Luther.

Newsflash | März 2024

Auf den Punkt.

Die Verordnung des Europäischen Parlaments und des Rates über die digitale operationale Resilienz im Finanzsektor (EU) 2022/2554 (Digital Operational Resilience Act; kurz **DORA**) ist bereits am **17. Januar 2023** in Kraft getreten. Das Ziel von DORA besteht in der Verbesserung der digitalen, operativen Widerstandsfähigkeit von EU-Finanzunternehmen, einschließlich IKT-Drittdienstleistern. Die Verordnung wurde unlängst als „Game Changer" bezeichnet, läutet sie doch einen Paradigmenwechsel im Finanzsektor ein: Mit DORA wurde erstmalig ein europaweit einheitlicher Rechtsrahmen (Single Rulebook) für ein effektives Risikomanagement von Cybersicherheits- und IKT-Risiken im Finanzsektor geschaffen, der zudem weitere Akteure – nämlich IKT-Drittdienstleister – in den Überwachungsrahmen der Europäischen Aufsicht einbezieht.

Die betroffenen Unternehmen haben nun bis zum **17. Januar 2025** Zeit, ihre Organisation, Prozesse und Systeme auf die Vorgaben von DORA einzurichten und umzustellen. In umfangreichen Abstimmungen werden derzeit die delegierten Verordnungen – sog. Level-2-Rechtsakte – der Europäischen Aufsichtsbehörden (EBA, EIOPA und ESMA, zusammen ESA) erarbeitet. Einzelne Regelungen der DORA werden durch technische Regulierungsstandards (Regulatory Technical Standards, RTS), technische Durchführungsstandards (Implementing Technical Standards, ITS) und Leitlinien (Guidelines) konkretisiert. Die ESA hat am 17. Januar 2024 die ersten finalen Entwürfe eines Teils der RTS und ITS veröffentlicht, die in den nächsten Monaten von der Europäischen Kommission zu verabschieden sind. Die finalen Entwürfe der zweiten Konsultationsrunde sollen am 17. Juli 2024 veröffentlicht werden.

Welche Unternehmen sind von DORA betroffen?

DORA gilt grundsätzlich für alle regulierten **Finanzunternehmen** in der EU (z.B. Kreditinstitute, Zahlungsinstitute, E-Geld-Institute, Wertpapierfirmen, Kontoinformationsdienstleister, Datenbereitstellungsdienste, Handelsplätze, Anbieter von Krypto-Dienstleistungen sowie Emittenten wertreferenzierter Token, Zentralverwahrer, Verwalter alternativer Investmentfonds und Verwaltungsgesellschaften, Versicherungs- und Rückversicherungsunternehmen, Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, Einrichtungen der betrieblichen Altersversor-

gung (EbAV), Ratingagenturen, Schwarmfinanzierungsdienstleister). Daneben werden insbesondere aber auch die **IKT-Drittdienstleister** in den Anwendungsbereich von DORA einbezogen.

Für Finanzunternehmen gilt der Grundsatz der Verhältnismäßigkeit (Proportionalität), so dass bei der Umsetzung der DORA-Anforderungen unter anderem Größe und Gesamtrisikoprofil des Unternehmens sowie Art, Umfang und Komplexität der Dienstleistungen zu beachten sind. Nach Aussage der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) betrifft DORA Schätzungen zufolge ca. 20.000 Finanzunternehmen in Europa und hat damit auch enorme Auswirkungen auf den Markt der IKT-Drittdienstleister.

Was ändert sich für Finanzunternehmen?

DORA stellt umfassende Anforderungen an Finanzunternehmen und deren Leitungsorgane mit dem Fokus auf das IKT-Risikomanagement, den Umgang mit IKT-bezogenen Vorfällen, dem Testen der digitalen operationalen Resilienz und dem Management des IKT-Drittparteirisikos.

