KLEYR GRASSO

Independent law firm

26/05/2023

Digital Operational Resilience Act (DORA)

Am 27. Dezember 2022 wurde im Amtsblatt der Europäischen Union die Verordnung (EU) 2022/2554 (die „**Verordnung**“) über die digitale operationelle Resistenz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 veröffentlicht.

Die Verordnung, die auch als Digital Operational Resilience Act („**DORA**“) bekannt ist, trat am 17. Januar 2023 in Kraft, zielt insbesondere auf eine Harmonisierung der Vorschriften zur digitalen operationellen Widerstandsfähigkeit im Finanzsektor innerhalb der Europäischen Union ab und sieht eine Implementierungsfrist von 24 Monaten, d.h. bis zum 17. Januar 2025 vor. Parallel hierzu wurde die Richtlinie (EU) 2022/2556 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 hinsichtlich der digitalen operationalen Resilienz im Finanzsektor („**Richtlinie**“) veröffentlicht. Diese bestimmt ebenfalls den 17. Januar 2025 als Stichtag, d.h. dass bezogen auf die Richtlinie die Mitgliedstaaten spätestens bis zu diesem Tag die erforderlichen Maßnahmen veröffentlichen und ab diesem Tag anwenden müssen.

DORA wurde erforderlich, da die weiterschreitende Digitalisierung und Vernetzung einerseits die Wettbewerbsfähigkeit der europäischen Unternehmen, einschließlich derer des Finanzsektors, sichert und verbessert, dieser aber andererseits auch erhebliche Risiken wie Cyberbedrohungen oder Informations- und Kommunikationstechnologie (IKT)-Störungen gegenüberstehen. Diese bereits seit geraumer Zeit bekannten Risiken haben aufgrund rezenter Entwicklungen in den letzten Jahren jedoch erheblich an Bedeutung gewonnen. Anzuführen sind hier die in der Presse umfänglich thematisierten Cyberangriffe auf Unternehmen sowie Behörden aber auch die Ausweitung des Homeoffice und die rasch fortschreitende Digitalisierung der Wirtschaft. Um diesen Risiken entgegen zu treten, wurde nun durch DORA ein einheitlicher und verbindlicher Rahmen für den Binnenmarkt geschaffen. Von Bedeutung für die effektive Implementierung werden jedoch naturgemäß über DORA und die Richtlinie hinaus, auch die delegierten Rechtsakte, die Leitlinien der Aufsichtsbehörden und die technischen Regulierungs- sowie Durchführungsstandards sein.

DORA richtet sich an die in Art. 2 (1) der Verordnung aufgeführten Unternehmen. Hierunter fallen u.a. Kreditinstitute, Zahlungsinstitute, Wertpapierfirmen, Verwalter alternativer Investmentfonds, Verwaltungsgesellschaften, Versicherungs- und Rückversicherungsunternehmen sowie IKT-Drittdienstleister („**Finanzunternehmen**“). Nach DORA sind IKT-Drittdienstleister Unternehmen die IKT-Dienstleistungen bereitstellen, d.h digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienst.

Die Verordnung gilt nach dessen Art. 2 (3) jedoch ausdrücklich nicht für eine Reihe von Unternehmen, von denen die Verwalter alternativer Investmentfonds im Sinne von Artikel 3 Absatz 2 der Richtlinie 2011/61/EU, d.h. die „lediglich“ registrierten AIFM hervorzuheben sind.

DORA besteht aus 5 für die Finanzunternehmen relevanten Grundpfeilern:

> IKT-Risikomanagement (Kapitel II, Art. 5 ff. der Verordnung)
> Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle (Kapitel III, Art. 17 ff. der Verordnung)
> Testen der digitalen operationalen Resilienz (Kapitel IV, Art. 24 ff. der Verordnung)
> Management des IKT-Drittparteienrisikos (Kapitel V, Art. 28 ff. der Verordnung)
> Vereinbarungen über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen (Kapitel VI, Art. 45 der Verordnung).

Auch DORA misst der Größe der Finanzunternehmen und der Bürde, die zusätzliche Anforderungen darstellen können, die erforderliche Bedeutung bei und verankert das Prinzip der Verhältnismäßigkeit in Art. 4. der Verordnung. Daher wenden die Finanzunternehmen die in Kapitel II festgelegten Vorschriften im Einklang mit dem Grundsatz der Verhältnismäßigkeit an, wobei ihrer Größe und ihrem Gesamtrisikoprofil sowie der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte Rechnung zu tragen ist. Darüber hinaus muss die Anwendung der Kapitel III und IV sowie des Kapitels V Abschnitt I durch die Finanzunternehmen in einem angemessenen Verhältnis zu ihrer Größe und ihrem Gesamtrisikoprofil sowie zu der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte stehen, wie dies in den einschlägigen

Vorschriften jener Kapitel ausdrücklich vorgesehen ist.

