

Nota van Inlichtingen 2 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
1.	Beschrijvend document – §2.3 en §2.9 Scope en herzieningsclausule	Kunnen afzonderlijk begrote herstelbegeleiding, technische adviesgesprekken en architectuuradvies die rechtstreeks voortkomen uit de bevindingen van een Security Assessment onder de raamovereenkomst worden afgenomen? Betreft dit de reguliere scope of de herzieningsclausule uit paragraaf 2.9? Graag aangeven welke adviesactiviteiten wel en niet zijn toegestaan en of hiervoor hetzelfde mandagtarief geldt.	Nee. Herstelbegeleiding, technische adviesgesprekken die verder gaan dan de bespreking van de rapportage en architectuuradvies maken geen onderdeel uit van de scope van de Raamovereenkomst en worden niet als Nadere Opdracht tegen het aangeboden tarief per mandag afgenomen. De KB kan dergelijke diensten afzonderlijk afnemen, bij Opdrachtnemer of bij een andere partij, met inachtneming van de daarvoor geldende regels.
2.	Beschrijvend document – §4 Gedragsverklaring Aanbesteden	Indien de Gedragsverklaring Aanbesteden voor de Inschrijver of een Derde aantoonbaar tijdig bij Justis is aangevraagd, maar niet binnen tien kalenderdagen na de voorlopige gunning beschikbaar is: welke procedure en welk bewijs hanteert KB dan?	Zoals aangegeven moeten alle bewijsmiddelen binnen de termijn van tien kalenderdagen aangeleverd worden. Inschrijver is zelf verantwoordelijk voor het tijdig aanvragen van de verklaring en daarbij moet rekening gehouden worden met de verwerkingstijd van Justis. De handelswijze van de KB staat omschreven binnen het Beschrijvend document.
3.	Beschrijvend document – §4 Referenties, kerncompetentie 1	Voor de referentie-eis ‘ een periode van 12 aaneengesloten maanden. Kan de inschrijver een referent gebruiken waarvan het contract kort na de inleverdatum minus 12 maanden (dus eind november 2025) is ingegaan en nog doorloopt en waarbij minimaal 4 pentesten zijn uitgevoerd ook benutten als referent?	Ja, mits de minimaal vier pentesten op het moment van Inschrijving reeds zijn uitgevoerd, binnen een periode van ten hoogste twaalf aaneengesloten maanden. Bij een lopende opdracht tellen uitsluitend de reeds gerealiseerde pentesten mee (zie het antwoord op vraag 73 van Nota van Inlichtingen 1).
4.	Beschrijvend document – §4 Referenties (algemeen)	Inschrijver neemt aan dat een referent uit een andere EU lidstaat ook toegestaan is, is dat correct?	Ja, dat is correct. Bijlage 2 dient volledig te worden ingevuld, inclusief de contactgegevens van de referent. Bij documenten in een andere taal kan de KB om een officiële vertaling verzoeken (paragraaf 7.12 van het Beschrijvend document).
5.	Beschrijvend document – §4 Referenties (algemeen)	Kan de KB bevestigen dat een referentieopdracht die door de rechtsvoorganger van Inschrijver of Derde is uitgevoerd, mag worden gebruikt wanneer de activiteiten, het personeel en de verplichtingen	Ja, mits Inschrijver (of de Derde) de rechtsopvolger is van de onderneming die de referentieopdracht heeft uitgevoerd en de betreffende activiteiten, inclusief de

Nota van Inlichtingen 2 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		aantoonbaar zijn voortgezet door de rechtsopvolger? Welke bewijsstukken verwacht de KB naast Bijlage 2 om deze continuïteit en de feitelijke uitvoering van de pentestwerkzaamheden aan te tonen?	daarvoor ingezette medewerkers, aantoonbaar zijn voortgezet. Inschrijver vermeldt dit in Bijlage 2 onder ‘Omschrijving aard van opdracht’. Aanvullend bewijs (zoals een uittreksel uit het handelsregister, een fusieakte of een overnameovereenkomst) wordt alleen op verzoek van de KB verstrekt.
6.	Programma van Eisen – E18 Nadere overeenkomst (inventarisatie) (vervolgvraag Nvl 1, vraag 224)	Kan de KB verduidelijken welke informatie minimaal beschikbaar wordt gesteld voorafgaand aan een offerteaanvraag (architectuur, testaccounts, documentatie, testvensters, contactpersonen, etc.)?	De KB hanteert geen vaste minimale set aan informatie. De benodigde informatie (zoals architectuur, testaccounts, documentatie, testvensters en contactpersonen) wordt per Nadere Opdracht tijdens de inventarisatie (E18) verstrekt, voor zover beschikbaar en noodzakelijk voor de gekozen methodiek (zie het antwoord op vraag 14 van Nota van Inlichtingen 1). Zie ook het antwoord op vraag 7.
7.	Programma van Eisen – E18 Nadere overeenkomst (inventarisatie) (vervolgvraag Nvl 1, vragen 225 t/m 228)	Ter verduidelijking van antwoorden 225 t/m 228 bedoelen wij een door Opdrachtnemer aangeleverde intakevragenlijst. Is de KB bereid die per aanvraag samen met Opdrachtnemer in te vullen en de beschikbare documentatie te verstrekken? De vragenlijst bevat, voor zover relevant, testobjecten, gebruikersrollen, koppelingen, methodiek, testvensters, locatievereisten, afhankelijkheden, rapportagewensen en eventuele hertesten. Ontbrekende informatie en de gevolgen daarvan worden vóór de offerte expliciet	Ja, dat is akkoord.
