BMC
YACHT GROUP

Informatiebeveiliging en privacy in de zorg

Niet meer vrijblijvend

mei 2018

Partners in verbetering

Informatiebeveiliging en privacy in de zorg

Niet meer vrijblijvend

BMC
Ir. Julius Duijts CISSP, senior adviseur
drs. Willem de Vries, senior adviseur

Inhoudsopgave

H1 | Informatiebeveiliging en privacy in de zorg – niet meer vrijblijvend

Privacy en informatiebeveiliging zijn in toenemende mate een thema in het maatschappelijk debat en de media, mede naar aanleiding van datalekken, cybercriminaliteit en beveiligingsproblemen bij publieke organisaties. Zorginstellingen zijn daarop geen uitzondering.

Met ingang van 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Deze Europese wet geeft regels voor de omgang met persoonsgegevens. De regels gelden ook voor zorginstellingen, net zoals voor gemeenten en andere maatschappelijke organisaties zoals onderwijsinstellingen. Het bestuur is verantwoordelijk voor de implementatie van deze wetgeving. De rechten van cliënten worden verstevigd en de bevoegdheden en capaciteit van de Autoriteit Persoonsgegevens als toezichthouder worden uitgebreid. Informatiebeveiliging is een belangrijke pijler in de bescherming van privacy, naast de andere eisen die de Algemene Verordening Gegevensbescherming (AVG) stelt (zie kader). De volwassenheid van zorginstellingen op dit gebied verschilt sterk. Sommige organisaties hebben informatieveiligheid en privacy volledig ingebed in de processen. Zij toetsen op de effectiviteit van privacymaatregelen en het management stuurt bij wanneer maatregelen niet of onvoldoende blijken te voldoen. Sommige organisaties bereiden zich voor op een NEN7510-certificering (zie kader). In andere organisaties ontbreekt het vaak nog aan integraal beleid, waardoor niet gewaarborgd is dat men voldoet aan de wetten en regels.

In dit whitepaper laten we zien hoe een zorgorganisatie grip krijgt op privacy en beveiliging van gegevens om zorgvuldig om te gaan met gegevens van cliënten en met welke praktische stappen dit kan worden gerealiseerd.

Algemene Verordening Gegevensbescherming (AVG)

De AVG geeft aan binnen welke kaders persoonsgegevens mogen worden verwerkt en beschrijft de rol van de toezichthouder, de Autoriteit Persoonsgegevens (AP). Onderwerpen die in uw organisatie geregeld moeten zijn om te voldoen aan de wet zijn:

- het opstellen en onderhouden van een verwerkingenregister
- rechtmatigheid van de verwerking (grondslag
- doelbinding
- proportionaliteit en subsidiariteit)
- bewaartermijnen
- verwerkersovereenkomsten
- melding van datalekken
- gegevensuitwisseling en informatieveiligheid

Ten opzichte van de Wbp stelt de AVG aanvullende eisen ten aanzien van bijvoorbeeld verantwoording, documentatie, evaluatie, de beoordeling vn de effecten van gegevensverwerking en de verplichte aanstelling van een functionaris gegevensbescherming.
Omdat er nog geen catalogus van praktische maatregelen is om te voldoen aan de eisen rond aantoonbaarheid en evaluatie in de AVG, heeft BMC een catalogus met beheersmaatregelen ontwikkeld als basis voor een degelijke implementatie.

NEN7510 Informatieveiligheid in de zorg

NEN 7510 is de Nederlandse norm voor informatieveiligheid die is ontwikkeld met participatie vanuit de zorgsector zelf. Zowel de Inspectie voor de GezondheidsZorg (IGZ) als de AP en andere toezichthouders gebruiken deze norm als basis voor het beoordelen van de informatieveiligheid van zorgaanbieders. Per 1 februari 2016 is het voor organisaties mogelijk om zich te certificeren voor de NEN7510-norm. Enkele honderden organisaties (groot en klein) hebben dat inmiddels gedaan. Op termijn zou dit een verplichting kunnen worden; hetzij via een wet, hetzij door aanbestedingseisen.

