WIRTSCHAFTSKAMMER ÖSTERREICH
Die Finanzdienstleister

Fachverband Finanzdienstleister
Bundessparte Information und Consulting
Wirtschaftskammer Österreich
Wiedner Hauptstraße 63 | 1045 Wien
T 05 90 900-4818
E finanzdienstleister@wko.at

Datum
13.3.2023

Sie wollen mehr Informationen?
Dann schauen Sie auch in unsere
Wissensdatenbank!

www.wko.at/wissensdatenbank oder
www.wko.at/wdb

Digital Operational Resilience Act (DORA)

1. Was ist der Digital Operational Resilience Act (DORA)?

Fragen
1.) Was regelt DORA?
2.) Welche Rechtsakte stehen in Verbindung mit DORA?

Am 16.1.2023 trat die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14.12.2022 über die Betriebsstabilität digitaler Systeme des Finanzsektors (**„Digital Operational Resilience Act"**, nachfolgend **DORA**) in Kraft. Mit DORA wird ein harmonisierter und umfassender Rechtsrahmen für die digitale operationelle Widerstandsfähigkeit der europäischen Finanzunternehmen eingeführt. Die Europäische Kommission wollte damit Lücken in der Finanzdienstleistungsgesetzgebung schließen, die bisher einen fragmentierten Einsatz für die operationelle Resilienz vorsah, und die Risiken der Informations- und Kommunikationstechnologien (IKT) nur am Rande behandelte. Eine bedeutende Auswirkung von DORA ist, dass auch IKT-Drittanbieter, die als kritisch eingestuft werden, in den Anwendungsbereich der Finanzdienstleistungsaufsicht einbezogen werden. Betroffene Unternehmen müssen DORA ab 17.1.2025 anwenden. Durch DORA werden betroffene Finanzunternehmen und IKT-Drittanbieter dazu verpflichtet, zahlreiche digitale Sicherheits- und Berichtspflichten einzuhalten, um die Finanzunternehmen widerstandsfähiger gegen Cyber-Angriffe zu machen und andere Risiken aus der Nutzung von IKT zu mindern.

Gleichzeitig mit DORA wurden weitere Richtlinien erlassen: Richtlinie (EU) 2022/2555 über Maßnahmen über ein hohes gemeinsames Cybersicherheitsniveau (**„NIS2-RL"**), Richtlinie 2022/2556 hinsichtlich der digitalen operationalen Resilienz im Finanzsektor (**„DORA-RL"**) sowie Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen. Die 11 Seiten umfassende DORA-RL enthält als Begleitmaßnahme jeweils einzelne Anpassungen von mehreren Richtlinien, die aufgrund von DORA erforderlich wurden. Die ab dem 17.1.2025 anwendbare DORA-RL muss noch von den EU-Mitgliedstaaten in nationales Recht umgesetzt werden. Die NIS2-RL ist die überarbeitete Version der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (**„NIS-RL"**). NIS2 ersetzt NIS, modernisiert den bestehenden Rechtsrahmen und weitet den Anwendungsbereich der Cybersicherheitsvorschriften auf neue Sektoren und Einrichtungen aus. In den Erwägungsgründen von DORA ist klargestellt, dass **DORA eine *lex specialis* zur NIS2-RL** verkörpert und somit den Vorschriften dieser Richtlinie vorgeht, wodurch Doppelgleisigkeiten vermieden werden sollen.

Zum DORA-Rahmenwerk gehören auch delegierte Rechtsakte sowie die von den zuständigen Europäischen Aufsichtsbehörden (ESA)[1] noch zu erstellenden Leitlinien und technischen Regulierungs- und Durchführungsstandards (RTS). Dadurch werden die Anforderungen an die Finanzunternehmen in allen EU-Mitgliedsstaaten einheitlich gestaltet.

Damit sichergestellt wird, dass die Finanzunternehmen die strengen gemeinsamen Standards einhalten, um IKT-bedingten Störungen und (Cyber-)Bedrohungen standhalten zu können, werden diese Unternehmen dazu verpflichtet, zahlreiche Maßnahmen zu ergreifen und Vorgänge zu beachten:

- Implementierung eines IKT-Risikomanagementrahmens und Business Continuity Management (Art 5 bis 14 DORA);

[1] Die Europäische Bankenaufsichtsbehörde (EBA), die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) und die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA).

- Berichterstattung zu IKT-Vorfällen (Art 15 bis 20 DORA);
- Prüfung der digitalen Betriebsstabilität (mit Durchführung von Penetrationstests (Art 21 bis 24 DORA);
- Steuerung und Überwachung von IKT-Drittdienstleister-Risiken (Art 25 bis 36 DORA);
- Informationsaustausch zwischen den betroffenen Unternehmen (Art 40 DORA).

2. Allgemeine Bestimmungen – Anwendungsbereich

Fragen
3.) Welche Unternehmen sind von DORA erfasst?
4.) Müssen Gewerbliche Vermögensberater die Vorgaben zu DORA beachten?

Gemäß Art 2 Abs 1 DORA gelten die Anforderungen der Verordnung für **„Finanzunternehmen"** und **IKT-Drittdienstleister, die Verträge mit Finanzunternehmen abschließen**. In den Anwendungsbereich von DORA fallen 20 Arten von Finanzunternehmen. Neben Kreditinstituten und Versicherungs- und Rückversicherungsunternehmen sind das unter anderem folgende Finanzunternehmen:

- Wertpapierfirmen, wobei Wertpapierdienstleistungsunternehmen vom Anwendungsbereich ausgenommen sind[2];
- Zahlungs- und E-Geldinstitute (inkl Kontoinformationsdienstleister)[3];
- Anbieter von Krypto-Dienstleistungen, die gemäß einer Verordnung des Europäischen Parlaments und des Rates über Märkte von Krypto-Werten (MiCA-VO) zugelassen sind, und Emittenten wertreferenzierter Token;
- Verwalter alternativer Investmentfonds (AIFM), sofern es sich nicht um einen registrierten AIFM gemäß Art 2 AIFMD bzw § 1 Abs 5 AIFMG handelt[4];
- Schwarmfinanzdienstleister (nicht aber Crowdinvesting-Plattformen mit einer Gewerbeberechtigung als Gewerblicher Vermögensberater)[5];
- Versicherungsvermittler, Rückversicherungsvermittler sowie Versicherungsvermittler in Nebentätigkeit.[6]

Die Definition von IKT-Drittdienstleistern umfasst Unternehmen, die digitale und Datendienste anbieten, einschließlich Anbieter von Cloud-Computing-Diensten, Software, Datenanalysediensten und Rechenzentren. Finanzunternehmen müssen in ihren Verträgen mit solchen IKT-Drittanbietern auch spezifische vertragliche Bestimmungen vorsehen.