8.	Programma van Eisen – E18 Nadere overeenkomst (inventarisatie) (vervolgvraag Nvl 1, vragen 222 en 223)	Antwoorden 222 en 223 onderscheiden kosteloze inventarisatie van voorbereiding en uitvoering van de Security Assessment. Bevestigt de KB dat technische handelingen zoals proefaanmeldingen, verificatie van bereikbaarheid en autorisaties, het uitvoeren van scripts en inhoudelijke analyse van broncode of configuraties onder de betaalde uitvoering vallen? Indien dergelijke handelingen noodzakelijk blijken om een betrouwbare offerte te maken, mogen partijen daarvoor vooraf een afzonderlijke betaalde voorbereidende fase overeenkomen?	Ja, dat wordt bevestigd. Technische handelingen zoals proefaanmeldingen, de verificatie van bereikbaarheid en autorisaties, het uitvoeren van scripts en de technische analyse van broncode of configuraties maken onderdeel uit van de uitvoering van de pentest (E32) en worden niet verlangd tijdens de kosteloze inventarisatie (E18). De inventarisatie zelf, waaronder het voeren van (intake)gesprekken en het bestuderen van beschikbare documentatie, blijft kosteloos (zie de

Nota van Inlichtingen 2 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
			<p>antwoorden op de vragen 222 en 223 van Nota van Inlichtingen 1).</p> <p>Bij het sluiten van de Nadere Overeenkomsten komen Partijen vooraf overeen welke betaalde voorbereidingswerkzaamheden er uitgevoerd moeten worden.</p>
9.	<p>Programma van Eisen – E23 en E24</p> <p>Annuleren en verzetten Nadere Opdracht (vervolgvraag Nvl 1, vragen 249 en 256)</p>	<p>Na beantwoording van vraag 249 geldt voor kosteloze verplaatsing een termijn van vijf werkdagen, terwijl voor kosteloze annulering een termijn van twee weken geldt. Hierdoor kan een opdracht binnen de annuleringstermijn alsnog kosteloos worden verplaatst en vervolgens, gerekend vanaf de nieuwe uitvoeringsdatum, kosteloos worden geannuleerd. Voor pentesten worden specialistische capaciteit en vanuit Opdrachtgevers voorbereidingen en activiteiten vooraf ingepland. Deze capaciteit maar ook voorbereidingsactiviteiten kunnen vanwege de benodigde aanlooptijd bij andere opdrachten niet zonder meer elders worden ingezet. Bent u daarom bereid voor zowel annulering als verplaatsing dezelfde termijn van twee weken vóór de geplande aanvang te hanteren?</p>	<p>Nee, dat is niet akkoord. De termijnen uit het antwoord op vraag 249 van Nota van Inlichtingen 1 blijven ongewijzigd.</p>
10.	<p>Programma van Eisen – E23 en E24</p> <p>Annuleren en verzetten Nadere Opdracht (vervolgvraag Nvl 1, vragen 249 en 256)</p>	<p>Indien u de verschillende termijnen voor annulering en verplaatsing handhaaft, kunt u dan bevestigen dat verplaatsing niet leidt tot het vervallen van de kostenvergoeding die bij annulering op het moment van die verplaatsing verschuldigd zou zijn geweest? Wij verzoeken u vast te leggen dat bij een latere annulering van een reeds verplaatste opdracht de oorspronkelijke uitvoeringsdatum bepalend blijft voor deze kostenvergoeding.</p>	<p>Nee, dat wordt niet bevestigd. Bij annulering van een verzette Nadere Opdracht is de nieuwe geplande aanvangsdatum bepalend voor de toepassing van E23. Kosten die Opdrachtnemer bij het verzetten binnen vijf werkdagen voor de geplande aanvang in rekening mag brengen (zie het antwoord op vraag 249 van Nota van Inlichtingen 1), blijven verschuldigd. Zie ook het antwoord op vraag 9.</p>
11.	<p>Programma van Eisen – E27</p> <p>Kwalificaties pentesters (vervolgvraag Nvl 1, vragen 274, 276 en 277)</p>	<p>Naar aanleiding van de antwoorden op vragen 274, 276 en 277 constateren wij dat de KB verschillende aanvullende vakinhoudelijke pentestcertificeringen als gelijkwaardig aan de in E27 genoemde certificeringen accepteert.</p>	<p>Ja, dat wordt bevestigd. Het persoonsgebonden certificaat eWPTX wordt geaccepteerd.</p>

Nota van Inlichtingen 2 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Kan de KB bevestigen dat ook eWPTX als gelijkwaardige persoonsgebonden certificering onder E27 wordt geaccepteerd? Indien dit niet het geval is, kan de KB toelichten op welk inhoudelijk criterium eWPTX afwijkt van de reeds aanvullend geaccepteerde certificeringen en daarom niet als gelijkwaardig wordt beschouwd?	
