

# DIGITAL OPERATIONAL RESILIENCE ACT RECHTSKONFORM UMSETZEN



DORA-Resilienz | Gesetzeskonform integriert.

Cyberisiken | Proaktiv beherrscht.

Strategien | Mandantenorientiert gestaltet.

## Überblick

Der Digital Operational Resilience Act regelt die Anforderungen an die Widerstandsfähigkeit digitaler Systeme im Finanzsektor von Banken über Versicherungen bis zu IT-Dienstleistern für Finanzunternehmen. Digitale Prozesse sind auch aus der Finanzwirtschaft nicht mehr wegzudenken und eröffnen neue Wege Effizienz und neue Dienstleistungsangebote. Doch die zunehmende Vernetzung bringt auch regulatorische Herausforderungen mit sich. Unternehmen müssen Risiken frühzeitig erkennen, technische Vorkehrungen treffen und die Betriebsfähigkeit bei Störungen sicherstellen über den gesamten digitalen Lebenszyklus hinweg. Mit DORA ist ein einheitlicher Rechtsrahmen in der EU geschaffen, dessen Einhaltung bei zunehmender Vernetzung zusätzliche Herausforderungen mit sich bringt.



## Betroffene Unternehmen

### Finanzunternehmen

Unternehmen aus dem Finanzsektor wie Banken, Versicherungen, Zahlungsdienstleister oder Wertpapierfirmen müssen sicherstellen, dass ihre digitalen Systeme und Prozesse den Anforderungen an digitale operationale Resilienz entsprechen, um IT-Risiken besser zu beherrschen und Vorfälle wirksam zu bewältigen.

### IKT-Drittdienstleister

Dienstleister wie ZK-Unternehmen, Softwarehäuser oder Hostingdienste, die IT-Leistungen für Finanzunternehmen erbringen, müssen vertraglich verpflichtet werden, DORA-konform zu handeln und Sicherheitsstandards einzuhalten. Kritische IKT-Dienstleister wie Cloud- oder Netzwerkbetreiber unterliegen zusätzlicher Aufsicht und müssen besondere Resilienzmaßnahmen nachweisen.

### Unternehmensgröße

Die DORA-Verordnung gilt unabhängig von der Unternehmensgröße. Lediglich für sehr kleine Ins geringem Risikoprofil gelten vereinfachte Vorgaben.

### Geografische Reichweite

Die Verordnung betrifft sowohl in der EU Unternehmen als auch außereuropäische Unternehmen, die IKT-Dienste für Finanzunternehmen im EU-Raum erbringen.

### Ausnahmen

Vom Anwendungsbereich ausgenommen sind etwa kleinere Versicherungsvertreter, bestimmte Einrichtungen der Altersversorgung sowie einzelne Finanzakteure, die bereits durch andere EU-Vorgaben explizit ausgenommen sind.

## Sanktionen

Verstöße gegen die DORA-Verordnung können empfindliche Folgen haben. Die nationalen Aufsichtsbehörden sind verpflichtet, wirksame, verhältnismäßige und abschreckende Sanktionen zu verhängen. Je nach Art und Schwere des Verstoßes können diese von formellen Anordnungen bis hin zu hohen Geldbußen i.H.v. 2 % des weltweiten Jahresumsatzes reichen. Auch Maßnahmen zur öffentlichen Bekanntmachung oder der Entzug von Zulassungen sind möglich.

## Fristen

**17. Januar 2025:** DORA tritt vollständig in Kraft. Ab diesem Datum müssen alle beaufsichtigten Finanzunternehmen und relevanten IKT-Dienstleister die Anforderungen zur digitalen Resilienz erfüllen, etwa beim Risikomanagement, bei Meldepflichten und bei der Steuerung von Drittanbietern.

**Bis Ende 2026:** Nationale Regelwerke wie die BAIT gelten übergangsweise weiter. Ab 1. Januar 2027 ersetzen DORA und die ergänzenden EU-Rechtsakte alle bisherigen IT-Vorgaben vollständig.





## Neue Pflichten (Auszug)

### Finanzunternehmen

- IKT-Risikomanagement implementieren
- DORA-konformes Vertragsmanagement für IKT-Dienstleister
- Technische Dokumentation und Informationsregister führen
- Resilienzbewertung vor Einsatz kritischer Systeme durchführen
- Meldepflichten bei schwerwiegenden IKT-Vorfällen beachten
- Informationen zur digitalen Resilienz klar kommunizieren
- Systeme müssen auch bei Störungen funktionsfähig

### IKT-Dienstleister

- Webschnittstellen und Anwendungen sicher und stabil gestalten, Cybersicherheitsstandards implementieren
- Meldung etwaiger Sicherheitsvorfälle an betroffene Finanzkunden
- Anpassung der eigenen AGB für Finanzkunden Vorhalten belastbarer Notfall- und Wiederherstellungspläne
- Informationspflichten gegenüber Finanzkunden und Behörden
- Weitergabe von Pflichten an Subdienstleister

## Unsere Beratung zur NIS-2-Compliance

### Beratung für Finanzunternehmen

#### Initialanalyse und Bestandsaufnahme

- Prüfung, ob und welche Systeme und Prozesse unter DORA fallen (DORA-Betroffenheitsanalyse)
- Identifikation von Resilienzanforderungen und regulatorischen Pflichten
- GAP-Analyse

#### Resilienzbewertung und Konformität

- Anpassung der Verträge mit IKT-Dienstleistern
- Unterstützung bei der Prüfung kritischer Funktionen und Nutzerpfade
- Beratung zur Durchführung von Resilienztests und Dokumentationspflichten

#### Informationspflichten und Transparenz

- Erstellung der rechtlichen DORA-Dokumentation, insb. von Sicherheitsrichtlinien und dem Informationsregister

#### Meldung und Behördenkommunikation

- Unterstützung bei der Kommunikation mit Aufsichtsbehörden
- Begleitung bei Meldungen, Prüfungen und Maßnahmen bei Vorfällen

### Beratung für IKT-Dienstleister

#### Verantwortung und Dienstleistersteuerung

- Prüfung vertraglicher Pflichten gegenüber Finanzunternehmen und Übernahme der Vertragsverhandlungen
- GAP-Analyse
- Begleitung bei der Umsetzung von Sicherheits- und Resilienzmaßnahmen
- Bereitstellung von Informationen zu Transparenzpflichten
- Unterstützung bei der Kommunikation mit Kunden und Behörden
- Schulungen von Geschäftsleitung und Mitarbeitern



Vertrauen Sie auf unsere Expertise –  
als starker Partner für rechtssichere  
und praxisnahe Lösungen rund um das  
Thema Informationssicherheit

Berlin    Hamburg  
Chemnitz    Köln  
Düsseldorf    München  
Frankfurt    Stuttgart

