PBLQ
verbinders in de informatiesamenleving

White paper

NEN

Hoe ondersteunen normen de implementatie van de AVG in de zorg?

THEO HOOGHIEMSTRA (PRINCIPAL CONSULTANT, PBLQ), SHIRIN GOLYARDI (SENIOR CONSULTANT NEN), RENÉ GOUWENS (PRODUCTMANAGER NEN)

Bij veel organisaties staat 25 mei 2018 rood omrand in de agenda. Het betreft namelijk de datum dat de Algemene verordening gegevensbescherming (AVG) van toepassing wordt.

De zorgsector zal veel impact ondervinden van de AVG en wel om een aantal redenen. Ten eerste zijn gezondheidsgegevens een bijzondere categorie binnen AVG vanwege de gevoeligheid van deze informatie. Ten tweede zijn er veel overdrachts-momenten van gezondheidsgegevens. En ten derde zijn bij de overdracht en gebruik van gezondheidsgegevens veel partijen en individuen betrokken. Er is dus een hoog risico op incidenten met een grote impact. Daarnaast dienen ook niet risicovolle verwerkingen van persoonsgegevens zorgvuldig plaats te vinden op grond van de AVG.

Informatiebeveiliging is een belangrijk aspect binnen de Nederlandse zorg. In dit artikel wordt de relatie gelegd tussen de AVG, NEN 7510:2017 en andere normen die een rol kunnen spelen bij het voldoen aan de AVG.

NEN 7510

De norm voor informatiebeveiliging in de zorg, NEN 7510:2017, heeft als doel het verbeteren van de beheersing van informatiebeveiliging specifiek voor de Nederlandse zorg. NEN 7510-2017 valt uiteen in twee normen: NEN 7510-1 ‘Informatiebeveiliging in de zorg – deel 1: managementsysteem’ en NEN 7510-2 ‘Informatiebeveiliging in de zorg – deel 2: Beheersmaatregelen’. De norm is bedoeld voor zowel zorginstellingen als andere beheerders van persoonlijke gezondheidsinformatie. De norm volgt een managementsysteembenadering, waarbij een organisatie via een risicobenadering vaststelt welke concrete beheersmaatregelen relevant voor haar zijn.

NEN 7510 vormt, samen met NEN 7512 'Informatiebeveiliging in de zorg – Vertrouwensbasis voor gegevensuitwisseling' en NEN 7513 'Logging – Vastleggen van acties op elektronische patiëntdossiers', een kader voor het toezicht op informatiebeveiliging door de Inspectie voor de Gezondheidszorg en Jeugd (IGJ) en de Autoriteit Persoonsgegevens (AP). De normen zijn een concrete Nederlandse invulling van de wereldwijde ISO-normen en Europese CEN-normen op het gebied van informatiebeveiliging in de zorg. Ze bieden een integraal kader en documenten voor informatiebeveiliging, toegespitst op de Nederlandse situatie.

AVG

De AVG is per 25 mei 2018 rechtstreeks van toepassing in de hele Europese Unie en vervangt de Wet bescherming persoonsgegevens (Wbp). In het kort zorgt de AVG voor:

1. Versterking en uitbreiding van de rechten van de betrokken personen:
   - Toestemming; de AVG specificeert de voorwaarden die gelden voor een organisatie om toestemming te verkrijgen om persoonsgegevens te kunnen verwerken. De toestemming dient vrij, specifiek, op basis van relevante informatie, ondubbelzinnig en noodzakelijk te zijn. Daarnaast dient de formulering van de toestemming actief geschreven te worden, in begrijpelijke taal en aantoonbaar te zijn. Het moet voor een ieder makkelijk zijn om toestemming in te trekken zoals het ook is gegeven.
   - Recht op vergetelheid; een ieder heeft al het recht om een organisatie te vragen hun persoonsgegevens te verwijderen. Straks kan een ieder eisen dat de organisatie de verwijdering doorgeeft aan alle andere organisaties die de persoonsgegevens van de desbetreffende organisatie hebben gekregen.
   - Recht *op dataportabiliteit*; Dit recht geldt voor een ieder die toestemming heeft gegeven voor het delen of gebruik maken van zijn/haar persoonsgegevens van door betrokkene verstrekte gegevens. Bijvoorbeeld via toestemming of een overeenkomst. De data moet op gestructureerde, machine leesbare wijze worden overgedragen.

2. Meer verantwoordelijkheden voor organisaties:
   - Verantwoordingsplicht; organisaties moeten, meer dan in het verleden, gedocumenteerd aantonen dat ze voldoen aan de eisen van de wet door middel van organisatorische en technische maatregelen.
   - Data protection impact assessment (DPIA); een instrument om vooraf de risico's van een gegevensverwerking in kaart te brengen. De uitkomst hiervan leidt tot maatregelen om de risico's te verkleinen. De eis is slechts verplicht voor gegevensverwerkingen met een hoog ingeschat risico (o.a. profilering, en verwerking op grote schaal).
   - Plicht tot het instellen van Functionaris voor de gegevensbescherming (FG); toezichthouder binnen een organisatie op de toepassing en naleving van de AVG.

Tegelijkertijd krijgen alle Europese toezichthouders meer bevoegdheden, onder meer het opleggen van hoge geldelijke boetes.

