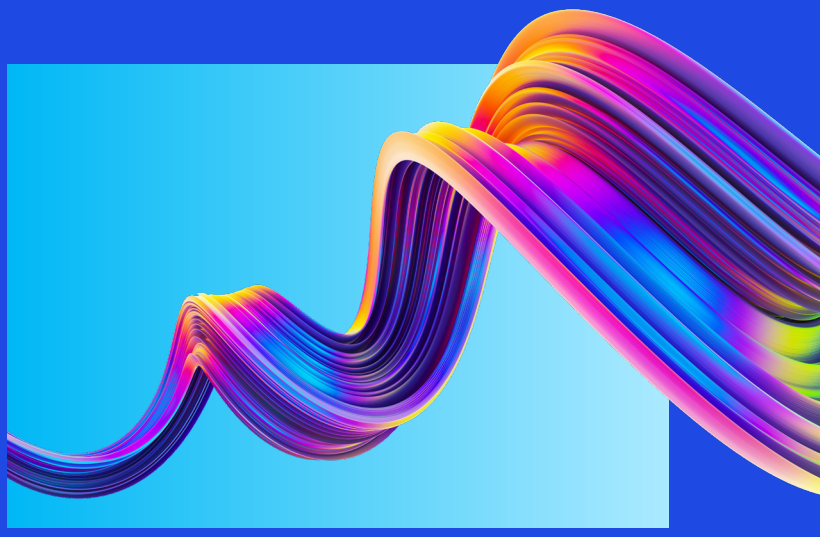
KPMG Law

Digital Operational Resilience Act (DORA)



Ausgangslage

Im Dezember 2022 wurde die Verordnung über die digitale operationale Resilienz im Finanzsektor („DORA") im Rahmen eines umfassenden Pakets zur Digitalisierung des Finanzsektors veröffentlicht und ist am 16. Januar 2023 in Kraft getreten. Die Verordnung sieht eine 24-monatige Umsetzungsfrist vor, wodurch DORA ab dem 17. Januar 2025 Anwendung findet.

Welche Unternehmen sind betroffen?

DORA betrifft Finanzunternehmen und Drittdienstleister von Informations- und Kommunikationstechnologien (IKT-Drittdienstleister). Der Begriff des Finanzunternehmens ist dabei weit auszulegen und ist nicht lediglich auf klassische Finanzdienstleister, wie Kreditinstitute, Zahlungsdienstleister oder Wertpapierfirmen beschränkt.

IKT-Dienstleister sind Anbieter von digitalen (Daten-) Diensten. Darunter fallen Cloud-Computing-Services, Softwareanbieter, Datenanalysedienste und Rechenzentren.

Was ist das Ziel von DORA?

Ziel von DORA ist die Harmonisierung der Vorschriften für IT-Systeme im Finanzsektor auf EU-Ebene, um ein detailliertes und umfassendes Rahmenwerk für die digitale Betriebsstabilität von EU-Finanzunternehmen zu schaffen.

Was ist zu tun?

DORA lässt sich in fünf Themenbereiche gliedern:

- IKT-Risikomanagement,
- IKT-Vorfälle und deren Meldung,
- Resilienz-Testungen,
- EU-Überwachungsrahmenwerk,
- IKT-Drittdienstleisterrisiken.

Auf allen Gebieten sollten Finanzdienstleister sich anpassen und ihre Beziehungen zu Drittdienstleistern überprüfen sowie die technischen Voraussetzungen erfüllen.

Die Herausforderung

Finanzunternehmen müssen nicht nur in technischer Hinsicht aufstocken, auch rechtlich gibt es Herausforderungen, die gemeistert werden sollten. Besondere Veränderungen ergeben sich dabei aus den Anforderungen in Kapitel V an Auslagerungsverträge zwischen Finanzunternehmen und IKT-Drittdienstleistern und in Kapitel II an die Governance und Organisation.

Auslagerungsverträge sollten angepasst werden

Anpassung bestehender Klauseln

Auslagerungsverträge mit IKT-Drittanbietern müssen künftig insbesondere die in Art. 30 DORA festgelegten wesentlichen Vertragsbestimmungen berücksichtigen. Dabei gelten die Vorgaben nach Art. 30 Abs. 2 DORA für sämtliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen, wohingegen Art. 30 Abs. 3 DORA Vertragsbestimmungen für IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktion normiert.

Die Vorgaben aus Art. 30 DORA entsprechen in weiten Teilen denjenigen Anforderungen an Auslagerungsverträge, die bereits durch AT 9 der MaRisk sowie die BaFin-Rundschreiben BAIT, KAIT, ZAIT und VAIT für jede Branche des Finanz- und Versicherungsmarktes bekannt sind. Ein erhöhter Anpassungsbedarf könnte sich jedenfalls für diejenigen Verträge ergeben, die den sonstigen Fremdbezug IT betreffen. Denn eine IKT-Dienstleistung nach DORA ist sehr weit zu verstehen und schließt eigentlich nur noch analoge Telefondienste aus.

