Digitale operationale Resilienz

Die neue EU-Verordnung zur digitalen operationalen Resilienz im Finanzsektor (DORA) legt ihren Fokus auf eine angemessene Cybersicherheit.

Im Dezember des vergangenen Jahres wurde eine neue, für Finanzunternehmen compliancerelevante Verordnung durch die europäische Legislative verabschiedet. Die Verordnung zur digitalen operationalen Resilienz im Finanzsektor – **D**igital **O**perational **R**esilience **A**ct, kurz DORA – trägt der zunehmenden Digitalisierung und Vernetzung dieses Sektors Rechnung. Sie normiert Standards, für einen EU-weit harmonisierten Umgang mit Risiken aus der Nutzung von Informations- und Kommunikationstechnologien (IKT).

Als „digitale operationale Resilienz" im Sinne der DORA-Verordnung wird die Fähigkeit verstanden, operative Integrität und Betriebszuverlässigkeit aufzubauen, fortwährend zu gewährleisten und zu überprüfen. Dazu gehören alle Maßnahmen des Instituts, die notwendig sind, um die Sicherheit der Informationssysteme und Netzwerke zur kontinuierlichen Erbringung von Finanzdienstleistungen und deren Qualität zu gewährleisten.

Mit der DORA werden damit erstmals konkrete und konsolidierte Anforderungen an die Finanzunternehmen gerichtet, die nicht durch finanzielle Resilienz zur Finanzstabilität und Marktintegrität beitragen, sondern diese auch durch angemessene Cybersicherheit stärken.

Im Fokus steht nunmehr konkret das operationelle Risiko aus dem Bezug von Informations- und Kommunikationstechnologie und somit die Kategorie der nicht-finanziellen Risiken.

DORA-Check-up

Wie bereits bei der Veröffentlichung der bankaufsichtlichen Anforderungen an die IT (BAIT) unterstützt die DZ CompliancePartner Sie gerne bei der Umsetzung der DORA. So führen wir gemeinsam mit Ihnen eine Reifegradanalyse Ihres Unternehmens bzgl. der DORA durch und ermitteln so relevante Gaps. Basierend auf den Ergebnissen können anschließend angemessene Handlungsbedarfe ermittelt und eine Priorisierung der nachfolgenden Schritte vorgenommen werden. So kann der Aufwand für die Umsetzung der komplexen Anforderungen bestmöglich eingeschätzt werden. Mit Veröffentlichung der Rechtsakte im kommenden Jahr erhalten Sie eine konkrete Maßnahmenliste von uns, anhand derer Sie sämtliche Anforderungen anhand der Zuständigkeiten festhalten und terminieren können.

Umsetzungsfristen und -anforderungen

Analog der Datenschutz-Grundverordnung (DSGVO), existiert eine Implementierungsfrist von 24 Monaten, womit die DORA verbindlich ab dem 17. Januar 2025 in den Mitgliedstaaten anzuwenden ist.

Inhaltlich soll das hohe Niveau an digitaler operationaler Resilienz durch folgende Anforderungen erreicht werden:

Chantal Pfeffer
Abteilungsleiterin
Informationssicherheit & Datenschutz,
E-Mail: chantal.pfeffer@dz-cp.de

Michael Switalla
Abteilungsleiter
Informationssicherheit & Datenschutz,
E-Mail: michael.switalla@dz-cp.de

- Risikomanagement im Bereich der Informations- und Kommunikationstechnologie (IKT)
- Meldung schwerwiegender IKT-bezogener Vorfälle und – auf freiwilliger Basis – erheblicher Cyber-Bedrohungen an die zuständigen Behörden
- Meldung schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle durch bestimmte Finanzunternehmen an die zuständigen Behörden
- Tests der digitalen operationalen Resilienz
- Austausch von Informationen und Erkenntnissen in Bezug auf Cyber-Bedrohungen und Schwachstellen
- Maßnahmen für das solide Management des IKT-Drittparteienrisikos

Anders als bei früheren Rechtsakten der Union rückt der traditionelle quantitative Risikomanagement-Ansatz hier in den Hintergrund und weicht einem gezielt qualitativen Ansatz, welcher einen eindeutigen Bezug zu den IKT-Risiken herstellt.

Im Ergebnis sollen Finanzunternehmen europaweit dazu befähigt werden, die IKT-Risiken nach denselben Grundregeln zu bewältigen. Proportional werden hier Faktoren wie das jeweilige Gesamtrisikoprofil oder die Größe des Unternehmens berücksichtigt.

Wie der BVR in seinem Rundschreiben vom 10. Januar 2023 informierte, ist der konkrete Handlungsbedarf für die Genossenschaftsbanken erst nach Vorliegen der technischen Regulierungsstandards vollständig ermittelbar. Diese werden über delegierte Rechtsakte planungsgemäß zu Beginn des Jahres 2024 bis hin zur zweiten Jahreshälfte 2024 erstellt. Innerhalb der Genossenschaftlichen FinanzGruppe werden geeignete Aktivitäten aufgesetzt und sukzessive ein Umsetzungsfahrplan für DORA im Zusammenspiel mit den technischen Regulierungsstandards erarbeitet. ▬