IKT-Risikomanagement

Finanzunternehmen müssen einen internen Governance- und Kontrollrahmen schaffen, der ein wirksames und umsichtiges Management von IKT-Risiken gewährleistet wobei das Leitungsorgan alle Vorkehrungen im Zusammenhang mit dem IKT-Managementrahmen definieren, genehmigen und überwachen muss, für die Umsetzung verantwortlich ist und die letztendliche Verantwortung für das Management der IKT-Risiken des Finanzunternehmens trägt. Es bedarf daher eines soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen, der Teil des Gesamtrisikomanagementsystems der Finanzunternehmen ist und es diesen ermöglicht, IKT-Risiken schnell, effizient und umfassend anzugehen und ein hohes Niveau an digitaler operationaler Resilienz zu gewährleisten. Die Finanzunternehmen müssen daher auch ihre zu Zwecken der Minimierung der IKT-Risiken und der hierfür eingesetzten IKT-Systeme, -Protokolle und –Tools stets auf dem neuesten Stand halten. Die Finanzunternehmen treffen neben einem angemessenen Schutz der IKT-Systeme auch Vorkehrungen im Hinblick auf Gegenmaßnahmen. Finanzunternehmen müssen Mechanismen schaffen, die es ermöglichen Probleme bei der Leistung von IKT-Netzwerken und IKT-bezogene Vorfälle, umgehend zu erkennen und potenzielle einzelne wesentliche Schwachstellen zu ermitteln. Es gilt überdies Richtlinien und Verfahren für die Datensicherung aufzustellen, sowie Wiedergewinnungs- und Wiederherstellungsverfahren und –methoden zu erstellen. Auf Anfrage muss der IKT-Risikomanagementrahmen der CSSF vorgelegt werden.

Behandlung, Klassifizierung und Berichterstattung IKT-bezogener, sowie zahlungsbezogener Vorfälle

Finanzunternehmen müssen einen Prozess für die Behandlung IKT-bezogener Vorfälle bestimmen und etablieren, um IKT-bezogene Vorfälle zu erkennen, zu behandeln und zu melden. Sämtliche IKT-bezogenen Vorfälle und erheblichen Cyberbedrohungen müssen durch die Finanzunternehmen erfasst und angemessene Verfahren und Prozesse eingerichtet werden, um die kohärente und integrierte Überwachung, Handhabung und Weiterverfolgung IKT-bezogener Vorfälle zu gewährleisten. Die IKT-bezogenen Vorfälle sind, nach den in Art. 18 (1) der Verordnung genannten Kriterien, durch das Finanzunternehmen zu klassifizieren. Die Cyberbedrohungen müssen durch die Finanzunternehmen auf der Grundlage der Kritikalität der risikobehafteten Dienste, einschließlich der Transaktionen und Geschäfte des Finanzunternehmens, der Anzahl und/oder Relevanz der betroffenen Kunden oder Gegenparteien im Finanzbereich und der geografischen Ausbreitung der Risikogebiete als erheblich eingestuft werden. Schwerwiegende Vorfälle sind nach Art. 46 der Verordnung der zuständigen Behörde zu melden. Darüber hinaus sind bei schwerwiegenden IKT-bezogenen Vorfällen, die Auswirkungen auf die finanziellen Interessen von Kunden haben, diese unverzüglich nach Kenntnis über den schwerwiegenden IKT-bezogenen Vorfall sowie die Maßnahmen, die ergriffen wurden, um die nachteiligen Auswirkungen eines solchen Vorfalls zu mindern, zu informieren.

Anzumerken ist, dass die ESA der Kommission die allgemeinen Entwürfe technischer Regulierungsstandards bis zum 17. Januar 2024 zu übermitteln hat, worin Folgendes präzisiert werden wird:

> die in Artikel 18 (1) der Verordnung genannten Kriterien, einschließlich der Wesentlichkeitsschwellen für die Bestimmung schwerwiegender IKT-bezogener Vorfälle oder gegebenenfalls schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle, die der Meldepflicht nach Artikel 19 Absatz 1 unterliegen

> die Kriterien, die von den zuständigen Behörden anzuwenden sind, um die Relevanz schwerwiegender IKT-bezogener Vorfälle oder gegebenenfalls schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle für die jeweils zuständigen Behörden in anderen Mitgliedstaaten zu bewerten, sowie die Einzelheiten in den Meldungen über schwerwiegende IKT-bezogene Vorfälle oder gegebenenfalls schwerwiegende zahlungsbezogene Betriebs- oder Sicherheitsvorfälle, die anderen zuständigen Behörden gemäß Artikel 19 Absätze 6 und 7 übermittelt werden müssen

> die in Artikel Absatz 2 genannten Kriterien, einschließlich hoher Wesentlichkeitsschwellen für die Bestimmung erheblicher Cyberbedrohungen.

