

Richtlijn Inhoud van de verkorte TPM voor aansluiting op VECOZO.

Versie 2.0 (5-7-2019)

Dit document geeft een toelichting op de eis zoals beschreven in de VECOZO Generieke Aansluitvoorwaarden (VGA) ten aanzien van de aantoonbaarheid van het voldoen aan NEN7510.

Het eerste hoofdstuk beschrijft in zijn algemeenheid de term TPM. Omdat er geen standaard is ten aanzien van een TPM is de informatie in hoofdstuk 1 samengesteld op basis van deskresearch en is een verwoording van de generieke toepassing van een TPM in Nederland.

Het tweede hoofdstuk beschrijft de specifieke voor VECOZO bedoelde TPM (verkorte TPM) welke minimaal voorhanden moet zijn om aan te tonen dat men voldoet aan de NEN7510. VECOZO hoeft namelijk geen inzicht in de volledige details en resultaten van de audit, maar wil wel zekerheid verkrijgen dat een partij aan de gestelde eis voldoet.

1 TPM algemeen

1.1 Wat is een TPM?

TPM staat voor Third Party Mededeling, ook wel Third Party Memorandum of Derdenverklaring genoemd.

Een onafhankelijke certificerende instantie kan een goedkeurende verklaring geven dat de processen in een organisatie voldoen aan vooraf opgestelde criteria. Dit kan in de vorm van een ISAE 3000 of 3402 rapport.

Men noemt dit een Third Party Mededeling omdat bij een TPM 3 partijen zijn betrokken. De eerste partij is de leverancier van diensten, de tweede partij is de afnemer van de diensten en de derde partij is een onafhankelijke derde (de auditor die op basis van een onderzoek (de audit) een oordeel geeft over de mate waarin de leverancier voldoet aan een bepaald normenkader.

1.2 Waarom een TPM?

Om kosten te besparen en de kwaliteit te verbeteren, maken partijen soms de bewuste keuze administratieve- en/of ICT-diensten uit te besteden aan een gespecialiseerde leverancier van administratieve- en/of ICT-diensten. Bij deze uitbesteding rijzen vragen als: hoe is het bij de leverancier gesteld met de beveiliging, continuïteit en privacy van gevoelige informatie? Om hier meer zekerheid over te krijgen kan de leverancier door middel van een audit worden onderzocht. Doel van het onderzoek is om de afnemer (of ander belanghebbenden) een redelijke mate van zekerheid te geven over de opzet en het bestaan (op enig moment) en de werking (gedurende een bepaalde periode) van beheersmaatregelen als onderdeel van een normenkader. Deze beheersmaatregelen dragen zorg voor het borgen van de betrouwbaarheid (juistheid, tijdigheid, volledigheid, exclusiviteit en continuïteit) van de door de leverancier geleverde diensten. Het resultaat van het onderzoek (de mate waarin de leverancier voldoet aan een normenkader) wordt verwoord in een TPM.

1.3 Wat is de meetlat waartegen beoordeeld wordt?

Tijdens het onderzoek worden de kwaliteit van beheersmaatregelen bepaald op basis van een vooraf overeengekomen normenkader. Dit normenkader kan bijvoorbeeld NEN7510 zijn, maar ook ISO27001. Aan het onderzoek is de inherente beperking verbonden dat niet met absolute, maar met redelijke mate van zekerheid kan worden vastgesteld of in alle gevallen de maatregelen uit het normenkader zijn toegepast. De beoordeling of een partij bijvoorbeeld voldoet aan de NEN7510 kan en mag gebaseerd zijn op de resultaten van andere onderzoeken op basis van een ander normenkader (ISO27001); het is de taak van de auditor om te beoordelen of de resultaten van andere onderzoeken als input kunnen dienen voor het op dat moment uit te voeren onderzoek.

1.4 Wie voert het onderzoek uit?

Het onderzoek dient uitgevoerd te zijn door of onder leiding te staan van een onafhankelijke auditor. Deze onafhankelijke auditor dient de TPM ook ondertekend te hebben.

1.5 Wat wordt er onderzocht?

Het object van het onderzoek wordt door de klant/afnemer in overleg met de producent/leverancier bepaald en is afhankelijk van het gekozen normenkader en de gewenste zekerheid.



2 Verkorte TPM

2.1 Wat is een verkorte TPM?

Een verkorte TPM is een soort samenvatting van de gehele TPM. Een verkorte TPM bevat niet alle details en eventuele bevindingen, maar geeft in het kort de eindconclusie weer van het onderzoek. Daarmee is een verkorte TPM een geschikt middel om, vanuit het oogpunt van zorgplicht, zekerheid te krijgen of een partij voldoet aan een bepaald normenkader zonder dat het noodzakelijk is dat de betreffende partij alle details hierover openbaar maakt.

VECOZO vraagt u dus niet om het auditrapport of een volledige TPM aan te leveren, maar om een verkorte TPM.

Een NEN7510 certificaat, afgegeven door een geaccrediteerde organisatie (zie ook paragraaf 2.4), zien wij ook als vorm van een verkorte TPM. Voor een geldig NEN7510 certificaat gelden onderstaande eisen niet.

2.2 Welke specifieke eisen gelden voor de verkorte TPM om te voldoen aan de VGA?

Een verkorte TPM dient minimaal te bevatten:

- (KvK) Naam van de onderzochte partij.
- Het toegepaste normenkader zijnde NEN7510:2017.
- Object van onderzoek, inclusief organisatorische scope in geval van bijvoorbeeld meerdere vestigingen en/of uitbesteding aan derden. Het object van onderzoek dient te zijn: alle locaties waar persoonsgegevens verwerkt worden (conform de Algemene Verordening Gegevensbescherming) met betrekking tot de (directe of indirecte) verlening van zorg en waarvan de verwerking onder de juridische verantwoordelijkheid van de betreffende partij valt.
- De naam en handtekening van de persoon die de verkorte TPM afgeeft.
- De titel van deze persoon, zijnde RE en/of CISA. Deze titel dient bovendien in het passende register geregistreerd en daarmee verifieerbaar te zijn (zie paragraaf 2.3 Registers).
- Datum waarop het onderzoek is afgerond.
- De uitspraak (conclusie) in hoeverre de onderzochte partij in opzet en bestaan voldoet aan het gestelde normenkader.

2.3 Registers om titels te verifiëren

- Bij Norea geregistreerde titel RE > website van Norea (<https://www.norea.nl/register>)
- Bij ISACA geregistreerde titel CISA > website van ISACA (Certification Number moet aangeleverd worden) (<http://www.isaca.org/CERTIFICATION/Pages/default.aspx> onder "Verify a Certification".)

2.4 Geaccrediteerde organisaties

Overzicht van geaccrediteerde organisaties welke mogen certificeren tegen NEN7510 is te vinden op de website van de NEN (<https://www.nen.nl/Normontwikkeling/Certificaten/Schemabeheer/Register-NEN-7510.htm>)

Op dezelfde pagina is een overzicht van organisaties welke gecertificeerd zijn volgens NEN7510.

--/--