Als Teil des **IKT-Risikomanagements** sind die Finanzunternehmen verpflichtet, einen internen **Governance- und Kontrollrahmen** (insbesondere Strategien, Leitlinien und Richtlinien, Verfahren sowie IKT-Protokolle) zur Gewährleistung eines umsichtigen Managements von IKT-Risiken zu implementieren. Die zentralen Elemente sind die Identifizierung, Klassifizierung und Dokumentation kritischer Funktionen, die Einrichtung von Schutz- und Präventionsmaßnahmen zur Überwachung aller Quellen von IKT-Risiken und damit zusammenhängend die Weiterentwicklung und Kommunikation. Dem zuständigen Leitungsorgan des Unternehmens kommt dabei eine herausragende Rolle zu, denn es trägt die Letztverantwortung für das Management der IKT-Risiken des Finanzunternehmens und die Gesamtverantwortung für die Festlegung und Genehmigung der Strategie für die digitale operationale Resilienz sowie für die Zuweisung angemessener Budgetmittel für den IKT-Risikomanagementrahmen. DORA erstreckt sich explizit auf die IKT-bezogene physische Infrastruktur (unter anderem Computer-Hardware, Server, relevante Räumlichkeiten, Rechenzentren etc.). Der IKT-Risikomanagementrahmen muss mindestens einmal jährlich überprüft und entsprechend gewonnener Erkenntnisse angepasst werden. Aus diesem Grund schließt sich an die Kontrollen ein Follow-up-Verfahren an, das die Beseitigung aufgefundener Probleme sicherstellen soll.

Ein weiterer Baustein der DORA ist das **Management von IKT-bezogenen Vorfällen**, welches die Überwachung, Protokollierung und gegebenenfalls Meldung von IKT-bezogenen Vorfällen umfasst. IKT-bezogene Vorfälle beeinträchtigen die Sicherheit der Netzwerk- und Informationssysteme und haben nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf die vom Finanzunternehmen erbrachten Dienstleistungen. DORA legt Kriterien fest, ab welcher Intensität ein solcher Vorfall zu melden ist. Die Berichterstattung hat über die von der ESA entwickelten Standardvorlagen zu erfolgen. Durch verpflichtende Berichte sind Kunden und Nutzer der Finanzunternehmen über Vorfälle und deren Auswirkungen zu informieren.

Das **Testen der digitalen operationale Resilienz** einschließlich Threat-Led Penetration Testing (TLPT) ist ein weiterer Teil des IKT-Risikomanagementrahmens. Die Tests sollen umfassen: Bewertungen und Überprüfungen der Anfälligkeit, Analysen von Open-Source-Software, Bewertungen der Netzsicherheit, Lückenanalysen, Analysen der physischen Sicherheit, Fragebögen und Scansoftwarelösungen, Quellcodeprüfungen und, soweit durchführbar, szenariobasierte Tests und Kompatibilitätstests.

Ausgewählte Finanzunternehmen müssen erweiterte Tests auf Basis von TLPT vornehmen. Kriterien für die Bestimmung dieser Finanzunternehmen sind die Relevanz der Dienstleistungen für den gesamten Finanzsektor, die Bedenken hinsichtlich der Finanzstabilität einschließlich des systemischen Charakters des Finanzunternehmens, das individuelle IKT-Risikoprofil sowie der IKT-Reifegrad des Finanzunternehmens. Der vorliegende Entwurf der RTS zu TLPTs soll im Juli 2024 an die Europäische Kommission übermittelt werden. Die BaFin hat bereits angekündigt, die beaufsichtigten Institute und Unternehmen möglichst frühzeitig zu informieren.

