Onderzoeksraad voor Veiligheid

2e Nota van Inlichtingen

Hierbij ontvangt u de vragen en de bijbehorende antwoorden naar aanleiding van de Europese aanbesteding Drukwerk en DTP 2026, selectieleidraad.:
Deze Nota van Inlichtingen behoort bij en maakt integraal onderdeel uit van de aanbesteding.

Deze Nota bestaat uit vragen van geïnteresseerden en de antwoorden van de Onderzoeksraad

Onderzoeksraad voor Veiligheid

Deel 1: Vragen geïnteresseerden en antwoorden van de Onderzoeksraad

Nr	Document	Paragraaf/ artikel	Vraag	Antwoord
33		Eis van Informatiebeveiliging	Wij hebben met ons bureau de BIO fit/gap analyse van de Rijksoverheid meermaals succesvol doorlopen, en kunnen hiervan bewijs overleggen. Meest recent was dit in 2023. De BIO2 was destijds nog niet van toepassing. Ook zijn we bezig met het traject van ISO27001 gecertificeerd worden. Volstaat voor het voldoen aan de eis van Informatiebeveiliging voor de OvV het overleggen van deze BIO fit/gap analyse, en een verklaring van de begeleidende partij dat we deze ISO27001 certificering succesvol gaan afronden, met een beoogde datum erbij?	De door u beschreven documenten zijn niet voldoende om te voldoen aan de gestelde geschiktheidseis. U dient bij inschrijving te beschikken over een aantoonbaar werkend Information Security Management System (ISMS) dat is ingericht conform ISO/IEC 27001 en voldoet aan de informatiebeveiligingseisen gebaseerd op de BIO2-maatregelen. Een BIO fit/gap-analyse toont op zichzelf niet aan dat sprake is van een werkend ISMS, noch dat wordt voldaan aan de BIO2-maatregelen. Evenmin geldt een verklaring of voornemen tot het behalen van ISO27001-certificering als bewijs dat op het moment van inschrijving aan deze eis wordt voldaan. Zoals opgenomen in de leidraad zal na voorgenomen gunning een geldig certificaat of een onafhankelijke auditverklaring worden gevraagd waaruit de opzet, het bestaan en de werking van het ISMS blijken. Indien u (nog) niet beschikt over een ISO27001-certificaat, kunt u in dat stadium een onafhankelijke auditverklaring overleggen, mits daaruit aantoonbaar blijkt dat uw ISMS voldoet aan de gestelde eisen (ISO27001 en BIO2) en daadwerkelijk operationeel is.
34		Eisen van ISO9001, ISO27001 en ISO14001 voor een combinatie	Indien meerdere partijen als combinatie inschrijven, volstaat het dan dat 1 van de combinanten voldoet aan ISO9001, ISO27001 en ISO14001? Bij actuele aanbestedingen van de Rijksoverheid op gebied van communicatiediensten volstaat dit. We zijn benieuwd of OvV deze lijn ook volgt.	Indien meerdere partijen in combinatie inschrijven, geldt dat de combinatie als geheel aan de gestelde eisen moet voldoen. Indien een beroep wordt gedaan op certificeringen van één van de combinanten (ISO9001, ISO27001 en ISO14001), dient deze partij een wezenlijke rol te vervullen bij de uitvoering van de opdracht en dient de toepassing van de betreffende managementsystemen aantoonbaar van toepassing te zijn op de uitvoering van de opdracht. Echter, de combinant die het drukwerk gaat verrichten, dient wel over het ISO-14001 certificaat te beschikken.
35		NvI-1 nr. 7	In de aanbestedingsstukken is opgenomen: "Op een onderaannemer mag wel door meerdere Gegadigden een beroep worden gedaan." Begrijpen wij deze bepaling correct dat eenzelfde onderaannemer zich tegelijkertijd mag verbinden aan meerdere gegadigden/inschrijvers en dat meerdere	Ja, uw interpretatie is juist. Dit geldt alleen voor een beroep op onderaaneming. Combinanten kunnen daarentegen zich slechts een keer aanmelden. Ook uw interpretatie m.b.t. het beroep doen op certificaten van een onderaannemer is juist.

