TaylorWessing

Digital Operational Resilience Act – DORA

Die Verordnung des europäischen Parlamentes und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors (Digital Operational Resilience Act – DORA) – ab 16.1.2023 in Kraft.

Anwendungsbereich von DORA

Die Digitalisierung des Finanzsektors durch den Einsatz von Informationstechnik (IT) schafft für Anbieter von Bank- und Finanzdienstleistungen zahlreiche neue Möglichkeiten, birgt für die Branche jedoch, angesichts der wachsenden Gefahr von Cyberangriffen, auch zahlreiche Risiken. In Zukunft wird mit dem sog. Digital Operational Resilience Act – („**DORA**") ein EU-weiter Rechtsrahmen für die digitale Widerstandsfähigkeit und Cybersicherheit im Finanzdienstleistungssektor zu beachten sein.

Was ist DORA?

Um die Stabilität des Finanzmarktes auch im Falle einer schwerwiegenden Störung zu gewährleisten und dessen Marktteilnehmer zu schützen, hat die EU-Kommission am 24. September 2020 den DORA-Regulationsentwurf im Rahmen eines umfassenden Pakets zur Digitalisierung des Finanzsektors (**Digital Finance Package**) vorgelegt, der auch die Digital Finance Strategy, die Retail Payment Strategy, einen Vorschlag zur Distributed-Ledger-Technologie (DLT) sowie den Act on Markets in Crypto Assets (MiCA) enthält.

Derzeit müssen sich Unternehmen des Finanz- und Versicherungssektors bei einem Einsatz von IT oder der Einbeziehung von IT-Dienstleistungen auf nationaler Ebene an eine Vielzahl aufsichtsrechtlicher Anforderungen mit Blick auf Cybersicherheit halten. In Deutschland zeigt sich dies etwa an den Vorgaben der BaFin-Rundschreiben BAIT, KAIT, ZAIT und VAIT, die für jede Branche des Finanz- und Versicherungsmarktes individuelle Regelungen aufstellen. Wir fangen hier in Deutschland also nicht bei Null an, sondern bauen auf einem Standard auf, der bereits seit Jahren im Fokus der Aufsicht steht und bereits eine gewisse Resilienz bewiesen hat.

Ziel von DORA ist die Harmonisierung der nationalen Vorschriften für die Sicherheit von IT-Systemen im Finanzsektor. Innerhalb der Europäischen Union soll so ein einheitlicher Rechtsakt über die digitale Betriebsstabilität von Finanzdienstleistungen entstehen. Bezweckt ist die Schaffung eines umfassenden Rahmens auf Ebene der Europäischen Union mit einheitlichen Vorschriften, die den Anforderungen an die digitale Betriebsstabilität von regulierten Unternehmen auf dem Finanzmarkt Rechnung tragen sowie die Schaffung eines gemeinsamen Aufsichtsrahmens für Drittanbieter von Informations- und Kommunikationstechnologien (**IKT**).

Wer ist von DORA betroffen?

DORA wird auf Finanzunternehmen und sog. IKT-Drittanbieter anwendbar sein. Unter einem IKT-Drittanbieter ist ein Unternehmen zu verstehen, welches digitale Dienste und Datendienste erbringt und schließt auch Anbieter von Cloud-Computing-Diensten, Software, Datenanalysediensten und Rechenzentren ein.

