“Gegevens cliënten op straat na datalek”

Zorginstellingen hebben meer dan ooit te maken met datalekken: privacygevoelige gegevens die per ongeluk bij iemand anders terechtkomen dan de bedoeling is. Sinds 2016 is het verplicht dergelijke lekken te melden, en ook in de media is er toenemende aandacht voor. De bewustwording neemt toe. Hoe is de privacywaarborging binnen uw organisatie geregeld?

Privacy in de zorg op de agenda

De meeste meldingen van datalekken die de Autoriteit Persoonsgegevens over 2016 ontving zijn afkomstig uit de sector gezondheid & welzijn. Zo is bij Nederlandse ziekenhuizen bijna dagelijks sprake van een datalek, en zijn koppen als “Gegevens patiënten huisartsenpraktijk onbeveiligd” niet meer vreemd. Juist binnen de zorg bevatten gegevens vaak gevoelige persoonsinformatie, die — wanneer deze in de verkeerde handen terechtkomt — kan leiden tot verontrustende situaties, voor zowel cliënt als zorgorganisatie.

Mogelijke risico’s

- Gestolen computers, verloren smartphones of rondslingerende USB-sticks zorgen ervoor dat informatie over cliënten op straat komt te liggen
- Op niet uitgelogde computers kan privacygevoelige informatie worden ingezien door onbevoegden en kwaadwillenden
- Correspondentie over persoonlijke gegevens wordt door onoplettendheid bij de verkeerde persoon bezorgd
- Professionals bespreken open op de gang de casus van één van uw cliënten
- Het cliëntenportaal of de website van uw organisatie mist het groene ‘slotje’ en is daarmee onvoldoende beveiligd

Scan Privacyrisico’s

Bent u als verantwoordelijke binnen uw zorginstelling benieuwd hoe uw organisatie omgaat met het onderwerp privacy? In samenwerking met haar partners heeft Pool Management & Organisatie de Scan Privacyrisico’s ontwikkeld om te beoordelen in hoeverre u als zorgaanbieder voldoet aan de wettelijke beveiligings-verplichtingen, zoals vastgesteld in de Wet bescherming persoonsgegevens (Wbp) en de aanstaande Europese Algemene verordening gegevensbescherming (Avg). Deze dwingen zorgaanbieders om o.a. passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen, te voorzien in procedures voor de meldplicht datalekken en een toezichthoudende functionaris gegevensbescherming aan te stellen.

Domeinen wettelijke verplichtingen:

- Governance
- Legal
- Organisatie
- ICT

De Scan bekijkt per domein de aspecten:

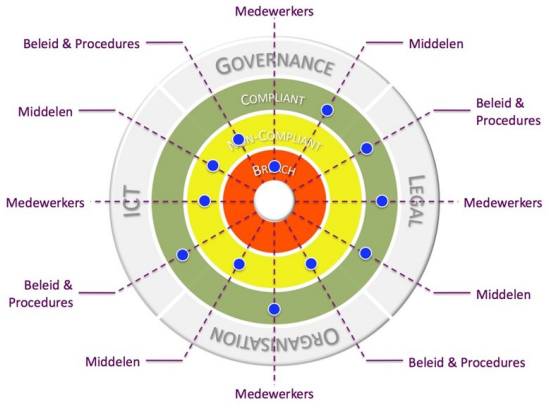
- Beleid & Procedures: structuur, sturing en verantwoording
- Medewerkers: eigen personeel en externen
- Middelen: infrastructuur, administraties, etc.

Domeinen en aspecten

De wettelijke verplichtingen beperken zich niet alleen tot voor de hand liggende domeinen als ICT of HR, maar hebben betrekking op *alle* domeinen binnen uw organisatie waar sprake is van gebruik en bewerking van persoonsgegevens. Per domein worden met de scan de aspecten Beleid & Procedures, Medewerkers en Middelen aan een kritische blik onderworpen.

De Privacy Monitor

De resultaten van het onderzoek – de Privacy Monitor – worden visueel gepresenteerd en aangevuld met een lijst specifieke bevindingen die op afzienbare termijn aandacht nodig hebben.



Uitvoering

Voorafgaand aan het onderzoek zal – met u en/of uw compliance officer – tijdens een voorgesprek van ongeveer 90 minuten worden bepaald welke informatie c.q. documenten van uw organisatie nodig zijn en welke functionarissen geïnterviewd zullen worden.

De daadwerkelijke uitvoering van de scan verloopt in fasen en duurt ongeveer twee weken. In die periode komen onder andere aan de orde:

- Dataverzameling en -analyse: er worden aan de hand van de vragenlijst documenten ter inzage en toegang tot het bedrijfsinformatiesysteem gevraagd
- Interviews en veldonderzoek: naar aanleiding van het voorgesprek en de data-analyse worden aanvullende interviews met gehouden met optioneel veldonderzoek (bezoek op locatie).

Tijdens de interviews en het veldonderzoek zullen alle privacygerelateerde zaken aan de orde komen die voorkomen in uw huidige werkprocessen, systemen, structuren, aansturing, gehanteerde werkwijzen, maar ook het gebruik van (management)informatie, relevante leidinggevende vaardigheden en privacyaspecten van de heersende organisatiecultuur.

Rapportage

Ter afronding van de scan worden de onderzoeksresultaten verwerkt in de Privacy Monitor en gerubriceerd in een lijst met specifieke bevindingen. Deze worden in een managementpresentatie aan u teruggekoppeld.

Aansluitend zal er ruimschoots gelegenheid zijn om van gedachten te wisselen over de waardering van uw privacyrisico's, het verbeterpotentieel in uw organisatie, de wijze waarop dit potentieel valt te benutten en de inschatting van het benodigde draagvlak.

Wie is Pool Management & Organisatie?

Pool Management & Organisatie is een netwerkorganisatie gespecialiseerd in integrale organisatieontwikkeling binnen zorg, overheid en onderwijs.

Wij hebben verschillende programma's ontwikkeld gericht op actuele thema's binnen de zorg, zoals Privacy in de zorg, Kwaliteit in de zorg, Zelfsturing in de zorg en Lean in de zorg.

Daarnaast is Pool Management & Organisatie deskundige op het gebied van:

- Zorgmanagement
- (Her)inrichting zorgorganisaties
- (Tijdelijke) directievoering of -vervanging
- Overbruggingsmanagement bij management-vacatures
- Cultuurverandering, draagvlakontwikkeling en acceptatie
- Werving en selectie hoger management en directie

Ons aanbod

Graag lichten wij onze aanpak toe en wisselen wij met u – geheel vrijblijvend – van gedachten over de hoe de privacywaarborging binnen uw organisatie is geregeld.

Onze experts, met concrete kennis en ervaring, staan voor u klaar. Bel ons voor een afspraak op 0546-568015 of mail naar info@pool-management.nl o.v.v. 'Privacy in de zorg'.