Eine bedeutende Ausnahme besteht für Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, sofern es sich bei diesen um Kleinstunternehmen, kleine oder mittlere Unternehmen handelt.[7] Somit werden nur solche Unternehmen mit 250 oder mehr Beschäftigten und Jahresumsatz 50 Mio Euro und/oder

[2] Art 2 Abs 1 lit e DORA; siehe zu der Ausnahme von Wertpapierdienstleistungsunternehmen Art 2 Abs 3 lit d DORA.
[3] Art 2 Abs 1 lit b DORA, wobei auch von der PSD2 ausgenommene Zahlungsinstitute vom Anwendungsbereich umfasst sind.
[4] Art 2 Abs 1 lit k DORA; registrierte AIFM sind nach Art 2 Abs 3 DORA ausgenommen.
[5] Art 2 Abs 1 lit s DORA.
[6] Art 2 Abs 1 lit o DORA.
[7] Art 2 Abs 3 lit e DORA; *Kleinstunternehmen*: Unternehmen, das weniger als 10 Personen beschäftigt und dessen Jahresumsatz bzw -bilanzsumme 2 Mio Euro nicht überschreitet; *Kleinunternehmen*: Unternehmen, das 10 oder mehr, aber weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw -bilanzsumme 2 Mio Euro überschreitet, jedoch nicht 10 Mio Euro; *Mittleres Unternehmen*: Unternehmen das kein Kleinunternehmen ist, das weniger als 250 Personen beschäftigt und dessen Jahresumsatz 50 Mio Euro und/oder dessen Jahresbilanzsumme 43 Mio Euro nicht überschreitet.

Jahresbilanzsumme 43 Mio Euro von DORA erfasst. Somit fallen insbesondere **Gewerbliche Vermögensberater** (bei der Kreditvermittlung, der Wertpapiervermittlung sowie im Veranlagungsbereich) nicht in den Anwendungsbereich von DORA. Bei der Versicherungsvermittlung ist das ebenfalls zutreffend, solange diese nicht größer als ein mittleres Unternehmen sind. Bezogen auf **Leasingunternehmen für den Bereich der Versicherungsvermittlung in Nebentätigkeit** ist DORA ebenfalls nicht anwendbar, solange diese nicht größer als ein mittleres Unternehmen sind. Sollten Leasingunternehmen aber bspw in der Konzernstruktur eines Kreditinstituts eingebunden sein, ist die Anwendbarkeit von DORA gesondert zu prüfen.

Hinweis: Trotz des weit gefassten Anwendungsbereichs sieht DORA mehrere Elemente der Verhältnismäßigkeit vor. Gemäß dem **Grundsatz der Verhältnismäßigkeit** müssen Finanzunternehmen, die in den Anwendungsbereich von DORA fallen, die DORA-Vorschriften einhalten, wobei ihre Größe und ihr Gesamtprofil als auch ihre Art, der Umfang und die Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte berücksichtigt werden.[8] In diesem Zusammenhang gibt es umfassende Erleichterungen für Finanzunternehmen, die die Kriterien als „Kleinstunternehmen" erfüllen (dh bis 9 Beschäftigte und Jahresumsatz bzw -bilanzsumme kleiner als 2 Mio Euro).[9] Auch für kleine und nicht verflochtene Wertpapierunternehmen gemäß Art 12 Abs 1 der Verordnung (EU) 2019/2033 („Klasse 3-Wertpapierfirmen"), die nach dem sektorspezifischen Unionsrecht aufgrund ihrer Größe bereits einem vereinfachten Aufsichtsregime unterliegen, wird im Einklang mit dem erwähnten Grundsatz der Verhältnismäßigkeit vorgesehen, dass sie einem vereinfachten IKT-Risikomanagementrahmen unterworfen werden.[10]

3. IKT-Risikomanagement, Berichterstattung und Testung

Fragen
5.) Welche Governancevorgaben muss die Geschäftsführung beachten?
6.) Wie oft muss der IKT-Risikomanagementrahmen überprüft werden?
7.) Welche Erleichterungen gelten für Klasse 3-Wertpapierfirmen?

DORA sieht vor, dass Finanzunternehmen über einen umfassenden Governance- und Kontrollrahmen für ein wirksames und umsichtiges Management von IKT-Risiken verfügen müssen.[11] Zu diesem Zweck ist ein solider, umfassender und gut dokumentierter IKT-Risikomanagementrahmen bestehend aus Strategien, Leit- und Richtlinien, Verfahren sowie IKT-Protokollen und -Tools aufzubauen und aufrechtzuerhalten.[12] Dem Leitungsorgan obliegt die ausdrückliche und letztendliche Verantwortung für die Festlegung, Genehmigung und Überwachung der Umsetzung aller notwendigen Vorkehrung in Bezug auf den IKT-Risikomanagementrahmen. Die sehr umfassenden Elemente der Verantwortlichkeiten des Leitungsorgans werden in Art 5 Abs 2 DORA angeführt.[13]

Diese umfassen insbesondere

i. die Einführung von Leitlinien um hohe Standards in Bezug auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten aufrechtzuhalten;

[8] Art 4 Abs 1 DORA.
[9] Siehe dazu im Detail unter Punkt 11.
[10] Siehe dazu Punkt 3.
[11] Art 5 Abs 1 DORA.
[12] Art 6 Abs 2 DORA.
[13] Vgl Art 5 Abs 2 DORA.

ii. die Festlegung und Genehmigung der Strategie für die digitale operationale Resilienz und Festlegung der angemessenen Toleranzschwellen für das IKT-Risiko des Finanzunternehmens;
iii. die Genehmigung, Überwachung und Überprüfung der IKT-Geschäftsfortführungsleitlinie und der IKT-Reaktions- und Wiederherstellungspläne,
iv. die Genehmigung und regelmäßige Prüfung der internen IKT-Revisionspläne; und
v. die Zuweisung angemessener Budgetmittel (einschließlich Sensibilisierungsprogramme für IKT-Sicherheit und Mitarbeiterschulungen).

