

Een Privacy Office

Privacy is een teamsport: je doet het met z'n allen

Waarom:

De naleving van de AVG is complex en gaat niet vanzelf. Intern toezicht op de naleving ervan is in zorg en welzijn niet altijd formeel georganiseerd. Idealiter is de daarvoor benodigde kennis in een Privacy Office (PO) gebundeld. Een PO draagt eraan bij dat privacy en informatiebeveiliging een blijvend thema is in de organisatie.

Hoe start je met een Privacy Office:

- Zorg voor een formele opdracht vanuit directie/bestuur om een PO op te zetten
- Benoem de leden van de PO (zie hieronder)
- Stel een statuut of reglement op om op terug te kunnen vallen: Leg taken, rollen en verantwoordelijkheden vast. En laat middelen reserveren.
- Weet wat er speelt in de organisatie: bv. breng de risico's in kaart en ga na hoe er wordt omgegaan met privacy regels
- Zorg voor prioritering en vaststellen van benodigde acties
- Organiseer een passende samenwerking: bv. agendavoering, periodieke bijeenkomsten, periodieke rapportage aan directie/bestuur.

Wat heeft een privacy office nodig en wie kan dat leveren:

- Deskundigheid over Privacy en toezichthouden → FG en PO
- Deskundigheid over Informatiebeveiliging → CISO, ISO of ICT manager
- Kennis van de praktijk → ambassadeurs vanuit verschillende lagen/afdelingen van de organisatie, vertegenwoordigers vanuit de ondernemingsraad (OR), cliënt-/patiëntvertegenwoordigers.
- Uitvoeringskracht: een secretaris, opleidingsadviseurs en communicatie professionals

Alle organisaties groot of klein hebben iets gemeen: namelijk het managen van risico's. Organisaties zijn dagelijks bezig met het minimaliseren van risico's. Dit kan door middel van het "[Three Lines of Defence](#)"-model (Bron: Instituut van International Auditors)



Een structuur waarbinnen de naleving van de AVG georganiseerd en gemonitord wordt, is het met elkaar opzetten van een Privacy Office. Dit is een tweedelijns verdedigingsmuur die fungeert als een interne toezichthouder. Deze tweede lijn controleert of de eerste lijn (degenen die binnen hun werkzaamheden persoonsgegevens verwerken) doet wat afgesproken is. De tweede lijn is deskundig als het gaat om de AVG en adviseert en informeert de eerste lijn hierover. De tweede lijn wordt intern georganiseerd.