universität wien

MASTER THESIS | MASTER'S THESIS

Titel | Title

Der Digital Operational Resilience Act und dessen Verhältnis zu anderen einschlägigen EU-Regulierungsmaßnahmen

verfasst von | submitted by

Benjamin Reyak LL.B.

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien | Vienna, 2025

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 999 082
Universitätslehrgang lt. Studienblatt | Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht [Vollzeit Deutsch]
Betreut von | Supervisor:	ao. Univ.-Prof. Mag. Dr. Siegfried Fina

Abstract (Deutsch)

Der Digital Operational Resilience Act, kurz DORA, als VO (EU) 2022/2554 soll die digitale Resilienz von Finanzunternehmen und deren Dienstleistern stärken. Die vorliegende Masterthesis soll den Inhalt von DORA übersichtlich, aber auch vollständig, wiedergeben und Vergleiche zu Rechtsakten der Europäischen Union anstellen, welche ähnlichen Zielen verschrieben wurden.

Der Inhalt wird umfassend dargestellt und bestehende Rechtsprobleme diskutiert. Aufgeworfenen Probleme sind aufgrund der Aktualität von DORA noch nicht ausjudiziert, sodass die gerichtliche Ausformung erst mit den zu erwartenden Schadenseintritten zu erwarten ist. Die Rolle von Behörden und Aufsichtsorganen, sowie weiteren Akteuren, den Testern und den IKT-Drittdienstleistern wird kritisch untersucht. Die verpflichtende Durchführung und der neue Einbezug von IKT-Drittdienstleistern werden erläutert, Abläufe dargestellt und praxisrelevante Fragen diskutiert.

Für den Vergleich mit Rechtsakten ähnlicher Zielrichtung wurden NIS-2 und die CER ausgewählt, die ebenfalls auf gesteigerte Sicherheit und Gefahrenabwehr im digitalen Raum ausgelegt sind. Es werden Gemeinsamkeiten besonders hinsichtlich der unternehmensinternen Managementsysteme und der Vorgaben für diese herausgearbeitet. Auch die Einbindung der zuständigen Behörden wird vergleichend dargestellt, um die Effektivität der Rechtsakte vergleichen zu können.

Abschließend kommt die Thesis zu dem Schluss, dass DORA zwar erheblichen Mehraufwand für alle Betroffenen bedeutet, welcher aber in wirtschaftlicher Verhältnismäßigkeit steht. Die Umsetzung von DORA ist im Vergleich zu NIS-2 und CER kleinschrittig und streng, bietet aber das größtmögliche Potenzial, die von der Europäischen Union angestrebten Ziele zu erreichen. Der Binnenmarkt, Finanzunternehmen und Verbraucher werden von DORA profitieren.

Abstract (English)

The Digital Operational Resilience Act, short DORA, as Regulation (EU) 2022/2554, aims to strengthen the digital resilience of financial companies and their service providers. This master's thesis aims to provide a clear but comprehensive overview of the contents of DORA and to draw comparisons with European Union legal acts.

The content is presented comprehensively, and existing legal issues are discussed. Due to the topicality of DORA, the issues raised have not yet been adjudicated and clarity might only be found retrospectively upon investigating future damages. The role of authorities and supervisory bodies, as well as other actors, testers, and third-party ICT service providers, is critically examined. The mandatory implementation and the new inclusion of third-party ICT service providers are explained, processes are presented, and practical questions are discussed.

NIS-2 and the CER, which are also designed to increase security in the digital space, were selected for comparison with legal acts of a similar nature. Similarities are identified, particularly with regard to internal management systems and their requirements. The involvement of the competent authorities is also presented in a comparative manner in order to evaluate the effectiveness of the legal acts.

Finally, the thesis concludes that although DORA means considerable additional effort for all those affected, following its principles is worthwile compared to the potential damage it prevents. In contrast to NIS and CER, DORA is a strict multi-stepwise approach, but offers the greatest potential for achieving the goals set by the European Union. Hence, the internal market, financial companies, and consumers will benefit from DORA.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AktG	Aktiengesetz (Deutschland)
Art.	Artikel
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
CER	Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen
CRR-Kreditinstitute	Capital Requirements Regulation
CSIRT	Computer Security Incident Response Team
DORA	Verordnung (EU) 2022/2554 - Digital Operational Resilience Act
DORA-VG	DORA-Vollzugsgesetz (Deutschland)
DSGVO	Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr (Datenschutzgrundverordnung)
EBA	European Banking Authority
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Network and Information Security Agency
ESA	Europäische Aufsichtsbehörden
ESFS	European System of Financial Supervision
ESMA	European Securities and Markets Authority
ESRB	European Systemic Risk Board
ESZB	Europäische System der Zentralbanken
EU	Europäische Union
EU-CyCLONe	European cyber crisis liaison organisation network
EZB	Europäische Zentralbank
f	folgend
ff	fortfolgend
FinmadiG	Finanzmarktdigitalisierungsgesetz (Deutschland)
FMA	Finanzmarktaufsicht
FMABG	Finanzmarktaufsichtsbehördengesetz (Österreich)
GL	Guideline
GmbhG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung (Deutschland)
Hrsg.	Herausgeber
IKT	Informations- und Kommunikationstechnologie
iVm	in Verbindung mit
JON	Joint Oversight Network
KWG	Kreditwesengesetz (Deutschland)

lit	littera
MaRisk	Mindestanforderungen an das Risikomanagement
NIS	Netzwerk- und Informationssysteme
Nr.	Nummer
RL	Richtlinie
Rn.	Randnummer
RTS	Regulatory Technical Standards
TIBER-Standard	Threat Intelligence-Based Ethical Red-Teaming
TKC	TIBER-EU Knowledge Center
TLPT	Threat-Led Penetration Testing
VO	Verordnung
VStG	Verwaltungsstrafgesetz (Österreich)
ZAG	Zahlungsdiensteaufsichtsgesetz (Deutschland)

Literaturverzeichnis

Alt, Rainer/ Puschmann, Thomas	Digitalisierung der Finanzindustrie: Grundlagen der Fintech-Evolution 1. Edition 2016 Berlin, Heidelberg
Anderl, Axel [Hrsg.]	#Cybercrime: Handbuch für die Praxis 1. Auflage 2023 Wien
Auer-Reinsdorff, Astrid/ Conrad, Isabell [Hrsg.]	Handbuch IT- und Datenschutzrecht 3. Auflage 2019 München
Bernau, Timo/ Lutterbach, Maike	Digital Operational Resilience Act (DORA) - Paradigmenwechsel in der IT-Aufsicht BKR: Zeitschrift für Bank- und Kapitalmarktrecht 2023, 506 - 513 München *[zit.: Bernau/Lutterbach, BKR 2023, 506]*
Blum, Lucas/ Adelberg, Philipp	Zeitenwende bei der Cybersecurity-Compliance: Ausweg aus der Haftungsfalle für die Geschäftsleitung Compliance Berater 05/2024, 145 Frankfurt am Main *[zit.: Blum/Adelberg, CB 2024, 145]*
Bomhard, Gerrit/ Siglmüller, Martin [Hrsg.]	IT-Sicherheitsrecht – Praxishandbuch 2. Auflage 2024 Baden-Baden
Brühl, Volker/ Dorschel, Joachim [Hrsg.]	Praxishandbuch Digital Banking 1. Auflage 2028 Wiesbaden
Calliess, Christian/ Ruffert, Matthias [Hrsg.]	EUV/AEUV - Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta 6. Auflage 2022 München *[zit.: Calliess/Ruffert, AEUV]*
Dellinger, Markus [Hrsg.]	Bankwesengesetz - BWG Kommentar 12. Lieferung 2024 Wien

Dittrich, Tilmann/ Heinelt, Christian
Der Europäische DORA - neue Sicherheitsvorgaben für den Finanzsektor
Recht Digital: RDi 2023, 164 - 172
München
[zit.: Dittrich/Heinelt, RDi 2023, 164]

Grieger, Ferdinand
Haftung des AG-Vorstands bei Schäden durch Cyberangriffe
Wertpapiermitteilungen - Zeitschrift für Wirtschafts- und Bankrecht 2021, 8 - 15
Köln
[zit.: Grieger, WM 2021, 8]

Hysek, Michael [Hrsg.]
Praxishandbuch DORA Digital Operational Resilience Act
1. Auflage 2025
Wien

Kreisl, René
DORA *ante portas*!,
Zeitschrift für Finanzmarktrecht 2024/252 578 - 583
Wien
[zit.: Kreisl, ZFR 2024/252, 578]

Lauck, Simon
Der IKT-Dienstleistungsbegriff in der DORA - Enge Auslegung von Art. 3 Nr. 21 DORA statt Korrekturen in Art. 30 DORA
BKR: Zeitschrift für Bank- und Kapitalmarktrecht 2025, 124 - 132
München
[zit.: Lauck, BKR 2025, 124]

Lipke, Martina Isabelle
Vertragsanpassungen nach DORA
BKR: Zeitschrift für Bank- und Kapitalmarktrecht 2025, 253 - 258
München
[zit.: Lipke, BKR 2025, 253]

Lischka, Konrad
Geldautomat mit Öffnungszeiten
manager magazin 12.07.2007
https://www.manager-magazin.de/digitales/it/a-494070.html
Hamburg

Merwald, Maximilian
Die Regelungen des DORA betreffend Auslagerungsvereinbarungen
Recht Digital: RDi 2024, 590 - 599
München
[zit.: Merwald, RDi 2024, 590]

Nägele, Thomas/ Apel, Simon [Hrsg.]
Beck´sche Online-Formulare IT- und Datenrecht
23. Edition 2025
München
[zit.: Nägele/Apel, BeckOF IT- und Datenrecht]

Priller, Martin
DORA in Versicherungsunternehmen - Regulatorik, Vorgehensmodell, praktische Aspekte, Erfolgsfaktoren
1. Auflage 2024
Karlsruhe

Schiefer, Martin/ Wieser, Lucas B.
NIS-2-RL: Wer trägt die Verantwortung im Unternehmen? Das "Leitungsorgan" in der NIS-2-RL
ecolex – Zeitschrift für Wirtschaftsrecht 2023/568, 900 - 902
Wien
[zit.: Schiefer/Wieser, ecolex 2023/568, 900]

Schiefer, Martin/ Wieser, Lucas B.
Cybersicherheitsrecht 2.0: Mangelhafte Compliance kommt teuer - Die NIS-2-RL und ihr Pflichtenprogramm für Unternehmen ecolex – Zeitschrift für Wirtschaftsrecht 2023/622, 1000 - 1004
Wien
[zit.: Schiefer/Wieser, ecolex 2023/622, 1000]

Schmidt, Arndt Alexander
Digital Operational Resilience Act (DORA) - Behördliche Eingriffs- und Sanktionierungsinstrumente Teil I, WM 2024, 2125, 2132
Wertpapiermitteilungen - Zeitschrift für Wirtschafts- und Bankrecht 2024, 2125 - 2135
Köln
[zit.: Schmidt, WM 2024, 2125]

Schmidt-Versteyl, Sarah
Cyber Risks – neuer Brennpunkt Managerhaftung?
Neue Juristische Wochenschrift 2019, 1637 - 1642
München
[zit.: Schmidt-Versteyl, NJW 2019, 1637]

Siglmüller, Jonas
Cyber Resilience Act und Digital Operational Resilience Act - Lässt sich IT-Sicherheit rechtlich erzwingen?
Zeitschrift für Product Compliance 2023, 221 - 225
Baden-Baden
[zit.: Siglmüller, ZfPC 2023, 221]

Škorjanc, Žiga
Digital Operational Resilience Act,
Österreichisches Bankarchiv - Zeitschrift für das gesamte Bank- und Börsenwesen 2023, 658 - 667
Wien
[zit.: Škorjanc, ÖBA 2023, 658]

Thiele, Clemens/ Wagner, Jessica
Vorbildliches IKT-Risikomanagement mit Auftragsverarbeitern im NIS-Zeitalter
jusIT - Zeitschrift für IT-Recht, Rechtsinformation und Datenschutz 2025/2, 6 - 16
Wien
[zit.: Thiele/Wagner jusIT 2025/2, 6]

Voigt, Paul/ Falk, Lucas
Der Cyber Resilience Act
MMR - Zeitschrift für IT-Recht und Recht der Digitalisierung 2023, 88 - 92
München
[zit.: Voigt/Falk MMR 2023, 88]

Waschbusch, Lisa/ Mundt, Elisa
Was bedeutet Industrie 4.0? Definition, Merkmale und Anwendung
Industry of Things 09.09.2024
https://www.industry-of-things.de/was-bedeutet-industrie-40-definition-merkmale-und-anwendung-a-828236/
Würzburg

A. Einleitung

Diese Masterthesis soll sich mit dem Digital Operational Resilience Act[1] der Europäischen Union, abgefasst unter der Verordnung 2022/2554, befassen.

Welche Anforderungen stellt der Digital Operational Resilience Act (DORA) der Europäischen Union an Unternehmen und Behörden und wie steht DORA im Verhältnis zu weiteren einschlägigen Regulierungsansätzen der Europäischen Union?

DORA stellt eine Reaktion der Europäischen Union auf eine sich verändernde Welt dar. In Zeiten der zunehmenden Digitalisierung spielen sich wirtschaftliche Vorgänge zunehmend im digitalen Raum ab. Die damit verbundenen Finanzströme werden durch diverse Angebote in den digitalen Raum verlegt. Zusätzlich verschiebt sich auch die Infrastruktur der Anbieter von Finanzdienstleistungen in den digitalen Raum.

Diese neuen Strukturen sind dort immer wieder neuen Gefahren in Form von Angriffen krimineller Organisationen oder auch staatlicher Akteure ausgesetzt, welche daraus illegale Vorteile erzielen wollen.

In DORA befasst die Europäische Union sich deswegen mit zwei großen Themenblöcken, die in dieser Arbeit analysiert und auf weitere Aspekte bezogen werden sollen. Zum einen definiert DORA die technischen Anforderungen zur Herstellung einer erhöhten Cyberresilienz an Finanzdienstleister dar. Dabei werden die Prozesse für sichere IT-Strukturen vorgeschrieben und deren regelmäßige Überprüfung und Aktualisierung sichergestellt. Dies soll unter anderem durch so genannte Penetrationstests erfolgen, welche in DORA konkretisiert werden.

Zum anderen befasst DORA sich mit der Rolle der Aufsichtsbehörden. Diese werden zur Überwachung der Umsetzungen der Vorgaben aus von DORA angehalten und kontrollieren die Finanzdienstleister daraufhin. Auch erstellen sie Risikoanalysen und verhängen entsprechende Sanktionen bei Nichteinhaltung der Vorgaben von DORA.

Auf europäischer Ebene ist die Europäische Bankenaufsichtsbehörde (kurz: EBA, European Banking Authority) mit Sitz in Paris die regulierende Behörde. Sie ist die

[1] Im Weiteren wird die VO 2022/2554 entsprechend dem allgemeinen Sprachgebrauch und ihrer Eigenschaft als Verordnung als „DORA, die“ bezeichnet.

Finanzmarktaufsicht der EU und damit federführend bei der Umsetzung und Durchführung der Vorgaben von DORA. Dabei greift sie nicht direkt in wirtschaftliches Geschehen ein, sondern entwickelt die Handlungsvorgaben für die jeweiligen nationalen Aufsichtsbehörden. Sie kontrolliert diese und kann im Fall eines Verstoßes direkt eingreifen.