Mit der letztendlichen Verantwortung des Leitungsorgans ist für dieses Organ eine regelmäßige Absolvierung von Fachschulungen zu IKT-Risiken vorgesehen, um die IKT-Risiken und deren Auswirkungen auf die Geschäftstätigkeit des Finanzunternehmens verstehen und bewerten zu können.[14]

Der umgesetzte IKT-Risikomanagementrahmen soll dafür Sorge tragen, alle Informations- und IKT-Assets, einschließlich Computer-Software, Hardware und Server, ordnungsgemäß und angemessen zu schützen sowie um alle relevanten physischen Komponenten und Infrastrukturen, wie etwa Räumlichkeiten, Rechenzentren und ausgewiesene sensible Bereiche zu schützen (einschließlich Beschädigung, unbefugter Zugriff und unbefugte Nutzung).[15] Den zuständigen Behörden sind auf Anfrage vollständige und aktuelle Informationen über IKT-Risiken und ihren IKT-Risikomanagementrahmen vorzulegen.[16]

Die betroffenen Finanzunternehmen werden dazu verpflichtet, die Zuständigkeit für das Management und die Überwachung des IKT-Risikos an eine Kontrollfunktion zu übertragen und ein angemessenes Maß an Unabhängigkeit dieser Kontrollfunktion sicherzustellen, um Interessenkonflikte zu vermeiden. Vorzusehen ist ebenfalls eine angemessene Trennung und Unabhängigkeit von IKT-Risikomanagementfunktionen, Kontrollfunktionen und internen Revisionsfunktionen.[17]

Eine Dokumentation und Überprüfung des IKT-Risikomanagementrahmens hat mindestens einmal jährlich, sonst auch bei Auftreten schwerwiegender IKT-bezogener Vorfälle und auch nach aufsichtsrechtlichen Anweisungen und Feststellungen, die sich aus einschlägigen Tests der digitalen operationalen Resilienz oder Auditverfahren ergeben, zu erfolgen. Die dabei gewonnenen Erkenntnisse sollen den Rahmen kontinuierlich verbessern. Auf Anfrage der zuständigen Aufsichtsbehörde ist ein Bericht über die Überprüfung des IKT-Risikomanagementrahmens vorzulegen.[18] Finanzunternehmen sind weiters dazu verpflichtet, den IKT-Risikomanagementrahmen regelmäßig einer internen Revision durch Revisoren, die über ausreichendes Wissen und ausreichende Fähigkeiten und Fachkenntnisse im Bereich IKT-Risiken verfügen müssen, zu unterziehen. Finanzunternehmen können die Überprüfung und Einhaltung der Anforderungen an das IKT-Risikomanagement an gruppeninterne oder externe Unternehmen auslagern, jedoch bleibt bei einer solchen Auslagerung weiterhin das Finanzunternehmen uneingeschränkt für die Überprüfung der Einhaltung der IKT-Risikomanagementanforderungen verantwortlich.[19]

[14] Vgl Art 5 Abs 2 DORA.
[15] Art 6 Abs 2 DORA.
[16] Art 6 Abs 3 DORA.
[17] Art 6 Abs 4 DORA.
[18] Art 6 Abs 5 DORA.
[19] Art 6 Abs 6 DORA.

Finanzunternehmen sind dazu verpflichtet, **IKT-Systeme, -Protokolle und -Tools** zu verwenden und diese stets auf dem neuesten Stand zu halten. Diese müssen in Einklang mit dem Grundsatz der Verhältnismäßigkeit für die Ausübung der Geschäftstätigkeit zuverlässig und angemessen sein. Ebenfalls sind alle IKT-gestützten Unternehmensfunktionen, Rollen und Verantwortlichkeiten als auch die Informations- und IKT-Assets, die diese Funktionen unterstützen, zu ermitteln und hinsichtlich der IKT-Risiken zu klassifizieren und dokumentieren. Mindestens einmal jährlich ist zu überprüfen, ob die Klassifizierung und Dokumentation noch angemessen sind.[20]

Finanzunternehmen haben zudem alle Quellen für IKT-Risiken, insbesondere das Risiko gegenüber anderen Finanzunternehmen, zu ermitteln und die relevanten Cyberbedrohungen und IKT-Schwachstellen zu bewerten.[21] Bei jeder wesentlichen Änderung der Netzwerk- und Informationssysteminfrastruktur, der Prozesse oder Verfahren, die eine Auswirkung auf IKT-gestützte Unternehmensfunktionen, Informations- oder IKT-Assets haben, ist eine Risikobewertung durchzuführen.[22] Finanzunternehmen müssen nicht nur alle Informations- und IKT-Assets ermitteln, sondern auch all jene internen und externen Informations- und IKT-Assets erfassen, die als kritisch gelten. Dabei ist ferner auch die Konfiguration dieser Assets als auch die Verbindung und Interdependenz zwischen den verschiedenen Assets zu erfassen.[23] Vorgesehen ist ebenfalls, dass Finanzunternehmen alle Prozesse, die von IKT-Drittdienstleistern abhängen, ermitteln und dokumentieren und weiters alle Vernetzungen mit IKT-Drittdienstleistern, die Dienste zur Unterstützung kritischer oder wichtiger Funktionen bereitstellen, ermitteln.[24] Für Dokumentationszwecke müssen entsprechende Inventare über genannte Informations- und IKT-Assets geführt werden, die regelmäßig sowie bei einer wesentlichen Änderung zu aktualisieren sind.[25]

Zum Schutz vor und zur Vorbeugung und Erkennung von IKT-Risiken sowie als Reaktion und zur Wiederherstellung sind entsprechende Maßnahmen vorgesehen wie die Implementierung einer umfassenden IKT-Geschäftsfortführungsleitlinie samt speziellen Plänen, insbesondere in Bezug auf kritische oder wichtige Funktionen, die ausgelagert oder durch vertragliche Vereinbarungen an IKT-Drittdienstleister vergeben wurden. Diese speziellen Pläne sollen bei IKT-Vorfällen aktiviert werden, um Eindämmungsmaßnahmen, Prozesse und Technologien für alle Arten IKT-bezogener Vorfälle zu ermöglichen, damit weiterer Schaden abgewendet wird.[26]

