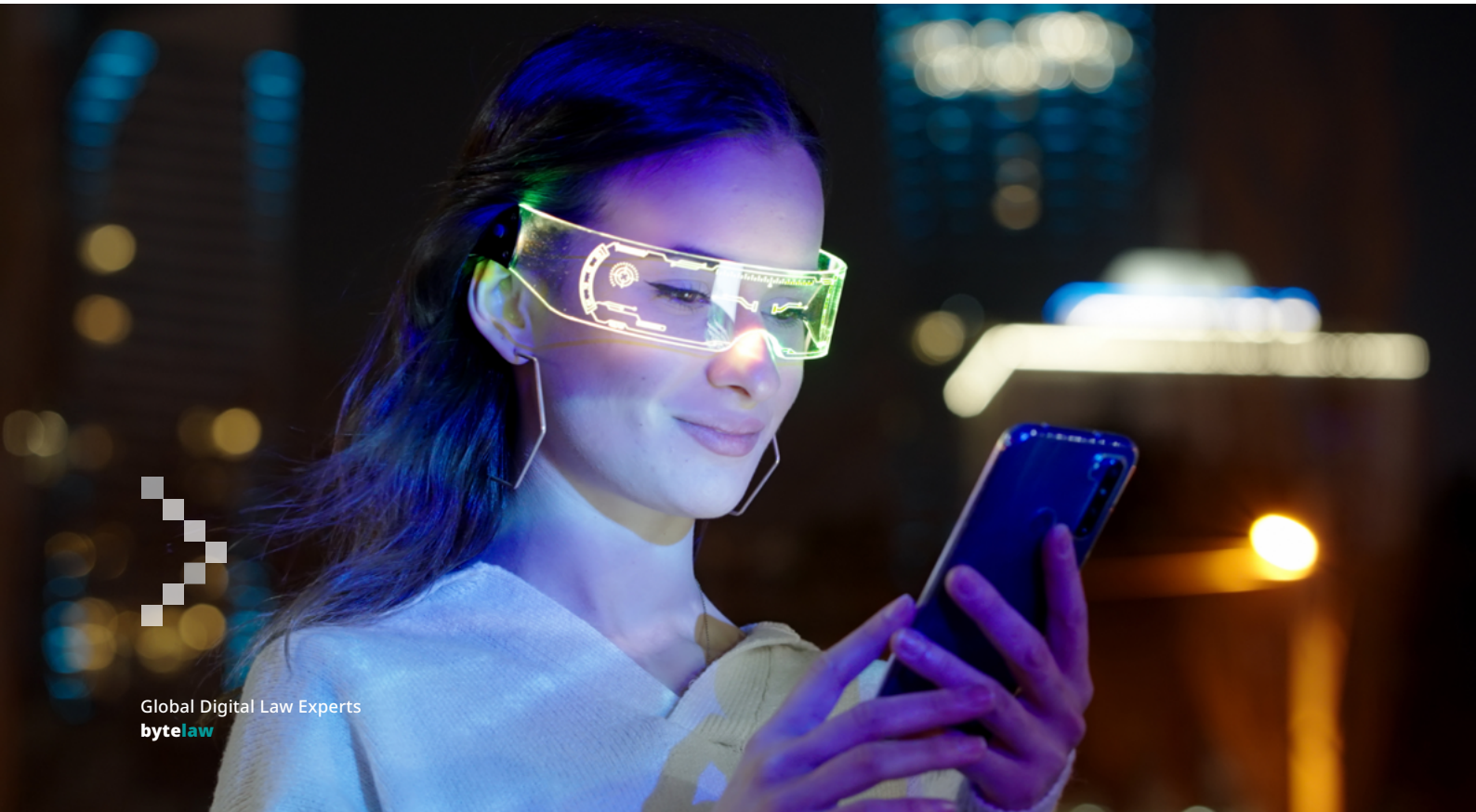
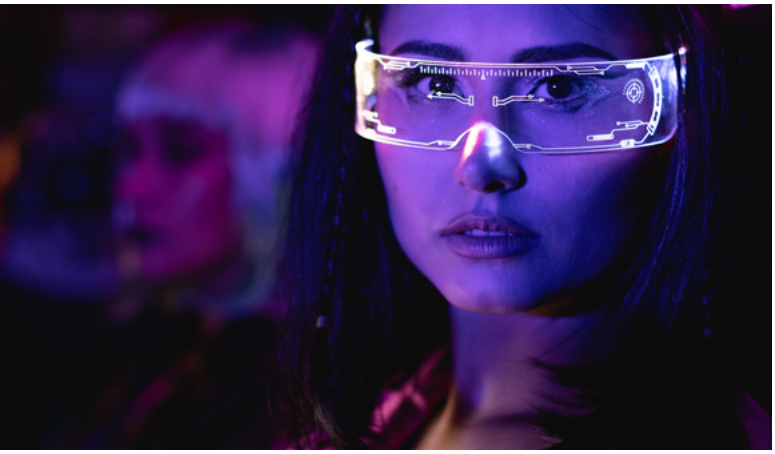
Digital Operational Resilience Act (DORA)
Executive Summary