Ontwikkelingen die privacy en informatiebeveiliging actueel maken

Er zijn ontwikkelingen die de noodzaak om gegevens van cliënten en medewerkers – door het waarborgen van privacy en informatiebeveiliging – steeds gewichtiger maken:

- Elke zorginstelling verwerkt op grote schaal persoonsgegevens. In de afgelopen jaren is de privacywetgeving stap voor stap aangescherpt met de meldplicht datalekken en boetebeleid in 2016 en in 2018 met de AVG. De verwerking van persoonsgegevens moet niet alleen voldoen aan de wettelijke kaders, maar uw organisatie moet dat ook kunnen aantonen.
- Vanwege de AVG krijgt de Autoriteit Persoonsgegevens (AP) als toezichthouder meer bevoegdheden en meer personeel. Vanaf kan elke overtreding leiden tot een boete. Opzet is daarvoor niet meer een criterium. Ook gaat de AP individuele klachten behandelen en kan zij een deel van het onderzoek uitbesteden aan de Functionaris Gegevensbescherming (FG) in uw eigen organisatie. Het aanstellen van een FG is voor een zorginstelling verplicht omdat op grote schaal gegevens over gezondheid verwerkt. Daarmee krijgt het toezicht een veel grotere slagkracht.
  Toezichthouders zoals de AP pleiten al jaren voor een betere informatieveiligheid in de zorg. De AP heeft zorgbestuurders er al verscheidene malen op In 2015 is een aantal bureaus jeugdzorg onderzocht en in 2016 verscheen er een onderzoek over het sociaal domein van de hand van de AP. Ook stuurde de AP een open brief aan raden van bestuur van zorginstellingen.
  Nu de AP meer middelen krijgt zal de druk stijgen om te komen tot goede privacy en informatieveiligheid.
- Zorginstellingen die het BSN gebruiken zijn verplicht om te voldoen aan NEN 7510 (art. 2 Besluit gebruik BSN in de zorg). Aangezien het BSN een sleutelrol speelt bij de communicatie in de keten en bij facturatie, betreft dit vrijwel alle zorgaanbieders. Enkele honderden organisaties (groot en klein) hebben zich in de afgelopen twee jaar gecertificeerd voor de NEN7510-norm. Het ligt voor de hand dat opdrachtgevers, zoals zorgverzekeraars en gemeenten, dit op de agenda zetten bij de jaarlijkse contractonderhandelingen en op termijn lijkt het waarschijnlijk dat certificering bij aanbestedingen een eis wordt.
- Datalekken, cybercriminaliteit en andere beveiligingsincidenten komen steeds meer voor. Het is niet de vraag of een groot incident optreedt in uw organisatie, maar wanneer. Een goed geïmplementeerd beleid voor informatieveiligheid en privacy maakt de kans op een incident kleiner en zorgt ervoor dat bestuurders aan hun zorgplicht voldoen. Dat maakt het beantwoorden van vragen door toezichthouders naar aanleiding van een incident een stuk gemakkelijker.
- Steeds vaker nemen individuele betrokkenen en groepen initiatieven om ontbrekende beveiligingsmaatregelen en niet adequate toepassing van privacywetgeving aan de kaak

te stellen. Maatschappelijke actoren zoals nieuwsmedia en actiegroepen maken proactief openbaar welke organisaties tekortschieten in de beveiliging en bewaking van privacy van alle partijen die door de AVG beschermd worden.
- Van bestuurders valt dan te verwachten dat zij hun organisatie adequaat kunnen vertegenwoordigen, Zij moeten goed op de hoogte zijn van de keuzes die de organisatie heeft gemaakt bij haar beleid en ze moeten deze keuzes professioneel kunnen uitdragen. Daarvoor moeten ze "gevoed' worden vanuit de organisatie.
- Bij de controle van de jaarrekening maken accountants steeds meer werk van hun verplichting om over de betrouwbaarheid en continuïteit van de ICT-systemen te bevinden en te rapporteren (BW 393.4).
- Eventuele boetes van de AP vormen een materieel risico wanneer privacy en informatiebeveiliging onvoldoende zijn geregeld.
- Opdrachtgevers, zoals gemeenten en zorgverzekeringen, stellen steeds meer eisen op het gebied van privacy en informatiebeveiliging aan zorginstellingen. Enerzijds vanuit hun zorgplicht en anderzijds om reputatieschade door incidenten bij een door hen gecontracteerde zorgaanbieder te voorkomen.

