
NOTA VAN INLICHTINGEN

Datum: 8 april 2025

Behorende bij:

Netwerk PNB locaties

Kenmerk: C2348739

Deze Nota van Inlichtingen verduidelijkt de antwoorden op de vragen 79, 126, 157 en 158 in de Nvl van 31 maart 2025 en dient te worden beschouwd als een integraal onderdeel van de Selectieleidraad. De gestelde vragen zoals opgenomen in deze Nota van Inlichtingen zijn letterlijk overgenomen zoals deze zijn gesteld.

Deze Nota van Inlichtingen is ter beschikking gesteld op www.tenderned.nl

Uiterste inleverdatum aanmelding : 23 april 2025, 12:00 uur
Inleverlocatie : elektronisch via TenderNed

Ref. Nr.	Onderwerp	Vraag	Antwoord
79	Bijlage 4. verwerkersovereenkomst art. 10.4	Inschrijver acht een potentieel ongelimiteerde contractuele boete niet proportioneel. Ook omdat gegeven de aard van de dienst een evt. tekortkoming wellicht niet in 1 of 2 dagen verholpen is. Art. 10.4 laat open of mitigerende maatregelen niet zijnde een definitieve oplossing de werking van dit boetebeding opschorten. Inschrijver stelt voor dit boetebeding te stellen op € 1.000,- per week met een maximum van € 10.000,-. Bent u daarmee akkoord?	Niet akkoord. Toelichting: boetes van de Autoriteit Persoonsgegevens kunnen veelvoudenvan dit bedrag bedragen.
126	Verwerkersovereenkomst art. 10.4	Verzoek om een maximum boete per overtreding op te nemen van 10.000 euro nu er enkel een boete per dag geldt.	Niet akkoord. Toelichting: boetes van de Autoriteit Persoonsgegevens kunnen veelvoudenvan dit bedrag bedragen.
157	Bijlage 1 Beschrijving Opdracht Netwerk PNB Locaties.pdf - Hoofdstuk 7 Eisen - Eisen Informatiebeveiliging en Privacy - Eis 3	De BIO is opgesteld door en voor de overheid. De basis voor te implementeren maatregelen in een bepaalde omgeving is een risico analyse op die omgeving. Uit 1.2 van de huidige BIO 1.04z: - Het lijnmanagement stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vast. - Op basis van de betrouwbaarheidseisen kiest, implementeert en draagt het lijnmanagement de maatregelen uit. Daarnaast zijn er verantwoordelijken vastgelegd in de BIO: Secretaris/algemeen directeur, Proceseigenaar en Dienstenleverancier. Het is daarom van belang dat de Opdrachtgever PNB niet een algemene eis voor compliant zijn aan de gehele BIO stelt aan de opdrachtnemer, maar duidelijk maakt voor welke maatregelen de opdrachtnemer (dienstenleverancier) verantwoordelijk is en BIO compliant moet zijn. Wilt u de geselecteerde maatregelen die van toepassing zijn publiceren? Zo niet, wilt u uitleggen waarom niet?	De provincie stelt in zijn algemeenheid te voldoen aan BIO Basis Beveiligingsniveau 2 (BBN2). Voor de leverancier geldt dat deze ISO27001 is gecertificeerd. De maatregelen zoals die opgetekend in de ISO-normering en dus mede zijn benoemd in de BIO 1.04 worden niet meegenomen in de audit. Binnen de BIO zullen alleen de maatregelen worden getoetst die a) van toepassing zijn onder de vermelding 'dienstenleverancier' vermeld bij de maatregelen en b) van toepassing zijn over de scope van de betreffende dienstverlening. Vooralsnog mag ervanuit worden gegaan dat dit alle aanvullende BIO-maatregelen betreft met de vermelding 'dienstenleverancier'.
158	Bijlage 1 Beschrijving Opdracht Netwerk PNB Locaties.pdf - Hoofdstuk 7 Eisen - Eisen Informatiebeveiliging en Privacy - Eis 3	Opdrachtnemer is reeds gecertificeerd voor de ISO27001:2022. - Waarom dan opnieuw een volledige audit op de BIO (inclusief de gehele ISO27001)? Dit is inefficiënt in tijd en geld voor beide partijen omdat hiermee onnodig dubbel werk wordt verricht. - Er is geen vastgestelde, erkende BIO audit of auditor. Een audit op de BIO geeft daarom nooit een uitsluitende en erkende uitslag door een geaccrediteerde instantie. M.a.w.: de uitkomsten van een audit zijn daarom altijd voor discussie vatbaar. Het is efficiënter om een gezamenlijk assessment van de geselecteerde BIO maatregelen voor opdrachtnemer uit te voeren en de uitkomst daarvan vast te leggen en waar nodig gezamenlijk aan verbeteringen te werken. Bent u het eens met bovenstaande en de conclusie en wilt u de opdracht hier op aanpassen? Zo niet, wilt u uitleggen waarom niet?	Stelling 1: De provincie stelt in zijn algemeenheid te voldoen aan BIO Basis Beveiligingsniveau 2 (BBN2). Voor de leverancier geldt dat deze ISO27001 is gecertificeerd. De maatregelen zoals die opgetekend in de ISO-normering en dus mede zijn benoemd in de BIO 1.04 worden niet meegenomen in de audit. Binnen de BIO zullen alleen de maatregelen worden getoetst die a) van toepassing zijn onder de vermelding 'dienstenleverancier' vermeld bij de maatregelen en b) van toepassing zijn over de scope van de betreffende dienstverlening. Voor de ISO wordt de certificering en de daarover geldende verklaring van toepasselijkheid verwacht. De gelijke ISO-maatregelen zoals weergegeven in de BIO worden dus niet opnieuw ge-audit. Stelling 2: De provincie is het niet eens met de stelling dat er discussie kan zijn over de bevindingen van een auditor aangaande maatregelen die zijn gesteld in de BIO. BIO-maatregelen zijn logische verduidelijkingen/uitlopers van de bovenliggende ISO-maatregelen en liggen in lijn met de al gestelde ISO-maatregel. Daarmee schept de BIO dus een verduidelijking om juist de discussie over algemeen gestelde maatregelen vanuit de ISO te voorkomen.