- Die Europäische Union hat am 17.01.2023 die **DORA**-Verordnung für Finanzunternehmen und Drittanbieter von Informations- und Kommunikationstechnik („IKT“) erlassen.
- Ziel der Verordnung ist es, Geschäftsunterbrechungen und wirtschaftliche Verluste durch Cyberbedrohungen und IT-Zwischenfälle vorzubeugen.
- Die neue Verordnung statuiert Compliancevorgaben in fünf zentralen Bereichen: Risikomanagement; Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle; Tests der digitalen operationellen Resilienz; Management des IKT-Drittparteienrisikos; Austausch von Informationen und Kenntnissen.
- Die **DORA**-Anforderungen müssen von den betroffenen Unternehmen bis zum 17.01.2025 umgesetzt werden.

Einleitung

Die Digitalisierung des europäischen Finanzsektors bietet Anbietern von Bank- und Finanzdienstleistungen zahlreiche neue Möglichkeiten. Gleichzeitig steigt jedoch, angesichts der wachsenden Gefahr durch Cyberangriffe, auch die Anzahl der Risiken. Um Geschäftsunterbrechungen und wirtschaftliche Verluste durch Cyberbedrohungen und IT-Zwischenfälle vorzubeugen, hat die Europäische Union am 17.01.2023 mit dem Digital Operational Resilience Act („**DORA**“) einen unionsweiten Rechtsrahmen erlassen, welcher die digitale Widerstandsfähigkeit und Cybersicherheit im Finanzdienstleistungssektor stärken soll.





Was ist DORA?

Bei **DORA** handelt es sich um eine von der Europäischen Union erlassene Verordnung, welche Teil eines größeren Gesetzespaketes zur Digitalisierung des Finanzsektors ist (Digital Finance Package). Ziel von **DORA** ist es, die Stabilität des Finanzmarktes auch im Falle von schwerwiegenden Störungen zu gewährleisten und alle Marktteilnehmer zu schützen, indem sichergestellt wird, dass Finanzunternehmen alle notwendigen Maßnahmen zur Absicherung gegen Cyberrisiken und -angriffe treffen. Zudem vereinheitlicht **DORA** bestehende europäische und nationale Standards und Vorgaben, um den Binnenmarkt störende doppelte Anforderungen und uneinheitliche Regelungen für europaweit tätige Finanzunternehmen in Zukunft zu vermeiden. Der Anknüpfungspunkt der neuen Verordnung ist dabei die Verwendung von Informations- und Kommunikationstechnologie ("IKT"). Darunter versteht die Europäische Kommission "alle technischen Medien, die für die Handhabung von Informationen und zur Unterstützung der Kommunikation eingesetzt werden", Beispiele dafür sind vor allem Computer- und Netzwerkhardware und die dazugehörige Software. An die betroffenen Unternehmen stellt **DORA** neue Compliance-Anforderungen, welche die Verarbeitung und Speicherung von Informationen betreffen.

Welche Unternehmen sind von DORA betroffen?

Die **DORA**-Verordnung ist auf Finanzunternehmen und Drittanbieter von Informations- und Kommunikationstechnik („IKT") anzuwenden, welche innerhalb der Europäischen Union tätig sind. Neben Kreditinstituten, Versicherungsunternehmen und Zahlungsinstituten, die bisher in Deutschland bereits durch BAIT, VAIT und ZAIT im Bereich IT und Informationssicherheit reguliert waren, wird die Anzahl der Organisationen ausgeweitet. Nunmehr werden folgende Organisationen vom Anwendungsbereich der **DORA** erfasst:

- Kreditinstitute
- Zahlungsinstitute
- Kontoinformationsdienstleister
- E-Geld-Institute
- Wertpapierfirmen
- Zentralverwahrer
- Zentrale Gegenparteien
- Handelsplätze
- Transaktionsregister
- Verwalter alternativer Investmentfonds
- Verwaltungsgesellschaften
- Datenbereitstellungsdienste
- Versicherungs- und Rückversicherungsunternehmen
- Einrichtungen der betrieblichen Altersvorsorge
- Ratingagenturen
- Administratoren kritischer Referenzwerte
- Schwarmfinanzierungsdienstleister
- Verbriefungsregister
- Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit
- IKT-Drittdienstleister
- Anbieter von Krypto-Vermögenswerten, die gemäß einer Verordnung des Europäischen Parlaments und des Rates über Märkte für Krypto-Vermögenswerte zugelassen sind, und Emittenten wertreferenzierter Token.

