Toezichtthema's DNB 2019

Verzekeraars

Thema's DNB toezicht - Verzekeraars	
Aandachtspunt	**Uitwerking**
Toekomststrategie	Net als in 2018 staat de verzekeringssector in 2019 voor belangrijke uitdagingen. DNB zal daarom ook in 2019 verzekeraars challengen op zaken als hun toekomststrategie, hun vermogen zich aan te passen aan een snel veranderende omgeving en hun risicobeheersing.
Scenario's Own Risk Solvency Assessment (ORSA)	De toekomststrategie van verzekeraars beoordeelt DNB door te kijken naar de ORSA-scenario's. DNB wil meer inzicht krijgen in de manier waarop verzekeraars de scenario's selecteren die ze in de ORSA gebruiken. In 2019 zal DNB zich vooral richten op de gevoeligheid van het basisscenario en van stress scenario's voor verschillende winstbronnen en parameters. Van april tot augustus 2019 zal DNB de door (een selectie van) de instellingen ingestuurde ORSA-rapporten analyseren. In september 2019 zal DNB de uitkomsten terugkoppelen.
Beheersing volmachten (schadeverzekeraars)	In 2019 wil DNB vaststellen of de risico's van het volmacht-kanaal adequaat beheerst worden door de verzekeraar. DNB zal hierbij specifiek aandacht besteden aan risico's in relatie tot datakwaliteit en uitbesteding. Als blijkt dat de risicobeheersing sectorbreed onvoldoende effectief is, zal DNB in samenwerking met het Verbond van Verzekeraars en de Nederlandse Vereniging van Gevolmachtigde Assurantiebedrijven nadere guidance geven of andere instrumentarium inzetten om de sector aan te zetten tot verbetering.
Doorlopende aandacht voor Insurtech	De impact van Insurtech – technologische innovatie in de verzekeringsbranche – blijft een speerpunt in het toezicht van DNB. Het is van belang dat verzekeraars technologische ontwikkelingen die gevolgen kunnen hebben voor hun bedrijfsmodellen in beeld hebben en daar adequaat op anticiperen. Insurtech brengt nieuwe operationele risico's met zich mee, of maakt de bestaande operationele risico's relevanter. Het thema-onderzoek dat DNB in 2019 uit zal voeren zal dan ook aandacht besteden aan beheersing van datakwaliteit en IT-risico's als cyber risk. DNB wil bereiken dat verzekeraars de kansen en risico's ten aanzien van technologische ontwikkelingen, innovaties en concurrentie voor hun bedrijfsmodel aantoonbaar in beeld hebben en dat zij strategische besluiten kunnen onderbouwen en implementeren.
Herstel en afwikkeling verzekeraars	Naar verwachting treedt 1 januari 2019 de Wet Herstel- en Afwikkeling Verzekeraars in werking. De wet moet er toe leiden dat verzekeraars beter kunnen worden afgewikkeld. DNB krijgt de verantwoordelijkheid om Voorbereidende Crisisplannen (VCP) op te vragen en resolutie(planning) uit te voeren. In een nog op te stellen good practice VCP om de sector bewust te maken van de noodzaak van het opstellen van een VCP zal DNB rekening houden met de proportionaliteit. Verder zal DNB een risicogebaseerde selectie van verzekeraars verzoeken om in lijn met de good practice een concept VCP op te stellen. DNB zal deze concepten beoordelen en haar bevindingen terugkoppelen aan de sector.
Integriteitstoezicht	In 2019 zal DNB zich onder meer richten op belangenverstrengeling bij beleidsbepalers van verzekeraars. In dit kader zullen de uitkomsten uit de jaarlijkse uitvraag inzake niet-financiële risico's en data analyses afkomstig uit andere bronnen gebruikt worden om dat risico scherper in kaart te brengen.

