

Nota van Inlichtingen - EA Reisagent - Erasmus MC

Nr.	Uw vraag heeft betrekking op	Verwijzing naar tekst in aanbestedingsdocumenten (bijlage en paginanummer, tekstpassage)	Concrete vraag	Antwoord
1	Algemeen	-	Wij danken u voor de inhoudelijke toelichting op het aantal geschatte dienstreizen. Zou u ons ook een inschatting kunnen geven op het percentage online boekingen per jaar?	Vermoedelijk gaat het om meer dan 80% van de boekingen. Aangezien dit een nieuwe dienstverlening betreft, kunnen we hier echter geen garanties over geven.
2	Algemeen	-	Wij danken u voor de inhoudelijke toelichting op het aantal geschatte dienstreizen. Zou u ons ook inzicht kunnen verschaffen in de meest geboekte bestemmingen? En een eventuele verdeling tussen continentale en intercontinentale reizen?	Het Erasmus MC heeft geen goed overzicht van deze bestemmingen. Op basis van een telling zijn het aantal geschatte dienstreizen bepaald. Mocht Inschrijver toch een indicatie willen, dan dient rekening gehouden te worden met 50% continentaal en 50% intercontinentaal.
3	Offerteleidraad	Hoofdstuk 5. Eigen verklaring	Het valt inschrijver op dat dat inschrijvers geen lid hoeven te zijn van de ANVR. Om de elementen van de dienstverlening die specifiek zijn voor deze sector te waarborgen stellen wij u voor dit wel verplicht te stellen gezien het een geldende norm is in onze branche en het u meer zekerheid biedt. Gaat u daar mee akkoord?	Wij passen de aanbesteding niet aan op dit onderdeel.
4	Nvl	Vraag 32 (over eis 88)	Inschrijver is tevreden met het aanpassen van eis 78, echter blijft eis 88 na het beantwoorden in NV11 staan. Deze controle heeft (in de huidige context) het doel om te controleren of inschrijver zich in heeft gespannen de voordelen en inkomsten terug te vloeien naar de Opdrachtgever. U geeft te kennen bereid te zijn de kosten voor deze controle te dragen, echter verandert dit niet dat dit een onevenredig zware eis is, waar inschrijver niet aan kan voldoen. Het eisen van een Assurance rapport (ISAE 3402, type 2) is uiterst ongebruikelijk in de branche. Grote accountantskantoren zoals Deloitte hebben hier zelfs geen standaardproces voor! Bent u na het aanpassen van eis 78, bereid eis 88 (controle van eis 78) te laten vervallen? Zo niet, staat u open om tijdens implementatie gezamenlijk te zoeken naar een andere manier om te controleren dat inschrijver zich heeft ingespannen om de voordelen en inkomsten terug te vloeien naar de Opdrachtgever? We vragen u op korte termijn te antwoorden op deze vraag, aangezien dit bepalend is voor het wel/niet inschrijven.	Het Erasmus MC laat deze eis vallen.
5	Nvl	Vraag 29 (over eis 69)	Inschrijver is blij dat u bereid bent eis 69 aan te passen. Helaas is het (zoals in vraag 29 aangeven) technisch niet mogelijk om de CO2-uitstoot voor autohuur aan te geven. In de huidige eis geeft u aan dat dit achteraf mag, maar ook dat is technisch simpelweg niet mogelijk. Bent u bereid om deze eis te laten vervallen?	Het Erasmus MC zal deze eis laten vervallen.