Für Finanzdienstleister ergeben sich aus DORA diverse Verpflichtungen, deren rechtliche Komplexität einer intensiven Begutachtung bedarf. Mit der Auferlegung umfassender Meldepflichten sorgt DORA auch für einen erheblichen Aufwuchs an Bürokratie in den betroffenen Unternehmen. Zahlreiche Handlungspläne müssen vorgehalten, nachgewiesen und regelmäßig aktualisiert werden. Dies dient zwar dem Ziel eines hohen Schutzniveaus für Anleger und Verbraucher, stellt jedoch auch einen nicht unerheblichen Kostenfaktor dar, welcher sich gegebenenfalls auf die Wettbewerbsfähigkeit auswirken kann.

I. Ziel der Thesis

Die Vorgaben von DORA sollen in dieser Arbeit dargestellt werden. Dabei werden Regelungsziele und -inhalte berücksichtigt, ebenso wie Auswirkungen auf die Praxis. Der Umgang mit sicherheitsrelevanten Vorfällen soll ebenso wie die Analyse der Bedrohungslage Einzug finden. Auch soll das Verfahren der bedrohungsorientierten Penetrationstests untersucht werden. Da DORA umfassende Sanktionen für den Fall des Nichteinhaltens der Vorgaben benennt, sind auch diese durch die angestrebte Masterthesis zu analysieren.

Die nationalen Aufsichtsbehörden innerhalb der Europäischen Union haben neben DORA auch nationale Regulierungen zu überwachen. Eine umfangreiche Belastung dieser Behörden durch DORA ist anzunehmen. Als Beispiel soll die österreichische FMA herangezogen werden. Die Umsetzung von DORA und die daraus resultierenden Verfahrensabläufe sollen dargestellt werden.

Die genaue Analyse der Vorgaben von DORA für Behörden soll im Zuge dieser Arbeit erfolgen. Dabei werden die unterschiedlichen Abschnitte getrennt analysiert und praxisrelevantere Felder auf entstehende Probleme untersucht. So soll eine klare Darstellung der Ziele von DORA vorgelegt werden. Die daraus resultierenden Schlüsse

münden in der konkreten Umsetzung der Vorgaben, welche es im Einzelnen zu betrachten gilt. Sie unterscheiden sich in Vorgehen und Wirkweise und sind entweder von den Finanzdienstleistern selbst oder den Aufsichtsbehörden zu erbringen.

Auch der Bezug zu Drittparteien, wie er im wirtschaftlichen Verkehr regelmäßig vorkommt, soll untersucht werden. Drittanbieter, die in ihrer geschäftlichen Tätigkeit auf Finanzdienstleister als Kunden zurückgreifen, unterliegen erstmals den strengen Vorgaben einer Richtlinie, die eigentlich Finanzunternehmen als Adressaten hat. Sie sind dabei nicht direkt von DORA erfasst, jedoch kann ein Finanzdienstleister sein Risiko nur einschätzen, wenn er die Befolgung von Vorgaben seiner Zuarbeiter und vorgeschalteten Dienstleister prüfen kann. Weil ein weitergehender Schutz zu begrüßen ist, profitieren am Ende alle Nutzer von Finanzdienstleistern, also alle Teilnehmer des Wirtschaftsverkehrs, davon, auch wenn die Anforderungen von DORA mit einer weitgehenden Belastung einherkommen können. Kleinere Unternehmen können in nicht vergleichbarer Weise auf personelle und fachliche Ressourcen zugreifen, sodass Ausnahmen für diese zu benennen sind.

Interessant erscheint die Beziehung von DORA zur NIS-2 Richtlinie. Stellt DORA eine sektorspezifische Verordnung zu NIS-2 dar? Es könnten Parallelen bestehen, welche Unternehmen eine gleichzeitige Umsetzung ermöglichen. In der Praxis werden Unternehmen entsprechend den angebotenen Dienstleistungen möglicherweise auf DORA, zugleich aber auch auf NIS-2 Rücksicht nehmen müssen.

Als weiteres regulatorisches Werk auf EU-Ebene ist die CER-Richtlinie bekannt. Auch sie beschäftigt sich teilweise mit der Sicherheit von IT-Systemen. Obgleich dort der Schutz der Einrichtungen als Ganzes im Vordergrund steht, könnten rechtliche Vorgaben beiden Zielen, von DORA und der CER, gleichermaßen dienen. Die Masterthesis soll hier Unterschiede und Gemeinsamkeiten herausstellen, eine möglichst effiziente Umsetzung beider Werke soll untersucht werden.

Erfreulich wäre es, wenn im Zuge der Arbeit Synergien zwischen den verschiedenen regulatorischen Normwerken der Europäischen Union gefunden würden und dadurch eine Verschlankung von Prozessen ermöglicht wird. Eine Automatisierung von Prozessen wäre wünschenswert, welche eine ökonomische Stärkung zu Folge hätte. Die große Herausforderung des Bürokratieabbaus, trotz steigender Bedrohung durch

kriminelle und staatliche Akteure, könnte dadurch einen Anschub erhalten. Auch muss die ausführliche Regulierung flexibel und offen sein für neue technologische Entwicklungen. Diese bieten im besten Fall ein gesteigertes Sicherheitsniveau, eröffnen aber gleichermaßen illegale Angriffsmöglichkeiten. Die Anpassungsfähigkeit der Vorgaben bei Beibehaltung des Ziels von DORA sowie ein hohes Maß an Praxistauglichkeit sind erstrebenswert.

Die Forschungsfrage soll beantwortet werden mit einer inhaltlichen Aufschlüsselung der wichtigsten Vorgaben von DORA, übersichtlich dargestellt und vertiefend auf Einzelaspekte bezogen bewertet. Im Kontext zu weiteren Regulierungsvorschriften sollen Unterschiede und Gemeinsamkeiten inhaltlicher und praktischer Natur vergleichend herausgestellt werden. Der Vollzug durch europäische und nationale Behörden soll ebenfalls thematisiert werden und mit den Neuerungen von DORA in Bezug gesetzt werden. Es soll eine umfassende inhaltliche Analyse von DORA geschaffen werden, die aber weitergehende Fragestellungen nicht außer Acht lässt und mit Blick auf die Ziele der Europäischen Union auch weitere Normen abdeckt, in Kontext setzt und ein Gesamtbild der Harmonisierungsbestrebungen im digitalen Raum schafft.

II. Historischer Hintergrund DORA

1. Digitalisierung der Finanzwelt

Die Finanzwelt steht seit jeher für die effiziente Abwicklung von Zahlungsgeschäften zwischen Verbrauchern, Unternehmen und auch Staaten. Mit Voranschreiten der technologischen Entwicklung änderten sich auch die konkreten Abläufe. Die Einführung der ersten Bankkarte 1946 in den USA, zunächst als individuelle Kundenkreditkarten, stellte eine erste Loslösung von physischen Zahlungsmitteln und eine Hinwendung zur Virtualisierung dar.[2] Es folgten erste Bankautomaten in London (1967) und New York (1969).[3] Ab 1997 entstanden erste Internet-Banking-Angebote in Europa, bis im Jahr 2000 mit PayPal eine neue Form eines Finanzinstitutes

[2] *Alt/Puschmann*, Digitalisierung der Finanzindustrie - Grundlagen der Fintech-Evolution, 1.1.1 Evolution und Funktion des Geldes, 4-7.
[3] *Lischka,* in Manager Magazin: Geldautomat mit Öffnungszeiten, 12.07.2007, https://www.manager-magazin.de/digitales/it/a-494070.html (zuletzt abgerufen am: 17.08.2025).

gegründet wurde.[4] Zahlungsvorgänge von Privatpersonen, aber auch von Unternehmen, verlagerten sich in den digitalen Raum, um eine höhere Transaktionsgeschwindigkeit, eine Anpassung an die Globalisierung und eine bessere Übersichtlichkeit zu erzielen. Die Verschmelzung von klassischen Bankprozessen mit der digitalen Welt ist Ausdruck der voranschreitenden Industrie 4.0, die sämtliches Handeln der Menschheit seit Jahren bestimmt.[5] Dies führt auch dazu, dass einzelne Aspekte der Finanzwelt von jungen, spezialisierten Unternehmen neu gedacht werden. So wird die Konnektivität der Finanzwelt mit der Nutzung von Smartphones und immer weiter steigenden Fähigkeiten von künstlicher Intelligenz stringent gesteigert.[6]

2. Neue Risiken durch die Digitalisierung

Die gesteigerte Nutzung digitaler Angebote erfordert eine parallel wachsende digitale Infrastruktur. Die Informations- und Kommunikationstechnologien (IKT) sind einem neuartigen Risiko ausgesetzt, das sich von Gefahren in der analogen Finanzwelt wesentlich unterscheidet. Risiken im IKT-Bereich werden als Teil des generellen operationellen Risikos von Finanzdienstleistern eingestuft. Dies rief mit steigender Relevanz die Kontrollinstanzen der Finanzwelt auf den Plan, welche das Funktionieren des Finanzmarktes gewährleisten müssen, gleichzeitig aber Verantwortung für die Sicherheit seiner Teilnehmer tragen.

Die Finanzaufsicht im Binnenraum der Europäischen Union unterliegt der Bestrebung nach Harmonisierung, um den Binnenmarkt effektiv zu schützen, als einen Raum zusammen zu halten und diesem damit wirtschaftspolitische Relevanz in der Welt zu garantieren.[7] Die rechtlichen Voraussetzungen sowohl für das Handeln der Finanzunternehmen selbst, als auch für die Aufsichtsbehörden, ergeben sich aus der Art des Unternehmens und den jeweiligen nationalen Gesetzen. In Österreich war

[4] *Alt/Puschmann,* Digitalisierung der Finanzindustrie - Grundlagen der Fintech-Evolution, 1.1.1 Evolution und Funktion des Geldes, 4-7.

[5] *Waschbusch/Mundt*, in Internet of Things: Was bedeutet Industrie 4.0? Definition, Merkmale und Anwendung, 09.09.2021, https://www.industry-of-things.de/was-bedeutet-industrie-40-definition-merkmale-und-anwendung-a-828236/ (zuletzt abgerufen am 17.08.2025).

[6] *Brühl,* in Brühl/Dorschel [Hrsg.] Praxishandbuch digital banking: Banking 4.0 – Strategische Herausforderungen im digitalen Zeitalter, 3, 4.

[7] *Bornemann/Brandes*, in Brühl/Dorschel [Hrsg.] Praxishandbuch digital banking: Rechtlicher Rahmen des Digital Banking, 357, 359.

dies für klassische Banken das Bankwesengesetz, für den Wertpapierhandel das Wertpapieraufsichtsgesetz, Versicherungen wurden vom Versicherungsaufsichtsgesetz normiert und Zahlungsdienstleister vom Zahlungsdienstegesetz. Diese gaben den Unternehmen jeweils grobe Rahmen vor, die entsprechende Sorgfaltspflichten der Geschäftsführer im Bezug auf IKT-Risiken normieren. Verstöße gegen die IKT-Sicherheit können danach als Verstoß gegen die jeweilige Sorgfaltspflicht gewertet werden.[8] Ergänzt wurden diese gesetzlichen Vorgaben durch eigene Richtlinien der Aufsichtsbehörden. Die Europäische Bankenaufsichtsbehörde (EBA) hat solche ebenso erlassen, wie nationale Aufsichtsbehörden, wie die österreichische Finanzmarktaufsicht (FMA) oder die deutsche Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

3. Rechtliche Vorgaben

Die immer komplexer werdenden Abläufe der digitalen Finanzwelt erfordern zunehmend Kompetenz und Kontrolle, sodass die Europäische Union als Gesetzgeber im Binnenmarkt veranlasst ist, neue Instanzen zu schaffen. Im Jahr 2004 wurde mit der Verordnung (EG) 460/2004 die Agentur der Europäischen Union für Cybersicherheit (ENISA) gegründet. Sie sollte die Sicherheit im digitalen Raum gewährleisten. Ihre Kompetenzen wurden dabei stetig ausgeweitet, zuletzt durch die VO (EU) 2019/881 und die VO (EU) 526/2013. Sie beheimatet auch das Sekretariat des Netzes der nationalen Reaktionsteams für Computersicherheitsverletzungen (computer security incident response teams, CSIRT). Nach der Finanzkrise hat zum 01.01.2011 auf Basis der Artikel 114, 127 Absatz 6 AEUV das Europäische Finanzaufsichtssystem (ESFS) seine Arbeit aufgenommen. Dies umfasst neben dem Europäischen Ausschuss für Systemrisiken (ESRB)[9] die Europäischen Aufsichtsbehörden (ESA), gegliedert in die Europäische Bankenaufsichtsbehörde[10], die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersvorsorge (EIOPA)[11] und die Europäische Wertpapier- und

[8] *Zahradnik/Richter-Schöller*, in Anderl [Hrsg.] #Cybercrime Handbuch für die Praxis: C.8. Exkurs: Vorgaben aus dem Aufsichtsrecht, 96, 96.
[9] VO 1092/2010.
[10] VO 1093/2010.
[11] VO 1094/2010.

Marktaufsichtsbehörde (ESMA)[12]. Weiter umfassen die ESA den Gemeinsamen Ausschuss der ESA und der nationalen Aufsichtsbehörden. Konkret wurde die Bankenaufsicht seit 2014 aufgeteilt von der Europäischen Zentralbank (EZB), der EBA und den nationalen Aufsichtsbehörden wahrgenommen.[13]

Im Jahr 2017 erlässt die EBA erstmals konkrete Vorgaben für die IKT-Risikobewertung.[14] Diese dienen den Aufsichtsbehörden bei der Einstufung der Anstrengungen von Finanzunternehmen im IKT-Risikobereich als Maßstab. Die Finanzunternehmen wiederum haben somit erstmals konkrete Vorgaben, an denen sie ihr Handeln orientieren können und eigenständig ihre Resilienz bewerten können. Die Vorgaben betreffen besonders die Bereiche der IT-Governance, Risikobewertung, die Erkennung von Sicherheits- und Integritätsverletzungen, sowie allgemeine Sicherheitsmaßnahmen und Pläne zur Geschäftsfortführung.[15]

Ersetzt wurden die Vorgaben bereits im Jahr 2019, um der sich schnell wandelnden digitalen Welt weiterhin zu entsprechen und neu entwickelte Technologien einzubeziehen. Außerdem wurden die Vorschriften inhaltlich vertieft, um eine genauere Aufsicht zu ermöglichen und den Finanzunternehmen mehr Planungssicherheit zu gewähren.[16]

Bereits im Jahr 2016 war mit der NIS-Richtlinie (Network and Information Security Directive)[17] ein hoher, europaeinheitlicher Mindeststandart für Netz- und Informationssysteme geschaffen worden. Nach der Umsetzung durch die Mitgliedsstaaten erfolgte im Jahr 2023 die Erneuerung der Anforderungen mit der NIS-2-Richtlinie.[18] Die Umsetzung der NIS-Richtlinie von 2016 durch die Mitgliedsstaaten hatte zu national unterschiedlichen Interpretationen und Ausgestaltungen geführt, welche dem Binnenmarkt wenig förderlich waren, sodass NIS-2 eine Vereinheitlichung anstrebte. NIS-2 beinhaltet außerdem die verpflichtende Schaffung von Anlaufstellen für Cybersicherheit und Cyberkrisenmanagement in den

[12] VO 1095/2010.
[13] VO 1024/2013.
[14] EBA/GL/2017/05.
[15] EBA/GL/2017/17, Leitlinie 2-6.
[16] EBA/GL/2019/04.
[17] RL 2016/1148/EU.
[18] RL 2022/2555/EU.

