Kennedy Van der Laan

ACIS symposium – actualiteiten financieel recht

Kennedy Van der Laan

ACIS symposium – 14 april 2023
actualiteiten financieel recht
Jan Broekhuizen

Digital Operational Resilience Act

Regulation (EU) 2022/2554

Kennedy Van der Laan

Onderwerpen

1. Achtergrond en tijdslijnen
2. Toepassingsgebied
3. Kernbegrippen
4. DORA en uitbesteding
5. Vereisten voor financiële instellingen
6. Vereisten aan overeenkomsten
7. “Oversight Framework” voor kritieke derde aanbieders

Kennedy Van der Laan

Achtergrond en tijdlijnen 01

Kennedy Van der Laan

Achtergrond

Digital Finance Strategy

Een competitieve Europese financiële sector waarin consumenten toegang hebben tot innovatieve financiële producten, waarbij de financiële stabiliteit en de rechten van consumenten zijn gewaarborgd

Doelstelling DORA:
Verhogen niveau digitale weerbaarheid financiële sector door: robuuste regeling met (strengere) uniforme vereisten mbt beveiliging netwerk- en informatiesystemen bedrijfsprocessen financiële entiteiten.

Gaps in wet- en regelgeving voor financiële diensten adresseren en overlap en doublures verwijderen

Andere voorstellen in verband met Digitial Finance Strategy bijvoorbeeld de regulering van crypto assets (MiCA)

Kennedy Van der Laan

Achtergrond

Harmonisatie & samenhang met bestaande EU-regelgeving

1. NIS II Richtlijn (EU) 2022/2555 – horizontaal cybersecurity framework
   - Overlap > naast elkaar, maar DORA lex specialis
   - Consistentie beoogd: Sterke relatie financiële sector en horizontale framework NIS cruciaal ivm consistentie nationale cybersecurity strategieën en informatie-uitwisseling
   - Oversight framework kritieke ICT-dienstverleners DORA complementair aan toezicht cloud providers onder NIS 2
2. Richtlijn weerbaarheid kritieke entiteiten (EU) 2022/2557 – fysieke weerbaarheid
   - Overlap > DORA overruled Hoofdstuk III en IV Richtlijn voor financiële entiteiten
     (geborgd in brede vereisten ICT-risicobeheer/rapportage)
3. PSD-2 richtlijn (EU) 2015/2366
   - Meldplicht ICT-incidenten DORA vervangt meldplicht onder PSD2 voor betaaldienstaanbieders
4. EIOPA guidelines on outsourcing to cloud service providers (+ EBA & ESMA guidelines)
   - DORA aanvullend nodig ter bestrijding systeemrisico's door blootstelling financiële sector aan beperkt aantal kritieke ICT-leveranciers
   - Ontbrekende mandaten & instrumenten nationale regelgeving voor toezichthouders tbv inzicht in afhankelijkheden en concentratie

Kennedy Van der Laan

Tijdslijnen

- 20 september 2020 — Proposal DORA
- Februari / juni 2021

  Adviezen Europees Economisch en Sociaal Comité, Europese Toezichthouder voor gegevensbescherming, Europese Centrale Bank
- 20 mei 2022 — Voorlopig akkoord (ER & EP)

  Wijzigingen t.o.v. proposal:
  - *Extra proportionaliteit aangebracht > partijen uitgezonderd & versimpeld kader bepaalde type ondernemingen (bijv. micro)*
  - *Verdere aanscherping samenhang met bestaande EU-regelgeving (NIS2, PSD2 etc)*
  - *Vrijwillige meldingsoptie cyberdreigingen toegevoegd*
- **16 januari 2023** — **Inwerkingtreding**
- < 17 juli 2024 — Deadline ontwerp technische reguleringsnormen tbv contractual terms vanuit ESA's (Joint Committee)
- < 17 januari 2025 — Einde implementatieperiode

Kennedy Van der Laan

Toepassingsgebied

02

Toepassingsgebied

Entiteiten zoals:

banken, **verzekeraars, verzekerings- en herverzekeringstussenpersonen**, beleggingsondernemingen, bedrijfspensioenvoorzieningen, aanbieders van crowdfundingdiensten, derde aanbieders van ICT diensten e.a.