Von den Finanzunternehmen verlangt DORA weiterhin das **Management der IKT-Drittparteirisiken** – und zwar während des gesamten Lebenszyklus des Bezugs. Voraussetzung hierfür ist, dass vor Vertragsabschluss bzw. -anpassung eine Risikoanalyse und Due Diligence stattfinden. Dabei sollen die Finanzunternehmen unter anderem berücksichtigen, wie abhängig sie von dem jeweiligen IKT-Drittdienstleister sind, und welche Risiken aus der Vertragsbeziehung entstehen könnten. Zu den vertraglichen Bestimmungen formuliert DORA Mindestanforderungen, über die sich das Finanzunternehmen und der IKT-Drittdienstleister frühzeitig verständigen müssen, auch weil Finanzunternehmen verpflichtet werden,

die Parameter ihrer IKT-Vertragsbeziehungen in ein Informationsregister einzutragen. Dieses Informationsregister soll es erlauben, die IKT-Drittparteirisiken zu managen und sogenannte kritische IKT-Drittdienstleister bestimmen zu können.

Was müssen IKT-Dienstleistungsverträge regeln?

Die Verträge mit IKT-Drittdienstleistern müssen in Zukunft eine Reihe neuer Regelungen beinhalten. Dazu gehören im Einzelnen: eine vollständige Leistungsbeschreibung mit quantitativen und qualitativen Leistungszielen, einschlägige Bestimmungen über Zugänglichkeit, Verfügbarkeit, Integrität, Sicherheit und Schutz personenbezogener Daten sowie Garantien für den Zugang, die Wiederherstellung und die Rückgabe bei Ausfall von IKT-Drittdienstleistern, Kündigungsfristen und Berichtspflichten der IKT-Drittdienstleister, Zugangsrechte, Kontroll- und Prüfstrategien des Finanzunternehmens oder eines beauftragten Dritten sowie unmissverständliche Kündigungsrechte und gegebenenfalls spezielle Ausstiegsstrategien. DORA sieht vor, dass hierzu Standardvertragsklauseln entwickelt werden. Es ist aber frühestens im Laufe des Jahres 2025 ein Ergebnis zu erwarten. Voraussetzungen bei Nutzung von Zertifikaten und Prüfberichten Dritter und Vorgaben für die Form bei Änderungen werden eingeführt.

Welche Besonderheiten gelten für die Unterstützung kritischer und wichtiger Funktionen?

Die RTS zur Leitlinie zum Management des IKT-Drittparteirisikos konkretisiert, wann von einer Nutzung von IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen und von IKT-Drittdienstleistern erbracht werden, auszugehen ist. Berücksichtigt werden die folgenden Kriterien: die Art der IKT-Dienstleistungen, der Standort des IKT-Drittdienstleisters oder seiner Muttergesellschaft sowie der Ort der Leistungserbringung und Datenverarbeitung, die Art der mit den IKT-Drittdienstleistern ausgetauschten Daten, Zugehörigkeit des IKT-Dienstleisters zur Gruppe des Finanzinstituts sowie der Aufsichtsrahmen des IKT-Drittdienstleisters. Ergibt die Risikoanalyse eines Finanzunternehmens, dass der IKT-Drittdienstleister kritische oder wichtige Funktionen unterstützt, verschärfen sich die regulatorischen Anforderungen an die Mindestinhalte der Verträge zwischen den Parteien. Leistungen, die bisher als (regulatorisch) eher unkritischer bloßer Fremdbezug von IKT-Dienstleistungen zu qualifizieren sind (und nicht als Auslagerung), können unter DORA sehr wohl als kritisch und wichtig zu validieren sein.

Was bedeutet DORA für sogenannte kritische IKT-Drittdienstleister?

