Provincie Noord-Brabant

Er zijn in het kader van de eerste Nota van Inlichtingen een aantal vragen gesteld m.b.t. eisen die in het kader van de technische bekwaamheid worden gesteld bij de aanbesteding. Specifiek gaat het daarbij over vragen die zijn gesteld over de eisen m.b.t. Informatiebeveiliging die zijn opgenomen in paragraaf 3.4.2 van het beschrijvend document. Gezien het belang van de antwoorden op deze vragen voor potentiele inschrijvers heeft de Provincie besloten om de vragen m.b.t. dit onderwerp die zijn ontvangen tot en met 21 februari j.l. vooruitlopend op de publicatie van de geplande Nota van Inlichten bij deze te publiceren.

Ref. nr.	Onderwerp	Vraag	Antwoord
1	3.4.2 Informatiebeveiliging	Belangrijk om te realiseren is dat voor analyseopdrachten binnen perceel 2, alle data binnen het platform van de Provincie Noord-Brabant blijft. De informatiebeveiligingseisen en -procedures van dit platform zijn dus leidend en bieden de specifieke beveiligingscontext. Er is dan geen directe noodzaak voor een ISO27001-certificering voor een leverancier voor perceel 2, aangezien de provinciale platform specifieke beveiligingsmaatregelen het beveiligingskader bieden. Het stellen van een ISO27001-certificeringseis voor perceel 2 kan, hoewel goedbedoeld, onbedoeld hindernissen opwerpen voor creativiteit en samenwerking. Voor organisaties met een focus op analyse en ontwikkeling, zoals de onze, kan het volgen van de uitgebreide vereisten van ISO27001 een aanzienlijke inspanning vergen, die niet in verhouding staat tot de aard van de werkzaamheden binnen dit perceel. Wij pleiten daarom voor een heroverweging van de ISO27001-certificeringseis voor perceel 2 en deze te laten	Wij stemmen er niet mee in om de betreffende eis te laten vervallen.
5	BIO (Baseline Informatiebeveiliging Overheid) daar waar informatie zich bevind.	De aanbesteding handelt om het inhuren van medewerkers die de Provincie inzet om op locatie van de Provincie op haar eigen systemen te laten werken aan BI, analytics en het dataplatform. Niets van de o.b.v. BIO te beveiligen data van de Provincie komt daarbij op systemen van de te contracteren opdrachtnemers terecht. De eis dat de systemen van die opdrachtnemers BIO compliant moeten zijn en dat dit via externe audits zou moeten worden aangetoond is dus niet van toepassing. Wij verzoeken u daarom deze eis te schrappen. Gaat u daarmee akkoord? Zo nee, beseft u dan dat het aantal potentiele inschrijvers voor de Provincie te laag zal zijn omdat geen van de aanbieders op de tijdelijk in te huren capapaciteit hierop ingericht zal zijn? Om deze stelling te bewijzen het volgende feit: Wij zetten voor miljoenen om in onze ICT services aan de meeste Nederlandse lokale overheden en laten andere partijen geen audit doen op onze systemen m.b.t. BIO Compliancy. De Provincie zou de eerste partij zijn waarvoor wij zoiets zouden laten doen.	In de wijze van aanbesteding is het ook mogelijk dat er door de medewerkers die worden ingehuurd wordt gewerkt op eigen apparatuur op een locatie buiten het provinciehuis. Aangezien informatiebeveiliging van toepassing is op de gehele keten gaan wij niet akkoord met het schrappen van de betreffende eis.

