gebracht?"	De bij eis 45 genoemde pentest en kwetsbaarheidsscans dient minimaal eenmaal per jaar te worden uitgevoerd door de opdrachtnemer. Dit is inderdaad voor eigen rekening. Volledigheidshalve wordt nog het volgende opgemerkt. Voor de bij eis 44 genoemde audit ligt dit anders. Deze kan op verzoek van de Regio worden uitgevoerd door een derde partij. De kosten voor de audit liggen dan bij de Regio. Eventueel aangetoonde gebreken zullen dan wel door de opdrachtnemer op eigen kosten moeten worden opgelost

103	NvI1 vraag 67 punt 1	Of Opdrachtgever vereist dat de Vervoer BV een losstaande oplossing dient te zijn of geïntegreerd mag worden binnen het Regio platform heeft veel gevolgen. Inschrijver verzoekt Opdrachtgever daarom een concreter antwoord te verstrekken dat nu al tot juiste berekeningen gaat leiden. Kan Opdrachtgever hierop concreet antwoorden?	Vervoer BV dient een losstaande omgeving te hebben waarbij wel gebruik wordt gemaakt van dezelfde software versies. Het Prijzenblad d.d. 17-12-2021 is daarop gewijzigd wat betreft de implementatiekosten. Wij gaan er verder vanuit dat de licentie en trainingskosten van gelijke hoogte zijn, aangezien van dezelfde software gebruik wordt gemaakt.
104	NvI1 vraag 26	Opdrachtgever beantwoordt deze vraag onder andere met “later eventueel ook toegepast worden voor eventuele cloud services en / of security monitoring”. Dat is voor Inschrijver zeer breed en onduidelijk waardoor Inschrijver over mogelijkheden, kosten, etc. nog geen uitspraken kan doen. Kan Opdrachtgever hiermee instemmen?	Het faciliteren van SSO via deze koppeling is een duidelijk afgebakende voorwaarde. Het is uiteraard vanzelfsprekend dat op eventuele toekomstige wensen door Inschrijver nu geen concreet voorstel kan worden gedaan. Deze maken dan ook geen onderdeel uit van deze uitvraag.
105	NvI1 vragen 43, 45, 54, 60, 65, 67, 76, 77, 80, 81	"Al deze vragen beantwoordt Opdrachtgever met de strekking “concrete afspraken hierover zullen tijdens het opmaken van de Service Level Agreement moeten worden gemaakt”. Inschrijver voorziet dat dit (grote) gevolgen voor “wat is mogelijk vanuit Inschrijver” en “welke extra kosten zijn daarmee gemoeid” kan hebben. Is het aldus toegestaan dat Inschrijver tijdens deze latere bespreking over de invulling: 1) Niet mee kan gaan met bepaalde wensen/eisen die dan volgen en nu nog niet bekend zijn? 2) Waar deze wensen/eisen impliceren dat de (jaarlijkse) kosten wijzigen, deze dan via een additioneel budget vanuit Opdrachtgever worden ingevuld?"	U suggereert dat de Regio andere eisen gaat stellen dan de minimum eisen die in het Offerteaanvraag document staan opgenomen. Dit is een misvatting. Uw inschrijving dient te voldoen aan de (minimum) eisen die opgenomen staan in het Offerteaanvraag document. Voor een juiste vergelijking van de inschrijvingen dient u te voldoen aan deze eisen en geeft u de daaraan (naar uw eigen inzicht) verbonden kosten van op. De aan de SLA verbonden kosten worden derhalve geacht meegenomen te zijn in uw prijsopgave. Mochten er gedurende de looptijd van de overeenkomst extra wensen zijn dan spreekt het voor zich dat Opdrachtnemer hiervoor nadien additionele kosten in rekening mag brengen.

			Concrete afspraken wordt in deze context dan ook bedoeld als een nadere precisering van de uitwerking van deze diverse minimum eisen in de SLA. Hieronder gaan wij nogmaals specifiek in op de in uw vraag herhaalde vragen uit de NVI 1: <u>Vraag 43 onderhoudsvenster</u> Het betreft hier eis 36. Aangegeven in de beantwoording is dat ruim op tijd én van te voren onderhoudsvensters aangekondigd moeten worden. Hieronder moet een termijn van 5 werkdagen (een werkweek) worden verstaan. Dat u niet exact een gelijke werkwijze hanteert is geen knock-out. Uw werkwijze zal hier echter wel minimaal aan moeten voldoen. Uw kostenopgave kunt u hierop afstemmen. <u>Vraag 45 verplichte ondersteuning functionaliteiten v.h. systeem.</u> Het betreft hier eis 15. Het antwoord op deze vraag lijkt ons helder en eenduidig. Wij geven specifiek nog aan dat hier bij de implementatie extra rekening mee moet worden gehouden. Ons antwoord was verder bevestigend. Uw kostenopgave kunt u hierop afstemmen. <u>Vraag 54 logboeken</u> Het betreft hier eis 41. Ons antwoord was bevestigend (interpretatie was correct). Hier geldt met name dat over de werkwijze tussen beide organisaties afspraken gemaakt moeten worden (een nadere precisering). Uw kostenopgave kunt u hierop afstemmen.
--	--	--	---

