Rollen en functies

Naast bestuur en directie zijn er verschillende rollen en functies betrokken bij informatiebeveiliging. De belangrijkste staan hieronder benoemd en kort uitgelegd.

Risico-eigenaren
In het algemeen zijn overal in de organisatie risico-eigenaren te benoemen. Zij spelen een belangrijke rol in de dagelijkse gang van zaken in hun eigen vakgebied om informatie veilig te houden:

- De *IT manager* draagt het risico van de IT
- De *HR manager* draagt het risico van de machtigingen van een medewerker: HR geeft op tijd door wie welke functie heeft en wat in die functie mag worden ingezien (autorisatie). HR geeft op tijd door of iemand bijvoorbeeld uit dienst is of van functie veranderd is en daardoor geen toegang tot, of rechten meer heeft voor bepaalde informatie.
- De *medewerker* draagt het risico van zijn of haar persoonlijk handelen rondom data: de medewerker die met persoonlijke gegevens rondloopt of iets moet invoeren of een systeem netjes moet afsluiten zodat niemand ongeautoriseerd in het systeem kan.
- De *cliënt*, en eventueel zijn of haar mantelzorger, draagt het risico van zorgvuldig omgaan met de toegang die zij hebben tot de eigen gegevens.
- *Partners in het zorgnetwerk* dragen risico voor de uitwisseling van informatie

Kortom: iedereen heeft op zijn eigen gebied of eigen niveau in de organisatie een rol te spelen om informatie veilig te houden. Van de bestuurder die bepaalde verwachtingen mag hebben, de directeur die het beleid uitzet, tot de facilitaire dienst die oplet dat alle deuren letterlijk gesloten blijven.

Specifieke functies, niet verplicht
Er zijn twee veel voorkomende functies die een grote rol spelen en specifiek gericht zijn op informatiebeveiliging. Dit zijn de CISO en de Privacy Officer:

- CISO staat voor 'Chief Information Security Officer'. De CISO is verantwoordelijk voor de uitvoering van het informatieveiligheidsbeleid en zorgt voor de bescherming van systeem en mensen. Van constante monitoring tot incidentmanagement. De CISO stelt elke maand een overzicht op van de afwijkingen en incidenten en bespreekt de voortgang van de informatiebeveligingsacties met het management. De CISO functioneert op managementniveau en heeft een meer coördinerende functie ten aanzien van de risico-eigenaren. Het is goed om de CISO direct onder de Raad van Bestuur te positioneren.

- De Privacy Officer, ook wel PO, werkt op managementniveau en leidt de strategie voor het privacy beleid, stuurt het bewustzijnsbeleid aan en verbetert de processen en compliance. De persoon heeft contact met de media en klanten aangaande privacy onderwerpen en houdt de data privacy ontwikkelingen bij. Een PO heeft daardoor meestal een juridische of IT-achtergrond op gebied van data privacy. Deze functie wordt ook wel Chief Privacy Officer (CPO) genoemd.

Bij bovenstaande functies heeft de NEN 7510 geen inhoudelijke eisen. De organisatie bepaalt zelf welke kennis, ervaring en positionering bij de functie hoort.

Verplichte functie
De rol van Functionaris Gegevensbescherming, ofwel FG, kent wel eisen.

- De Algemene verordening gegevensbescherming AVG (artikel 39) geeft aan dat de Functionaris Gegevensbescherming gevraagd en ongevraagd advies geeft over het beleid van de AVG in de organisatie. De FG ziet toe op de naleving ervan en werkt aan AVG bewustzijn in de organisatie. De FG is contactpersoon voor de Autoriteit Persoonsgegevens (AP). Deze functionaris rapporteert aan het management, maar heeft ook een zelfstandige en onafhankelijke rol om de AVG te kunnen bewaken. Een FG kan eventueel meerdere rollen en werkzaamheden combineren, als dit geen tegenstrijdigheden oplevert.

Combineren van functies en rollen
Bovenstaande functies lijken op elkaar en vooral bij kleinere organisaties lijkt het daarom handig om verschillende functies met elkaar of met andere functies te combineren. De persoon kan daarmee echter in een rolconflict komen. Wat kan wel en wat kan niet?

- Bij het *informatiebeveiligingsbeleid*, wordt veelal implementatie én toezicht gecombineerd in dezelfde functie: bij de CISO.

- Bij het *privacybeleid* wordt uitvoering en toezicht echter gescheiden. Hierbij spelen zowel de Privacy Officer als de Functionaris Gegevensbescherming een rol. De PO is verantwoordelijk voor het uitvoeren en bewaken van het privacybeleid. Dit is vaak een operationeel uitvoerende rol. Deze persoon is veelal het dagelijkse aanspreekpunt voor gegevensbescherming. Als er een nieuwe applicatie of technologie wordt gebruikt, of er is een nieuwe onderzoeksvraag bij de data manager, of werkprocessen worden herzien, dan wordt de PO hier bij gevraagd om te kijken naar de privacy-vraagstukken.

- De rol van CISO en Privacy Officer kunnen in een kleinere organisatie eventueel inhoudelijk gecombineerd worden. Het is daarbij wel belangrijk om te kijken of het werk in de beschikbare tijd gedaan kan worden.

- De FG houdt toezicht en indien nodig moet deze persoon kunnen handhaven en contact opnemen met de Autoriteit Persoonsgegevens (AP). Als de FG ook over het uitvoeren van het privacybeleid gaat, zou deze persoon zijn eigen werk moeten keuren en eventueel melden bij de AP. Ofwel: de slager keurt zijn eigen vlees. Combineer daarom de functie van FG niet met de functie van CISO of Privacy Officer. Eventueel kan een FG wel meerdere organisaties tegelijk bedienen en kunnen organisaties dus samen gebruik maken van één persoon.

Overigens ligt de eindverantwoordelijkheid voor het beveiligings- en privacybeleid nooit bij deze functionarissen, maar altijd bij het bestuur en de directie.