Als Teil der allgemeinen IKT-Geschäftsfortführungsleitlinie müssen Finanzunternehmen eine Analyse der Auswirkungen auf den Geschäftsbetrieb (Business-Impact-Analyse) durchführen, um ihre Gefährdung durch schwerwiegende Betriebsstörungen anhand quantitativer und qualitativer Kriterien zu ermitteln.[27] Finanzunternehmen haben über eine Krisenmanagementfunktion zu verfügen, die bei Aktivierung der IKT-Geschäftsfortführungspläne oder der IKT-Reaktions- und Wiederherstellungspläne in der Lage sein wird, die interne und externe Kommunikation zu steuern.[28] Finanzunternehmen werden auch dazu verpflichtet, Richtlinien und Verfahren zur Datensicherung als auch zu Wiedergewinnungs- und Wiederherstellungsverfahren und -methoden zu entwickeln und zu

[20] Art 8 Abs 1 DORA.
[21] Art 8 Abs 2 DORA.
[22] Art 8 Abs 3 DORA.
[23] Art 8 Abs 4 DORA.
[24] Art 8 Abs 5 DORA.
[25] Art 8 Abs 6 DORA.
[26] Art 11 Abs 2 DORA.
[27] Art 11 Abs 5 DORA.
[28] Art 11 Abs 7 DORA.

dokumentieren.[29] Ferner müssen Finanzunternehmen über Kapazitäten und Personal verfügen, um Informationen über Schwachstellen und Cyberbedrohungen, IKT-bezogene Vorfälle (insbesondere Cyberangriffe) zu sammeln, um die wahrscheinlichen Auswirkungen auf die digitale operationale Resilienz zu untersuchen.[30] Zudem sind obligatorische Schulungen zur digitalen operationalen Resilienz für alle Mitarbeiter und Führungskräfte vorgesehen.[31]

Schließlich müssen Finanzunternehmen als Teil des IKT-Risikomanagementrahmens über Kommunikationspläne verfügen, die eine Offenlegung zumindest von schwerwiegenden IKT-bezogenen Vorfällen oder Schwachstellen gegenüber Kunden, anderen Finanzunternehmen und der Öffentlichkeit ermöglichen.[32]

Art 16 DORA sieht im Einklang mit dem Grundsatz der Verhältnismäßigkeit vor, dass bestimmte in Abs 1 genannte Finanzunternehmen, die nach dem sektorspezifischen Unionsrecht aufgrund ihrer Größe oder den von ihnen erbrachten Dienstleistungen weniger strengen Anforderungen oder Ausnahmen unterliegen, die Art 5 bis 15 DORA betreffend das IKT-Risikomanagement nicht einhalten müssen. Diese Finanzunternehmen unterliegen stattdessen einem **vereinfachten IKT-Risikomanagementrahmen**. Von diesem vereinfachten Aufsichtsregime profitieren gemäß Art 16 Abs 1 DORA insbesondere kleine und nicht verflochtene Wertpapierfirmen (sog **Klasse 3-Wertpapierfirmen**) oder kleine Einrichtungen der betrieblichen Altersversorgung. Diese Finanzunternehmen haben unter anderem

i. einen soliden und dokumentierten IKT-Risikomanagementrahmen zu errichten und aufrechtzuerhalten;
ii. die Sicherheit und das Funktionieren aller IKT-Systeme fortlaufend zu überwachen;
iii. die Auswirkungen von IKT-Risiken durch den Einsatz solider, resilienter und aktualisierter IKT-Systeme, -Protokolle und -Tools, die für die Durchführung der Tätigkeiten und die Bereitstellung von Diensten angemessen sind, zu minimieren;
iv. eine rasche Ermittlung und Aufdeckung der Ursachen von IKT-Risiken und -Anomalien in den Netzwerk- und Informationssystemen zu ermöglichen;
v. die wesentlichen Abhängigkeiten von IKT-Drittdienstleistern zu ermitteln;
vi. die Kontinuität kritischer oder wichtiger Funktionen durch Geschäftsfortführungspläne sowie Gegen- und Wiederherstellungsmaßnahmen, die auch Sicherungs- und Wiedergewinnungsmaßnahmen umfassen, zu gewährleisten;
vii. eine regelmäßige Testung der Geschäftsfortführungspläne und der in (vi) genannten Maßnahmen als auch der durchgeführten Kontrollen zum soliden IKT-Risikomanagementrahmen vorzunehmen; und
viii. gegebenenfalls die Schlussfolgerungen aus den gemäß (vii) durchgeführten Tests und der Analyse von IKT-Vorfällen in die IKT-Risikobewertung einzubeziehen und entsprechende Sensibilisierungs- und Schulungsmaßnahmen zu setzen.[33]

4. IKT-bezogene Vorfälle und deren Bewältigung, Klassifizierung und Meldung

Fragen
8.) Welche Vorfälle sind zu melden und was ist dabei mitzuteilen?
9.) Wann sind solche Vorfälle zu melden?

[29] Art 12 Abs 1 DORA.
[30] Art 13 Abs 1 DORA.
[31] Art 13 Abs 6 DORA.
[32] Art 14 Abs 1 DORA.
[33] Art 16 DORA.

Wie bereits eingangs erwähnt, sind künftig schwerwiegende IKT-bezogene Vorfälle zu melden.[34] Die Mitgliedsstaaten haben eine einzige nationale Behörde als zentrale Meldestelle zur Meldung von schwerwiegenden IKT-bezogenen Vorfällen zu benennen. Finanzunternehmen werden zu diesem Zweck verpflichtet, einen Prozess für die Behandlung IKT-bezogener Vorfälle einzurichten, um IKT-bezogene Vorfälle zu erkennen, zu behandeln und zu melden.[35] DORA sieht diesbezüglich von Finanzunternehmen die Einführung von Verfahren zur Klassifizierung von IKT-bezogenen Vorfällen anhand vorgegebener Kriterien vor, wobei die ESA noch RTS-Entwürfe hinsichtlich der Kriterien für die Bestimmung schwerwiegender (i) IKT-bezogener Vorfälle, (ii) Cyberbedrohungen, und (iii) zahlungsbezogener Betriebs- und Sicherheitsvorfälle erarbeiten werden.[36]

Die ESA sind in DORA außerdem damit beauftragt, gemeinsame Entwürfe von RTS zu erarbeiten um (i) den Inhalt von Meldungen über schwerwiegende IKT-bezogene Vorfälle, (ii) die Fristen für die Erstmeldung und weitere Meldungen, und (iii) den Inhalt der Meldung erheblicher Cyberbedrohungen festzulegen. Um eine EU-weite Harmonisierung zu gewährleisten, ist auch vorgesehen, dass diese Behörden gemeinsame RTS-Entwürfe zur Festlegung von Standardformularen, Vorlagen und Verfahren für Finanzunternehmen zur Meldung von schwerwiegenden IKT-bezogenen Vorfällen und erheblichen Cyberbedrohungen erarbeiten sollen. DORA sieht dazu vor, dass die ESA bei der Ausarbeitung dieser Entwürfe die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität der Dienstleistungen, Tätigkeiten und Geschäfte zu berücksichtigen haben, um die jeweiligen Besonderheiten der Finanzsektoren gegebenenfalls durch unterschiedliche Fristen zu berücksichtigen.[37]