Privacy en informatieveiligheid zijn breder geworden dan alleen 'een ICT-onderwerp'. Alle medewerkers hebben er een rol in en dragen er verantwoordelijkheid voor. Sturing door het bestuur en het management is noodzakelijk, want zij dragen uiteindelijk de verantwoordelijkheid voor de beveiliging en privacy van (persoons)gegevens. Het ligt voor de hand dat kleinere organisaties bij deze complexe materie eerder hulp van buiten nodig hebben dan de grote organisaties.

Risico's voor zorginstellingen

- De nieuwe wet geeft de AP een krachtiger positie bij toezicht en handhaving. Een AP-"inval" of andere incidenten op het gebeid van privacy of informatiebeveiliging dwarsbomen altijd de normale bedrijfsvoering. Bovendien leiden ze vaak intern en extern tot veel ophef en extra kosten.
- Bij klachten of ophef komt is het aan de verantwoordelijke bestuurder in het om toelichting te geven. Bij een onvoldoende voorbereiding kost het veel tijd – vaak in een 'stressvolle' situatie – om zijn of haar publieke optreden goed voor te bereiden en de gevolgen van de 'slechte beurt' zoveel mogelijk te beperken. Bovendien kan de positie van de bestuurder in het geding komen.
- Er ontstaat reputatieschade als gevolg van datalekken, hacken en publiciteit, of wanneer de organisatie genoemd wordt in een rapport van de AP.
- Boetes en ad hoc maatregelen naar aanleiding van incidenten en publiciteit brengen financiële schade met zich mee. Daarnaast kan reputatieschade op termijn leiden tot afname van inkomsten.
- Op termijn zullen alleen zorginstellingen opdrachten krijgen wanneer zij privacy en informatiebeveiliging aantoonbaar op orde hebben. Gemeenten en zorgaanbieders kunnen het zich niet veroorloven dat zij hun burgers en klanten verwijzen naar zorgaanbieders die niet "in control" zijn. Daarmee is immers ook hun reputatie in het geding.
- Omdat zorgaanbieders werken met een BSN, moeten zij wettelijk voldoen aan NEN 7510 (informatieveiligheid in de zorg). Deze norm wordt door toezichthouders (IGZ en AP) gebruikt als meetlat. Certificering is sinds begin 2016 mogelijk, maar het valt te verwachten dat certificering een verplichting wordt. Dat zal lastig worden voor de organisatie die nog geen ervaring heeft met certificering.

- Bij de controle van de jaarrekening kunnen problemen ontstaan, zoals door onvoldoende aantoonbare betrouwbaarheid en continuïteit van ICT-systemen. Het is niet ondenkbeeldig dat toezichthouders daarvoor boetes geven.

Het positieve spiegelbeeld van de genoemde risico's is een goed ingerichte privacy- en informatieveiligheid. Het vertrouwen dat de instelling zich gedraagt zoals het betaamt, zorgt voor stabiliteit en goede relaties.

H2 | Zorgvuldig omgaan met gegevens van cliënten: grip krijgen op Privacy en informatiebeveiliging

Wat levert de zorg voor privacy en informatiebeveiliging u op?

Elke organisatie behoort aantoonbaar te voldoen aan de normen, regels en wetten voor informatiebeveiliging en privacy. De gegevens van de cliënt zijn dan goed beschermd, zodat ze deze met vertrouwen kunnen delen met de betrokken professionals.

