DORA: Wissenswertes …

Wir haben uns erlaubt, den derzeit aus 16 Fragestellungen bestehenden Fragenkatalog der BaFin aufzugreifen und etwas unabhängiger von der Internet-Seite der BaFin aufzubereiten, damit dieser u.a. auch ohne Internet zur Verfügung gestellt bzw. eingesehen werden kann. Die aktuelle Fassung ist jeweils hier einsehbar. Dieser Link sollte auch genutzt werden da die BaFin angekündigt hat, den Fragenkatalog fortlaufend zu aktualisiert.

Gerne stellen wir Ihnen diesen hier zur Verfügung.

Der nachfolgende Fragenkatalog zu DORA vermittelt, ohne Anspruch auf Vollständigkeit, einen ersten Überblick über die wichtigsten Fragestellungen zu DORA und deren Umsetzung.

1. Für welche Unternehmen gilt DORA?

DORA ist eine finanzsektorübergreifende europäische Verordnung und bündelt und harmonisiert Regelungen bestehender sektoraler europäischer Verordnungen und Richtlinien.

In den Geltungsbereich der europäischen Verordnung DORA fallen (Artikel 2 Absatz 1 DORA):

(a) CRR-Kreditinstitute,

(b) Zahlungsinstitute,

(c) Kontoinformationsdienstleister,

(d) E-Geld-Institute,

(e) Wertpapierfirmen,

(f) Anbieter von Krypto-Dienstleistungen, die gemäß der Verordnung des Europäischen Parlaments und des Rates über Märkte von Krypto-Werten (MiCAR) zugelassen sind, und Emittenten wertreferenzierter Token,

(g) Zentralverwahrer,

(h) zentrale Gegenparteien,

(i) Handelsplätze,

(j) Transaktionsregister,

(k) Verwalter alternativer Investmentfonds,

(l) Verwaltungsgesellschaften

(m) Datenbereitstellungsdienste,

(n) Versicherungs- und Rückversicherungsunternehmen,

(o) Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit,

(p) Einrichtungen der betrieblichen Altersversorgung,

(q) Ratingagenturen,

(r) Administratoren kritischer Referenzwerte,

(s) Schwarmfinanzierungsdienstleister,

(t) Verbriefungsregister

(u) IKT-Dienstleister

Ausnahmen gelten für die folgenden Unternehmen (Artikel 2 Absatz 3 DORA):

(a) Verwalter alternativer Investmentfonds im Sinne von Artikel 3 Absatz 2 der Richtlinie 2011/61/EU;

(b) Versicherungs- und Rückversicherungsunternehmen im Sinne von Artikel 4 der Richtlinie 2009/138/EG;

(c) Einrichtungen der betrieblichen Altersversorgung, die Altersversorgungssysteme mit insgesamt weniger als 15 Versorgungsanwärtern betreiben;

(d) gemäß den Artikeln 2 und 3 der Richtlinie 2014/65/EU ausgenommene natürliche oder juristische Personen;

(e) Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, bei denen es sich um Kleinstunternehmen oder kleine oder mittlere Unternehmen handelt;

(f) Postgiroämter im Sinne von Artikel 2 Absatz 5 Nummer 3 der Richtlinie 2013/36/EU.

2. Ab wann wird DORA angewendet?

Die Regelungen von DORA sind ab dem 17. Januar 2025 anwendbar.

3. Wie wird ein IKT-bezogener Vorfall in DORA definiert?

Ein „IKT-bezogener Vorfall“ ist ein von dem Institut oder Unternehmen nicht geplantes Ereignis bzw. eine Reihe verbundener Ereignisse, das bzw. die die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigt und nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf die vom Finanzunternehmen erbrachten Dienstleistungen hat (Art. 3 Absatz 1 Nr. 8 DORA).

4. Was sind IKT-Dienstleistungen im Sinne von DORA?

„IKT-Dienstleistungen“ sind digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzerinnen und Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen.

Dazu gehört auch die technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware- Aktualisierungen , mit Ausnahme herkömmlicher analoger Telefondienste (Art. 3 Absatz 1 Nr. 21 DORA).

5. Stehen IKT-Drittdienstleister durch DORA künftig unter der Finanzdienstleistungsaufsicht?

Kritische IKT-Drittdienstleister unterstehen der Überwachung europäischer Aufsichtsbehörden, die klar von einer Aufsicht über Finanzunternehmen zu unterscheiden ist.

