

Nota van Inlichtingen 2 220026REG Basisdienstverlening Platform Duurzaam Drechtsteden DEF 06-11-2023

#	Fase	Label	Onderwerp	Vraag	Antwoord
1	NvI1	Vraag 8	Certificering CRM-software	In uw antwoord op vraag 8 inzake Certificering CRM-software laat u een eis vervallen en stelt u als nieuwe eis de certificering ISO 27001. Hiervoor gelden dezelfde punten als waarom u de eis van NEN-ISO 16175-3 certificering liet vallen: Dit is eveneens geen eis in de VNG handreiking voor kwaliteitscriteria energieloketten. En ook deze eis handhaven werkt (fors) kostenverhogend en verlaagt de toegankelijkheid voor meerdere marktpartijen. Gaat u akkoord met het aanpassen van deze eis naar één van de volgende twee mogelijkheden: 1) Periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISAE3xxx SOC type II) of; 2) Een Assurance rapport van een auditor die is aangesloten bij NOREA. Hiermee voldoet u aan hetgeen wordt gesteld vanuit de Vereniging van Nederlandse gemeenten / Informatiebeveiligingsdienst voor Gemeenten om informatiebeveiliging aan te tonen	Hiermee gaan wij niet akkoord. Wel volstaat het wanneer de Inschrijver aangeeft bereid te zijn deze certificering binnen maximaal 1,5 jaar na opdrachtverlening te behalen. De aanbestedende dienst toetst hiervan na 1 jaar de status.
2	NvI1	Vraag 8	Certificering CRM-software	In de beantwoording op de vraag over de ISO normering lijkt het of u voorbij gaat aan de BIO Normering op BBN2 niveau. Een leverancier zou moeten voldoen aan de Baselinetoets BIO op BBN niveau 2 voor deze opdracht. Gaat u ermee akkoord als de opdrachtnemer kan aantonen te voldoen aan deze toets zoals deze door de informatiebeveiligingsdienst is weergegeven op https://www.informatiebeveiligingsdienst.nl/product/baselinetoets-bbn-bio/ ? Daarmee wordt meer dan de ISO Norm getoetst, voldoet de opdrachtnemer aantoonbaar aan de onderliggende eisen die de opdrachtgever stelt en voldoet de opdrachtgever aantoonbaar aan zijn verplichtingen in het kader van de verplichte BIO normering voor de overheid.	Hiermee gaan wij niet akkoord. De BIO is afgeleid van ISO27001 en ISO27002 en verder afgestemd op overheidsprocessen en -systemen. Enkel het invullen van de baselinetoets is te summier en geeft geen (volledige) inzage in hoe de levercier voldoet, dan wel ontbreken periodieke controles (audits).