➢ Uitgesloten entiteiten, onder meer

- Beheerders alternatieve beleggingsinstellingen (art. 3 lid 2 AIFMD richtlijn)
- Verzekerings- en herverzekeringsondernemingen als bedoeld in art. 4 Richtlijn Solvabiliteit II
- Cumulatieve vereisten o.a. premie-inkomsten <5M p/j en totale technische voorzieningen <25M
- Instellingen voor bedrijfspensioenvoorzieningen <15; leden
- **Micro, kleine of middelgrote (her)verzekeringstussenpersonen**

Kennedy Van der Laan

Kernbegrippen

03

Enkele kernbegrippen

1. ICT Diensten
2. Kritieke of belangrijke functie
3. Kritieke derde aanbieder van ICT Diensten
4. ICT-concentratierisico

ICT Diensten

Brede opvatting definitie “ICT-diensten” onder DORA

Ook digitale en gegevensdiensten die doorlopend via ICT systemen aan 1 of meer interne/externe gebruikers wordt geleverd

Incl. ‘over the top’-services (bepaalde telefoondiensten)

Kritieke of belangrijke functie

“Kritieke of belangrijke functie”: een functie waarvan de verstoring wezenlijk afbreuk zou doen aan de financiële prestaties van een financiële entiteit of aan de soliditeit of de continuïteit van haar diensten en activiteiten, of waarvan de beëindiging of gebrekkige of mislukte uitvoering wezenlijk afbreuk zou doen aan de permanente naleving door een financiële entiteit van de voorwaarden en verplichtingen uit hoofde van haar vergunning of haar andere verplichtingen uit hoofde van het toepasselijke recht inzake financiële diensten;

omvat de “kritieke functies” als bedoeld in artikel 2, lid 1, punt 35, van Richtlijn 2014/59/EU:

activiteiten, diensten of bedrijfsactiviteiten waarvan de onderbreking naar alle waarschijnlijkheid in een of meer lidstaten tot een **verstoring van essentiële diensten aan de reële economie** zal leiden of, wegens de omvang of het marktaandeel van een instelling of groep, haar verwevenheid met entiteiten binnen en buiten een groep, haar complexiteit of haar grensoverschrijdende activiteiten, **de financiële stabiliteit zal verstoren**, vooral wat de vervangbaarheid ervan betreft.

Kennedy Van der Laan

Kritieke derde aanbieder ICT diensten

Kritieke derde aanbieder van ICT Diensten: een derde aanbieder van ICT-diensten die overeenkomstig artikel 31 DORA is aangewezen als cruciaal. **Criteria**, onder meer

a) de systemische effecten op de stabiliteit, continuïteit of kwaliteit van de verlening van financiële diensten ingeval de betrokken derde aanbieder van ICT-diensten te maken zou krijgen met een grootschalige operationele verstoring van de dienstverlening,
b) het systemische karakter of belang van de financiële entiteiten die afhankelijk zijn van de betrokken derde aanbieder van ICT-diensten,
c) de afhankelijkheid van financiële entiteiten ten aanzien van de diensten die door de betrokken derde aanbieder van ICT diensten worden verleend met betrekking tot **kritieke of belangrijke functies** van financiële entiteiten waarbij uiteindelijk dezelfde derde aanbieder van ICT-diensten betrokken is,
d) de graad van substitueerbaarheid van de derde aanbieder van ICT-diensten

Kennedy Van der Laan

Kritieke derde aanbieder ICT diensten

Nooit “kritiek” zijn:

(i) financiële entiteiten die ICT-diensten verlenen aan andere financiële entiteiten;

(ii) derde aanbieders van ICT-diensten die onderworpen zijn aan oversightkaders die zijn vastgesteld ter ondersteuning van de in artikel 127, lid 2, van het Verdrag betreffende de werking van de Europese Unie bedoelde taken;

(iii) aanbieders van ICT-diensten **binnen een groep**;

(iv) derde aanbieders van ICT-diensten die **uitsluitend in één lidstaat ICT-diensten verlenen aan financiële entiteiten die alleen in die lidstaat actief zijn**.

