DORA soll die digitale Widerstandsfähigkeit durch Regulierung erhöhen

Kommentar von Rechtsanwalt Mag. Stephan Novotny, ein auf Versicherungs- und Datenschutzrecht spezialisierter Anwalt der seit mehr als 10 Jahren mit eigener Kanzlei in Wien tätig ist.

Daher: Fragen Sie bei Ihren Partnern schon jetzt an, wie Sie sich die künftige Zusammenarbeit unter DORA vorstellen. Die Verordnung (EU) 2022/2554 des Europäischen Parlaments und Rates, auch 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. Die zunehmende Nutzung digitaler Technologien bringt mögliche Cyberbedrohungen und IKT-Störungen als Folge mit sich. Durch DORA werden die bestehenden Lücken der bereits geregelten operationellen Resilienz gefüllt, Risiken der IKT nicht mehr nur am Rande behandelt und es soll zu einer harmonisierten digitalen Betriebs- und Cyber-Resilienz im Finanzsektor kommen.

DORA bringt zahlreiche Vorschriften für die Technik und das Management von IKT-Systemen.

IKT steht für Informations- und Kommunikationstechnologie, worunter laut DORA fast alles fällt, außer die normale Telefonie. Konkret steht in Art. 21 Punkt 3:

„IKT-Dienstleistungen sind digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung 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.

DORA, FMA-Prüfschwerpunkt 2024

Bereits Anfang Jänner kündigten die beiden Vorstände der Finanzmarktaufsicht Österreich Helmut Ettl und Eduard Müller an: „DORA bringt sehr grundlegende und sehr weitreichende regulatorische Neuerungen. Es ist daher von essenzieller Bedeutung, dass sich die betroffenen Finanzdienstleister und Drittanbieter rechtzeitig auf dieses neue Aufsichtsregime vorbereiten“.

Und weiter: „Die FMA hat daher einen Aufsichtsschwerpunkt auf die rechtzeitige Vorbereitung des Marktes auf die Herausforderungen dieser neuen Regulierung gelegt und wird beaufsichtigte Unternehmen wie auch Drittanbieter dabei eng begleiten.“ Um das zu erreichen, wird die FMA „die für den österreichischen Finanzmarkt relevanten IKT -Dienstleister identifizieren“ und jene „IKT-Drittanbieter, die als kritisch eingestuft werden, in den Anwendungsbereich der Finanzmarktaufsicht“ einbeziehen.

Mag. Stephan Novotny

Für wen gilt DORA?

Vereinfacht gesprochen, betrifft DORA die verschiedensten „Arten von Finanzunternehmen“ und in letzter Konsequenz auch deren Berater und Vermittler. Konkret nennt Art 2 der DORA 21 Kategorien von Unternehmen, darunter unter anderem Kreditinstitute, Wertpapierfirmen, Versicherungs- und Rückversicherungsunternehmen, aber auch Versicherungsvermittler sowie IKT-Drittanbieter, die Verträge mit Finanzunternehmen abschließen. Durch das Einbeziehen von IKT-Drittanbietern spannt DORA den Bogen weiter als etwaige bisherige Regelungen. Dies ist aufgrund zunehmender Digitalisierung und Outsourcing geboten. Während große Akteure wie Microsoft, Google und Co aufgrund von nationa-

len und EU-weiten Regelungen 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, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, bei denen es sich um Kleinstunternehmen, oder kleine oder mittlere Unternehmen handelt.

Ein „Kleinstunternehmen" ist gem. Art. 3 Z 60 DORA ein Finanzunternehmen, bei dem es sich nicht um einen Handelsplatz, eine zentrale Gegenpartei, ein Transaktionsregister oder einen Zentralverwahrer handelt, das weniger als 10 Personen beschäftigt und dessen Jahresumsatz bzw. -Bilanzsumme 2 Milllionen EUR nicht überschreitet. Ein „Kleinunternehmen" ist gem. Art. 3 Z 63 DORA ein Finanzunternehmen, das 10 oder mehr, aber weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. -bilanzsumme 2 Millionen Euro überschreitet, nicht jedoch 10 Millionen Euro. Ein „mittleres Unternehmen" ist gem. Art. 3 Z 64 DORA ein Finanzunternehmen, das kein Kleinunternehmen ist, das weniger als 250 Personen beschäftigt und dessen Jahresumsatz 50 Millionen Euro und/oder dessen Jahresbilanzsumme 43 Millionen Euro nicht überschreitet.

Ziele und Säulen der Verordnung

Das Ziel von DORA, die Harmonisierung der digitalen Resilienz innerhalb der EU, soll durch gemeinsame Ordnung der Anforderungen aufgrund von 4 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

Eine Prüfung der digitalen Betriebsstabilität soll durch externe Parteien vor-

genommen 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 bei diesen 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.

Die DORA schreibt wörtlich im Erwägungsgrund (21)

„Um die vollständige Kontrolle über das IKT-Risiko zu behalten, müssen Finanzunternehmen über umfassende Kapazitäten verfügen, die ein leistungsfähiges und wirksames IKT-Risikomanagement sowie spezifische Mechanismen und Strategien für die Handhabung aller IKT-bezogener Vorfälle und für die Meldung schwerwiegender IKT-bezogener Vorfälle ermöglichen. Ebenso sollten Finanzunternehmen über Leit- und Richtlinien für die Erprobung von IKT-Systemen, -Kontrollen und -Prozessen sowie für das Management des IKT-Drittparteienrisikos verfügen."

Diese Ziele der Verordnung 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 der Prüfaufwand geht, zeigt Erwägungsgrund (73) der 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."

Ob und wie die FMA diese Prüfung durchführen kann, wenn der Server des Cloud-Anbieters vielleicht in Manila steht, wird sich zeigen. Und 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 schon ein wesentliches Druckmittel. Konkret schreibt Art.35 Punkt 8 „ein Zwangsgeld von pro Tag bis zu 1 Prozent des weltweiten Tagesumsatzes für eine Dauer von bis zu sechs Monaten" vor. 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 (Erwägungsgrund 81).

DORA schafft einheitliche Rahmenbedingungen, aufgrund welcher aktuellen und zukünftigen Cyber-Bedrohungen und IKT-Störungen entgegengewirkt werden soll. Durch fortlaufende Angleichungen an moderne Technologien und sich stetig ändernde Gefahren wird sich einerseits die langfristige Effektivität der Verordnung zeigen und andererseits, wie gut Finanzinstitute in der Lage sind, die neuen Standards zu implementieren.