Standpunkt

DORA: Digital Operational Resilience Act

Die Europäische Kommission hat mit dem Digital Operational Resilience Act (DORA) einen verbindlichen Regulierungsrahmen eingeführt, um die digitale Widerstandsfähigkeit des Finanzsektors in der EU nachhaltig zu stärken.

DORA gilt seit Januar 2025 für Banken, Versicherungen, Wertpapierfirmen und kritische IKT-Dienstleister in der gesamten EU.

Stabilität sichern – auch unter Druck

Die Anforderungen an digitale Resilienz sind Realität geworden:
Seit Januar 2025 ist DORA in der gesamten EU verbindlich umzusetzen.

Finanzinstitute und ihre kritischen IKT-Dienstleister müssen nachweisen, dass sie auch unter extremen Bedingungen – etwa bei Cyberattacken, Systemausfällen oder Lieferkettenproblemen – handlungsfähig bleiben.

DORA bündelt und harmonisiert bestehende regulatorische Vorgaben zur digitalen Betriebsstabilität. Die Verordnung etabliert einen einheitlichen europäischen Rahmen für die Risikobewertung und Steuerung von Informations- und Kommunikationstechnologien (IKT).

Wir begleiten Banken und Finanzdienstleister bei der Umsetzung: von der DORA-Governance über Reporting-Prozesse bis zu resilienten Betriebsarchitekturen.

Finanzielle Stabilität in Europa

Nach dem Inkrafttreten der DORA-Verordnung besteht erheblicher Handlungsdruck bei der nachhaltigen Umsetzung der Vorgaben – das betonen auch europäische Regulierungsbehörden wie das European Systemic Risk Board (ESRB).

Das ESRB hatte bereits in einem früheren Bericht empfohlen, die Anforderungen an das Risikomanagement von Drittanbietern für alle in Europa tätigen Finanzunternehmen zu vereinheitlichen und zu verschärfen. Anlass dafür waren unter anderem die zunehmenden Cyberangriffe auf den Finanzsektor, bei denen Cyberrisiken zu den größten systemischen Bedrohungen gezählt werden.

Die EU reagierte darauf mit klaren Vorgaben: Finanzdienstleister müssen heute jederzeit in der Lage sein, ihre Betriebsfähigkeit sicherzustellen, auch im Fall schwerwiegender Störungen oder Ausfälle innerhalb ihrer IT-Landschaft. Genau hier setzt DORA an und verankert erstmals ein einheitliches operatives Resilienzregime für die Finanzbranche.

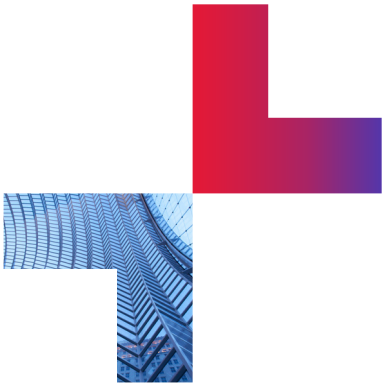
Cyberresilienz als strategische Pflicht

Die Dringlichkeit ergibt sich auch aus den Erfahrungen der COVID-19-Pandemie: In dieser Phase nahm die digitale Nutzung von Finanzdienstleistungen sprunghaft zu, was die Abhängigkeit von IKT-Systemen stark erhöhte. Gleichzeitig stieg die Zahl der Cyberangriffe signifikant. Laut EU-Kommission verzeichneten einige Finanzinstitute bis zu 38 % mehr Attacken im Vergleich zu den Vorjahren.

Trotzdem fehlte lange ein abgestimmtes Vorgehen. Mit DORA wurde diese Lücke geschlossen: Die Verordnung bietet heute einen einheitlichen Standard für IKT-Risikomanagement, Vorfallreaktion, Prüfungspflichten und Drittanbieterkontrolle – verbindlich und EU-weit anwendbar.

Um die Widerstandsfähigkeit der Finanzinstitute bei potenziellen IKT-Störungen zu erhöhen und gegen Cyberrisiken besser gewappnet zu sein, wurde mit DORA eine einheitliche Regulierung geschaffen, die heute für alle gilt.

Globale Auswirkungen



Einheitliche Resilienzstandards mit internationaler Wirkung

DORA schafft einen klaren und verbindlichen Rahmen für das IKT-Risikomanagement in der EU und wirkt weit über Europa hinaus: Auch internationale IKT-Dienstleister und SaaS-Anbieter, die mit europäischen Finanzunternehmen zusammenarbeiten, müssen DORA-konforme Prozesse und Strukturen vorweisen.

