NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Privacy Control Framework: beheersingsdoelstellingen en -controles voor privacyaudits en assurance-opdrachten

Doelstellingen van het Privacy Control Framework (PCF)

Het primaire doel van het PCF is het bieden van een handreiking aan (audit) professionals bij het beoordelen of de controledoelstellingen van een entiteit met betrekking tot privacy en bescherming van persoonsgegevens worden bereikt. Naast de kernelementen van de Algemene Verordening Gegevensbescherming (AVG) is rekening gehouden met *'best practices'* op het gebied van privacy- en gegevensbescherming en informatie *lifecycle management*. Als zodanig kan het PCF worden gebruikt als startpunt voor op maat gemaakte privacyaudits. Het PCF bevat de voorgeschreven doelstellingen en elementen voor privacy-opdrachten op basis van de NOREA Assurance richtlijn 3000.

Gebruik van het Privacy Control Framework

De manier waarop dit PCF in de praktijk wordt gebruikt is afhankelijk van de doelstellingen van de gebruiker. Over het algemeen worden drie soorten gebruikers onderscheiden:

1. De IT-auditor die de privacymaatregelen van een entiteit en het behalen van privacydoelstellingen beoordeelt, met als doel de mate van privacybeheersing of AVG-voorbereiding te beoordelen en tot een advies te komen;

2. De IT-auditor die een privacy assurance-opdracht uitvoert op basis van NOREA richtlijn 3000 en op basis van deze werkzaamheden een assurance rapport afgeeft;

3. Andere professionals (zoals risicomanagers, functionarissen voor de gegevensbescherming, beveiligings- en/of privacymedewerkers) die de privacy-impact of de stand van zaken van de AVG-implementatie in een entiteit wensen te beoordelen.

Bij de beoordeling van de privacybeheersingsmaatregelen kan de betrokken IT-auditor het PCF gebruiken als een algemeen toetsingskader. Aanscherping kan noodzakelijk zijn gegeven de specifieke situatie. Beheersingsdoelstellingen (control objectives, sectie 2) en vooral de beheersingsmaatregelen (controls, sectie 3) moeten op de scope en het doel van de opdracht zijn afgestemd.

Assurance-opdrachten

In het geval van assurance-opdrachten kan het PCF dienen als basis voor de criteria die moeten worden ingebed in het assurance-rapport volgens NOREA richtlijn 3000. Daarvoor kan de IT-auditor de beheersingsdoelstellingen in sectie 2 als uitgangspunt gebruiken voor de scope en de te toetsen beheersingsmaatregelen. De beheersingsmaatregelen ('controls') in deel 3 geven voorbeelden, maar het is de verantwoordelijkheid van de entiteit om ze aan te scherpen of, waar nodig, te wijzigen, gegeven de specifieke kenmerken van de entiteit.

De IT-auditor stelt vast in welke mate de door de entiteit beschreven beheersingsmaatregelen toereikend zijn om, binnen de context van de betreffende entiteit de beheersingsdoelstellingen te realiseren.

De aldus geselecteerde controles kunnen door de IT-auditor worden getest om voldoende en geschikte assurance-informatie te verkrijgen om met een redelijke mate van zekerheid het bestaan of de werking van de beheersingsmaatregelen vast te stellen. Dit niveau van zekerheid is het maximale niveau dat bereikt kan worden, gegeven de NOREA assurance richtlijnen.

NOTE: Het karakter van de rapportage, meestal bestemd voor een brede groep gebruikers, en de intentie van de AVG brengt met zich mee dat een lager zekerheidsniveau (beperkte mate van zekerheid) tot misinterpretaties zouden kunnen leiden; dit wordt derhalve afgeraden.

Privacy Audit Proof 2.0

Met de introductie van het PCF komt de richtlijn 3600 'Assurance-opdrachten met betrekking tot de bescherming van persoonsgegevens (Privacy-audits)' te vervallen.

In plaats daarvan zal het keurmerk 'Privacy Audit Proof' vanaf 2018 worden gebaseerd op een positief assurance-rapport, afgegeven door een Register IT-auditor (RE) met het PCF als toetsingskader. Om de verantwoordelijkheden van de IT-auditor en de betreffende entiteit duidelijk tot uitdrukking te brengen moet het rapport bij voorkeur zijn uitgebracht onder de NOREA richtlijn 3000-A(ttest). De doelgroep van het rapport (gebruikersgroep) wordt door de opdrachtgever bepaald en moet expliciet de goedkeuring hebben van de IT-auditor. Ter voorkoming van misinterpretatie is het gebruik van het 'Privacy Audit Proof' keurmerk alleen bedoeld voor assurance-rapporten met een redelijke mate van zekerheid, zonder beperkingen in het oordeel. Het is de verantwoordelijkheid van de IT-auditor om toe te zien op het juiste gebruik van het keurmerk, zoals vastgelegd in de gebruiksvoorwaarden. Als startpunt voor de oordeelsvorming geldt het register van verwerkingen van de betreffende verwerkings-verantwoordelijke, zoals bedoeld in artikel 30 AVG.