Neue Vertragsbestimmungen

Nichtsdestotrotz werden durch DORA auch neue Vertragsbestimmungen eingeführt. So sieht zum Beispiel durch Art. 30 Abs. 2 i) DORA vor, dass vertragliche Vereinbarungen zukünftig auch Bedingungen für die Teilnahme von IKT-Drittdienstleistern an Programmen zur Sensibilisierung für IKT-Sicherheit oder Schulungen zur digitalen operationalen Resilienz umfassen. Im Falle der Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen sollen vertragliche Vereinbarungen nach Art. 30 Abs. 3 d) DORA die Verpflichtung des IKT-Drittdienstleisters enthalten, sich an bestimmten Tests des Finanzunternehmens zu beteiligen. Auch diesbezüglich müssen bestehende Auslagerungsverträge angepasst werden.

Weitere Anforderungen

Darüber hinaus können sich aus Art. 26, 28 und 29 DORA weitere Anforderungen an Verträge ergeben. Betroffen sind die Vereinbarung der Teilnahme an gebündelten Tests von IKT-Systemen, Kündigungsrechte und Übergangsregelungen sowie die Handhabung der Vergabe von Unteraufträgen.

Erhöhter Detaillierungsbedarf

Eine weitere Herausforderung ist der erhöhte Detaillierungsbedarf in den Auslagerungsverträgen. Zu denken ist etwa an eine mögliche Überprüfung und gegebenenfalls Anpassung von Meldepflichten, Vorgaben zum Informationsaustausch oder auch Regelungen zur Kostentragung bei Mitwirkungspflichten von IKT-Drittdienstleistern.

Zudem gilt es abzuwarten, zu verfolgen und zu berücksichtigen, wie sich die Aufsicht zu DORA positionieren wird und ob sich daraus gegebenenfalls ein weiterer Anpassungsbedarf für Auslagerungsverträge mit IKT-Drittdienstleistern ergibt. Bestehende oder sich anbahnende Auslagerungsverträge sollten deshalb schon jetzt einer gründlichen Analyse unterzogen werden, um die sich aus DORA ergebenden Anforderungen zu berücksichtigen und mögliche rechtliche Risiken auszuschließen.

Was jetzt zu tun ist

DORA findet ab dem 17. Januar 2025 Anwendung und die Anpassung der Verträge kostet erfahrungsgemäß Zeit. Unternehmen sollten daher jetzt mit der Umsetzung beginnen. Das ist zu tun:

- Bestehende Verträge mit IKT-Drittdienstleistern sollten auf die Anforderungen von DORA überprüft werden.
- Neu abzuschließende Verträge sollten jetzt schon den Anforderungen von DORA genügen und vor Abschluss dahingehenden analysiert werden.

Was wir Ihnen bieten können

Aufgrund unserer umfassenden Erfahrung im Bereich von Finanzdienstleistungen und den hiermit einhergehenden Herausforderungen, insbesondere der Implementierung neuer Vorgaben, sind wir ein verlässlicher Partner bei der Umsetzung der Vorgaben von DORA, insbesondere im Bereich der Governance und des Vertragsmanagements. Unsere Leistungen beziehen sich insbesondere auf das Entwerfen der neuen wesentlichen Vertragsbestimmungen sowie die Unterstützung bei deren Verhandlung mit den IKT-Dienstleistern. Zusätzlich könnten wir bei Bedarf bei entsprechenden Auseinandersetzungen mit Aufsichtsbehörden unterstützen.

Wir beraten Sie gerne ganzheitlich zu der Implementierung von DORA in Zusammenarbeit mit Expertinnen und Experten aus dem Bereich Financial Services der KPMG AG Wirtschaftsprüfungsgesellschaft. Diese verfügen über ein umfassendes fachliches Repertoire (nähere Informationen auf der Seite von KPMG), unter anderem in den Disziplinen Managementberatung, Information Security Management, Information Risk Management, Business Continuity Management, Outsourcing und Cloud-Lösungen.

Wir freuen uns auf Ihre Kontaktaufnahme.

Kontakt

KPMG Law Rechtsanwaltsgesellschaft mbH
THE SQUAIRE/Am Flughafen
60549 Frankfurt am Main

Dr. Andreas Wieland
Rechtsanwalt,
Partner,
T +49 69 951195848
awieland@kpmg-law.com

Dr. Christopher Peinemann
Rechtsanwalt,
Senior Manager,
T +49 69 951195875
cpeinemann@kpmg-law.com

www.kpmg-law.de

KPMG Law in den sozialen Netzwerken