Nr.	Uw vraag heeft betrekking op	Verwijzing naar tekst in aanbestedingsdocumenten (bijlage en paginanummer, tekstpassage)	Concrete vraag	Antwoord
6	Nvl	Vraag 51 (over eis 20)	Single sign on is een totale nieuwe eis t.o.v. vorige versie van de eis, die in onze optiek helemaal niet van toepassing is. Voldoet inschrijver met een login met e-mail en wachtwoord (zoals gevraagd in vraag 17)?	Ja, de eis is aangepast.
7	PvE	Eis 52	Inschrijvers ontkomen er niet aan dat enkele (kleine) onderdelen van systemen niet in NL of de EER gehost worden. Systemen als bijvoorbeeld "Cognito Forms" (voor het indienen van reisaanvragen) worden in de sector zeer veel gebruikt én in de VS gehost. Binnen deze aanbesteding zal u zaken doen met een reisintermediair die vanwege haar uitvoering noodzakelijke informatie zal moeten delen met bijvoorbeeld airlines of hotels, welke wereldwijd gevestigd zijn. Inschrijver voldoet aan de strenge 27001 en 27701 ISO-normeringen en voldoet tevens aan de AVG-wetgeving. Echter ontkomen (ook) wij er niet aan om enkele (minimale) onderdelen van onze systemen buiten de EER te hosten. Wij verzoeken u dan ook met klem om ook de VS toe te staan als hostlocatie. Uiteraard begrijpen wij uw wens om zoveel mogelijk in NL of de EER te hosten, inschrijver spant zich hier dan ook doorlopend voor in. Bent u bereid deze eis aan te passen?	Het is begrijpelijk dat voor een aantal zaken een platform wordt gebruikt wat in de VS wordt gehost, zoals voor het boeken van vluchten of hotels. In zulke gevallen stellen wij als eis dat Data Privacy Framework wordt gevolgd en er goede afspraken zijn tussen de leverancier als verwerker en haar subverwerkers. Deze afspraken moeten hetzelfde niveau van beveiliging borgen als die bereikt wordt met systemen in de EU. Wij verwachten wel dat de aanbieder kan specificeren welke groepen (classificaties) van gegevens worden verwerkt door welke (sub)verwerker en voor welk doeleinde.
8	Eis 48		Eis 48: Dit is een ongebruikelijk verzoek in de reisbranche. Een ISO27001-accreditatie toont aan dat een organisatie de risico's met betrekking tot gegevensbeveiliging beheerst, waarom is deze eis dan nodig? Het apart hosten van gegevens van het Erasmus MC zou aanzienlijke kosten voor het TMC met zich meebrengen en is naar onze mening onnodig. Stemt u in met het schrappen van deze eis?	De eis doelt op een logische en functionele scheiding van gegevens van klanten. Dit is essentieel voor het borgen van privacy en de beveiliging van gegevens. Naast de beveiliging tegen ongeautoriseerde toegang en aanvallen helpt functionele scheiding bij het voldoen aan wettelijke vereisten zoals de GDPR. We stellen voor dat u in uw beantwoording toelicht op welke manier dat in uw geval is ingericht. De eis komt niet te vervallen.
9	Beveiliging Programma van Eisen Eis 64 Vervolg vraag nummer 87		Volstaat een gelijkwaardig document en/of Plan van Aanpak t.b.v. de ISO27001 i.p.v. de ISO27001 certificering bij gunning? Daarnaast zijn wij PCI/DSS en AVG gecertificeerd. Onze systemen zijn ISO27001 gecertificeerd. Volstaat dit?	Zie de offerteleidraad paragraaf 5.2.2.2, onderdeel C en Ad 3. Dit geldt ook voor eis 64. Inschrijver dient aan te tonen dat er sprake is van een gelijkwaardig certificaat / gelijkwaardige werkwijze.
10	Vraag 52/Programma van eisen	Eis 48	Kunt u toelichten wat u met deze eis bedoelt?	De eis doelt op een logische en functionele scheiding van gegevens van klanten. Dit is essentieel voor het borgen van privacy en de beveiliging van gegevens. Naast de beveiliging tegen ongeautoriseerde toegang en aanvallen helpt functionele scheiding bij het voldoen aan wettelijke vereisten zoals de GDPR.

