# Toezichtthema's DNB 2019

## Trustkantoren

| Thema's DNB toezicht - Trustkantoren | |
|---|---|
| **Aandachtspunt** | **Uitwerking** |
| **Wet toezicht trustkantoren 2018** | Een belangrijke wijziging voor zowel trustkantoren als DNB is de nieuwe Wet toezicht trustkantoren (Wtt) 2018 die op 5 juli 2018 door de Tweede Kamer is aangenomen en die naar verwachting in 2019 in werking treedt. De Wtt 2018 brengt aanvullende eisen voor trustkantoren met zich mee. Zo moeten trustkantoren onder andere een tweede beleidsbepaler hebben en een interne compliance functie. Daarnaast moeten ze aan DNB verplichte aanvullende rapportages aanleveren. DNB krijgt met de nieuwe wet meer bevoegdheden, kan hogere sancties opleggen en mag daarnaast opgelegde sancties openbaar maken. DNB toetst via haar jaarlijkse uitvraag en door interactie met specifieke trustkantoren of trustkantoren beschikken over een onafhankelijke en effectieve interne compliance functie conform de Wtt 2018.<br>DNB stelt dat de trustsector zijn eigen verantwoordelijkheid moet laten zien, zowel individueel als collectief, om aan de nieuwe verplichtingen te voldoen. Trustkantoren die niet aan de aangescherpte eisen kunnen voldoen, en dus niet de benodigde professionaliseringsslag kunnen of willen maken, zullen volgens DNB geleidelijk van het toneel moeten verdwijnen (via handhaving of uit eigen beweging). |
| **Financieel-economische criminaliteit** | DNB oefent in 2019 wederom op risicogebaseerde wijze intensief toezicht uit op de trustsector. Hierbij identificeert DNB de kantoren die een verhoogd risico vormen op bijvoorbeeld mogelijke betrokken bij financieel-economisch criminaliteit. DNB voert onderzoeken uit naar de systematische analyse van integriteitsrisico's door trustkantoren en maatschappelijke ondermijnende georganiseerde criminaliteit. DNB is van oordeel dat naast toezicht en aangescherpte wetgeving er ook een heel duidelijke rol is weggelegd voor trustkantoren om de risico's op al dan niet bewuste betrokkenheid bij financieel-economische criminaliteit te mitigeren. |
| **Maatschappelijke betamelijkheid** | DNB schenkt naast instelling-specifiek toezicht ook in breder verband aandacht aan de beheersing van integriteitsrisico's en de wijze waarop trustkantoren invulling geven aan het vereiste van maatschappelijke betamelijkheid. DNB beoordeelt hoe trustkantoren hun beleid en procedures hebben ingericht, zodat zij de risico's die kleven aan maatschappelijk onbetamelijk handelen voldoende in beeld hebben. |
| **Fiscale risico's** | DNB onderzoekt de beheersing van fiscale risico's verbonden aan cliënten van trustkantoren. DNB beoordeelt in 2019 ook in hoeverre trustkantoren de in 2018 uitgebrachte Good Practice agressieve belastingplanning wordt gebruikt in de risicobeheersing. |
| **Toekomstgerichtheid en duurzaamheid** | DNB onderzoekt het verandervermogen bij een risicogebaseerde selectie van trustkantoren met aandacht voor de houdbaarheid van bedrijfsmodellen. De uitkomsten hiervan worden besproken in toezichtgesprekken met individuele instellingen en worden sector breed teruggekoppeld. |

| 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.<br><br>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

Bianca van Tilburg
HVG Law LLP
bianca.van.tilburg@hvglaw.nl
+31 (0)88 – 407 0431

Devika Kharagjitsing
HVG Law LLP
devika.kharagjitsing@hvglaw.nl
+31 (0)88 – 407 1859