Mitgliedsstaaten. Zusammen mit der Richtlinie über die Resilienz kritischer Einrichtungen (CER)[19] bedeutet NIS-2 eine deutliche Verschärfung der Sicherheitsvorgaben der Europäischen Union an ihre Mitglieder. Es kommen diverse weitere rechtliche Maßnahmen, wie der Cyber Resilience Act, Digital Services Act, der Data Act oder die e-Privacy-Verordnung hinzu. Alle verfolgten das Ziel, die Europäische Union im digitalen Raum zu stärken.[20]

Dennoch erschienen alle diese Bemühungen dem Europäischen Parlament nicht ausreichend für die Komplexität des Finanzmarktes innerhalb der Europäischen Union. Daher startete das Parlament bereits im Mai 2017 eine Initiative für die Schaffung spezieller Regelungen zum Schutz des Finanzmarktes, welche Big Data, Blockchain, Cybersicherheit, Finanzstabilität und Interoperabilität, aber auch Finanz- und IT-Kenntnisse umfassen soll.[21] Nach einigen Zwischenlösungen wurde schließlich am 14. Dezember 2022 der Digital Operational Resilience Act (DORA) verabschiedet. Ziel von DORA ist es, technologieoffen die Widerstandsfähigkeit europäischer Finanzunternehmen aller Art und ihren IKT-Drittdienstleistern zu gewährleisten, zu vereinheitlichen und zu stärken. Die Sammlung der Handlungsvorgaben in einem Rechtsakt soll für die betroffenen Unternehmen eine Erleichterung darstellen und bestenfalls Synergien bei der Umsetzung der erforderlichen Tests oder bei Erkenntnissen zu Cyberbedrohungen mit sich bringen. Lücken in der Umsetzung und in der Sicherheit sollen durch die Vorgaben von DORA geschlossen werden, es soll Sensibilität hinsichtlich potenzieller Angriffsziele geschaffen werden. Das In-Kraft-Treten und die Umsetzung von DORA erfolgten zum 17. Januar 2025 in den Mitgliedsstaaten der Europäischen Union.

[19] RL 2022/2557/EU.
[20] *Voigt/Falk*, Der Cyber Resilience Act, MMR 2023, 88, 89.
[21] *Europäisches Parlament*, Entschließung der Europäischen Parlaments vom 17. Mai 2017 zur Finanztechnologie: Einfluss der Technologie auf die Zukunft des Finanzsektors, ABl C 30 vom 30.08.2018, 57.

B. Data Operational Resilience Act

I. Inhalt und Zielsetzung

1. Inhaltliche Bestimmungen

Der Gesetzgeber begleitet und kommentiert die Inhalte und die Zielsetzung ausführlich in den Erwägungsgründen. Mit diesem Instrument werden die Normen präzisiert und der Telos im Falle einer Auslegung gelenkt.

a. Kapitel I

Artikel 1 DORA beginnt mit der Definition des Gegenstandes von DORA. Wer soll von der neuen Regelung betroffen sein und in welcher konkreten Hinsicht. DORA benennt dafür das bereichsspezifische Risikomanagement im IKT-Sektor von Finanzunternehmen. Umfasst ist der Umgang mit sicherheitsbezogenen Vorfällen, insbesondere die Meldung solcher und das nachfolgende Handeln des betroffenen Unternehmens. Weiter wird ein Informationsaustausch zwischen Unternehmen und Behörden reglementiert und gefördert. Zum Schutz werden verbindliche Regelungen für Tests der Resilienz vorgeschrieben. Neu ist bei DORA der Einbezug von IKT-Drittdienstleistern für Finanzunternehmen. Dies ist eine Reaktion auf gewandelte Marktteilnehmer, die zunehmend auf Outsourcing setzen. Artikel 2 DORA bestimmt die betroffenen Finanzunternehmen detailliert. Die umfassende Geltung für die Finanzunternehmen sichert eine einheitliche Geltung von DORA, nimmt aber auch einzelne Institutionen vom Geltungsbereich aus. Als solche Ausnahmen sind in Artikel 2 Absatz 3 DORA Verwalter alternativer Investmentfonds gemäß RL 2011/61/EU, Versicherungs- und Rückversicherungsunternehmen gemäß RL 2009/138/EG, Einrichtungen der betrieblichen Altersversorgung unter der Grenze von 15 Versorgungsanwärtern, natürliche und juristische Personen im Sinne der RL 2014/65/EU (Finanzmarktrichtlinie), Versicherungsvermittler sowie vergleichbar Tätige als Kleinstunternehmen, kleine oder mittlere Unternehmen und abschließend Postgiroämter im Sinne der RL 2013/36/EU genannt. Die zersplitterte Regulierung einzelner Zweige auf dem von DORA betroffenen Geschäftsfeld der Finanzunternehmen soll damit vereinheitlicht werden und Übersichtlichkeit

hinzugewonnen werden.[22] Auch nationale Regulierungsansätze werden im Zuge eines einheitlichen Binnenmarktes von DORA in ihrer Ausgestaltung als Verordnung geregelt.[23]

Nach ausführlicher Begriffsdefinition in Artikel 3 DORA nimmt Artikel 4 DORA Bezug auf ein elementares Prinzip, die Verhältnismäßigkeit. Entscheidend für die Strenge der Umsetzung von DORA in ihren Ausprägungen sollen Größe des Unternehmens und das Gesamtrisikoprofil, aus der konkreten Tätigkeit abgeleitet, sein. Art, Umfang und Komplexität von Dienstleistungen, Tätigkeiten und Geschäften sind Maßstab und verhindern damit eine Überregulierung von Unternehmen, die keine entsprechenden Compliance-Kapazitäten bereitstellen können.[24]

b. Kapitel II

Konkrete regulatorische Vorgaben macht DORA in den Artikeln 5 bis 16, dem zweiten Kapitel. Mit Ausnahmen im Zuge des Verhältnismäßigkeitsgrundsatzes aus Artikel 4 DORA für Kleinstunternehmen werden hier interne Strukturen vorausgesetzt, welche auf IKT-Ereignisse reagieren müssen und Teil eines stets vorhandenen IKT-Risikomanagements sein müssen. Insbesondere Organe der Geschäftsführung werden hier ihrer Verantwortung zugeführt.

Es sind interne Governance- und Kontrollrahmen zu schaffen, welche geeignet sind, ein wirksames und umsichtiges IKT-Risikomanagement zu gewährleisten. Ein hohes Maß an digitaler operationaler Resilienz ist dabei das Ziel und entspricht dem Grundgedanken hinter DORA insgesamt.[25] Für die Umsetzung und eine ausreichende Budgetierung verantwortlich sind die jeweiligen Leitungsorgane (Artikel 5 Absatz 2 Satz 1 DORA). Eine laufende Kontrolle und regelmäßige Anpassungen der Prozesse sind verpflichtend, um sich wandelnden Bedrohungen etwas entgegen setzen zu können. Dazu sollen auch externe Schulungen dienen, welche als verpflichtend für die Verantwortlichen definiert werden (Artikel 5 Absatz 4 DORA).

[22] Erwägungsgrund 12 DORA.
[23] Erwägungsgründe 8, 14 DORA.
[24] Erwägungsgrund 36 DORA.
[25] Erwägungsgrund 12 DORA.

Der Umfang der Maßnahmen des IKT-Risikomanagements wird in Artikel 6 DORA aufgezählt. Es zählen konkrete Strategien, Leit- und Richtlinien, Verfahren, Protokolle und Tools zu den vorgegebenen Maßnahmen für eine hohe digitale Resilienz. Dabei ist die Aufschlüsselung des Bestands der Umsetzungen das Mindestmaß, weitere freiwillige Sicherheitsmechanismen sind nicht ausgeschlossen. Die Kontrolle darüber ist wiederum an eine unabhängige Kontrollinstanz zu übertragen, deren Agieren intern nicht beeinträchtigt werden darf. Die Durchführung der Kontrolle der Vorgaben ist dabei einmal jährlich erforderlich, außer es liegen konkrete Vorfälle vor, die eine häufigere Kontrolle erforderlich machen. Erkenntnisse aus den Kontrollen sind nach einem vorab festgelegten Verfahren auszuwerten und Folgen einzuleiten (Artikel 6 Absatz 7 DORA). Dies stellt sicher, dass die Kontrollen auch den positiven Zweck erfüllen, zuverlässiger die digitale Resilienz zu steigern. Ergänzend zu den internen Prozessen sind auch externe Prozesse vorgeschrieben. So ist nicht nur die verbindliche Kommunikation mit Regulierungsbehörden, sondern auch mit anderen Finanzunternehmen sowie mit betroffenen Kunden vorab zu klären, um in Fall eines IKT-Sicherheitsverstoßes handlungsfähig zu bleiben und den Schaden möglichst minimieren zu können.

Artikel 7 stellt die Anforderungen an die IKT-Systeme, -Protokolle und -Tools dar. Diese müssen der Größe des Finanzunternehmens angemessen sein, aktualisiert werden, auf ihre Zuverlässigkeit geprüft werden und ihrem Zweck entsprechend umfassend funktional ausgestattet sein. Die jeweilige Verantwortlichkeit von Beteiligten ist dafür vorab eindeutig festzulegen, ebenfalls um Handlungsfähigkeit sicherzustellen (Artikel 8 DORA). Alle IKT-Systeme sind kontinuierlich auf ihre Funktionstüchtigkeit zu prüfen, was durch festzulegende interne Richtlinien gewährleistet werden soll (Artikel 9 DORA). Je kritischer der Bereich des IKT-Systems, desto umfassender hat die Prüfung zu erfolgen. Die Einschätzung der Kritikalität obliegt dabei den internen Strukturen und wird erst im Nachhinein von externen beurteilt. Sämtliche Maßnahmen sind zu dokumentieren, um bei späteren Haftungsfragen heran gezogen werden zu können.

Anomalien in der Funktionsweise von IKT-Systemen sollen durch entsprechende Mechanismen automatisiert erkannt werden können. Diese sind regelmäßig auf ihre

Funktion zu überprüfen. Dafür werden intern mehrere Kontrollebenen festgelegt und Alarmschwellen definiert, die mit ausreichenden Ressourcen zu unterbauen sind, um eine wirkungsvolle Prüfung zu gewährleisten (Artikel 10 DORA).

Artikel 11 schreibt die Implementierung einer IKT-Geschäftsfortführungsleitlinie vor, die in die allgemeinen Geschäftsfortführungsrichtlinien des Finanzunternehmens zu implementieren sind. Diese umfasst Regelungen, Pläne, Verfahren und Mechanismen, die eine Reaktion auf Vorfälle gewährleisten und die Fortführung kritischer Funktionen sicherstellt. Eine Risikobewertung hat vorab mit einer Business-Impact-Analyse zu erfolgen, die auf die ergriffenen Maßnahmen abgestimmt ist. Regelmäßige Tests, mindestens einmal jährlich, sind dabei vorgesehen, mit Ausnahme von Kleinstunternehmen. Die Ergebnisse sind der zuständigen Behörde zu übermitteln.

Im Falle eines IKT-Vorfalls müssen Systeme zur Wiederherstellung und Wiedergewinnung geschaffen worden sein (Artikel 12 DORA). Diese umfassen zu dokumentierende Maßnahmen zur Datensicherung und Methoden zur Wiedergewinnung und -herstellung. Auch diese sind regelmäßig zu testen. Eine Trennung von logischen und physischen Quellsystemen ist bei diesen Maßnahmen verpflichtend, um eine Manipulation gerade durch die IKT-Risikomanagementsysteme auszuschließen. Ebenfalls sind Redundanzen einzubauen, welche Totalausfälle verhindern sollen. Bei Zentralverwahrern wird ein zweiter, geografisch getrennter Standort gefordert, der dadurch nicht automatisch vom gleichen Vorfall wie der Primärstandort betroffen sein soll. Dies schützt gegen physische Angriffe auf kritische Infrastruktur.

Für Prognosen über mögliche Schwachstellen im IKT-Bereich und daraus resultierende Angriffspunkte müssen Finanzunternehmen personelle und materielle Ressourcen bereithalten (Artikel 13 DORA). Diese befassen sich mit der nachträglichen Aufarbeitung von Vorfällen und erarbeiten auf Grundlage dieser Handlungsempfehlungen für die Zukunft. Die Erkenntnisse dieser Prozesse sind wiederum der zuständigen Behörde mitzuteilen. Das Wissen stammt somit aus einer Eigenverantwortung, deren Wahrnehmung nachträglich zur Kenntnis genommen wird.

Interne und externe Kommunikationsstrategien sind von den Unternehmen generell festzulegen und sollen verantwortungsbewusst entsprechend der Schwere der Vorfälle zur Offenlegung genutzt werden (Artikel 14 DORA). Es ist eine konkrete Person im Unternehmen zu beauftragen, die die Umsetzung dieser Strategien verantwortet.

Artikel 15 DORA verpflichtet die ESA, gemeinsam mit der ENISA, Entwürfe technischer Standards zu entwickeln, die den Finanzunternehmen helfen können, ihre Abläufe zu planen und eine Einschätzung des IKT-Risikos vorzunehmen.[26]

Schließlich nimmt Artikel 16 DORA ausgewählte Finanzunternehmen wieder von den Vorgaben aus. Für diese gilt aufgrund ihrer individuellen Leistungsfähigkeit im Governancebereich ein vereinfachter IKT-Risikomanagementrahmen, der dem Verhältnismäßigkeitsgrundsatz aus Artikel 4 DORA Rechnung tragen soll. Die zuständige Behörde kann von dem Finanzunternehmen einen Bericht zu einem schwerwiegenden Vorfall und daraus erfolgten Erkenntnissen und der Umsetzung des IKT-Risikomanagementrahmens anfordern.

c. Kapitel III

Eine Konkretisierung der Handlungsvorgaben für Finanzunternehmen wird in den Artikeln 17 ff DORA vorgenommen. Es sind Prozesse einzurichten, die IKT-bezogene Vorfälle erkennen, behandeln und melden. Dies schreibt vor, dass alle IKT-bezogenen Vorfälle zu erfassen sind, nach erkennen dauerhaft zu überwachen sind und die Ursachen erforscht werden müssen. Eine Mitteilung an die zuständige höhere Führungseben ist ebenfalls verpflichtend (Artikel 17 Absatz 3 lit e DORA), was bei Haftungsfragen Relevanz entfalten könnte.

Sodann hat nach Erkenntnis eines IKT-bezogenen Vorfalls eine Klassifizierung zu erfolgen. Diese richtet sich gemäß Artikel 18 DORA intern nach der Reichweite der betroffenen Kundschaft, dem Wert des betroffenen Geschäftsbereiches und der Reichweite des Reputationsschadens. Auch die Dauer des Vorfalls, die geografische Ausbreitung und die erfolgten Einschränkungen sind Maßstäbe für die Einstufung des Vorfalls. Je risikobehafteter der betroffene Geschäftsbereich für das jeweilige

[26] Veröffentlicht als delegierte Verordnung (EU) 2024/1774 der Kommission vom 13. März 2024.

