D1

Actieplan

Algemene Verordening Persoonsgegevens (AVG)

college
Sanering
zorginstellingen

(5 januari 2018)

Inleiding 1

Dit Actieplan is in nauwe samenwerking met de Nederlandse Zorgautoriteit (NZa) tot stand gekomen. In dit plan zijn concrete activiteiten benoemd waarmee het College sanering zorginstellingen (CSZ) al aan de slag is, of gaat, of die in de komende periode breder worden uitgerold.

CSZ is op de hoogte van risico's op het gebied van informatiebeveiliging en privacybescherming. Dit illustreert onder andere de ransomware aanval van 12 mei jl, waar zorginstellingen in Nederland en CSZ gelukkig geen slachtoffer van zijn geweest, maar wel leidt tot het (nog) verder aanscherpen van technische maatregelen. Op 15 december 2016 is het PBLQ-rapport over beveiliging van patiëntgegevens aan de Tweede Kamer gestuurd. De doelen die hieruit zijn voortgekomen worden vormgegeven in acties om structureel de informatiebeveiliging op een hoger niveau te brengen.

Dit actieplan richt zich allereerst op het inventariseren, delen en uitrollen van de in de praktijk bewezen 'goede voorbeelden', die gebruikt kunnen worden voor een brede implementatie. Hierbij is het van belang zowel in te zetten op cultuur, structuur en compliance.

Het actieplan maakt onderscheid tussen doelen en acties die gericht zijn op verschillende niveau's en onderdelen bij het CSZ. Het gaat daarbij om het bestuur en management, Functionaris gegevensbescherming (FG) en Information Security Officer (ISO), medewerkers, cliënten en gemachtigden.

In de volgende paragrafen wordt ingegaan op deze verschillende onderdelen. Daarbij worden activiteiten opgebouwd vanuit activiteiten die gericht zijn op het bevorderen van goed gedrag, het delen van goede voorbeelden, het bundelen van krachten en bieden van handvatten voor het anticiperen op wet- en regelgeving en de komst van de Algemene Verordening Gegevensbescherming (AVG).

Het totaal aan activiteiten zal van alle betrokkenen een forse extra inspanning vragen. Gezien de zeer beperkte omvang van het CSZ is het daarom te verwachten dat er enige zaken vertraging op lopen en de ondersteunende middelen die hiervoor beschikbaar zijn niet voldoende zullen zijn. Daarnaast ligt het in de lijn der verwachting dat organisatorische wijzigingen per 1 juli 2018 geëffectueerd zullen gaan worden.

Bestuur en Management 2

Het PBLQ-rapport merkt het volgende op over de rol van bestuur en management: 'Informatiebeveiliging en privacybescherming landen alleen in een organisatie als dit van hoog naar laag door de organisatie gedragen wordt en op een realistische wijze kan worden uitgevoerd. Wat betreft leiderschap is het daarom van belang dat de leiding het belang van informatiebeveiliging en privacybescherming begrijpt, dit actief uitdraagt binnen en buiten de organisatie en de uitvoering ervan faciliteert, bijvoorbeeld door voldoende personeel en ondersteunende middelen hiervoor beschikbaar te stellen.'

Doelen

- Informatiebeveiliging en bescherming van persoonsgegevens zijn onderdeel van de integrale management verantwoordelijkheid.
- Informatiebeveiliging en bescherming van persoonsgegevens zijn geïntegreerd in de governance en P&C-cyclus (Plan & Control).
- Overzicht, inzicht in gegevensverwerkingen is geborgd.
- Bestuurders zorgen voor voldoende resources voor informatiebeveiliging en bescherming van persoonsgegevens.
- Bestuurders zorgen ervoor dat in de organisatie risico's inzichtelijk gemaakt worden en dat duidelijk is wat er gebeurt als het zich voordoet.

Acties gericht op bestuur en management

Bevorderen goed gedrag

- Het Bestuur controleert informatiebeveiliging-beleid en legt hierover verantwoording af.
- In communicatie wordt het belang van naleving van relevante wet- en regelgeving op het gebied van informatiebeveiliging.
- Informatiebeveiliging en het naleven daarvan (bestuurders zijn hiervoor eindverantwoordelijk) dienen onderdeel te zijn van de planning en control cyclus van het Bestuur.

Goede voorbeelden delen

- Checklist cyber security op niveau Raad van Bestuur[1].
- Toolkit privacybescherming en informatieveiligheid/-beveiliging.

Krachten bundelen

- Het voorstel is om de Checklist cyber security op niveau Raad voor bestuur uit te breiden met privacy vragen.