Zentral ist dabei:

Alle Anbieter kritischer IKT-Dienstleistungen, die unabhängig vom Sitz in Europa tätig sind, unterliegen den DORA-Vorgaben. Dazu zählen:

- IKT-Anbieter für Finanzdienstleistungen
- Technologielieferanten mit hoher Abhängigkeit
- SaaS-Plattformen mit Relevanz für Betriebsfähigkeit und Sicherheit

Wer DORA nicht erfüllt, riskiert empfindliche Sanktionen. Die Europäische Aufsichtsbehörde kann Bußgelder bis zu *1 % des durchschnittlichen weltweiten Tagesumsatzes* verhängen.

Neue Anforderungen für globale Partner

DORA schreibt auch vor, dass *Finanzinstitute keine kritischen IKT-Services* von Anbietern nutzen dürfen, die keinen Sitz oder keine gesicherte Präsenz in einem EU-Mitgliedsstaat haben. Auch Tochtergesellschaften, die erst nach der Klassifikation eines Anbieters als „kritisch“ in der EU gegründet wurden, gelten unter Umständen nicht als zulässig.

Dies betrifft insbesondere globale Dienstleister mit Sitz außerhalb des EWR, die künftig nachweisen müssen, dass sie den europäischen Gerichtsbarkeits- und Datenanforderungen unterliegen. Diese Vorgabe ist strategisch bedeutsam. Auch wenn die Kommission hierfür *keine explizite Begründung* liefert, ist sie im Kontext von Cyber-Resilienz und Datenhoheit zu verstehen.

Wer betroffen ist und was nicht geregelt wird

Die DORA-Verordnung gilt heute verbindlich für nahezu alle Finanzmarktteilnehmenden der EU – darunter Kreditinstitute, Zahlungsdienstleister, Versicherungen, Investmentgesellschaften, Datenbereitsteller sowie deren kritische IKT-Dienstleister.

Ziel der DORA-Verordnung ist eine harmonisierte, sektorübergreifende Regulierung für das IKT-Risikomanagement.

Die Verordnung enthält jedoch keine eigenständigen Anforderungen an die Speicherung oder Verarbeitung von Daten innerhalb der Union. Sie verweist stattdessen auf bestehende handelsrechtliche Verpflichtungen und Ausnahmen.

Was gilt für Anbieter außerhalb des EWR?

Für Drittstaaten-Anbieter, die außerhalb des europäischen Geltungsbereichs agieren, wird derzeit ein eigenes Überwachungsrahmenwerk erarbeitet. Dieses soll definieren, unter welchen Voraussetzungen solche Anbieter dennoch regulierungskonform beauftragt werden können – z. B. durch vertragliche Sicherheiten oder bewährte Kontrollmechanismen.

Differenzierung nach Größe, Tätigkeit und Risiko

Nicht alle Unternehmen im Finanzsektor sind gleichermaßen betroffen. Der DORA-Anwendungsbereich unterscheidet z. B. nach:

- Unternehmensgröße
- Risikoprofil
- Kritikalität der angebotenen Services für den Finanzmarkt

Beispiel: *Unternehmen für Karten- oder Zahlungssysteme unterliegen derzeit nicht der DORA-Verordnung. Gleiches gilt für Abschlussprüfer, deren mögliche Einbeziehung derzeit von der Europäischen Kommission geprüft wird. Eine Entscheidung hierzu wird bis Ende 2026 erwartet.*

Balance zwischen Sicherheit und Marktzugang

Um den Zugang neuer Marktteilnehmer nicht zu erschweren, wurde eine gleitende Skala für Schwellenwerte eingeführt. Sie ermöglicht eine abgestufte Anwendung von DORA – je größer das Risiko der Operation, desto stärker die regulatorischen Anforderungen. Dies zielt auf einen Schutz ohne Innovationsbremse ab.

Harmonisierung statt Flickenteppich

Was DORA besser macht und wo es Unterschiede gibt

DORA ist das erste europäische Regelwerk, das eine einheitliche und rechtsverbindliche Struktur für das IKT-Risikomanagement im Finanzsektor schafft – mit klaren Verantwortlichkeiten, verbindlichen Prüfroutinen und stringenter Aufsicht.

