Hart Advocaten: tijd om ICT-kennis bij te spijkeren

Leon Engelen - 18 december 2024

Kennis van ICT-risicomanagement wordt onderdeel van de personentoetsing in de financiële sector.

DNB heeft op 28 november bevestigd dat zij de in de Digital Operational Resilience Act (Dora) voorgeschreven kennis en vaardigheden van beleidsbepalers integreert in de door haar uitgevoerde personentoetsing. Het is de verwachting dat de AFM hier op een vergelijkbare wijze mee omgaat voor de bij haar onder toezicht staande ondernemingen, zoals beleggingsondernemingen en beheerders van beleggingsinstellingen. Het is dus aan te raden om – waar nodig – de kennis en vaardigheden bij te spijkeren.

Kennis is een must

Financiële ondernemingen zijn druk bezig met het implementeren van de verplichtingen uit Dora. Dit gebeurt bijvoorbeeld door het aanpassen van interne beleidsstukken en het *re-paperen* van bestaande uitbestedingsovereenkomsten met (kritieke) ICT-dienstverleners. Dit artikel vraagt aandacht voor een wat onderbelichte verplichting uit Dora: de kennis en vaardigheden van beleidsbepalers en medewerkers op het gebied van ICT-risicomanagement.

Dora schrijft voor beleidsbepalers het volgende voor:

"De leden van het leidinggevend orgaan van de financiële entiteit onderhouden actief voldoende kennis en vaardigheden om ICT-risico en de gevolgen daarvan voor de verplichtingen van de financiële entiteit te begrijpen en te beoordelen, onder meer door regelmatig specifieke opleidingen te volgen die in verhouding staan tot het te beheren ICT-risico"

Ook voor de medewerkers van financiële ondernemingen schrijft Dora scholing voor:

"Financiële entiteiten ontwikkelen bewustmakingsprogramma's op het gebied van ICT-beveiliging en opleidingen inzake digitale operationele weerbaarheid als verplichte modules in de opleidingsprogramma's voor het personeel. (...)"

Tot en met het hoogste niveau van de financiële onderneming moet er dus voldoende kennis en vaardigheden zijn om ICT-risico's te begrijpen en beoordelen. Een begrijpelijke gedachte gelet op de technische aard van deze risico's en de toenemende mate waarin ICT-diensten noodzakelijk zijn voor financiële ondernemingen.

In Dora zien we voor wat betreft het vereiste niveau van kennis en vaardigheden de volgende drietrapsraket:

1. voor alle medewerkers geldt dat zij opleiding moeten volgen op het gebied van digitale weerbaarheid en bewust moeten zijn van de ICT-beveiliging;
2. het gehele bestuur moet bovendien voldoende kennis en vaardigheden bezitten over Dora en ICT-risico's die relevant zijn voor de financiële onderneming; en
3. van de bestuurder(s) waar de Dora *compliance* en het ICT-risicomanagement in de portefeuille zit wordt de meest diepgaande kennis en vaardigheden op dit gebied verwacht.

Het is aan te raden – voor zover hier niet al mee begonnen is – om als beleidsbepalers relevante scholing op dit gebied te volgen en het opleidingsprogramma voor de werknemers hierop aan te passen. Hierna ga ik nader in op de gevolgen voor de personentoetsing van (mede-)beleidsbepalers.

Dora en personentoetsing

Voor financiële ondernemingen gaat Dora dus een stap verder dan het actief onderhouden van de kennis en vaardigheden over de wetgeving en ICT-risicomanagement. DNB heeft recent expliciet genoemd dat het ICT-risicomanagement onder Dora onderdeel wordt van de personentoetsing voor (mede-)beleidsbepalers van financiële ondernemingen onder haar toezicht. Het ligt in de lijn der verwachtingen dat de AFM hetzelfde zal doen voor de ondernemingen onder haar toezicht.

Voor (mede-)beleidsbepalers is de verplichte geschiktheids- en betrouwbaarheidstoetsing voorafgaand aan een benoeming al lange tijd gemeengoed. Sinds de gewijzigde Beleidsregel geschiktheid 2012 wordt het beheersen en mitigeren van ICT-risico's ook al meegenomen.

DNB heeft nu aangegeven een stap verder te gaan in het personentoetsingsproces. Bij zowel de beoordeling van het toetsingsdossier als gedurende de toetsingsgesprekken kan Dora aan de orde komen. Kandidaten wordt ook vragen gesteld over Dora, ICT-risicomanagement en de digitale weerbaarheid van de financiële onderneming. Dit brengt een duidelijke verhoging van het vereiste kennisniveau voor kandidaat (mede-)beleidsbepalers met zich, aangezien (aantoonbare) kennis van deze juridisch- en ICT-technische materie vereist is voor de goedkeuring van een voorgenomen benoeming.

Overigens kan deze aanpassing van het toetsingsbeleid van DNB ook van belang zijn voor (mede-)beleidsbepalers in functie. Denk bijvoorbeeld aan een hertoetsing of de beoordeling van het collectief bij een voorgenomen benoeming van een nieuw lid van het bestuur.

DNB stelt dat van de kandidaat (mede-)beleidsbepaler verwacht wordt dat hij of zij:

- kan aangeven wat Dora is en wat de belangrijkste eisen uit deze wetgeving zijn;
- voldoende kennis en vaardigheden heeft op het gebied van ICT-risicomanagement,

ICT-incidenten, (periodiek) testen van digitale operationele weerbaarheid, beheersing van uitbestedingsrisico's en uitwisselingen van informatie over cyberdreigingen;
- in staat is om verantwoordelijkheid te dragen voor het ICT-risicomanagement, strategie en beleid op een adequate wijze te vormen, en (toe te zien op) besluitvormingen hieromtrent; en
- in voldoende mate beschikt over de relevante competenties uit de Beleidsregel geschiktheid 2012, zoals adaptief vermogen, helikopterzicht, omgevingssensitiviteit, onafhankelijke oordeelsvorming en overtuigingskracht.

De toetsing hiervan en het vereiste kennis- en vaardigheidsniveau wordt uiteraard wel afgestemd op de beoogde functie en de aard, omvang en het risicoprofiel van de financiële onderneming waar de beoogde beleidsbepaler aan de slag wil gaan. Bovendien wordt ook op dit onderwerp in het kader van de geschiktheidstoetsing naar het collectief gekeken. Dat wil zeggen dat van een beleidsbepaler waar ICT-risicobeheer in de portefeuille valt, diepgaandere kennis en vaardigheden vereist wordt dan van de beleidsbepalers waarbij dit niet het geval is.

Wat betekent dit in de praktijk?

In de praktijk brengt de impact van Dora op de (mede-)beleidsbepalers huiswerk met zich. Zorg dat u als (mede-)beleidsbepaler op de hoogte bent van Dora en het ICT-risicomanagement, en hier in de praktijk mee om kunt gaan. Dit is belangrijk voor de Dora *compliance* en eventueel de personentoetsing, maar het beheersen van de risico's uit het digitale domein is vooral van cruciaal belang voor een beheerste bedrijfsvoering in het huidige digitale tijdperk.

Niet alleen de (mede-)beleidsbepaler dient geschoold te zijn over Dora overigens. Ook het personeel van de financiële onderneming moet een Dora bewustwordings- en opleidingsprogramma doorlopen.

Leon Engelen is advocaat bij Hart Advocaten, onderdeel van het expertpanel dat maandelijks een bijdrage voor Investment Officer schrijft.

Dit artikel is afkomstig van Investment Officer, een journalistiek platform voor professionals werkzaam in de beleggingsindustrie.

www.investmentofficer.com