Dies zeigt sich beispielsweise daran, dass kritische IKT-Drittdienstleister als Nicht-Finanzunternehmen keine Zulassung bei Finanzaufsichtsbehörden beantragen müssen und diese ihnen im Umkehrschluss auch nicht entzogen werden kann.

Auch beschränkt sich der Überwachungsbereich der Aufsichtsbehörden nicht auf das gesamte Unternehmen, sondern auf den in Artikel 33 Absatz 3 DORA festgelegten Bewertungsrahmen. Er hat das Management der IKT-Risiken, die vom kritischen IKT-Drittdienstleister für Finanzunternehmen ausgehen können, zum Schwerpunkt.

Ebenso sind die Befugnisse der Aufsichtsbehörden beschränkt (Artikel 35 DORA). Die Aufsichtsbehörden haben demnach zum Beispiel keine Befugnis zur Abbestellung von Geschäftsleiten oder den Einsatz von Sonderbeauftragten.

6. Wieso hat die EU mit DORA eine Überwachung von kritischen IKT-Drittdienstleistern etabliert?

Aktuell zeigt sich innerhalb der EU ein sehr heterogenes Bild in Bezug auf die Überwachung von kritischen IKT-Drittdienstleistern.

Während beispielsweise in Deutschland durch das Gesetz zur Stärkung der Finanzmarktintegrität (FISG) weitgehende Befugnisse für Aufsichtsbehörden gegenüber Auslagerungsunternehmen eingeführt wurden, bestehen ähnliche Rechte in anderen Ländern der EU nicht oder nicht in gleichem Maße.

Angesichts der Risiken, die sich aus der Konzentration der Abhängigkeiten von kritischen IKT-Drittdienstleistern grenzüberschreitend ergeben, ist dies ein potenzielles Systemrisiko für den europäischen Finanzmarkt (vgl. Erwägungsgrund 30 zu DORA).

Das Vorgehen der EU entspricht ihrer Strategie, den europäischen Binnenmarkt mit einheitlichen Regeln zu vertiefen. Es wird auch zu weniger Aufwand für die grenzüberschreitend agierenden Finanzunternehmen führen.

7. Welche Rechte erhalten europäische Aufsichtsbehörden bei der Überwachung?

Europäische Aufsichtsbehörden werden ab Januar 2025 gegenüber kritischen IKT-Drittdienstleistern u.a. das Recht haben,

- Informationen anzufordern,
- allgemeine Untersuchungen und Prüfungen, einschließlich Vor-Ort-Prüfungen, durchzuführen,
- Empfehlungen auszusprechen zur IKT-Sicherheit (z.B. bzgl. Patching, Updates, Verschlüsselung), zu den Geschäftsbedingungen und zur geplanten Vergabe von Unteraufträgen einschließlich des Verzichts auf weitere Unteraufträge und
- öffentlich bekanntzugeben, wenn ein beaufsichtigtes Unternehmen diese Empfehlungen nicht einhält und wenn Sanktionen verhängt wurden.

Als ultima ratio wird es nationalen Aufsichtsbehörden möglich sein, die Nutzung oder den Einsatz von Diensten auszusetzen oder die Kündigung dieser zu verlangen.

8. Müssen Finanzunternehmen kritische IKT-Drittdienstleister künftig nicht mehr überwachen oder prüfen, wenn dies die Aufsicht übernimmt?

Finanzunternehmen müssen die Nutzung von IKT-Drittdienstleistern mit Blick auf ihr eigenes Unternehmen stets überwachen.

Die Überwachung von kritischen IKT-Drittdienstleistern durch die Aufsicht erfolgt hingegen mit Blick auf den gesamten Finanzmarkt. Daher entbindet die Überwachung eines als kritisch eingestuften IKT-Drittdienstleisters durch die Aufsicht die Finanzunternehmen nicht von ihren eigenen regulatorischen Verpflichtungen. Im Gegenteil: Finanzunternehmen bleiben vielmehr voll verantwortlich.

Zusätzlich zu ihrer eigenen Überwachung profitieren die Finanzunternehmen ab 2025 von der systemweiten Überwachung durch die Aufsicht – nämlich, indem sie beispielsweise die Übersicht über die nicht oder nicht vollständig umgesetzten Empfehlungen kritischer IKT-Drittdienstleister einsehen können.

9. Werden Unternehmen als kritische IKT-Drittdienstleister in Zukunft überwacht, weil sie in der Vergangenheit negativ aufgefallen sind?