12.	Programma van Eisen – E36 Opslag van data (vervolgvraag Nvl 1, vraag 299)	<p>Naar aanleiding van het antwoord op vraag 299: Kan de Aanbesteder ermee instemmen dat opslag in een afgeschermd en beveiligde cloudomgeving binnen de Europese Unie/EER eveneens voldoet aan E36, mits aantoonbaar passende technische en organisatorische beveiligingsmaatregelen zijn getroffen en de gegevens worden verwerkt conform de toepasselijke Nederlandse en Europese wet- en regelgeving?</p> <p>Indien de Aanbesteder daadwerkelijk vereist dat de data uitsluitend fysiek in Nederland wordt opgeslagen, kunt u dan nader toelichten welke juridische, compliance- of beveiligingsgrondslag aan deze aanvullende geografische beperking ten grondslag ligt?</p>	Uw voorstel is akkoord. Opslag en verwerking van data binnen de EER is ook toegestaan. <i>Dit is een wijziging van E36 en van de antwoorden op de vragen 299 tot en met 303 van Nota van Inlichtingen 1, voor zover daarin opslag in Nederland wordt vereist.</i>
13.	Programma van Eisen – E36 Opslag van data (vervolgvraag Nvl 1, vraag 299)	Wij begrijpen de eis aldus dat gegevens van de KB en gegevens die tijdens de uitvoering van pentesten worden gegenereerd, in Nederland dienen te worden opgeslagen. Kan opdrachtgever bevestigen dat het gebruik van cloudgebaseerde/SaaS-pentesttooling is toegestaan, mits eventuele opslag van KB-gegevens en tijdens de pentest gegenereerde gegevens uitsluitend in Nederland plaatsvindt en eventuele verwerking buiten Nederland uitsluitend binnen de EER geschiedt?	Ja, dat wordt bevestigd. Opslag en verwerking van de gegevens van de KB en de tijdens de pentest gegenereerde gegevens mag daarbij binnen de EER plaatsvinden; opslag uitsluitend in Nederland is niet vereist (zie het antwoord op vraag 12). Voor AI-functionnalité in de pentesttooling geldt E41 (zie de antwoorden op de vragen 30 en 31).
14.	Programma van Eisen – E36 Opslag van data (vervolgvraag Nvl 1, vraag 301)	Antwoord 301 staat een cloudomgeving met opslag in Nederland toe, mits deze uitsluitend door Opdrachtnemer wordt beheerd. Heeft deze voorwaarde betrekking op het functionele beheer van de tenant, toegangsrechten en gegevens? Blijft technisch infrastructuurbeheer door een hostingprovider toegestaan, en onder welke voorwaarden mag die provider bij storingen ondersteuning verlenen waarbij mogelijk toegang tot KB gegevens ontstaat? Graag onderscheid maken tussen de opslaglocatie en de toegestane locatie van ondersteunend personeel.	Zie het antwoord op vraag 12.

Nota van Inlichtingen 2 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
15.	Programma van Eisen – E36 Opslag van data (vervolgvraag Nvl 1, vraag 299)	Kunt u specifiek aangeven op welk soort data/gegevens E36 van toepassing is? Valt hieronder bijvoorbeeld ook de data die inschrijver gebruikt en nodig heeft voor project- en opdrachtmanagement en haar administratie daaromheen?	Ja. E36 is van toepassing op alle gegevens van de KB en de gegevens die tijdens de uitvoering van de pentesten worden gegenereerd, dus ook op de gegevens voor project- en opdrachtmanagement en de administratie daaromheen. Voor al deze gegevens is opslag en verwerking binnen de EER toegestaan. Zie het antwoord op vraag 12.
16.	Programma van Eisen – E36 Opslag van data (verwerking administratieve gegevens)	Inschrijver gebruikt Salesforce voor klantregistratie en commerciële dossierafhandeling. Is het toegestaan hierin de naam van de KB, zakelijke contactgegevens, verkoopkansen, offertes, opdrachtbevestigingen en de administratieve voortgang vast te leggen, mits opslag en verwerking aantoonbaar binnen de EER plaatsvinden? Technische scopegegevens, testresultaten, kwetsbaarheden, accountgegevens en rapportages worden daarbij buiten Salesforce gehouden en uitsluitend in Nederland opgeslagen. Indien de KB dit niet toestaat, welke van de genoemde administratieve gegevens mogen wel in Salesforce worden verwerkt?	Ja, dat is akkoord. Zie ook het antwoord op vraag 12.
17.	Programma van Eisen – E36 Opslag van data (vervolgvraag Nvl 1, vragen 299 t/m 303)	Naar aanleiding van antwoorden 299 t/m 303: Inschrijver gebruikt Microsoft 365 voor zakelijke mail en agenda's. Is de KB bereid hiervoor opslag en verwerking binnen de EER toe te staan, uitsluitend voor contactgegevens, planningsafspraken en commerciële correspondentie? Technische informatie, accountgegevens, bevindingen en rapportages worden dan uitsluitend via een afzonderlijke voorziening met opslag in Nederland uitgewisseld. Of wat is de expliciete verwachting hieromtrent vanuit KB, graag concrete specificatie.	Ja, dat is akkoord. Zie ook het antwoord op vraag 12.
18.	Programma van Eisen – E36 en E46 Opslag en verwerking binnen de EER (vervolgvraag Nvl 1, vragen 303 en 306)	Indien toegang vanuit andere EER-landen toegestaan blijft, wilt u verduidelijken wat onder 'geen opslag buiten Nederland' wordt verstaan? Omvat dit verbod ook tijdelijke lokale bestanden, browser- en applicatiecaches, wisselbestanden, logbestanden, klembordgegevens en screenshots op het apparaat van de medewerker? Welke minimale technische maatregelen moeten voorkomen dat KB-gegevens bij gebruik van een Nederlandse test- of	Zie het antwoord op vraag 12. De eis 'geen opslag buiten Nederland' vervalt daarmee. De gegevens, inclusief tijdelijke lokale bestanden, caches, logbestanden en schermafbeeldingen op het apparaat van de medewerker, worden niet buiten de EER opgeslagen (E46).

Nota van Inlichtingen 2 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		werkomgeving alsnog buiten Nederland worden opgeslagen, en hoe moet Opdrachtnemer de naleving hiervan aantonen?	
