Dit bestand bevat nota van inlichtingen 2. d.d. 20-03-2026 voor de Europees openbare aanbesteding SIEM/SOC - Steenwijkerland met referentienummer: 2025-028781

Dit is de tweede en tevens laatste nota van inlichtingen.
Het is derhalve niet meer mogelijk om vragen te stellen.

Indien inschrijver meent dat de aanbestedingsdocumenten onduidelijkheden en/of tegenstrijdigheden bevatten, dan wel de geschiktheidseisen, het programma van eisen of de gunningscriteria onduidelijk of ongeoorloofd zijn, dan wel de wijze van beoordelen onduidelijk is, dan wel de aanbestedingsdocumenten geheel of ten dele strijdig zouden zijn met het recht, dan dient de potentiële inschrijver zijn bezwaren uiterlijk 5 kalenderdagen na verzending van deze nota van Inlichtingen, schriftelijk en gemotiveerd aan de aanbestedende dienst uiteen te zetten, bij gebreke waarvan ieder recht om tegen de inhoud van de aanbestedingsdocumenten te ageren vervalt.

Vraag	Document	Pagina	Paragraaf/artikel	Vraag	Motivatie vraag	Antwoord
1	Nota van inlichtingen 1			Kan opdrachtgever de Nota van Inlichtingen 1 ook in Excel formaat publiceren?		Ja, dit excelbestand is reeds met u gedeeld op maandag 16 februari 2026. Het bestand is terug te vinden via het dashboard in TenderNed onder Documenten / Nota van Inlichtingen.
2	Nota van inlichtingen 1	diverse pagina's	Incident Response	Inschrijver verstaat onder Incident Response de volgende dienstverlening: - Incident- en crisismanagement, - Forensisch onderzoek, en - Ransomware-onderhandelingen en settlements. Voor deze werkzaamheden wordt doorgaans een incident response retainer afgesloten, inclusief SLA met KPI's over reactietijden en gereduceerde tarieven. Deze tarieven liggen in de praktijk significant hoger dan het maximale uurtarief van €150 zoals opgenomen in het prijzenblad. Om onze onafhankelijkheid te borgen en te voorkomen dat "de slager zijn eigen vlees keurt", maken deze diensten bewust geen onderdeel uit van onze reguliere SIEM/SOC-dienstverlening. Hiervoor werken we samen met gespecialiseerde partners. Inschrijver constateert dat in de beantwoording van de vragen over Incident Response in Nvl 1 verschillende definities lijken te worden gehanteerd door de aanbestedende dienst. Kan de aanbestedende dienst daarom bevestigen dat onder Incident Response in het kader van deze aanbesteding wordt verstaan: ondersteuning vanuit de SIEM/SOC-dienstverlener bij een kritiek incident in de vorm van eerste analyse (initiële forensische duiding) en eerste herstelondersteuning? En kan tevens worden bevestigd dat onder Incident Response in deze aanbesteding expliciet niet wordt verstaan: volledig incident- of crisismanagement, diepgaand forensisch onderzoek en ransomware-onderhandelingen en settlements, waarvoor doorgaans een separate incident response retainer inclusief SLA met KPI's en afwijkende (hogere) tarieven wordt afgesloten?	Om scope van deze aanbesteding op gebied van Incident Response te duiden	Onder Incident Response wordt conform PvE-eis 4.17 technische ondersteuning en forensisch onderzoek verstaan; ransomware-onderhandelingen en volledig crisismanagement vallen buiten de scope van deze opdracht.
3	Nota van inlichtingen 1		antwoord op vraag 5	In uw antwoord geeft u aan dat Defender for Office en Defender for CloudApps buiten de scope van de opdracht vallen. In het antwoord op vraag 62 geeft u aan dat u volledige 365 E5 telemetrie verwacht binnen Microsoft Sentinel. In het antwoord op vraag 92 geeft u aan dat er binnen de Azure-tenant verschillende Microsoft Defender componenten (zoals Defender for Endpoint, Identity en Office 365) actief zijn. De 3 antwoorden lijken conflicterend. Kunt u duidelijkheid verschaffen rondom de juiste scope? Kortom, zijn alle Microsoft Defender componenten onderdeel van de scope? Dus inclusief Defender for Office en Defender for CloudApps?	Voor het bepalen van de juiste scope voor inschrijving	Alle Microsoft Defender-componenten, inclusief Defender for Office en Defender for CloudApps, maken integraal onderdeel uit van de monitoring-scope.