Finanzunternehmen ist, desto schwerwiegender ist der Vorfall einzustufen. Die Höhe eines erlittenen Schadens, direkt oder indirekt, ist ebenfalls ein Faktor dafür. Auch hierfür werden die ESA zusammen mit der ENISA verpflichtet, Entwürfe für technische Regulierungsstandards zu entwerfen, die sowohl den Finanzunternehmen, als auch den zuständigen Behörden als Maßstab dienen sollen.[27]

Ist ein IKT-bezogener Vorfall als schwerwiegend klassifiziert worden, hat das Finanzunternehmen entsprechend Artikel 19 DORA zu verfahren. Die Meldung an die zuständige Behörde ist dabei die wichtigste Anforderung.[28] Bei Cyberbedrohungen, die vom Finanzunternehmen bemerkt werden, aber nicht einen direkten Angriff auf das Unternehmen darstellen, ist eine Meldung an die zuständigen Behörden freiwillig. Auch betroffene Kunden des Finanzunternehmens sind zu informieren, um geeignete Schutzmaßnahmen ergreifen zu können.

Die Meldung von Vorfällen teilt sich in drei einzelne Meldestufen zu unterschiedlichen Zeitpunkten (Artikel 19 Absatz 4 DORA). Es hat eine Erstmeldung zu erfolgen, deren Zweck der Hinweis auf potenzielle Schäden ist. Die Zwischenmeldung hat zu erfolgen, sobald erhebliche Änderungen der Umstände seit der Erstmeldung eingetreten sind. Jede Änderung soll der zuständigen Behörde mitgeteilt werden, sodass diese immer einen aktuellen Wissensstand über den Vorfall hat. Bei Zweifeln kann die zuständige Behörde eine solche Zwischenmeldung auch aktiv anfordern. Nach Abschluss der Ursachenanalyse des IKT-bezogenen Vorfalls hat eine Abschlussmeldung zu erfolgen, die auch einen Bericht über die tatsächlichen Auswirkungen des Vorfalls zu enthalten hat. Der Meldeprozess kann, ohne dabei die Haftung umgehen zu können, an einen Drittdienstleister ausgelagert werden, solange dies den jeweiligen sektorspezifischen Rechtsvorschriften entspricht.

Die zuständige Behörde wiederum muss die Meldung des schwerwiegenden Vorfalls an festgelegte Empfänger weiterleiten. Dies dient dem vollumfänglichen Schutz des gesamten Sektors, sowie nachgeschalteten Einrichtungen und Marktteilnehmern. Diese Empfänger können je nach Sachlage die EBA, die ESMA oder die EIOPA, die EZB, weitere zuständige Behörden und die CSIRTs sein. Auch eine unionsweite Verbreitung

[27] Veröffentlicht als delegierte Verordnung (EU) 2024/1772 der Kommission vom 13. März 2024.
[28] Erwägungsgrund 52 ff DORA.

der Meldung kann vorgenommen werden, sollte der Vorfall das Potential aufweisen, grenzüberschreitend eine Beeinträchtigung darzustellen.

Erneut werden die ESA beauftragt, entsprechende Richtlinien zu erarbeiten, die Meldungen und Fristen näher beschreiben und eine Umsetzung für Finanzunternehmen und zuständige Behörden vereinfachen (Artikel 20 DORA). Darüber hinaus strebt die Europäische Union eine zentrale Plattform an, auf der IKT-bezogene Vorfälle gesammelt und deren Folgen bewertet werden. Dazu soll die EBA einen Bericht über die Durchführbarkeit vorlegen.[29]

Die zuständige Behörde kann nach einer erfolgten Erstmeldung dem betroffenen Finanzunternehmen im rechtlich möglichen Rahmen Informationen zur Verfügung stellen, die die Eindämmung eines Vorfalls unterstützen und auf aus der Vergangenheit gewonnen Erkenntnissen beruhen (Artikel 22 DORA). Trotzdem bleibt da Finanzunternehmen selbst umfänglich verantwortlich für den Vorfall und muss den Umgang damit selbstständig handhaben können. Eine Pflicht zur Unterstützung durch die zuständige Behörde besteht nicht.

Artikel 23 DORA erweitert die Regelungen zur Meldung schwerwiegender IKT-bezogener Vorfälle auch auf solche, die zahlungsbezogenen Betriebs- und Sicherheitsvorfälle, Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister und E-Geld-Institute betreffen. Das Sicherheitsnetz soll den Finanzsektor somit umfassend schützen.

d. Kapitel IV

Das wichtigste Mittel zur Erreichung einer hohen digitalen Resilienz und der Verhinderung von IKT-bezogenen Vorfällen sind Tests, die den aktuellen Stand der Maßnahmen widerspiegeln.

Ein umfassendes und solides Programm für Tests der digitalen operationalen Resilienz ist für Finanzunternehmen, die keine Kleinstunternehmen sind, im Maßstab des Artikel 4 DORA verpflichtend (Artikel 24 DORA). Mit diesem Programm soll die Resilienz erkannt und sollen notwendige Korrekturmaßnahmen umgesetzt werden

[29] Veröffentlicht als delegierte Verordnungen (EU) 2025/301 und (EU) 2025/302 der Kommission vom 23. Oktober 2024.

können. Die Tests sind mindestens einmal jährlich von internen oder externen unabhängigen Testern durchzuführen. Interne Tester sind dabei mit ausreichend Ressourcen auszustatten[30] und Interessenskonflikte dürfen nicht vorliegen. Die Art und Weise der Tests hat risikobasiert ausgewählt zu werden, sodass eine genaue Abstimmung auf das einzelne Finanzunternehmen erfolgen muss. Absatz 5 schreibt vor, dass vorab die Verfahren zur Behebung von festgestellten Mängeln zu definieren sind, sodass die Umsetzung unverzüglich und vollständig erfolgen kann. Als Testfelder werden Schwachstellen, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, die physische Sicherheit der Einrichtungen, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen genannt, sowie szenarienbasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests (Artikel 25 DORA).[31] Zentralverwahrer und zentrale weitere Vertragsparteien müssen solche Tests bereits durchgeführt haben, bevor sie IKT-Dienstleistungen für Finanzunternehmen erbringen dürfen.

Die zuständigen Behörden wählen gemäß Artikel 4 Absatz 2 iVm Artikel 26 Absatz 8 DORA Finanzunternehmen aus, die ein besonders hohes Gesamtrisiko tragen, die ein besonders komplexes Geschäftsfeld haben, die besonders relevant für die Stabilität der Finanzmärkte sind oder die aufgrund ihres Geschäftsbetriebs im IKT-Bereich vermutete Schwächen aufweisen könnten. Diese ausgewählten Finanzunternehmen müssen sich mindestens alle drei Jahre dem so genannten Thread-Led-Penetration-Testing (TLPT) unterziehen. Diese erweiterten Tests für IKT-Systeme sind besonders tiefgehend, erfolgen bedrohungsorientiert und werden an Live-Produktionssystemen durchgeführt. Damit wird ein möglichst umfassendes und realitätsnahes Bedrohungsszenario erzeugt. Die Finanzunternehmen bestimmen zunächst selbst, welche Funktionen vom TLPT geprüft werden, die Auswahl wird jedoch von der zuständigen Behörde noch validiert. Es sollen regelmäßig mehrere, im besten Fall sogar alle kritischen Funktionen des Finanzunternehmens einbezogen werden. Auch IKT-Drittdienstleister, die im Auftrag von Finanzunternehmen stehen, müssen sich dem TLPT unterziehen (Artikel 26 Absatz 3 DORA). Im Falle von mehreren Finanzunternehmen, die auf

[30] Erwägungsgrund 61 DORA.
[31] Erwägungsgrund 56 DORA.

denselben IKT-Drittdienstleister zurückgreifen, ist eine Bündelung des TLPT möglich.[32] Dies dient der Kosteneffizienz und soll eine erhöhte Akzeptanz der aufwändigen Vorgänge schaffen.

Die Ergebnisse des TLPT sind der zuständigen Behörde vorzulegen und die Umsetzung gegebenenfalls erforderlicher Abhilfemaßnahmen ist vorzuweisen. Daraufhin stellt die zuständige Behörde dem Finanzunternehmen eine Bescheinigung über die Durchführung des TLPT aus, welche im Umgang mit Vertragspartnern anzugeben ist. Eine Haftungsbefreiung für die Finanzunternehmen über die Folgen der Tests wird ausdrücklich nicht vorgenommen (Artikel 26 Absatz 7 DORA). Werden interne Tester eingesetzt, müssen für jeden dritten Test trotzdem externe Tester eingesetzt werden, um eine objektive und konfliktfreie Bewertung vornehmen zu können.

Wieder werden die ESA beauftragt, in Einvernehmen mit der EZB Entwürfe zur technischen Regulierung des TLPT zu entwerfen.[33]

Um den TLPT die erforderliche Aussagekraft zukommen zu lassen und sie als wirkungsstärkste Mittel zur Überprüfung der digitalen operationalen Resilienz auszuzeichnen, werden besonders hohe Anforderungen an die durchführenden Tester gestellt. Artikel 27 DORA nennt als Voraussetzung für diese höchste Eignung und Ansehen, Fachwissen in technischer und organisatorischer Art über TLPT, eine Zertifizierung durch eine Akkreditierungsstelle innerhalb der Europäischen Union oder formale Verhaltenskodizes, Nachweise über die Durchführung mit besonderem Augenmerk auf den Schutz vertraulicher Daten und eine entsprechende Berufshaftpflichtversicherung. Diese hohen Anforderungen sollen bewirken, dass nur nachgewiesen kompetente Tester für TLPT in Finanzunternehmen zugelassen werden.

Für interne Tester muss weiterhin eine Genehmigung durch die zuständige Behörde ausgestellt werden und eine Prüfung der ausreichend zur Verfügung gestellten Ressourcen durchgeführt worden sein. Der Anbieter der Bedrohungsanalyse darf nicht dem Finanzunternehmen selbst angehören. Für externe Tester muss das

[32] Erwägungsgrund 60 DORA.
[33] Veröffentlicht als delegierte Verordnung (EU) 2025/1190 der Kommission vom 13. Februar 2025.

Finanzunternehmen selbstständig die Sicherheit der Durchführung vom TLPT garantieren und entsprechende vertragliche Absicherungen vereinbaren.

e. Kapitel V

Eine weitrechende Ausdehnung des Anwendungsbereiches von DORA stellt die Einbeziehung von IKT-Drittdienstleistern dar. Erstmals wird das Drittparteienrisiko erfasst und Maßnahmen auch für Drittanbieter werden normiert.

Die Finanzunternehmen müssen das Risiko, welches durch die Verwendung von IKT-Dienstleistungen seitens Drittanbieters entsteht, selbst in ihrem IKT-Risikomanagementrahmen berücksichtigen. Verantwortlichkeit und Haftung bleiben zu jedem Zeitpunkt beim Finanzunternehmen selbst (Artikel 28 Absatz 1 lit a DORA). Die Einbindung von IKT-Drittdienstleistern in das interne Risikomanagement erfolgt dabei nach dem Prinzip der Verhältnismäßigkeit. In der Risikoabwägung erfolgen ähnliche Maßnahmen, die auch auf das Finanzunternehmen selbst angewendet werden, wie regelmäßige Überprüfungen und Aktualisierungen der operationellen Verflechtungen. Besondere Aufmerksamkeit ist solchen IKT-Drittdienstleistern zu widmen, die nicht ohne Weiteres ersetzbar sind oder die mehrfache vertragliche Vereinbarungen haben, die eine stärkere Verflechtung begründen (Artikel 29 Absatz 1 DORA). Die IKT-Drittdienstleister können Teile ihrer Aufgaben wiederum an Drittdienstleister weiterreichen. Diese sind dem Finanzunternehmen anzuzeigen, sodass die Erweiterung der beteiligten Unternehmen in die Risikoabwägung einfließen kann. Sowohl der IKT-Drittdienstleister, als auch dessen Drittdienstleister müssen sich auch bei Sitz in einem Drittstaat an die Datenschutzvorschriften der Europäischen Union halten. Dies dient dem Verbraucherschutz, ist aber auch Teil der Risikoabwägung des Finanzunternehmens.

Das Finanzunternehmen hat der zuständigen Behörde mindestens einmal jährlich einen Bericht über seine Beziehungen zu IKT-Drittdienstleistern zu erstatten. Dieser Bericht beinhaltet auf Verlangen das verpflichtend zu führende Informationsregister über sämtliche vertraglichen Vereinbarungen mit genutzten IKT-Drittdienstleistern. Bereits in der Planungsphase ist die zuständige Behörde von einer anstehenden

Änderung der vertraglichen Beziehungen zu IKT-Drittdienstleistern in Kenntnis zu setzen.

Jedem Abschluss von vertraglichen Vereinbarungen mit IKT-Drittdienstleistern hat eine Prüfung durch das Finanzunternehmen vorauszugehen. Diese dienen der Bewertung des Risikos, was durch die ausgelagerte Tätigkeit auf den IKT-Drittdienstleister übergeht. Um die Verantwortung für dieses Risiko tragen zu können, muss das Finanzunternehmen konkrete Standards für Informationssicherheit mit dem Drittdienstleister vereinbaren. Diese sind zu prüfen, indem dem Finanzunternehmen umfassende Zugangs-, Inspektions- und Auditrechte eingeräumt werden. Die eingegangenen Verträge müssen gemäß Artikel 28 Absatz 7 DORA kündbar sein, wenn erhebliche Verstöße des Drittdienstleisters gegen Gesetze, Vorschriften oder Verträge vorliegen, Unregelmäßigkeiten bei den erfolgenden Kontrollen, nachweisliche Schwachstellen des Dienstleisters im IKT-Risikomanagement oder bei einer durch die Auslagerung erfolgten Einschränkung der Aufsicht der zuständigen Behörde. Ein direkter Ausstieg aus den vertraglichen Vereinbarungen muss ermöglicht werden, sollte der IKT-Drittdienstleister seine Geschäftstätigkeit unterbrechen, die regulatorischen Anforderungen nicht mehr erfüllen oder die erbrachte Leistung nicht der erforderlichen Kontinuität und Qualität entsprechen. Die Ausstiegspläne sind vorab zu dokumentieren und müssen regelmäßig geprüft und getestet werden. Eine Rückführung von Daten, die an den IKT-Drittdienstleister übertragen wurden, muss sichergestellt werden, sodass auch ein Übergang auf einen Ersatzdienstleister ermöglicht wird. Die Geschäftstätigkeit des Finanzunternehmens darf nicht durch eine Beeinträchtigung des IKT-Drittdienstleisters eingeschränkt werden.

