BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

DORA – Ein Überblick

Dr. Katharina Fechler

Referat GIT 3
Grundsatz IT-Aufsicht und Aufsichtsunterstützung

DORA - Digital Operational Resilience Act

Ziele

- Stärkung der **Sicherheit und operationalen Resilienz** des gesamten europäischen Finanzsektors
- Schaffung einheitlicher und konsistenter Anforderungen für den gesamten Finanzsektor
  → **Harmonisierung**
- Berücksichtigung proportionaler Anforderungen
  → **Prinzip der Proportionalität**

Anwendungsbereich

- **Finanzsektorübergreifend**
- CRR-Kreditinstitute, Zahlungsinstitute (einschließlich registrierter Kontoinformationsdienstleister), E-Geld-Institute, Wertpapierfirmen, Anbieter von Krypto-Dienstleistungen (MiCA), CSD, CCP, Handelsplätze, Transaktionsregister, Verwaltungsgesellschaften, AIFM, Datenbereitstellungsdienste, Versicherungs- und Rückversicherungsunternehmen, Versicherungsvermittler, EbAVs, Ratingagenturen, Administratoren kritischer Referenzwerte, Verbriefungsregister, Schwarm-finanzierungsdienstleister
- Erweiterungen im FinmadiG vorgesehen

Geltungsbereich: Ausnahmen & Vereinfachungen

Ausnahmen vom Anwendungsbereich (Artikel 2 Absatz 3 DORA):

- Verwalter alternativer Investmentfonds im Sinne von Artikel 3 Absatz 2 der Richtlinie 2011/61/EU;
- Versicherungs- und Rückversicherungsunternehmen im Sinne von Artikel 4 der Richtlinie 2009/138/EG;
- Einrichtungen der betrieblichen Altersversorgung, die Altersversorgungssysteme mit insgesamt weniger als 15 Versorgungsanwärtern betreiben;
- gemäß den Artikeln 2 und 3 der Richtlinie 2014/65/EU ausgenommene natürliche oder juristische Personen;
- Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, bei denen es sich um Kleinstunternehmen oder kleine oder mittlere Unternehmen handelt;
- Postgiroämter im Sinne von Artikel 2 Absatz 5 Nummer 3 der Richtlinie 2013/36/EU.

Vereinfachungen (Artikel 16: vereinfachter IKT-Risikomanagementrahmen für Artikel 5 bis 15):

- kleine **EbAVs**
- kleine und nicht verflochtene **Wertpapierfirmen**
- **Kleinstunternehmen**

Kleinstunternehmen

Finanzunternehmen, das weniger als zehn Personen beschäftigt und dessen Jahresumsatz bzw. -bilanzsumme 2 Mio. EUR nicht überschreitet.

Kleinunternehmen

Finanzunternehmen, das zehn oder mehr, aber weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. -bilanzsumme 2 Mio. EUR überschreitet, nicht jedoch 10 Mio. EUR.

Mittleres Unternehmen

Finanzunternehmen, das kein Kleinunternehmen ist, das weniger als 250 Personen beschäftigt und dessen Jahresumsatz 50 Mio. EUR und/oder dessen Jahresbilanzsumme 43 Mio. EUR nicht überschreitet.

Wesentliche Elemente in DORA

IKT-Risikomanagement

- **Governance und Organisation**
- **IKT-Risikomanagement-rahmen**
- **IKT -Systeme, -Protokolle und –Tools**
- **Lernprozesse und Weiterentwicklung**
- **Kommunikation**

IKT-Drittpartei-risikomanagement

- **Allgemeine Prinzipien** (u. a. Informationsregister über IKT-Drittparteivertrags-beziehungen, Mitteilungen an die Aufsichtsbehörden, und Mindestvertrags-bestandteile)

EU-Überwachungs-rahmenwerk

- Überwachung von **kritischen IKT-Drittdienstleistern**

IKT-Vorfallmeldewesen

- Festlegung von **Definitionen** IKT-bezogener Vorfälle
- **Klassifikationskriterien** von IKT-bezogenen Vorfällen
- **Meldeprozess,** Berichtswesen von IKT-bezogenen Vorfällen und Cyberbedrohungen

Testen der digitalen operationalen Resilienz

- **Basistests**
- Gesamter Finanzsektor
- Schwachstellenscans, Quellcodetests, Performancetests etc.