19.	Programma van Eisen – E36 en E46 Opslag en verwerking binnen de EER (vervolgvraag Nvl 1, vragen 303, 306 en 332)	Antwoord 303 staat toegang tot KB-omgevingen en gegevens vanuit andere EER-landen toe, mits opslag uitsluitend in Nederland plaatsvindt. Antwoord 332 stelt voor AI-infrastructuur expliciet Nederland als locatie-eis. Deze antwoorden hanteren verschillende geografische grenzen voor onderdelen van dezelfde dienstverlening. Bent u bereid één uniform uitgangspunt vast te leggen waarbij alle werkzaamheden met toegang tot KB-omgevingen, gegevens en testresultaten uitsluitend worden uitgevoerd door medewerkers die zich tijdens die werkzaamheden fysiek in Nederland bevinden, en alle daarbij gebruikte test-, opslag-, rapportage- en AI-infrastructuur eveneens fysiek in Nederland staat? Dit biedt één eenduidig uitgangspunt voor uitvoering, beveiliging en vergelijking van aanbiedingen.	Nee, dat is niet akkoord. Zie het antwoord op vraag 12. Voor de opslag en verwerking van de gegevens, de toegang daartoe en de inzet van AI-tools geldt de EER als grens (zie ook het antwoord op vraag 30). De KB schrijft niet voor dat de werkzaamheden uitsluitend vanuit Nederland worden uitgevoerd.
20.	Programma van Eisen – E37 Ernstige kwetsbaarheden (vervolgvraag Nvl 1, vraag 311)	Antwoord 311 verlangt onmiddellijke telefonische melding van bevindingen vanaf CVSS High, ook buiten kantooruren. Bevestigt de KB dat dit geldt zodra een dergelijke bevinding tijdens de overeengekomen werkzaamheden wordt vastgesteld en geen permanente bereikbaarheidsdienst buiten de geplande werkzaamheden vereist? Kan per Nadere Opdracht tevens een vervangend contactpersoon en escalatieprocedure worden vastgelegd voor het geval de eerste contactpersoon niet bereikbaar is?	Ja, dat wordt bevestigd.
21.	Programma van Eisen – E38 en E56 Vertraging door een oorzaak aan de zijde van de KB (vervolgvraag Nvl 1, vragen 249 en 314)	Antwoorden 249 en 314 verwijzen bij vertraging door de KB naar E56. Bevestigt de KB dat aantoonbaar bestede tijd aan het vaststellen en afstemmen van ontbrekende toegang, defecte testaccounts of een niet beschikbare omgeving als reeds uitgevoerde werkzaamheden wordt behandeld wanneer de oorzaak bij de KB ligt? Welke schriftelijke vastlegging is daarvoor vereist en mogen de hierdoor noodzakelijke werkzaamheden voor hervatting na akkoord aanvullend worden begroot?	Ja, mits de oorzaak aantoonbaar aan de zijde van de KB ligt en Opdrachtnemer de KB direct schriftelijk (per e-mail) informeert over de belemmering en de daaraan bestede tijd onderbouwt.

Nota van Inlichtingen 2 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
22.	Programma van Eisen – Testautorisatie (vervolgvraag Nvl 1, vraag 318)	Naar aanleiding van uw antwoord op vraag 318: Kunt u bevestigen dat Opdrachtnemer bij iedere Nadere Opdracht haar eigen model vrijwaringsverklaring mag voorleggen, op grond waarvan Opdrachtgever Opdrachtnemer vrijwaart voor de daarin omschreven risico's, en dat deze verklaring vóór aanvang van de werkzaamheden door Opdrachtgever wordt ondertekend?	Gedeeltelijk. Opdrachtnemer mag een eigen model voor de testautorisatie voorstellen; de definitieve inhoud wordt per Nadere Opdracht in overleg vastgesteld en vóór aanvang door de KB ondertekend (zie het antwoord op vraag 318 van Nota van Inlichtingen 1). De vrijwaring door de KB is beperkt tot hetgeen is opgenomen in de antwoorden op de vragen 319 en 323 van Nota van Inlichtingen 1 en in het antwoord op vraag 24; een ruimere vrijwaring in een model van Opdrachtnemer wordt niet overeengekomen.
23.	Programma van Eisen – Testautorisatie (vervolgvraag Nvl 1, vragen 318, 319 en 322)	In antwoord 318 geeft u aan dat de definitieve inhoud van de testautorisatie in overleg wordt vastgesteld en dat Opdrachtnemer een eigen model mag voorstellen. De inhoud is echter essentieel om vooraf te kunnen beoordelen of de werkzaamheden voldoende zijn geautoriseerd en de positie van zowel Opdrachtnemer als de uitvoerende medewerkers voldoende is geborgd. Bent u bereid vóór de inschrijfdeadline een modeltestautorisatie te publiceren, inclusief de in antwoord 319 bedoelde regeling voor toestemming van derden, en inschrijvers daarna gelegenheid te geven hierover verduidelijkingsvragen te stellen? Indien nodig verzoeken wij u hiervoor de planning aan te passen.	Nee, dat is niet akkoord. De KB publiceert geen model voor de testautorisatie en past de planning niet aan. De minimale inhoud van de testautorisatie is opgenomen in het antwoord op vraag 318 van Nota van Inlichtingen 1 en de regeling voor toestemming van derden in het antwoord op vraag 319 van Nota van Inlichtingen 1. Zie ook het antwoord op vraag 22.
24.	Programma van Eisen – Testautorisatie (vervolgvraag Nvl 1, vragen 318 en 319)	Antwoord 319 bepaalt dat Opdrachtnemer niet aansprakelijk wordt gehouden voor aanspraken van derden die uitsluitend voortvloeien uit ontbrekende toestemming. Kunt u bevestigen dat de testautorisatie en deze bescherming mede betrekking hebben op de individuele medewerkers die namens Opdrachtnemer binnen de geautoriseerde scope en conform de afspraken handelen? Bent u daarnaast bereid expliciet vast te leggen dat de KB bij dergelijke aanspraken de bevoegdheid en verleende toestemmingen onderbouwt en Opdrachtnemer en deze medewerkers vrijwaart voor daarmee samenhangende aanspraken van derden en redelijke kosten van verweer?	Ja, beide punten worden bevestigd.

