PRESSEMITTEILUNG | OKTOBER 2024

DORA-Verordnung – Neue verpflichtende Cybersicherheitsanforderungen ab 17.01.2025

Die Frist zur Umsetzung der **DORA-Verordnung** (Digital Operational Resilience Act) läuft am 17.01.2025 ab. Verpflichtet zur Umsetzung sind unter anderem alle **erlaubten Kapitalverwaltungsgesellschaften und Wertpapierinstitute.** Hauptziel ist es, die digitale Resilienz und Cybersicherheit von Finanzmarktteilnehmern zu stärken und sicherzustellen, dass Unternehmen in der Lage sind, auf Cyberangriffe und IT-Störungen schnell und effektiv zu reagieren.

Dies bedeutet jedoch, dass sich die Verpflichteten auf **zahlreiche neue und komplexe Anforderungen** einstellen müssen, die über den bisherigen KAIT- und BAIT-Standards hinausgehen. Das sind unter anderem:

- **Steuerung von IKT-Drittdienstleistern:** Vereinbarung strengere Vertragsanforderungen und Durchführung einer regelmäßigen Risikobewertung von wichtigen und kritischen IKT-Drittdienstleister. Dokumentation und Berichterstattung bei der Aufsicht nach Aufforderung, um sicherzustellen, dass IKT-Drittdienstleister ebenfalls den Cybersicherheitsstandards entsprechen.

- **Meldung IKT-bezogener Vorfälle:** Etablierung von technischen Maßnahmen zum Erkennen und Abwehren von Cyberangriffen. Dazu gehört das technische Monitoring, regelmäßige Überprüfung und Aktualisierung von Sicherheitssystemen, die Klassifizierung von Vorfällen und die Meldung schwerwiegender Vorfälle an die zuständigen Behörden.

- **IKT-Risikomanagementrahmen:** Implementierung eines IKT-Risikomanagements, welches die systematische Identifizierung, Bewertung, Überwachung und Steuerung von Risiken umfasst, die sich aus der Nutzung von Informations- und Kommunikationstechnologie (IKT) ergeben, um die operationelle Resilienz zu stärken und Cyberbedrohungen effektiv entgegenzuwirken.

Die DORA-Verordnung ist ein **wichtiger Schritt** in Richtung einer sichereren und widerstandsfähigeren digitalen Zukunft für den Finanzsektor. Sie erfordert jedoch **große Anstrengungen**, um die vielen neuen Regelungen zu erfüllen und die digitale Sicherheit zu gewährleisten, da in vielen Fällen internen Strukturen, Prozesse und IT-Systeme grundlegend überarbeitet werden müssen, um den neuen Vorgaben gerecht zu werden.
Wer diese Anforderungen nicht ernst nimmt, riskiert nicht nur Bußgelder, sondern auch massive reputationsschädigende und finanzielle Folgen im Fall eines Cyberangriffs.

Pressekontakt: orangekey consulting GmbH
Petra Klein, Geschäftsführerin
Hütten 87
20355 Hamburg

Telefon: 040 328 929 71
Mobil: 0173 201 88 81
E-Mail: petra.klein@orange-key.de
www.orange-key.de