[1] https://www.ncsc.nl/actueel/factsheets/checklist-beveiliging-van-ics-scada-systemen.html

Handvatten voor wet- en regelgeving / Anticiperen op de komst AVG

- Er wordt door VWS een generieke Factsheet AVG opgesteld. Hierin wordt ook ingegaan op de consequenties voor bestuurders in de zorg.
- Er wordt gekeken of de afstemming en coördinatie tussen juristen die zich bezighouden met voorbereiding op AVG verbeterd kan worden.

Functionaris Gegevensbescherming (FG) en Information Security Officer (ISO) 3

Het PBLQ-rapport merkt het volgende op over de rol van Functionaris Gegevensbescherming (FG) en een Information Security Officer (ISO): "Laat de leiding ervoor zorgen dat er voldoende mensen en middelen beschikbaar zijn voor het continu monitoren en verbeteren van informatiebeveiliging en privacybescherming. Dit omvat het aanwijzen (rol of functie) van een Functionaris Gegevensbescherming (FG) en een Information Security Officer (ISO)". Vanwege de voormelde beperkte omvang van het CSZ alsmede de verwachte organisatorische wijzigingen is er geen ISO aangewezen.

Doelen

- FG's en ISO's beschikken over voldoende kennis en vaardigheden en hebben de vereiste autoriteit in de organisatie.
- Specialistische deskundigheid met betrekking tot informatiebeveiliging en privacybescherming bij privacy professionals (alle medewerkers van het CSZ) wordt bevorderd.
- Privacy professionals (alle medewerkers van het CSZ) kennen de wetten en normen en kunnen deze vertalen naar hun eigen praktijk.
- Privacy professionals (alle medewerkers van het CSZ) fungeren als katalysator van de noodzakelijke (cultuur)veranderingen.

Acties gericht op FG/ISO

Bevorderen goed gedrag

- Inventariseren van opleidingsaanbod en beoordelen of deze voldoet aan de behoefte (o.a. accreditatie, tijd en geld).
- FG's en ISO's geven aan in hoeverre het opleidingsaanbod aansluit op de behoefte.

Goede voorbeelden delen

- Toolkit privacybescherming en informatieveiligheid/-beveiliging.
- Waarschuwingen en maatregelen versturen naar aanleiding van acute dreigingen (bijvoorbeeld ransomware) en kwetsbaarheden aangeven.
- Adviseren over preventieve maatregelen.

- Ingeval van ICT-beveiligingsincidenten helpen de technische-, privacy-, financiële-, en imagoschade zo veel mogelijk te beperken, door te adviseren en ondersteunen over de technische en organisatorische afhandeling (waaronder analyse van meldenswaardigheid) van de gemelde incidenten.

Krachten bundelen

- Voor het opleidingsaanbod wordt onderzocht in hoeverre accreditatie van opleiding geregeld moet worden. Waar nodig wordt een passend opleidingsaanbod ontwikkeld.
- Wegens het vormen van een personele unie tussen CSZ en NZa zal er overleg en samenwerking ontstaan tussen de FG's van CSZ en NZa.
- Platform waarop FG's en ISO's elkaar kunnen vinden en informatie uitwisselen (intervisie), Daarnaast worden door brancheorganisaties bijeenkomsten georganiseerd om kennis en ervaringen te delen en onderling af te stemmen.

Handvatten voor wet- en regelgeving / Anticiperen op de komst AVG

- Voorbereiden op de AVG door middel van coördinatie en afstemming van de juristen (Pels Rijcken) die hierbij betrokken zijn. Dit kan mogelijk worden versterkt door een gezamenlijk platform met alle maatregelen, uitleg en hulpmiddelen die breed toegankelijk zijn.
- Om het veld voor te bereiden op de komst van de AVG zal VWS een ondersteunende rol bieden door aan brancheorganisaties uitleg, goede voorbeelden en eventuele hulpmiddelen beschikbaar te stellen en te fungeren als informatiepunt voor de brancheorganisaties voor (zorg)specifieke vragen. De AP (Autoriteit Persoonsgegevens) wordt hierbij betrokken.
- Ondersteuning bij beheer van risico analyse.

Medewerkers 4

Het PBLQ-rapport was er onder meer op gericht om het belang van de bescherming van gegevens verankerd te krijgen in de praktijk, in het gedrag van leidinggevenden en medewerkers én in de (aanspreek)cultuur. Volgens het rapport is de bewustwording toegenomen omdat hiervoor meer capaciteit ten algemene beschikbaar is. Drivers hiervoor zijn onder andere de meldplicht datalekken (artikel 34a Wet bescherming persoonsgegevens) en de toename van cyberdreigingen, zoals ransomware. Bewustwordingscampagnes hebben bijgedragen aan meer bewustwording. Hier wordt verder op ingezet.