Testen der digitalen operationalen Resilienz

DORA – unter Berücksichtigung des Verhältnismäßigkeitsprinzips - verpflichtet die Finanzunternehmen als integralem Bestandteil ihres IKT-Risikomanagementrahmens und konkret zwecks Vorbereitung auf die Handhabung IKT-bezogener Vorfälle, zur Aufdeckung von Schwächen, Mängeln und Lücken in Bezug auf die digitale operationale Resilienz und zur Umsetzung von Korrekturmaßnahmen dazu, ein umfassendes Programm für das Testen der digitalen operationalen Resilienz zu erstellen, zu pflegen und zu überprüfen. Die digitale operationale Resilienz ist unter Berücksichtigung eines risikobasierten Ansatzes regelmäßig, mindestens jährlich, zu testen. Diese Tests können bestehen aus Schwachstellenbewertung und –scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen oder sich darstellen, soweit umsetzbar, in Form von szenariobasierten Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests.

Management des IKT-Drittparteienrisikos

Das IKT-Drittparteienrisiko (d.h. ein IKT-bezogenes Risiko, das für ein Finanzunternehmen im Zusammenhang mit dessen Nutzung von IKT-Dienstleistungen entstehen kann, die von IKT-Drittdienstleistern oder deren Unterauftragnehmern, einschließlich über Vereinbarungen zur Auslagerung, bereitgestellt werden) ist integraler Bestandteil des IKT-Risikos und muss innerhalb des IKT-Risikomanagementrahmens gemanagt werden. Eine der wesentlichsten Zielsetzungen von DORA ist es, einen Rahmen für dieses

Management der IKT-Drittrisiken zu schaffen. Finanzunternehmen, die vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen für die Ausübung ihrer Geschäftstätigkeit getroffen haben, bleiben jederzeit in vollem Umfang für die Einhaltung und Erfüllung aller Verpflichtungen von DORA und nach dem anwendbaren Finanzdienstleistungsrecht verantwortlich.
DORA sieht vor, dass Finanzunternehmen im Rahmen des IKT-Risikomanagementrahmens eine Strategie für das IKT-Drittparteienrisiko, welche insbesondere Leitlinien für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger von IKT-Drittdienstleistern bereitgestellten Funktionen zu umfassen hat, beschließen und regelmäßig überprüfen. Auch ist ein Informationsregister das sich auf alle vertraglichen Vereinbarungen über die Nutzung von durch IKT-Drittdienstleister bereitgestellten IKT-Dienstleistungen bezieht, zu führen und auf aktuellem Stand zu halten. Die in dem Informationsregister aufgeführten vertraglichen Vereinbarungen sind zu dokumentieren, wobei zwischen Vereinbarungen, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen abdecken, und solchen unterschieden wird, bei denen dies nicht der Fall ist. Neben einer allgemeinen diesbezüglichen jährlichen Berichtspflicht und der Pflicht die zuständige Behörde zeitnah über jede geplante vertragliche Vereinbarung über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen sowie in dem Fall, dass eine Funktion kritisch oder wichtig geworden ist hinaus, muss auf Anfrage das Informationsregister oder Teile hiervon zur Verfügung zu gestellt werden.
In Bezug auf die schriftliche Vereinbarung sieht DORA vor, dass es zwingend eines schriftlichen Vertrages zwischen dem Finanzunternehmen und dem IKT-Drittdienstleisters bedarf, in dem die wechselseitigen Rechte und Pflichte eindeutig festgelegt werden und der mindestens die Elemente des Artikels 30 Absatz 2 enthält. Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Artikel 30 Absatz 2 genannten Elementen mindestens die Elemente des Artikel 30 Absatz 3, d.h. es bedarf zwingend weiterer Vertragsbestimmungen wie beispielsweise Kündigungs- und Berichtspflichten und der Anforderungen an den IKT-Drittdienstleister, Notfallpläne zu implementieren und zu testen.
Bis zum 17. Januar 2024 sollen die ESA Standardvertragsklauseln erarbeitet, die von den Finanzunternehmen und IKT-Drittdienstleistern bei der Aushandlung vertraglicher Vereinbarungen erwogen werden sollen.

Vereinbarungen über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen

DORA sieht außerdem vor, dass Finanzunternehmen auch untereinander Vereinbarung treffen können, um Informationen und Erkenntnisse über Cyberbedrohungen austauschen zu können, einschließlich Indikatoren für Beeinträchtigungen, Taktiken, Techniken und Verfahren, Cybersicherheitswarnungen und Konfigurationstools, soweit dieser Austausch von Informationen und Erkenntnissen. Dies ist zu begrüßen, da hierdurch die digitale operationale Resilienz von Finanzunternehmen und damit die Zielsetzung von DORA vereinfacht wird.

To-Do

Sämtliche Finanzunternehmen, d.h. diejenigen Unternehmen, die in den Anwendungsbereich von DORA fallen, sollten - sofern noch nicht erfolgt – sich im Detail mit DORA befassen und den erforderlichen Handlungsrahmen zeitnah festlegen.

KEY CONTACT

Mevlüde-Aysun TOKBAG Partner

Stefanie KREUZER Senior Associate

Fabian FRANKUS Senior Associate

Garry REULAND Senior Associate