Resilienz durch Regulierung: Ein genauerer Blick auf die DORA-Verordnung – Teil 2
Persönliche Haftung der Geschäftsführung!

In der November-Ausgabe haben wir Sie erstmals auf DORA hingewiesen und auch die Frage beantwortet, ob DORA wirklich nur die Großen betreffen wird. Heute sehen wir uns die Aufgaben, die durch DORA auf Sie zukommen näher an.

Was ist DORA?

Die Verordnung (EU) 2022/2554, bekannt als Digital Operational Resilience Act (kurz DORA), trat am 16.01.2023 in Kraft. Aufgrund des Verordnungs-Charakters bedarf es keiner nationalen Umsetzung und es kommt zu einer direkten Anwendung ab dem 17.01.2025.

Besonders im Finanz- und Versicherungsbereich hat die Nutzung von IKT-Systemen sowie die allgemeine Digitalisierung und Vernetzung stark an Bedeutung gewonnen. Mögliche Cyberbedrohungen und IKT-Störungen sind die Folge. Durch DORA werden bestehende Lücken gefüllt. Es soll zu einer harmonisierten digitalen Betriebs- und Cyber-Resilienz im Finanzsektor kommen.

Zahlreiche Vorschriften für Technik und Management von IKT-Systemen.

IKT steht für Informations- und Kommunikationstechnologie, worunter laut DORA fast alles fällt: „IKT-Dienstleistungen sind digitale Dienste und Datendienste, die über IKT-Systeme … Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste".

Diese IKT-Zulieferer sind künftig zu kontrollieren, vertraglich zu verpflichten und deren Verträge in einem Informationsregister zu dokumentieren. Kritische IT-Anbieter müssen besonders strenge Vorgaben erfüllen und werden erstmals der Finanzmarktaufsicht unterworfen. Stresstests werden nötig, Strafen vorgeschrieben.

Für wen gilt DORA?

Vereinfacht gesprochen, betrifft DORA die verschiedensten „Arten von Finanzunternehmen" und in letzter Konsequenz auch deren Berater und Vermittler (siehe dazu unseren Beitrag im November). Konkret nennt DORA 21 Kategorien von Unternehmen, darunter u. a. Kreditinstitute, Wertpapierfirmen, Versicherer und Rückversicherer, aber auch Vermittler sowie IKT-Drittanbieter, die Verträge mit Finanzunternehmen abschließen. Durch das Einbeziehen von IKT-Drittanbietern spannt DORA den Bogen weiter als bisherige Regelungen. Dies ist aufgrund zunehmender Digitalisierung und Outsourcing geboten. Während große Akteure wie Microsoft, Google & Co bereits hohe IT-Standards zu erfüllen haben, ist für kleinere IKT-Drittanbieter eine größere Veränderung durch DORA zu erwarten.

Verhältnismäßigkeit? Ausnahmen?

Die DORA definiert im Artikel 4 den Grundsatz der Verhältnismäßigkeit. Das bedeutet, dass Finanzunternehmen, die von der Verordnung umfasst sind, grundsätzlich die Vorschriften einhalten müssen. Aber es doch „für Kleine" Ausnahmen und Erleichterungen bei einigen Vorgaben gibt. Siehe dazu etwa Artikel 16 der DORA, wonach für kleine und nicht verflochtene Wertpapierfirmen ein vereinfachtes Risikomanagementsystem gilt.

Ausgenommen vom Anwendungsbereich der Verordnung sind unter anderem Versicherungsvermittler bei denen es sich um Kleinstunternehmen, oder kleine oder mittlere Unternehmen handelt. Auch Versicherungsvermittler in Nebentätigkeit.

Ein „Kleinstunternehmen" ist laut DORA ein Finanzunternehmen … , das weniger als zehn Personen beschäftigt und dessen Jahresumsatz bzw. -Bilanzsumme 2 Mio. Euro nicht überschreitet.

Ein „Kleinunternehmen" ist laut DORA ein Finanzunternehmen, das zehn oder mehr, aber weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. -bilanzsumme 2 Mio. Euro überschreitet, nicht jedoch 10 Mio. Euro.

Ein „mittleres Unternehmen" ist laut DORA ein Finanzunternehmen, das kein Kleinunternehmen ist, das weniger als 250 Personen beschäftigt und dessen Jahresumsatz 50 Mio. Euro und/oder dessen Jahresbilanzsumme 43 Mio. Euro nicht überschreitet.

Von RA Mag. Stephan Novotny

RA Mag. Stephan Novotny ist ein auf Versicherungs- und Datenschutzrecht spezialisierter Anwalt, der seit mehr als zehn Jahren mit eigener Kanzlei in Wien tätig ist.

Ziele und Säulen der DORA

Das Ziel – die Harmonisierung der digitalen Resilienz innerhalb der EU – soll durch gemeinsame Ordnung der Anforderungen aufgrund von vier Säulen erreicht werden.

IKT-Risikomanagement

DORA sieht vor, dass Finanzunternehmen eine klare Governance-Struktur sowie ein Risikomanagement einrichten, was regelmäßig überprüft werden soll.

