Sie wollen mehr Informationen?
Dann schauen Sie auch in unsere **Wissensdatenbank**!
www.wko.at/wissensdatenbank oder
www.wko.at/wdb

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

Datum
29.8.2025

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 dem vom österreichischen Parlament erlassenen DORA-VG[1] wurde die FMA als zuständige Behörde für den Vollzug der DORA benannt.

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-Drittdienstleister in den Anwendungsbereich der Finanzdienstleistungsaufsicht einbezogen werden. Betroffene Unternehmen müssen DORA ab 17.1.2025 anwenden. Durch DORA werden betroffene Finanzunternehmen und IKT-Drittdienstleister 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 (ESAs)[2] noch zu erstellenden Leitlinien und technischen Regulierungs- und Durchführungsstandards (RTS und ITS). 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,

[1] Bundesgesetz über das Wirksamwerden der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA-Vollzugsgesetz – DORA-VG), BGBl I 112/2024.
[2] Die Europäische Bankenaufsichtsbehörde (EBA), die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) und die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA).

werden diese Unternehmen dazu verpflichtet, zahlreiche Maßnahmen zu ergreifen und Vorgänge zu beachten:

- Implementierung eines IKT-Risikomanagementrahmens und Business Continuity Management (Art 5 bis 15 DORA);
- Berichterstattung zu IKT-Vorfällen (Art 17 bis 20 DORA);
- Prüfung der digitalen Betriebsstabilität (mit Durchführung von Penetrationstests (Art 21 bis 27 DORA));
- Steuerung und Überwachung von IKT-Drittdienstleister-Risiken (Art 28 bis 36 DORA);
- Informationsaustausch zwischen den betroffenen Unternehmen (Art 40 DORA).

Um hierzu verpflichtete Unternehmen zu unterstützen, stellen Aufsichtsbehörden regelmäßig aktualisierte Informationen zur Anwendung von DORA zur Verfügung:

- Informationsseite der FMA[3]
- Informationsseite der BaFin[4]
- Informationsseite der ESMA[5]
- Informationsseite der EBA[6]
- Informationsseite der EIOPA[7]

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[8] und Versicherungs- und Rückversicherungsunternehmen sind das unter anderem folgende Finanzunternehmen:

- Wertpapierfirmen, wobei Wertpapierdienstleistungsunternehmen vom Anwendungsbereich ausgenommen sind[9];
- Zahlungs- und E-Geldinstitute (inkl Kontoinformationsdienstleister)[10];
- 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[11];
- Schwarmfinanzdienstleister (nicht aber Crowdinvesting-Plattformen mit einer Gewerbeberechtigung als Gewerblicher Vermögensberater)[12];

[3] https://www.fma.gv.at/querschnittsthemen/dora.
[4] https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html.
[5] https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora.
[6] https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act.
[7] https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.
[8] Anzumerken ist, dass mit § 3 DORA-VG der Anwendungsbereich der DORA auf alle Kreditinstitute gemäß § 1 Abs 1 BWG erweitert wurde.
[9] Art 2 Abs 1 lit e DORA; siehe zu der Ausnahme von Wertpapierdienstleistungsunternehmen Art 2 Abs 3 lit d DORA.
[10] Art 2 Abs 1 lit b DORA, wobei auch von der PSD2 ausgenommene Zahlungsinstitute vom Anwendungsbereich umfasst sind.
[11] Art 2 Abs 1 lit k DORA; registrierte AIFM sind nach Art 2 Abs 3 DORA ausgenommen.
[12] Art 2 Abs 1 lit s DORA.

- Versicherungsvermittler, Rückversicherungsvermittler sowie Versicherungsvermittler in Nebentätigkeit.[13]

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.[14] Somit werden nur solche Unternehmen mit 250 oder mehr Beschäftigten und Jahresumsatz 50 Mio Euro und/oder Jahresbilanzsumme 43 Mio Euro von DORA erfasst. Daher fallen insbesondere **Gewerbliche Vermögensberater** (bei der Kreditvermittlung, der Wertpapiervermittlung sowie im Veranlagungsbereich) nicht in den Anwendungsbereich von DORA.[15] 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. Hinsichtlich der Umsatzerlöse und Mitarbeiteranzahl ist dabei aus Sicht des Fachverbands lediglich auf die Umsatzerlöse und Mitarbeiter abzustellen, welche schlussendlich der Versicherungsvermittlung in Nebentätigkeit zuordenbar sind. Sollten Leasingunternehmen aber bspw in der Konzernstruktur eines Kreditinstituts eingebunden sein, ist die Anwendbarkeit von DORA gesondert zu prüfen.

In Annex 1 wird die mögliche Betroffenheit der Berufsgruppen der Finanzdienstleister dargestellt.

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.[16] 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).[17] 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

[13] Art 2 Abs 1 lit o DORA.
[14] 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.
[15] Zu beachten ist, dass die von DORA betroffenen Finanzunternehmen für vertraglich gebundene Vermittler oder Wertpapiervermittler beim Risikomanagementrahmen den Zugang zu Daten des Unternehmens dahingehend regeln müssen, dass die Authentizität, Integrität und Vertraulichkeit von Daten aufrechterhalten wird.
[16] Art 4 Abs 1 DORA.
[17] Siehe dazu im Detail unter Punkt 11.

Grundsatz der Verhältnismäßigkeit vorgesehen, dass sie einem vereinfachten IKT-Risikomanagementrahmen unterworfen werden.[18]

3. Konkretisierung der DORA-Vorgaben durch die ESAs

Fragen
5.) Welche RTS, ITS und Leitfäden wurden von den ESAs erarbeitet?

Die Verordnung trägt den ESAs, wie eingangs erwähnt, an mehreren Stellen auf, RTS, ITS und Leitfäden zu erarbeiten, die bei der Umsetzung durch die betroffenen Finanzunternehmen zusätzlich zu berücksichtigen sein werden.

Die ESAs haben am 17.1.2024 die erste Tranche und am 17.7.2024 die zweite Tranche an RTS, ITS und Leitlinien (als Entwürfe) veröffentlicht, wodurch das DORA-Rahmenwerk sehr umfangreich wurde. Der Inhalt ausgewählter Rechtsakte und des DORA-Vollzugsgesetzes wird im Folgenden dargestellt.