4	Nota van inlichtingen 1		vraag 9 en 39	Bij de beantwoording van vraag 9 geeft u aan dat opdrachtnemer een IR retainer moet leveren, echter in het antwoord van vraag 39 geeft u aan geen IR retainer te verwachten. Het is voor opdrachtnemer onduidelijk wat u precies verwacht, kunt u dit nogmaals toelichten?	Dit is belangrijk voor de juiste pricing.	De levering van een IR-retainer is verplicht conform PvE-eis 4.17.
5	Nota van inlichtingen 1	6	vraag 39	Het door de gemeente vastgestelde maximale uurtarief voor incident-responsewerkzaamheden door een CERT wijkt in significante mate af van marktconforme tarieven voor vergelijkbare hooggespecialiseerde dienstverlening. Binnen dit tariefniveau is het voor geen enkele Inschrijver mogelijk om de vereiste kwaliteit, beschikbaarheid en deskundigheid te borgen die noodzakelijk zijn voor een adequaat incident-responseproces. Dit vormt een risico voor de continuïteit en effectiviteit van de gevraagde dienstverlening. In het belang van de uitvoerbaarheid en betrouwbaarheid van de opdracht verzoekt Inschrijver de gemeente daarom het vastgestelde tarief minimaal te verdubbelen. Kan de gemeente bevestigen dat zij bereid is deze aanpassing door te voeren?		Het maximale uurtarief voor Incident Response-werkzaamheden wordt verhoogd naar € 300,- om de gevraagde expertise, kwaliteit en beschikbaarheid te kunnen borgen.
6	Nota van inlichtingen 1	6	vraag 39	In document "Gewijzigd n.a.v. Nvl 2 - Bijlage 3 - Prijsinvulformulier" kan Inschrijver slechts één uurprijs vermelden. Dit is tegenstrijdig aan wat de gemeente aangeeft: "per IR-rol". Kunt u in dat geval als er meerdere rollen moeten worden geprijsd hier ook ruimte voor creeeren in het prijsinvulformulier?		Per abuis is aangegeven dat inschrijver uurtarieven moet opgeven. Het betreft één maximaal uurtarief die geldt voor meerdere rollen die worden kunnen ingezet tijdens uitvoeren van incident response. De uurtarieven voor in te zetten rollen mogen niet hoger liggen dan het opgegeven maximum uurtarief.
7	Nota van inlichtingen 1		antwoord op vraag 40	Kunt u het precieze aantal pagina's per subgunningscriterium verduidelijken?	Uw antwoord schept verwarring omdat het verwijst naar het antywoord op vraag 34 maar die vraag wijkt af (vraagt om 6 en niet om 7 pagina's) en gaat ook gaat over een ander subgunningscriterium.	Het plan van aanpak voor kwaliteitscriterium 1 - Partnerschap mag maximaal 6 A4 bevatten (zie antwoord op vraag 34 Nvl 1). Daarnaast mag het plan van aanpak voor kwaliteitscriterium 3 - maximaal 6 A4 en één extra bijlage A3 bevatten (zie antwoord op vraag 40 Nvl 1).
8	Nota van inlichtingen 1	8	vraag 57	Wat bedoelt de gemeente precies met de zinsnede "een volledige dekking van de benoemde bronnen om de gewenste integrale monitoring te kunnen realiseren"?		Met "volledige dekking" wordt bedoeld dat alle relevante beveiligingsgebeurtenissen uit de benoemde bronnen geanalyseerd moeten worden om een integraal en samenhangend dreigingsbeeld van de omgeving te borgen.

