Digital Operational Resilience Act (DORA)

Sicherstellung der digitalen Resilienz durch erhöhte Reaktionsfähigkeit

Januar 2023

Digitale Betriebsstabilität der EU-Finanzunternehmen
Die Verordnung der Europäischen Kommission verpflichtet Finanzunternehmen, den Aufsichtsbehörden und Marktteilnehmern im Falle größerer IT-bezogener Vorfälle unverzüglich und umfassend Bericht zu erstatten, damit das EU-Finanzsystem als Ganzes rasch und angemessen auf Störungen reagieren und die Resilienz des Systems aufrechterhalten kann.

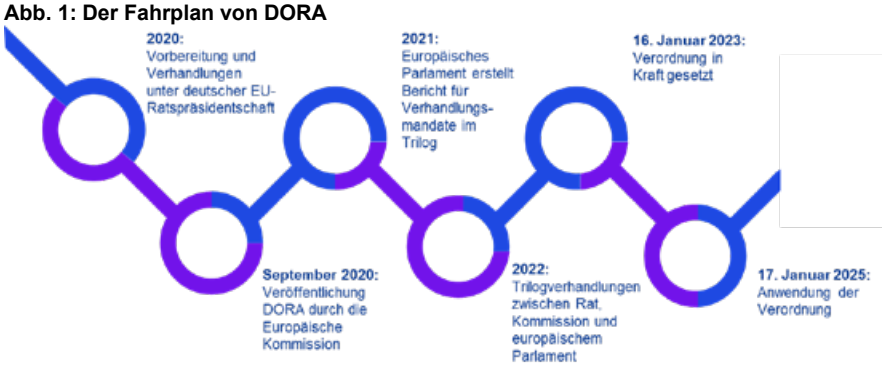
DORA – kurz erläutert

DORA ist Teil der Strategie für das digitale Finanzpaket der EU-Kommission zur Schaffung einer angemessenen Cyber-Sicherheit und Stärkung der Resilienz der Finanzunternehmen gegen Bedrohungen. Der Rat hat am 28. November 2022 den Rechtsakt zu DORA angenommen und am 27. Dezember 2022 im Amtsblatt veröffentlicht. Dadurch tritt dieser innerhalb von 20 Tagen in Kraft. Die Umsetzungsfrist für die Implementierung beträgt zwei Jahre.

Die schnelle und ursachenbezogene Erkennung größerer IT-bezogener Vorfälle soll die Grundlage für die wirksame Behandlung auftretender Finanzmarktbedrohungen bilden. Art und Umfang der Meldepflichten werden entsprechend zunehmen. Eine Voraussetzung für eine schnelle und ursachengerechte Meldung von IKT-Vorfällen (Informations- und Kommunikationstechnologie) ist unter anderem ein angemessenes und wirksames IKT-Risikomanagement.

Die nachfolgende Abbildung zeigt den Fahrplan der Inkraftsetzung bis zur verpflichtenden Anwendung:

Abb. 1: Der Fahrplan von DORA



Quelle: KPMG AG Wirtschaftsprüfungsgesellschaft, 2023

Geltungsbereich und Hintergrund

DORA wird unter anderem für Kreditinstitute, Versicherungsunternehmen, Vermögensverwalter sowie für IKT-Drittanbieter Anwendung finden.

DORA zielt auf die Vereinheitlichung bestehender europäischer sowie nationaler Standards und Vorgaben ab, um ein detailliertes und umfassendes Rahmenwerk für die digitale Betriebsstabilität von EU-Finanzunternehmen zu schaffen.

Der Vorschlag erweitert in diesem Zusammenhang bereits bestehende Vorschriften wie beispielsweise BAIT, VAIT und KAIT.

DORA – Anforderungen im Überblick

! Die Verordnung tritt am 16. Januar 2023 in Kraft und ist innerhalb von zwei Jahren bis zum 17. Januar 2025 umzusetzen.

Governance
DORA sieht die Gesamtverantwortung des Leitungsorgans für die digitale Betriebsstabilität als allumfassendes Prinzip vor.
Beispiel zur Umsetzung: Einheitliches Governance- und Kontrollrahmenwerk für die wirksame Steuerung aller IKT-Risiken.