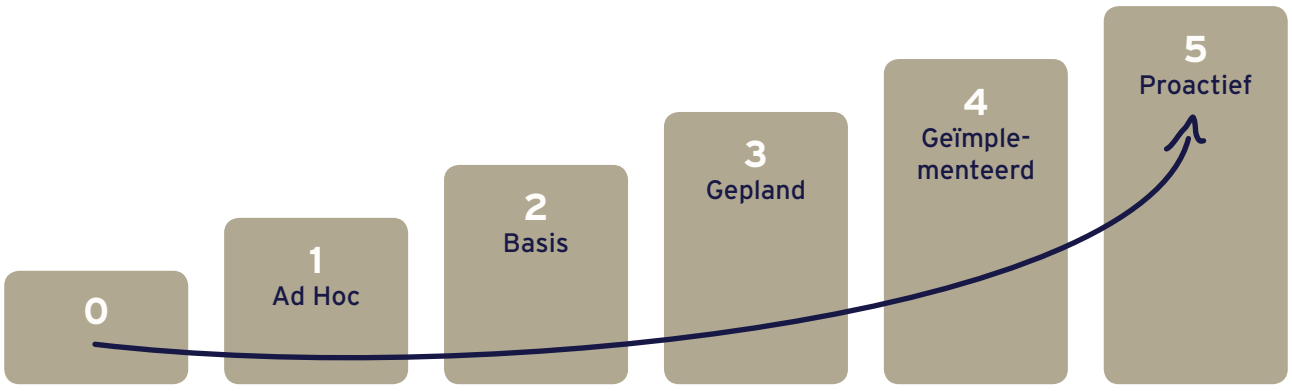
In die situatie zijn bestuurders in control. Zij kunnen bewuste, onderbouwde keuzes maken ten aanzien van risico's. Als er zich onverhoopt toch een incident voordoet, is de organisatie klaar om erop te reageren. Zij kan het lekken van informatie vaststellen, stoppen, het datalek melden bij de AP en maatregelen treffen om herhaling te voorkomen. Bovendien staan informatieveiligheid en privacy voortdurend in het licht van verbetering.

Bestuurders, management en medewerkers staan ervoor dat er passende maatregelen getroffen zijn om incidenten te voorkomen. Dat vormt ook een goede basis voor gesprekken met cliëntenraad, medezeggenschaporganen, advies- en toezichtorganen en met de samenleving als geheel, waarin privacy en informatieveiligheid steeds vaker aan de orde komen.

Zo wordt met een goed ingerichte informatieveiligheid en privacy het vertrouwen van cliënten en hun families en vrienden in uw organisatie versterkt.

Waar staat uw organisatie nu in deze actuele ontwikkeling?

Het is lastig om het geheel te overzien wanneer je er midden in staat. Een blik van buiten zorgt voor onafhankelijkheid en brengt 'blinde vlekken' aan het licht. De onafhankelijke, maar deskundige buitenstaander stelt u in staat om bewuste keuzes te maken bij het treffen van maatregelen of het accepteren van risico's. Vervolgens kunt u de nodige maatregelen implementeren, al of niet met externe ondersteuning.



0	1 Ad Hoc	2 Basis	3 Gepland	4 Geïmplementeerd	5 Proactief
Geen aandacht voor informatiebeveiliging/ privacy.	Beperkt aantal ad hoc maatregelen, tijdelijke rollen.	Basisset maatregelen genomen, globaal beleid, rollen belegd.	Volledig beleid, implementatieplan voor de maatregelen op basis van risicoanalyse.	Geïmplementeerd beleid en maatregelen, evaluatie geïntegreerd in P&C Cyclus.	Proactieve sturing op ontwikkelingen, integratie van audits.

BMC kan u helpen: stap voor stap

De volledige invoering van NEN 7510 omvat meer dan honderd beheersmaatregelen. Dat betekent veel werk, want de norm vereist ook de inbedding/verankering ervan in de organisatie. Dat gaat niet van de ene op de andere dag. De gestage ontwikkeling naar de gewenste status van uw organisatie kent verschillende, te onderscheiden stadia.

Stapsgewijze invoering maakt het proces beheersbaar. Het ijken van motiverende mijlpalen op weg naar volledige conformiteit zorgt voor overzicht in het voortgangsproces.

Wij onderscheiden vijf implementatieniveaus:

Implementatieniveau 0: onbekend

Er is geen aandacht voor informatieveiligheid. Deze situatie is met name aan de orde in organisaties in oprichting. Alle aandacht is gericht op het doel, de doelgroep en de medewerkers van de organisatie. "Gegevensbeveiliging? Dat zien we later wel."

Implementatieniveau 1: ad hoc

De status:

Op dit niveau ontstaan de eerste activiteiten, meestal op operationeel niveau. Rollen – zoals die van privacyofficer (ook: privacybeheerder) of securityofficer (ook: informatieveiligheidsbeheerder of CISO) – worden niet of alleen tijdelijk, bijvoorbeeld in een project, benoemd. Maatregelen worden getroffen in specifieke deelgebieden of als onderdeel van de implementatie van nieuwe systemen. Vaak ligt dan het accent op technische beveiliging. De controle vindt plaats in de marge van andere controles, zoals de controle van de jaarrekening of de certificering van het primaire proces. De resultaten kunnen aanleiding zijn om meer aandacht aan privacy en/of informatieveiligheid te besteden, als opstap naar het volgende implementatieniveau.