IKT-bezogene Vorfälle und deren Bewältigung

Bevor ein Service eines IKT-Drittdienstleisters in Anspruch genommen wird, hat das jeweilige Finanzunternehmen eine Überprüfung des Dienstleisters vorzunehmen, darüber hinaus soll es kategorisieren, ob es sich bei der Auslagerung um kritische oder wichtige Funktionen handelt.

Prüfung der digitalen Betriebsstabilität

Diese Prüfung soll durch externe Parteien vorgenommen werden. Kann sichergestellt werden, dass kein Interessenskonflikt besteht, besteht die Möglichkeit, diese Prüfung auch von einer internen Partei durchführen zu lassen. Insbesondere sollen Schwachstellen, Mängel und Lücken identifiziert und bearbeitet werden. Falls es sich um kritische oder wichtige Funktionen handelt, ist die genannte Prüfung einmal jährlich durchzuführen.

Steuerung von IKT-Drittdienstleister-Risiken

Aufgrund ihrer Verantwortung für die Einhaltung aller Verpflichtungen von beauftragten Dienstleistern müssen Finanzunternehmen sicherstellen, dass ihre Drittanbieter ebenfalls hohen Sicherheitsstandards entsprechen. Es gilt, Strategien und Leitlinien für IKT-Drittdienstleister-Risiken zu entwickeln und regelmäßig zu überprüfen, um Ausfallrisiken zu minimieren. Außerdem sind vertragliche Vereinbarungen mit Drittdienstleistern in einem Informationsregister zu führen, welches durch die FMA jederzeit angefordert und geprüft werden kann.

Diese Ziele der DORA zu erfüllen bedeutet in der Praxis eine enorme Herausforderung, sowohl technisch, personell und finanziell. Vom Dokumentations- und Prüfaufwand und der damit einhergehenden Haftung für die Normunterworfenen gar nicht zu reden.

Wie weit geht der Prüfaufwand laut DORA?

„Verträge über die Bereitstellung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen sollten zudem Bestimmungen enthalten, die Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens oder eines beauftragten Dritten sowie das Recht auf Anfertigung von Kopien regeln, die als wesentliche Instrumente für die laufende Überwachung der Leistung des IKT-Drittdienstleisters durch die Finanzunternehmen dienen, gepaart mit der uneingeschränkten Zusammenarbeit des Drittdienstleisters während der Inspektionen. In gleicher Weise sollte die für das Finanzunternehmen zuständige Behörde auf der Grundlage von Mitteilungen über das Recht verfügen, den IKT-Drittdienstleister vorbehaltlich des Schutzes vertraulicher Informationen zu inspizieren und zu prüfen."

Wie die FMA diese Prüfung durchführen kann, wenn der Server des Cloud-Anbieters vielleicht in Manila steht, wird sich zeigen. Ob der Cloud-Anbieter bereit sein wird, die in Artikel 43 definierte Pflicht, „die Gebühren für die Durchführung von Überwachungsaufgaben vollständig zu decken", zu erfüllen, ebenso.

Allerdings gibt es ein wesentliches Druckmittel, nämlich „ein Zwangsgeld von pro Tag bis zu 1% des weltweiten Tagesumsatzes für eine Dauer von bis zu sechs Monaten". Und: Kritische IKT-Dienstleister aus Drittländern dürfen nur in Anspruch genommen werden, wenn sie binnen zwölf Monaten, nachdem sie als kritische IKT-Dienstleister eingestuft wurden, ein Tochterunternehmen in der EU gegründet haben.

Michael Herzhofer, AFPA-Obmann warnt: Auch Geschäftsführung wird sich intensiv um DORA kümmern und für sich selbst „vorsorgen" müssen.

Gerade die „üblich gewordenen" Auslagerungen sollte man sich genau ansehen. Die oft gehörte Ausrede, „Details dazu gehen mich nichts an, dafür habe ich eine Firma, die für die Ordnungsgemäßheit haftet", hilft nicht mehr. Sie als Geschäftsführer sind dafür persönlich haftbar. Das ist eine der wichtigsten Neuerungen der DORA. Art. 5 Abs. 2 a besagt, dass das Leitungsorgan „die letztendliche Verantwortung für das Management der IKT-Risiken" trägt. Dies bedeutet, dass Sie ihre diesbezügliche Verantwortung künftig nicht mehr an die IT-Leitung abgeben können. Die Geschäftsleitung hat dann umfangreiche Genehmigungs-, Überwachungs- und Überprüfungspflichten, deren Nichtbeachtung haftbar macht. Auch müssen Mitglieder des Leitungsorgans in Zukunft regelmäßig spezielle Schulungen absolvieren, um ihre Kenntnisse und Fähigkeit bzgl. IKT-Risiken aktiv auf dem neuesten Stand zu halten.

Michael Herzhofer ist AFPA-Obmann und Geschäftsführer der Secura Gruppe (Foto: Fineart Photos by Andrea Schober)

Es ist daher unerlässlich, dass Geschäftsführer und Vorstand sich intensiv mit DORA beschäftigen. Finaler Tipp zur persönlichen Haftung: **Checken Sie die eigene D&O-Versicherung**, um zu erfahren, ob und wie gut Sie selbst abgesichert sind. •

Von AFPA

Für Rückfragen:
RA Mag. Stephan Novotny, kanzlei@ra-novotny.at
Michael Herzhofer, mh@afpa.at