Die erste Tranche der Rechtsakte umfasst:

- RTS zur Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und des vereinfachten IKT-Risikomanagementrahmens (**RTS IKT-RM**[19]; Art 15 und Art 16 Abs 3 DORA);
- RTS zur Spezifizierung des detaillierten Inhalts der Leitlinie für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden (**RTS TPPol**[20]; Art 28 Abs 10 DORA);
- RTS zur Festlegung der Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen, der Wesentlichkeitsschwellen und der Einzelheiten von Meldungen schwerwiegender Vorfälle (**RTS Class**[21]; Art 18 Abs 4 DORA);
- Delegierter Rechtsakt zu den Kriterien zur Festlegung der Kriterien für die Einstufung von IKT-Drittdienstleistern als für Finanzunternehmen kritisch (Art 31 Abs 6 DORA);[22]
- ITS zur Erstellung einer Standardvorlage für das Informationsregister (**ITS Reg**[23]; Art 28 Abs 9 DORA);
- Delegierter Rechtsakt zur Festlegung der Höhe der von der federführenden Überwachungsbehörde bei kritischen IKT-Drittdienstleistern zu erhebenden Überwachungsgebühren und der Art und Weise der Entrichtung dieser Gebühren (Art 43 Abs 2 DORA).[24]

Die zweite Tranche der Rechtsakte umfasst:

[18] Siehe dazu Punkt 3.
[19] DelVO 2024/1774 der Europäischen Kommission vom 13.3.2024, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401774.
[20] DelVO 2024/1773 der Europäischen Kommission vom 13.3.2024, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401773.
[21] DelVO 2024/1772 der Europäischen Kommission vom 13.3.2024, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401772.
[22] DelVO 2024/1502 der Europäischen Kommission vom 22.2.2024, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401502.
[23] DelVO 2024/2956 der Europäischen Kommission vom 29.11.2024, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202402956.
[24] DelVO 2024/1505 der Europäischen Kommission vom 22.2.2024, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401774.

- RTS zu Threat Led Penetration Testing (**RTS TLPT**; Art 26 Abs 11 DORA);[25]
- RTS zur Spezifizierung von Elementen bei der Untervergabe von kritischen oder wichtigen Funktionen (**RTS-E SUB**, Art 30 Abs 5 DORA);[26]
- RTS zur Festlegung des Inhalts der Meldung schwerwiegender IKT-Vorfälle und erheblicher Cyberbedrohungen sowie zur Bestimmung der Fristen der Meldung von schwerwiegenden Vorfällen (**RTS INC-REP**; Art 20 lit a) DORA) und ITS zur Festlegung von Standardformularen, Vorlagen und Verfahren solcher Vorfälle (Art 20 lit b) DORA);[27]
- Leitlinien zu den geschätzten aggregierten Kosten und Verlusten durch schwerwiegende IKT-bezogene Vorfälle (Art 11 Abs 11 DORA);[28]
- Leitlinien für die Zusammenarbeit bei der Überwachung und den Informationsaustausch zwischen den ESAs und den zuständigen Behörden (Art 32 Abs 7 DORA);[29]
- RTS zur Harmonisierung der Voraussetzungen für die Durchführung der Überwachungstätigkeiten (Art 41 DORA);[30]
- RTS zu der Zusammensetzung der gemeinsamen Prüfungsteams (Art 41 Abs 1 lit c).[31]

4. IKT-Risikomanagement, Berichterstattung und Testung

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

a) Inhalt des IKT-Risikomanagementrahmens

DORA sieht vor, dass Finanzunternehmen über einen umfassenden Governance- und Kontrollrahmen für ein wirksames und umsichtiges Management von IKT-Risiken verfügen müssen.[32] 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.[33] 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.[34]

[25] DelVO 2025/1190 der Europäischen Kommission vom 13.2.2025 abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202501190.
[26] DelVO 2025/532 der Europäischen Kommission vom 24.3.2025 abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202500532.
[27] DelVO 2025/302 der Europäischen Kommission vom 23.10.2024, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202500302.
[28] JC/GL/2024/34, abrufbar unter https://www.eba.europa.eu/sites/default/files/2025-03/48958acb-1c6d-40f0-9784-961713759972/JC%202024-34_Draft%20final%20report%20GL%20on%20costs%20and%20losses_for%20translation_DE_COR2.pdf.
[29] JC/GL/2024/36 abrufbar unter https://www.esma.europa.eu/sites/default/files/2024-11/JC-GL-2024-36_Guidelines_on_DORA_oversight_cooperation_DE.pdf.
[30] DelVO 2025/295 der Europäischen Kommission vom 24.10.2024 abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202500295.
[31] DelVO 2025/420 der Europäischen Kommission vom 16.12.2024, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202500420.
[32] Art 5 Abs 1 DORA.
[33] Art 6 Abs 2 DORA.
[34] Vgl Art 5 Abs 2 DORA.

Diese umfassen insbesondere

i. die Einführung von Leitlinien um hohe Standards in Bezug auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten aufrechtzuhalten;
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.[35]

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).[36] Den zuständigen Behörden sind auf Anfrage vollständige und aktuelle Informationen über IKT-Risiken und ihren IKT-Risikomanagementrahmen vorzulegen.[37]

Zum Schutz vor und zur Vorbeugung und Erkennung von IKT-Risiken sowie als Reaktion und zur Wiederherstellung sind als Teil des IKT-Risikomanagementrahmens 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.[38] 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.[39] 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.[40] Finanzunternehmen werden auch dazu verpflichtet, Richtlinien und Verfahren zur Datensicherung als auch zu Wiedergewinnungs- und Wiederherstellungsverfahren und -methoden zu entwickeln und zu dokumentieren.[41] Ferner müssen Finanzunternehmen über Kapazitäten und Personal verfügen, um Informationen über Schwachstellen und

[35] Vgl Art 5 Abs 2 DORA.
[36] Art 6 Abs 2 DORA.
[37] Art 6 Abs 3 DORA.
[38] Art 11 Abs 2 DORA.
[39] Art 11 Abs 5 DORA.
[40] Art 11 Abs 7 DORA.
[41] Art 12 Abs 1 DORA.

Cyberbedrohungen, IKT-bezogene Vorfälle (insbesondere Cyberangriffe) zu sammeln, um die wahrscheinlichen Auswirkungen auf die digitale operationale Resilienz zu untersuchen.[42] Zudem sind obligatorische Schulungen zur digitalen operationalen Resilienz für alle Mitarbeiter und Führungskräfte vorgesehen.[43] So sind insbesondere in der IKT-Geschäftsfortführungsleitlinie die Vorgaben für die Wiederherstellungszeit und die Wiederherstellungspunkte zu regeln, zB haben zentrale Gegenparteien für ihre kritischen Funktionen eine Wiederherstellungszeit von maximal 2 Stunden vorzusehen.[44] Je nach Geschäftsmodell werden Finanzunternehmen zu beurteilen haben, welche Ausfallzeit und Wiederherstellungsmaßnahmen bzw. Vorkehrungen notwendig werden. So sind bspw. bei einem Unternehmen, welches zeitkritische Aufträge durchführt, bei einem Ausfall von kritischen IKT-Assets Vorkehrungen dahingehend zu treffen, dass ein Ausfall so kurz wie möglich dauert.

