Deutsche Stiftung für Recht und Informatik

DORA – Gesetzliche Verordnung von IT-Sicherheit im Finanzsektor

Verena Reichstein
DLA Piper

Herbstakademie 2024

Verordnung über digitale operationale Resilienz im Finanzsektor („*Digital Operational Resilience Act*“, kurz *DORA*) – (EU) 2022/ 2554

Hintergrund:

- Zunehmende Abhängigkeit des Finanzsektors von **IKT-Leistungen und insbesondere IKT-Drittdienstleistern**
- Steigende **Cybersicherheitsrisiken**
- Status quo: EU-weite **Fragmentierung** der IT-Sicherheitsvorschriften im Finanzsektor mit Überschneidungen und Unstimmigkeiten

Ziele:

- Erhöhung der IT- **Sicherheit und digitalen Betriebsstabilität** des gesamten europäischen Finanzsektors
- Schaffung **einheitlicher und konsistenter Anforderungen** für den gesamten Finanzsektor
- Einführung proportionaler Anforderungen **(Prinzip der Proportionalität)**

In Kraft seit 16. Januar 2023

✓ *Übergangsfrist, um die Anforderungen umzusetzen*
✓ *Konkretisierung durch die EU-Aufsichtsbehörden*

Anwendung ab 17. Januar 2025

DORA in der Regulierungslandschaft

Cybersicherheit Strategie

Gesetz über Cyber Security (CSA)

DORA

NIS2 Richtlinie

Gesetz über Cyber Resilience (CRA)

Banken

Governance, Risikomanagement und Outsourcing Anforderungen:

- EBA-Governance-Leitlinien;
- MaRisk (BaFiN);
- BAIT (BaFin);
- EBA Auslagerungsleitlinien
- EBA-Governance-Leitlinien
- …

DORA

- **Governance, Risikomanagement und Outsourcing Anforderungen** EU-weit in erhöhtem Maße harmonisiert durch unmittelbare Anwendbarkeit und erweiterten Anwendungsbereich
- Zusätzliche Befugnisse der EU-Aufsichtsbehörden, Abhängigkeiten der in der EU tätigen Finanzunternehmen von IKT-Drittdienstleistern umfassend zu erfassen und Risiken zu überwachen

Versicherungen

Governance, Risikomanagement und Outsourcing Anforderungen

- Solvabilität II-Richtlinie;
- MaGo (BaFiN);
- VAIT (BaFin);
- EIOPA Governance-Leitlinie
- EIPOA Cloud-Leitlinien
- …

Anwendungsbereich von DORA

Adressaten:

- **Finanzunternehmen** – weit und Finanzsektor übergreifend definiert; auszugsweise:

Kreditinstitute	Transaktionsregister	Handelsplätze
Zahlungsinstitute	Verwaltungs-gesellschaften	E-Geld-Institute
(Rück)Versicherer	Datenbereitstellung	Wertpapierfirmen
Krypto-Dienstleister	(Rück)Versicherungs-vermittler	Handelsplätze

- **Mittelbar: IKT-Drittdienstleister** (*Unternehmen, das IKT-Dienstleistungen anbietet*)

- Besondere Überwachungsbefugnisse in Bezug auf **Kritische IKT-Drittdienstleister**

IKT-Dienstleistungen (Art. 3 Nr. 21 DORA), weit definiert:

„sämtliche digitalen Dienste und Datendienste, die einem oder mehreren internen oder externen Nutzern dauerhaft über IKT-Systeme bereitgestellt werden, einschließlich der Bereitstellung von Hardware inklusive technischer Unterstützung mittels Software-Aktualisierungen“

Soft- und Hardware	Datendienste
Betrieb von IT	Cloud Services
IT-Projektmanagement	Betriebs-unterstützung

Grundprinzipien von DORA

Risikobasierter Ansatz (Art. 4 DORA)

→ Umsetzung von DORA-Anforderungen im Einklang mit dem **Grundsatz der Verhältnismäßigkeit** unter Berücksichtigung von