Finanzunternehmen werden zudem dazu verpflichtet, schwerwiegende IKT-Vorfälle innerhalb der (festzulegenden) Fristen an die zuständigen nationalen Behörden in Form von Erst-, Zwischen- und Abschlussberichten vorzulegen.[38] Die Erstmeldung und anschließende Meldungen sollen alle Informationen enthalten, die die zuständige Behörde benötigt, um die Signifikanz des schwerwiegenden IKT-bezogenen Vorfalls zu ermitteln und mögliche grenzüberschreitende Auswirkungen zu bewerten.[39] IKT-bezogene Vorfälle, die Auswirkungen auf die finanziellen Interessen von Kunden des Finanzunternehmens haben, sind dem Kunden unverzüglich mitzuteilen. Die Kunden sind zudem über die ergriffenen Maßnahmen zu unterrichten.[40]

Zudem ist vorgesehen, dass die ESA in Abstimmung mit der Europäischen Zentralbank und der ENISA bis zum 17.1.2025 einen gemeinsamen Bericht erstellen, in dem die Durchführbarkeit einer weiteren Zentralisierung der Meldung von Vorfällen durch die **Einrichtung einer einheitlichen EU-Plattform** für die Meldung schwerwiegender IKT-bezogener Vorfälle durch Finanzunternehmen evaluiert wird.[41]

[34] Art 19 Abs 1 DORA.
[35] Art 17 Abs 1 DORA.
[36] Art 18 Abs 1 und 3 DORA.
[37] Art 20 DORA.
[38] Art 19 Abs 4 DORA.
[39] Art 19 Abs 1 DORA.
[40] Art 19 Abs 2 DORA.
[41] Art 21 Abs 1 DORA.

5. Prüfung der digitalen Betriebsstabilität

Fragen
10.) Welche Tests sind durchzuführen?

Zur Vorbereitung auf die Handhabung IKT-bezogener Vorfälle und das Testen der digitalen operationalen Resilienz müssen Finanzunternehmen ein solides und umfassendes Programm umsetzen, erstellen, pflegen und überprüfen.[42] Dabei ist sicherzustellen, dass Tests von unabhängigen, internen oder externen Parteien durchgeführt werden. Sofern Tests von internen Testern durchgeführt werden, ist sicherzustellen, dass während der Konzeptions- und Durchführungsphase der Prüfung keine Interessenkonflikte entstehen.[43] IKT-Systeme und -Anwendungen, die kritische oder wichtige Funktionen unterstützen, sind mindestens einmal jährlich auf operationale Resilienz zu testen.[44] Durchzuführende Tests umfassen zB Schwachstellenbewertung und -scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen (soweit durchführbar), szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und **Penetrationstests**.[45]

6. Steuerung von IKT-Drittdienstleister-Risiken

Fragen
11.) Was ist bei vertraglichen Vereinbarungen mit IKT-Drittdienstleistern zu beachten?
12.) Wie erfolgt die Dokumentation von vertraglichen Vereinbarungen mit IKT-Drittdienstleistern?

Eines der zentralen Ziele von DORA besteht darin, einen geeigneten Rahmen für ein solides Management von IKT-Drittrisiken zu schaffen. Finanzunternehmen bleiben jederzeit in vollem Umfang für die Einhaltung und Erfüllung aller Verpflichtungen nach der Verordnung durch die von ihnen beauftragten IKT-Drittdienstleister verantwortlich.[46] Vorgesehen ist, 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.[47] Dazu ist ein **Informationsregister** mit allen vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die Dritte bereitstellen, zu führen.[48] Auf Verlangen der Behörde ist das vollständige Informationsregister oder sind auf Anfrage bestimmte Teile des Registers und Informationen, die für eine wirksame Beaufsichtigung notwendig werden, zur Verfügung zu stellen.[49] Die zuständige Behörde kann das Finanzunternehmen dazu zwingen, Verträge mit IKT-Drittdienstleistern vorübergehend teilweise oder vollständig auszusetzen, bis die Risiken beseitigt sind.[50]

[42] Art 24 Abs 1 DORA.
[43] Art 24 Abs 4 DORA.
[44] Art 24 Abs 4 DORA.
[45] Art 25 Abs 1 DORA.
[46] Art 28 Abs 1 DORA.
[47] Art 28 Abs 2 DORA.
[48] Art 28 Abs 3 DORA.
[49] Art 28 Abs 3 DORA.
[50] Art 42 Abs 6 DORA.

Die Dokumentation umfasst auch eine Kategorisierung von Vereinbarungen danach, ob die Vereinbarungen die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen abdecken oder dies nicht der Fall ist.[51] Den zuständigen Behörden ist weiters mindestens einmal jährlich ein Bericht zur Anzahl neuer Vereinbarungen und den Kategorien von IKT-Drittdienstleistern zu erstatten.[52]

DORA sieht vor, das vertragliche Vereinbarungen nur abgeschlossen werden dürfen, wenn angemessene Standards für Informationssicherheit eingehalten werden. Betreffen vertragliche Vereinbarungen kritische oder wichtige Funktionen, so muss vor Abschluss der Vereinbarung angemessen berücksichtigt werden, ob die IKT-Drittdienstleister die aktuellsten und höchsten Qualitätsstandards für die Informationssicherheit anwenden.[53] Finanzunternehmen haben insbesondere sicherzustellen, dass die vertraglichen Vereinbarungen bestimmte wichtige Kündigungsgründe enthalten. So wird ein Finanzunternehmen verpflichtet, eine Vereinbarung mit einem IKT-Drittdienstleister zu kündigen, wenn ein erheblicher Verstoß des IKT-Drittdienstleisters gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen festgestellt wird.[54] Finanzunternehmen müssen auch Ausstiegsstrategien erarbeiten, um mit Ausfällen von IKT-Drittdienstleistern umgehen zu können. Dabei darf aber eine Vertragskündigung der Einhaltung regulatorischer Anforderungen nicht zuwiderlaufen oder die angebotenen Dienstleistungen qualitativ beeinträchtigen.[55]