IKT-Risikomanagement
DORA setzt ein ganzheitliches IKT-Risikomanagement-Rahmenwerk als Grundlage für resiliente Finanzunternehmen voraus.
Beispiel zur Umsetzung: Etablierung widerstandsfähiger IKT-Systeme mit Blick auf den gesamteuropäischen Wirtschaftsraum.

Schutz und Prävention
Um die Reaktionsfähigkeit zu erhöhen, spezifiziert DORA unter anderem Anforderungen an Prozesse und Systeme zur umgehenden Erkennung und Abwehr potenzieller Gefährdungen.
Beispiel zur Umsetzung: Automatische Netzwerkisolierung im Falle von Cyberangriffen.

Vertragsmanagement
DORA bestimmt Anforderungen an Verträge mit IKT-Drittparteien, die in das Vertragsmanagement der Finanzunternehmen Eingang finden müssen.
Beispiel zur Umsetzung: Kategorisierung der (Bestands)Verträge, Festlegung von Sollanforderungen, Gap-Analyse.

IKT-bezogene Vorfälle
DORA forciert eine Vereinheitlichung der Meldepflichten von schwerwiegenden IKT-Vorfällen auf die gesamte europäische Finanzwirtschaft.
Beispiel zur Umsetzung: Einheitliche Verfahren zur Überwachung, Klassifizierung und Meldung schwerwiegender IKT-Vorfälle an nationale/europäische Behörden.

Prüfung digitale Betriebsstabilität
Durch den risikobasierten Ansatz bei Tests werden kritische IT-Systeme auf ihre Betriebsstabilität und Absicherung in Bezug auf potenzielle IKT-Störungen regelmäßig überprüft.
Beispiel zur Umsetzung: Mindestens alle drei Jahre muss ein Penetrationstest an Live-Produktionssystemen erfolgen.

Steuerung IKT-Drittanbieter
Mit der Verordnung soll Finanzunternehmen eine solide Überwachung des Risikos durch IKT-Drittanbieter ermöglicht werden.
Beispiel zur Umsetzung: Überprüfung der Aufbau- und Ablauforganisation in der Dienstleistersteuerung inklusive Dokumentations- und Reportingvorgaben.

Versicherungsschutz für IKT-Risiken
DORA verändert etwa im Hinblick auf IKT-Drittrisiken die Anforderungen an Verantwortlichkeit und Haftungsrisiken der Unternehmen und Geschäftsleiter.
Beispiel zur Umsetzung: Überprüfung und ggf. Anpassung des Umfangs und der Bedingungen des Versicherungsschutzes (insb. Cyberversicherung und D&O-Versicherung)

Einige wesentliche Herausforderungen in der Umsetzung der Anforderungen

- Komplexität des einheitlichen IKT-Risikomanagement-Rahmenwerks und der Steuerung über die verschiedenen Disziplinen hinweg
- Ausweitung und Vereinheitlichung der Meldepflichten
- Erweiterte Anforderungen an das IKT-Drittpartei-Risikomanagement

Was können Finanzinstitute jetzt tun, um diesen Herausforderungen zu begegnen?

1. **Verstehen, dass ein neuer, einheitlicher Ansatz erforderlich ist.** Finanzinstitute werden Änderungen vornehmen müssen, um die neue Verordnung einhalten zu können. Weiterhin müssen die einheitlicheren Erwartungen der Aufsichtsbehörden in Bezug auf Risikomanagement, Kontrollen und Berichterstattung erfüllt werden. In einigen Fällen wird eine Umgestaltung der Betriebsmodelle erforderlich sein.

2. **Kennen des aktuellen Stands.** Finanzinstitute sollten ihre derzeitige Position bzw. ihren DORA-Reifegrad kennen. Ein erster Schritt besteht in der Erkennung von Lücken und der Mobilisierung von Ressourcen, welche für die Planung und Umsetzung einer erfolgreichen Umstellung erforderlich wären. Dies sollte unter Berücksichtigung anderer Vorhaben erfolgen, wie zum Beispiel von B/V/K/ZAIT-Projekten.