Toezichtthema's DNB 2019

Verzekeraars

Thema's DNB toezicht – sector overstijgend	
Aandachtspunt	**Uitwerking**
Voornaamste risico's	DNB heeft een aantal risico's benoemd die ook in 2019 om bijzondere aandacht vragen in het toezicht. Het gaat hierbij om de volgende risico's: politieke onzekerheid (vooral Brexit), verandervermogen, cyberaanvallen en IT-disrupties, financieel-economische criminaliteit, herbeprijzing van risico's en veranderende yield curve en kwetsbaarheden op de vastgoedmarkten. Met uitzondering van deze laatste figureerden deze risico's ook al prominent in de Toezicht Vooruitblik 2018. Ze zijn nog steeds actueel.
Technologische vernieuwing	Veel financiële innovaties komen voort uit nieuwe of verbeterde onderliggende technologieën. DNB ziet in toenemende mate financiële innovaties op basis van onder meer kunstmatige intelligentie en distributed ledger technology (DLT). Het is voor DNB van belang deze onderliggende technologieën en de implicaties daarvan voor de financiële sector te begrijpen. DNB doet om deze reden in 2019 nader onderzoek naar onder meer kunstmatige intelligentie en DLT. Ook de opkomst van crypto's vraag om een adequate toezichtreactie. Vanwege de risico's van crypto's voor consumenten en in het kader van het bestrijden van witwassen en terrorismefinanciering is een passend en proportioneel regelgevend kader van belang. DNB blijft daarom in 2019 betrokken bij de verkenning van regulering van crypto's. Digitalisering biedt ook mogelijkheden om effectiever en efficiënter toezicht te houden, zoals snellere en betere inzichten krijgen uit geautomatiseerde verworven en geanalyseerde data, en kansen om de interne bedrijfsvoering van DNB te versterken.
Toekomstgerichtheid en duurzaamheid	In 2019 onderzoekt DNB het verandervermogen bij een risico-gebaseerde selectie van kleine banken, verzekeraars, pensioenfondsen en trustkantoren. De nadruk zal liggen op het verandervermogen ten aanzien van technologische innovatie en het kunnen oplossen van hardnekkige problemen. Het onderzoek van DNB richt zich in het bijzonder op de rol van intern toezicht en het middle management. Afgelopen jaren heeft DNB onderzocht aan welke klimaat-gerelateerde risico's financiële instellingen bloot staan. Als volgende stap zal DNB de beheersing van die risico's verankeren in de beoordelingskaders voor het toezicht op banken, verzekeraars en pensioenfondsen. Hierbij zal ook de dialoog gezocht worden met de sector om van elkaars ervaringen en best practices te kunnen leren. DNB blijft zich in 2019 inzetten voor het vergroten van de rol van het financiële stelsel bij het beheersen van klimaat-gerelateerde risico's en de financiering van groene investeringen. Dit sluit ook aan bij internationale, Europese en nationale (klimaatakkoord) ontwikkelingen. Daarnaast besteedt DNB in 2019 ook aandacht aan de inwerkingtreding van de eis aan kantoorpanden om vanaf 2023 te voldoen aan minimaal energielabel 2023. Deze eis heeft direct gevolgen voor aan kantoren gerelateerde beleggingen en leningen. Van belang is dat instellingen in kaart hebben welk deel van hun bedrijfsleningen met vastgoed als onderpand kantoren betreft en wat de energielabelverdeling is.

Financieel-economische criminaliteit	Financiële instellingen geven nog onvoldoende adequate invulling aan hun poortwachtersfunctie. De aanpak van DNB om deze invulling te verbeteren bestaat uit vier onderdelen: (i) er vindt risico-gebaseerd thematisch en instellings-specifiek onderzoek plaats naar de beheersing van integriteitsrisico's, (ii) leidinggevende verantwoordelijken worden aangesproken op hun verantwoordelijkheid voor het borgen van de poortwachtersfunctie en het zorgdragen voor de juiste compliance-houding binnen instellingen, (iii) nauwe samenwerking met partners binnen het Financieel Expertise Centrum (FEC) en (iv) ontwikkelen van nieuwe preventiemethoden. DNB zal zich in 2019 met haar thema onderzoeken richten op de volgende specifieke gebieden: (a) de voorkoming van betrokkenheid van financiële instellingen bij witwassen en terrorismefinanciering, (b) fiscale risico's en maatschappelijke onbetamelijkheid en (c) ondermijnende en georganiseerde criminaliteit.

Thema's Autoriteit Persoonsgegevens (AP) toezicht – Financial services - Sector overstijgend

Aandachtspunt	Uitwerking
(Register van (niet-gemelde)) datalekken	Sinds het van kracht zijn van de Wet Meldplicht Datalekken op 1 januari 2016, zijn organisaties verplicht om datalekken te melden en een register daarvan bij te houden. Voordat de Algemene Verordening Gegevensbescherming (AVG) in werking trad op 25 mei 2018, lag de focus van de AP voornamelijk op het stimuleren van de verantwoordelijkheden van organisaties om datalekken te melden en (intern) te registreren. Onder de AVG moeten ook niet-gemelde datalekken worden geregistreerd. De AP heeft aangegeven in 2019 extra aandacht te zullen besteden aan niet-gemelde datalekken en datalekken die (mede) zijn veroorzaakt door ernstige tekortkomingen in de beveiliging. De AP zou dit kunnen controleren door dergelijke registers bij de desbetreffende organisaties op te vragen.
(Tekortkomingen in) de beveiliging van persoonsgegevens	De AP geeft aan dat een adequate beveiliging van persoonsgegevens van groot belang is, met name indien binnen een organisatie veel (gevoelige) persoonsgegevens worden verwerkt. Het niet op orde hebben van de beveiliging en/of toegangsautorisatie kan grote risico's met zich meebrengen voor de bescherming van persoonsgegevens, voornamelijk als hierdoor een datalek ontstaat. Derhalve heeft de AP ook aangegeven extra aandacht te zullen besteden aan datalekken die (mede) zijn veroorzaakt door ernstige tekortkomingen in de beveiliging (zoals hierboven aangegeven).

Contact

Pieter van Rijsbergen
HVG Law
pieter.van.rijsbergen@hvglaw.nl
+31 (0) 88 - 407 0490