Entsprechende Entwürfe für technische Durchführungsstandards werden von den ESA erarbeitet und nach Annahme durch die Europäische Kommission den Finanzunternehmen zur Verfügung gestellt (Artikel 28 Absatz 9, 10 DORA).[34]

Für Verträge zwischen Finanzunternehmen und IKT-Drittdienstleistern gelten besondere vertragliche Mindestbestandteile. Diese werden in Artikel 30 DORA

[34] Veröffentlicht als delegierte Verordnung (EU) 2024/2956 der Kommission vom 29. November 2024 und delegierte Verordnung (EU) 2024/1773 vom 13. März 2024.

aufgezählt. Für die Übernahme von als kritisch oder wichtig eingestuften Tätigkeiten gelten weitergehende Vorgaben (Artikel 30 Absatz 3 DORA). Die ESA entwickeln dazu passende technische Regulierungsstandards, die als Standardvertragsklauseln von den Finanzunternehmen zu verwenden sind.[35]

Die Einstufung als kritischer IKT-Drittdienstleister erfolgt durch die ESA. Entscheidend ist wieder die mögliche Beeinträchtigung von Stabilität, Kontinuität oder Qualität der Finanzdienstleistungen, sollte der IKT-Drittdienstleister ausfallen. Auch die Reichweite des den IKT-Drittdienstleister beauftragenden Finanzunternehmens ist entscheidend sowie die Abhängigkeit, die durch die konkrete ausgelagerte Tätigkeit entstehen kann. Eine Alternativlosigkeit des IKT-Drittdienstleisters mangels Konkurrenten auf dem Markt oder aufgrund einer nur schwer vollziehbaren Migration zu einem Konkurrenten stellt ebenfalls ein Kriterium für einen kritischen IKT-Drittdienstleiter dar. Durch die Konzentration im digitalen Bereich auf wenige international tätige Konzerne, oft aus den Vereinigten Staaten von Amerika stammend, nimmt dieses Kriterium besondere Bedeutung ein. Europäische Finanzunternehmen sind mangels europäischer Alternativen regelmäßig abhängig von den digitalen Dienstleistungen aus drittstaatsangehörigen Technologiekonzernen. Gemäß Artikel 31 Absatz 12 DORA erfordert eine Inanspruchnahme dieser, sollten sie als kritisch eingestuft worden sein, eine Gründung einer innereuropäischen Niederlassung innerhalb von zwölf Monaten nach der Einstufung. IKT-Drittdienstleister können zusätzlich selbst beantragen, als kritischer eingestuft zu werden. Eine Entscheidung darüber hat innerhalb von sechs Monaten ab Antragstellung von der EBA, ESMA oder der EIOPA getroffen zu werden.

Die ESA haben dem IKT-Drittdienstleister seine Einstufung als kritisch mitzuteilen, sowie den Beginn der Überwachung durch die zuständigen Behörden. Der IKT-Drittdienstleister muss seine Einstufung als kritisch dem beauftragenden Finanzunternehmen mitteilen. Von den ESA werden die als kritisch eingestuften IKT-Drittdienstleister in einer jährlich aktualisierten Liste veröffentlicht.

Die Überwachung der kritischen IKT-Drittdienstleister erfolgt durch einen Unterausschuss des Gemeinsamen Ausschuss, welcher gemäß Artikel 57 Absatz 1 der

[35] Veröffentlicht als delegierte Verordnung (EU) 2025/532 der Kommission vom 24. März 2025.

Verordnungen (EU) 1093/2010, (EU) 1094/2010 und (EU) 1095/2010 geschaffen wird. Darin wird die jeweils zuständige Überwachungsbehörde gemäß Artikel 31 Absatz 1 lit b DORA benannt. Im Überwachungsforum sitzen neben den Vorsitzenden der ESA auch Vertreter der zuständigen nationalen Behörde und Beobachter von weiteren europäischen Aufsichtsbehörden. Unterstütz werden sie von unabhängigen Sachverständigen, die im Interesse der Europäischen Union als Ganzes beraten müssen.

Die federführende europäische Überwachungsbehörde, ernannt gemäß Artikel 31 Absatz 1 lit b DORA, die nicht gleich der zuständigen (nationalen) Behörde ist, ist für den IKT-Drittdienstleister vorrangige Anlaufstelle. Kriterien bei der Bewertung des IKT-Drittdienstleisters sind sämtliche IKT-Anforderungen, die Sicherheit, Kontinuität, Skalierbarkeit und Qualität beeinträchtigen. Auch die physische Sicherheit der Geschäftsvorgänge, Risikomanagementprozesse, Governance-Regelungen, der Umgang mit IKT-bezogenen Vorfällen und zugehörige Tests und Audits sind Maßstab. Dafür wird ein individuell auf den IKT-Drittdienstleister angepasster Überwachungsplan erstellt, der dem Dienstleister zur Verfügung zu stellen ist.

Die federführenden Behörden EBA, ESMA und EIOPA stimmen sich bei der Überwachung der jeweils zugeteilten IKT-Drittdienstleister ab, indem sie ein Joint Oversight Network (JON)[36] gründen.

Umfangreiche Befugnisse werden der federführende Überwachungsbehörde eingeräumt. Diese kann alle einschlägigen Informationen und Unterlagen anfordern, die zur Erfüllung ihrer Aufgabe erforderlich sind (Artikel 37 DORA). Auch technische Unterlagen jeglicher Art sind der federführenden Behörde bei Untersuchungen und Inspektionen mitzuteilen (Artikel 38, 39 DORA). Eine Überprüfung der Abhilfemaßnahmen ist durch einen Bericht des IKT-Drittdienstleisters sicherzustellen. Neben der umfassenden Überwachung soll die federführende Behörde auch Empfehlungen aussprechen, die die konkrete Lage im überwachten Unternehmen verbessern sollen.

[36] Erwägungsgrund 94 DORA.

Die Durchsetzung der Maßnahmen der federführenden Überwachungsbehörde kann mit einem Zwangsgeld forciert werden (Artikel 35 Absatz 6 DORA). Dieses orientiert sich am durchschnittlichen weltweiten Tagesumsatz des IKT-Drittdienstleisters. Damit liegt den Überwachungsbehörden ein wirkungsvolles Instrument gegenüber dem zu Überwachenden vor. Die Konzentration von IKT-Drittdienstleistungen auf wenige internationale Unternehmen lässt hohe weltweite Tagesumsätze entstehen und damit mögliche Summen von Bußgeldern, die die Unternehmen empfindlich treffen können. Die Befugnisse der federführenden Überwachungsbehörde erstrecken sich bei einer Verweigerung der angemessenen Kommunikation durch den IKT-Drittdienstleister auf alle Standorte in einem Drittland, die sich im Eigentum des Unternehmens befinden. Damit wird eine Durchsetzung der Überwachung auch für Drittstaaten gewährleistet. Die Zusammenarbeit mit dem IKT-Drittdienstleister und nationalen zuständigen Behörden in den Drittstaaten ist für einige Maßnahmen jedoch erforderlich. Es können Abkommen geschlossen werden, die vorsorglich eine Zusammenarbeit mit den ESA und nationalen Behörden von Drittstaaten sicherstellen (Artikel 36 Absatz 2 DORA).

Ein IKT-Drittdienstleister kann innerhalb von 60 Tagen nach Eingang der Empfehlungen der federführenden Überwachungsbehörde seine Absicht äußern, Folge zu leisten oder aber eine Gegendarstellung abgeben (Artikel 40 Absatz 1 DORA). Für den Fall keiner Äußerung oder einer unzureichenden Äußerung durch den IKT-Drittdienstleister wird die Behörde öffentlich darüber berichten, um den potenziellen Kundenkreis zu sensibilisieren und Druck auf den IKT-Drittdienstleister auszuüben. Wird im Zuge des Verfahrens nach den Empfehlungen durch die Behörde keine Einigkeit erzielt, kann die Behörde die Nutzung des IKT-Drittdienstleisters durch das Finanzunternehmen vorübergehend oder endgültig einschränken. Auch können bei besonders schweren Vorfällen Änderungen an den vertraglichen Vereinbarungen zwischen Drittdienstleister und Finanzunternehmen von der Behörde erwirkt werden.

Die Kosten der Überwachung des IKT-Drittdienstleister sind von diesem selbst zu tragen (Artikel 43 Absatz 1 DORA). Es ist bei der Rechnungsstellung auf die Verhältnismäßigkeit zu achten. Kosten für IKT-Systeme der ESA, die für die

Überwachung vorab benötigt werden, sind hingegen von der Europäischen Union und den zuständigen nationalen Behörden zu übernehmen.[37]

Die ESA können Verwaltungsvereinbarungen mit den Regulierungs- und Überwachungsbehörden von Drittländern bezüglich der IKT-Drittdienstleister schließen, über welche sie alle fünf Jahre dem Europäischen Parlament, dem Rat und der Kommission Bericht erstatten müssen (Artikel 44 DORA).

f. Kapitel VI

Artikel 45 gewährt den Finanzunternehmen die Möglichkeit, Informationen über Cyberbedrohungen untereinander auszutauschen und den Umgang bei der Aufklärung von IKT-bezogenen Vorfällen voneinander zu lernen. Dies ist dann zulässig, wenn die digitale operationale Resilienz insgesamt gestärkt wird und eine Sensibilisierung für Cyberrisiken geschaffen wird, es innerhalb einer vertrauenswürdigen Gemeinschaft von Finanzunternehmen erfolgt und der Schutz sensibler Informationen und Daten dauerhaft gewährleistet ist. Insbesondere dürfen dadurch Wettbewerbsregeln nicht verletzt werden, keine Marktabsprachen getroffen werden und auch Kontrollmechanismen durch die Behörden nicht beeinträchtigt werden. Vielmehr sind staatliche Behörden in den Austausch einzubeziehen, wenn ihre Tätigkeitsfelder betroffen sind.

g. Kapitel VII

Die für die Durchsetzung von DORA zuständige Behörde richtet sich gemäß Artikel 46 DORA nach der Art des Finanzunternehmens. In einer Vielzahl von Verordnungen der Europäischen Union werden den Finanzunternehmen zuständige Behörden zugewiesen, die nun auch für DORA zuständig sind. Zuständige nationale, federführende europäische und weitere involvierte Behörden sollen darüber hinaus untereinander zusammenarbeiten (Artikel 48, 49 DORA) und auch mit Behörden, die für die Kontrolle und Durchführung der VO (EU) 2022/2555 (NIS-2) verantwortlich sind, kooperieren (Artikel 47 DORA). Der Austausch der hierfür erforderlichen Informationen unterliegt einem besonders strengen Berufsgeheimnis (Artikel 55 DORA). Jeder Austausch bedarf einer nationalen oder europäischen

[37] Erwägungsgrund 96 DORA.

Rechtsgrundlage und jede Person, die bei einer zuständigen Behörde, einem Marktteilnehmer oder einer zugehörigen natürlichen oder juristischen Person beschäftigt ist, fällt unter dieses strenge Berufsgeheimnis.

Auch muss bei der Ausübung der Plichten der Behörden auf den Datenschutz aus der VO (EU) 2016/679 (DSGVO) und dem Gegenstück für die europäischen Behörden VO (EU) 2018/1725 geachtet werden. Dies umfasst den Grundsatz der Datenminimierung, dass also personenbezogenen Daten nur soweit verarbeitet werden dürfen, wie es zur Erfüllung der Aufgaben erforderlich ist.

Die zuständigen nationalen Behörden sind mit allen Aufsichts-, Untersuchungs- und Sanktionsbefugnissen auszustatten, die zur Erfüllung der Aufgaben erforderlich sind. Artikel 50 Absatz 2 DORA gibt dafür ein Mindestmaß vor, welches Zugriff auf Daten, Vor-Ort-Inspektionen und Vorladungen und Befragungen, sowie das Verlangen von Korrektur- und Abhilfemaßnahmen umfasst.

Dazu kommen verwaltungsrechtliche Sanktionen, die von den Mitgliedsstaaten in wirksamer, verhältnismäßiger und abschreckender Weise festzulegen sind. Diese müssen mindestens Weisungserteilungen, Unterlassungsverlangen, finanzielle Druckmittel und die Verpflichtung zu öffentlichen Bekanntmachungen enthalten. Bei juristischen Personen müssen sowohl die Sanktionsbefugnisse, als auch die verwaltungsrechtlichen Sanktionen auch gegenüber Mitgliedern des Leitungsorgans verhängt werden können.

Als schärfstes Schwert dürfen die Mitgliedsstaaten strafrechtliche Sanktionen vorsehen (Artikel 52 DORA). Dies schließt verwaltungsrechtliche Sanktionen im konkreten Fall aus, um eine Doppelbestrafung zu vermeiden.[38]

Verwaltungsrechtliche Sanktionen sind von den zuständigen Behörden auf ihren amtlichen Webseiten öffentlich bekannt zu machen. Dazu gehört neben der Sanktion selbst die Angabe der Art des Verstoßes und die Nennung der Identität der Verantwortlichen. Es kann ein Aufschub oder eine Anonymisierung der Meldung erfolgen, wenn dies entsprechende Gründe erfordern (Artikel 54 Absatz 3 DORA). Grundsätzlich darf die Meldung nur so lange öffentlich einsehbar bleiben, wie es nach

[38] Deutschland und Österreich haben von dieser Möglichkeit keinen Gebrauch gemacht.

dem Zweck der Veröffentlichung dienlich ist. Dies ist die Warnung eines potenziell betroffenen Kreises an Marktteilnehmern sowie die Druckausübung auf die Verantwortlichen. Maximal fünf Jahre lang darf eine Mitteilung insgesamt veröffentlich sein.

2. Ziele und Methodik

Die Europäische Kommission verfolgt mit DORA unterschiedliche Ziele, die sie mit unterschiedlichsten Methoden in der Ausführung von DORA umzusetzen anstrebt.

a. Ziele

Das große Projekt der Europäischen Kommission ist die digitale Transformation der europäischen Finanzsektors.[39] Europa als einheitlicher Wirtschaftsraum liegt hinsichtlich digitaler Prozesse hinter dem amerikanischen und dem asiatischen Raum zurück. Ziel der Maßnahmen der Europäischen Union ist es, die wirtschaftlichen Abläufe im Binnenmarkt durch eine starke Digitalisierung wettbewerbsfähig zu halten und Innovationen zu fördern. Dabei sind stets auch Verbraucherinteressen zu berücksichtigen, deren Schutz ebenfalls im Interesse der Kommission liegt. Um diesen Zielen näher zu kommen, wurde DORA geschaffen, die kritische IKT-Dienstleister im Finanzsektor regulieren soll.

Dazu kommt das Ziel, eine reibungslose Funktion des Finanzmarktes innerhalb der Europäischen Union zu gewährleisten.[40] Die Bedrohungen dessen sind durch die Verlagerung der Tätigkeiten in den digitalen Raum stark angestiegen. Digitale Angriffe treten vielfältig und schnell wandelnd auf, was eine dauerhaft hohe Wachsamkeit erfordert.