Dazu ist noch vorgesehen, dass von den ESA bis 17.1.2024 **Standardvertragsklauseln** erarbeitet werden, die von den Finanzunternehmen und IKT-Drittdienstleistern bei der Aushandlung vertraglicher Vereinbarungen erwogen werden sollen.[56] Für den Inhalt dieser Vereinbarungen gibt es strenge Vorgaben, so etwa

i. die klare und vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen (unter Angabe, ob eine Vergabe von Unteraufträgen für IKT-Dienstleistungen, die wichtige Funktionen oder wesentliche Teile davon unterstützen, zulässig ist);
ii. Bestimmungen über Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz (einschließlich des Schutzes personenbezogener Daten),
iii. Beschreibungen der Dienstleistungsgüte, einschließlich Aktualisierungen und Überarbeitungen;
iv. die Verpflichtung des ITK-Dienstleisters dem Finanzunternehmen bei einem IKT-Vorfall, der mit dem bereitgestellten IKT-Dienst in Verbindung steht, ohne zusätzlich Kosten oder zu vorab festzusetzenden Kosten Unterstützung zu leisten;
v. Kündigungsrechte und damit zusammenhängende Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarungen entsprechend den Erwartungen der zuständigen Behörden;
vi. Bedingungen für die Teilnahme von IKT-Drittdienstleistern an den von den Finanzunternehmen angebotenen Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz.[57]

Finanzunternehmen werden ferner dazu verpflichtet zeitnah **über jede geplante vertragliche Vereinbarung** über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder

[51] Art 28 Abs 4 DORA.
[52] Art 28 Abs 3 DORA.
[53] Art 28 Abs 5 DORA.
[54] Art 28 Abs 7 DORA.
[55] Art 28 Abs 8 DORA.
[56] Art 28 Abs 9 DORA.
[57] Art 30 Abs 2 DORA.

wichtiger Funktionen an die zuständige Behörde zu melden.[58] Es ist auch vorgesehen, dass die ESA durch RTS die Bedingungen für Untervergaben präzisieren werden, die bei der Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen zu berücksichtigen sind.[59]

7. Kritische IKT-Dienstleister und Aufsichtsrahmen

Fragen
13.) Wer ist ein kritischer IKT-Drittdienstleister?
14.) Wie erfolgt die Überwachung durch zuständige Behörden?

DORA enthält für **kritische IKT-Drittdienstleister** eine gesonderte Reihe von Bestimmungen. Die Kriterien zur Einstufung als kritischer IKT-Drittdienstleister sind in Art 31 Abs 2 DORA angeführt. Die ESA erstellen, veröffentlichen und aktualisieren die Liste kritischer IKT-Drittdienstleister auf Unionsebene über den Gemeinsamen Ausschuss.[60] Zu beachten ist weiters, dass Finanzunternehmen nur dann Dienstleistungen eines als kritisch eingestuften IKT-Drittdienstleisters mit Sitz in einem Drittland in Anspruch nehmen können, wenn dieser innerhalb von 12 Monaten nach der Einstufung ein Tochterunternehmen in der Union gegründet hat.[61]

Der Gemeinsame Ausschuss richtet ein Überwachungsforum, welcher sich aus mehreren hochrangigen Vertretern von europäischen und nationalen Behörden zusammensetzt, ein. Eine der ESA agiert nach in der Verordnung vorgesehenen Kriterien[62] als federführende Überwachungsbehörde mit weitreichenden Kompetenzen in der Beaufsichtigung der IKT-Drittdienstleister insbesondere dahingehend, ob jeder kritische IKT-Drittdienstleister über umfassende, fundierte und wirksame Vorschriften, Verfahren, Mechanismen und Vorkehrungen für das Management von IKT-Risiken verfügt, die dieser für Finanzunternehmen mit sich bringen kann.[63] Die federführende Überwachungsbehörde nimmt nach Durchführung einer Bewertung des IKT-Drittdienstleisters einen klaren, detaillierten und individuellen Überwachungsplan an, in dem die für jeden kritischen IKT-Drittdienstleister vorgesehenen jährlichen Überwachungsziele und wichtigsten Überwachungsmaßnahmen beschrieben werden. Dem IKT-Drittdienstleister wird der Entwurf des Überwachungsplans vorab übermittelt. Auch wird diesem die Möglichkeit eingeräumt, eine begründete Erklärung vorzulegen, in der die erwarteten Auswirkungen auf Kunden, bei denen es sich um nicht in den Anwendungsbereich der Verordnung fallende Unternehmen handelt, mitgeteilt werden und gegebenenfalls Lösungen zur Risikominderung enthalten sind.[64] Die federführenden Überwachungsbehörden werden weitreichende Befugnisse haben, einschließlich der Befugnis Zugang zu relevanten Informationen und Unterlagen zu verlangen und allgemeine Untersuchungen und Inspektionen durchzuführen sowie Zwangsgelder bei Nichteinhaltung von Maßnahmen zu verhängen, zu denen ein IKT-Drittdienstleister verpflichtet wurde.[65]

[58] Art 28 Abs 3 DORA.
[59] Art 30 Abs 5 DORA.
[60] Art 31 Abs 9 DORA.
[61] Art 31 Abs 12 DORA.
[62] Vgl Art 31 Abs 1 DORA.
[63] Art 33 Abs 2 DORA.
[64] Art 33 Abs 4 DORA.
[65] Art 35 Abs 1, 6 und 8 DORA; Zwangsgelder in Höhe von bis zu 1% des durchschnittlichen weltweiten Tagesumsatzes (pro Tag) bis zur Einhaltung der Vorschriften und für höchstens sechs Monate nach Mitteilung der Entscheidung über die Verhängung eines Zwangsgelds.

8. Vereinbarungen über den Austausch von Informationen

Fragen
15.) Was ist beim Austausch von Informationen zwischen Unternehmen zu beachten?