De ontwikkeling:

Van ad hoc naar basis

- Voor privacy wordt een inventarisatie van verwerking van persoonsgegevens gemaakt en deze wordt getoetst aan wet- en regelgeving.
- De uitvoering van het actieplan brengt de organisatie naar het niveau 'basis'.
- Voor informatieveiligheid wordt een scan gemaakt op grond van een basisset van beveiligingsmaatregelen.
- Daarop volgt een plan-van-aanpak voor de implementatie van de basisset van maatregelen.

Implementatieniveau 2: basis

De status:

Op het basisniveau is benoemd welke functionarissen de sleutelrollen vervullen. Zij gaan het beleid en de implementatie daarvan vorm te geven. Daarvoor worden ze opgeleid. Het beleid krijgt vorm in algemene termen en wordt gespiegeld aan wet- en regelgeving. De meest voor de hand liggende maatregelen zijn getroffen. Voor privacy is er een verwerkingsregister, de rechtmatigheid van de bewerkingen is gewaarborgd. Verwerkersovereenkomsten zijn afgesloten en processen rond de meldplicht datalekken zijn ingericht. Voor informatieveiligheid zijn er basismaatregelen op het gebied van gedrag van medewerkers, fysieke beveiliging en beveiliging van netwerken, systemen en eindgebruikersapparaten. Dat schept de uitgangssituatie om privacy en informatieveiligheid structureel op te pakken.

De ontwikkeling:

Van basis naar gepland

- Structureel oppakken bestaat uit een goede zelfevaluatie van de maatregelen die al getroffen zijn ten opzichte van de maatregelen die nodig zijn om duurzaam te voldoen aan NEN 7510 en aan de privacywetgeving.
- Omdat er nog geen catalogus van praktische maatregelen is om te voldoen aan de eisen rond aantoonbaarheid en evaluatie in de AVG, heeft BMC een catalogus met beheersmaatregelen ontwikkeld als basis voor een degelijke implementatie.
- Naast de zelfevaluatie wordt er voor informatieveiligheid een risicoanalyse en een dataclassificatie uitgevoerd.
- Op basis daarvan wordt voor zowel privacy als informatieveiligheid beleid verder uitgewerkt voor de deelgebieden binnen de instelling.

Implementatieniveau 3: gepland

De status:

Op dit niveau is er integraal beleid geformuleerd dat de gehele privacywetgeving en NEN 7510 omvat. Voor informatieveiligheid zijn op basis van een risicoanalyse en het principe 'pas toe of leg uit' ('comply or explain') de te implementeren maatregelen gekozen en geprioriteerd. Deze zijn vaak nog niet volledig geïmplementeerd. Wel wordt daar in deze fase actief aan gewerkt door de maatregelen uit te werken in bijvoorbeeld procesbeschrijvingen, praktische richtlijnen en gedragscodes. Daarbij zijn steeds meer disciplines betrokken, zoals HR, facilitaire zaken, lijnmanagers en proceseigenaren in het primaire proces.

De ontwikkeling:

Van gepland naar geïmplementeerd

- Alle medewerkers worden bewust gemaakt van hun verantwoordelijkheid voor privacy en informatieveiligheid. Dit wordt bijvoorbeeld besproken tijdens werkoverleggen.
- Door middel van geregeld voortgangsoverleg en een eventuele herhaling van de zelfevaluatie en risicoanalyse wordt de voortgang bewaakt en bijgestuurd. Daarbij is ook de hoogste leiding van de organisatie op gezette tijden betrokken.

Implementatieniveau 4: geïmplementeerd

De status:

Op dit niveau zijn het beleid en de maatregelen volledig geïmplementeerd. Ze worden eventueel bijgesteld op basis van periodieke evaluaties en risicoanalyses, volgens de 'plan-do-check-act' cyclus die ook uit het kwaliteitsmanagement bekend is. Dat maatregelen worden uitgevoerd, is aantoonbaar. Dit wordt ook bewaakt in de P&C-cyclus en getoetst door middel van interne en externe audits. Voorafgaand aan belangrijke wijzigingen in processen en systemen wordt de impact ervan onderzocht op privacy en informatieveiligheid. Op dit niveau kan ook een NEN7510-certificeringsaudit met succes worden doorlopen.

