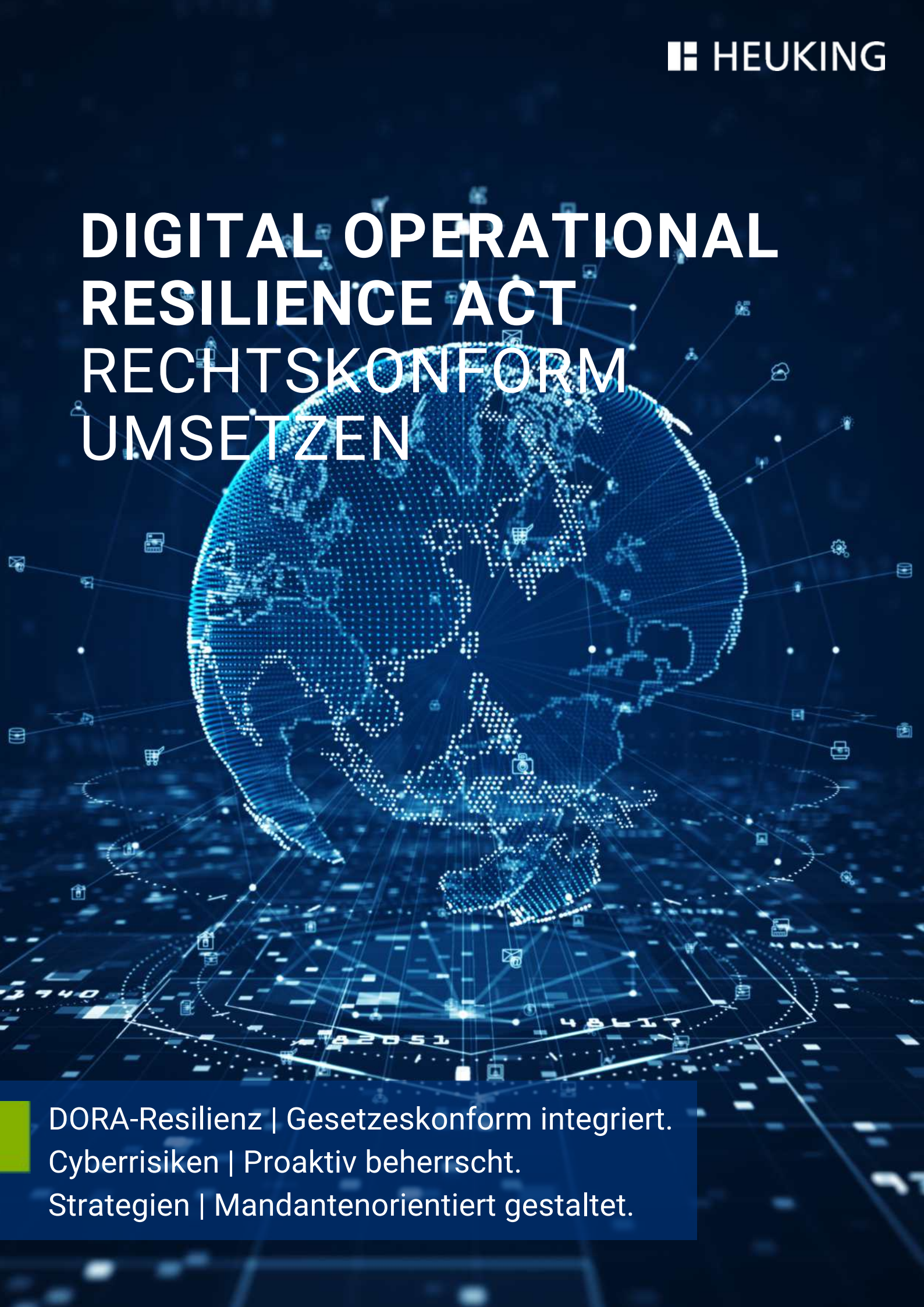
HEUKING

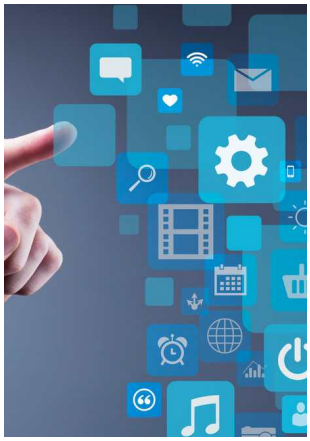
DIGITAL OPERATIONAL RESILIENCE ACT RECHTSKONFORM UMSETZEN



DORA-Resilienz | Gesetzeskonform integriert.
Cyberrisiken | Proaktiv beherrscht.
Strategien | Mandantenorientiert gestaltet.

Überblick

Der Digital Operational Resilience Act regelt die Anforderungen an die Widerstandsfähigkeit digitaler Systeme im Finanzsektor von Banken bis zu IT-Dienstleistern. Digitale Prozesse sind heute aus Finanzwirtschaft, Alltag und Regulierung nicht mehr wegzudenken und ermöglichen neue Wege für Sicherheit und Effizienz, etwa durch robuste IT-Strukturen, klare Meldewege oder standardisierte Prüfverfahren. Mit DORA schafft die EU einen einheitlichen Rechtsrahmen. 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.



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

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

Unternehmensgröße

Die DORA-Verordnung gilt unabhängig von der Größe des Unternehmens. Lediglich für sehr kleine Institute mit geringem Risikoprofil gelten vereinfachte Vorgaben.

Geografische Reichweite

Die Verordnung betrifft sowohl in der EU ansässige Unternehmen als auch außereuropäische Dienstleister, sofern sie IKT-Dienste für regulierte Finanzunternehmen im EU-Raum erbringen

Ausnahmen

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

Umsetzungsfristen

- **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)

Finanzinstitute

- IKT-Risikomanagement umsetzen
- 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 bleiben

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 DORA-Compliance

Beratung für Finanzinstitute

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

- 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
- Bereitstellung resilienzbezogener Informationen für Aufsicht und Kunden

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 Finanzinstituten und Übernahme der Vertragsverhandlungen
- DORA GAP-Analyse
- Begleitung bei der Umsetzung von Sicherheits- und Resilienzmaßnahmen
- Bereitstellung von Informationen zu Transparenzpflichten
- Unterstützung bei der Kommunikation mit Kunden und Behörden
- Schulung von Geschäftsleitung und Mitarbeitern

HEUKING

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

Dr. Hans Markus Wulf
Rechtsanwalt | Partner
Fachanwalt für IT-Recht
ISO/IEC 27001 Auditor (TÜV)
CIPP/E, Datenschutzauditor (TÜV)

m.wulf@heuking.de

Berlin
Chemnitz
Düsseldorf
Frankfurt
Hamburg
Köln
München
Stuttgart

JUVE Handbuch 2024|2025 Wirtschafts Kanzleien

FÜHRENDE KANZLEI Legal500 DEUTSCHLAND 2025

Chambers TOP RANKED Germany 2025 HEUKING

heuking.de