AVG en NEN 7510

NEN 7510:2017 geeft invulling aan een deel van de bepalingen uit de AVG. Onderstaand overzicht geeft een aanwijzing hoe NEN 7510 een invulling geeft op het 10-stappenplan van het AP1:

- Bewustwording (art. 5 AVG) 18.1.1
- Rechten van betrokkenen (art. 12-22 AVG) 12.1.1
- Overzicht van en inzicht in verwerkingsactiviteiten (art. 30 AVG) 8.1.1
- Data Impact Protection Assessment (art. 35 AVG) 7510-1 6.1, 8.2.1
- Privacy-by-design and –by-default (art. 25 AVG) 6.1.5, 14.1.1
- Functionaris gegevensbescherming (art. 37 AVG) 6.1.1
- Meldplicht datalekken (art. 33 AVG) 16.1.5
- Verwerkersovereenkomst (art. 28 AVG) 15.1.2
- Leidende toezichthouder (art. 51 AVG) 18.1.4
- Toestemming (art. 6 AVG) 18.1.4

Definitie van gezondheidsgegevens:
Gezondheidsgegevens worden in overweging 35 van de AVG gedefinieerd als: ‘alle gegevens (…) die betrekking hebben op de gezondheidstoestand van een betrokkene en die informatie geven over de lichamelijke of geestelijke gezondheidstoestand van de betrokkene in het verleden, het heden en de toekomst.’

Gezondheidsgegevens (of -informatie) beperkt zich in de reikwijdte van NEN 7510:2017 niet tot de gegevens bij zorgaanbieders, maar ook tot het verwerken van gezondheidsgegevens buiten de zorg, zoals bij persoonlijke gezondheidsomgevingen.
Zie bijvoorbeeld het gecursiveerde deel in onderstaande beheersmaatregel, die uitgaat van de systemen en niet van een bepaald type organisatie.

9.2.1 Registratie en afmelden van gebruikers

Beheersmaatregel:
Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.

Zorgspecifieke beheersmaatregel:
De toegang tot gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoort onderhevig te zijn aan een formeel gebruikersregistratieproces.
Procedures voor het registreren van gebruikers behoren te garanderen dat het vereiste niveau van authenticatie van de geclaimde identiteit van gebruikers overeenkomt met het (de) toegangsniveau(s) waarover de gebruiker zal gaan beschikken.
De gebruikersregistratiegegevens behoren regelmatig te worden beoordeeld om te garanderen dat ze volledig en juist zijn en dat toegang nog altijd vereist is.
[...]

[1] Zie ook de website van het AP voor meer informatie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/voorbereiding-op-de-avg

NEN 7510:2017 blijkt ook nog op een andere manier aan te sluiten op de AVG. Artikel 42 AVG roept op tot bevordering van certificeringsmechanismen. NEN 7510:2017 is voor zorgorganisaties en persoonlijke gezondheidsomgevingen te hanteren als certificeringsmechanisme.

Andere relevante normen

Naast de bovengenoemde nationale normen zijn er meerdere internationale normen die een belangrijke aanvulling geven in de aansluiting van normen op de AVG, zoals:

- ISO/IEC CD 27552 - Security techniques — Enhancement to ISO/IEC 27001 for privacy management — Requirements (norm in ontwikkeling);
- ISO/IEC 19592-1 en ISO/IEC 19592-2 Information technology – Security techniques – Secret sharing;
- ISO/IEC 29100 - Information technology – Security techniques – Privacy framework;
- ISO/IEC 29101 - Information technology – Security techniques – Privacy architecture framework
- ISO/IEC 29134:2017 - Information technology — Security techniques — Guidelines for privacy impact assessment

Ook dit kader is nog niet compleet, maar zo wordt wel gebouwd aan een normenstelsel dat op termijn een gericht en volledig antwoord zal geven op de vraag hoe normen een invulling kunnen geven aan de AVG.

AVG grondslagen en NEN 7510

NEN 7510 is beperkt tot de informatiebeveiligingsbepaling in de AVG. Om de gehele AVG te kunnen certificeren, is meer noodzakelijk dan alleen het voldoen aan NEN 7510. Bovendien biedt de AVG - naast de in NEN 7510 genoemde grondslag van toestemming – nog vijf mogelijke grondslagen om persoonsgegevens te mogen verwerken.
Denk daarbij bijvoorbeeld aan:

1) De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst (bijvoorbeeld een verwerkersovereenkomst).
2) De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting (bijvoorbeeld de WGBO of de Wet publieke gezondheid).
3) De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen (bijvoorbeeld bij zorg als er sprake is van levensbedreigende situaties).
4) De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
5) De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

De verwerkingsverantwoordelijke (in de praktijk de zorgaanbieder of, in geval van uitbesteding, bijvoorbeeld de leverancier van persoonlijke gezondheidsomgevingen) is en blijft zelf verantwoordelijk om te beoordelen of de verwerking van persoonsgegevens gebaseerd kan worden op één van de grondslagen.

Conclusie

Door gebruik te maken van (inter)nationale normen op het gebied van informatiebeveiliging en gegevensbeschermingen en het inbedden van de grondslagen van AVG in het informatiebeveiligingsmanagementsysteem, ontstaat er een systeem dat niet alleen borging geeft aan informatiebeveiliging, maar daarnaast ook steeds meer een volledige invulling geeft in het voldoen aan de AVG. Het geboden kader vanuit normen is nu niet volledig, maar een belangrijke stap in een groeimodel dat een duidelijke opdracht geeft aan normalisatie voor de komende jaren.

Meer informatie over NEN 7510 vindt u op www.nen.nl/nen7510.