DORA: ENDSPURT BIS ZUM 17.01.2025

Die Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA-VO) ist ab 17.01.2025 anwendbar.

Sie definiert Vorgaben zum IKT-Risikomanagement, zu IKT-bezogenen Vorfällen, sowie zu Resilienztests und zum Management des IKT-Drittparteienrisikomanagements. Darüber hinaus wird ein neuer Überwachungsrahmen für kritische IKT-Drittdienstleister geschaffen. Außerdem wird ein Austausch zu Cyberbedrohungen zwischen den Finanzunternehmen ermöglicht.
Die Anforderungen aus DORA bedingen teils sehr spezifische Vorbereitungsarbeiten, die eine strukturierte Herangehensweise erfordern. Zudem sind keine Übergangsfristen vorgesehen.
Nutzen Sie somit die verbleibende Zeit, um die letzten Lücken zwischen den DORA-Vorgaben und Ihren Vorbereitungen zu schließen!

Sind Sie bereit? Erfüllen Sie bereits die folgenden beispielhaft ausgewählten Erfordernisse?

IKT-Risikomanagement

Governance und Organisation:

- ☐ Ein Governance- und Kontrollrahmen iZm IKT-Risiken ist eingerichtet.
- ☐ Die Geschäftsleitung hat ausreichend Know-How auf dem Gebiet IKT-Risiken und Digitalisierung.
- ☐ Eine eigene Auslagerungsfunktion ist eingerichtet.

IKT-Risikomanagementrahmen:

- ☐ Der IKT-Risikomanagementrahmen ist Teil des gesamten Risikomanagementsystems und wird jährlich überprüft.
- ☐ Eine unabhängige Kontrollfunktion ist eingerichtet.
- ☐ Der IKT-Risikomanagementrahmen umfasst eine Strategie für die Betriebsstabilität digitaler Systeme.

IKT-Asset-Inventar:

- ☐ Alle IKT-Assets sind klassifiziert und inventarisiert.

FMA-Hinweise:
Es gelten Ausnahmen bzw. Erleichterungen für Kleinstunternehmen und Unternehmen, für die der vereinfachte IKT-Risikomanagementrahmen zur Anwendung gelangt (Art 16 Abs 1 DORA-VO).

IKT-bezogene Vorfälle

Prozess:

- ☐ Ein formeller Prozess für die Behandlung und Klassifizierung von IKT-Vorfällen ist vorhanden.

Behördliche Meldung:

- ☐ Schwerwiegende IKT-bezogene Vorfälle können unmittelbar ab DORA-Start korrekt klassifiziert und an die FMA gemeldet werden.

FMA-Hinweise:

- Die Meldung von schwerwiegenden IKT-bezogenen Vorfällen erfolgt für alle Unternehmen (auch signifikante Institute) über die Incoming Plattform.
- Eine Meldung von schwerwiegende Cyberbedrohungen an die FMA ist ab 17.1.2025 auf freiwilliger Basis (über die Incoming Plattform) möglich.

Testen der digitalen operationalen Resilienz

Testprogramm:

- ☐ Ein solides und umfassendes Testprogramm ist erstellt.
- ☐ Prozesse zur Überprüfung des Testprogramms sind etabliert.
- ☐ Ressourcen für Tester sowie Maßnahmen gegen Interessenskonflikte bei internen Testern sind bereitgestellt.
- ☐ Verfahren und Leitlinien zum Follow-Up nach Tests sind eingerichtet.
- ☐ Ein zumindest jährlicher Testrhythmus bei allen IKT-Systemen und -Anwendungen, die kritische oder wichtige Funktionen unterstützen, ist etabliert.

FMA-Hinweise:

- Finanzunternehmen, für die ein Threat-Led Penetration Test (TLPT) noch im Jahr 2025 geplant ist, werden jedenfalls rechtzeitig vor Testbeginn informiert.