3. **Realistische Einschätzungen über mögliche Kosten.** Abhängig von der individuellen Ist-Situation der Finanzinstitute gehen zusätzliche DORA-Anforderungen mit erhöhten Investitionen und Ressourcenbelastungen einher. Künftige Rentabilitätsziele oder konkurrierende Projekte können einerseits beeinträchtigt werden, andererseits können neben der Herstellung der Compliance aber auch Chancen im Digitalisierungsfortschritt betrachtet werden.

4. **Ergreifung der Chance.** DORA ist keine reine Compliance-Anforderung. Durch die Vereinheitlichung der Regulierung bietet DORA Finanzinstituten die Möglichkeit, operative Risikokontrollkapazitäten – sofern relevant, auch international – zu bündeln. Gleichzeitig wird ein hohes Maß an operativer Bereitschaft und Widerstandsfähigkeit in der gesamten Organisation erreicht. Weitere Optimierungspotenziale für ein einheitliches IKT-Risikomanagement und dessen Steuerung über die Disziplinen hinweg kann Automatisierung bringen, beispielsweise durch die Nutzung von GRC- oder Vertragsmanagement-Tools.

Fazit

Zusammenfassend lässt sich sagen, dass DORA eine Antwort auf das immer komplexere technologische Umfeld ist, in dem sich Finanzunternehmen bewegen. Die Notwendigkeit für den europäischen Finanzmarkt, auf größere IT-Zwischenfälle vorbereitet zu sein und wirksam darauf reagieren zu können, ist größer denn je.

Unterstützung durch KPMG

Wir bieten **das fachliche Repertoire über alle relevanten DORA-Disziplinen**: Management-Beratung, ISM, IRM, BCM, Outsourcing und Cloud, Verständnis für Prozesse, Risiken und Kontrollen, rechtliche Anforderungen, Vertragsgestaltung sowie Governance-Strukturen

Wir kennen die Unternehmen der Financial-Services-Branche aufgrund zahlreicher, relevanter Projekterfahrungen **und können zusätzlich auf den Kenntnissen unseres Vorgehensmodells aufbauen**

KPMG hat direkten Zugriff auf **weltweite Expertise und Erfahrungen** aus dem KPMG-Netzwerk, welche sich speziell auf den Finanzsektor bezieht

Neben unserer fachlichen und methodischen Expertise bieten wir **Know-how für eine toolbasierte Umsetzung**, zum Beispiel zu marktüblichen GRC-Tools für ein effizientes Managen und Steuern der Risiken und Kontrollen oder Tools für ein effizientes Management von IKT-Drittanbietern und deren Verträge

Unser Vorgehen für eine DORA-Gap-Analyse

Mithilfe einer fünfphasigen Gap-Analyse werden Abweichungen zwischen der DORA und dem aktuellen Umsetzungsstand identifiziert. Dabei analysieren wir die bestehende schriftlich fixierte Ordnung, führen Workshops und Interviews mit den Themenverantwortlichen durch und überprüfen bei Bedarf den tatsächlichen Umsetzungsstand. Für die Ableitung der Gaps und Entwicklung der Maßnahmen werden relevante andere Compliance- oder Cyber-Projekte berücksichtigt. Als Ergebnis erhalten Sie einen Aktionsplan mit priorisierten Maßnahmenvorschlägen inklusive Roadmap und Aufwandsschätzung zur Schließung der Gaps.

Abb. 2: Die fünfphasige Gap-Analyse

Quelle: KPMG AG Wirtschaftsprüfungsgesellschaft, 2023

Kontakt

Gerne unterstützt Sie unser Team.

KPMG AG
Wirtschaftsprüfungsgesellschaft

Vaike Metzger
Partnerin, Financial Services
München
M +49 172 2895793
vmetzger@kpmg.com

Nadine Schmitz
Partnerin, Financial Services
Köln
M +49 174 3015 954
nschmitz@kpmg.com

Peter Hertlein
Director, Financial Services
Nürnberg
M +49 174 3060018
phertlein@kpmg.com

KPMG Law
Rechtsanwaltsgesellschaft mbH

Dr. Matthias Henke
Partner, Legal Financial Services
Düsseldorf/Frankfurt
M +49 174 9044502
mhenke@kpmg-law.com

Dr. Frank Püttgen
Senior Manager, Legal Financial Services
Köln
M +49 151 55109012
fpuettgen@kpmg-law.com

www.kpmg.de

www.kpmg.de/socialmedia