Nota van Inlichtingen 2 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
25.	Programma van Eisen – E40 Bewaren en vernietigen (vervolgvraag Nvl 1, vraag 329)	Wanneer start de termijn van maximaal zes (6) maanden uit E40? Na afronding van de testwerkzaamheden, na oplevering van de definitieve rapportage of na acceptatie door de KB?	De termijn van maximaal zes maanden gaat in op het moment van Acceptatie van de (laatste) rapportage van de Nadere Opdracht, inclusief een eventuele hertest binnen dezelfde Nadere Opdracht.
26.	Programma van Eisen – E40 Bewaren en vernietigen (vervolgvraag Nvl 1, vraag 329)	Hoe verhoudt de termijn zich tot een eventuele hertest binnen dezelfde nadere opdracht? Wil de KB bevestigen dat de termijn pas ingaat na oplevering van de hertestrapportage? Of stelt de KB bij een hertest na vernietiging de oorspronkelijke rapportage zelf te beschikking?	Ja, voor zover de hertest onderdeel is van dezelfde Nadere Opdracht. De termijn gaat dan in op het moment van Acceptatie van de hertestrapportage (zie het antwoord op vraag 25). Vindt een hertest plaats na de vernietiging, dan stelt de KB de oorspronkelijke rapportage ter beschikking.
27.	Programma van Eisen – E40 Bewaren en vernietigen (vervolgvraag Nvl 1, vraag 440)	E40 verlangt vernietiging na maximaal zes maanden, terwijl antwoord 440 een garantie van zes maanden na Acceptatie voorschrijft. Vanaf welk moment begint de vernietigingstermijn? Bevestigt de KB dat noodzakelijk technisch bewijsmateriaal tot het einde van de garantieteriode mag worden bewaard? Indien niet, hoe moeten partijen een garantieaanspraak beoordelen wanneer het daarvoor benodigde bewijsmateriaal verplicht is vernietigd	Ja, dat wordt bevestigd. De vernietigingstermijn gaat in op het moment van Acceptatie (zie het antwoord op vraag 25) en valt daarmee samen met de garantietermijn van zes maanden na Acceptatie (zie het antwoord op vraag 440 van Nota van Inlichtingen 1). Is binnen de garantietermijn een aanspraak gemeld, dan mag Opdrachtnemer het technische bewijsmateriaal dat op die aanspraak betrekking heeft in overleg met de KB bewaren tot de afhandeling ervan (E40). Daarna wordt het vernietigd.
28.	Programma van Eisen – E40 Bewaren en vernietigen (vervolgvraag Nvl 1, vraag 329)	Gaat de KB akkoord met een Certificate of Destruction in de vorm van een verklaring die een tekenbevoegde van de Opdrachtnemer ondertekent (en indien het antwoord ja is, welke toegevoegde waarde heeft zo'n Certificate dan nog boven bv. een email)? Of vereist de KB een verklaring van een onafhankelijke derde? (en indien het antwoord ja is, hoe ziet het KB dat voor zich?)	Ja, een door een tekenbevoegde van Opdrachtnemer ondertekende verklaring volstaat; een verklaring van een onafhankelijke derde is niet vereist.
29.	Programma van Eisen – E40 Bewaren en vernietigen (vervolgvraag Nvl 1, vragen 463 en 521)	Volgens antwoorden 463 en 521 mogen gegevens op back upmedia na de reguliere cyclus worden verwijderd. Bevestigt de KB dat het Certificate of Destruction onderscheid mag maken tussen reeds vernietigde actieve gegevens en resterende back-up kopieën die	Ja, dat wordt bevestigd. Partijen komen tijdens de implementatie van de Raamovereenkomst nadere termijnen overeen omtrent het verwijderen van back-up kopieën.

Nota van Inlichtingen 2 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		volgens een vastgelegde cyclus worden verwijderd? Welke maximale verwijdertermijn accepteert de KB en mag een tussentijdse terugzetting niet leiden tot hernieuwde actieve bewaring van deze gegevens?	
30.	Programma van Eisen – E41 Inzet AI (vervolgvraag Nvl 1, vraag 332)	<p>Naar aanleiding van het antwoord op vraag 332 begrijpen wij dat de KB uitsluitend AI-tools toestaat die on-premise of dedicated in een datacenter in Nederland draaien.</p> <p>Kan de KB ermee instemmen dat ook gebruik mag worden gemaakt van een private, afgeschermdde AI-omgeving die binnen de EU/EER wordt gehost, waarbij de omgeving uitsluitend door Opdrachtnemer wordt gebruikt, data van de KB niet wordt gebruikt voor het trainen van AI-modellen en passende technische en organisatorische maatregelen zijn getroffen om de vertrouwelijkheid en beveiliging van KB-data te waarborgen?</p> <p>Indien de KB hier niet mee kan instemmen, kunt u dan toelichten welk specifiek beveiligings-, privacy- of juridisch risico vereist dat de AI-omgeving fysiek in Nederland wordt gehost in plaats van elders binnen de EU/EER?</p>	Uw voorstel is akkoord. Dit is een wijziging van E41 en van het antwoord op vraag 332 van Nota van Inlichtingen 1.
31.	Programma van Eisen – E41 Inzet AI (vervolgvraag Nvl 1, vragen 338 t/m 341)	Kan opdrachtgever verduidelijken of het verbod op cloudgebaseerde AI ook geldt voor AI-functionality die onderdeel is van pentesttooling, maar waarbij geen gegevens van de KB of tijdens de pentest gegenereerde gegevens door deze AI-functionality worden verwerkt?	Nee. E41 geldt alleen voor AI-functionality waarmee gegevens van de KB of tijdens de pentest gegenereerde gegevens worden verwerkt (zie de antwoorden op de vragen 338 en 340 van Nota van Inlichtingen 1). Opdrachtnemer moet op verzoek van de KB kunnen aantonen dat de AI-functionality deze gegevens niet verwerkt. Zie ook het antwoord op vraag 30.