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.[45]

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.[46] DORA sieht kein Verbot der Auslagerung von IKT-Risikomanagementfunktionen vor. Diesbezüglich weist Art 6 Abs 10 DORA explizit auf die Auslagerbarkeit der „Überprüfung der Einhaltung der Anforderungen für das IKT-Risikomanagement“ im Einklang mit den sektorspezifischen Rechtsvorschriften der Union und der Mitgliedstaaten an gruppeninterne oder externe Unternehmen hin.

Durch die als DelVO (EU) 2024/1774 der Kommission veröffentlichten RTS („**RTS IKT-RM**“) erfolgt eine Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement (Art 15) und des vereinfachten IKT-RMR (Art 16 Abs 3). Hinsichtlich der RTS gemäß Art 15 werden unter "Titel II - Weitere Harmonisierung von Tools, Methoden, Prozessen und Richtlinien für IKT-Risikomanagement" u. a. folgende Anforderungsbereiche konkretisiert: (i) IKT-Sicherheitsstrategien, -verfahren, -protokolle und -instrumente; (ii) Personalpolitik und Zugangs-/Zugriffskontrollen; (iii) Erkennung von und Reaktion auf IKT-bezogene Vorfälle; (iv) IKT-Betriebskontinuitätsmanagement und (v) Bericht über die Überprüfung des IKT-RMR.

b) Vereinfachter IKT-Risikomanagementrahmen für Klasse 3-Wertpapierfirmen

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

[42] Art 13 Abs 1 DORA.
[43] Art 13 Abs 6 DORA.
[44] Art 24 Abs 2 DelVO (EU) 2024/1774 der Europäischen Kommission vom 13.3.2024.
[45] Art 14 Abs 1 DORA.
[46] Art 6 Abs 4 DORA.

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.[47]

Für kleine und nicht verflochtene Wertpapierfirmen und andere gemäß Art 16 Abs 1 DORA betroffene Unternehmen werden die Anforderungen in den RTS IKT-RM[48] unter "Titel III – Vereinfachter IKT-Risikomanagementrahmen" zur Umsetzung eines vereinfachten IKT-RMR gemäß Art 16 DORA beschrieben. Der vereinfachte IKT-RMR umfasst im Groben dieselben Anforderungen wie an den regulären IKT-RMR (dh Identifikation von IKT-Assets, Schutz- und Präventionsmaßnahmen, Business Continuity Management, Testen der Resilienz), wobei punktuelle Vereinfachungen anwendbar sind.

Auffallend ist, dass die Anforderungen an den vereinfachten RMR, welchen Klasse 3-Wertpapierfirmen zu beachten haben, nicht wesentlich geringfügiger sind. Die FMA hat über den Sommer einen Aufsichtsschwerpunkt zur Digitalisierung 2024 durchgeführt, der auch eine DORA-Gap-Analyse zum (vereinfachten) IKT-RMR zum Gegenstand hatte, bei welcher der Umsetzungsstand beim betroffenen Finanzunternehmen hinsichtlich des IKT-RMR erhoben wurde. Die Checkliste für den vereinfachten IKT-RMR war nur um ca. 20% kürzer als jene für den regulären IKR-RMR. Erleichterungen gibt es zB bei den Anforderungen an die Kommunikation und dahingehend, dass bspw. keine unabhängige IKT-Risiko-Kontrollfunktion einzurichten und kein Krisenkommunikationsbeauftragter zu benennen ist. Essenziell für den RMR und der damit verbunden Maßnahmen ist die Identifikation von IKT-Assets, um eine entsprechende Risikoanalyse durchführen zu können. Je nach Komplexität der vorhandenen IT-Infrastruktur und abhängig vom Geschäftsmodells des Finanzunternehmens sind die erforderlichen Schutz- und Präventionsmaßnahmen zu setzen als auch das Business Continuity Management festzulegen.

[47] Art 16 DORA.
[48] Art 28 bis 41 DelVO (EU) 2024/1774 der Europäischen Kommission vom 13.3.2024.

c) Berichterstattung und Testung

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.[49] 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.[50]

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.[51]

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.[52]

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.[53] 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.[54] 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.[55] 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.[56] Für Dokumentationszwecke müssen entsprechende Inventare über

[49] Art 6 Abs 5 DORA.
[50] Art 6 Abs 6 DORA (nicht anwendbar auf Kleinstunternehmen); Art 28 Abs 5 RTS IKT-RMR (anwendbar auf Klasse 3-Wertpapierfirmen).
[51] Art 6 Abs 6 DORA; Art 28 Abs 3 RTS IKT-RMS (anwendbar auf Klasse 3-Wertpapierfirmen).
[52] Art 8 Abs 1 DORA.
[53] Art 8 Abs 2 DORA.
[54] Art 8 Abs 3 DORA.
[55] Art 8 Abs 4 DORA.
[56] Art 8 Abs 5 DORA.

genannte Informations- und IKT-Assets geführt werden, die regelmäßig sowie bei einer wesentlichen Änderung zu aktualisieren sind.[57]

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

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

Künftig sind schwerwiegende IKT-bezogene Vorfälle zu melden.[58] Die Mitgliedstaaten haben eine einzige nationale Behörde als zentrale Meldestelle zur Meldung von schwerwiegenden IKT-bezogenen Vorfällen zu benennen. Mit dem DORA-VG wurde die FMA als zuständige Behörde festgelegt. 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.[59]

Die RTS Class[60] regelt die Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen, der Wesentlichkeitsschwellen und der Einzelheiten von Meldungen schwerwiegender Vorfälle. Die RTS unterscheiden hierzu, u. a. basierend auf (i) der Anzahl betroffener Kunden, Finanzpartner und Transaktionen, (ii) Auswirkungen auf die Reputation, (iii) der Dauer und Ausfallzeiten von Diensten, (iv) der geografischen Ausbreitung, (v) dem Vorliegen von Datenverlusten, (vi) der Kritikalität betroffener Dienste, (vii) den wirtschaftlichen Auswirkungen zwischen "schwerwiegenden" und "normalen" IKT-bezogenen Vorfällen. Die Schwelle für das Kriterium „Dauer und Ausfallzeiten“ ist zB erreicht, wenn der Vorfall mehr als 24 Stunden dauert oder die Ausfallzeiten bei IKT-Diensten zur Unterstützung kritischer oder wichtiger Funktionen mehr als 2 Stunden betragen. Die Wesentlichkeitsschwelle für das Kriterium „wirtschaftliche Auswirkungen“ ist bspw. erreicht, wenn die Kosten und Verluste durch den Vorfall 100.000,- Euro (wahrscheinlich) übersteigen.[61]

