DORA: KONFORMITÄT ALTERNATIVLOS. NICHT CHANCENLOS.

Inklusive Schnell-Checkliste und KI-Optionen

adesso

Die Einführung neuer Verordnungen führt oft zu Diskussionen über Aufwand und Nutzen. Doch wenn der Zeitpunkt des Inkrafttretens näher rückt, zählt nur noch eines: die effektive Umsetzung.

So auch bei DORA (Digital Operational Resilience Act), die im Januar 2025 in Kraft tritt. Diese Verordnung stärkt die Widerstandsfähigkeit des EU-Finanzsektors gegen Bedrohungen aus dem Cyberraum und IKT-Risiken. Finanzunternehmen, die von der DORA-Verordnung betroffen sind, müssen bis zum 17. Januar 2025 alle aufsichtsrechtlichen Anforderungen erfüllen. Um diese Herausforderung als (Wettbewerbs-)Vorteil zu nutzen, müssen Sie DORA schlank, fristgerecht und mit maximaler Effizienz umsetzen. Wer jetzt handelt, kann nicht nur Risiken minimieren, sondern sich auch einen Wettbewerbsvorteil sichern.

JETZT GENAU HINSCHAUEN. DAS LOHNT SICH.

Erfahren Sie hier mehr über die wichtigsten Bestandteile von DORA sowie die Auswirkungen und Handlungsanforderungen für Finanzunternehmen. Unsere kompakte Checkliste ermöglicht Ihnen, den eigenen DORA-Reifegrad besser einzuschätzen.

Unser Ziel ist, dass Sie diese regulatorischen Verpflichtungen optimal für Ihre Organisation umsetzen. Unser Ansatz: **DORA.KI** – das adesso Analysetool auf GenAI-Basis. Die Anwendung ermöglicht es Ihnen, alle bestehenden Verträge mit IKT-Dienstleistern initial und dann kontinuierlich zu analysieren.

I. Warum DORA?

Zweck und Anwendungsbereiche

DORA zielt darauf ab, ein einheitliches Rahmenwerk für die digitale operative Resilienz im Finanzsektor der EU zu gewährleisten. Die Verordnung gilt für eine Vielzahl von Finanzunternehmen, einschließlich Banken, Zahlungsinstituten, Versicherungsunternehmen sowie Drittanbietern von kritischen Technologiedienstleistungen, die für betroffene Institute arbeiten. Inhaltlich werden strenge Maßnahmen vorgegeben, um sicherzustellen, dass alle betroffenen Organisationen in der Lage sind, IKT-bezogene Störungen jeglicher Art abzuwehren bzw. die damit verbundenen Auswirkungen minimal zu halten. Dazu gehört eine optimierte Reaktionsfähigkeit bei entsprechenden Vorfällen sowie Anpassungen, die eine schnelle Reaktivierung bei IKT-bedingten Schadensfällen ermöglichen. Nicht alle (Cyber-)Gefahren lassen sich komplett ausschließen – umso wichtiger ist es, auf kritische Situationen optimal vorbereitet zu sein und jederzeitige Handlungsfähigkeit zu gewährleisten.

II. Warum ist das Einhalten für Unternehmen wichtig?

Erhöhte Sicherheit und Resilienz

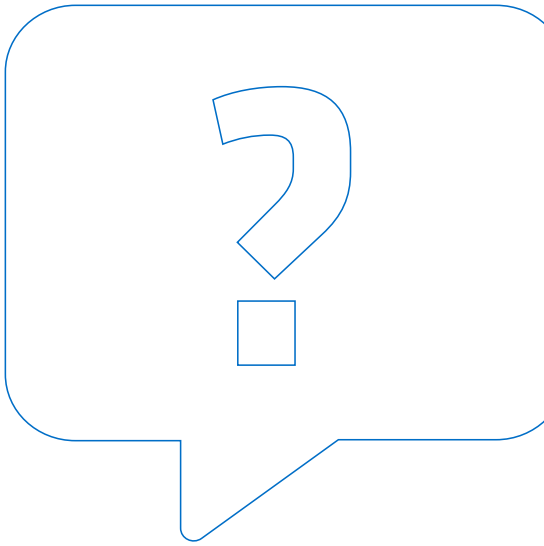
Der besondere Fokus auf das IKT-Risikomanagement und die Vorfallberichterstattung innerhalb von DORA sind entscheidend für die Stärkung der allgemeinen Sicherheitslage im Finanzwesen. Mit der Durchsetzung strenger und kontinuierlicher Kontrollen werden Unternehmen faktisch resilienter gegen Cyberangriffe, Datenlecks und Systemausfälle. Davon profitiert der operative Betrieb nachhaltig.

Regulatorische Konformität und Vermeidung von Strafen

Das Einhalten von DORA ist nicht optional. Verstöße können zu erheblichen Geldstrafen und Reputationsschäden führen. Finanzinstitute müssen die Vorschriften priorisieren, um Strafen zu vermeiden und das Vertrauen von Kunden, Partnern und Aufsichtsbehörden zu bewahren.

Betriebliche Effizienz und Risikominderung

DORA fördert einen proaktiven Ansatz im Risikomanagement und verpflichtet Unternehmen, Schwachstellen zu erkennen, bevor sie ausgenutzt werden. Durch die Umsetzung der DORA-Anforderungen können Unternehmen ihre Effizienz steigern und die Wahrscheinlichkeit kostspieliger Störungen signifikant verringern.