9	Nota van inlichtingen 1	10	vraag 78	Inschrijver maakt zoals vereist gebruik van de Microsoft Sentinel omgeving van de gemeente. Alle logbronnen worden eraan gekoppeld en alle loginformatie bevindt zich alleen in deze omgeving. Daarnaast maakt Inschrijver echter ook gebruik - zoals standaard het geval is bij MSSP's - van een eigen Sentinel omgeving (dedicated voor de gemeente) die via Azure Lighthouse gekoppeld is met de Sentinel omgeving van de gemeente. Alle use-cases draaien in onze omgeving en acteren via de Lighthouse koppeling op de logdata die volledig bij de gemeente is opgeslagen. Incident response vindt plaats vanuit onze SOAR-omgeving waarin de SOC-analisten primair werken. De gemeente krijgt hier inzicht in via ons ServiceNow-gebaseerde klantportaal dat gekoppeld kan worden aan de ITSM-omgeving van de gemeente. Een opvolgende SOC-partij kan zijn eigen XOAR-omgeving en use-cases eenvoudig koppelen aan de Sentinel van de gemeente (waar zich na een exit alle logdata, en alle klantspecifieke en door Microsoft geleverde use-cases bevinden) en de ITSM van de gemeente (waar zich na een exit alle incidenten bevinden) zodat de continuïteit van de security monitoring niet in gevaar komt. Kan de gemeente bevestigen dat zij met deze werkwijze akkoord gaat?		Nee, niet akkoord. Use-cases die dienen op de omgeving van opdrachtgever te staan. Lighthouse mag wel gebruikt worden voor monitoringsdoeleinden.
10	Nota van inlichtingen 1	11	vraag 89	Inschrijver begrijpt dat 99,9% beschikbaarheid gewenst is voor 24x7 monitoring, maar onderkent ook dat componenten op klantlocatie (sensoren, logcollectors e.d.) in dit soort dienstverlening vrijwel altijd enkelvoudig worden uitgevoerd. Daarbij geldt bovendien dat dit soort componenten afhankelijk zijn van de beschikbaarheid van de IT-omgeving van de gemeente zelf. Kan de gemeente bevestigen dat dergelijke componenten in dat geval buiten de genoemde beschikbaarheid vallen?		De gemeente bevestigt dat componenten op locatie die voor hun werking afhankelijk zijn van de gemeentelijke infrastructuur, conform PvE eis 11.9, buiten de geëiste beschikbaarheid van 99,9% vallen.
11	Nota van inlichtingen 1		vraag 96	In de uitvraag wordt "Incident Response (CERT)" gebruikt als aanduiding voor één van de SOC-activiteiten. In de beantwoording van vraag 96 wordt echter niet ingegaan op wat u verstaat onder een CERT. Wij verzoeken u te verduidelijken: a) Wat verstaat u onder "CERT" in de context van deze opdracht — is dit een afzonderlijke entiteit, een specifiek team, of ziet u dit als onderdeel van de bredere incidentresponsecapaciteit van het SOC? b) Hoe ziet u de verhouding tussen CERT en Incident Response?		Het CERT is het gespecialiseerde team binnen de organisatie van opdrachtnemer dat Incident Response-taken uitvoert. Zie eis 4.17 van het Programma van Eisen.
12	Nota van inlichtingen 1		vraag 99, 102 en 104	Inschrijver krijgt de indruk dat de gemeente lijkt twee zaken door elkaar te halen. Het feit dat de data van de gemeente wordt opgeslagen binnen de MS EU Data Boundary doet geen afbreuk aan het feit dat de US Freedom Act een extraterritoriale wet is die ook van toepassing is op data buiten de VS. De data van de gemeente valt ondanks de contractuele afspraken die de gemeente zelf via het VNG contract met Microsoft heeft ook nog steeds onder de reikwijdte van deze wet. Een volledige garantie kan Microsoft dus niet geven, en inschrijver in dat opzicht ook niet. Daarnaast lijkt u uw eigen antwoord op vraag 102 tegen te spreken met de antwoordein op vragen 99 en 104. Het uitdrukkelijke verzoek is derhalve om uw antwoord te heroverwegen en aan te sluiten bij uw antwoord op vraag 102, aangezien u anders feitelijk een disproportionele eis stelt, nu geen enkele marktpartij deze garantie kan geven.		Het antwoord op vraag 102 van Nota van inlichtingen 1 is juist.