Kennedy Van der Laan

ICT-concentratierisico

Een blootstelling aan individuele of aan meerdere onderling verbonden **kritieke derde aanbieders van ICT-diensten**, waardoor een bepaalde mate van afhankelijkheid ten aanzien van deze aanbieders ontstaat, zodat de onbeschikbaarheid, het falen of een ander soort tekortkoming van deze aanbieder het vermogen van een financiële entiteit om **kritieke of belangrijke functies** te vervullen in gevaar kan brengen, ertoe kan leiden dat zij andere soorten nadelige effecten, waaronder grote verliezen, ondervindt, of de **financiële stabiliteit van de Unie in haar geheel in gevaar kan brengen**

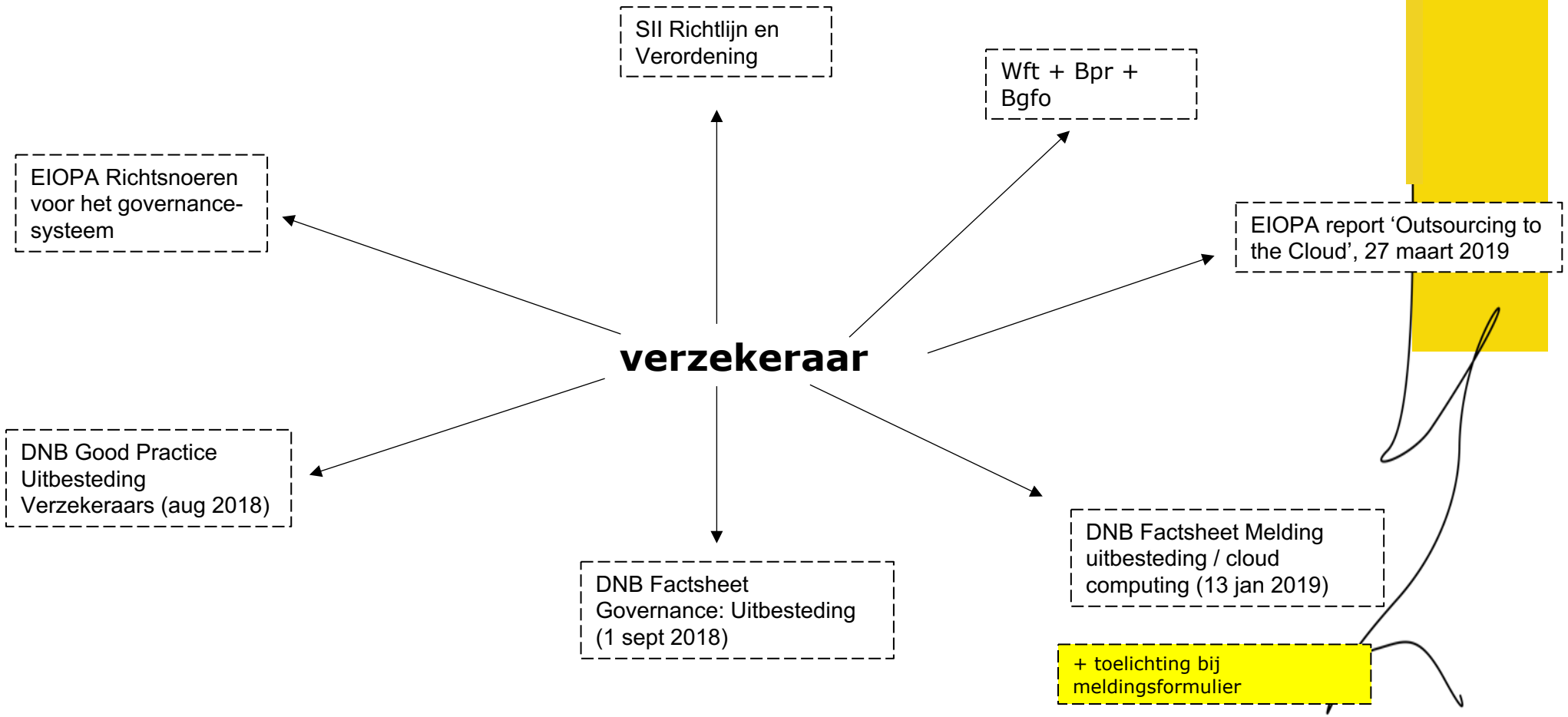
Kennedy Van der Laan

Dora en uitbesteding

04

Publiekrechtelijk kader

Waar vinden we de “klassieke” uitbestedingsregels voor verzekeraars?