Ein IKT-bezogener Vorfall wird als schwerwiegend klassifiziert, wenn kritische Dienste beeinträchtigt sind und eine der folgenden beiden Bedingungen erfüllt ist:

(i) es findet ein böswilliger und unbefugter Zugriff auf Netzwerk- und Informationssysteme statt und dieser Zugriff kann zu Verlusten von Daten führen;
(ii) zwei oder mehr der Wesentlichkeitsschwellen bzgl. der folgenden Kriterien sind erreicht: (a) betroffene Kunden, finanzielle Gegenparteien oder Transaktionen; (b) Reputationsschaden; (c) Dauer und Ausfallzeiten; (d) geografische Ausbreitung; (e) Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten; (f) wirtschaftliche Auswirkungen.[62]

Zudem können wiederholte Vorfälle, welche für sich einzeln betrachtet nicht die Kriterien für einen schwerwiegenden IKT-bezogenen Vorfall erfüllen, bei kumulierter Betrachtungsweise als schwerwiegende Vorfälle meldepflichtig werden: (i) sie sind innerhalb von sechs Monaten mindestens zwei Mal aufgetreten; (ii) sie haben dieselbe offensichtliche Ursache; (iii) sie

[57] Art 8 Abs 6 DORA.
[58] Art 19 Abs 1 DORA.
[59] Art 17 Abs 1 DORA.
[60] DelVO (EU) 2024/1772 der Europäischen Kommission vom 13.3.2024.
[61] Art 9 Abs 1 bis 6 DelVO (EU) 2024/1772 der Europäischen Kommission vom 13.3.2024.
[62] Art 8 Abs 1 (EU) 2024/1772 der Europäischen Kommission vom 13.3.2024.

erfüllen zusammengenommen die festgelegten Kriterien für die Betrachtung als schwerwiegender Vorfall.[63]

Die RTS INC-REP[64] konkretisieren die Anforderungen zur Meldung schwerwiegender IKT-Vorfälle sowie erheblicher Cyberbedrohungen. Konkretisiert werden insbesondere allgemeine Meldeerfordernisse, Inhalte der Meldung über schwerwiegende IKT-Vorfälle, Fristen für die Erst-, Zwischen- und Abschlussmeldung als auch Inhalte der Meldung erheblicher Cyberbedrohungen. Annex I enthält ca. 100 Datenfelder (gesamt für Erst-, Zwischen- und Abschlussmeldung), die u. a. folgende Themen abfragen: Allgemeine Informationen über das Finanzunternehmen, Beschreibung des Vorfalls, Auswirkungen, Vorfallbehandlung, Ursachen, Präventionsmaßnahmen, etc.[65]

Die Erstmeldung ist so früh wie möglich innerhalb von 4 Stunden ab der Klassifizierung des Vorfalls als schwerwiegend, jedoch nicht später als 24 Stunden ab der Kenntnisnahme vom Vorfall vorzunehmen.[66] Ein Zwischenbericht ist spätestens innerhalb von 72 Stunden nach Übermittlung der ersten Meldung vorzulegen, auch wenn der Vorfall nicht behoben werden konnte, oder früher bei Wiederherstellung des normalen Geschäftsbetriebs. Die Finanzunternehmen legen in jedem Fall nach Aufnahme der regulären Tätigkeit unverzüglich einen aktualisierten Zwischenbericht vor.[67] Der Abschlussbericht ist spätestens einen Monat nach Vorlage des letzten aktualisierten Zwischenberichts vorzulegen.[68]

Die Meldung an die FMA hat über die FMA Incoming-Plattform durch Verwendung der Meldeformulare gemäß Annex I der RTS INC-REP[69] zu erfolgen.

Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, haben gemäß Art 11 Abs 10 DORA den zuständigen Behörden auf Anfrage die geschätzten aggregierten jährlichen Kosten und Verluste, die durch schwerwiegende IKT-bezogene Vorfälle verursacht wurden, zu melden. Durch diese gemäß Art 11 Abs 11 DORA mandatierten Leitlinien werden die Anforderungen an die geforderte Schätzung der aggregierten jährlichen Kosten und Verluste konkretisiert. Der Referenzzeitraum ist das Geschäftsjahr und als Grundlage für die Schätzungen sind die geprüften Jahresabschlüsse heranzuziehen. Einzubeziehen sind IKT-Vorfälle, die als schwerwiegend klassifiziert wurden und für die eine Abschlussmeldung erfolgt ist. Es ist auch eine Aufschlüsselung von bestimmten Kostenpositionen vorzunehmen.

Zudem ist vorgesehen, dass die ESAs 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**

[63] Art 8 Abs 2 DelVO (EU) 2024/1772 der Europäischen Kommission vom 13.3.2024.
[64] DelVO 2025/302 der Europäischen Kommission vom 23.10.2024, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202500302.
[65] DelVO 2025/302 der Europäischen Kommission vom 23.10.2024, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202500302.
[66] Art 6 Abs 1 lit a der RTS INC-REP, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202500302.
[67] Art 6 Abs 1 lit b der RTS INC-REP, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202500302.
[68] Art 6 Abs 1 lit c der RTS INC-REP, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202500302.
[69] DelVO 2025/302 der Europäischen Kommission vom 23.10.2024, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202500302.

einheitlichen EU-Plattform für die Meldung schwerwiegender IKT-bezogener Vorfälle durch Finanzunternehmen evaluiert wird.[70]

6. Prüfung der digitalen Betriebsstabilität

Fragen
11.) 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.[71] 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.[72] IKT-Systeme und -Anwendungen, die kritische oder wichtige Funktionen unterstützen, sind mindestens einmal jährlich auf operationale Resilienz zu testen.[73] 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**.[74]