Mit der Sicherhit der IKT-Systeme wird nicht nur die Geschäftstätigkeit der Finanzunternehmen geschützt, sondern auch die Daten und das Vermögen der Kunden, welche auch aus dem privaten Bereich kommen. Der Verbraucherschutz ist

[39] *Europäische Kommsission*, Mitteilung vom 24.9.2020 über eine Strategie für ein digitales Finanzwesen in der EU, COM (2020) 591 final, 1, 5.
[40] *Europäische Kommsission*, Mitteilung vom 24.9.2020 über eine Strategie für ein digitales Finanzwesen in der EU, COM (2020) 591 final, 22.

ein generell hoch gewichtetes Anliegen der Europäischen Union und DORA soll auch diesem Nachdruck verleihen.

b. Zusammenfassung der Methodik

DORA hat fünf maßgebliche Säulen, die die Umsetzung prägen und unterschiedliche Ansatzpunkte für die Erreichung der Ziele haben.[41]

aa. Interne Regulierung

Das IKT-Risikomanagement der Finanzunternehmen ist in DORA umfassend neu geregelt. Es müssen intern neue Strategien, Richtlinien und Verfahren festgelegt werden, die auf unterschiedliche Szenarien vorbereitet sind und klare Handlungsvorgaben aufweisen. Direkt betroffen davon sind alle Standorte eines Finanzunternehmens, weil jeder einzelne auch physische Risiken bedeutet, interne Compliance-Abteilungen und die Geschäftsführungen als Verantwortliche selbst. Kapitel 2 DORA ist Schwerpunkt der entsprechenden Regelungen dazu. Die ausführlichen Vorgaben sollen die vollständige Umsetzung durch die Finanzunternehmen unterstützen.[42]

bb. Externe Regulierung

Nach der Regulierung interner Abläufe ist der Umgang mit IKT-bezogenen Vorfällen in DORA nach außen normiert. Dieser umfasst die ausführliche Verpflichtung der Finanzunternehmen, über ihre Maßnahmen zur Steigerung der digitalen operationalen Resilienz an die zuständigen Behörden zu berichten. Beim Vorliegen von Vorfällen werden diese Pflichten nochmals verschärft. Den Behörden wird somit ein umfassender Wissensstand vermittelt, wie die generelle Situation im Finanzsektor, aber auch die Reaktionsfähigkeiten in konkreten Krisensituationen ausgeprägt sind. Entsprechende Maßnahmen der Behörden können daraufhin erfolgen. Der Eigenverantwortung wird somit eine umfassende Kontrolle aufgesetzt. Behörden entscheiden auch, ob Wettbewerber einbezogen werden. Die Informationsverbreitung innerhalb des Finanzsektors tritt damit neben die Kontrolle

[41] *Škorjanc*, Digital Operational Resilience Act, ÖBA 9/2023, 658, 659.
[42] *Thiele/Wagner*, Vorbildliches IKT-Risikomanagement mit Auftragsverarbeitern im NIS-Zeitalter, jusIT 2025/2, 6, 10.

als Methodik, um im Finanzsektor die erwünschten Ziele zu erreichen. Außerdem können und sollen die Behörden unterstützend den Finanzunternehmen zur Seite stehen. Ein reines Gegeneinander ist nicht gewünscht, sondern eine gemeinsame Arbeit zur Erreichung der übergeordneten Ziele erforderlich. Normiert ist dieses Vorgehen in Kapitel 3 DORA.

cc. Tests

Von den umfassenden Vorgaben ausgenommen ist eine sehr spezifisch ausgearbeitete Methodik, die Tests der digitalen operationalen Resilienz. Die Penetrationstests der Systeme der Finanzunternehmen sind die nächste Stufe in der vorgeschriebenen Strategie. Nach intern wirkenden Vorgaben und Pflichten zur umfangreichen Kommunikation werden nachweisbare Ergebnisse durch Tests gefordert. Objektive Ergebnisse werden durch die Tests generiert, welche den aktuellen Stand über jede in der Theorie aufgestellte Leitlinie hinaus widerspiegeln. Damit geht die Europäische Kommission in Kapitel 4 DORA sehr weit in ihrer Anforderung an die Kontrolle der Einhaltung von DORA und der Erreichung der Ziele.

dd. Erweiterter Anwendungsgegenstand

Neuartigste Regulierung ist die Ausweitung des Anwendungsbereiches von DORA auch auf IKT-Drittanbieter. Diese sind originär nicht Teil des Finanzsektors, bieten diesem aber Leistungen an und werden, um einen ganzheitlichen Schutz zu erreichen, auch von DORA erfasst. Auch diese unterliegen gemäß Kapitel 5 DORA den Anforderungen an interne Abläufe und auch den Pflichten zu Berichten an zuständige Behörden sowie den Kontrollen durch diese. Für die Ausgestaltung der vertraglichen Vereinbarungen sichert sich die Europäische Kommission erstmals tiefgehende Kontrolle über Inhalt, Umfang und Bestand durch die Einschaltung der zuständigen Behörden.

Die IKT-Drittdienstleister unterliegen neben der Regulierung ihrer vertraglichen Vereinbarungen auch der direkten Kontrolle der Behörden. Kapitel 5 ermöglicht weitreichenden Zugriff der Behörden auf betriebliche Abläufe, ähnlich dem der Finanzunternehmen selbst. Aufgrund des oft internationalen Aufbaus der Drittdienstleister sind die Befugnisse der Behörden sogar weiter, als bei

Finanzunternehmen selbst. Die Einhaltung der Anforderungen an Betriebsstandorte und Zugang zu außerhalb der Europäischen Union gelegenen Einrichtungen und Abläufen, in Zusammenarbeit mit den jeweiligen nationalen Behörden, sind erforderlich.

ee. Informationsaustausch

Zur Schaffung einer erhöhten Sensibilität für die digitale operationale Resilienz dient auch der gewünschte und geförderte Austausch von Informationen aus Kapitel 6 DORA. Damit soll vorhandenes Wissen den Marktteilnehmern zugänglich gemacht werden und diese von der Erfahrung anderer profitieren, was wiederum den Zielen von DORA zuträglich ist.

ff. Zwischenfazit

Zusammenfassend bedient DORA sich der Kontrolle durch Behörden, fordert aber auch Eigenverantwortung der Finanzunternehmen durch internes und externes Handeln. Tests dienen der Kontrolle und der Selbstüberprüfung. Bußgelder sind schmerzhafte Sanktionsmechanismen, die von den Behörden eingesetzt werden können. In bestimmten Fällen wird öffentlicher Druck erzeugt, welcher gegenüber Konkurrenten, Dienstleistern und Verbrauchern besteht und ein Handeln der Finanzunternehmen erzwingen soll.

II. Folgegesetzgebung

1. Begleitrichtlinie 2022/2556

Mit der Einführung von DORA wurden auch umfangreiche Änderungen bereits bestehender Richtlinien der Europäische Union erforderlich. Das Zusammenspiel der Normen, aber auch die Systematik des Überwachungsrahmens um IKT-Bereich werden durch DORA verändert und bedürfen für die Umsetzung einer Anpassung. Dies sind besonders Verweise zwischen den einzelnen Richtlinien. Definitionen und Geltungsbereiche beruhen oft auf Gruppen von Finanzunternehmen und anderen Akteuren, die in DORA definiert werden. Damit sind neue Verweise erforderlich, was mit der Richtlinie (EU) 2022/2556 zum 17.01.2025 umgesetzt wurde.

Betroffen sind die Richtlinien 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 und (EU) 2016/234. Sie behandeln alle Akteure am Finanzmarkt, deren Regulierung mit DORA in Berührung kommen kann.

2. Nationale Umsetzungen

DORA als Verordnung der Europäischen Union ist gemäß Artikel 288 AEUV grundsätzlich unmittelbar anwendbar und bedarf keiner Umsetzung durch die Mitgliedsstaaten. Trotzdem sind im Fall von DORA umfassende gesetzgeberische Entscheidungen zu treffen, welche ein Tätigwerden eines jeden Mitgliedsstaates erfordern.

a. Österreich

In Österreich wurde am 03.07.2024 das DORA-Vollzugsgesetz beschlossen, welches mit DORA zusammen am 17.01.2025 in Kraft getreten ist. Im Zuge dessen wurden auch Anpassungen am Bankwesengesetz, am Börsengesetz, dem Finanzmarktaufsichtsgesetz sowie dem Versicherungsaufsichtsgesetz und dem Wertpapieraufsichtsgesetz vorgenommen. Ebenfalls am Alternative Investmentfonds Manager-Gesetz, am Investmentfondsgesetz, am Pensionskassengesetz und am Zahlungsdienstegesetz. Die umfangreichen Änderungen dienen der Anpassung an die neuen Vorgaben von DORA und richten die nationalen Gesetze auf die europäische Verordnung aus.

Das DORA-Vollzugsgesetz normiert den nationalen Anwendungsbereich von DORA in Österreich. Alle Punkte, in denen DORA den Mitgliedsstaaten einen Beurteilungsspielraum lässt, sind darin festgesetzt. Außerdem werden nationale Zuständigkeiten geregelt.

Die Finanzmarktaufsicht wird gemäß § 2 DORA-VG als zuständige Behörde festgelegt. Damit erweitert sich ihr Aufgabenbereich umfangreich. § 5 DORA-VG reguliert die Zusammenarbeit der FMA mit der Österreichischen Nationalbank, welche ebenfalls hoheitliche Aufgaben im Finanzmarkt wahrnimmt, aber keine Kollisionen mit der FMA hervorrufen soll. Der Anwendungsbereich von DORA wird in § 3 DORA-VG erweitert auf alle Kreditinstitute gemäß § 1 Absatz 1 Bankwesengesetz, was umfassender ist, als der von DORA verwendete Begriff der Verordnung (EU) 575/2013. Die

Vereinheitlichung der Regulierung ist in Österreich damit etwas umfassender, als das von DORA vorgegebene Mindestmaß. Gemeinnützige Bauvereine sind hingegen gemäß § 3 Absatz 2 DORA-VG vom Anwendungsbereich ausgenommen, obwohl sie unter die Definition des § 1 Absatz 1 Bankenwesen fallen.[43] Damit hat Österreich von der Regelung des Artikel 2 Absatz 4 DORA Gebrauch gemacht.

Alle nationalen Ausprägungen haben sich an Artikel 4 DORA, dem Verhältnismäßigkeitsgrundsatz zu orientieren. Für eine Überschreitung dieses Rahmens durch das DORA-VG sind in der aktuellen Fassung keine Anzeichen zu finden.

b. Deutschland

Die Umsetzung von DORA in Deutschland erfolgte mit dem Beschluss des Gesetzes über die Digitalisierung des Finanzmarktes (Finanzmarktdigitalisierungsgesetz - FinmadiG) am 27.12.2024. Damit wurden nationale Gesetze sehr umfassend an DORA angepasst. Wo eine zuständige Behörde zu benennen ist, wurde die Bundesanstalt für Finanzdienstleistungsaufsicht benannt. Diese ist damit für sämtliche Geschäftsfelder, die DORA reguliert, die zuständige nationale Behörde. Ihre Kompetenzen wurden in den geänderten Gesetzen entsprechend den bereits existierenden Regulatorien für einzelne Geschäftsfelder auf dem Finanzmarkt ergänzt. Es handelt sich darüber hinaus vorrangig um redaktionelle Anpassungen der nationalen Gesetzeslage.

Auch die Zusammenarbeit mit der Deutschen Bundesbank durch die BaFin als zuständige nationale Behörde wird geregelt.[44] Die Deutsche Bundesbank übernimmt dabei die operativen Aufgaben der Artikel 26, 27 DORA in Zusammenarbeit mit der BaFin, welche als zuständige Behörde am Verfahren teilnimmt.

Das FinmadiG nennt Ausnahmeregelungen nicht von Artikel 2 DORA umfasster Kreditinstitute, die als CRR-Kreditinstitute im Kreditwesengesetz zu betrachten sind und damit von einzelnen Regelungen von DORA ausgenommen sind. Ebenfalls im Kreditwesengesetz werden Ordnungswidrigkeiten, welche Verstöße gegen DORA darstellen, definiert (Artikel 3 Ziffer 15 FinmadiG). Die Definition der

[43] *Gollmann,* in Hysek Praxishandbuch DORA, 2.7.2. Seite 37.
[44] Beispiel: Artikel 2 Ziffer 1 FinmadiG für das Kryptomärkteaufsichtsgesetz.

Ordnungswidrigkeiten erfolgt im Zuge des FinmadiG auch für die weiteren angepassten nationalen Gesetze.

Versicherungs-Holdinggesellschaften werden explizit dem vereinfachten IKT-Risikomanagementrahmen des Artikel 16 DORA unterworfen (Artikel 11 Ziffer 4 FinmadiG).

III. DORA in der Praxis

DORA richtet vielseitige neue Anforderungen an die Marktteilnehmer des Finanzsektors. Die unterschiedlichen Ansätze zur Erreichung der von der Europäischen Kommission bezweckten Ziele fordern in vielen Unternehmen umfangreiche Anpassungen.[45] Ausgewählte Herausforderungen für die Praxis, die durch DORA entstehen, sollen hier dargestellt werden.

1. Der IKT-Dienstleistungsbegriff

Viele digitale Dienstleistungen werden in der Finanzbranche technisch nicht von den Finanzunternehmen selbst operiert, sondern an spezialisierte Unternehmen ausgegliedert. Nicht selten stammen diese aus den Vereinigten Staaten von Amerika, aber auch europäische Unternehmen sind umfangreich vertreten. Diese unterliegen durch DORA einer neuen Stufe der Regulierung. Von der Qualifikation als IKT-Dienstleistung hängen der abzuschließende Vertrag und sein Inhalt gemäß Artikel 30 DORA ab.

a. Reichweite des Begriffs der IKT-Dienstleistungen

In Artikel 3 Nr. 21 DORA wird die IKT-Dienstleistung als dauerhaft bereitgestellter digitaler Dienst und Datendienst legaldefiniert, welcher technischer Unterstützung bedarf und regelmäßige Software- oder Firmwareaktualisierungen erfährt. Eine weite Auslegung des Begriffs dient der Schaffung eines hohen Maßes an digitaler operationaler Resilienz, was dem Hauptziel von DORA entspricht.[46] Es sind in der weiten Auslegung sowohl interne, als auch externe Prozesse als IKT-Dienstleistung

[45] *Dittrich/Heinelt*, Der Europäische DORA - neue Sicherheitsvorgaben für den Finanzsektor, RDi 2023, 164 Rn. 44.
[46] *Hornung/Schallbruch* in Bomhard/Siglmüller IT-Sicherheitsrecht § 29 Rn. 16.

erfasst.[47] Damit fallen zahlreiche Dienstleistungen unter den Begriff. Noch ausweitender ist die Ansicht, dass im Zweifel immer von einer IKT-Dienstleistung auszugehen ist. Damit soll der Schutz durch DORA maximale Wirkung entfalten können und die strengen vertraglichen Vorgaben immer zur Anwendung kommen.[48] Diese Ansicht stützt sich auf einen Umkehrschluss aus Erwägungsgrund 38 DORA. Sie verkennt dabei aber, dass dieser sich nur auf Kommunikationsdienste bezieht und nicht zwingend auf den Überbegriff digitaler Dienste auszuweiten ist. Die Ausweitung wird abgelehnt, um eine Unterscheidung zwischen digitalen Dienstleistungen und Dienstleistungen im Bereich des Datenschutzes und des allgemeinen Drittparteienrisikos durch andere Dienstleistungen trennscharf zu ermöglichen und den Umfang des Begriffes nicht ausufern zu lassen.[49]

Digitale Dienste als abgrenzender Begriff ist im Europarecht kein neuer Wortlaut, sodass auf bereits bekannte Auslegungen zurückgegriffen werden kann. In Artikel 1 Absatz 1 lit b RL (EU) 2015/1535 wird eine elektronisch erbrachte Dienstleistung einschränkender legaldefiniert, als in DORA. So sind dort Geräte für die elektronische Verarbeitung erforderlich, die Speicherung von Daten und eine vollständig elektronische Versendung, Weiterleitung und der Empfang. Diese konkretisierte Definition wird in weiteren Richtlinien aufgenommen, sodass von einem vom Gesetzgeber gewollten und fortgesetzten Verständnis ausgegangen werden darf.[50] Der Begriff der IKT-Dienstleistung als digitale Dienstleistung darf somit nicht zu extensiv ausgelegt werden, sondern bedarf eines tatsächlichen technischen Digitalbezugs. Es ist eine umfassende Prägung des Vertrags durch die digitale Dienstleistung mit dem Dienstleister zu erwarten, die der Hauptleistungspflicht entspricht.[51]

Strittig ist, ob auch bereits regulierte IKT-Dienstleister unter die strengen Anforderungen der Artikel 28 ff DORA fallen. Dies sind beispielsweise Ratingagenturen, die bereits unter der Kontrolle der Finanzbehörden stehen. Diesen

[47] Erwägungsgrund 27 DORA.
[48] *Merwald*, Die Regelungen des DORA betreffend Auslagerungsvereinbarungen, RDi 2024, 590 (592).
[49] *Lauck*, Der IKT-Dienstleistungsbegriff in der DORA, BKR 2025, 124, 125.
[50] Siehe Artikel 2 Nr. 5 VO (EU) 2019/881 und Artikel 6 Nr. 23 RL (EU) 2022/2555.
[51] *Bernau/Lutterbach*, Digital Operational Resilience Act (DORA) - Paradigmenwechsel in der IT-Aufsicht, BKR 2023, 506, 507 f.

könnte aufgrund dessen ein erhöhtes Vertrauen zukommen, sodass die erweiterten Anforderungen an den Vertrag als IKT-Dienstleister entbehrlich sein könnten.[52] Während manche nationalen Aufsichtsbehörden dazu explizit keine Festlegung treffen[53], nimmt die EBA als übergeordnete Behörde bereits einzelne Unternehmen, wie die erwähnten Ratingagenturen, von der Auslagerung und damit zusammenhängenden Regulatorien aus.[54] Dies ist jedoch nicht auf DORA zu übertragen, da IKT-Drittdienstleistungen wie oben festgestellt keine Auslagerung voraussetzen, sondern auch rein interne Dienstleistungen digitaler Art darstellen können.