Künftig als kritisch eingestufte IKT-Drittdienstleister werden von den Europäischen Aufsichtsbehörden überwacht, weil die von ihnen angebotenen Dienstleistungen nicht oder nur sehr schwer kurzfristig von anderen Dienstleistern übernommen werden könnten, oder sie die Stabilität des Finanzsystems beeinflussen könnten. Die Europäischen Aufsichtsbehörden können ab Januar 2025 von kritischen IKT-Drittdienstleistern Informationen anfordern, allgemeine Untersuchungen und (Vor-Ort-) Prüfungen durchführen, Empfehlungen zu Geschäftsbedingungen und zur Unterbeauftragung sowie Sicherheitsempfehlungen aussprechen (z.B. bezüglich Patching, Updates, Verschlüsselung). Sie können öffentlich bekanntgeben, dass ein beaufsichtigtes Unternehmen diese Empfehlungen nicht einhält, und dass Sanktionen verhängt wurden. Als ultimative Maßnahme wird es nationalen Aufsichtsbehörden möglich sein, die Nutzung oder den Einsatz von Diensten auszusetzen oder die Dienste zu kündigen. Die Europäischen Aufsichtsbehörden haben bereits Kriterien zur Bestimmung der Kritikalität erarbeitet, und die EU-Kommission wird die finalen Kriterien in einem delegierten Rechtsakt veröffentlichen. Ein ausschlaggebendes Kriterium wird die Frage sein, welche systemischen Auswirkungen auf die Stabilität, Kontinuität oder Qualität der Erbringung von Finanzdienstleistungen zu erwarten wären, wenn der betreffende IKT-Drittdienstleister einer umfassenden Betriebsstörung unterliegt.

Wie werden die kritischen IKT-Drittdienstleister bestimmt?

Die Europäischen Aufsichtsbehörden nehmen über den Gemeinsamen Ausschuss und auf Empfehlung des Überwachungsforums die Einstufung der IKT-Drittdienstleister, die für Finanzunternehmen kritisch sind, vor. Die Europäische Kommission hat in der delegierten Verordnung vom 22. Februar 2024 die Kriterien für die Einstufung von IKT-Drittdienstleistern als kritisch präzisiert. Mit Unterkriterien und Schwellenwerten werden die systemischen Auswirkungen eines Ausfalls dieses IKT-Drittdienstleisters für das jeweilige Finanzunternehmen, die systemische Bedeutung der Finanzunternehmen, die diesen IKT-Drittdienstleister nutzen, unter Berücksichtigung der systemrelevanten, diesen IKT-Dritt-

dienstleister auch nutzenden Institute sowie systemrelevanten Finanzunternehmen und der Grad der Substituierbarkeit in zwei Stufen, einer quantitativen und einer qualitativen Stufe, bestimmt, wobei die Kritikalität der unterstützten Funktionen allein und zusätzlich in „Stufe 2“ berücksichtigt wird. So gilt bei einem IKT-Drittdienstleister das Unterkriterium der „Stufe 1“ der systemischen Auswirkungen auf die Stabilität, Kontinuität und Qualität der Erbringung von Finanzdienstleistungen als erfüllt, wenn der Anteil eines IKT-Drittdienstleisters an der Dienstleistungserbringung bezogen auf die Gesamtanzahl und die Gesamtvermögenswerte bei mindestens einer der in den DORA-Anwendungsbereich fallenden Kategorien von Finanzunternehmen mindestens 10 % beträgt. Das Unterkriterium der fehlenden Substituierbarkeit wird in „Stufe 1“ ebenfalls als erfüllt angesehen, wenn der Anteil der Finanzunternehmen, für die kein alternativer IKT-Drittdienstleister verfügbar ist, oder für die eine Migration der Dienste höchst schwierig ist, gemessen an der Gesamtanzahl der Finanzunternehmen in dieser Kategorie 10 % überschreitet.

Was ist zu tun? Warum kann man nicht warten?

Die Finanzunternehmen und die IKT-Drittdienstleister stehen nun vor dem entscheidenden Schritt, die erforderlichen Umsetzungsmaßnahmen zu identifizieren und eine Strategie zu entwickeln, um die Einhaltung der DORA-Vorschriften bis zum Stichtag **17. Januar 2025** zu erreichen. Die nachfolgenden Handlungsempfehlungen sollen dabei unterstützen:

1. Der initiale Schritt im Transformationsprozess ist für das Finanzunternehmen wie für IKT-Drittdienstleister eine **Positionsbestimmung** zur Anwendbarkeit von DORA auf die eigenen Geschäftsaktivitäten.

