## Praktijk verstoort Europese markt

# Strenge NEN-normen bij IT-aanbestedingen?

**IT-aanbestedingsdocumenten bevatten vaak een eindeloze reeks aan eisen waarop de inschrijver simpelweg ‘ja’ dient te antwoorden. Voor het gemak verwijzen deze eisen vaak naar normenkaders. Sommige van deze normenkaders zijn vastgesteld door internationale organisaties (zoals ISO) en anderen door nationale instituten (zoals NEN). In dit artikel belichten Menno de Wijs en Jeroen van Helden de vraag waar een aanbestedende dienst of inschrijver op moet letten bij het specificeren van opdrachten aan de hand van normenkaders.**

Beeld: Shutterstock



AG0324_IT-studie_2.indd 62 06-06-2024 11:30

HET AANBESTEDINGSRECHTELIJK KADER IS VOOR ALLE IT-AANBESTEDINGEN VERGELIJKBAAR, maar om het concreet te maken zoomen wij in dit artikel in op informatiebeveiliging in de zorg. Een eis die wij met enige regelmaat voorbij zien komen in IT-aanbestedingen binnen het zorgdomein is dat de inschrijver en diens onderaannemers dienen te beschikken over een NEN 7510 certificaat.
Wat houdt dit precies in?

De NEN 7510 geeft een kader voor de inrichting van organisatorische en technische beveiligingsmaatregelen binnen de gezondheidszorg. Het beschrijft hoe risico's beheerst kunnen worden en welke beheersmaatregelen genomen kunnen worden om te waarborgen dat data beschikbaar, integer en vertrouwelijk blijven. De NEN 7510 wordt aangevuld met enkele normen waarin elementen uit de NEN 7510 verder zijn uitgewerkt, zoals de NEN 7512 (gegevensuitwisseling) en NEN 7513 (logging). Dat er specifiek voor informatiebeveiliging in de zorg een norm is ontwikkeld laat zich eenvoudig verklaren. Het wemelt hier niet alleen van de bijzondere persoonsgegevens, maar ook vindt veelvuldig uitwisseling van die gegevens plaats.
Denk bijvoorbeeld aan patiëntportalen waar patiënten toegang krijgen tot hun gegevens, de uitwisseling van uitslagen tussen het lab en zorginstellingen, of communicatie tussen specialisten en huisartsen.

Naleving van NEN 7510, NEN 7512 en NEN 7513 is door de wetgever wettelijk verplicht gesteld. Ingevolge de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpg) moet een zorgaanbieder ervoor zorgen dat diens zorginformatiesysteem voldoet aan NEN 7510, NEN 7512 en NEN 7513 en dat hij overeenkomstig deze normen gebruik maakt van het elektronisch uitwisselingssysteem waarop hij is aangesloten [1].

## Advies bij NEN

Een goed begrip van de NEN 7510 norm is – gelet op de technische en specialistische inhoud – vaak niet weggelegd voor het bestuur of de afdeling IT van een zorgaanbieder. Op de markt zijn dan ook veel partijen actief die zorgaanbieders adviseren over het implementeren van maatregelen om aan deze norm te voldoen. Onderdeel van een dergelijk traject is vaak certificering. Certificering is weliswaar niet wettelijk verplicht voor zorgaanbieders, maar vaak toch een logische stap. Daarmee kan de zorgaanbieder immers aantonen dat zij voldoet aan de NEN 7510 en kan zij aantonen dat zij dus voldoet aan haar wettelijke verplichting om conform die norm te werken.
Bovendien schrijft NEN 7510 voor dat periodiek een beoordeling plaatsvindt die aantoont dat volgens de norm wordt gewerkt [2].

## Eis aan inschrijvers

De meeste zorgaanbieders ontwikkelen en beheren uiteraard niet zelf hun zorginformatiesystemen. Zij maken daarvoor gebruik van de diensten van IT-leveranciers. Gelet op het voorgaande is het geen verrassing om te lezen dat veel zorgaanbieders aan hun IT- leveranciers opleggen dat zij op hun beurt ook dienen te voldoen aan de NEN 7510.
Ter controle daarvan zien wij met enige regelmaat in (concept-)aanbestedingsdocumenten de eis terugkomen dat de inschrijver, én door haar in te schakelen derden, dienen te beschikken over een NEN 7510 certificaat.

## Problematiek

De eis van een NEN 7510 certificaat kan problematisch zijn. Veel IT-leveranciers werken met buiten Nederland

> Met een NEN 7510 certificaat toont de zorgaanbieder aan dat hij voldoet aan de wettelijke verplichting van die norm



AG0324_IT-studie_2.indd 63 06-06-2024 11:30

Vaak wordt gedacht dat NEN 7510 hetzelfde is als de internationale ISO27001, maar dat is onjuist

gevestigde onderaannemers. Die onderaannemers zullen geen NEN 7510 certificaat hebben, aangezien dit een Nederlandse norm betreft. Uit de praktijk begrijpen wij dat een buiten Nederland gevestigde onderneming geen certificaat kan aanvragen: de certificerende partijen bieden simpelweg geen certificeringsdiensten aan buiten Nederland.