In der Erwägungsgründen der Verordnung wird erwähnt, dass die Zusammenarbeit und der Austausch von Informationen und Erfahrungen zwischen Finanzunternehmen für die Erhöhung von Sicherheit wichtig und erwünscht ist. Daher können Finanzunternehmen Informationen und Erkenntnisse über Cyberbedrohungen untereinander austauschen, einschließlich der Indikatoren für Beeinträchtigungen, Taktiken, Techniken und Verfahren, Cybersicherheitswarnungen und Konfigurationstools. Voraussetzung dafür ist, dass dieser Austausch von Informationen und Erkenntnissen:

i. darauf abzielt, die digitale operationelle Resilienz von Finanzunternehmen zu stärken;
ii. innerhalb von vertrauenswürdigen Gemeinschaften von Finanzunternehmen stattfindet; und
iii. durch Vereinbarungen über den Informationsaustausch umgesetzt wird, die den potenziell sensiblen Charakter der ausgetauschten Informationen schützen und Verhaltensregeln unterliegen, die das Geschäftsgeheimnis, den Schutz personenbezogener Daten und die Leitlinien für die Wettbewerbspolitik in vollem Umfang wahren.[66]

9. Beaufsichtigung und Durchsetzung durch Behörden

Fragen
16.) Welche österreichischen Behörden sind für die Einhaltung von DORA zuständig?

DORA überträgt die Aufsicht über die Einhaltung der Anforderungen an die jeweils zuständigen Behörden, die für die Beaufsichtigung der in den Geltungsbereich fallenden Finanzunternehmen verantwortlich sind.[67] In Österreich wird das in weiten Teilen die FMA sein. Für den Bereich der Versicherungsvermittlung oder den Bereich des Leasinggeschäfts (Versicherungsvermittlung in Nebentätigkeit) wäre das voraussichtlich die Gewerbebehörde. Die zuständigen Behörden verfügen zu diesem Zweck über alle Aufsichts-, Untersuchungs- und Sanktionsbefugnisse, die zur Erfüllung ihrer Aufsichtspflichten erforderlich sind. Die Befugnisse der zuständigen Behörde umfassen den Zugriff auf Unterlagen und Daten jeglicher Form, die Durchführung von Vor-Ort-Inspektionen und Übersuchungen einschließlich der Vorladung von Vertretern der Finanzunternehmen zur Abgabe von (mündlichen oder schriftlichen) Erklärungen und der Befragung jeder anderen natürlichen oder juristischen Person (soweit diese zustimmen) sowie das Verlangen von Korrektur- und Abhilfemaßnahmen und die Anwendung von verwaltungsrechtlichen Sanktionen bei Verstößen gegen die Anforderungen der Verordnung.[68]

10. Konkretisierung der DORA-Vorgaben durch die ESA

Fragen
17.) Welche RTS werden von den ESA noch erarbeitet?

[66] Art 45 Abs 1 DORA; siehe auch zB ErwGr 32 DORA.
[67] Art 46 DORA.
[68] Art 50 Abs 1 und 2 DORA.

Die Verordnung trägt den ESA (wie eingangs erwähnt) an mehreren Stellen auf, RTS zu erarbeiten, die bei der Umsetzung durch die betroffenen Finanzunternehmen zusätzlich zu berücksichtigen sein werden. Wichtige noch zu konkretisierende RTS wären insbesondere:

- Details zum **IKT-Risikomanagement**, so etwa (i) Festlegung der Elemente hinsichtlich der IKT-Sicherheitsrichtlinien, -verfahren, -protokolle, (ii) Festlegung der Komponenten der Informationssicherheitsleitlinie, (iii) Weiterentwicklung der Erkennungsmechanismen, (iv) Spezifizierung der Komponenten der IKT-Geschäftsfortführungsleitlinie; (v) Spezifizierung der Tests von IKT-Geschäftsfortführungsplänen, (vi) Spezifizierung der Komponenten der IKT-Reaktions- und Wiederherstellungspläne, (vii) Spezifizierung von Inhalt und Form des Berichts über die Überprüfung des IKT-Risikomanagementrahmens[69];
- Details **zum vereinfachten IKT-Risikomanagement**, so zB Spezifizierung (i) der Elemente, die zum IKT-Risikomanagementrahmen aufzunehmen sind, (ii) der Komponenten der IKT-Geschäftsfortführungsleitlinie, (iii) weiterer Elemente in Bezug auf Systeme, Protokolle und Tools zur Minimierung der Auswirkungen von IKT-Risiken, (iv) der Vorschriften für die Tests der Geschäftsfortführungspläne und Kontrollen, und (iv) von Inhalt und Form des Prüfberichts[70];
- weitere Details zur **Klassifizierung von IKT-bezogenen Vorfällen und Cyberdrohungen**, zB Wesentlichkeitsschwellen für die Bestimmung von IKT-bezogenen Vorfällen und Cyberdrohungen[71];
- Details zu **Berichtspflicht, Meldungsfristen, -vorlagen und -inhalten** über schwerwiegende IKT-bezogene Vorfälle und erheblicher Cyberbedrohungen[72];
- Details zu **erweiterten Tests von IKT-Tools, -Systemen und -Prozessen** auf Basis von bedrohungsorientierten Penetrationstests[73];
- Details zum **Management des IKT-Drittparteienrisikos**, wie zB Inhalt der Leitlinie für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer und wichtiger Funktionen[74], sowie Kriterien für die Untervergabe von IKT-Dienstleistungen[75];
- Details zum **Überwachungsrahmenwerk für kritische IKT-Drittdienstleister**, so zB zu Inhalt, Struktur und Format der Informationen, die IKT-Drittdienstleister offenlegen und melden müssen.[76]

11. Erleichterungen und Ausnahmen für Kleinstunternehmen auf einen Blick

Fragen
18.) Welche Erleichterungen sieht DORA für Kleinstunternehmen vor?

Wie bereits unter Punkt 2 angeführt, sollen die meisten Anforderungen für Finanzunternehmen aller Größen gelten. DORA ermöglicht unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit jedoch eine verhältnismäßige Anwendung der Anforderungen für Kleinstunternehmen.[77] Die Erleichterungen für Kleinstunternehmen sind insbesondere:

[69] Art 15 Abs 3 DORA; Entwürfe bis 17.1.2014.
[70] Art 16 Abs 3 DORA; Entwürfe bis 17.1.2024.
[71] Art 18 Abs 3 DORA; Entwürfe bis 17.1.2024.
[72] Art 20 DORA; Entwürfe bis 17.7.2024.
[73] Art 26 DORA; Entwürfe bis 17.7.2024.
[74] Art 28 DORA, Entwürfe bis 17.1.2024.
[75] Art 30 Abs 5 DORA, Entwürfe bis 17.7.2024.
[76] Art 41 DORA, Entwürfe bis 17.7.2024.
[77] Vgl Punkt 2 zur Definition von Kleinstunternehmen. Für bestimmte Kleinunternehmen, die zugleich in Art 16 DORA angeführt sind, ist ein vereinfachter IKT-Risikomanagementrahmen anwendbar.

