Bereit für DORA? Diese Vertragsanpassungen sind notwendig

Mit der fortschreitenden Digitalisierung steigt auch das Risiko für Cyberangriffe im Finanzsektor. Um Marktteilnehmende zu schützen, hatte die EU im Dezember 2022 den Digital Operational Resilience Act (DORA) beschlossen. Er soll IKT-Risiken reduzieren (IKT= Informations- und Kommunikationstechnologien). Finanzunternehmen und andere Dienstleister müssen die Verordnung über die digitale operationale Resilienz im Finanzsektor, wie DORA auf Deutsch heißt, bis zum 17. Januar 2025 umgesetzt haben. DORA soll die operationale Resilienz und Sicherheit des Finanzsektors stärken und die Vorschriften für IT-Systeme im Finanzsektor auf EU-Ebene harmonisieren. Die Verordnung soll einen einheitlichen Rahmen für ein effektives Management von Cybersicherheits- und IKT-Risiken im Finanzsektor schaffen.

Die neuen Regeln sind bereits seit dem 16. Januar 2023 in Kraft. Da die Vorbereitungen für die Finanzunternehmen sehr aufwändig sind, ist die Umsetzungsfrist entsprechend lang.

DORA betrifft Finanzunternehmen und IKT-Drittanbieter

Beachten müssen den Digital Operational Resilience Act Finanzunternehmen und Drittdienstleister von Informations- und Kommunikationstechnologien (IKT-Drittdienstleister). Vom Begriff des Finanzunternehmens umfasst sind nicht nur klassische Finanzdienstleister wie Kreditinstitute, Zahlungsdienstleister oder Wertpapierfirmen, sondern beispielsweise auch Datenbereitstellungsdienste oder Ratingagenturen. Unter den Begriff des IKT-Drittdienstleisters fallen Anbieter von digitalen (Daten-) Diensten. Das sind vor allem Cloud-Computing- Services, Softwareanbieter, Datenanalysedienste und Rechenzentren.

Unternehmen sollten Auslagerungsverträge anpassen

Zur Umsetzung von DORA sollten Finanzunternehmen nicht nur technische Maßnahmen vornehmen, sondern auch ihre Verträge überprüfen. Denn IKT-Risiken ergeben sich nicht nur bei der Verwendung eigener Technologien, sondern auch bei Drittdienstleistern. Daher sieht DORA in Kapitel V auch Anforderungen für Auslagerungsverträge zwischen Finanzunternehmen und IKT-Drittdienstleistern vor.

Bestehende Klauseln müssen angepasst werden

Zunächst sollten Unternehmen bestehende Klauseln in Auslagerungsverträgen mit IKT-Drittanbietern überprüfen und anpassen. Art. 30 DORA legt wesentliche Vertragsbestimmungen für diese Verträge fest. Diese müssen künftig in sämtlichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen enthalten sein. Art. 30 Abs. 3 DORA normiert weitere Anforderungen an die Vertragsbestimmungen für IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen.

Die Anforderungen an Auslagerungsverträge gem. Art. 30 DORA entsprechen weitgehend den Vorgaben von AT 9 der MaRisk sowie denen der BaFin-Rundschreiben BAIT, KAIT, ZAIT und VAIT. Jedenfalls für Verträge, die den „sonstigen Fremdbezug IT“ betreffen, könnte sich ein erhöhter Anpassungsbedarf ergeben. Denn

IKT-Dienstleistungen nach DORA umfassen nahezu alle TK-Dienstleistungen außer analogen Telefondiensten.

DORA erfordert zusätzliche Vertragsbestimmungen

Neben der Anpassung bestehender Klauseln werden nach DORA auch neue Vertragsbestimmungen notwendig. Zum Beispiel müssen nach Art. 30 Abs. 2 i) DORA 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.

Für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen sind ebenfalls zusätzliche Klauseln in Auslagerungsverträgen vorgesehen: Vertragliche Vereinbarungen nach Art. 30 Abs. 3 d) DORA sollen IKT-Drittdienstleisters verpflichten, sich an bestimmten Tests des Finanzunternehmens zu beteiligen.

Weitere Anforderungen an Verträge ergeben sich aus Art. 26, 28 und 29 DORA. Dabei geht es beispielsweise um die Teilnahme an gebündelten Tests von IKT-Systemen, Kündigungsrechte und Übergangsregelungen sowie die Handhabung der Vergabe von Unteraufträgen.

Auslagerungsverträge sollen detaillierter werden

DORA schreibt außerdem vor, dass Auslagerungsverträgen detaillierter werden, insbesondere im Hinblick auf eine mögliche Überprüfung. Hier müssen gegebenenfalls Meldepflichten angepasst werden und Vorgaben zum Informationsaustausch oder auch Regelungen zur Kostentragung bei Mitwirkungspflichten von IKT-Drittdienstleistern aufgenommen werden.

Es bleibt abzuwarten, wie sich die Aufsicht zu DORA positionieren wird. Daraus könnte sich weiterer Anpassungsbedarf für Auslagerungsverträge mit IKT-Drittdienstleistern ergeben. Unternehmen sollten daher schon jetzt bestehende und sich anbahnende Auslagerungsverträge analysieren und ggf. auf die Bestimmungen von DORA anpassen, um kein Risiko einzugehen.

So sollten Finanzunternehmen jetzt handeln

Unternehmen müssen ihre Verträge bis zum 17. Januar 2025 angepasst haben, da DORA ab dann gilt. Die Anpassung kostet erfahrungsgemäß viel Zeit. Finanzunternehmen sollten daher so früh wie möglich mit der Umsetzung beginnen. Zum einen sollten sie bestehende Verträge mit IKT-Drittdienstleistern im Hinblick auf die Anforderungen von DORA überprüfen und ggf. anpassen. Bei neu abzuschließenden Verträgen sollten sie schon jetzt die Vorgaben von DORA berücksichtigen.

Je nach Größe des Vertragsportfolios empfehlen sich standardisierte und industrialisierte Ansätze zum Auslesen und Überprüfen der Verträge.

Der Digital Operational Resilience Act ist zwar mit viel Aufwand verbunden. Jedoch sind die Maßnahmen im

eigenen Interesse der Unternehmen, da sie das Risiko für Cyberangriffe reduzieren.

Weitere Informationen zur KI-unterstützten Vertragsanalyse von KPMG Law können Sie in unserem Flyer nachlesen.

Ansprechpartner:

Dr. Matthias Magnus Henke
Tel: +49 211 4155597362
mhenke@kpmg-law.com

Dr. Frank Püttgen
Tel: +49 221 2716891414
fpuettgen@kpmg-law.com

Dr. Christopher Peinemann, LL.M.
Tel: +49 69 951195-875
cpeinemann@kpmg-law.com