Die RTS zu TLPT[75] legen fest, welche Finanzunternehmen zur Durchführung von Threat-Led Penetration Testing (TLPT) alle drei Jahre verpflichtet sind und konkretisieren die Anforderungen an den durchzuführenden TLPT. Von den ESAs wird ein zweistufiger Ansatz zur Identifizierung von Finanzunternehmen für den TLPT wie folgt vorgeschlagen: (i) Erfüllung bestimmter Kriterien und Schwellenwerte (global oder lokal systemrelevante Kreditinstitute; Zahlungsinstitute mit Zahlungstransaktionen von über 150 Mrd. Euro in den letzten zwei Jahren; Zentralverwahrer; zentrale Gegenparteien etc.)[76] und (ii) Flexibilität der zuständigen Behörde, weitere Finanzunternehmen als Verpflichtete zu identifizieren bzw. diese bei fehlender Systemrelevanz und IKT-Reife von der Verpflichtung zu TLPT auszunehmen.[77] Das DORA-VG enthält Vorgaben für die Zusammenarbeit zwischen der FMA und der österreichischen Nationalbank (OeNB) im Rahmen der Durchführung erweiterter Tests (TLPT) gemäß Art 26 DORA. Aus der Sicht des Fachverbands gibt es in Bezug auf Rechtsträger gemäß § 1 Abs 1 Z 4 (Wertpapierfirmen), Z 5 (Anbieter von Kryptowerte-Dienstleistungen gemäß MiCA-VO), Z 10 (konzessionierte AIFM) und Z 15 (Schwarmfinanzierungsdienstleister) DORA-VG derzeit in Österreich keine Rechtsträger, die – unabhängig vom vorausgesetzten großen IKT-Reifegrad - als „systemrelevante Finanzunternehmen“ anzusehen sind. Gemäß Art 26 Abs 1 sind Klasse 3-Wertpapierfirmen und Kleinstunternehmen jedenfalls von der Durchführung von TLPT ausgenommen.

[70] Art 21 Abs 1 DORA.
[71] Art 24 Abs 1 DORA.
[72] Art 24 Abs 4 DORA.
[73] Art 24 Abs 4 DORA.
[74] Art 25 Abs 1 DORA.
[75] Finaler Entwurf der RTS zu TLPT abrufbar unter https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-29_-_Final_report_DORA_RTS_on_TLPT.pdf.
[76] Art 2 Abs 1 lit b Finaler Entwurf der RTS zu TLPT, abrufbar unter https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-29_-_Final_report_DORA_RTS_on_TLPT.pdf.
[77] Art 2 Abs 4 Finaler Entwurf der RTS zu TLPT, abrufbar unter https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-29_-_Final_report_DORA_RTS_on_TLPT.pdf.

7. Steuerung von IKT-Drittdienstleister-Risiken

Fragen
12.) Was ist bei vertraglichen Vereinbarungen mit IKT-Drittdienstleistern zu beachten?
13.) 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.[78] 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.[79] Dazu ist ein **Informationsregister** mit allen vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die Dritte bereitstellen, zu führen.[80]

DORA sieht vor, dass vertragliche Vereinbarungen nur abgeschlossen werden dürfen, wenn angemessene Standards für die 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.[81] Aus Sicht des Fachverbands haben die ESAs für jene Unternehmen, die sie in die Liste der kritischen IKT-Drittdienstleister auf Unionsebene aufnehmen, zu beurteilen, ob diese die aktuellsten und höchsten Qualitätsstands für die Informationssicherheit anwenden. Dies ergibt sich insbesondere aus Art 33 Abs 2 DORA, welcher vorsieht, dass die federführende Überwachungsbehörde zu bewerten hat, ob jeder (in die Liste aufgenommene) kritische IKT-Drittdienstleister über umfassende, fundierte und wirksame Vorschriften, Verfahren, Mechanismen und Vorkehrungen für das Management der IKT-Risiken verfügt, die er für Finanzunternehmen mit sich bringen kann.

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.[82] 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.[83]

Art 30 Abs 4 DORA sieht vor, dass Finanzunternehmen und IKT-Drittdienstleister bei der Aushandlung vertraglicher Vereinbarungen die Verwendung von Standardvertragsklauseln, die

[78] Art 28 Abs 1 DORA.
[79] Art 28 Abs 2 DORA.
[80] Art 28 Abs 3 DORA.
[81] Art 28 Abs 5 DORA.
[82] Art 28 Abs 7 DORA.
[83] Art 28 Abs 8 DORA.

von Behörden für bestimmte Dienstleistungen entwickelt wurden, erwägen. In der Verordnung ist kein direktes Mandat an die ESAs zur Erarbeitung von Entwürfen technischer Regulierungsstandards enthalten und dementsprechend auch keine Frist. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat eine Aufsichtsmitteilung mit Umsetzungshinweisen zu DORA (Stand: Juni 2024)[84] veröffentlicht. Darin teilt die BaFin insbesondere mit, dass aktuell allerdings keine Standardvertragsklauseln vorliegen, und beaufsichtigte Unternehmen daher nicht die Veröffentlichung von Standardvertragsklauseln zur Umsetzung der Mindestvertragsinhalte abwarten sollten. Es ist somit wohl nicht damit zu rechnen, dass die Aufsichtsbehörden Standardvertragsklauseln zur Verfügung stellen werden. Die BaFin hat jedoch ein Excel-Dokument zu Mindestvertragsinhalten veröffentlicht, die eine Übersicht der Vertragsinhalte, die gemäß DORA bzw. den RTS TPPol[85] und RTS-E SUB[86] verpflichtend zu vereinbaren sind, enthält.[87] Für die Anpassung der bestehenden vertraglichen Vereinbarungen mit IKT-Drittdienstleistern ist keine Übergangsfrist vorgesehen.

In diesem Zusammenhang weist aber Art 3 Abs 1 RTS TPPol[88] darauf hin, dass es einen dokumentierten Zeitplan für die Implementierung geben soll und die Umsetzung rechtzeitig erfolgen soll. Eine Anpassung der vertraglichen Vereinbarungen soll demnach sobald als möglich vorgenommen werden. Die Anforderungen hinsichtlich der Vertragsbeziehung mit IKT-Drittdienstleistern betreffen die Überwachung und Verwaltung vertraglicher Vereinbarungen sowie Ausstiegsstrategien einschließlich Kündigungsmöglichkeiten.

Sollte sich bei Vertragsverhandlungen mit einem IKT-Drittdienstleister herausstellen, dass dieser nicht bereit ist, die gemäß DORA bzw. den jeweiligen RTS vorgesehenen Vertragsbestimmungen zu akzeptieren, hat ein Finanzunternehmen alternative IKT-Drittdienstleister zu finden, die dazu bereit sind. Eine entsprechende Dokumentation samt realistischen Implementierungsplan hat in diesem Fall zu erfolgen, um allfällige Sanktionen durch Aufsichtsbehörden zu vermeiden. Kritische IKT-Drittdienstleister werden von den ESAs beaufsichtigt werden, sodass davon auszugehen ist, dass diese zeitnah die Vorgaben betreffend Standardvertragsklauseln erfüllen werden. Bei kleineren Anbietern, die nicht viele Finanzunternehmen als Kunden haben, kann dieser Prozess wohl schwerfälliger werden.