Bisherige Vorschriften, etwa aus DSGVO, NIS-Richtlinie oder nationalem Aufsichtsrecht, wurden häufig unterschiedlich interpretiert oder unvollständig umgesetzt. Das führte zu Unsicherheiten in der Umsetzung und zu erhöhtem Aufwand bei internationalen Finanzakteuren.

DORA setzt hier an:

- Gemeinsame Standards für alle regulierten Institute
- Verbindliche Regeln statt bloßer Empfehlungen
- Starke Aufsicht und durchgängiges Kontrollmodell

Was ist der Unterschied zu NIS/NIS2?

Die NIS-Richtlinien betreffen alle kritischen Infrastrukturen – von Energie bis Transport. DORA hingegen gilt ausschließlich für:

- Finanzmarktakteure innerhalb der EU
- Kritische IKT-Dienstleister, die von Finanzunternehmen beauftragt werden

Beide Regelwerke gelten parallel, allerdings regelt DORA spezifischer und detaillierter den Finanzsektor.
Im Konfliktfall gelten laut Lex-specialis-Grundsatz die DORA-Vorgaben.

Zur Einordnung: Während das NIST Cyber Security Framework (CSF) nur Empfehlungen ausspricht, fordert DORA regulatorische Nachweise.

Einheitliche Kontrolle durch europäische Aufsichtsbehörden

Um sicherzustellen, dass DORA nicht nur auf dem Papier existiert, wurde ein stringentes Aufsichtskonzept etabliert.

Für jedes regulierte Unternehmen wird ein sogenannter CTPP (Critical Third-Party Provider) benannt. Die Überwachung dieser CTPPs übernehmen jeweils die zuständigen ESA-Behörden:

- EBA – European Banking Authority [1]
- EIOPA – European Insurance and Occupational Pensions Authority [2]
- ESMA – European Securities and Markets Authority [3]

Diese Behörden sind dafür verantwortlich, die Einhaltung der Vorgaben bei Dienstleistern zu kontrollieren und das Risiko systemischer Ausfälle frühzeitig zu minimieren.

Warum das wichtig ist

Gerade kritische Drittanbieter wie Cloud-Dienste oder KYC-Plattformen betreuen viele Finanzinstitute gleichzeitig. Ein Ausfall kann daher Kaskadeneffekte auslösen – mit potenziell systemischen Folgen für die Finanzmärkte. DORA will genau das verhindern

[1] The European Banking Authority
[2] The European Insurance and Occupational Pensions Authority
[3] The European Securities and Markets Authority

Die fünf DORA-Säulen

Die DORA-Verordnung ist seit dem 17. Januar 2025 für Finanzinstitute verbindlich. Von Cybertests bis Drittanbietersteuerung definiert sie fünf Säulen zur Sicherung der digitalen Resilienz. Für Banken bedeutet das: Sie müssen operative Resilienz nicht nur nachweisen, sondern systematisch aufbauen – transparent, prüfbar und regulatorisch konform.

1. Digitale Belastungstests:
Angreifbarkeit simulieren, Resilienz beweisen

Finanzinstitute müssen regelmäßig *bedrohungs-basierte Penetrationstests (TLPT)* durchführen. Kritische IT-Dienstleister sind verpflichtend einzubinden. Ziel ist es, Schwachstellen systematisch aufzudecken und zu beheben, bevor reale Angriffe sie ausnutzen.

Für Banken bedeutet das: jährliche Testzyklen, technische Transparenz und dokumentierte Nachweise gegenüber Aufsichtsbehörden.

2. IKT-Risikomanagement:
Governance greifbar machen

DORA fordert ein umfassendes, dokumentiertes Management aller IKT-Risiken inklusive Frühwarnindikatoren, Reaktionsstrategien und Business-Continuity-Plänen.

Das Besondere: Die Verantwortung liegt explizit bei der Geschäftsleitung. Risiken müssen identifiziert, bewertet und steuerbar gemacht werden – kontinuierlich und mit revisionssicherem Monitoring.

3. IKT-Vorfälle melden:
schnell, strukturiert, europaweit

Jedes relevante IKT-Ereignis muss gemeldet werden: vom Ausfall bis zur Sicherheitslücke. Berichte gehen zentral an den EU-Hub statt an mehrere nationale Stellen.

Ziel: einheitliche Verfahren, weniger Meldepflichten, mehr Erkenntnisse.

Pflicht: ein Monat Zeit für einen Ursachenbericht bei schwerwiegenden Vorfällen inklusive Maßnahmen und Auswirkungen.