Nr	Document	Paragraaf/ artikel	Vraag	Antwoord
			gegadigden voor dezelfde geschiktheidseisen een beroep mogen doen op diezelfde onderaannemer? Kunt u tevens bevestigen dat dit ook geldt indien de betreffende onderaannemer dezelfde certificeringen, expertise, referenties en/of overige ter beschikking gestelde capaciteit aan meerdere gegadigden beschikbaar stelt in het kader van deze aanbesteding? Indien hier beperkingen aan verbonden zijn, verzoeken wij u deze expliciet te benoemen.	
36		NvI-1 nr. 7	Klop het dat eenzelfde onderaannemer kan inschrijven met meerdere gegadigden? Als voorbeeld: Onderaannemer A schrijft in met Hoofdaannemer X en ook met Hoofdaannemer Y? Mag dat?	Ja, dit is toegestaan.
37		7.3.2 Geschiktheidseisen	De aanbestedende dienst vraagt inschrijvers om toe te lichten welke ervaring zij hebben met het omgaan met vertrouwelijke informatie en documenten, inclusief een beschrijving van de daarbij gehanteerde werkwijzen en maatregelen. Tegelijkertijd wordt als geschiktheidseis een aantoonbaar werkend ISMS conform ISO/IEC 27001 en BIO2 verlangd. Kan aanbestedende dienst toelichten waarom deze aanvullende eis noodzakelijk wordt geacht voor de hoofdopdrachtnemer, indien de inschrijver reeds aantoonbaar ervaring heeft met het verwerken van vertrouwelijke informatie en de daarbij getroffen organisatorische en technische beveiligingsmaatregelen beschrijft, terwijl de onderaannemer die verantwoordelijk is voor de productie en verwerking van bestanden beschikt over een ISO 27001-gecertificeerd ISMS en BIO2-conforme maatregelen? Wij constateren dat binnen de markt van gespecialiseerde DTP-bureaus een formeel ISMS conform ISO/IEC 27001 niet gebruikelijk is. Gelet op het feit dat de aanbestedende dienst in het selectiecriterium reeds uitgebreid beoordeelt welke technische, organisatorische en operationele maatregelen inschrijvers treffen ter bescherming van vertrouwelijke informatie, cybersecurity en embargo's, verzoeken wij toe te lichten welk aanvullend doel met deze geschiktheidseis wordt beoogd en hoe deze eis zich verhoudt tot het proportionaliteitsbeginsel.	Omgaan met vertrouwelijke informatie en werken met een embargo is voor de Onderzoeksraad van groot belang. De inhoud van rapporten mag absoluut niet voor de datum van publicatie van een onderzoeksrapport uitlekken. Een werkend ISMS borgt dat niet. Daarom vragen we dat uit in selectiecriterium 1. Zoals uit de andere antwoorden blijkt, mag u voor dit criterium een beroep doen op een ander. We willen die borging echter wel toegelicht zien.

Nr	Document	Paragraaf/ artikel	Vraag	Antwoord
38		7.3.2 Geschiktheidseisen	In antwoord op vraag 7 geeft u aan: "De eisen ten aanzien van kwaliteitszorg (ISO-9001) en informatiebeveiliging (ISO-27001 of gelijkwaardig en BIO 2) gelden voor de gehele opdracht van DTP en drukwerk, dus voor de hoofdopdrachtnemer en de onderaannemer(s)." Wij verzoeken u te verduidelijken hoe dit antwoord zich verhoudt tot de bepaling dat Geschiktheidseisen door hoofd- en onderaannemer gezamenlijk kunnen worden ingevuld. Kunt u bevestigen welke van onderstaande interpretaties juist is? A. De hoofdaannemer en de onderaannemer dienen ieder afzonderlijk te beschikken over een aantoonbaar werkend ISMS conform ISO/IEC 27001 en BIO2. Een hoofdaannemer die zelf niet aan deze geschiktheidseis voldoet, kan zich hiervoor niet beroepen op een onderaannemer. of B. Een hoofdaannemer mag zich voor deze geschiktheidseis beroepen op een onderaannemer die beschikt over een aantoonbaar werkend ISMS conform ISO/IEC 27001 en BIO2, waarbij hoofd- en onderaannemer gezamenlijk aan de geschiktheidseis voldoen. Wij verzoeken u expliciet aan te geven welke interpretatie van toepassing is	Interpretatie B is van toepassing.
39			In de Nota van Inlichtingen geeft de Onderzoeksraad meerdere malen aan dat een geldig ISO/IEC 27001-certificaat slechts wordt geaccepteerd indien tevens sprake is van een onafhankelijke audit waarbij een expliciete mapping heeft plaatsgevonden op ISO 27001-controls én BIO2-maatregelen, inclusief bewijs van de werking van het ISMS. Kan de Onderzoeksraad bevestigen dat een geldig ISO/IEC 27001-certificaat, afgegeven door een geaccrediteerde certificerende instelling, op zichzelf onvoldoende is om aan deze geschiktheidseis te voldoen? Indien dit inderdaad het standpunt van de Onderzoeksraad is, verzoeken wij de Onderzoeksraad te motiveren waarom deze aanvullende eis proportioneel wordt geacht. BIO2 is immers gebaseerd op ISO/IEC 27001 en ISO/IEC 27002 en een geldig ISO/IEC 27001-certificaat toont reeds aan dat sprake is van een aantoonbaar werkend Information Security Management	Zie antwoord vraag 37.

Nr	Document	Paragraaf/ artikel	Vraag	Antwoord
			System, inclusief risicobeheersing, interne audits, management reviews en continue verbetering. Daarnaast verzoeken wij de Onderzoeksraad toe te lichten welke specifieke BIO2-maatregelen zij noodzakelijk acht voor de uitvoering van deze opdracht en welke risico's hiermee worden afgedekt die volgens de Onderzoeksraad niet reeds door een gecertificeerd ISO/IEC 27001-managementsysteem worden beheerst. Wij constateren dat een verplichting tot aanvullende BIO2-auditmapping potentieel leidt tot uitsluiting van een aanzienlijk aantal ISO/IEC 27001-gecertificeerde marktpartijen die hun informatiebeveiliging aantoonbaar op orde hebben, maar niet beschikken over een separate BIO2-auditverklaring. Kan de Onderzoeksraad daarom verduidelijken welke concrete aanvullende BIO2-eisen worden verlangd bovenop een geldig ISO/IEC 27001-certificaat en waarom deze noodzakelijk en proportioneel worden geacht voor de uitvoering van deze opdracht?	