32.	Programma van Eisen – E50 Audit (vervolgvraag Nvl 1, vragen 363 en 417)	Aanbestedende dienst geeft in haar antwoord aan dat in de definitieve versie van de raamovereenkomst de kosten verdeling van de audit nader wordt uitgewerkt. Het lijkt inschrijver gewenst en redelijk	Er is niet door de KB aangegeven dat er een kostenregeling uitgewerkt gaat worden binnen de

Nota van Inlichtingen 2 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		datvoordat de definitieve inschrijving wordt gedaan duidelijk is wat de aanbestedende dienst hiervoor voorstelt. Inschrijver gaat er dan ook vanuit dat de definitieve versie van de raamovereenkomst onderdeel is van de volgende Nota van Inlichtingen, c.q. dat in de Nota van Inlichtingen is opgenomen hoe het voorstel voor de in de definitieve versie van de raamovereenkomst op te nemen kosten verdeling er uit komt te zien.	<p>Raamovereenkomst. In het antwoord is enkel het volgende aangegeven:</p> <p><i>De KB zal de kosten voor uitvoering van de audit initieel zelf dragen. Indien bij de audit gebreken worden geconstateerd, worden de kosten van de audit doorbelast aan Opdrachtnemer. Deze kostenregeling wordt in de definitieve Raamovereenkomst verwerkt.</i></p> <p>Het is dus niet zo dat er nog iets uitgewerkt gaat worden in de Raamovereenkomst. Er wordt dus verder ook geen gehoor gegeven aan uw verzoek. Zie ook het antwoord op vraag 33.</p>
33.	Programma van Eisen – E50 Audit (vervolgvraag Nvl 1, vraag 363)	Antwoord 363 bepaalt dat auditkosten bij geconstateerde gebreken aan Opdrachtnemer worden doorbelast. Is de KB bereid vooraf de voorgenomen werkzaamheden en een kostenbegroting te delen, zodat Opdrachtnemer daarop kan reageren? Bevestigt de KB dat uitsluitend redelijke, aantoonbare kosten worden doorbelast, met een specificatie van de geconstateerde gebreken en de daaraan gerelateerde auditwerkzaamheden?	Ja, dat is akkoord en de KB bevestigt dit.
34.	Programma van Eisen – E50 Audit (vervolgvraag Nvl 1, vragen 363, 417 en 446)	Bij antwoord 446 zijn de voorgestelde voorwaarden voor factuurcontrole geaccepteerd, terwijl antwoorden 363 en 417 voor algemene audits andere voorwaarden bevatten. Bevestigt de KB dat een controle van facturen en de daaraan ten grondslag liggende projectadministratie onder de voorwaarden van antwoord 446 blijft vallen? Welk regime geldt wanneer een controle zowel facturatie als de inhoudelijke uitvoering betreft, en worden doel, afbakening en kostenregeling vooraf schriftelijk vastgelegd?	Ja, dat wordt bevestigd. Een controle van facturen en de daaraan ten grondslag liggende projectadministratie (artikel 15.3 ARBIT-2022) valt onder de voorwaarden uit het antwoord op vraag 446 van Nota van Inlichtingen 1. Een controle die (mede) de inhoudelijke uitvoering betreft, geldt als audit en valt onder E50 en de antwoorden op de vragen 363 en 417 van Nota van Inlichtingen 1.
35.	Bijlage 2 – Invulbijlage referenties (beroep op Derde)	Kan de KB bevestigen dat Bijlage 2 volstaat wanneer onder “Omschrijving aard van opdracht” concreet wordt vermeld dat de Derde de pentestwerkzaamheden feitelijk heeft uitgevoerd, met naam	Ja, dat wordt bevestigd. Aanvullend bewijs is bij de Inschrijving niet vereist. Wel gelden de overige voorwaarden voor een beroep op een Derde, waaronder

Nota van Inlichtingen 2 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		van de Derde en volledige contactgegevens van de referent? Is aanvullend bewijs, zoals een ondertekende verklaring of overeenkomst, niet vereist?	een eigen UEA van de Derde en Bijlage 8 (zie het antwoord op vraag 76 van Nota van Inlichtingen 1). De KB kan de juistheid van de referentie controleren bij de referent.
36.	Bijlage 2 – Invulbijlage referenties (vervolgvraag Nvl 1, vraag 379)	In antwoord 379 bevestigt u dat geen minimale contractwaarde of omzet geldt en dat de financiële gegevens uitsluitend ter informatie worden gevraagd. Het verplicht verstrekken van deze commerciële informatie lijkt daarmee geen noodzakelijke bijdrage te leveren aan de toetsing van de kerncompetenties. Wilt u heroverwegen of deze velden kunnen vervallen? Indien u een indicatie van de omvang noodzakelijk acht, kunt u dan bevestigen dat de referentie boven een door u vastgestelde ondergrens ligt, zoals het aantal van vijf pentesten in lijn met het recent aantal uitgevoerde pentesten door KB?	Nee, dat is niet akkoord. De velden blijven gehandhaafd (zie het antwoord op vraag 382 van Nota van Inlichtingen 1); een onderbouwde schatting is toegestaan. De KB stelt geen ondergrens aan de omvang van een referentie, anders dan de kerncompetenties in hoofdstuk 4 van het Beschrijvend document.