III. Betrifft DORA mein Unternehmen?

Banken- und Finanzdienstleistungen

Hier finden Sie eine Auflistung aller Unternehmens- und Institutsformen, die von DORA betroffen sind. Sollten Sie aufgrund der spezifischen Ausrichtung Ihres individuellen Geschäftsmodells innerhalb der Finanzindustrie noch offene Fragen bezüglich Ihrer DORA-Betroffenheit haben, stehen wir Ihnen jederzeit zu Ihrer Verfügung.

Artikel 2 – Geltungsbereich

(1) Unbeschadet der Absätze 3 und 4 gilt diese Verordnung für folgende Unternehmen:

a) Kreditinstitute,
b) Zahlungsinstitute, einschließlich gemäß der Richtlinie (EU) 2015/2366 ausgenommene Zahlungsinstitute,
c) Kontoinformationsdienstleister,
d) E-Geld-Institute, einschließlich gemäß der Richtlinie 2009/110/EG ausgenommene E-Geld-Institute,
e) Wertpapierfirmen,
f) Anbieter von Krypto-Dienstleistungen, die gemäß einer Verordnung des Europäischen Parlaments und des Rates über Märkte von Krypto-Werten und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 (im Folgenden „Verordnung über Märkte von Krypto-Werten") 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-Drittdienstleister.

DORA-CHECKLISTE. FRAGEN, DIE SIE SICH JETZT STELLEN SOLLTEN.

1. Risikomanagement und Governance

Können Sie Ihre IKT-Risiken bereits ganzheitlich bewerten und kennen Sie alle (DORA-) relevanten Cybersicherheitsmaßnahmen, die in Ihrer Organisation ab Januar 2025 nachweispflichtig abrufbar sein müssen?

☐ Ja ☐ Nein ☐ Unklar

2. Vorfälle behandeln. Berichte erstatten.

Verfügen Sie bereits über einsatzfähige Systeme, die ein automatisiertes Monitoring sowie eine schnelle Vorfallsteuerung ermöglichen – inklusive regelkonformer Berichte?

☐ Ja ☐ Nein ☐ Unklar

3. Resilienz: Testen. Testen. Testen.

Haben Sie bereits ausreichend dimensionierte – automatisierte – Testprozesse aufgesetzt, um Ihre IKT-Systeme und Ihre Verfahren regelmäßig zu kontrollieren und mögliche ‚Einfallstore' – z. B. für Cyberangriffe – frühzeitig zu identifizieren?

☐ Ja ☐ Nein ☐ Unklar

4. Der (nicht) unsichtbare Dritte.

Können Sie bereits nachweisen, dass zwischen Ihnen und den für Sie tätigen Drittanbietern vertragliche Vereinbarungen bestehen, die alle Abhängigkeiten offenlegen? Und ob diese Vereinbarungen die kritischen Prozesse und Funktionen ausreichend absichern und damit die DORA-Konformität für beide Seiten nachweisen?

☐ Ja ☐ Nein ☐ Unklar

5. Im ständigen geregelten Austausch bleiben.

Ist der ständige sowie standardisierte Austausch zu aktuellen Cyberrisiken zwischen allen relevanten Einheiten in Ihrer Organisation sowie zwischen Ihren Einheiten und Drittanbietern – inklusive klarer Rollenprofile und Zuordnungen – bereits belegbar implementiert?

☐ Ja ☐ Nein ☐ Unklar

Auch wenn fünf Fragen und deren Beantwortung kein detailliertes Bild zeichnen: Ein Trend lässt sich für Sie ablesen. „Nein" und „Unklar" sollten ab Inkrafttreten von DORA keine Option mehr sein. Unsere adesso-Expertinnen und -Experten stehen jederzeit für eine unverbindliche Lageeinschätzung zur Verfügung.

DORA UND KI? DAS PASST!

DORA.KI bietet JETZT Unterstützung bei der Einhaltung der Vorschriften und ermöglicht es Ihnen, IKT-Risiken proaktiv und effizient in einer zunehmend komplexen regulatorischen Umgebung zu managen.

DORA.KI Neue Herausforderungen. Neue Lösungswege.

Automatisiertes Compliance-Management

Wir entwickelten DORA.KI, um Unternehmen bei der Navigation durch die Komplexität der DORA-Compliance zu unterstützen. Durch automatisierte Überwachung und Berichterstattung hilft DORA.KI Institutionen, einen Echtzeitüberblick über ihren Compliance-Status im IKT-Drittparteienrisikomanagement zu behalten und sicherzustellen, dass sie alle regulatorischen Anforderungen erfüllen.

Risikobewertung und -management

DORA.KI bietet robuste Risikobewertungsfunktionen, die es Unternehmen ermöglichen, potenzielle IKT-Risiken zu erkennen und zu bewältigen, bevor sie eskalieren. Dieser proaktive Ansatz entspricht dem Schwerpunkt von DORA auf Prävention und Risikominderung.

Risikomanagement bei Drittanbietern

DORA.KI bietet Features zur Bewertung und Überwachung der Resilienz von IKT-Drittanbietern und stellt sicher, dass Unternehmen vor Schwachstellen in ihren Lieferketten geschützt sind.

Die wesentlichen Erfolgsparameter von DORA.KI im Einsatz für den Finanzsektor:

- Zeit
- Kosten
- Risiko

KONTAKT

Kommen Sie **jetzt** auf uns zu und erfahren Sie, wie KI Ihnen bei der Umsetzung von DORA unmittelbar helfen kann.

Marc Dielmann
Business Development Director

M +49 162 2921395
E Marc.Dielmann@adesso.de

Tobias Dieter
Principal Consultant

M +49 152 38860995
E tobias.dieter@adesso.de

adesso SE
Adessoplatz 1
44269 Dortmund
Deutschland
T +49 231 7000-7000
F +49 231 7000-1000
E info@adesso.de
www.adesso.de

adesso