			<u>Vraag 60 informatie bij aanval/security breach</u> Het betreft hier eis 50. De Opdrachtgever stelt geen specifiek inhoudelijke eisen. Per scenario kan de benodigde data verschillen. Doelstelling van Opdrachtgever is om in dergelijke situaties zoveel als mogelijk logs en data te kunnen verkrijgen om te kunnen bepalen of er (daadwerkelijk) sprake is geweest van inzage en/of diefstal van datagegevens. Concrete afspraken wordt in deze context dan ook bedoeld als een nadere precisering van de uitwerking van deze scenario's in de SLA. <u>Vraag 65 rapportage kwetsbaarheden / scans / pentesten</u> Het betreft hier eis 46. In deze eis worden door Opdrachtgever geen specifieke inhoudelijke eisen gesteld aan deze rapportages. Alleen in eis 45 wordt een minimale frequentie geëist van 1 x per jaar. Gevraagd in deze vraag is overigens naar de doelstelling van deze rapportages. Hierop is geantwoord "gericht op het aantoonbaar in control zijn van bedrijfskritieke processen". Samen met de inschrijver zal vastgesteld worden hoe deze rapportage vorm moet krijgen (een nadere precisering). Tegen deze achtergrond (1 x per jaar en beantwoordend aan de doelstelling van de rapportage) is het voor u mogelijk om op dit onderdeel uw kostenopgave hierop af te stemmen. De kosten worden geacht deel uit te maken van, of de licentiekosten, of worden ondergebracht bij minimaal benodigde (door u aanbevolen) jaarlijkse ondersteunende uren. Alle overige (extra) door de Regio gewenste/geïnitieerde rapportages zijn additioneel.
--	--	--	---

			<u>Vraag 67 pentesten en kwetsbaarheden scan</u> Het betreft hier eis 45. We verwijzen u naar onze toelichting hiervoor bij vraag 65 <u>Vraag 76 kpi's</u> Het betreft hier (een onderdeel van) eis 33. In ons antwoord op deze vraag hebben wij er reeds 3 benoemd. Uitgewerkt in eisen 34 en 35 <u>Vraag 77 kpi's helpdesk?</u> Het betreft hier (een onderdeel van) eis 33. Zie hiervoor bij vraag 76. <u>Vraag 80 responstijden helpdesk</u> Het betreft hier eis 14. Het is gebruikelijk om een tabel op te stellen waar op basis van urgentie en impact een prioriteit uit naar voren komt voor een incidentafhandeling. Afhankelijk van de bepaalde prioriteit volgt dan een reactie- en een oplostijd. Dit zou vanuit het perspectief van Opdrachtgever kunnen zijn: P1 -> Binnen 1 uur reactie, binnen 4 uur opgelost P2 -> Binnen 2 uur reactie, binnen 8 uur opgelost P3 -> Binnen 8 uur reactie, binnen 24 uur opgelost P4 -> Binnen 8 uur reactie, binnen 10 werkdagen opgelost Wat Opdrachtgever betreft zijn deze waarden en de onderliggende definities richtlijnen die tijdens de SLA onderhandeling definitief worden vastgelegd. <u>81 concretisering onderhoud aan het systeem</u> Het betreft hier eis 11. In ons antwoord hebben wij verwezen naar ITIL, BSL, ASL. Deze 'frameworks' beschrijven in een duidelijke context wat onder deze definities dient te worden verstaan.
--	--	--	--

