Consultatie Uitvoeringswet Algemene Verordening Gegevensbescherming

Het is geen geheim dat in de implementatie van de norm voor informatiebeveiliging NEN7510 (nog steeds) een uitdaging is in de eerste lijn. Hoewel de aanscherping van de privacywetgeving sinds 1-1-2016 het bewustzijn heeft aangewakkerd, zijn daarmee voor menig praktiserend professional de frustraties toegenomen. Frustraties door de constatering dat het implementeren van een ISMS veel energie, tijd en geld kost.
Sinds 1-1-2016 stelt de wetgever dat het de taak is van de **verantwoordelijke** er voor te zorgen dat de **bewerker**:

- zelf voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen
- de verantwoordelijke in staat stelt om aan de wettelijke plichten te voldoen (artikel 14 Wbp) http://bit.ly/2juELrq

Op 15-12-2016 informeert Minister Schippers de Kamer over het onderzoekrapport "Beveiliging van patiëntgegevens", van het adviesbureau PBLQ (http://bit.ly/2ihFnhv). In haar brief refereert ze aan de conclusies van het PBLQ onderzoek (http://bit.ly/2ihThAr) Het PBLQ rapport bevat een aantal aanbevelingen:

1. Bevorder goed gedrag. Te beginnen vanuit het management.
2. Zorg voor navolging van good practices.
3. Bundel de krachten waardoor de effectiviteit van informatiebeveiliging en privacybescherming kan worden vergroot. Maak sectorale afspraken. Denk na over een model bewerkersovereenkomst.
4. Biedt begrijpelijke praktische handvatten voor wet- en regelgeving. Bijvoorbeeld door de regelgeving te presenteren in sectorale en beroepsgerichte gedragscodes en thematische richtsnoeren.
5. Anticipeer op de komst van de Algemene Verordening Gegevensbescherming (AVG) door de lat voor informatiebeveiliging en privacybescherming hoger dan de vigerende wet- en regelgeving te leggen. Schep duidelijke kaders onder welke voorwaarden gepseudonimiseerde patiëntgegevens gebruikt mogen worden bij (wetenschappelijk) onderzoek en kwaliteitsregisters.

Prima aanbevelingen maar de focus ligt daarbij toch vooral op de rol van de zorgaanbieder/zorgprofessional in zijn rol als **verantwoordelijke.**

In de beleidsregels meldplicht datalekken worden suggesties gegeven voor de **afspraken** die tussen verantwoordelijke en **bewerker** dienen te worden gemaakt. De veronderstelling dat de gemiddelde eerstelijns zorgaanbieder/ zorgprofessional over voldoende competenties, inzichten en invloed beschikt om in staat te zijn daarin zijn rol als verantwoordelijke naar behoren te vervullen

is te optimistisch. Zo de suggesties uit het PBLQ rapport al worden overgenomen, zullen de effecten daarvan veel tijd gaan kosten.

De AVG komt de eerstelijns zorgaanbieder/zorgprofessional tegemoet komt door meer verantwoordelijkheid toe te dichten aan de bewerker. Ook de invloed daarvan zal niet direct merkbaar zijn. Samengevat: veel tijd zal verloren gaan tot het moment dat voldoende maatregelen zijn genomen we wettelijk als wenselijk beschouwen. Dit in het besef dat vanaf het moment dat de zorg verplicht werd om het BSN te gaan gebruiken (juni 2009(!) zorgaanbieders al verplicht zijn om te voldoen aan de NEN7510 (http://bit.ly/2jFz9v4).

Dit overziend lijkt het uitermate wenselijk om de nadrukkelijke scope, die zich nu richt op de eerstelijns zorgaanbieder/zorgprofessional te verleggen. Dat kan door de doorsnee eerstelijns zorgaanbieder/zorgprofessional niet dan wel minimaal te belasten zaken die zich buiten zijn primaire aandachtsgebied (optimale zorgverlening aan de cliënt) liggen. Dat kan door de doorsnee eerstelijns zorgaanbieder/zorgprofessional, net als zijn cliënt te beschouwen als een **consument** in zijn relatie tot de bewerker (de IT leverancier van wie producten en of diensten worden afgenomen).

Dat kan door het stellen van standaard eisen aan bewerkers die producten en/ of diensten aanbieden voor de zorg. Wellicht kan dan ook de ACM een rol spelen bij de vervulling van de (te) omvangrijke taken die nu alleen op het bordje van de AP liggen.

Rob Stadt, FG/DPO
stadt@kngf.nl