Der Begriff kritische IKT-Drittdienstleister steht in keinem Zusammenhang mit den Erfahrungen der Aufsicht mit diesem Dienstleister oder dessen Reputation in der Öffentlichkeit.

Die Einstufung als kritischer IKT-Drittdienstleister erfolgt vielmehr in Bezug auf dessen Rolle für den Finanzmarkt. Sie wird auf Basis eines detaillierten Kriterienkatalogs der EU-Kommission bestimmt (dazu ESAs specify criticality criteria and oversight fees for critical ICT third-party providers under DORA (europa.eu)).

Eine Rolle spielen dabei zum Beispiel

- systematische Auswirkungen der Zusammenarbeit mit einem IKT-Drittdienstleister auf die Stabilität, Kontinuität oder Qualität der Erbringung von Finanzdienstleistungen, falls der kritische IKT-Drittdienstleister einer umfassenden Betriebsstörung ausgesetzt wäre,
- dem systemischen Charakter oder der Bedeutung der Finanzunternehmen, die den IKT-Drittdienstleister nutzen
- oder die Abhängigkeit der Finanzindustrie vom IKT-Drittdienstleister und
- der Grad der Substituierbarkeit des IKT-Drittdienstleisters.

Bei der Einstufung nutzt die Aufsicht primär die Informationsregister der Finanzunternehmen als Datenquelle.

Die Grundlage hierfür: Die ESAs haben auf Aufforderung der EU-Kommission Kriterien zur Bestimmung der Kritikalität erarbeitet und ihre gemeinsame Stellungnahme im September 2023 an die EU-Kommission übermittelt.

Die EU-Kommission wird die finalen Kriterien in einem delegierten Rechtsakt veröffentlichen.

10. Kommen durch die Überwachung kritischer IKT-Drittdienstleister künftig noch mehr Kosten auf Finanzunternehmen zu?

Die Kosten der Überwachung müssen von den als kritische IKT-Drittdienstleister eingestuften Unternehmen selbst getragen werden.

Dies gilt auch für Dienstleister, die sich auf Antrag – also freiwillig – dem Überwachungsrahmenwerk unterwerfen.

11. Werden Cloud-Dienstleister künftig als Kritische IKT-Drittdienstleister überwacht?

Anbieter von Cloud-Dienstleistungen stehen klar im Fokus von DORA (vgl. Erwägungsgrund 20 zu DORA), jedoch unterfällt nicht jeder Cloud-Anbieter automatisch dem Überwachungsrahmenwerk der europäischen Aufsichtsbehörden.

Vielmehr wird die Auswertung der Informationsregister der Finanzunternehmen im Jahr 2025 zeigen, ob der Einstufungsprozess zur Bestimmung kritischer IKT-Drittdienstleister auch dazu führt, dass künftig Cloud-Dienstleister überwacht werden. Denn dabei handelt es sich immer um Entscheidungen im Einzelfall.

Die ESAs haben auf Aufforderung der EU-Kommission Kriterien zur Bestimmung der Kritikalität erarbeitet und ihre gemeinsame Stellungnahme im September 2023 an die EU-Kommission übermittelt (s. dazu ESAs specify criticality criteria and oversight fees for critical ICT third-party providers under DORA (europa.eu)).

Die EU-Kommission wird die finalen Kriterien in einem delegierten Rechtsakt veröffentlichen.

12. Wann müssen beaufsichtigte Unternehmen einen IKT-bezogenen Vorfall melden?

Ein IKT-bezogener Vorfall ist dann zu melden, wenn der Vorfall die entsprechenden Klassifikationskriterien erfüllt.

Der Klassifikationsprozess sowie die Klassifikationskriterien basieren auf den in Artikel 18 DORA genannten Anforderungen und werden in einem Regulatory Technical Standard (RTS) genauer geregelt.

Das Konsultationspapier des RTS wurde im Zeitraum vom 19. Juni – 11. September öffentlich konsultiert und wird nach abschließender Bearbeitung im kommenden Jahr veröffentlicht.

Nach der Veröffentlichung des RTS werden Sie hier auf der DORA-Informationsseite der BaFin über die genaue Ausgestaltung des Klassifikationsprozesses und der Klassifikationskriterien informiert.

13. An wen sind diese Meldungen eines IKT-bezogenen Vorfalls zu erstatten?

Die BaFin fungiert als zentraler Meldehub für alle unter ihrer Aufsicht stehenden Finanzunternehmen.

Die Meldungen sollen über das MVP-Portal eingereicht werden.