Kennedy Van der Laan

DORA en uitbesteding

DORA gaat over het beheer van ICT-risico's wanneer ICT diensten door derden worden verleend

DORA vormt daarmee een aanvulling op het voor uitbestedingen geldende sectorale recht, zoals in het Solvency II regime

Solvency II uitbesteding: overeenkomst tussen een verzekeraar en een al dan niet onder toezicht staande dienstverlener op grond waarvan deze dienstverlener een proces, een dienst of een activiteit uitvoert die anders door de verzekeraar zelf zou worden uitgevoerd.

Kennedy Van der Laan

Uitbesteding in de Wft

Wft: het door een financiële onderneming verlenen van een opdracht aan een derde tot het ten behoeve van die financiële onderneming verrichten van werkzaamheden:

a. die **deel uitmaken van of voortvloeien uit het uitoefenen van haar bedrijf** of het verlenen van financiële diensten;

of b. die deel uitmaken van de **wezenlijke bedrijfsprocessen** ter ondersteuning daarvan.

Met de term “wezenlijke” wordt tot uitdrukking gebracht dat de regels voor uitbesteding niet voor elke werkzaamheid van belang zijn. Deze materialiteitsdrempel wordt in de verschillende regelingen met verschillende termen aangeduid. Ze komt echter telkens op hetzelfde neer: een beperking van de reikwijdte van de uitbestedingsregels tot de voor het toezicht relevante werkzaamheden.

De beperking tot “wezenlijke activiteiten” komt overeen met een beperking tot “**kritieke of belangrijke** operationele taken”.

Uitbesteding in Solvency II

In Solvency II worden die “wezenlijke werkzaamheden” omschreven in termen van de gevolgen waartoe ze niet mogen leiden. Die gevolgen zijn:

(a) wezenlijke afbreuk aan de kwaliteit van het governancesysteem,
(b) onnodige toename van het operationele risico,
(c) afbreuk aan het vermogen van de toezichthouder om te controleren of de onderneming haar verplichtingen nakomt, en
(d) ondermijning van de continuïteit of toereikendheid van de dienstverlening aan de cliënten.

DORA legt daarnaast een (bredere) nadruk op ondermijning financiële prestaties van de instelling of bredere financiële stabiliteit van de markten

Uitbesteding en “quasi – uitbesteding”

Waar intra-group uitbesteding nooit “kritiek” kan zijn in de zin van DORA, is van “uitbesteding” per definitie geen sprake wanneer een verzekeraar of bemiddelaar diensten laat verrichten door een bijkantoor in een derde-land.

Zie in dit verbond **EIOPA’s Supervisory Statement on the use of governance arrangements in third countries** van 3 februari 2023

“3.4 The third country branch should neither perform regulated functions or activities in such a way that leads to the undertaking or intermediary being ***disproportionally dependent*** *on the arrangement in a third country for its activities in the EEA nor should the operation of that branch* ***materially impair the system of governance, increase operational risk or undermine policyholder protection****.”*

Kennedy Van der Laan

Vereisten voor financiële instellingen 05

Kennedy Van der Laan

Vereisten voor financiële instellingen

Vereisten voor financiële instellingen m.b.t.:

i. ICT-risicobeheer (Hoofdstuk II, art 5 t/m 16);
ii. Meldingsplicht ernstige ICT incidenten en cyberdreigingen (aan toezichthouder en in toekomst wellicht op central Europees nivo) (Hoofdstuk III, art. 17 t/m 22)
iii. Testen van digitale operationele weerbaarheid (Hoofdstuk IV, art 24 t/m 27);
iv. Informatieuitwisseling cyberdreigingen en –kwetsbaarheden binnen “vertrouwensgemeenschappen” van instellingen (art. 45);
v. Beheersmaatregelen ICT-risico derden, aan de hand van beginselen (instelling blijft verantwoordelijk, beheer aan de hand van evenredigheidsbeginsel) (Hoofdstuk V, art 28 en 29).