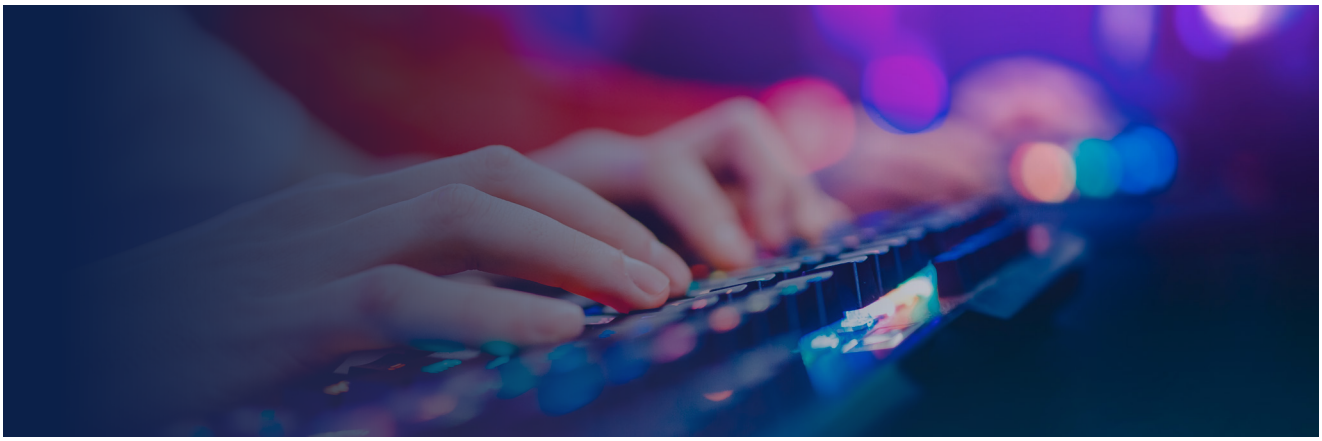
Welche Unternehmen unter die Sammelbezeichnung der Finanzunternehmen zu fassen sind, wird in Art. 2 Abs. 1 a) bis t) DORA aufgelistet. Demnach sind nicht nur Kreditinstitute, Zahlungsdienstleister, E-Geld-Institute und Wertpapierfirmen vom Anwendungsbereich von DORA umfasst, sondern beispielsweise auch Datenbereitstellungsdienste, Versicherungs- und Rückversicherungsunternehmen, Crowdfunding-Dienstleister, Ratingagenturen und Anbieter von Krypto-Dienstleistungen.

Der insgesamt sehr weite Anwendungsbereich von DORA soll nach dem Willen des europäischen Gesetzgebers für eine möglichst einheitliche Anwendung der gesetzlichen Verpflichtungen im Hinblick auf IKT-Risiken sorgen und letztlich gleiche Wettbewerbsbedingungen für die betroffenen Unternehmen schaffen.Die Verordnung des europäischen Parlamentes und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors (Digital Operational Resilience Act – DORA) – ab 16.1.2023 in Kraft.

Was sind die zentralen Verpflichtungen unter DORA?

Die neue Verordnung berücksichtigt, dass zwischen Finanzunternehmen in Bezug auf Größe, Unternehmensprofile oder das Ausmaß digitaler Risiken erhebliche Unterschiede bestehen. Aus diesem Grund verfolgt DORA einen risikobasierten Regulierungsansatz unter Beachtung der Verhältnismäßigkeit (sog. Proportionalitätsprinzip). Dies dient dazu, den weiten Anwendungsbereich von DORA zu korrigieren und sorgt dafür, dass je nach Größe des Unternehmens unterschiedliche Anforderungen gelten. Dadurch fallen auch Kleinstunternehmen nahezu gänzlich aus dem Anwendungsbereich von DORA heraus. DORA wurde zudem technologieneutral ausgestaltet, wodurch auch künftige technologische Entwicklungen auf dem Finanzmarkt erfasst werden sollen.

DORA sieht dabei eine Reihe von Handlungsfeldern vor, die entsprechenden Anpassungsaufwand auf Seiten der Finanzunternehmen nach sich ziehen. Diese sollen im inhaltlichen Überblick näher beleuchtet werden.



DORA - ein inhaltlicher Überblick

Nachdem wir uns im oberen Teil mit dem Anwendungsbereich von DORA beschäftigt haben, betrachten wir nun die inhaltlichen Regelungen der neuen europäischen Verordnung etwas genauer. Dieser Blogbeitrag beleuchtet fünf Handlungsfelder von DORA, die entsprechenden Anpassungsaufwand auf Seiten der betroffenen Finanzunternehmen nach sich ziehen werden.

Am 27. Dezember 2022 wurde die Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA) im Amtsblatt der Europäischen Union veröffentlicht. DORA tritt am zwanzigsten Tag nach der Veröffentlichung im Amtsblatt der Europäischen Union – und damit am 16. Januar 2023 – in Kraft und muss von den betroffenen Unternehmen nach einer Umsetzungsfrist von 24 Monaten nach der Veröffentlichung, folglich ab dem 17. Januar 2025 angewendet werden (Art. 64 DORA). Die Anforderungen

der DORA sind damit in allen EU-Mitgliedstaaten einheitlich. Hieran anknüpfend werden die Europäischen Aufsichtsbehörden (ESAs), die Europäische Bankenaufsichtsbehörde (EBA), die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) und die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA) zur Konkretisierung des Rechtsakts technische Standards (sog. Regulatory Technical Standards – RTS) ausarbeiten, die von den jeweiligen Unternehmen erfüllt werden müssen.