Was regelt die DORA-Verordnung?

Die Compliancevorgaben, die **DORA** statuiert, lassen sich in fünf verschiedene Kategorien einteilen, welche im Folgenden näher beleuchtet werden:

1. Risikomanagement

Im Bereich des Risikomanagements statuiert die neue Verordnung, dass Finanzunternehmen belastbare IKT-Systeme einrichten und pflegen müssen. Dabei ist besonders darauf zu achten, dass bestehende IKT-Risiken minimiert werden, die Risikoquellen identifiziert werden und Schutz- und Präventionsmaßnahmen vorhanden sind. Zudem muss ein System zur Erkennung anomaler Aktivitäten sorfältig etabliert werden. Finanzunternehmen müssen weiterhin umfassende Business-Continuity-Richtlinien/ Notfall- und Wiederherstellungspläne einführen. Außerdem sollten betroffene Unternehmen die Aufgaben und Verantwortlichkeiten für alle IKT-bezogenen Funktionen festlegen, interne IKT-Revisionspläne erstellen sowie Leitlinien zu Vereinbarungen über die Nutzung von IKT-Dienstleistungen anfertigen. Zu beachten ist die IKT-Risikomanagementmaßnahmen müssen in die Geschäftsstrategie implementiert werden. Die Verantwortung für die Umsetzung trägt dabei der Vorstand oder der Geschäftsführer als Leitungsorgan des Finanzunternehmens.

2. Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle

DORA enthält zudem eine Verpflichtung zur Meldung von IKT-bezogenen Vorfällen. In Zukunft sind Finanzunternehmen verpflichtet einen Managementprozess zur Überwachung und Protokollierung von IKT-Vorfällen zu implementieren. Etwaige Vorfälle sind dann nach Kriterien, die in der Verordnung dargelegt sind, zu klassifizieren. Dazu gehören beispielsweise Dauer, geographische Ausbreitung und wirtschaftliche Auswirkungen des Vorfalls. Bei schwerwiegenden IKT-Vorfällen muss das betroffene Unternehmen mehrere Meldungen an die europäischen Behörden vornehmen:

- Eine Erstmeldung
- Eine Zwischenmeldung ▸ wenn eine Statusänderung des ursprünglichen Vorfalls gegeben ist
- Eine Abschlussmeldung ▸ nach Beendigung der Ursachenanalyse.

3. Tests der digitalen operationalen Resilienz

Eine weitere Anforderung der **DORA**-Verordnung sind Tests der digitalen operationalen Resilienz eines Unternehmens. Die Risikomanagementmaßnahmen müssen dabei mindestens einmal pro Jahr durch interne oder externe Prüfer auf seine Schwachstellen kontrolliert werden. Dies erfolgt durch den Einsatz bekannter Verfahren wie z.B. Leistungstests, End-to-End-Tests oder Penetrationstests.

4. Management des IKT-Drittparteienrisikos
DORA legt im Rahmen des Risikomanagements von Finanzunternehmen auch einen großen Fokus auf die Risiken durch Drittanbieter. Oft lagern Unternehmen ihre IT an große Technologieanbieter aus. Dadurch entstehen potenzielle Risiken, welche im Rahmen des Risikomanagements berücksichtigt werden müssen. Diese Risiken müssen Finanzunternehmen zukünftig bewerten und in ihrem Risikomanagementrahmen berücksichtigen. Dazu gibt **DORA** wesentliche Mindestbestandteile von Auslagerungsverträgen vor, wie z.B. Kündigungsrechte und umfassende Überwachungsrechte des Finanzunternehmens. Zudem erschafft **DORA** einen europäischen Aufsichtsrahmen für kritische IKT-Drittanbieter. Danach dürfen die Aufsichtsbehörden bei kritischen IKT-Drittanbietern Unterlagen anfordern, Vor-Ort Prüfungen durchführen und Zwangsgelder verhängen.

5. Austausch von Informationen und Kenntnissen
Ein weiterer zentraler Bestandteil ist der Informationsaustausch zwischen Finanzunternehmen. Nach der **DORA**-Verordnung dürfen Finanzdienstleister zukünftig relevante Informationen bezüglich Cyberbedrohungen austauschen. Dies gilt insbesondere für Erkenntnisse über Techniken und Verfahren, sowie aktuelle Beeinträchtigungen. Der Austausch ist dabei nur zulässig, wenn er auf die Stärkung der digitalen operationalen Resilienz der Unternehmen abzielt, innerhalb einer vertrauenswürdigen Gemeinschaft stattfindet und durch Vereinbarungen umgesetzt wird, die den sensiblen Charakter der Informationen schützen.