Eine Einschränkung der IKT-Dienstleistung hat also nicht durch die Art des Dienstleisters, sondern durch die Art der konkreten Dienstleistung und ihrer Gewichtung im Vertrag stattzufinden. Dazu kommt, dass Artikel 3 Nr. 21 DORA eine dauerhafte Bereitstellung des digitalen Produktes erfordert. Damit sind einmalig erbrachte Dienstleistungen gerade nicht umfasst, was ebenfalls limitierend auf den Begriff der IKT-Dienstleistung und damit die vertraglichen Voraussetzungen für IKT-Drittdienstleister wirkt.

b. Probleme im praktischen Ablauf

Ein Finanzunternehmen schließt diverse Verträge über digitale Produkte ab, um seinem Geschäftsbetrieb nachkommen zu können.

Jedes Unternehmen ist auf die Überlassung von Software angewiesen, um digitale Systeme betreiben zu können. Der bloße Einmalerwerb ist dabei noch keine Dienstleistung von Dauer.[55] Mietlizenzen hingegen sind aufgrund ihrer Rechtsgestalt als Dauerschuldverhältnis als fortlaufende IKT-Dienstleistung zu qualifizieren. Da Software regelmäßig sicherheitsrelevante Updates benötigt, werden von

[52] *Lauck*, Der IKT-Dienstleistungsbegriff in der DORA, BKR 2025, 124, 126.
[53] Beispiel: Central Bank of Ireland, die auch als irische Bankenaufsicht auftritt https://www.centralbank.ie/regulation/digital-operational-resilience-act-dora/dora---frequently-asked-questions (zuletzt abgerufen am 17.08.2025).
[54] EBA/GL/2019/02 Abschnitt 3 Rn. 28.
[55] *FMA*, DORA-Webinar 5.11.2024 – Hinweise zu während des Webinars erhaltenen Fragen, Rn. 17 https://www.fma.gv.at/querschnittsthemen/dora/ (zuletzt abgerufen am 17.08.2025).

Finanzunternehmen verwendete digitale Programme meist unter den Begriff der IKT-Dienstleistung fallen.[56]

Viel Relevanz kommt bei den IKT-Dienstleistungen Cloud-Diensten wie dem Hosting oder dem Cloud-Computing zu. Diese sind im digitalen Zeitalter unentbehrlich, weil sie erhebliche operationelle Möglichkeiten bereitstellen, aber beim Finanzunternehmen keine eigene Infrastruktur erforderlich ist. Erwägungsgrund 20 DORA definiert diese als IKT-Dienstleistungen. Auch hier kann jedoch wieder auf die Hauptleistungspflicht eines Vertrags mit einem IKT-Dienstleister abgestellt werden, um eine ausufernde Anwendung der Artikel 28 ff DORA zu verhindern.[57]

Kommunikationsdienste, welche intern und extern von Finanzunternehmen, wie von jedem anderen Unternehmen auch, verwendet werden, fallen im Umkehrschluss zu Artikel 3 Nr. 21 DORA ebenfalls unter den Begriff der IKT-Dienstleistung, da nur analoge Telefondienste ausgenommen sind.[58]

c. Zwischenfazit

Artikel 30 DORA enthält umfassende Vorgaben für Verträge mit IKT-Drittdienstleistern. Aufgrund dieses gesteigerten Umfangs und dem damit verbundenen Aufwand ist die Einstufung als IKT-Dienstleistung für das Finanzunternehmen relevant. Für kritische IKT-Dienstleistungen gelten dazu die Bedingungen des Artikel 30 Absatz 3, welche nochmals weitreichender sind. Eine Begrenzung der dortigen Mindestanforderungen durch das Verhältnismäßigkeitsprinzip aus Artikel 4 DORA kann nicht vorgenommen werden, weil Artikel 4 Absatz 2 DORA eine ausdrückliche Anwendbarkeit des Prinzips im jeweiligen Artikel des Kapitel 5 Abschnitt 1 DORA voraussetzt, diese aber nicht vorliegt.[59] Die Begrenzung hat damit nur am Punkt der IKT-Dienstleistung zu erfolgen. Jede darunterfallende Dienstleistung, die an Dritte ausgelagert wird, hat sich an die Vorgaben des Artikel 30 DORA zu halten. Eine Begrenzung durch eine nicht allzu

[56] *FMA*, DORA-Webinar 5.11.2024 – Hinweise zu während des Webinars erhaltenen Fragen, Rn. 9 https://www.fma.gv.at/querschnittsthemen/dora/ (zuletzt abgerufen am 17.08.2025).
[57] *Lauck,* Der IKT-Dienstleistungsbegriff in der DORA, BKR 2025, 124, 126.
[58] *Lauck,* Der IKT-Dienstleistungsbegriff in der DORA, BKR 2025, 124, 127.
[59] *Lauck,* Der IKT-Dienstleistungsbegriff in der DORA, BKR 2025, 124, 129.

ausufernde Auslegung des Begriffes der IKLT-Dienstleistung ist im Interesse der Finanzunternehmen, damit diese vertraglich flexibler bleiben und nicht in jeder geschäftlichen Vereinbarung die hohen Mindeststandards umsetzen müssen. Andererseits dient es dem Ziel von DORA, ein hohes Maß an digitaler operationaler Resilienz zu schaffen, wenn auch IKT-Drittdienstleister möglichst oft und umfangreich in die Methodik von DORA eingebunden werden.

2. Vertragsanpassungen mit IKT-Drittdienstleistern

a. Bisherige Problematik

Wird eine Dienstleistung als IKT-Dienstleistung eingestuft und diese durch einen Drittdienstleister erbracht, sind bestehende Verträge von Finanzunternehmen mit diesen an die Vorgaben von DORA anzupassen. Sollten die Dienstleistungen als kritisch oder wichtig im Sinne von Artikel 30 Absatz 3 DORA eingestuft werden, muss der IKT-Drittdienstleister dem Finanzunternehmen und auch den federführenden Überwachungsbehörden umfassende Befugnisse gewähren. Diese können so umfangreich sein, dass sogar der Fortbestand der vertraglichen Beziehung fraglich sein könnte.

Ohne die Regelungen von DORA waren Finanzunternehmen in den Vertragsverhandlungen mit IKT-Drittdienstleistern im Nachteil, was Kontrollzugänge und andere einschneidende Berechtigungen angeht.[60] Mit der direkten Anwendbarkeit auf IKT-Drittdienstleister von DORA sind die umfassenden Kontrollrechte und weitgehenden Verpflichtungen des Dienstleisters dem Finanzunternehmen und den federführenden Überwachungsbehörden gegenüber gesetzlich normiert, sodass kein Nachteil mehr in Vertragsverhandlungen besteht. Die Vorgaben sind direkt anwendbar und finden somit unmittelbar ihren Weg in den Vertrag.

b. Einordnung als kritisch/wichtig

Der Umfang des Begriffs der IKT-Dienstleistung wurde bereits ausführlich behandelt, wenn auch noch keine abschließende Definition vorliegt. Bisher wurde nur eine

[60] *Lipke*, Vertragsanpassungen nach DORA, BKR 2025, 253, 254.

Eingrenzung des Begriffs vorgenommen. Nächster Schritt für die Einordnung, welche vertraglichen Voraussetzungen aus Artikel 30 DORA zu erfüllen sind, ist die Abgrenzung, ob es sich bei der IKT-Dienstleistung um eine kritische oder wichtige Dienstleistung handelt.

Bisherige nationale Regelungen zur Auslagerung kritischer IKT-Dienstleistungen, beispielsweise die deutschen § 25b KWG oder § 26 ZAG, werden neben DORA bestehen bleiben.[61] Der Anwendungsbereich wird durch DORA lediglich erweitert. Artikel 3 Nr. 22 DORA definiert kritische und wichtige Funktionen als solche, die bei einer Fehlfunktion einen Ausfall der finanziellen Leistungsfähigkeit des Finanzunternehmens herbeiführen können, die Solidität oder Geschäftsfortführung und Dienstleistungen erheblich beeinträchtigen würden oder eine fortdauernde Einhaltung von Zulassungsvoraussetzungen für Finanzunternehmen oder andere regulatorische Vorgaben verhindern würde. Nähere Ausführungen zu „kritisch“ und „wichtig“ enthält DORA nicht. Eine Auslegung entsprechend der konkreten Branche des Finanzunternehmens wird damit wahrscheinlich.[62] DORA beinhaltet ein sehr weit gefasstes Verständnis zu Finanzunternehmen, die unterschiedliche Geschäftsfelder bedienen. Aufgrund dessen wird es eine unterschiedliche Gewichtung von IKT-Dienstleistungen als kritisch oder wichtig geben. Im Bereich des Versicherungswesens hat sich eine Eingrenzung etabliert, die auf die Geschäftstätigkeit Rücksicht nimmt: „Eine kritische Funktion ist Teil des Wertschöpfungskerns des Versicherungsunternehmens, deren Unterbrechung oder Störung in kurzer Zeit zu einer Beeinträchtigung der Ende-zu-Ende-Kundenerfahrung, der regulatorischen Pflichten einschließlich der Reputation oder der finanziellen Solidität führt. Eine wichtige Funktion ist hilfsweise oder unterstützend zur Erbringung der wesentlichen Versicherungstätigkeit notwendig, gehört jedoch nicht zur primären Wertschöpfung. Eine Unterbrechung oder Störung kann für einen

[61] *Bernau/Lutterbach*, Digital Operational Resilience Act (DORA) - Paradigmenwechsel in der IT-Aufsicht, BKR 2023, 506, 508.

[62] Final report on Draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554, JC 2023, 84, S. 21
https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_84_-_Final_report_on_draft_RTS_to_specify_the_policy_on_ICT_services_supporting_critical_or_important_functions.pdf (zuletzt abgerufen am 17.08.2025).

festzulegenden Zeitraum hingenommen werden, ohne schwerwiegende Auswirkung auf Kundenerfahrung, regulatorische Pflichten oder finanzielle Solidität zu haben."[63] Damit wird dem Umstand, dass Versicherungsschutz für den Kunden auch gewährt werden kann, wenn eine IKT-Dienstleistung kurzzeitig ausfällt, Rechnung getragen. Eine Übernahme dieser Definition in andere Branchen erscheint sinnvoll, ist jedoch nicht zwingend vorgegeben.

c. Kündigung von IKT-Drittdienstleistern

Artikel 30 Absatz 2 lit h iVm Artikel 28 Absatz 7 DORA treffen umfangreiche Vorgaben hinsichtlich einer Kündigung von Verträgen mit IKT-Drittdienstleistern. Diese ist dabei stets als ultima ratio zu verstehen. Bisherige vertragliche Kündigungsvereinbarungen haben besonders auf hohe Anfangsinvestitionen von IKT-Drittdienstleistern Rücksicht genommen, um diesen Planungssicherheit zu verschaffen.[64] Oft wurde bei Verstößen gegen die Vertragsvereinbarungen seitens des Dienstleisters auf Vertragsstrafen und Schadensersatz zurückgegriffen, statt eine Beendigung des Vertrags herbeizuführen. Der Dienstleister selbst konnte hauptsächlich bei Nichtzahlung durch das Finanzunternehmen kündigen.[65]

DORA gibt klare Kündigungsgründe vor, die zwingend Bestandteil des Vertrags werden müssen, sollte es sich um eine IKT-Dienstleistung für das Finanzunternehmen handeln. Verstöße gegen Gesetze, Vorschriften oder Vertragsbedingungen, Erkenntnisse aus der Überwachung des IKT-Drittparteienrisikos, die als Beeinträchtigung wahrgenommen werden können und auch nachweisliche Schwächen des Dienstleisters im IKT-Risikomanagement, sowie Einschränkungen in der Beaufsichtigung des Finanzunternehmens durch die zuständige Behörde sind Kündigungsgründe und als solche im Vertrag zu erwähnen (Artikel 28 Absatz 7 DORA). Auch Subunternehmer der IKT-Drittdienstleisters sind relevant, wenn mit diesem vertragliche Vereinbarungen entgegen den Willen des Finanzunternehmens geschlossen werden.[66] DORA setzt im Vergleich zur alten Rechtslage damit das

[63] *Priller*, DORA in Versicherungsunternehmen, Abschnitt 4.1 Rn. 14 ff.
[64] *Lipke*, Vertragsanpassungen nach DORA, BKR 2025, 253, 255.
[65] *Nägele/Apel*, BeckOF IT- und Datenrecht 1.16 Anmerkungen Rn. 52.
[66] Artikel 7 Absatz 1 lit a-c des „Final report on Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services

gewünschte Ergebnis deutlich strenger und nachdrücklicher um, damit die digitale operationale Resilienz nachhaltig gestärkt wird.[67]

d. Vertragsanpassung

Weil viele IKT-Drittdienstleister bereits in den Diensten von Finanzunternehmen stehen, sind zur Umsetzung von DORA, welche ab dem 17.01.2025 zu erfolgen hat, Anpassungen in den Verträgen erforderlich.