Betroffenen Unternehmen ist zu raten, den persönlichen Anwendungsbereich von DORA zu prüfen und sich mit den gesetzlichen Verpflichtungen bereits frühzeitig vertraut zu machen. DORA enthält fünf Themenbereiche, die im Folgenden zusammenfassend dargestellt und eingeordnet werden.

1. IKT-Risikomanagement

Wenig überraschend muss das Risikomanagement von regulierten Finanzmarktteilnehmern auch nach DORA künftig das IKT-Risiko umfassen. Das ist nach der MaRisk und den aufsichtsrechtlichen Vorgaben an die IT in BAIT, KAIT, ZAIT und VAIT keine neue Vorgabe. Allerdings sind die Vorgaben in DORA konkreter und nun auf Gesetzesebene verankert und nicht mehr nur in Verwaltungsvorschriften der BaFin.

Kapitel II von DORA enthält Vorschriften zum IKT-Risikomanagement von Finanzunternehmen. Ein Einsatz von IKT muss durch das Finanzunternehmen in die Unternehmensstrategie integriert werden. Die Gesamtverantwortung für das Risikomanagement liegt dabei grundsätzlich bei der Geschäftsleitung des jeweiligen Finanzunternehmens. Zudem werden mit DORA Verpflichtungen eingeführt, die sicherstellen sollen, dass IKT-Systeme kontinuierlich überwacht und kontrolliert werden, sowie durch regelmäßige Updates auf dem aktuellsten Stand gehalten werden. Um Ausfallzeiten von IKT-Systemen zu minimieren, müssen betroffene Unternehmen auch Strategien für Datensicherung und Wiederherstellungsverfahren einrichten. Sämtliche interne Risikodokumente müssen verschriftlicht sein, um entsprechend intern und extern überprüfbar zu sein.

2. Berichterstattung / Meldepflichten

DORA enthält zudem eine Verpflichtung zur Meldung von IKT-bezogenen Vorfällen. Nach Kapitel III von DORA werden Finanzunternehmen künftig verpflichtet sein, einen Managementprozess zur Überwachung und Protokollierung von IKT-bezogenen Vorfällen zu implementieren. Einen derartigen IKT-bezogenen Vorfall definiert die Verordnung als ein unvorhergesehenes in den Netz- und Informationssystemen festgestelltes Ereignis, das von böswilligen Handlungen herrühren kann und die Sicherheit von Netz- und Informationssystemen und der von diesen Systemen verarbeiteten, gespeicherten oder übertragenen Informationen beeinträchtigt oder nachteilige Auswirkungen auf die Verfügbarkeit, Vertraulichkeit, Kontinuität oder Authentizität der vom Finanzunternehmen erbrachten Finanzdienstleistungen hat (vgl. Art. 3 Nr. 6 DORA).

Finanzunternehmen müssen nach Art. 15 DORA Frühwarnindikatoren einrichten, um Cyberangriffe zu erkennen und zu bewältigen. Weiterhin schafft DORA einheitliche und standardisierte Vorgaben zum Vorgehen bei IT-Sicherheitsvorfällen. So beschreibt beispielsweise Art. 16 DORA ein Verfahren zur Klassifizierung, basierend auf Faktoren wie Dauer und Schwere des IKT-bezogenen Vorfalls auf die IKT-Systeme des Finanzunternehmens.

Schwerwiegende IKT-bezogene Vorfälle (vgl. Art. 3 Nr. 7 DORA) müssen durch das jeweilige Finanzunternehmen gemäß Art. 17 DORA der zuständigen Aufsichtsbehörde (vgl. Art. 41 DORA) gemeldet werden.

Bereits unter der derzeit geltenden Rechtslage bestehen Berichts- und Meldepflichten etwa durch die Zweite Zahlungsdiensterichtlinie (PSD II-Richtlinie) für Zahlungsdienstleister oder die Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie). Die DORA-Verordnung baut dabei auf der NIS-Richtlinie auf und beseitigt mögliche

Überschneidungen durch eine Ausnahme mittels des lex specialis Prinzips, sodass die Regelungen der DORA grundsätzlich Vorrang genießen sollten.