37.	Bijlage 3A – Raamovereenkomst art. 1.2 Model Nadere Overeenkomst	In het Programma van Eisen en in de Concept Raamovereenkomst wordt gesproken over/verwezen naar de Nadere Overeenkomst. Dit document wordt door inschrijver niet aangetroffen. Kunt u dit document alsnog beschikbaar stellen en inschrijvers de gelegenheid geven hun vragen over te stellen?	Nee. Er wordt geen afzonderlijk model Nadere Overeenkomst gehanteerd. De Nadere Overeenkomst komt tot stand door ondertekening van de offerte door de KB (E22). Artikel 1.2 van de Raamovereenkomst wordt hierop aangepast (zie het antwoord op vraag 390 van Nota van Inlichtingen 1).
38.	Bijlage 3A – Raamovereenkomst (aanvullende bepalingen) (vervolgvraag Nvl 1, vraag 405)	In uw antwoord op vraag 405 geeft u aan dat u niet kunt instemmen met de door ons voorgestelde tussentijdse opzegmogelijkheid. Wij begrijpen dat Opdrachtgever belang heeft bij continuïteit van de dienstverlening. Tegelijkertijd vinden wij het van belang dat partijen de mogelijkheid hebben de Overeenkomst tussentijds te beëindigen indien voortzetting daarvan redelijkerwijs niet langer van hen kan worden verlangd. Om daarbij voldoende rekening te houden met de belangen van beide partijen, stellen wij voor een opzegtermijn van vier maanden overeen te komen en de volgende bepaling op te nemen: “Ieder der partijen is bevoegd de Overeenkomst tussentijds door	Nee, dat is niet akkoord. Met het oog op de continuïteit van de dienstverlening komt er geen tussentijdse opzegmogelijkheid voor Opdrachtnemer.

Nota van Inlichtingen 2 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		opzegging te beëindigen met inachtneming van een opzegtermijn van vier (4) maanden.” Kunt u hiermee instemmen?	
39.	Bijlage 4 – ARBIT-2022 art. 8 Intellectuele eigendomsrechten (vervolgvraag Nvl 1, vraag 428)	In uw antwoord op vraag 428 geeft u aan dat u niet kunt instemmen met de voorgestelde wijziging van artikel 8.3 ARBIT-2022. Wij verzoeken u dit standpunt te heroverwegen. Met ons voorstel blijft gewaarborgd dat Opdrachtgever, ongeacht de uitkomst van een eventueel geschil over de intellectuele eigendomsrechten, kan voortgaan met het Overeengekomen gebruik van de Prestatie. Bent u bereid uw standpunt te heroverwegen en alsnog in te stemmen met de in vraag 428 voorgestelde wijziging van artikel 8.3 ARBIT-2022?	Nee, dat is niet akkoord. De KB handhaaft het antwoord op vraag 428 van Nota van Inlichtingen 1. Artikel 8.3 ARBIT-2022 blijft ongewijzigd.
40.	Bijlage 4 – ARBIT-2022 art. 12 Garanties (vervolgvraag Nvl 1, vraag 441)	In uw antwoord op vraag 441 geeft u aan dat artikel 12.3 ARBIT-2022 van toepassing blijft, waarbij de garantietermijn wordt verkort naar zes maanden. Deze verkorting neemt ons bezwaar echter niet weg. Een garantieverplichting is naar onze mening niet passend bij de aard van de gevraagde adviesdienstverlening, aangezien onze bevindingen en adviezen zijn gebaseerd op de omstandigheden en beschikbare informatie ten tijde van de uitvoering van de werkzaamheden en deze omstandigheden nadien kunnen wijzigen. Wij verzoeken u daarom uw standpunt te heroverwegen en artikel 12.3 ARBIT-2022 alsnog buiten toepassing te verklaren. Kunt u hiermee instemmen?	Nee, dat is niet akkoord. De garantie is beperkt tot Gebreken in de geleverde Prestatie en houdt niet in dat alle kwetsbaarheden worden ontdekt of dat de geteste omgeving na de test vrij blijft van kwetsbaarheden (zie de antwoorden op de vragen 440 en 443 van Nota van Inlichtingen 1).
41.	Bijlage 4 – ARBIT-2022 art. 15 Betaling en controle (vervolgvraag Nvl 1, vraag 448)	In uw antwoord op vraag 448 geeft u aan dat u niet kunt instemmen met het buiten toepassing verklaren van artikel 15.5 sub a ARBIT-2022. Wij stellen daarom voor een middenweg te hanteren. Opdrachtnemer zal haar verplichtingen niet opschorten wegens een incidentele betalingsachterstand, maar dient deze mogelijkheid wel te behouden indien Opdrachtgever structureel tekortschiet in haar betalingsverplichtingen en ook na een schriftelijke ingebrekestelling en een redelijke hersteltermijn niet tot betaling overgaat. Bent u bereid artikel 15.5 sub a ARBIT-2022 op deze wijze aan te passen?	Nee, dat is niet akkoord. Artikel 15.5 ARBIT-2022 blijft ongewijzigd. Bij een betalingsachterstand heeft Opdrachtnemer recht op de wettelijke rente en de kostenvergoeding op grond van artikel 15.2 ARBIT-2022.
42.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding (vervolgvraag Nvl 1, vraag 467)	In uw antwoord op vraag 467 geeft u aan dat betaalde boetes in mindering strekken op een eventueel verschuldigde schadevergoeding. Dank voor deze aanpassing. Wij kunnen echter niet instemmen met de hoogte van de boete van € 50.000 per overtreding, nu wij dit bedrag disproportioneel achten. Wij verzoeken	Uw voorstel is akkoord.

Nota van Inlichtingen 2 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		u daarom de hoogte van de boete te heroverwegen en deze te beperken tot maximaal € 25.000 per overtreding. Kunt u hiermee instemmen?	