Doelen

- Blijvende en geborgde awareness voor informatiebeveiliging en bescherming van persoonsgegevens bij medewerkers.
- Medewerkers beschikken over voldoende kennis en hebben een juiste houding ten aanzien van informatiebeveiliging en bescherming van persoonsgegevens en handelen hiernaar.
- Medewerkers hebben vaardigheden en middelen tot hun beschikking om juist te kunnen handelen. Inzicht in de eigen verantwoordelijkheden in relatie tot informatiebeveiliging en bescherming van persoonsgegevens.

- Bevorderen dat dienstverleners (ICT leveranciers, gemachtigden etc.) de risico's van verkeerd omgaan met gegevens inzien, en bewust zo veilig mogelijk hier mee om gaan.

Acties gericht op medewerkers

Bevorderen goed gedrag

- Adviseren om medewerkers, voor zover van toepassing, te laten deelnemen aan campagnes cq. informatiemeetings om de bewustwording te vergroten en met name kleine datalekken te voorkomen.

Goede voorbeelden delen

- Bestaande (e-learning) modules op het terrein van informatiebeveiliging en gegevensbescherming inventariseren en die zo mogelijk breed beschikbaar stellen. Een projectleider (gezien de beperkte omvang van het CSZ zal de directie / het bestuur dit op zich moeten nemen) zal inventariseren welke instrumenten breder inzetbaar en deelbaar zijn en zal die beschikbaar stellen aan alle zorgaanbieders.
- Stimuleren van het gebruik van hulpmiddelen voor het beheer van wachtwoorden.
- "10 geboden" opstellen voor informatiebeveiliging om die in de organisatie te verspreiden.

Krachten bundelen

- Gebruik maken van (bestaande) informatiefilmpjes als middel om boodschap over het belang van informatiebeveiliging en privacy te herhalen. Dit wordt opgepakt door de projectleider (gezien de beperkte omvang van het CSZ zal de directie / het bestuur dit op zich moeten nemen).
- Adviseren om nieuwe medewerkers een introductie aan te bieden over informatiebeveiliging en privacy en hier bij de opleiding van medewerkers (binnen organisatie) ook aandacht aan te besteden.

Handvatten voor wet- en regelgeving / Anticiperen op de komst AVG

- De bestuurder stelt een factsheet op met belangrijkste punten rond informatiebeveiliging en privacy op medewerkerniveau.
- De bestuurder stelt een factsheet op om medewerkers te informeren over de komst AVG en de veranderingen die dit voor medewerkers heeft en organiseert hierover op de praktijk aansluitende workshops.

Cliënten / gemachtigden 5

Doelen

- Bewustzijn van rechten en verantwoordelijkheden met betrekking tot informatiebeveiliging en gegevensbescherming.
- Bewustzijn van de eigen verantwoordelijkheid voor informatiebeveiliging en de bescherming van de eigen gegevens.
- De cliënt heeft kennis van rechten en plichten (toestemming, inzage, recht op vergeten).

- De cliënt wordt zo veel mogelijk geholpen met vaardigheden en middelen om juist te kunnen handelen.

Acties gericht cliënten

Bevorderen goed gedrag

- Cliënt laten helpen privacylekken te melden bijvoorbeeld door meldpunt binnen organisatie in te richten waar cliënten terecht kunnen.
- Zorgaanbieders kunnen de eigen verantwoordelijkheid van cliënt expliciet maken door cliënten hierover met een heldere folder te informeren.

Krachten bundelen

- Generieke folders opstellen.

Activiteiten 6

Activiteiten / Acties				
	Bestuur & Management	FG's & ISO's	Medewerkers	Cliënten / gemachtigden
Al uitgevoerd	- Bekendheid van het bestuur met de risico's voor omgang van informatie onder het bestuur.	- Onderwerp op agenda organisatie	- Awareness bescherming persoonsgegevens	- Aandacht voor voorlichting
Nog uit te voeren	- Kennis en ervaring delen met rest van organisatie met betrekking tot risico's omgang informatie. - Brede bestuurlijke aandacht	- Uitbreiden samenwerking CSZ – NZa - Certificering FG - Deelname trainingsprogramma	- Bevorderen eigen verantwoordelijkheid tot bescherming van persoonsgegevens - Aandacht voor opleidingen en eventuele gedragscodes	- Samenwerking met VWS uitbreiden. - Folders / informatie op website voor aandacht bescherming persoonsgegevens.

	voor privacy.			