3. Prüfung der digitalen Betriebsstabilität durch Test-Verfahren

DORA schreibt weiterhin auch umfassende Verfahren zur Feststellung und Überprüfung der IT-Sicherheit mittels geeigneter Tests vor (Kapitel IV DORA). Dabei sind diese Prüfungen anhand des bereits erwähnen risikobasierten Ansatzes unter Berücksichtigung der Größe und Geschäfts- und Risikoprofile der jeweiligen Finanzunternehmen durchzuführen. Die DORA-Verordnung listet in Art. 22 Abs. 1 Beispiele geeigneter Tests auf, darunter Bewertungen und Überprüfungen der Anfälligkeit, Analysen von OpenSource-Software, Bewertungen der Netzsicherheit, Lückenanalysen, Analysen der physischen Sicherheit, Überprüfungen der physischen Sicherheit, Fragebögen und Scansoftwarelösungen, Quellcodeprüfungen, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests oder Penetrationstests.

Finanzunternehmen müssen mindestens einmal jährlich alle kritischen IKT-Systeme und IKT-Anwendungen prüfen. Diese Prüfungen können dabei sowohl durch externe als auch durch interne Prüfer durchgeführt werden (vgl. Art. 21 Abs. 4, 6 DORA).

Systemrelevante Institute hingegen werden höheren Anforderungen mit Blick auf die Prüfung ihrer IKT-Systeme unterworfen. DORA sieht für diese Institute erweiterte Prüfungen durch die Durchführung sog. bedrohungsorientierter Penetrationstests vor, wobei diese Tests in regelmäßigen Abständen mindestens alle drei Jahre durchzuführen sind.

4. IKT-Risiken Dritter / Outsourcing

Da Institute ihre IT häufig an große Technologieanbieter auslagern oder solche Anbieter für einzelne Dienstleistungen verwenden, werden Finanzinstitute deshalb im Rahmen ihres Risikomanagements verpflichtet, auch IKT-Drittparteienrisiken zu betrachten (Kapitel V DORA). So legt etwa Art. 27 DORA wesentliche Vertragsbestimmungen für Auslagerungsverträge fest. Derartige Verträge müssen z.B. eine Beschreibung aller Funktionen und Dienstleistungen des IKT-Drittanbieters, fortlaufende Überwachungsrechte des Finanzunternehmens oder auch Kündigungsrechte und Ausstiegsstrategien enthalten. Diese Vorgaben knüpfen nahtlos an das bestehende Auslagerungsregime für regulierte Finanzmarktteilnehmer an.

5. Europäisches Überwachungsrahmenwerk für kritische IKT Drittdienstleister

Besonders hervorzuheben ist der Aufbau eines europäischen Überwachungsregimes für kritische Technologieanbieter, die im Finanzsektor genutzt werden. Das ist auf europäischer Ebene neu, in Deutschland wurde eine entsprechende Kompetenz der BaFin bereits durch das Gesetz zur Stärkung der Finanzmarktintegrität (FISG) in § 25b Abs. 4a KWG eingeführt. Allerdings gehen die Befugnisse der BaFin beim Durchgriff auf das IT-Auslagerungsunternehmen nicht so weit, wie es DORA vorsieht. Nach § 25b KWG kann die BaFin im Einzelfall geeignete Anordnungen gegenüber IT-Auslagerungsunternehmen erlassen. Die aufsichtlichen Befugnisse bei der Überwachung der IKT-Drittanbieter nach Art. 33 DORA sind wesentlich detaillierter und weitgehender. Sie umfassen beispielsweise die Anforderung von Informationen und Unterlagen, Vor-Ort-Prüfungen oder auch die Verhängung von Zwangsgeldern, um den jeweiligen kritischen IKT-Drittanbieter zur Einhaltung der gesetzlichen Regelungen zu zwingen. Die neuen Befugnisse ermöglichen der BaFin eine umfassende Aufsicht der kritischen IKT-Drittanbieter.