Was ist jetzt zu tun?

Mit der Veröffentlichung im Amtsblatt der Europäischen Union am 27.12.2022 wurde das formelle Gesetzgebungsverfahren zur **DORA**-Verordnung abgeschlossen. Am 17.01.2023 trat die Verordnung in Kraft, allerdings ist für die Anwendung der neuen Regelungen eine Übergangsfrist von 2 Jahren vorgesehen. Somit müssen die betroffenen Unternehmen die Anforderungen ab dem 17.01.2025 erfüllen. Dies heißt jedoch keineswegs, dass Unternehmen sich mit der Implementierung noch Zeit lassen können, denn das Treffen geeigneter Maßnahmen kann ein langwieriger und aufwendiger Prozess sein. Gerade in großen Unternehmen wird es einige Zeit brauchen, um eine derartige Compliancestruktur aufzubauen, die den **DORA**-Anforderungen genügt. Zudem wird sich die Umsetzung der vorgeschriebenen Maßnahmen von Organisation zu Organisation unterscheiden. Gerade deshalb ist es wichtig sich frühzeitig mit den Anforderungen von **DORA** auseinanderzusetzen und diese zeitnah zu implementieren.

Damit Ihnen die Vorbereitung gelingt haben wir im Folgenden die wichtigsten Schritte einer guten Vorbereitung zusammengefasst:

1. Betroffenheit klären
Zunächst sollten Sie klären, ob Ihr Unternehmen in den Anwendungsbereich der **DORA**-Verordnung fällt.

2. Risikobewertung
Bewerten Sie im nächsten Schritt Ihr derzeitiges IKT-Risiko, sowie aktuelle Meldeverfahren und Ihre Fähigkeit zur Bedrohungserkennung. Dies kann mittels einer Resilienz-Prüfung wichtiger Funktionen und Systeme geschehen. Auch eine Überprüfung Ihres derzeitigen Security-Awareness-Programms ist an dieser Stelle von Vorteil.

3. Kritische IKT-Drittdienstleister bestimmen
Zusätzlich zu der Bestimmung Ihrer eigenen Risiken muss eine Identifikation der kritischen IKT-Drittdienstleister vorgenommen werden. Dabei ist ein besonderer Fokus auf deren Schwachstellen und den daraus resultierenden Risiken für Ihr Unternehmen zu legen. Vor diesem Hintergrund sind besonders die vertraglichen Anforderungen an Vereinbarungen mit IKT-Drittleistern zu beachten. Überprüfen Sie an dieser Stelle bestehende Verträge und achten Sie bei der Aufsetzung von neuen Verträgen darauf, dass die gesetzlichen Mindestelemente enthalten sind.

4. Budgets zuweisen
Nach der Bewertung der einschlägigen Risiken lässt sich bestimmen, wie hoch der Arbeitsaufwand und somit auch das Budget für die Umsetzung der Maßnahmen sein sollte. Beachten Sie dabei sowohl die Kosten für die Umsetzung von DORA-Anforderungen als auch Kosten für die Implementierung eines effektiven Security-Awareness-Programms bzw. -trainings.

5. Maßnahmenauswahl
Nun gilt es zusammen mit den Entscheidungsträgern geeignete Maßnahmen auszuwählen, welche zu dem Risikoprofil Ihres Unternehmens passen. Bei der Auswahl der Maßnahmen sollte ein besonderer Fokus auf die IKT-Drittdienstleister gelegt werden. Einigen Sie sich mit Ihren Partnern gemeinsam auf Maßnahmen und wechseln Sie notfalls Ihren Dienstleister.

6. Umsetzung der Maßnahmen & Gap-Analyse
Konnten Sie sich mit Ihren Partnern auf ein geeignetes Maßnahmenportfolio einigen, so müssen die Maßnahmen im nächsten Schritt umgesetzt werden. Ist dies geschehen, so sollten Sie erneut eine Gap-Analyse durchführen, um sicherzustellen, dass die gesetzlichen Anforderungen eingehalten werden.

Ihre Ansprechpartner für alle Fragen rund um DORA und Cybersicherheit:

Dirk Koch
Rechtsanwalt | Partner
CEHv11 – Certified Ethical Hacker
Data Protection Risk Manager CIPP/E
koch@byte.law

Olga Stepanova, LL.M. (Berkeley)
Rechtsanwältin | Partnerin
Fachanwältin für gewerblichen Rechtsschutz und für Informationstechnologierecht
stepanova@byte.law

bytelaw Rechtsanwälte
Bockenheimer Landstraße 51-53
60325 Frankfurt

T +49 (0) 69 - 1 53 91 91 90
M info@byte.law
I byte.law