- Ausnahme von der Einrichtung einer Funktion, um die mit IKT-Drittdienstleistern über die Nutzung von IKT-Dienstleistungen geschlossenen Vereinbarungen zu überwachen[78];
- Ausnahme von der Übertragung der Zuständigkeit für das IKT-Management und der Überwachung des IKT-Risikos an eine Kontrollfunktion[79];
- Ausnahme von der Durchführung einer internen Revision durch Revisoren[80];
- keine Risikobewertung für wesentliche Änderungen der Netzwerk- und Informationssysteminfrastruktur und keine mindestens jährliche IKT-Risikobewertung für alle älteren IKT-Systeme[81];
- keine Implementierung von IKT-Reaktions- und Wiederherstellungsplänen als Teil des IKT-Risikomanagementrahmens[82];
- keine Aufnahme bestimmter Elemente in die Testpläne: und zwar (i) Szenarien für Cyberangriffe, und (ii) Umstellungen von der primären IKT-Infrastruktur auf die redundanten Kapazitäten, Backups und Systeme[83];
- keine Verpflichtung über ein Krisenmanagement zu verfügen, welches klare Verfahren für die Abwicklung interner und externer Krisenkommunikation festlegt[84];
- keine Meldung an die zuständigen Behörden, die geschätzten aggregierten jährlichen Kosten und Verluste, die durch schwerwiegende IKT-bezogene Vorfälle verursacht wurden[85];
- keine generelle Verpflichtung zur Unterhaltung redundanter IKT-Kapazitäten mit Ressourcen, Fähigkeiten und Funktionen. Es erfolgt eine Bewertung auf Grundlage des Risikoprofils, ob redundante IKT-Kapazitäten unterhalten werden müssen[86];
- keine Verpflichtung einschlägige technologische Entwicklungen fortlaufend zu überwachen, um die möglichen Auswirkungen des Einsatzes solcher neuen Technologien auf die Anforderungen an die IKT-Sicherheit zu verstehen[87];
- keine Verpflichtung (i) ein solides und umfassendes Programm zum Testen der digitalen operationalen Resilienz zu erstellen; (ii) unabhängige (interne oder externe) Tests durchzuführen, (iii) mindestens einmal jährlich angemessene Tests durchzuführen; (iv) mindestens alle drei Jahre anhand von TLPT erweiterte Tests durchzuführen; stattdessen Durchführung von Tests, indem ein risikobasierter Ansatz mit einer strategischen Planung für IKT-Tests kombiniert wird[88];
- keine Verpflichtung im Rahmen des IKT-Risikomanagementrahmens eine Strategie für das IKT-Drittparteienrisiko zu haben und dieses regelmäßig zu überprüfen[89];
- können mit IKT-Drittdienstleistern vereinbaren, dass Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens auf einen unabhängigen Dritten übertragen werden.[90]

[78] Art 5 Abs 3 DORA.
[79] Art 6 Abs 4 DORA.
[80] Art 6 Abs 6 DORA.
[81] Art 8 Abs 3 DORA.
[82] Art 11 Abs 3 DORA.
[83] Art 11 Abs 5 DORA.
[84] Art 11 Abs 7 DORA.
[85] Art 11 Abs 10 DORA.
[86] Art 12 Abs 4 DORA.
[87] Art 12 Abs 4 DORA.
[88] Art 24 Abs 1 bis 4, Art 25 Abs 3 und Art 26 Abs 1 DORA.
[89] Art 28 Abs 2 DORA.
[90] Art 30 Abs 3 DORA.

12. Betrachtung von DORA mit anderen rechtlichen Anforderungen, Ausblick und praktische Überlegungen

DORA sollte trotz aller Komplexität und dem nicht unwesentlichen Umfang nicht isoliert betrachtet werden. Bei der Gesetzgebung wurde nämlich Wert auf eine Verknüpfung von DORA mit anderen vergleichbaren Initiativen gesetzt, insbesondere mit der NIS2-RL sowie mit bereits bestehenden Initiativen wie den Leitlinien der Europäischen Bankenaufsichtsbehörde (EBA) zu Auslagerungsvereinbarungen und den EBA-Leitlinien für IKT und Sicherheitsrisikomanagement.

Es fällt auf, dass bei DORA eine generelle Ausnahme für Kleinstunternehmen fehlt, die beispielsweise das Netz- und Informationssicherheitsgesetz („NISG“) und auch die neue NIS2-RL vorsieht. Die NIS2-RL sieht sogar (von einigen Ausnahmen abgesehen) vor, dass grundsätzlich nur jene Unternehmen in den betroffenen Sektoren in den Anwendungsbereich der NIS2-RL fallen, die 50 oder mehr Mitarbeiter und einen Jahresumsatz bzw eine Jahresbilanz von über 10 Mio Euro haben. Somit wird deutlich, dass für Finanzunternehmen bedeutend strengere Schwellenwerte gelten.

Bis DORA ab dem 17.1.2025 anzuwenden ist, muss eine Vielzahl von sekundärrechtlichen Vorschriften ausgearbeitet werden, die detaillierte, technische Regeln für die wesentlichen Bestimmungen von DORA enthalten werden. Für von DORA betroffene Finanzunternehmen wird die Prüfung, welche konkreten Anforderungen – abhängig von der eigenen Unternehmensgröße und ausgeübten Tätigkeit – zu beachten und somit umzusetzen sind, eine der großen Herausforderungen dieses neuen EU-Regelwerks. Zwar sieht DORA mit Verweis auf den Grundsatz der Verhältnismäßigkeit wesentliche Erleichterungen einerseits für bestimmte in Art 16 DORA angeführte „kleinere Unternehmen“, die einen vereinfachten IKT-Risikomanagementrahmen verwenden können, und andererseits generell für Kleinstunternehmen bestimmte Ausnahmen vom komplexen IKT-Risikomanagementrahmen vor, jedoch wird abzuwarten sein, wie aufwendig (in zeitlicher und kostenmäßiger Sicht) die Einhaltung der von den ESA durch RTS noch zu konkretisierenden Vorgaben für diese und alle anderen größeren Finanzunternehmen sein wird.

Autor:
Mag. Hakan Ündemir, Bakk., LL.M., MBA, Referent des Fachverbands Finanzdienstleister (WKÖ)