Management des IKT-Drittparteienrisikos

Informationsregister:

- ☐ Ein Informationsregister, das sich auf alle vertraglichen Vereinbarungen über die Nutzung von durch IKT-Drittdienstleister bereitgestellten IKT-Dienstleistungen bezieht, ist eingerichtet.
- ☐ Prozesse sehen die zeitnahe ex-ante Anzeige an die FMA über geplante vertragliche Vereinbarungen hinsichtlich IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, vor. Für den Fall, dass eine (bestehende) Funktion kritisch oder wichtig geworden ist, ist die FMA ebenso zu informieren.

Strategie für das IKT-Drittparteienrisiko:

- ☐ Die Strategie für das IKT-Drittparteienrisikomanagement ist beschlossen.
- ☐ Dabei ist gegebenenfalls die Strategie zur Nutzung mehrerer Anbieter berücksichtigt.
- ☐ Das Leitungsorgan prüft Risiken zu Verträgen über IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen.

Due Diligence:

- ☐ Vorvertragliche DORA-Verpflichtungen sind berücksichtigt.
- ☐ Verträge werden nur mit IKT-Drittdienstleistern, welche angemessene Standards für Informationssicherheit einhalten, abgeschlossen.
- ☐ Die Häufigkeit von Audits und Inspektionen von IKT-Drittdienstleistern ist vorab auf der Grundlage eines risikobasierten Ansatzes bestimmt.

Vertragsvorgaben:

- ☐ DORA-Mindestvertragsvorgaben werden erfüllt.
- ☐ Die zusätzlichen Vertragsanforderungen bezüglich der Nutzung von IKT-Dienstleistungen, die kritische oder wichtige Funktonen unterstützen, werden eingehalten.

Ausstiegsstrategien:

- ☐ Für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, sind Ausstiegsstrategien eingerichtet.

FMA-Hinweise:

- Für die neue ex-ante Anzeige gemäß Art. 28 Abs. 3 DORA wird je nach sektoraler Ausgestaltung ein adaptiertes/neues Formular auf der Incoming Plattform zur Verfügung gestellt.

Meldung Informationsregister an die FMA – Zeitvorgaben:

- Informationsregister sind 2025 für das Referenzdatum 31.03.2025 aufzubereiten.
- Die Meldung der Informationsregister an die FMA hat in der ersten Aprilwoche zu erfolgen.
- Die Meldung von signifikanten Kreditinstituten erfolgt nicht an die FMA.

Die FMA selbst hat Informationsregister an die ESAs bis zum 30.04.2025 zu übermitteln.

Vorbereitung Informationsregister:

- Bereiten Sie das Informationsregister insb. auf Basis des **ITS zum Informationsregister** zeitnah vor.

Überwachungsrahmen für kritische IKT-Drittdienstleister

☐ Die Einstufung kritischer IKT-Drittdienstleister basiert auf den Inhalten der Informationsregister; eine ordnungsgemäße Führung und die zeitgerechte Übermittlung dieser Register an die FMA sind sichergestellt.

FMA-Hinweise:

- Der neue Überwachungsrahmen startet voraussichtlich im vierten Quartal 2025.

Informationsaustausch & Notfallübungen

Informationsaustauschvereinbarungen:

☐ Vereinbarungen über den Austausch von Informationen und Erkenntnissen über Cyberbedrohungen zwischen den Finanzunternehmen (z.B. Austrian Trust Circle oder FS-ISAC) werden der FMA mitgeteilt.

FMA-Hinweise:

- Ein erster Round Table findet in der ersten Märzwoche 2025 statt.
- Die FMA unterstützt den durch DORA ermöglichten Informationsaustausch zu Cyberbedrohungen.

Weitere Informationen können Sie der **FMA-DORA-Website** entnehmen. Auch auf der **Website der Europäischen Kommission** findet sich ein Überblick zum Stand der rechtlichen DORA-Spezifizierungen.

Durch sämtliche Maßnahmen sollen die Chancen der Digitalisierung genutzt und gleichzeitig damit verknüpfte Risiken konsequent adressiert werden.

Im Ergebnis profitiert Ihr Unternehmen durch die nachhaltige Stärkung von IKT- und Cybersicherheit!