13	Nota van inlichtingen 1		Antwoord 103	Op basis van art. 4.3 van de Verwerkersovereenkomst mag Verwerker Persoonsgegevens buiten de EER (laten) verwerken wanneer is voldaan aan de voorwaarden van artikel 45 of 46 AVG. In de eerste vragenronden hebben we u gevraagd te bevestigen dat dit evenwel geldt in relatie tot Eis 5.3, waarvan u aangeeft niet akkoord te gaan. Om de eerdere vraag te verduidelijken: Begrijpt Inschrijver goed dat u er akkoord mee gaat dat er gegevensverwerking plaatsvindt buiten de EER, wanneer is voldaan aan de voorwaarden van artikel 44-46 AVG, mits de opslag van de data plaatsvindt binnen de EER? Zo niet, kan Opdrachtgever dan toelichten hoe Eis 5.3 zich dan verhoudt tot art. 4.3 van de Verwerkersovereenkomst?		Opdrachtgever gaat akkoord dat gegevensverwerking buiten de EER plaatsvindt, mit is voldaan aan voorwaarden van artikel 45-46 AVG en opslag van data plaatsvindt binnen de EER.
14	Nota van inlichtingen 1		Vraag 103	Uw antwoord op deze vraag haalt de onduidelijkheid helaas niet weg. Op grond van de Overeenkomst prevaleert de verwerkersovereenkomst boven de NVI's en de aanbestedingsdocumentatie. In de verwerkersovereenkomst is opgenomen dat persoonsgegevens in overeenstemming met de AVG buiten de EER mogen worden verwerkt. Als u dat niet wilt is het advies om de verwerkersovereenkomst ook uitdrukkelijk op dit punt aan te passen.		Zie het antwoord op vraag 14.

15	Nota van inlichtingen 1		Vraag 109	U geeft aan dat we ISO 9001 of een vergelijkbare certificering aan mogen leveren. Wij willen benadrukken dat de kwaliteit, betrouwbaarheid en procesbeheersing van onze dienstverlening aantoonbaar zijn geborgd via onze bestaande certificeringen: - ISO 27001 — waarmee wij voldoen aan internationaal erkende normen voor informatiebeveiliging, risicobeheer en gecontroleerde procesvoering. - ISAE 3402 Type II — waarmee wij onze interne beheersmaatregelen, controlemechanismen en proceskwaliteit onafhankelijk laten toetsen op effectiviteit en consistentie. Gezamenlijk bieden deze certificeringen een aantoonbaar solide raamwerk voor kwaliteitsbeheer, risicobeheersing en voortdurende verbetering binnen onze dienstverlening. Onze vraag is daarom: Kunt u bevestigen of ISO 27001 en ISAE 3402 als gelijkwaardig of voldoende alternatief mogen worden beschouwd voor ISO 9001 binnen deze aanbesteding, gezien de mate van procescontrole, volwassenheid en kwaliteitsborging die wij hiermee kunnen aantonen?		Niet akkoord. ISO 9001 is de internationale norm voor kwaliteitsmanagement die leidt tot een certificaat na een geslaagde audit. De norm helpt organisaties om: - klantgericht te werken; - risico's en kansen gestructureerd te benaderen; - processen te verbeteren, en te bouwen aan een cultuur van kwaliteit. ISAE 3402 is geen certificering, maar een assurance-verklaring die door een externe auditor wordt afgegeven. ISAE 3402 beschrijft een volledig systeem en laat ruimte voor maatwerk in beheersmaatregelen. Bij ISAE 3402 draait het om het behalen van beheersdoelstellingen. ISAE 3402 is gebruikelijk binnen de financiële sector. ISO-27001 en ISO-9001 zijn beide managementsysteemnormen, maar zij hebben een fundamenteel verschillend doel en toepassingsgebied. ISO-27001 richt zich op informatiebeveiliging, terwijl ISO-9001 focust op kwaliteitsmanagement van bedrijfsprocessen. De aanbestedende dienst is daarom van mening dat ISO 27001 en/of ISAE 3402 niet kan worden gekwalificeerd als een norm voor kwaliteitsmanagement.