14. Müssen auch Cyberbedrohungen gemeldet werden?

Gemäß Artikel 19 Absatz 2 DORA ist die Meldung von Cyberbedrohungen freiwillig.

Finanzunternehmen können auf freiwilliger Basis erhebliche Cyberbedrohungen melden, wenn sie der Auffassung sind, dass die Bedrohung für das Finanzsystem, die Dienstnutzer oder die Kundinnen und Kunden relevant ist.

Die BaFin begrüßt die Nutzung dieser freiwilligen Meldung außerordentlich und wird einen entsprechenden Meldeweg zur Verfügung stellen.

15. Wie werden die Anforderungen an das Threat-Led Penetration Testing (TLPT aus Artikel 26 und 27 DORA ab 2025 in Deutschland umgesetzt?

Die wesentliche Testmethodik und die Testverfahren für TLPT sollen im Einklang mit dem TIBER-EU-Rahmenwerk erfolgen (Artikel 26 Absatz 11 DORA).

Deshalb werden die operativen Aufgaben mit Bezug zu TLPT - wie bereits unter TIBER-DE - von der Deutschen Bundesbank wahrgenommen.

Durch DORA werden solche Tests zu einem aufsichtlichen Instrument und Teil des IKT-Risikomanagementrahmens eines Finanzunternehmens. Daher wird die jeweils zuständige Aufsichtsbehörde (in Deutschland die BaFin bzw. für signifikante Kreditinstitute die EZB) diese Tests in die aufsichtlichen Prozesse einbinden.

Dies betrifft insbesondere die Aspekte Identifikation von Finanzunternehmen, die künftig TLPT durchführen müssen, die Festlegung der Testfrequenz, die Validierung des Testumfangs und die Berücksichtigung der Testergebnisse in der laufenden Aufsicht.

16. Welche Institute und Unternehmen müssen die erweiterten Anforderungen an das Testen im Sinne von TLPT aus Artikel 26 und 27 DORA ab 2025 in Deutschland erfüllen?

Allgemeine Anforderungen an das Testen gibt es für alle Finanzunternehmen im Anwendungsbereich von DORA (Artikel 24 und 25 DORA).

Ein solides und umfassendes Programm für das Testen der digitalen operationalen Resilienz ist ein integraler Bestandteil des IKT-Risikomanagementrahmens.

Die Anforderung für erweiterte Tests auf Basis von TLPT im Sinne von Artikel 26 und 27 DORA gilt nur für ausgewählte Finanzunternehmen, die entsprechend den Kriterien in Artikel 26 Absatz 8 DORA auf Basis der folgenden Kriterien durch die zuständige Aufsichtsbehörde identifiziert werden:

- wirkungsbezogenen Faktoren, darunter insbesondere inwieweit sich die vom Finanzunternehmen erbrachten Dienstleistungen und ausgeführten Tätigkeiten auf den Finanzsektor auswirken;
- etwaigen Bedenken hinsichtlich der Finanzstabilität, einschließlich des systemischen Charakters des Finanzunternehmens auf Unionsebene oder auf nationaler Ebene, je nach Sachlage;
- dem spezifischen IKT-Risikoprofil, dem IKT-Reifegrad des Finanzunternehmens oder einschlägigen technologischen Merkmalen.

Diese Kriterien werden durch einen technischen Regulierungsstandard (RTS) durch die ESAs in Zusammenarbeit mit den zuständigen Behörden spezifiziert.

Die öffentliche Konsultation des RTS-Entwurfs ist von Dezember 2023 bis Februar 2024 geplant. Der finale Entwurf soll im Juli 2024 an die Europäische Kommission übermittelt werden.

Die BaFin wird die von ihr beaufsichtigten Institute und Unternehmen möglichst frühzeitig über eine Identifikation informieren.

Gerne unterstützen wir Sie bei der Aufnahme des Status Quo, einer Projektplanung sowie der Erstellung der entsprechenden Prozesse, Dokumente, Schriftlich fixierten Ordnung, IKS-Maßnahmen sowie der Ergänzung der bestehenden unternehmensinhärenten Abläufen in den betroffenen Unternehmensbereichen.

Für Fragen, Anregungen und Projektanfragen kommen Sie gerne auf den Autor zu.

compliance-net GmbH
Robert-Bosch-Straße 32
63303 Dreieich
Telefon: +49 6103 3760 960
E-Mail: Partners@compliance-net.com
Webseite: compliance-net.com
Fachseite: compliance-net.de

Wir sind Ihr Lotse, der Sie durch die Beständigkeit des Wandels sicher begleitet!