De ontwikkeling:

Van geïmplementeerd naar pro-actief

- Nu krijgt – vanuit de rust dat de actuele situatie goed verankerd is – de toekomstvisie een hogere plaats. Er wordt, naast de bewaking van alle afspraken en interne regels, ook vooruitgekeken naar verwachte en denkbare ontwikkelingen op het gebied van wet- en regelgeving en techniek. Ook worden andere actuele en toekomstige ontwikkelingen binnen de organisatie bij dit perspectief betrokken, zoals organisatieveranderingen, de invoering van nieuwe informatiesystemen, of nieuwe samenwerkingsvormen.

Implementatieniveau 5: proactief

De status:

Op dit niveau wordt er, naast de bewaking van alle afspraken en interne regels, ook vooruitgekeken naar toekomstige ontwikkelingen op het gebied van wet- en regelgeving en techniek. Ook worden andere actuele en verwachte ontwikkelingen binnen de organisatie bij dit perspectief betrokken, zoals organisatieveranderingen, de invoering van nieuwe informatiesystemen, of andere samenwerkingsvormen.

Naast de uitvoering van de maatregelen is er veel aandacht voor de effectiviteit ervan. Testen van de beveiliging door externe technische specialisten (in de vorm van 'penetratietesten') kunnen daaraan bijdragen. Maatregelen uit verschillende normen worden gecombineerd en op elkaar afgestemd.

Op het niveau 'proactief' strekt de bemoeienis zich ook uit tot ketenpartners ten aanzien van privacy en informatieveiligheid. Op basis van deze implementatieniveaus geeft BMC inzicht in waar uw organisatie staat. Zowel ten aanzien van beleid als ten aanzien van de maatschappelijke beeldvorming hebben deze partners immers een aanzienlijke invloed op uw prestaties en de resultaten die u boekt voor uw cliënten.

De ontwikkeling:

BMC kan voor u onderzoeken op welk niveau uw organisatie momenteel staat en of dat voor de verschillende onderdelen van uw organisatie in gelijke mate geldt. En laat BMC u helpen uw ambities en mogelijkheden te vertalen in het stappenplan dat past bij uw gemeentelijke organisatie.

Uw resultaat

De begeleiding van BMC draagt in belangrijke mate bij aan het resultaat dat elke gemeente voor haar burgers, bedrijven en maatschappelijke organisaties wil realiseren: optimale betrouwbaarheid op het gebied van privacy en informatieveiligheid. Het vertrouwen dat alle gegevens bij in goede handen zijn, staat in de lokale samenleving en daarbuiten niet ter discussie. Bestuurders en medewerkers zijn zich bewust van hun verantwoordelijkheden en handelen daarnaar. Risico's voor alle partijen – inclusief voor uw organisatie en haar bestuurders en medewerkers zelf – zijn tot een minimum beperkt. Er is ruimte om tijdig anticiperend na te denken en te handelen ten aanzien van toekomstige ontwikkelingen. Aan deze gedachtevorming kunnen bestuurders, medewerkers en medezeggenschapsgremia deelnemen op basis van ruim voldoende kennis en kunde. De zorginstelling neemt in de regio, de provincie en op landelijk niveau een verantwoorde en vertrouwenwekkende plaats in in de rangorde van publieke organisaties die hun zaken goed op orde hebben ten aanzien van privacy en informatiebeveiliging.

H3 | Concreet: de aanpak van BMC

Voor elk implementatieniveau ondersteunt BMC u bij de borging en verbetering van privacy en informatieveiligheid. De ontwikkeling gebeurt in nauwe samenspraak met uw medewerkers.
De inhoudelijke experts van BMC hebben diverse werkvormen ontwikkeld met ondersteuning van hun collega's die gespecialiseerd zijn op het gebied van training en ontwikkeling.