TLPT

- **Fortgeschrittene Tests**
- TLPT: Threat Led Penetration Tests
- Nur „systemrelevante“ Finanzunternehmen mit hohem IKT-Reifegrad
- TIBER-EU als „Blaupause“

Information Sharing & Cyberübungen

- Freiwilliger **Austausch von Informationen und Erkenntnissen** zwischen Finanzunternehmen zur Verbesserung der „Situational Awareness“
- Sektorübergreifende **Krisenmanagement- und Notfallübungen** mit Cyberbezug zur Verbesserung der Kommunikation und Stärkung der Resilienz im Finanzsektor

Europäische Umsetzungsarbeiten

Erstellung der Level-2- und Level-3-Rechtstexte in EU Arbeitsgruppen

Die öffentliche Konsultation erfolgte bis zum 11. September 2023 für:

Vorlage bei EU-Kommission bis zum 17. Januar 2024

- RTS zum **IKT-Risikomanagementrahmen** (Art. 15)
- RTS zum vereinfachten **IKT-Risikomanagementrahmen** (Art. 16 Abs. 3)
- RTS zu Kriterien für die Klassifizierung von **IKT-bezogenen Vorfällen** (Art. 18 Abs. 3)
- ITS zur Erstellung einer Standardvorlage für das **Informationsregister** (Art. 28 Abs. 9)
- RTS zur Leitlinie in Bezug auf die **Nutzung von IKT-Dienstleistungen** (Art. 28 Abs. 10)

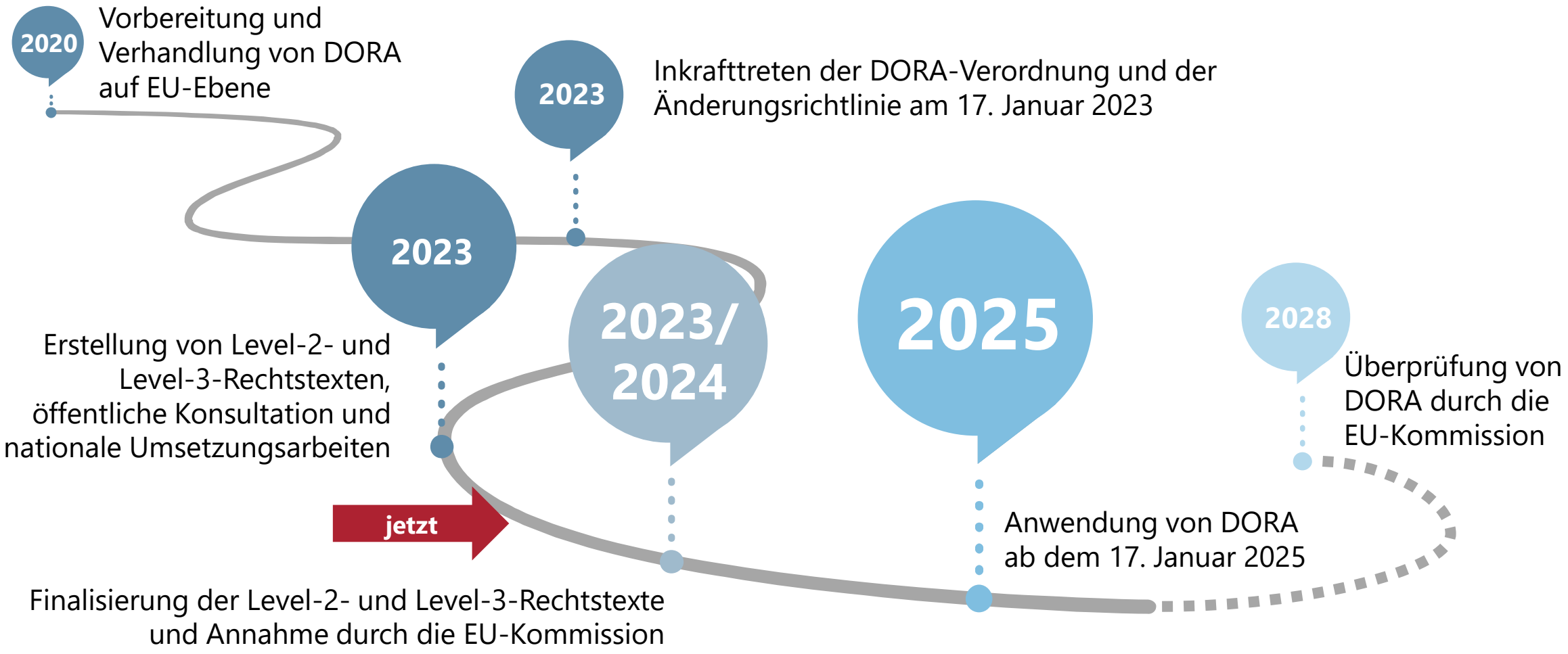
Europäische Umsetzungsarbeiten

Ausstehene öffentliche Konsultation:

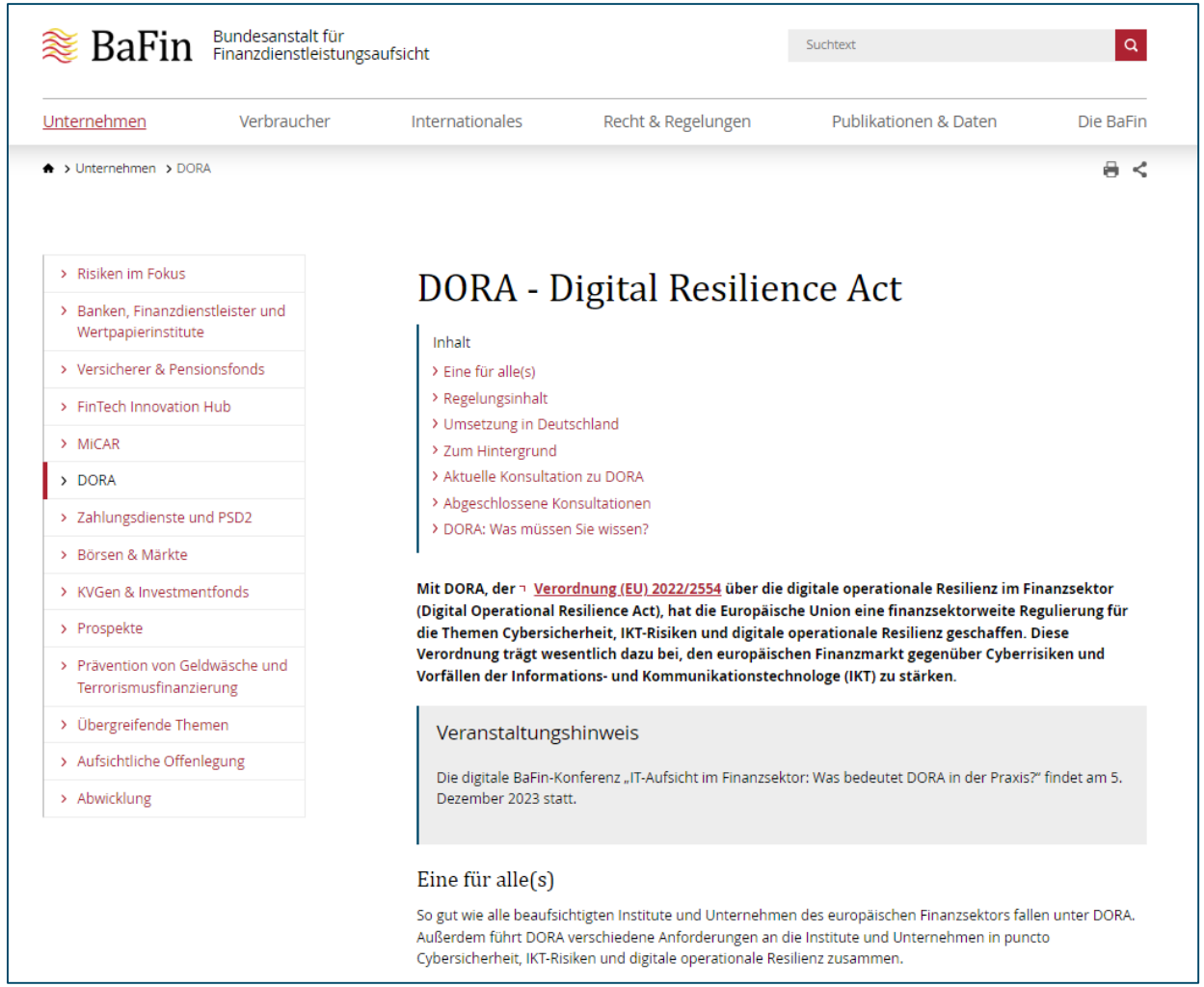
- Leitlinien für die Schätzung der aggregierten Kosten und Verluste verursacht durch schwerwiegende **IKT-bezogene Vorfälle** (Art. 11 Abs. 11)
- RTS zur Päzisierung der Meldung von schwerwiegenden **IKT-bezogenen Vorfällen** (Art. 20 lit. a), ITS zur Festlegung eines Standardformats (Art. 20 lit. b)
- RTS zur Präzisierung von Aspekten des **TLPT** (Art. 26 Abs. 11)
- RTS zur Präzisierung von Aspekten der **Untervergabe von IKT-Dienstleistungen** zur Unterstützung kritischer oder wichtiger Funktionen (Art. 30 Abs. 5)
- Leitlinien für die Kooperation zwischen den ESAs und den zuständigen Behörden hinsichtlich der Struktur der **Überwachung** von kritischen IKT-Drittdienstleistern(Art. 32 Abs.7)
- RTS zur Präzisierung der Durchführung der **Überwachung** von IKT-Drittdienstleistern (Art. 41 Abs. 2)

Vorlage bei EU-Kommission bis zum 17. Juli 2024

Vergangenes, aktuelles und nächste Schritte



Informationen & Kontakt



www.bafin.de/dora

DORA@bafin.de

Dr. Katharina Fechler
GIT 3 Grundsatz IT-Aufsicht und Aufsichtsunterstützung
Katharina.Fechler@bafin.de
+49 (0)228 4108-4473

Lucas Pausewang
GIT 1 Cybersicherheit in der Digitalisierung
Lucas.Pausewang@bafin.de
+49 (0)228 4108-7269

BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Vielen Dank!