Kennedy Van der Laan

Vereisten aan overeenkomsten

06

Kennedy Van der Laan

Vereisten aan overeenkomsten met ICT dienstverleners

Contractuele bepalingen (art. 30):

- **1 schriftelijk document**, op papier of downloadbaar, duurzaam toegankelijk formaat
- Inhoud overeenkomst bij *alle* uitbestedingen
  a. Duidelijke omschrijving diensten + of onderuitbesteding is toegestaan (bij kritiek of belangrijk)
  b. Locatie diensten + gegevens
  c. Beschikbaarheid, authenticiteit, integriteit, vertrouwelijkheid (persoons)gegevens
  d. Toegang, herstel, teruggave data bij beëindig (insolventie, resolutie, faillissement of einde ovk)
  e. Service levels
  f. Incidentmanagement (kosteloos of vooraf bepaalde prijzen)
  g. Medewerkingsverplichting toezichthouders
  h. Beëindigingsmogelijkheden en – opzegtermijnen
  i. Deelname IT-leverancier aan bewustwordingsprogramma's / opleidingen digitale operationele weerbaarheid van financiële instelling

Kennedy Van der Laan

Vereisten aan overeenkomsten met ICT dienstverleners

- Aanvullend: bij uitbesteding van **kritieke of belangrijke functies**

  a. Service levels+ (nauwkeurige kwantitatieve en kwalitatieve prestatiedoelstellingen)
  b. Kennisgevingstermijnen & rapportageverplichtingen
  c. Verplichting dienstverlener bedrijfsnoodplannen
  d. Medewerkingsverplichting TLPT ("dreigingsgestuurde penetratietest" threat led penetration testing)
  e. Monitoringsrecht (door onbeperkte audit, toegang, inspectierechten), garantieniveaus, volledige medewerking tijdens audit toezichthouder, informatieplicht over bijzonderheden tbv inspecties en audits)
  f. Exit strategieën

Kennedy Van der Laan

Vereisten aan overeenkomsten met ICT dienstverleners

- Bij micro-ondernemingen mogen de rechten van toegang, inspectie en audit van de financiële entiteit worden gedelegeerd aan een onafhankelijke derde partij die wordt aangesteld door de derde aanbieder van ICT-diensten, waarbij de financiële entiteit de derde partij te allen tijde om informatie en garanties kan verzoeken met betrekking tot de prestaties van de derde aanbieder van ICT-diensten

- Gebruik modelcontractbepalingen ontwikkeld door overheidsinstanties

- Ontwerp technische reguleringsnormen Joint Committee (ESA's) voor financiële entiteiten tbv bepaling wanneer over te gaan tot uitbesteding van ICT diensten die kritische of belangrijke functies ondersteunen
    - Factoren: algehele risicoprofiel financiële instelling & aard, schaal en complexiteit diensten

Kennedy Van der Laan

“Oversight Framework” kritieke derde aanbieders

07

Kennedy Van der Laan

Oversight Framework voor kritieke derde aanbieders van ICT diensten

- Oversight Forum

  Het oversightforum beoordeelt de afhankelijkheden van financiële entiteiten ten aanzien van derde aanbieders van ICT-diensten op basis van de informatie die het van de bevoegde autoriteiten ontvangt.

- Joint Committee ESA's
  - Wijzen kritieke derde aanbieders aan
  - Kennisgeving > mogelijkheid tot bezwaar/input IT leverancier
  - Vaststelling lijst kritieke derde aanbieders, publicatie, actualiseren (jaarlijks)
  - Wijst voor iedere leverancier **Lead Overseer** aan

Kennedy Van der Laan

Vragen?

Kennedy Van der Laan

Amsterdam
Molenwerf 16
1014 BG Amsterdam
Postbus 58188, 1040 HD
+31 20 5506 666