De NEN 7510 heeft een internationale tegenhanger waarvan vaak gedacht wordt dat die identiek is, namelijk de ISO27001. Dat lijkt niet geheel juist, aangezien de NEN 7510 drie extra beheersmaatregelen kent en ruim 30 beheersmaatregelen in de NEN 7510 een extra specificatie bevatten. Ondanks de identieke basisnorm is de NEN 7510 dus uitgebreider. Daar komt nog bij dat de wet nu eenmaal de NEN 7510 voorschrijft en niet de ISO27001 [3]. Het simpelweg volstaan met voldoen aan de internationale tegenhanger is dus niet voldoende.

Het behoeft geen toelichting dat voorgaande praktijk de Europese interne markt verstoort. Er is namelijk sprake van een drempel voor buitenlandse partijen om mee te dingen naar een te gunnen opdracht. Vanuit die optiek dringt zich de vraag op: is het eigenlijk wel toegestaan een NEN 7510 certificaat te eisen en partijen zonder certificaat uit te sluiten?

## Interne markt

Het eisen van een certificaat dat onmogelijk is te bemachtigen door een ondernemer in een andere Europese lidstaat, laat weinig over van de Europese gedachte dat er één interne markt is binnen Europa. Buiten Nederland gevestigde partijen maken dan immers geen kans op de te gunnen opdracht. Het Werkingsverdrag van de Europese Unie verbiedt alle maatregelen die invoer tussen de lidstaten op enige wijze beperkt [4]. Daar komt bij dat de Aanbestedingswet [5] (in artikel 1.8 Aw) bepaalt dat ondernemers op gelijke en niet-discriminerende wijze moeten worden behandeld. Het feitelijk uitsluiten van ondernemers omdat zij niet in Nederland zijn gevestigd zou discriminerend zijn. De Aanbestedingswet bepaalt bovendien uitdrukkelijk dat als een certificaat wordt geëist, dat de aanbestedende dienst niet zomaar inschrijvers zonder certificaat mag uitsluiten. Toegestaan moet worden dat een inschrijver zónder certificaat mag aantonen dat zij voldoet aan alle – aan het certificaat verbonden – voorwaarden [6]. Dat bewijs mag een inschrijver met ieder passend middel leveren [7]. Als een inschrijver kan aantonen dat zij aan alle eisen van de NEN 7510 voldoet, dan moet die inschrijver dus kunnen meedingen naar de opdracht.

## Afronding

Misvatting is dus dat zorginstellingen en hun leveranciers over een NEN 7510 certificaat moeten beschikken. De wettelijke verplichting beperkt zich tot het vereiste dat zij werken volgens die norm. Een certificaat is weliswaar een eenvoudig bewijsstuk om aan te tonen dat aan de norm wordt voldaan, maar het is geen hard vereiste. Ook op andere manieren mag worden aangetoond dat voldaan wordt aan de eisen die onderdeel zijn van de NEN 7510 norm, denk bijvoorbeeld aan een interne audit. Iedere eis die daarmee in strijd is, zal bij een rechter geen stand mogen houden wegens strijd met Europees- en Nederlands recht.

Komt u een dergelijke eis toch tegen, wees dan proactief en stel hierover vragen. Dat zal de deur moeten openen naar de mogelijkheid om die buiten Nederland gevestigde onderaannemer in te schakelen. Dat maakt wellicht het verschil waarmee uw inschrijving nét iets hoger scoort.

***referenties***

*[1] Artikel 15j Wabvpg samen met de artikelen 3 t/m 5 Besluit elektronische gegevensverwerking door zorgaanbieders. Zie ook artikel 2.*

*[2] Regeling gebruik burgerservicenummer in de zorg, zie o.a. onderdeel 18.2.1 in NEN 7510.*

*[3] Artikel 2 Regeling gebruik burgerservicenummer in de zorg.*

*[4] Artikel 34 VWEU.*

*[5] Waarvan in het algemeen kan worden gezegd dat weliswaar academische ziekenhuizen gebonden zijn aan de Aanbestedingswet maar niet alle zorginstellingen.*

*[6] Aldus artikel 2.78a leden 3 en 4 Aw.*

*[7] Zo bevestigt ook de Commissie van Aanbestedingsexperts in advies 442: "5.3.11. (...) De Commissie wijst er overigens op dat een inschrijver daarnaast op basis van de artikelen 2.77, lid 1, en 2.78 Aw 2012 met elk passend middel mag aantonen dat de door hem voorgestelde oplossing op gelijkwaardige wijze voldoet."*

**Menno de Wijs**
is advocaat aanbestedingsrecht bij De CLERCQ Advocaten Notariaat. Dagelijks adviseert en procedeert hij op het gebied van IT-aanbestedingsrecht en ondernemingsrecht.

**Jeroen van Helden**
is advocaat IT, Privacy & Cybersecurity bij De Clercq Advocaten Notariaat. Dagelijks adviseert en procedeert hij op het gebied van (internationale) privacy, dataprotectie en IT-projecten.



AG0324_IT-studie_2.indd 64 06-06-2024 11:30