RTS-E SUB[89] enthält ca. 20 Anforderungen bei der Untervergabe von kritischen oder wichtigen Funktionen, die in IKT-Vereinbarungen aufgenommen werden müssen. Von Finanzunternehmen wird bspw. verlangt „die Subunternehmerbedingungen entlang der gesamten IKT-Subunternehmerkette“ zu überwachen. Es bestehen diesbezüglich Bedenken hinsichtlich der praktischen Durchführbarkeit einer Überwachung der gesamten Unterauftragskette, insbesondere angesichts der Tatsache, dass dies auch eine Überprüfung der mit diesen Unterauftragnehmern abgeschlossenen Vertragsdokumente umfassen würde.

[84] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Aufsichtsmitteilung Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand: Juni 2024; abrufbar unter https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Aufsichtsmitteilung/dl_2024_07_08_Aufsichtsmitteilung_Umsetzungshinweise_DORA.html.
[85] DelVO (EU) 2024/1773 der Europäischen Kommission vom 13.3.2024.
[86] DelVO 2025/532 der Europäischen Kommission vom 24.3.2025, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202500532.
[87] Checkliste der BaFin zu Vertragsbestimmungen (Fassung: Juli 2025) verfügbar unter https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/dl_Mindestvertragsinhalte_DORA_DE_EN.html?nn=19659934.
[88] DelVO (EU) 2024/1773 der Europäischen Kommission vom 13.3.2024.
[89] DelVO 2025/532 der Europäischen Kommission vom 24.3.2025, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202500532.

Die ITS Reg[90] verpflichtet Finanzunternehmen im Rahmen ihres IKT-RMR, ein Informationsregister, das alle vertraglichen Vereinbarungen über die Nutzung von durch IKT-Drittdienstleistern bereitgestellten IKT-Dienstleistungen umfasst, zu führen und zu aktualisieren. Diese ITS liefern Hinweise und Standardvorlagen zur Erfassung von IKT-Dienstleistungen. Im Wesentlichen handelt es sich dabei im Ergebnis um eine Erweiterung bestehender Auslagerungsregister, wobei die neuen Dokumentationspflichten alle bezogenen IKT-Drittdienstleistungen umfassen. Vorgesehen ist, dass Finanzunternehmen Informationen zur IKT-Lieferkette und IKT-Subdienstleistern nur zu melden haben, wenn die bereitgestellte IKT-Dienstleistung eine kritische oder wichtige Funktion unterstützt. 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.[91] Den zuständigen Behörden ist weiters mindestens einmal jährlich ein Bericht zur Anzahl neuer Vereinbarungen und den Kategorien von IKT-Drittdienstleistern zu erstatten.[92]

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.[93] Die zuständige Behörde kann das Finanzunternehmen dazu zwingen, Verträge mit IKT-Drittdienstleistern vorübergehend teilweise oder vollständig auszusetzen, bis die Risiken beseitigt sind.[94] Finanzunternehmen werden ferner dazu verpflichtet zeitnah **über jede geplante vertragliche Vereinbarung** über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen an die zuständige Behörde zu melden.[95]

In einer Arbeitsgruppe des Kompetenzzentrum Sicheres Österreich (KSÖ) (gemeinsam mit Teilnehmern aus der Finanzwirtschaft und einigen Fachverbänden) wurde eine Mustervorlage mit den gesetzlichen Mindestanforderungen zwischen Finanzunternehmen und IKT-Dienstleistern, die keine „kritischen oder wichtigen" Funktionen unterstützen zu den DORA-Verpflichtungen, ausgearbeitet. Diese Mustervorlage[96] kann kostenlos zur kommerziellen Nutzung verwendet werden.

Die KSÖ-Arbeitsgruppe plant auch die Erstellung (i) einer umfangreicheren Mustervorlage für IKT-Drittdienstleistungen, die kritische oder wichtige Funktionen unterstützen, und (ii) eines IT-Security-Fragebogens, welcher an die IKT-Drittdienstleister gerichtet ist, zur Beurteilung der Geeignetheit des IKT-Drittdienstleisters durch Finanzunternehmen (diese Notwendigkeit ergibt sich aus Artikel 28 Abs 4 lit d) DORA, wonach Finanzunternehmen bei potenziellen IKT-Drittdienstleistern der gebotenen Sorgfaltspflicht nachzukommen und während des gesamten Auswahl- und Bewertungsprozesses sicherzustellen haben, dass der IKT-Drittdienstleister geeignet ist). Der KSÖ wird den IT-Security Fragebogens im Herbst 2025 präsentieren.

[90] DelVO 2024/2956 der Europäischen Kommission vom 29.11.2024, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202402956.
[91] Art 28 Abs 4 DORA.
[92] Art 28 Abs 3 DORA.
[93] Art 28 Abs 3 DORA.
[94] Art 42 Abs 6 DORA.
[95] Art 28 Abs 3 DORA.
[96] Abrufbar unter https://www.wko.at/oe/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/it-dienstleistung/ikt-zusatzvereinbarung-dora. Diese Mustervorlage stellt lediglich eine Orientierungshilfe dar und kann davon abgewichen werden (insbesondere hinsichtlich der kommerziellen Punke).

8. Kritische IKT-Dienstleister und Aufsichtsrahmen

Fragen
14.) Wer ist ein kritischer IKT-Drittdienstleister?
15.) 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 ESAs erstellen, veröffentlichen und aktualisieren die Liste kritischer IKT-Drittdienstleister auf Unionsebene über den Gemeinsamen Ausschuss.[97] Die FMA teilt auf ihrer Homepage mit, dass die Veröffentlichung der kritischen IKT-Dienstleister, die der direkten Aufsicht der ESAs unterliegen werden, im zweiten Halbjahr 2025 erfolgen soll. Die betroffenen Finanzunternehmen mussten ihre Informationsregister bis spätestens 11.4.2025 mit dem Referenzdatum 30.3.2025 bei der FMA über die Incoming Plattform einmelden. Die FMA musste die aggregierten Informationen bis zum 30.04.2025 an die ESAs weiterleiten. Diese werden die Einstufung von IKT-Drittdienstleistern als kritisch vornehmen.

