NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Ministerie van Volksgezondheid,
Welzijn en Sport
Postbus 20305
2500 EJ DEN HAAG

Datum : dinsdag 9 juni 2020
Kenmerk : NOREA /AB2020/wo89
Betreft : Reactie NOREA n.a.v. consultatie Wetsvoorstel Elektronische Gegevensuitwisseling in de Zorg

Geachte heer/mevrouw,

Met interesse hebben wij kennis genomen van het concept Wetsvoorstel Elektronische Gegevensuitwisseling in de Zorg. Als NOREA, de beroepsorganisatie van IT-auditors, willen wij graag reageren op artikel 3 en de daarbij behorende Memorie van Toelichting, betreffende de certificering van informatietechnologieproducten of -diensten.

In artikel 3 wordt vermeld dat de informatietechnologieproducten of -diensten dienen te worden gecertificeerd door een door de Minister aangewezen instelling, die dient te beschikken over een accreditatie van de Stichting Raad voor Accreditatie. Wij wijzen er in dat verband op dat certificering een beperkte mate van diepgang heeft, waarbij onder andere een controlerend accountant niet kan steunen op de uitkomsten van een certificering, waardoor deze alsnog zelfstandig audit-werkzaamheden dient uit te voeren tijdens een jaarrekeningcontrole bij een zorginstelling die gebruik maakt van de gecertificeerde dienst.

IT-auditors die zijn ingeschreven in het register van NOREA (een zusterorganisatie van de Nederlandse Beroepsvereniging voor Accountants (NBA)), zijn bevoegd om Assurance-rapportages uit te brengen waarin verslag wordt gedaan van de toetsingswerkzaamheden op een systeem of een dienst. De rapportage laat duidelijk zien welke maatregelen zijn getoetst, of de beheersingsmaatregelen gedurende de verslagperiode hebben gefunctioneerd, wat de eventuele bevindingen zijn en het hiermee samenhangende

POSTADRES
POSTBUS 7984
1008 AD AMSTERDAM

BEZOEKADRES
ANTONIO VIVALDISTRAAT 2-8
1083 HP AMSTERDAM

E-MAIL EN WEBSITE
NOREA@NOREA.NL
WWW.NOREA.NL

OVERIG
TEL: 00 31 (0)20 301 03 80
KVK-NR: 40537540
IBAN: NL02ABNA0475165403

oordeel. Dit rapport wordt opgesteld op basis van de NOREA-Richtlijn 3000, welke is ontleend aan de Standaard 3000 van NBA.

Een dergelijke rapportage kan zowel door de zorginstelling zelf als door de controlerend accountant worden gebruikt om zekerheid te krijgen over een betrouwbare gegevensverwerking. Er wordt daarmee volledig tegemoet gekomen aan de doelstelling die met artikel 3 wordt beoogd.

Wij willen derhalve verzoeken de specifieke verwijzing te schrappen inzake het moeten beschikken over een accreditatie van de Stichting Raad voor Accreditatie. Hiermee wordt de mogelijkheid gecreëerd om -waar gewenst- een onderzoek te laten uitvoeren door een erkende register IT-auditor, op basis van assurance-richtlijnen.

Volledigheidshalve wijzen we in dat verband ook op soortgelijke audit- en assurance-trajecten, waarbij Register IT-auditors worden ingezet ten behoeve van het verstrekken van zekerheid over informatietechnologieproducten en -diensten en/of de beoordeling van de vereiste technische of organisatorische beveiligingsmaatregelen op grond van de voornoemde assurance-richtlijnen. Voorbeelden daarvan zijn: de VIPP-assessments (VWS), DigiD-assessments (BZK/Logius), SUWINET-audits (SZW/UWV) en de audits krachtens de Wet Politiegegevens (MVJ/BZK/MinvDef).

Uiteraard zijn we graag bereid tot nadere toelichting en overleg over een eventuele auditaanpak als alternatief voor of aanvulling op de voorgestelde certificering en accreditatie.

Met vriendelijke groet,

Namens het bestuur,

i/o

I.J.M. Vettewinkel-Raymakers RE,
Voorzitter