Achtergrond | Edwin Feldmann

De rol van de Register EDP-auditor wordt groter

'Er is geen keurmerk dat stelt dat je AVG-proof bent'

Een officieel certificaat of keurmerk dat laat zien dat een organisatie aan de AVG voldoet, is er niet. Maar als het aan de beroepsvereniging van IT-auditors NOREA, waarin alle Register EDP (Electronic Data Processing, red.) auditors geregistreerd staan, ligt kan hun Privacy Control Framework binnenkort leiden tot een certificering zoals bedoeld in de Europese privacywetgeving.

Het is een kwestie van tijd voordat de Autoriteit Persoonsgegevens (AP) certificeringscriteria goedkeurt voor bedrijven die willen aantonen dat ze er alles aan gedaan hebben om aan de AVG te voldoen. Het Privacy Control Framework van de NOREA voldoet aan alle eisen die daaraan worden gesteld.

De vereniging van Register (RE) IT-auditors telt ongeveer 1750 leden. De hoofdtaak van een IT-auditor is het vaststellen dat de IT bij organisaties zodanig wordt beheerst dat er sprake is van een betrouwbare gegevensverwerking. "IT-auditors controleren bijvoorbeeld of organisaties goed beveiligd zijn tegen cyberaanvallen, of ze zich houden aan wet- en regelgeving op het gebied van informatiebeveiliging. Maar ook het vaststellen dat er geen datalekken zijn, en dat alles ingericht is zodat er sprake is van een efficiënte en betrouwbare gegevensverwerking", legt Marc Welters uit als bestuurslid van de beroepsvereniging van IT-auditors NOREA.

En de IT-auditors krijgen veel vragen over de AVG. "De AVG leidt nog tot veel onduidelijkheid", bevestigt Ed Ridderbeekx, zelfstandig IT-auditor en ook betrokken bij de NOREA. De NOREA heeft in april van dit jaar het Privacy Control Framework uitgebracht."

Dat is een lijst met normen die IT-auditors kunnen gebruiken om bij hun klanten een privacy-audit te doen. "Dat wil helaas niet zeggen dat er zich geen privacy-incidenten of datalekken meer kunnen voordoen. Maar juist die bewijslast dat je er alles aan gedaan hebt om alles op orde te hebben, is juridisch belangrijk bij de AVG. De AVG legt namelijk veel nadruk op die aantoonbaarheid. Daarom is die verklaring van de IT-auditor zo belangrijk", stelt Ridderbeekx.

AVG keurmerk

Veel bedrijven hebben moeite om te voldoen aan de complexe Europese privacywet. Vanwege die onduidelijkheid en het gebrek aan een certificaat of keurmerk, is een aantal bedrijven zelf ook normenkaders gaan ontwikkelen. Zo zijn er allerlei 'AVG-keurmerken' ontstaan die eigenlijk niets garanderen, constateert Welters. "Die bedrijven beweren dat als je dat keurmerk draagt, dat je dan AVG-proof bent, maar dat kan niet want alleen de AP bepaalt of een organisatie 'AVG-proof' is."

Zijn collega Ridderbeekx vult hem aan: "Eigenlijk komt dat hele proces te laat. Dat is wel begrijpelijk want voor 25 mei lag de nadruk vooral op het voldoen aan de wet en niet zozeer op het certificeren. En nu men allerlei inspanningen heeft gedaan om aan de wet te voldoen, zouden organisaties het wel fijn vinden als ze dat op de een of andere manier kunnen bezegelen naar de markt of de concurrentie toe", zegt Ridderbeekx.

"Er zijn landen waar de autoriteit wat betreft certificering veel meer de regie in handen neemt." Dat beaamt Welters: "De Autoriteit Persoonsgegevens zou meer de regie in handen moeten nemen bij het opstellen van een certificaat voor de AVG."