- **Größe und Art** des Finanzunternehmens
- **Umfang und Komplexität** (Risikoprofil) der Dienstleistungen, Tätigkeiten und Geschäfte des Finanzunternehmens umzusetzen

Gesamtverantwortlichkeit des Vorstandes (Art. 5 Abs. 2 DORA)

→ Eine vollständige Delegation der Verantwortung für das Management von IKT-Risiken scheidet aus

→ Überwachung der Genehmigungs- und Kontrollverfahren

→ Persönliche Sanktionen gegenüber **Mitgliedern des Vorstandes** möglich

Wesentliche Pflichten von Finanzunternehmen nach DORA

Risikomanagement

- → Governance und Organisation, insb. Einrichtung einer unabhängigen Kontrollfunktion
- → Etablieren eines IKT-Managementrahmens (insb. Strategien, Leitlinien, Prozesse, IT-Notfallpläne) zur IKT-Risikominimierung
- → Systeme, Protokolle und Tools auf dem neuesten Stand der Technik
- → Interne Revision und ständige Überwachung und Weiterentwicklung
- → Kommunikation

Management von Drittparteienrisiken

- → Informationsregister über alle Verträge mit IKT-Drittdienstleistern
- → Etablierung einer Strategie zum Management von Risiken durch IKT-Drittdienstleister
- → Auswahl- und Risiko-bewertungsverfahren ("Due Diligence") vor Vertragsschluss mit IKT-Drittdienstleistern einschließlich der „Lieferkette“
- → Mindestanforderungen an Vertragsinhalte

Meldepflichten

- → Einführung eines Managementrahmens zur Überwachung, Protokollierung und Meldung von IKT-bezogenen Vorfällen
- → Klassifizierung von IKT-bezogenen Vorfällen
- → Meldung von IKT-Vorfällen an Behörden und Kunden, welche als „schwerwiegend“ klassifiziert werden
- → Optional Meldung von erheblichen Cyber-Bedrohungen an Behörden und Kunden

Testen der digitalen operationalen Resilienz

Etablieren eines Programms zum Testen der digitalen Betriebsstabilität nach risikobasiertem Ansatz, z.B.

- → Schwachstellenscans
- → Quellcodetests
- → Performancetests
- → Überprüfungen physischer Sicherheit
- → Penetrationstests

Erweiterte Penetrationstests **(TLTP)** in Bezug auf Systeme, die kritische oder wichtige Funktionen unterstützen

Verpflichtende Bestimmungen in Verträgen mit IKT-Drittdienstleistern

Argumentation der EU-Kommission:

*Steigende **Abhängigkeit** der Finanzunternehmen von IKT-Dienstleistungen und Schwierigkeit, Verträge auszuhandeln, die das Aufsichtsrecht berücksichtigen*

Anforderungen an Vertragsinhalt nach DORA sind abhängig von der betroffenen Funktion:

Kritisch oder wichtig sind Funktionen, wenn ihr Ausfall eine erhebliche Beeinträchtigung

- der finanziellen Leistungsfähigkeit,
- der Geschäftsfortführung oder
- regulatorischer Art

darstellen würde

Thema	In allen Verträgen	Kritische/wichtige Funktionen
IT-Sicherheit	✓	**Erweitert**
Form, Vertragsaufbau und Vertragsänderungen	✓	✓
Leistungsbeschreibung und Service Levels	✓	**Erweitert**
Unterbeauftragung	✗	✓
Ort der Leistungserbringung und Datenverarbeitung	✓	✓
Datenschutz, Vertraulichkeit und Zugang zu Daten	✓	✓
IKT-Vorfälle	✓	✓
Kooperation mit Aufsichtsbehörden	✓	✓
Teilnahme an Schulungen des Finanzunternehmens	✓	✓
Kündigungsrechte und -fristen	✓	**Erweitert**
Berichtspflichten	✗	✓
Prüf- und Auditrechte	✗	✓
Notfallpläne und erweiterte IKT-Sicherheitsvorkehrungen	✗	✓
Exit-Pläne	✗	✓
Teilnahme an TLTP	✗	✓

Meldepflichten

IKT-bezogener Vorfall:

Nicht geplantes Ereignis, welches die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigt und nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf die vom Finanzunternehmen erbrachten Dienste hat

Kriterien für die Einstufung als „*schwerwiegend*“:

- Anzahl betroffener Kunden und Transaktionen
- Geografische Ausbreitung
- Auswirkung auf Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten
- Reputationsschädigende Auswirkungen
- Ausfallzeit
- Wirtschaftliche Auswirkungen für das Finanzunternehmen

Timeline for die Meldung an Behörden:

Erstmeldung
binnen 4 Stunden ab Klassifizierung als „schwerwiegend“, spätestens jedoch innerhalb von 24 Stunden ab Feststellung*

Zwischenmeldung
spätestens innerhalb von 72 Stunden ab Klassifizierung als „schwerwiegend“ oder sobald sich der Status verändert*

Abschlussmeldung
spätestens innerhalb von einem Monat nach der letzten Zwischenmeldung*

*Nach derzeitigem Stand des Entwurfes Regulatorischer Technischer Standards durch die Europäischen Aufsichtsbehörden [**nicht final**]

Aufsicht über Finanzunternehmen

Zuständige Behörden

- Besondere Aufsicht über kritische IKT-Drittdienstleister durch die sog. „federführende Überwachungsbehörde“
- Die bisher grundsätzlich für die Beaufsichtigung des Finanzunternehmens zuständige Behörde
- BaFin gegenüber Banken und Versicherungsunternehmen in Deutschland

Zusammenarbeit

- Zusammenarbeit der zuständigen Behörden in/mit NIS-Strukturen und -Einrichtungen (Cybersicherheit)
- Zusammenarbeit untereinander und, falls erforderlich, mit der sog. „federführenden Überwachungsbehörde“ und Austausch von Informationen über kritische Drittdienstleister
- Sektorenübergreifende Übungen, Kommunikation und Zusammenarbeit im Finanzsektor

Aufsichtsrechtliche Maßnahmen

Zuständige (nationale) Behörden müssen über **hinreichende Aufsichts-, Untersuchungs- und** Sanktionsbefugnisse verfügen, wobei sich der genaue Umfang aus nationalen Durchführungsregelungen ergeben wird und zumindest folgendes umfassen muss:

- Zugang zu **Dokumenten und Daten**
- **Vor-Ort-Inspektionen** und **Untersuchungen**
- Aufforderung zu **Korrektur- und Abhilfemaßnahmen**
- **Unterlassungsanordnung**
- **Bußgelder**
- Anforderung bestehender Aufzeichnungen von Datenübertragungen, die sich im Besitz eines **Telekommunikationsunternehmens** befinden (soweit nach nationalem Recht zulässig)
- **Öffentliche Bekanntgabe** von Verwaltungssanktionen

Mitgliedstaaten können auch **strafrechtliche Sanktionen** vorsehen

Ausblick

→ Finanzunternehmen müssen evaluieren,

- welche Anforderungen aus DORA sie ggf. **bereits umgesetzt** haben und
- welche weitergehenden Anforderungen sie, abhängig von ihrer jeweiligen Größe und genauen Tätigkeit (Risikobasierter Ansatz), **konkret umzusetzen haben**

→ Erheblich erweitert wurden – neben dem Anwendungsbereich von DORA – insbesondere die **Meldepflichten** und verpflichtend **mit IKT-Drittdienstleistern** zu vereinbarende **Vertragsinhalte**

→ Durch die deutliche Ausweitung des Anwendungsbereichs und der verpflichtend zu vereinbarenden Vertragsinhalte ist eine **Neu-/Nachverhandlung eines großen Teils der Verträge mit IKT-Drittdienstleistern notwendig**

→ Auch **IKT-Drittdienstleister** sollten sich vor diesem Hintergrund und vor dem Hintergrund der Aufsicht europäischer Behörden über **kritische IKT-Drittdienstleister** mit DORA-Anforderungen auseinandersetzen

Dringender Handlungsbedarf aufgrund der inzwischen zeitnahen Umsetzung der Vorgaben

Deutsche Stiftung für Recht und Informatik

Vielen Dank

Verena Reichstein
DLA Piper