43.	Bijlage 4 – ARBIT-2022 art. 18 Verwerking gegevens (vervolgvraag Nvl 1, vraag 473)	In uw antwoord op vraag 473 geeft u aan dat u niet kunt instemmen met de voorgestelde wijziging van artikel 18.4 ARBIT-2022. Ons bezwaar tegen de huidige bepaling blijft echter bestaan. Een verplichting om elkaar bij iedere aanspraak van een derde te betrekken, achten wij te verstrekkend. Wij vinden het passender dat partijen per aanspraak kunnen beoordelen of het betrekken van de andere partij bij het voeren van verweer aangewezen is. Wij verzoeken u daarom de voorgestelde wijziging nogmaals in overweging te nemen. Kunt u hiermee alsnog instemmen?	Uw voorstel is akkoord.
44.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid (vervolgvraag Nvl 1, vraag 489)	In uw antwoord op vraag 489 geeft u aan dat u niet kunt instemmen met de door ons voorgestelde wijziging en dat u de aansprakelijkheidsregeling van artikel 26 ARBIT-2022, gelet op de aard van de werkzaamheden, proportioneel acht. Daarnaast geeft u aan bereid te zijn de aansprakelijkheid voor persoons- en zaakschade als bedoeld in artikel 26.2 te beperken tot € 2.500.000 per kalenderjaar. Ons bezwaar ziet echter op zowel artikel 26.2 als artikel 26.3 ARBIT-2022. De daarin opgenomen aansprakelijkheidsbeperkingen kunnen leiden tot een aansprakelijkheid die niet meer in redelijke verhouding staat tot de vergoeding die voor de dienstverlening wordt ontvangen. Wij vinden het daarom van belang dat de aansprakelijkheid in beide gevallen in verhouding staat tot de waarde van de opdracht. Wij verzoeken u daarom nogmaals om zowel artikel 26.2 als artikel 26.3 ARBIT-2022 aan te passen en voor beide artikelen de aansprakelijkheid te beperken tot maximaal viermaal de Vergoeding per gebeurtenis, waarbij voor de Vergoeding alleen het gedeelte in aanmerking wordt genomen dat betrekking heeft op de laatste twaalf maanden waarin de betreffende Prestatie is verricht en samenhangende gebeurtenissen als één gebeurtenis worden aangemerkt. Kunt u alsnog instemmen met ons tekstvoorstel bij vraag 489 van de nota van inlichtingen ter vervangen van artikel 26.2 en 26.3 ARBIT-2022?	Nee, dat is niet akkoord. Gelet op de aard van de werkzaamheden acht de KB de beperkingen van artikel 26.2 en 26.3 ARBIT-2022, met de in dat antwoord opgenomen beperking tot € 2.500.000,- per kalenderjaar voor persoons- en zaakschade, proportioneel.

Nota van Inlichtingen 2 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
45.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid (vervolgvraag Nvl 1, vraag 499)	In uw antwoord op vraag 499 geeft u aan dat u artikel 26.4 sub d ARBIT-2022 niet wenst aan te passen en dat eerst zal worden vastgesteld of sprake is van een verwerkersrelatie. Ons bezwaar tegen de huidige formulering blijft echter bestaan. Ongeacht de kwalificatie van de verhouding tussen partijen kunnen wij niet instemmen met onbeperkte aansprakelijkheid voor bestuurlijke boetes die door een toezichthoudende autoriteit aan Opdrachtgever worden opgelegd. Een dergelijke boete wordt immers opgelegd wegens een overtreding van verplichtingen die op grond van de AVG op de betreffende partij zelf rusten. Voor een verhaalsactie op grond van artikel 82 AVG ligt dit anders. Voor zover aan de voorwaarden van artikel 82 AVG is voldaan, zijn wij bereid de aansprakelijkheidsbeperking voor een dergelijke verhaalsactie buiten toepassing te laten. Wij verzoeken u daarom uw standpunt te heroverwegen en artikel 26.4 sub d ARBIT-2022 alsnog als volgt te wijzigen: “In geval van een verhaalsactie op grond van artikel 82 AVG.” Kunt u hiermee instemmen?	Nee, dat is niet akkoord. Artikel 26.4 sub d ARBIT-2022 wordt niet gewijzigd. Opdrachtnemer is uitsluitend aansprakelijk voor schade (waaronder een boete) voor zover deze aan Opdrachtnemer is toe te rekenen (zie het antwoord op vraag 503 van Nota van Inlichtingen 1).
46.	Bijlage 4 – ARBIT-2022 art. 34 Voortdurende verplichtingen	U stelt hier dat de geheimhouding voor onbepaald tijd is. Inschrijver acht dit disproportioneel. Kunt u dit beperken tot bijvoorbeeld max. 3 jaar?	Nee, dat is niet akkoord. Gelet op de aard van de informatie (kwetsbaarheden in de systemen van de KB) blijft de geheimhoudingsverplichting na het einde van de Overeenkomst voortduren (artikel 34 ARBIT-2022) en wordt deze niet in duur beperkt.
47.	Bijlage 5 – Prijzenblad	Kunt u bevestigen dat het aangeboden mandagtarief betrekking heeft op acht uren van één pentester en niet op acht uur inzet van een volledig team? Indien voor een Nadere Opdracht meerdere pentesters nodig zijn of door de KB worden verlangd, begrijpen wij dat de vooraf overeen te komen vaste aanneemsom wordt berekend op basis van de totale begrote inzet van alle betrokken medewerkers tegen dit mandagtarief. Twee pentesters die ieder acht uur werken vertegenwoordigen dan twee mandagen. Is deze uitleg correct?	Ja, dat is correct. Het tarief per mandag betreft acht uur inzet van één medewerker (E55). Bij inzet van meerdere medewerkers wordt de vaste aanneemsom berekend op basis van de totale begrote inzet van alle medewerkers tegen dit tarief.