16	Nota van inlichtingen 1	15	vraag 119 en 120	Kunt u bevestigen dat het antwoord op vraag 119 klopt en het antwoord op vraag 120 komt te vervallen, gezien de inherente tegenstrijdigheid van beide antwoorden?	De antwoorden van de gemeente op de NvI-1 vragen 32, 77, 78, 97, 118 en 120 zijn tegenstrijdig aan het in vraag 119 gegeven antwoord. Inschrijver acht het van belang dat duidelijk is dat met deze dienst sprake is van een shared managed dienst die tegelijkertijd ook aan andere klanten wordt geleverd op basis van dezelfde configuraties en usecases. Deze zijn bovendien bedrijfsdebiet van inschrijver en kan zij om die reden dus niet overdragen bij een exit. Uw eis is in dit opzicht ook niet proportioneel. Inschrijver kan eventueel wel een lijst delen van de logbronnen die zijn aangesloten, zodat de nieuwe leverancier weet welke logbronnen hij dient aan te sluiten om de dienstverlening tenminste te kunnen continueren. Eventuele specifieke usescases die op aanvraag van de gemeente worden ontwikkeld en waarvoor zij ook separaat betaald kunnen uiteraard wel worden overgedragen.	Antwoorden op vraag 119 en 120 zijn juist. Bij beëindiging dienen alle klantspecifieke configuraties en voor de gemeente ontwikkelde use-cases overgedragen te worden; intellectuele eigendomsrechten op standaard, gedeelde use-cases blijven bij de opdrachtnemer.
17	Nota van inlichtingen 1		Antwoord op vraag 133 en 134	De NvI bestuderend valt mij direct één ding op, nl dat de antwoorden op de vragen 133 en 134 elkaar tegenspreken. In vraag 133 geeft u aan dat de concept SLA niet bij Inschrijving hoeft te worden ingediend en in vraag 134 stelt u 'het bij inschrijving in te dienen SLA'. Kunt u aangeven op welk moment u verwacht dat er een concept SLA wordt overlegd?		De voorlopig gegunde partij dient bij voorlopige gunning een concept SLA te overleggen. De definitieve versie wordt, in samenspraak, na definitieve gunning vastgesteld.
18	Nota van inlichtingen 1		Vervolgvraag NVI 1 vraag 285	In het prijsblad wordt verzocht een prijs per asset op te geven. Aangezien de kosten van SIEM/SOC-dienstverlening in belangrijke mate worden bepaald door het gegenereerde logvolume (bijvoorbeeld uitgedrukt in GB per dag) en niet uitsluitend door het aantal assets, verzoeken wij u te verduidelijken of het is toegestaan de prijsstelling te baseren op logvolume (aantal GB) per dag, eventueel omgerekend naar een prijs per asset op basis van een overeengekomen uitgangspunt. Indien prijsstelling uitsluitend per asset dient plaats te vinden, verzoeken wij u aan te geven welke uitgangspunten ten aanzien van gemiddeld logvolume per asset gehanteerd dienen te worden gebaseerd op de fictieve 50 GB, zodat een eerlijke en vergelijkbare prijsopgave kan worden gedaan.		Conform het prijsinvulformulier dient de inschrijver de prijzen uitsluitend per asset op te geven. Dit om een uniforme, eenduidige en transparische vergelijking van de inschrijvingen mogelijk te maken. Een prijsstelling op basis van logvolume (zoals aantal GB per dag), al dan niet omgerekend naar een prijs per asset, is niet toegestaan. Het is de inschatting van de opdrachtgever dat logvolume voor deze opdracht geen relevante kostenbepalende factor vormt voor de opdrachtnemer, aangezien alle kosten die voortvloeien uit licenties, data-ingest of andere Microsoft Azure gerelateerde verbruiks- of platformkosten volledig voor rekening van de opdrachtgever zijn. Het hanteren van aannames omtrent gemiddeld logvolume per asset is daarom niet noodzakelijk. De inschrijver dient een integrale prijs per asset op te geven waarin alle kosten voor de uitvoering van de SIEM/SOC-dienstverlening zijn verdisconteerd.