2. Sodann ist für Finanzunternehmen eine **Gap-Analyse** erforderlich zur Identifizierung des Handlungsbedarfs in den von DORA betroffenen Bereichen Governance, IKT-Risikomanagement, Testing, IKT-Berichterstattung und Risikomanagement von IKT-Drittdienstleistern. Im Rahmen der Gap-Analyse ist einerseits das durch DORA adressierte Proportionalitätsprinzip sowie andererseits der Status des Finanzunternehmens im Hinblick auf die Compliance seiner Organisation und Prozesse mit der bestehenden Regulierung im Bereich der IKT-Auslagerung (z.B. BAIT, ZAIT, VAIT, KAIT) zu berücksichtigen.

3. Ein zentraler Baustein von DORA ist das **Management der IKT-Drittparteirisiken**: Für Finanzunternehmen und IKT-Drittdienstleister gleichermaßen wichtig und im Hinblick darauf, dass DORA keine Übergangsfristen vorsieht, enorm zeitkritisch ist die Anpassung der Verträge an die Mindestanforderungen von DORA. In diesem Kontext ist initial zu klären, ob der IKT-Dienstleister kritische und wichtige Funktionen unterstützt. Diese Risikoanalyse ist frühzeitig zu initiieren, da sie maßgeblich für den Detaillierungsgrad der Vertragsgestaltung und daran anknüpfend die sowohl beim Finanzunternehmen als auch beim IKT-Drittdienstleister zu implementierenden Prozesse ist.

4. IKT-Drittdienstleister haben auf Basis der vorzunehmenden Positionsbestimmung und Risikoanalyse im Wege einer eigenen Gap-Analyse zu ermitteln, welcher Änderungsbedarf sich für ihre Geschäftsabläufe aus den geänderten Anforderungen für die Finanzunternehmen, aus den vertraglichen Zusagen sowie aus der Überwachung durch die Europäischen Aufsichtsbehörden im Übrigen ergibt.

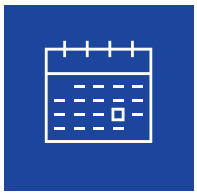
5. Aus den Ergebnissen der Gap-Analyse sind die abgeleiteten To-dos zu priorisieren und die **Transformation** in den betroffenen Geschäftsfeldern zu initiieren. Die Umsetzung von DORA kann hierbei nur interdisziplinär unter Einbindung informationstechnischer, rechtlicher und organisatorisch-prozessualer Kompetenzen erfolgen.

Ihre Kontakte:

Nicole Bittlingmayer
Rechtsanwältin, Partnerin
Frankfurt a.M.
T +49 69 27229 24710
nicole.bittlingmayer@luther-lawfirm.com

Dr. Stefanie Hellmich, LL.M.
Rechtsanwältin, Partnerin
Frankfurt a.M.
T +49 69 27229 24118
stefanie.hellmich@luther-lawfirm.com

Veranstaltungen, Veröffentlichungen und Blog



Eine Übersicht mit unseren Veranstaltungen finden Sie hier.

Eine Liste unserer aktuellen Veröffentlichungen finden Sie hier.

Unseren Blog finden Sie hier.

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Nicole Bittlingmayer
Luther Rechtsanwaltsgesellschaft mbH
An der Welle 10, 60322 Frankfurt a.M., T: +49 69 27229 0
nicole.bittlingmayer@luther-lawfirm.com

Bildnachweis: ipopba/AdobeStock: Seite 1; Olaf Hermann, Jörg Modrow, Frank Eidel: Seite 2

Haftungsausschluss

Obgleich dieser Newsletter sorgfältig erstellt wurde, wird keine Haftung für Fehler oder Auslassungen übernommen. Die Informationen dieses Newsletters stellen keinen anwaltlichen oder steuerlichen Rechtsrat dar und ersetzen keine auf den Einzelfall bezogene anwaltliche oder steuerliche Beratung. Hierfür stehen unsere Ansprechpartner an den einzelnen Standorten zur Verfügung.

Stand: März 2024