6	BIO (Baseline Informatiebeveiliging Overheid)	We willen u erop wijzen dat de BIO niet integraal opgelegd kan worden aan dienstenleveranciers. Het voldoen aan de overheidsnorm BIO is uiteindelijk aan de Provincie. Tegelijkertijd weten we dat de BIO gestoeld is op ISO 27001, waaraan inschrijver voldoet. We stellen daarom voor om hier aan te geven dat de informatiebeveiliging bij leverancier plaatsvindt volgens de norm ISO 27001. Gaat u hiermee akkoord? Zo nee, - waarom niet? - wat is volgens de Provincie de toegevoegde waarde van BIO bovenop de genoemde ISO normering?	De Baseline Informatiebeveiliging Overheid (BIO) is inderdaad gestoeld op de ISO27001, echter in de BIO zijn boven op de eisen vanuit de ISO27001 door de overheid extra maatregelen toegevoegd. Deze maatregelen, ook wel verplichte overheidsmaatregelen genoemd, hebben een verplichtend karakter en moeten derhalve geimplementeerd worden. Het uitbesteden van de dienst ontslaat de overheid dus niet dat de betreffende maatregelen geimplementeerd dienen te worden. Wij gaan dus niet akkoord met het aanbieden van de dienst op basis van alleen een ISO27001 certificaat. De dienst zal ook BIO compliant moeten zijn. Voorwat betreft het intergraal opleggen van de BIO eisen het volgende: wij hebben vastgesteld dat de informatie binnen de aanbesteede dienst van het niveau BBN2 is en daar mee is de gehele BIO van toepassing. (BBN1 en BBN2)
33	Beschrijvend document 3.4.2. pagina 20	Indien u niet akkoord kan gaan om de bepaling over de BIO te laten vervallen, kunt u dan (1) specificeren wat u bedoelt met 'voor de gehele keten' indien het perceel B betreft? En (2) kunt u aangeven welke eisen u stelt aan een onafhankelijke auditor en de verklaring die deze onafhankelijke auditor moet afgeven?	Met de gehele keten wordt bedoeld alles wat nodig is om de gevraagde dienst aan te bieden (mens, apparatuur, informatie, locaties etc). Voorwat betreft de auditor, bij gunning zal er een toets plaatsvinden door een externe auditor om vast te stellen of de betreffende inschrijver voldoet aan de gestelde BIO eisen.
62	Beschrijvend document 3.4.2. pagina 20	Inschrijver stelt voor om de bepaling over de BIO te laten vervallen voor perceel B. De inschrijver zal, indien de aanbesteding gewonnen wordt immers werkzaam zijn binnen de omgeving van de provincie Noord-Brabant conform haar werkprocessen. De provincie is al BIO-compliant. Wat voegt het wel/niet BIO compliant zijn van inschrijver hier aan toe?	Zie het antwoord op vraag 5, 6 en 33.
137	Algemeen	In de stukken staat dat "Inschrijver dient BIO (Baseline Informatiebeveiliging Overheid) compliant te zijn voor de gehele keten welke betrekking heeft op de aard van de leveringen en de diensten als omschreven in dit document. Deze compliance dient bij gunning aangetoond te worden door een zogenaamde in-control verklaring opgesteld door een onafhankelijke auditor.". Nu zijn wij wel ISO27001, NEN 7510 (Nederlandse norm voor informatiebeveiliging in de zorgsector)? Is/blijft een bij gunning aantoonbare BIO-compliancy verplicht of mag dat evt ook later aangetoond worden? BIO-compliancy is zeer ongebruikelijk om te eisen bij een aanbesteding.	De Baseline Informatiebeveiliging Overheid (BIO) is gestoeld op de ISO27001, echter in de BIO zijn boven op de eisen vanuit de ISO27001 door de overheid extra maatregelen toegevoegd. Deze maatregelen, ook wel verplichte overheidsmaatregelen genoemd, hebben een verplichtend karakter en moeten derhalve geimplementeerd worden. Het uitbesteden van de dienst ontslaat de overheid dus niet dat de betreffende maatregelen geimplementeerd dienen te worden. Wij gaan dus niet akkoord met het aanbieden van de dienst op basis van alleen een ISO27001 certificaat. De dienst zal ook BIO compliant moeten
200	Beschrijvend document, 3.4.2 Informatiebeveiliging - in-control verklaring	Aanbesteder eist een in-control verklaring opgesteld door een onafhankelijke auditor voor het compliant zijn aan de BIO. Inschrijver beschikt over diverse ISO-certificaten (waaronder ISO 27001 en ISO 27701) en ISAE assurance reports. Bent u akkoord dat dit de eis mbt de in-control verklaring afdoende afdekt?	De Baseline Informatiebeveiliging Overheid (BIO) is gestoeld op de ISO27001, echter in de BIO zijn boven op de eisen vanuit de ISO27001 door de overheid extra maatregelen toegevoegd. Deze maatregelen, ook wel verplichte overheidsmaatregelen genoemd, hebben een verplichtend karakter en moeten derhalve geimplementeerd worden. Het uitbesteden van de dienst ontslaat de overheid dus niet dat de betreffende maatregelen geimplementeerd dienen te worden. Wij zijn dus van mening dat het door u gestelde onvoldoende dekking biedt en gaan hier dus niet mee akkoord.