Die Einstufung eines Technologieanbieters als kritischer IKT-Drittdienstleister und dessen Überwachung obliegt den ESAs. Dabei basiert die Ernennung auf festgelegten Kriterien, wie etwa:

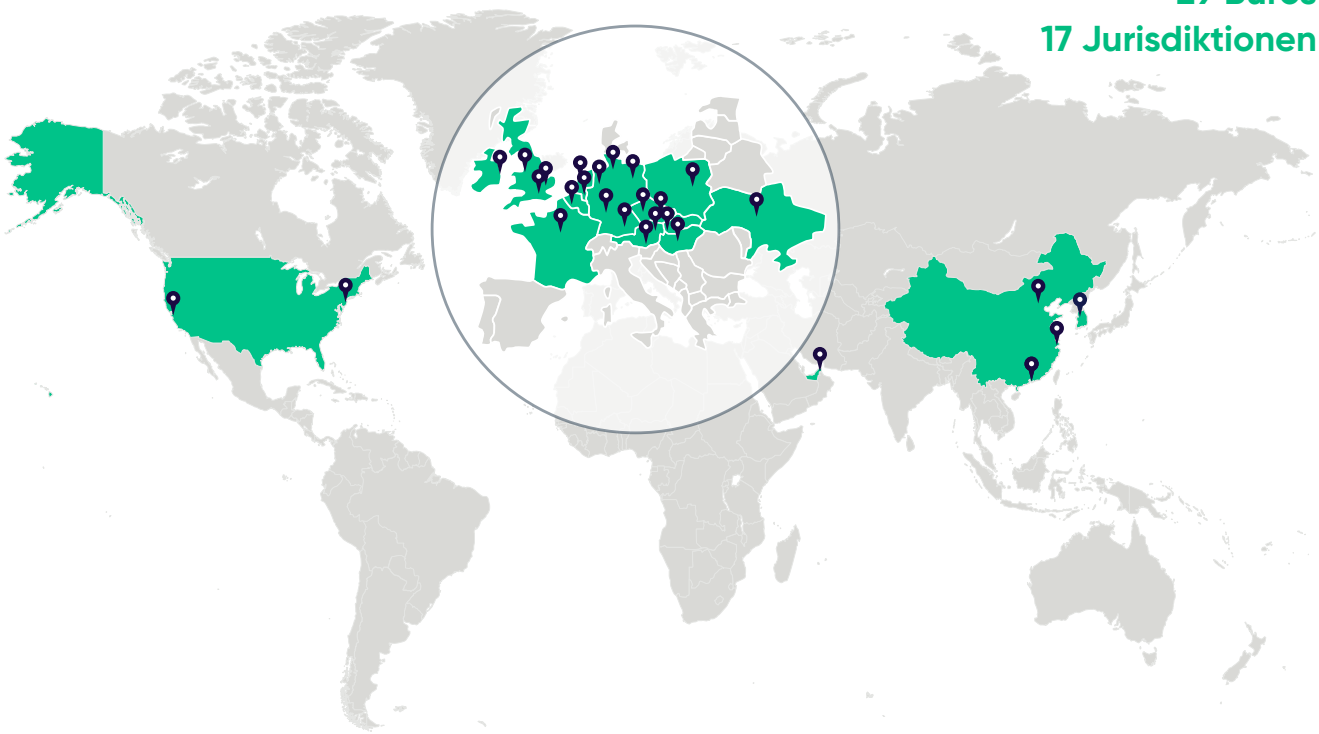
- Systemische Auswirkungen auf die Finanzdienstleistungen bei Defiziten der Stabilität, Kontinuität und Qualität der IKT-Leistungen
- Abhängigkeit von Finanzunternehmen von den Dienstleistungen des betreffenden IKT-Drittdienstleisters
- Grad der Substituierbarkeit des IKT-Drittanbieters
- Zahl der Mitgliedstaaten, welche die IKT-Leistungen nutzen

Zusammenfassung und Ausblick

Durch den umfassenden Anwendungsbereich von DORA werden Unternehmen aus zahlreichen Bereichen des Finanzsektors erfasst. Mit DORA wird ein Rechtsrahmen entstehen, der bestehende regulatorische Anforderungen an die IT-Sicherheit für die gesamte Finanzbranche zusammenfasst und einen europäisch einheitlichen Aufsichtsrahmen schafft.

Erstmals sind nun auch kritische IKT-Dienstleister, die als Auslagerungsunternehmen für regulierte Finanzmarktteilnehmer agieren, von der Regulierung umfasst.

1100+ Anwält:innen
300+ Partner:innen
29 Büros
17 Jurisdiktionen



Haben Sie Fragen? Wir helfen Ihnen gerne!

Ihre Ansprechpartnerin

Dr. Verena Ritter-Döring
Partner
+49 69 97130 0
v.ritter-doering@taylorwessing.com