IKT- Drittdienstleister haben den Finanzunternehmen, für die sie Dienstleistungen erbringen, ihre Einstufung als kritischer IKT-Drittdienstleister mitzuteilen.[98] Zu beachten ist, 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.[99]

Der Gemeinsame Ausschuss richtet ein Überwachungsforum, welcher sich aus mehreren hochrangigen Vertretern von europäischen und nationalen Behörden zusammensetzt, ein. Eine der ESAs agiert nach in der Verordnung vorgesehenen Kriterien[100] 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.[101] 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.[102] 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

[97] Art 31 Abs 9 DORA.
[98] Art 31 Abs 5 DORA.
[99] Art 31 Abs 12 DORA.
[100] Vgl Art 31 Abs 1 DORA.
[101] Art 33 Abs 2 DORA.
[102] Art 33 Abs 4 DORA.

denen ein IKT-Drittdienstleister verpflichtet wurde.[103] Es ist davon auszugehen, dass die großen IT-Konzerne (Microsoft, Amazon, Alphabet (Google), Oracle, SAP etc.) und andere IKT-Drittdienstleister, die über entsprechende Marktpräsenz im Finanzbereich verfügen, als kritische IKT-Drittdienstleister qualifiziert werden. Durch die direkte Überwachung der kritischen IKT-Drittdienstleister durch die zuständigen Aufsichtsbehörden ist davon auszugehen, dass die vertraglichen Verhandlungen zwischen Finanzunternehmen und kritischen IKT-Drittdienstleistern hinsichtlich der wesentlichen Vertragsbestimmungen allenfalls einfacher verlaufen könnten.

9. Vereinbarungen über den Austausch von Informationen

Fragen
16.) 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 auf freiwilliger Basis 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
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.[104]

10. Beaufsichtigung und Durchsetzung durch Behörden

Fragen
17.) 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.[105] Zur wirksamen Anwendung von DORA in Österreich wurde das DORA-Vollzugsgesetz (DORA-VG) am 4.7.2024 vom Nationalrat beschlossen, welches am 17.1.2025 in Kraft treten wird. Durch das DORA-VG erfolgt insbesondere eine Klarstellung des Anwendungsbereichs von DORA in Bezug auf nationale Institute. Im DORA-VG wird die österreichische Finanzmarktaufsichtsbehörde (FMA) als zuständige Behörde festgelegt und werden der FMA die erforderlichen Aufsichts- und Sanktionsbefugnisse zugewiesen und näher konkretisiert. Für den Bereich der Versicherungsvermittlung oder den Bereich des

[103] 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.
[104] Art 45 Abs 1 DORA; siehe auch zB ErwGr 32 DORA.
[105] Art 46 DORA.

Leasinggeschäfts (Versicherungsvermittlung in Nebentätigkeit) ist mangels Regelung im DORA-VG aus unserer Sicht die Gewerbebehörde die zuständige Aufsichtsbehörde. Das DORA-VG enthält Vorgaben für die Zusammenarbeit zwischen der FMA und der österreichischen Nationalbank (OeNB) im Rahmen der Durchführung erweiterter Tests gemäß Art 26 DORA. Darüber hinaus sieht das DORA-VG Strafbestimmungen bei Verstößen gegen DORA sowohl für natürliche als auch juristische Personen vor. Für natürliche Personen sind Verwaltungsstrafen von bis zu 150.000,- Euro, für juristische Personen von bis zu 500.000,- Euro oder bis zu 1% des jährlichen Gesamtnettoumsatzes, je nachdem welcher Betrag höher ist, vorgesehen. Neben diesen Geldstrafen kann die FMA zudem die verhängten Verwaltungsstrafen und die davon betroffenen Unternehmen auf ihrer Website veröffentlichen (sog. "Naming & Shaming").

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.[106] Die Erleichterungen für Kleinstunternehmen sind insbesondere:

- Ausnahme von der Einrichtung einer Funktion, um die mit IKT-Drittdienstleistern über die Nutzung von IKT-Dienstleistungen geschlossenen Vereinbarungen zu überwachen[107];
- Ausnahme von der Übertragung der Zuständigkeit für das IKT-Management und der Überwachung des IKT-Risikos an eine Kontrollfunktion[108];
- Ausnahme von der Durchführung einer internen Revision durch Revisoren[109];
- keine Risikobewertung für wesentliche Änderungen der Netzwerk- und Informationssysteminfrastruktur und keine mindestens jährliche IKT-Risikobewertung für alle älteren IKT-Systeme[110];
- keine Implementierung von IKT-Reaktions- und Wiederherstellungsplänen als Teil des IKT-Risikomanagementrahmens[111];
- 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[112];
- keine Verpflichtung über ein Krisenmanagement zu verfügen, welches klare Verfahren für die Abwicklung interner und externer Krisenkommunikation festlegt[113];
- keine Meldung an die zuständigen Behörden, die geschätzten aggregierten jährlichen Kosten und Verluste, die durch schwerwiegende IKT-bezogene Vorfälle verursacht wurden[114];

[106] Vgl Punkt 2 zur Definition von Kleinstunternehmen. Für bestimmte Kleinunternehmen, die zugleich in Art 16 DORA angeführt sind, ist ein vereinfachter IKT-Risikomanagementrahmen anwendbar.
[107] Art 5 Abs 3 DORA.
[108] Art 6 Abs 4 DORA.
[109] Art 6 Abs 6 DORA.
[110] Art 8 Abs 3 DORA.
[111] Art 11 Abs 3 DORA.
[112] Art 11 Abs 5 DORA.
[113] Art 11 Abs 7 DORA.
[114] Art 11 Abs 10 DORA.

- 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[115];
- 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[116];
- 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[117];
- keine Verpflichtung im Rahmen des IKT-Risikomanagementrahmens eine Strategie für das IKT-Drittparteienrisiko zu haben und dieses regelmäßig zu überprüfen[118];
- können mit IKT-Drittdienstleistern vereinbaren, dass Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens auf einen unabhängigen Dritten übertragen werden.[119]

12. Fazit

Von DORA betroffene Finanzunternehmen haben ein sehr komplexes neues Rahmenwerk umzusetzen, welches insbesondere kleinere Finanzunternehmen aufgrund des großen Umfangs der Rechtsakte vor große Herausforderungen stellt. Unter Berücksichtigung des Grundsatzes der Proportionalität (dh Berücksichtigung von Größe und Gesamtrisikoprofil des Unternehmens sowie Art, Umfang und Komplexität der Dienstleistungen) sind zahlreiche Maßnahmen zu treffen, die von den eingesetzten IKT-Systemen und der Komplexität des Geschäftsmodells des Finanzunternehmens abhängig sind. Es bleibt abzuwarten, wie die zuständigen Aufsichtsbehörden diesen Grundsatz bei Prüfungen auslegen werden.