- scans en assessments om uw situatie in kaart te brengen;
- het opstellen van beleid en onderbouwde keuzes van maatregelen;
- het maken van concrete plannen voor de verdere inrichting in uw organisatie;
- het ondersteunen van en adviseren bij de implementatie

Implementatieniveau	Diensten Privacy	Diensten Informatiebeveiliging
1. Ad Hoc	• Management Workshop • Toetsing aan het privacykader • Opstellen van een register van verwerkingen	• Management Workshop • Scan Informatiebeveiliging
2. Basis	• Inrichtingsplan beheersingsmaat-regelen voor privacy • Toetsing rechtmatigheid van verwerkingen en gegevensuitwisseling • Privacy Impact Assessment	• Opstellen van informatiebeveiligingsbeleid • Zelfevaluatie beveiligingsmaatregelen NEN 7510 • Dataclassificatie • Risicoanalyse • Plan van aanpak voor implementatie
3. Gepland	• Assessment beheersingsmaatregelen (opzet en/of bestaan) • Toetsing rechtmatigheid van verkeringen en gegevensuitwisseling • Advies en ondersteuning bij implementatie • Privacy Impact Assessment • Training en bewustwording	• Assessment (opzet en/of bestaan) • Risicoanalyse • Implementatieplan • Advies en ondersteuning bij implementatie • Training en bewustwording
4. Geïmplementeerd	• Assessment (opzet en bestaan) • Toetsing rechtmatigheid van verkeringen en gegevensuitwisseling • Advies en ondersteuning bij evaluatie/ verbetering • Privacy Impact Assessment	• Assessment (opzet en bestaan) voorbereiding certificeringsaudit • Advies en ondersteuning
5. Pro-Actief	• Advies en ondersteuning bij evaluatie/ verbetering	• Advies en ondersteuning bij evaluatie/ verbetering
Alle niveaus	• Training en bewustwording • Privacy Impact Assessments • Jaarlijkse check met verschillende modules: - Update verwerkingenregister - Toetsing rechtmatigheid - Evaluatie beheersingsmaatregelen • Interim Functionaris gegevensbescherming of privacy expert	• Training en bewustwording • Beveiligingsadviezen • Jaarlijkse checkup met verschillende modules, zoals: - Zelfevaluatie - Risico-analyse - Plan van Aanpak • Interim informatiebeveiligingsexpert

Toelichting op de werkvormen

Managementworkshop
In de managementworkshop maken bestuurders en managers kennis met regelgeving rond privacy en informatieveiligheid. Daarmee krijgen zij samen een globale indruk van de actuele situatie van de organisatie. De workshop beslaat een dagdeel en omvat in ieder geval een intake en een rapportage . Naar gelang de situatie kan de workshop gericht zijn op privacy, informatieveiligheid of beide. In de workshop wordt een inventarisatie gemaakt van uw belangrijkste processen, systemen en gegevens. De deelnemers ontdekken de aandachtspunten voor hun organisatie op hoofdlijnen.

Toetsing aan het privacykader
In de privacyevaluatie wordt de verwerking van persoonsgegevens geïnventariseerd en getoetst aan het wettelijk kader van de AVG en andere regels die van toepassing zijn. Het gaat onder andere om: rechtmatigheid van de verwerking (grondslag, doelbinding, proportionaliteit en subsidiariteit), bewaartermijnen, verwerkingsregister, verwerkersovereenkomsten, melding van datalekken, gegevensuitwisseling en informatieveiligheid. Wanneer er nog geen systematische inventarisatie van verwerking van persoonsgegevens heeft plaatsgevonden, kan dit worden opgenomen in het onderzoek.

Assessment beheersing privacy
In het privacyassessment wordt onderzocht welke maatregelen uit de catalogus met beheersmaatregelen voor de AVG in de organisatie in opzet aanwezig zijn. Op basis daarvan wordt er een plan gemaakt voor de verdere implementatie, waarna de organisatie of instelling niet alleen voldoet aan wet- en regelgeving, maar ze kan dit niveau ook in stand houden, aantonen, evalueren en waar nodig verbeteren.

Scan informatiebeveiliging
Deze scan is bedoeld voor organisaties die informatieveiligheid nog niet structureel hebben ontwikkeld en geïmplementeerd. De deelnemers leveren op basis van een vragenlijst documenten aan over beleid en maatregelen op het gebied van informatieveiligheid. Deze worden met de normen en de stand van de techniek vergeleken en tijdens een beperkt aantal interviews of in een workshop met betrokkenen besproken, bijvoorbeeld verantwoordelijken voor en uitvoerenden van HR-, kwaliteits- en ICT-beleid. Op basis daarvan worden de belangrijkste issues gerapporteerd en worden er vervolgstappen geadviseerd.

