DORA-Verordnung –
Veränderungen für europäische Finanzunternehmen

Der Europäische Gesetzgeber setzte mit der Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (Digital Operational Resilience Act, DORA, Verordnung (EU) 2022/2554) einen umfassenden rechtlichen Rahmen für die digitale operationelle Widerstandsfähigkeit europäischer Finanzunternehmen.

Wenn auch die **DORA-Verordnung** schon Anfang 2023 in Kraft getreten ist, haben die betroffenen Unternehmen im Finanzbereich mit dem Jahreswechsel, konkret ab dem 17.01.2025, die festgelegten Regelungen zu befolgen.

Ziel der DORA-Verordnung ist es die Risiken im Bereich der Informations- und Kommunikationstechnologien, kurz IKT, durch die Verordnungsvorschriften einzudämmen. Dadurch soll die Standhaftigkeit des europäischen Finanzmarktes gegen Cyberangriffe gestärkt werden sowie der Schutz von Anlegern und Verbrauchern gefestigt werden.

Anzuwenden haben die Vorschriften Finanzunternehmen und IKT-Drittdienstleister, die Verträge mit Finanzunternehmen abschließen. Zu den Finanzunternehmen zählen neben Kreditinstitute u.a. auch Wertpapierfirmen, Zahlungs- und E-Geldinstitute sowie Anbieter von Krypto-Dienstleistungen. Zu den IKT-Drittdienstleistern zählen u.a. Softwareanbieter, Datenanalysedienste und Rechenzentren – explizit erfasst sind Anbieter, die Zahlungen abwickeln oder eine Zahlungsinfrastruktur betreiben.

Diese Unternehmen unterliegen umfassenden Governance- und Kontrollpflichten, um den Risiken der IKT standhalten zu können. Daraus ergibt sich die Notwendigkeit eines Risikomanagement, wodurch eine Implementierung und ständigen Weiterentwicklung von Strategien, Richtlinien, IKT-Protokollen und -Tools im Unternehmen verbunden sind. Die Leitungsorgane der Unternehmen tragen dabei die Verantwortung, dass alle dafür notwendigen Maßnahmen ergriffen werden. Die Verordnung sieht auch regelmäßige Schulungen zu IKT-Risiken für das Leitungsorgan vor, damit gewährleistet werden kann, dass Risiken und Auswirkungen auf die Geschäftsfähigkeit des Finanzunternehmens verstanden und bewertet werden können. Außerdem ergibt sich aus den Vorschriften eine zumindest jährlich durchgeführte Dokumentations- und Überprüfungspflicht des IKT-Risikomanagement.

Unter anderem müssen Finanzunternehmen Quellen für IKT-Risiken ermitteln sowie Cyberbedrohungen und Schwachstellen der IKT bewerten, damit diese wieder weiterentwickelt und verbessert werden können.

Es müssen zukünftig auch schwerwiegende IKT-bezogene Vorfälle an eine nationale Behörde gemeldet werden. Finanzunternehmen müssen daher aufgrund der DORA-Verordnung ein Verfahren zur Klassifizierung solcher Vorfälle anhand vorgegebener Kriterien vorsehen. Sollte ein Vorfall Auswirkungen auf finanzielle Kundeninteressen haben, müssen diese rasch über den Zwischenfall und die ergriffenen Maßnahmen im Zusammenhang mit dem IKT-Vorfall informieren.

Obwohl die meisten Vorschriften der Verordnung für alle Finanzunternehmen, unabhängig von ihrer Größe gelten, gibt es Ausnahmen. Unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes kommt es zu einer verhältnismäßigen Anwendung der Anforderungen für Kleinstunternehmen – für sie gibt es einige Erleichterungen. Kleinstunternehmen im Sinne dieser Verordnung sind Finanzunternehmen, die nicht Handelsplatz, zentrale Gegenpartei, Transaktionsregister oder Zentralverwahrer sind und weniger als 10 Personen beschäftigen sowie nicht mehr als € 2 Mio. Jahresumsatz/-bilanz aufweisen.

Damit die europäische DORA-Verordnung effektiv in Österreich angewendet werden kann, sollen mit dem nationalen DORA-Vollzugsgesetz die nötigen begleitenden Maßnahmen gesetzt werden. Die österreichische Regierungsvorlage sieht inhaltlich eine Klarstellung der Finanzmarktaufsicht (FMA) als zuständige Behörde sowie die Ausstattung dieser mit Aufsichts- und Sanktionsbefugnissen vor. Weiters soll durch das Vollzugsgesetz eine Erweiterung des Anwendungsbereiches der DORA-Verordnung auf nationale Institute **gem. § 1 Abs 1 BWG**, die nicht von der DORA-Verordnung genannt werden, vorgenommen werden. Das Vollzugsgesetz legt zudem Regelungen der Zusammenarbeit mit der österreichischen Nationalbank (OeNB) fest. Ein weiteres Ziel ist es, bestehende Rechtsakte im Finanzmarktbereich an die Verordnung dadurch anzupassen.

Aufgrund der umfassenden Vorgaben sowie deren Vorbereitung war eine relativ lange Übergangszeit vorgesehen die jedoch am 17.01.2025 endet. Eine zeitnahe Auseinandersetzung mit der DORA-Verordnung ist zu empfehlen, um die nötigen Implementierungsschritte im Unternehmen noch rechtzeitig zu setzen.