Nr.	Uw vraag heeft betrekking op	Verwijzing naar tekst in aanbestedingsdocumenten (bijlage en paginanummer, tekstpassage)	Concrete vraag	Antwoord
11	Vraag 52/Programma van eisen	Eis 54	Zoals vermeld in onze vraag wordt hoofdzakelijk gebruik gemaakt van systemen van derde partijen. Het is leverancier niet toegestaan daar security/ PEN testen op uit te voeren. Voor zover door leverancier zelf pentesten worden gedaan, worden uitkomsten hiervan niet gedeeld met derden (inclusief klanten) vanuit veiligheidsoverweging. Bent u bereid deze eis te laten vervallen?	De eis is dat het Erasmus MC als opdrachtgever in staat blijft om te voldoen aan de voor haar geldende wet- en regelgeving. De vraag over pentesten lijkt daarmee niet in lijn te zijn en een eis om te voldoen aan wet- en regelgeving kan niet vervallen. Als leverancier heeft u een keuze om partijen te selecteren met wie u samenwerkt. Daarom kunt u als eis aan dergelijke partijen opleggen dat zij hun beveiliging testen, bijvoorbeeld door pentesten. Het feit dat u een bepaalde verwerking door een derde partij laat uitvoeren ontslaat u niet van de verantwoordelijkheid om de verwerking veilig te laten verlopen. Zo wordt dat ook gezien vanuit de AVG. Het is logisch dat een partij geen rapportages deelt van pentesten met details van gevonden kwetsbaarheden. Maar het is ook logisch dat er op hoofdlijnen over gecommuniceerd kan worden, zoals bijvoorbeeld een managementsamenvatting, frequentie van uitvoer en status van de opvolging van bevindingen.
12	Vraag 52 en 85/Programma van eisen/Eis 59	Eis 59	De applicatie betreft een systeem van een derde partij. Of en in hoeverre dit aangesloten kan worden op de centrale IAM voorzieningen van het Erasmus MC zal gezamenlijk met de derde partij leverancier onderzocht moeten worden. Bent u bereid van deze eis een inspanningsverplichting te maken?	Van deze eis kan helaas geen inspanningsverplichting gemaakt worden. We stellen voor dat u aangeeft welke integratievoorzieningen mogelijk zijn.
13	Vraag 31, 32 en 61/Programma van eisen	Eis 77, 78 en 88	Indien u akkoord bent met het verrekenen van de leveranciersinkomsten in de fees en doorgifte geen harde eis meer is (eis 78 inspanningsverplichting), bent u dan ook bereid om eis 88 te laten vervallen? Zoals u daarin aangeeft ziet de ISAE 3402 audit er op om vast te stellen dat alle voordelen en inkomsten terugvloeien naar opdrachtgever. Nu dat geen harde eis meer is lijkt het niet meer nuttig en wordt een ISAE 3402 audit nog meer dan het al was buitenproportioneel zwaar en kostbaar. De kosten kunnen al gauw tientallen duizenden euro's bedragen per audit.	Zie het antwoord op vraag 4.
14	Vraag 55, 56 en 57/Bijlage 6 AIV	Artikel 19/Blz. 8	Aansprakelijkheid voor onverzekerde risico's tot EUR 1.250.000 is niet acceptabel. Zoals gezegd is in Nederland beroepsaansprakelijkheid in onze branche niet verzekeraar en is vermogensschade van opdrachtgever niet verzekerd. Dit is voor inschrijver een overweging om niet in te schrijven. Wij verzoeken u derhalve nogmaals om of onderscheid te maken voor beroepsaansprakelijkheid, waaronder vermogensschades van opdrachtnemer zoals gevolgschade en gemiste opbrengsten, of om de aansprakelijkheid te beperken tot een proportioneel bedrag van EUR 100.000. Bent u bereid dit aan te passen?	Erasmus MC brengt voor indirecte en directe schade een onderscheid aan in de beperking van het bedrag: •De aansprakelijkheid van Leverancier voor directe schade is per gebeurtenis beperkt tot een bedrag van EUR 1.250.000. •De aansprakelijkheid van Leverancier voor indirecte schade is per gebeurtenis beperkt tot een bedrag van EUR 250.000. Voor Erasmus MC geldt voor indirecte schade ook een beperking van de aansprakelijkheid tot een bedrag van EUR 250.000. Alle voorwaarden van artikel 19 AIV blijven hierbij verder in stand.
15	Vraag 60/Bijlage 7 Concept overeenkomst	12.1/Blz. 8	Het bezwaar ziet met name op het woord "voorgenomen" in artikel 12.1. In verband met vertrouwelijkheid zal niet over elke voorgenomen verandering geïnformeerd kunnen worden. Bent u bereid dit te laten vervallen?	Erasmus MC vervangt het woord 'voorgenomen' door 'aanstaande'. Leverancier is alleen verplicht Erasmus MC te informeren over daadwerkelijke veranderingen die gaan plaatsvinden.

Nr.	Uw vraag heeft betrekking op	Verwijzing naar tekst in aanbestedingsdocumenten (bijlage en paginanummer, tekstpassage)	Concrete vraag	Antwoord
16	Prijzenblad	Regel 23 en 24	Zijn de op te geven fees voor groepsreizen (regel 23 en 24) per persoon of per groepsreis? Gezien de aantallen gaan wij uit van per persoon, maar wij kunnen dit niet herleiden uit uw aanbestedingsstukken. Kunt u ons vermoeden bevestigen dan wel ontkrachten? Graag uw toelichting.	Dit betreft een prijs per groepsreis.