4. Informationsaustausch: lernen aus der Gemeinschaft

DORA fördert den sicheren Austausch von Cyberbedrohungsdaten, auch unter Finanzinstituten. Ziel ist es, Bedrohungen frühzeitig zu erkennen und kollektive Resilienz aufzubauen.

Erlaubt: Austausch auch innerhalb von Instituten, vorausgesetzt, er erfolgt anonymisiert und datenschutzkonform.

5. Drittanbieter-Steuerung: Kontrolle über kritische IKT

Banken müssen nachweisen, wie sie *kritische IKT-Dienstleister überwachen* inklusive vertraglicher Absicherung und Exit-Szenarien. Besonders relevant ist dies für Cloud-Dienste.

Neu: Die ESAs (z. B. EBA oder ESMA) dürfen bei Regelverstößen Strafen bis zu 1 % des weltweiten Tagesumsatzes verhängen – für bis zu sechs Monate. [4]

[4] EUR-Lex

Was wir für Sie tun können

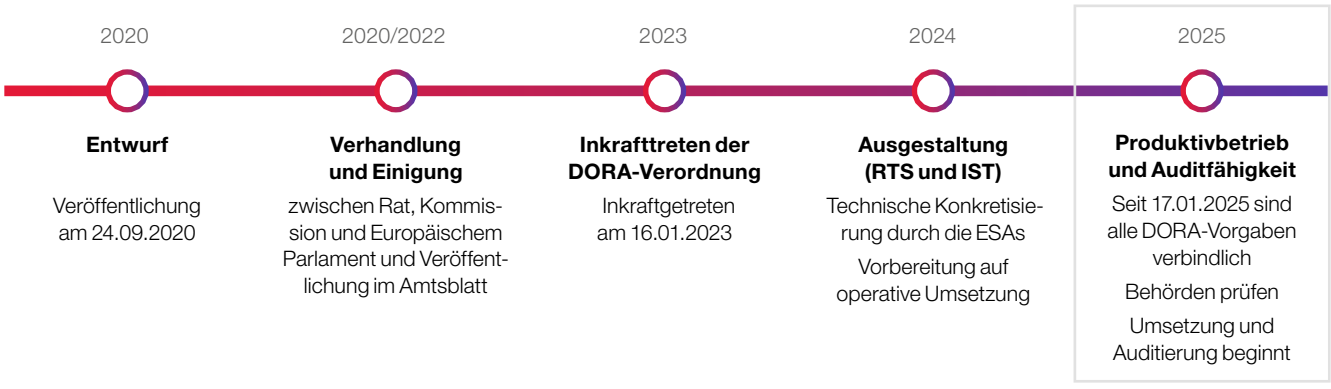
DORA betrifft über 20.000 Finanzunternehmen und IKT-Dienstleister allein in der EU. Seit dem 17. Januar 2025 gelten die Anforderungen verbindlich: Aufsicht, Prüfung und Auditierung haben begonnen.

Für viele Banken ist DORA nicht nur eine regulatorische Pflicht, sondern ein Katalysator für nachhaltige Resilienz. Die Verordnung schafft erstmals einen gemeinsamen Rahmen für Cybersicherheit und IKT-Risikomanagement – und verändert dadurch bestehende Prozesse, Verantwortlichkeiten und Governance-Strukturen.

Gleichzeitig bleibt die Umsetzungsfrist kurz. Wer jetzt noch wartet, riskiert unnötige Komplexität, Zeitdruck und Ineffizienzen. *Unsere Empfehlung:* Beginnen Sie jetzt mit der gezielten Prüfung Ihrer IKT-Prozesse, Verträge und Kontrollmodelle.

Wir unterstützen Sie dabei – mit einem klar strukturierten Fahrplan und einem erfahrenen Team von Expertinnen und Experten.

Gemeinsam schaffen wir eine belastbare Grundlage, mit der Sie alle DORA-Vorgaben sicher und auditfähig erfüllen.



Über CGI

Als globaler Dienstleister für IT- und Geschäftsprozesse entwickeln wir für unsere Kunden ergebnisorientierte Strategien für ihre digitale Transformation und unterstützen sie mit End-to-End-Services, durch die sie greifbare Ergebnisse erzielen. Unsere weltweit 94.000 Mitarbeitenden entwickeln innovative Lösungen wie KI entlang der gesamten Wertschöpfungskette und werden im Hinblick auf Zeit- und Budgettreue regelmäßig mit Bestnoten bewertet.

Für weitere Informationen besuchen Sie uns auf cgi.com/de