			Het is lastig om als Opdrachtgever dit concreter te maken. De gehanteerde termen zijn algemeen bekende begrippen als het gaat om onderhoud en beheer van een applicatie. Kortgezegd komt het erop neer dat de Opdrachtnemer er voor zorg draagt dat de applicatie beschikbaar is, goed presteert en up-to-date blijft. En dat hiervoor geen aanvullende kosten worden doorbelast aan Opdrachtgever. Een constructie die standaard is in de wereld van SaaS, dit in tegenstelling tot een applicatie die op traditionele wijze op de infrastructuur van de opdrachtgever zou worden geïnstalleerd. De genoemde methodieken (of een combinatie daarvan) kunnen door de opdrachtnemer worden gebruikt. Wat Opdrachtgever betreft zijn deze methodieken en de onderliggende definities richtlijnen die tijdens het opstellen van de SLA definitief worden vastgelegd.
106	NvI1 vraag 61	Inschrijver leest een fout in de vraag die door haar is gesteld. Inschrijver bedoelt te vragen of Opdrachtgever het eens is dat programma van eisen eis 53 impliceert dat Inschrijver moet voorzien in een SIEM met een SOC. Inschrijver suggereert met haar vraag 61 echter te verwijzen naar dat Opdrachtgever deze SIEM oplossing levert en dat is incorrect omdat het immers het platform van inschrijver betreft dat op deze manier beveiligd wordt. Blijft daarmee het antwoord van Opdrachtgever hetzelfde?	Het antwoord blijft hetzelfde. Het ligt inderdaad voor de hand dat de opdrachtnemer voorziet in een SIEM en een SOC om aan eis 53 te voldoen. Eis 61 moet hier los van worden gezien. Dit betreft medewerking aan een kwetsbaarheden scan vanuit de Regio. Een scan uitgevoerd vanuit de Regio zal niet op de interne infrastructuur van de opdrachtnemer worden uitgevoerd maar heeft dan betrekking op het voor ons wel bereikbare deel van de configuratie.
107	NvI1 vraag 44, 68	Opdrachtgever beantwoordt deze vraag niet met een policy waaraan voldaan moet worden. Kan Opdrachtgever alsnog de policy toevoegen waaraan voldaan moet worden?	Inloggen op de applicatie dient plaats te vinden op basis van het Active Directory account van de betreffende medewerker op het Regio netwerk voor middel van SSO. Het is dus niet wenselijk dat medewerkers een apart account specifiek voor de aangeboden applicatie krijgen.

			De algemene doelstelling is om applicaties voor medewerkers bereikbaar te maken via eenmalig inlog op het Regio netwerk.
108	NvI1 vraag 33, 71	"Op een gedeelte van de totaaloplossing die Inschrijver voor ogen heeft, kan niet aan de NEN 7510-eis worden voldaan. Dit reden hiervoor is dat dit gedeelte van de oplossing staat in de cloud van Amazon Web Services (AWS) en deze cloud voldoet niet aan Nederlandse NEN-normeringen. Dit betekent niet dat het platform niet aan de hoogste eisen voldoet, maar er wordt hier gevraagd om een formele certificering en die is niet bij alle softwareleveranciers zo logisch als voor Opdrachtgever. Inschrijver kan met haar eigen platform en het belangrijkste deel van de financiële oplossing NEN 7510 certificering aantonen. a) Is Opdrachtgever bereid haar NEN 7510-eis alsnog te laten vervallen? Als alternatief kan voor de onderdelen waar niet kan worden voldaan aan de NEN 7510-eis, wel het certificaat ISAE-3402 Type II worden overlegd. b) Indien nee, dan moet Inschrijver voor het afhandelen van de binnengekomen inkoopfacturen bij het in stand houden van de NEN 7510-eis terugvallen (zie ook eerdere vraag op basis van NvI 1 vraag 62) op de installatie van Scan Sys IC en Exact Synergy binnen de huidige omgeving van Opdrachtgever. Inschrijver ziet hier ruimte voor vanwege eis 62. Is deze interpretatie van de eisen 62 en 71 correct?"	a.) De Regio zal i.v.m. haar werkzaamheden de NEN 7510 eis niet kunnen laten vervallen. Er komen situaties voor bij onze rechtstreekse dienstverlening aan burgers waarbij op facturen die in rekening worden gebracht persoonsgegevens komen te staan. Deze facturen worden verwerkt in het financieel systeem. b.) Zoals aangegeven in ons antwoord bij vraag 62 heeft het de voorkeur om te werken met een software oplossing die zelfstandig beschikt over een factuurherkenning- en/of accorderingsmodule (eis 67). Uw interpretatie van eis 62 is correct. Indien de software oplossing niet zelfstandig beschikt over deze functionaliteiten dan dient deze alsnog gerealiseerd te worden in een voor de Regio meest efficiënte en praktisch werkbaar oplossing.
109	NvI1 vraag 32, 70	"Opdrachtgever benoemt nu NEN—ISO 16175-1 als vervangende norm van NEN2082. Niet alle softwareleveranciers die Inschrijver betreft bij haar aanbieding voldoen aan deze NEN-norm. Wel leest Inschrijver verderop in uw antwoord dat logging moet	In de beantwoording van vraag 32 uit de eerste NvI staat aangegeven, citaat: " <i>Uw applicatie dient derhalve conform de NEN-ISO 16175-1 of op een andere aantoonbare manier data te loggen (copy certificaat van uw Statement of Applicability SoFa)</i> ".