Assessment informatiebeveiliging
Voor organisaties die zelf al structureel beleid hebben ontwikkeld en geïmplementeerd zijn er assessments. Daarin worden alle aspecten van informatieveiligheid onderzocht, zoals governance, beleid, organisatorische en technische beveiligingsmaatregelen. In overleg met de opdrachtgever wordt afgesproken of het assessment alleen gaat over de opzet van de beheersingsmaatregelen of dat ook de uitvoering (of het bestaan) van de beheersingsmaatregelen wordt onderzocht. Ook bij een assessment wordt documentonderzoek gecombineerd met interviews, maar het aantal daarvan is groter dan bij een scan. Daarnaast kunnen ook andere vormen van onderzoek worden ingezet, zoals demonstraties en rondleidingen.

Risicoanalyse
Als aanvulling op een scan of een assessment of als basis voor de uitwerking van beleid kan er een risicoanalyse worden uitgevoerd. Daarin worden specifieke bedreigingen voor uw organisatie in kaart gebracht en geeft u zelf een weging aan de risico's, in samenspraak met onze adviseurs. Een risicoanalyse helpt om prioriteiten te stellen, maatregelen te nemen en de restrisico's bewust te accepteren.

Wanneer de organisatie een hoger niveau van volwassenheid heeft bereikt, verschuiven risicoanalyses van organisatiebreed naar procesniveau. Hiermee komen proceseigenaren – en dus lijnverantwoordelijken – verder 'in control' op de specifieke risico's binnen hun verantwoordelijkheidsgebied. Ze kunnen dan ook gedegen afwegingen maken over de implementatie van maatregelen binnen hun processen.

Adequate inrichting van privacy en informatiebeveiliging

Op basis van scan, assessment en/of risicoanalyse helpt BMC u om u verder te ontwikkelen en maatregelen te definiëren en te implementeren, zoals:

- het opstellen van een jaar- of meerjarenplan;
- het inrichten van privacy en/of informatieveiligheid;
- het ontwikkelen van beleid;
- implementatie van voor privacy relevante processen en beleid;
- implementatie van managementsystemen, processen en beveiligingsmaatregelen;
- ondersteuning/coaching van verantwoordelijken voor privacy, informatieveiligheid of kwaliteit;
- invulling van de rol van privacy- of informatieveiligheidsbeheerder/- officer in uw organisatie, tijdelijk, parttime of in vaste dienst.

Waarom BMC?

BMC geeft integraal advies door kennis en ervaring van zorg, privacy en informatiebeveiliging te combineren. BMC verstaat de taal van verschillende disciplines, van bestuursniveau tot op de werkvloer. BMC neemt de organisatie mee in haar ontwikkeling en stemt haar advies daarop af.

Relevante bronnen

- Algemene Verordening Gegevensbescherming: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- Handleiding AVG van de AP https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleiding_avg.pdf
- NEN7510: https://www.nen.nl/NEN-Shop/Norm/NEN-75102011-nl.htm
- Regeling gebruik BSN in de zorg http://wetten.overheid.nl/BWBR0023923/2018-04-20

Contact

Heeft u vragen of wilt u vrijblijvend met ons in contact komen, dan kunt u telefonisch contact opnemen via (033) 496 52 00 of stuur een e-mail aan:

Ir. Julius Duijts CISSP
senior adviseur
06 - 29 52 55 31

drs. Willem de Vries
senior adviseur
06 - 51 62 97 80

Colofon

Informatiebeveiliging en Privacy in de zorg - niet meer vrijblijvend
april 2018

Auteurs: Ir. Julius Duijts CISSP,, senior adviseur
drs. Willem de Vries, senior adviseur

Productie: PR & Marketing, BMC

Druk: Randstand Groep Nederland

BMC
Spacelab 4
3824 MR Amersfoort

P.O. box 490
3800 AL Amersfoort

033 - 496 52 00
info@bmc.nl
www.bmc.nl

Kijk voor meer informatie ook eens op onze website **www.bmc.nl**