19	Nota van inlichtingen 1		Antwoord op vraag 355	In vraag 355 heeft u aangegeven vast te houden aan de eenzijdige verlengingsmogelijkheid tot een maximale periode van 10 jaar. Wij vragen u dit te heroverwegen en in ieder geval de laatste periode met wederzijdse instemming te laten zijn. De eenzijdige periode geldt dan tot 8 jaar. Het is uiteraard uw recht om vast te houden om de eenzijdigheid voor de gehele periode. Kunt u hier spoedig op antwoorden? Indien u vasthoudt aan het eerder gegeven antwoord, dan zijn wij helaas genoodzaakt om af te haken en u succes te wensen met de selectie van de voor u juiste partij.		Niet akkoord. De aanbestedende dienst handhaaft de eenzijdige verlengingsoptie.
20	Bijlage 3 - prijsinvulformulier			In het prijzenblad is geen post opgenomen voor mobiele devices (iOS/Android). Betekent dit dat mobiele devices niet gemonitord dienen te worden als onderdeel van de dienstverlening?	Expliciete duidelijkheid over de monitoring scope is belangrijk voor de omvang en kosten van de dienstverlening.	Mobiele apparaten (iOS/Android) zijn als asset geen onderdeel van de actieve monitoring- en beheerscope en hoeven niet te worden opgenomen in de prijsopgave per asset.

21	Bijlage 3 - prijsinvulformulier			Bij het afnemen van incident response is het gebruikelijk om een retainer te hanteren als vergoeding voor stand-by zijn van het response team. Wanneer geen retainer wordt gehanteerd zullen deze kosten door aanbieders in de kosten van het SOC of het uurtarief voor incident response worden verdisconteerd, wat in beide gevallen leidt tot vertroebling van de kosten. In het bijzonder vergroot dit de spanning tussen het maximale IR tarief en wat marktconform is voor dergelijke diensten. Bent u bereid een aparte post in het prijzenblad op te nemen voor een incident response retainer?	Zie vraag.	Zie antwoord op vraag 7. Indien Incident (conform eis 4.17 Pve) ingezet moet worden dan liggen uurtarieven niet hoger dan het opgegeven maximum uurtarief.
22	Bijlage 3 - prijsinvulformulier			De huidige maximale prijs voor incidentresponse is nu 150 EUR. Opdrachtnemer is van mening dat dit niet marktconform is, zeker als er geen retainer wordt afgenomen en in het geval van incidenten buiten kantoortijden. Gaat opdrachtgever ermee akkoord dit bedrag te verhogen naar 300 EUR per uur?	Bij niet-marktconforme maximum prijzen is er risico op minder aanbiedingen en afbreuk aan kwaliteit van in te zetten specialisten, wat afbreuk doet aan de doelstelling van de aanbesteding voor gemeente Steenwijkerland.	Ja, het maximale uurtarief voor Incident Response-werkzaamheden wordt verhoogd naar € 300,-.
23	Bijlage 3 - prijsinvulformulier			U hanteert één maximum tarief voor Incident Response. In onze ervaring is incident response regelmatig vereist buiten kantoortijden. Dit brengt hogere personeelskosten met zich mee. Bent u bereid verschillende maximum tarieven te hanteren voor binnen en buiten kantoortijden?		Nee, verschillende tarieven voor binnen of buiten kantoortijden zijn niet toegestaan, aangezien het verhoogde maximumtarief van € 300,- hiervoor voldoende ruimte biedt.
24	Uitnodiging tot Inschrijving	8	1.3.2	De uitvraag noemt u als onderdeel van de scope 'advies en ondersteuning bij de inrichting, het beheer en de optimalisatie van technische beveiligingsoplossingen'. Kunt u aangeven wat de aard en (maximale) omvang van deze advieswerkzaamheden naar verwachting zal zijn, zodat inschrijver hiervoor een passende kosteninschatting kan maken? Of kunt u een advies-tarief opnemen in het prijzenblad zodat advieswerkzaamheden op nacalculatie in rekening kunnen worden gebracht?	Wanneer genoemde advieswerkzaamheden onderdeel zijn van het vaste tarief voor monitoring en response, maar niet vooraf bekend is hoeveel werk dit (maximaal) zal zijn dan bestaat het risico dat de kosten voor de dienstverlening voor inschrijver niet goed te managen zijn.	Advies en ondersteuning op andere beveiligingsstukken, anders dan deze SiemSoc, vallen buiten de scope.