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

[115] Art 12 Abs 4 DORA.
[116] Art 12 Abs 4 DORA.
[117] Art 24 Abs 1 bis 4; Art 25 Abs 3 und Art 26 Abs 1 DORA.
[118] Art 28 Abs 2 DORA.
[119] Art 30 Abs 3 DORA.

Annex 1: Betroffenheit von Berufsgruppen der Finanzdienstleister von DORA[120]

Berufsgruppe	Betroffenheit	Anwendbare Bestimmungen
1. Gewerbliche Vermögensberater	□ Nein	keine
2. Leasingunternehmen	□ Nein	keine
	□ Versicherungsvermittlung in Nebentätigkeit und großes Unternehmen (mehr als 250 Mitarbeitern oder Jahresumsatz über 50 Mio. Euro/Bilanzsumme über 43 Mio. Euro)	IKT-Risikomanagementrahmen (Art 5 bis 15 DORA); Berichterstattung zu IKT-Vorfällen (Art 17 bis 21 DORA); Testen der digitalen operationalen Resilienz (Art 24 bis 27 DORA); Steuerung und Überwachung von IKT-Drittdienstleister-Risiken (Art 28 bis 30 DORA)
3. Wertpapierdienstleistungsunternehmen	□ Nein	keine
4. Wertpapierfirma	□ Ja	Für Klasse 2-Wertpapierfirmen: IKT-Risikomanagementrahmen (Art 5 bis 15 DORA); Berichterstattung zu IKT-Vorfällen (Art 17 bis 21 DORA); Testen der digitalen operationalen Resilienz (Art 24 bis 27 DORA); Steuerung und Überwachung von IKT-Drittdienstleister-Risiken (Art 28 bis 30 DORA); bestimmte Ausnahmen, wenn Kleinstunternehmen[121] Für Klasse 3-Wertpapierfirmen: **Vereinfachter IKT-Risikomanagementrahmen gemäß Art 16 Abs 3 DORA**[122] (*Art 5 bis 15 sind nicht anwendbar*); Berichterstattung zu IKT-Vorfällen (Art 17 bis 20); Testen der digitalen operationalen Resilienz (Art 24 bis 25 DORA); Steuerung und Überwachung von IKT-Drittdienstleister-Risiken (Art 28 bis 30 DORA)

[120] Es ist zu beachten, dass diese Darstellung keine Gruppenszenarien beleuchtet. Sollte beispielsweise ein Leasingunternehmen oder eine Wertpapierfirma in einer Kreditinstitutsgruppe integriert sein, ist dies gesondert zu prüfen (insbesondere Auslagerungen von Bankgeschäften).
[121] Kleinstunternehmen: Unternehmen, das weniger als 10 Personen beschäftigt und dessen Jahresumsatz bzw -bilanzsumme 2 Mio Euro nicht überschreitet
[122] Die in der DORA-Verordnung angeführten Ausnahmen für Kleinstunternehmen sind (soweit ersichtlich) in den RTS für den vereinfachten RMR berücksichtigt.

5. Zahlungs- und E-Geldinstitute (inkl Kontoinformationsdienstleister)	□ Ja	IKT-Risikomanagementrahmen (Art 5 bis 15 DORA); Berichterstattung zu IKT-Vorfällen (Art 17 bis 23 DORA); Testen der digitalen operationalen Resilienz (Art 24 bis 27 DORA); Steuerung und Überwachung von IKT-Drittdienstleister-Risiken (Art 28 bis 30 DORA); bestimmte Ausnahmen, wenn Kleinstunternehmen
6. Anbieter von Krypto-Dienstleistungen, die gemäß MiCA-VO zugelassen sind, und Emittenten wertreferenzierter Token	□ Ja	IKT-Risikomanagementrahmen (Art 5 bis 15 DORA); Berichterstattung zu IKT-Vorfällen (Art 17 bis 21 DORA); Testen der digitalen operationalen Resilienz (Art 24 bis 27 DORA); Steuerung und Überwachung von IKT-Drittdienstleister-Risiken (Art 28 bis 30 DORA); bestimmte Ausnahmen, wenn Kleinstunternehmen
7. Verwalter alternativer Investmentfonds (AIFM), sofern es sich nicht um einen registrierten AIFM gemäß Art 2 AIFMD bzw § 1 Abs 5 AIFMG handelt	□ Ja	IKT-Risikomanagementrahmen (Art 5 bis 15 DORA); Berichterstattung zu IKT-Vorfällen (Art 17 bis 21 DORA); Testen der digitalen operationalen Resilienz (Art 24 bis 27 DORA); Steuerung und Überwachung von IKT-Drittdienstleister-Risiken (Art 28 bis 30 DORA); bestimmte Ausnahmen, wenn Kleinstunternehmen
8. Schwarmfinanzdienstleister gemäß ECSP	□ Ja	IKT-Risikomanagementrahmen (Art 5 bis 15 DORA); Berichterstattung zu IKT-Vorfällen (Art 17 bis 21 DORA); Testen der digitalen operationalen Resilienz (Art 24 bis 27 DORA); Steuerung und Überwachung von IKT-Drittdienstleister-Risiken (Art 28 bis 30 DORA); bestimmte Ausnahmen, wenn Kleinstunternehmen
9. Crowdinvesting-Plattformen mit einer Gewerbeberechtigung als Gewerblicher Vermögensberater	□ Nein	keine
10. Versicherungsvermittler, Rückversicherungsvermittler sowie Versicherungsvermittler in Nebentätigkeit	□ grundsätzlich nein	keine
	□ Versicherungsvermittlung (in Nebentätigkeit[123]) und großes Unternehmen (mehr als 250 Mitarbeitern oder Jahresumsatz über 50 Mio. Euro/Bilanzsumme über 43 Mio. Euro).	IKT-Risikomanagementrahmen (Art 5 bis 15 DORA); Berichterstattung zu IKT-Vorfällen (Art 17 bis 21 DORA); Testen der digitalen operationalen Resilienz (Art 24 bis 27 DORA); Steuerung und Überwachung von IKT-Drittdienstleister-Risiken (Art 28 bis 30 DORA)

[123] Aus Sicht des Fachverbands ist lediglich auf die Umsatzerlöse und Mitarbeiter abzustellen, welche der Versicherungsvermittlung (in Nebentätigkeit) zuordenbar sind.