		plaatsvinden op aanmaken, wijzigen en/of verwijderen van informatie. Aan deze eis kunnen de betreffende leveranciers wel voldoen. Het is Inschrijver onvoldoende duidelijk hoe te handelen als geen formeel certificaat NEN-ISO 16175-1 kan worden bijgevoegd. a) Volstaat de toezegging van Inschrijver dat deze logging wel plaatsvindt en op punten zelfs gespecificeerd ingeregeld kan worden? b) Indien niet, wat verstaat Opdrachtgever dan onder “of een andere aantoonbare manier data te loggen”? c) Is Opdrachtgever bereid deze formele eis van certificering te laten vervallen?"	Opdrachtgever kan niet bepalen of alle onderaannemers ook zelfstandig aan de gestelde certificeringsnormen (moeten) voldoen of dat de certificering van de hoofdaannemer voldoende is. Een formele toezegging door de hoofdaannemer is in deze daarom vereist en voldoende om aan te tonen dat deze logging plaatsvindt.
110	NvI1 vraag 62	Inschrijver leest deze eis zo dat de bestaande oplossingen Scan Sys ImageCapture en Exact Synergy Enterprise binnen de omgeving van Opdrachtgever actief kunnen/moeten blijven, wanneer Inschrijver een financieel systeem levert voor de overige functionaliteit en een koppeling naar Synergy en Scan Sys IC realiseert voor het binnenhalen van de geautoriseerde inkomende facturen. Interpreteert Inschrijver dat correct?	Het is correct dat de bestaande oplossingen (Scan Sys en Synergy) actief kunnen blijven binnen de omgeving van opdrachtgever, het is dan vereist dat een koppeling wordt gemaakt vanuit het nieuwe financiële systeem naar deze oplossingen. Het is echter niet een eis dat deze oplossingen (Scan Sys en Synergy) actief blijven binnen de omgeving van de opdrachtgever, deze oplossingen kunnen ook vervangen worden door soortgelijke oplossingen van inschrijver.
111	Demonstratie	Inschrijver is voornemens de oplossing tijdens de voorgestelde demo in februari, mits deze daarvoor in aanmerking komt, vanaf een lokaal systeem te presenteren. Daarmee ligt de focus op de inhoudelijke oplossing in plaats van het reeds geheel inrichten van een cloudoplossing voor RGV en SSO en MFA eisen. Uiteraard kan het benaderen van de oplossing in de cloud wel worden gepresenteerd, maar de ingerichte financiële administratie staat dan nog wel lokaal. Is Opdrachtgever hiermee akkoord?	Het is akkoord om bij de presentatie gebruik te maken van een lokaal systeem. Voorwaarde is wel dat de getoonde functionaliteit en prestaties identiek zijn aan die van de daadwerkelijk aangeboden SaaS oplossing.

112	NvI1 vraag 39	Volstaat het om de genoemde ISO27001 en NEN7510 certificaten en bijbehorende SofA aan de inschrijving toe te voegen?	Wij vermoeden dat u eis 39 bedoeld i.p.v. vraag 39. Ja, dat volstaat.
113	NvI – Pagina 12/13 - Vraag 33 mbt Eis 39	"In het antwoord van de Opdrachtgever staat "in hoeverre de controls van NEN 7510 feitelijk ook kunnen steunen op de door inschrijver aangeboden controls zal bij vervolg moeten worden gecheckt". Kunnen wij hieruit concluderen dat het voor Inschrijver afdoende is om ISO27001-gecertificeerd te zijn en voor de aanvullende eisen vanuit NEN7510 afdoende beheersmaatregelen te hebben geïmplementeerd die bij vervolg worden gecheckt?"	Zie ook vraag 109. Ook hier maken wij de opmerking: 'Opdrachtgever kan niet bepalen of alle onderaannemers ook zelfstandig aan de gestelde certificeringsnormen (moeten) voldoen of dat de certificering van de hoofdaannemer voldoende is.' Gelet op vraag 33 lijkt het erop dat Inschrijver de applicatie host bij Microsoft op het Azure platform. Vanuit Microsoft is hier aanvullende informatie over te vinden: https://pulse.microsoft.com/nl-nl/work-productivity-nl-na/fa2-in-de-cloud-voldoen-aan-nen-7510-en-nta-7516/ Mede op basis hiervan willen wij bevestigend antwoorden op deze vraag.