25	Bijlage 5 - Programma van Eisen		1.1	PvE eis 1.1 vereist dat alle inzage- en beheeracties van de opdrachtnemer worden vastgelegd in een auditlog. Vanuit het oogpunt van onafhankelijke controle ligt het beheer van deze auditlog bij de opdrachtgever als tenant-eigenaar, niet bij de opdrachtnemer wiens handelen wordt gelogd. Bevestigt u dat het beheer van de auditlogfunctionaliteit en de retentie-instellingen bij de opdrachtgever berust, en dat de opdrachtnemer hiertoe geen wijzigingsbevoegdheid heeft?		De gemeente bevestigt dat zij als eigenaar van de Microsoft Azure-tenant verantwoordelijk is voor het beheer van de auditlogfunctionaliteit en de bijbehorende retentie-instellingen.
26	Bijlage 5 - Programma van Eisen		4,17	Gezien de aard van de gevraagde Incident Response (IR) dienstverlening (Programma van Eisen 4,17), waarbij naar verwachting onderzoek wordt verricht naar (mogelijk) betrokken persoonsgegevens in het kader van beveiligingsincidenten, is het in de markt gebruikelijk dat de uitvoerende partij beschikt over een geldige vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr), zijnde een POB-vergunning voor het uitvoeren van particulier onderzoek. Kunt u bevestigen dat van inschrijvers wordt verwacht dat zij beschikken over een dergelijke POB-vergunning, zodat rechtmatig onderzoek naar persoonsgegevens kan worden uitgevoerd?		Ja, opdrachtnemer dient voor het rechtmatig uitvoeren van forensisch onderzoek naar persoonsgegevens te beschikken over een geldige POB-vergunning op grond van de Wpbr.
27	Bijlage 5 - Programma van Eisen		4.7	In het programma van eisen (4.7) is opgenomen dat de Opdrachtgever de dienstverlening gedurende de looptijd van de overeenkomst kan op- en afschalen. Inschrijver begrijpt dat het IT-landschap en de bijbehorende logbronnen niet statisch zijn en dat flexibiliteit gewenst is. Tegelijkertijd brengt de inrichting en instandhouding van de dienstverlening (zoals onboarding van logbronnen, use case ontwikkeling, platformconfiguratie, kennisopbouw en capaciteitsplanning) initiële en structurele kosten met zich mee, die mede zijn gebaseerd op de omvang van de afgesproken scope. Kunt u verduidelijken: a) Of er een minimale afname (bijvoorbeeld in aantal logbronnen, datavolume of afgesproken scope) gedurende de contractperiode wordt gegarandeerd; b) Op welke wijze wordt geborgd dat afschaling niet zodanig plaatsvindt dat voor Opdrachtnemer disproportionele kosten of onevenredige risico's ontstaan; c) Of bij substantiële afschaling herijking van prijs- en capaciteitsafspraken plaatsvindt.	Inschrijver verzoekt om bevestiging dat eventuele afschaling proportioneel en redelijk zal plaatsvinden, met inachtneming van het evenwicht tussen flexibiliteit voor Opdrachtgever en bedrijfseconomische uitvoerbaarheid voor Opdrachtnemer. Bij niet proportionele op-/afschaling is er risico op afbreuk aan de kwaliteit van dienstverlening, wat afbreuk doet aan de doelstelling van de aanbesteding voor gemeente Steenwijkerland	De gemeente biedt geen minimale afnamegarantie, maar bevestigt dat afschaling proportioneel zal plaatsvinden op basis van de werkelijk gerealiseerde aantallen assets.
28	Nota van inlichtingen 1		Vraag 119	Mededeling aanbestedende dienst: Foutief antwoord op vraag 119 van Nota van Inlichtingen 2.		Per abuis is aanbestedende dienst akkoord gegaan met vraag 119. Via deze weg wordt het antwoord aangepast naar: Aanbestedende dienst gaat niet akkoord.