Onafhankelijk

IT-auditors toetsen een bepaalde (IT-) situatie aan een norm . "Als de situatie daarvan afwijkt, constateren we dat en helpen we de betreffende organisatie om de situatie te verbeteren", vertelt Ridderbeekx. Het werk van de Register IT-auditor is echter wel aan strenge eisen en voorwaarden onderhevig. "Het is meer dan alleen maar met een checklist door de IT-organisatie lopen. Je vormt een oordeel over iets ten opzichte van een norm, dat dat doe je ten behoeve van een andere partij. Je bent altijd onafhankelijk." Die onafhankelijkheid wordt gegarandeerd door de beroepsvereniging en de beroepsregels verbonden aan het register van IT-auditors. Elke IT auditor heeft een opleiding van twee tot drie jaar achter de rug. Verder moeten ze nog aan een aantal andere kwaliteitseisen voldoen en alleen dan blijven ze ingeschreven in het register van IT-auditors.

assuranceverklaring geven op basis van een bepaalde werkingsperiode. Bijvoorbeeld dat er is vastgesteld dat specifieke beheersmaatregelen in de IT-processen gedurende 2017 naar behoren hebben gefunctioneerd. Een ISO-certificaat zoals ISO 27001 (informatiebeveiliging) zegt iets over het bestaan van het managementsysteem voor informatiebeveiliging op een bepaald moment in de tijd."

Slechtnieuwsgesprek

Het toetsen van de IT-kant van een organisatie, betekent ook dat IT-auditors geregeld een 'slechtnieuwsgesprek' aan moeten gaan als het allemaal niet zo op orde blijkt. "Zo'n boodschap valt niet altijd in goede aarde en toch breng ik die boodschap." Welters vergelijkt de situatie met een arts die iets bij een patiënt ziet, maar het hem niet vertelt. Dan komt die patiënt één of twee jaar later bij hem en blijkt hij ernstig ziek te zijn. Dan zegt hij ook: 'Had het me toen maar gezegd.' De arts die hem daar niet voor waarschuwt, is geen goede arts. Daar komt bij dat hij gehouden is aan onpartijdige, onafhankelijke en vaktechnisch solide oordeelsvorming. De situatie mooier voordoen dan ze is past daar zeker niet in. Vroegtijdige en transparante communicatie naar de opdrachtgever en het management wél. Zou hij ten onrechte een goedkeurende verklaring afgeven, dan moet hij zich voor de tuchtrechter verantwoorden en kan hij uit het register worden geschrapt.

Marc Welters

Steeds belangrijker

Hoewel het werk van IT-auditors bij veel mensen nog onbekend is, wordt de rol die ze in organisaties spelen wel groter. "Register IT-auditors maken steeds vaker deel uit van de accountantsteams die de jaarcontroles bij bedrijven en instellingen doen. Hun taak is een oordeel te vellen over de betrouwbaarheid van de computersystemen in het kader van de jaarrekeningcontrole. Omdat bedrijven en instellingen hier voor hun bedrijfsvoering steeds meer van afhankelijk zijn, neemt het belang van deze oordelen ook toe", zegt Welters. Hoewel de IT-auditors veel gebreken zien in de cyberbeveiliging van organisaties komt het onderwerp nog maar mondjesmaat terug in de accountantsverklaringen. Overigens ziet hij wel dat daar meer aandacht voor komt. "De budgetten voor IT-auditors zijn de laatste vijftien jaar flink gestegen", vertelt Welters. IT maakt een essentieel onderdeel uit van veel organisaties en daarom wordt de rol van de IT-auditor de komende jaren nog groter, voorspelt hij.

'De Autoriteit Persoonsgegevens zou meer de regie moeten nemen bij het opstellen van een certificaat voor de AVG'

Daarin verschilt het werk bijvoorbeeld van een pentester of ethische hacker die de IT-infrastructuur van een organisatie op de proef stelt. Een ander verschil is dat als een RE IT-auditor zijn werkt niet goed doet, hij als persoon aansprakelijk is en tuchtrechtelijk aangesproken kan worden. Een RE IT-auditor is beëdigd en kan via de tuchtrechter aansprakelijk gesteld worden. "Dat is een extra waarborg om ervoor te zorgen dat wij ons werk goed uitvoeren." Ook verschilt een officiële IT-audit met bijvoorbeeld een ISO-normering of NEN-certificering, legt Welters uit. "Een auditor kan een