Dafür sind die typischen Konstrukte von Verträgen, mit denen IKT-Dienstleistungen regelmäßig vereinbart werden, zu beachten. Meist wird ein Rahmenvertrag geschlossen, der die allgemeinen Parameter einer Zusammenarbeit zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister festlegt. Darauf bauen so genannte Leistungsscheine auf, die einzelne Aspekte der zu erbringenden Leistung definieren und die Dienstleistung spezifizieren mit den gewünschten Zielen.[68]

Spätestens in diesem Teil eines Vertrags sind die Vorgaben aus Artikel 30 DORA einzuarbeiten, um den gesetzlichen Anforderungen zu entsprechen. Als genauestes vertragliches Element kommen dann Servicevereinbarungen zum Einsatz, die geforderte Qualitätsstandards definieren und genaue Anforderungen des Finanzunternehmens an die Dienstleistung umfassen. Dies sind beispielsweise Verfügbarkeit, Antwort- und Reaktionszeit von Systemen oder die Implementierung in das bereits bestehende IT-System des Finanzunternehmens. Auch hier könnten Vorgaben aus DORA zu integrieren sein. Der Datenschutz wird dem oft als separater Anhang angefügt. Für Finanzunternehmen gelten dazu noch die Vorgaben nationaler Behörden für Auslagerungen, sollten solche existieren. Am Beispiel Deutschlands ist dafür AT 9 Tz. 7 der Mindestanforderungen an das Risikomanagement (MaRisk), regelmäßig herausgegeben von der Bundesanstalt für Finanzdienstleistungsaufsicht, zu nennen. Dies erfordert zusätzlich zu den Verträgen weitere Anhänge, die in die Vereinbarungen zu integrieren sind. Selbst mit diesen nationalen

supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554“, JC 2024, 53, 26 July 2024.
https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024_53_Final_report_DORA_RTS_on_subcontracting.pdf (zuletzt abgerufen am 17.08.2025).

[67] *Lipke*, Vertragsanpassungen nach DORA, BKR 2025, 253, 257.

[68] *Lipke*, Vertragsanpassungen nach DORA, BKR 2025, 253, 257.

Zusatzanforderungen werden die Vorgaben von DORA regelmäßig nicht zu erreichen sein, sondern Anpassungen sind erforderlich.[69]

Aufgrund der vielschichtigen Vereinbarungen ist es von hoher Bedeutung, sämtliche bestehenden Vertragswerke auf ihre Inhalte erneut zu prüfen und bei Bedarf eine Anpassung an die Vorgaben aus DORA vorzunehmen. Widersprüche zu DORA dürfen nicht mehr enthalten sein, ebenso dürfen die hohen Ansprüche an das IKT-Risikomanagement nicht unterlaufen werden, indem vermeintlich gleichwertige Klauseln umgedeutet werden. Vielmehr bleibt nur eine Anpassung jedes einzelnen Vertragsbestandteils an DORA übrig oder das Hinzufügen eines speziellen Anhangs, der DORA in den Vertrag aufnimmt.[70] Um den Aufwand der Vertragsanpassung zu minimieren, bietet sich der spezielle Anhang an, wenn er bei Widersprüchen zum restlichen Vertrag DORA den Vorrang gewährt.

e. Zwischenfazit

Es ist durch DORA somit erforderlich, die jeweiligen vertraglichen IKT-Dienstleistungen auf ihre Kritikalität hin zu prüfen und im Anschluss die Verträge an DORA anzupassen. Auch neue Vertragsabschlüsse sind dafür denkbar, stellen aber einen hohen Aufwand dar. Der personelle und strukturelle Aufwand für Unternehmen ist bei der Umsetzung von DORA damit erheblich gestiegen. Vorgaben für die Umsetzung in der Praxis haben die ESA der Europäischen Kommission bereits zukommen lassen und diese wurden in der delegierten Verordnung (EU) 2025/532 verabschiedet. Diese wirkt konkretisierend, trotzdem ist die Arbeit mit existierenden Dokumenten und der Anpassung dieser während ihrer Verwendung aufwändig, aber erforderlich. Bewährte Vorlagen an Vertragswerken müssen ebenfalls überarbeitet und auch ihre Rechtssicherheit auf DORA hin angepasst werden.

3. Haftungsfragen

In Unternehmen verändert DORA nicht nur die Anforderungen an das IKT-Risikomanagement und interne Compliance- und Governanceabläufe, sondern ergibt auch für Ausfälle in diesen Bereichen neue Haftungsfragen.

[69] *Lipke*, Vertragsanpassungen nach DORA, BKR 2025, 253, 257.
[70] *Lipke*, Vertragsanpassungen nach DORA, BKR 2025, 253, 257 f.

a. Haftung des Finanzunternehmens

Auslagerungen an Drittdienstleister können das Finanzunternehmen nicht von seinen Pflichten im IKT-Risikomanagement freistellen.[71] Das Finanzunternehmen selbst bleibt umfangreich verantwortlich für die Einhaltung der Vorgaben aus DORA und muss darauf bei seinen Drittdienstleistern hinwirken, sowie eine effektive Kontrolle vornehmen.

b. Haftung der Mitarbeiter

Die Verantwortlichkeit intern wird ebenfalls neu geregelt. Sobald ein Finanzunternehmen von einem IKT-bezogenen Vorfall betroffen ist und entsprechende Maßnahmen erforderlich werden, können Schadensersatzansprüche von Kunden und anderen Dienstleistern entstehen. Ebenfalls können Bußgelder im Zuge der Überprüfung der Finanzunternehmen anfallen. Auch nachträgliche Aufklärung und mögliche Rechtsstreitigkeiten können zusätzliche Kosten bedeuten. Im Bereich der Cybersicherheit, unter die IKT-bezogene Vorfälle regelmäßig fallen werden, ist eine Mitarbeiterhaftung aufgrund der begrenzten Haftung für betrieblich veranlasste Tätigkeiten selten gegeben.[72] Weiter stellen die potenziellen Schäden für einzelne Mitarbeiter eine nicht zu bewältigende finanzielle Belastung dar.

c. Direkte Haftung der Geschäftsführung

DORA benennt eindeutig die Verantwortlichkeit des Leitungsorgans für einzelne Abläufe. Artikel 5 Absatz 2 DORA benennt die Verantwortlichkeit der Leitungsorgane für das IKT-Risikomanagement, auch gegenüber IKT-Drittdienstleistern, Absatz 3, und der zugehörigen Dokumentation. Auch könne gemäß Artikel 50 Absatz 5 DORA Mitglieder der Leitungsorgane für verwaltungsrechtliche Sanktionen verantwortlich gemacht werden, wenn nationales Recht dies bestimmt. In Verbindung mit der eindeutigen Verpflichtung eines verantwortlichen Mitglieds des Leitungsorganes kann eine Haftung der Geschäftsführung gegenüber dem Unternehmen begründet werden.[73] Allgemein obliegt der Geschäftsführung die Umsetzung der rechtlichen

[71] Beispiel: Artikel 19 Absatz 5 DORA.
[72] *Schmidt-Versteyl,* Cyber Risks – neuer Brennpunkt Managerhaftung?, NJW 2019, 1637, 1638.
[73] Beispiel aus Deutschland: BGH, Urteil vom 18. 9. 2018 - II ZR 152/17, NJW 2019, 596.

Anforderungen an das Unternehmen, die so genannte Legalitätsflicht. Diese sind in den allgemeinen gesellschaftsrechtlichen Verantwortlichkeitsnormen, beispielsweise in Deutschland in § 43 Absatz 2 GmbHG oder § 93 Absatz 2 Satz 1 AktG, verankert.[74] DORA stellt diesen gegenüber eine spezialgesetzliche Vorgabe dar. Die Verantwortlichkeit des Leitungsorgans und damit der Geschäftsführung wird ausdrücklich zugewiesen und ist bei Haftungsfragen nicht abzustreiten, sollte der IKT-bezogene Vorfall aus dem zu verantwortenden Geschäftsbereich stammen.

Für Geschäftsführungen bedeutet dies, dass die Umsetzung der Vorgaben von DORA auch im persönlichen Interesse regelmäßig zu kontrollieren ist. Dabei können externe spezialisierte Prüfer beauftragt werden. Diese können Berichte für die interne Kontrolle erstellen und dem Leitungsorgan damit Gewissheit über den Stand des IKT-Risikomanagements im Finanzunternehmen geben. Eine Übertragung der Verantwortlichkeit auf ein einzelnes Mitglied der Geschäftsführung, die regelmäßig aus mehreren Personen besteht, ist nicht möglich. Die Haftungsfreistellung der übrigen Mitglieder des Leitungsorgans scheitert an einer generellen Überwachungsfunktion dieser, auch gegenüber dem ausgewählt zuständigen Mitglied.[75] Fehlt es an der Überwachung oder der Nichteinleitung von Maßnahmen aufgrund der gewonnenen Erkenntnisse, liegt eine Pflichtverletzung vor. Die Delegierung von bestimmten Tätigkeiten im Rahmen des IKT-Risikomanagements ist damit noch zulässig, eine Übertragung der Verantwortung ist jedoch regelmäßig ausgeschlossen. Positionen innerhalb des Finanzunternehmens, die bisher mit der Kontrolle bestimmter Maßnahmen in diesem Feld betraut waren, werden damit entlastet.

d. Versicherung des Haftungsrisiko

Geschäftsführungen versichern regelmäßig das Risiko der eigenen Verantwortung dem Unternehmen gegenüber. Zu unterscheiden ist zwischen einer Versicherung des Unternehmens durch die Geschäftsführung und einer Versicherung der Geschäftsführung gegenüber dem Unternehmen.

[74] *Blum/Adelberg,* Zeitenwende bei der Cybersecurity-Compliance: Ausweg aus der Haftungsfalle für die Geschäftsleitung, CB 2024, 145, 145.
[75] *Conrad/Streitz,* in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht § 33 Rn. 75 f.

aa. Versicherung des Finanzunternehmens

Eine Versicherung für Finanzunternehmen gegen die Auswirkungen von IKT-bezogenen Vorfällen scheint eine sinnvolle Maßnahme zu sein. Die Optionen für die Versicherung gegen die Haftung aus Cyberrisiken, unter die das IKT-Risiko fallen kann, sind vielfältig.[76] Drittschäden für Kunden von Finanzunternehmen können ebenso abgedeckt werden, wie Eigenschäden durch Haftung gegenüber Dienstleistern und Bußgelder. Aufgrund der hohen Wahrscheinlichkeit eines Schadenseintritts und den nicht abzuschätzenden daraus resultierenden Schäden wird die Versicherung eine sehr hohe Prämie enthalten müssen.

bb. Versicherung der Geschäftsführung

Gerade bei einer so ausdrücklichen Verantwortlichkeit, wie DORA sie festschreibt, scheint die Versicherung der Geschäftsführung für ihre Handlungen dem Unternehmen gegenüber eine attraktive Option. Aufgrund des Umfangs und der Komplexität der Anforderungen aus DORA, ist die Gefahr von fehlerhaften Compliance-Lösungen in Finanzunternehmen hoch. Auch die Implementierung der Vorgaben in bereits bestehende Verträge und interne Prozesse kann an vielen Stellen zu unbeabsichtigten Versäumnissen führen, sodass das Risiko eines Haftungsfalles für die Geschäftsführung hoch ist. Entsprechende Produkte sind bereits marktverfügbar, eine konkrete Anpassung an DORA ist bei den abgeschlossenen Verträgen regelmäßig erforderlich. DORA stellt weitreichende Anforderungen, welche keinem großen Interpretationsspielraum ausgesetzt sind, sodass die Vorgaben mit hoher Wahrscheinlichkeit durch das Unvermögen der korrekten Umsetzung ausgelöst werden. Damit ist eine Haftung der Geschäftsführung sehr wahrscheinlich, was sich auf die Bewertung der jeweiligen Versicherung auswirkt.

e. Zwischenfazit

Durch die direkte Haftbarmachung des Leitungsorgans schafft DORA eine direkte Verantwortlichkeit der Führungsebene. Damit wird der hohe Stellenwert des Ziels, eine gesteigerte digitale operationale Resilienz zu erzeugen, betont. Auch wird der Umsetzung durch den direkten Druck eine sehr hohe Priorität eingeräumt, wovon

[76] *Grieger*, Haftung des AG-Vorstands bei Schäden durch Cyberangriffe, WM 2021, 8, 15.

insgesamt die Finanzbranche profitieren wird, aber auch hohen Druck und Handlungszwang bei den Finanzunternehmen bedeutet. Die Ausgestaltung von DORA zeigt ein entschlossenes Handeln der Europäischen Kommission, die mit ihrer Strategie die Europäische Union in der Digitalisierung voranbringen möchte.

C. Die Rolle von Aufsichtsbehörden

Die Durchsetzung von DORA wird von den zuständigen nationalen Behörden überprüft. Diese sind werden von den Finanzunternehmen aktiv eingeschaltet, sollte es zu IKT-bezogenen Vorfällen kommen, können aber auch selbstständig tätig werden.

I. Meldung von IKT-bezogenen Vorfällen

IKT-bezogene Vorfälle in Finanzunternehmen sind gemäß Artikel 19 DORA verpflichtend der zuständigen Behörde zu melden. Die Abläufe dafür sind vorgegeben und sollte von den Unternehmen vorab eindeutig festgelegt sein.

1. Interne Einstufung

Tritt ein IKT-Bezogener Vorfall in einem Finanzunternehmen auf, ist seine individuelle Klassifizierung entscheidend für das Prozedere der Meldung. Anhaltspunkte dafür gibt Artikel 18 DORA, welcher zusätzlich eine Konkretisierung dieser die ESA in einer Ausarbeitung der technischen Standards fordert. Diese wurden nach Inkrafttreten von DORA auch von der EBA veröffentlicht und dienen den Finanzunternehmen als konkrete Anhaltspunkte.[77] Eine Klassifizierung von IKT-bezogenen Vorfällen soll durch diese einfacher und genauer sein. Sind von diesem Vorfall kritische Systeme nicht betroffen, ist eine Klassifikation als schwerwiegend nicht erforderlich, sodass auch eine Meldung nicht zu erfolgen hat.

Sind kritische Systeme betroffen, ist anhand der Regulatory Technical Standards (RTS) zu entscheiden, wie umfangreich der Vorfall ist und ob die Schwelle zur Kritikalität

[77] Final report on Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554:
https://www.eba.europa.eu/sites/default/files/2024-01/4f2654f4-3152-48b6-af01-431215400f9f/JC%202023%2083%20-%20Final%20Report%20on%20draft%20RTS%20on%20classification%20of%20major%20incidents%22and%20significant%20cyber%20threats.pdf (zuletzt abgerufen am 17.08.2025).

überschritten wurde. Ein Vorfall, bei dem potenziell Daten des Finanzunternehmens unbefugt an Dritte gelangen könnten, ist dagegen stets als schwerwiegender Vorfall zu klassifizieren, sodass dort immer eine Meldung zu erfolgen hat. Bei einem solche Fall ist ein erfolgreiches Eindringen eines unbefugten Dritten bereits gegeben. Jedoch können Vorfälle auch bemerkt werden, bevor ein erfolgreiches Eindringen in die IKT-Systeme des Finanzunternehmen stattgefunden hat. Auch diese Vorfälle können als schwerwiegend zu klassifizieren sein, wenn bestimmte Parameter kumuliert vorliegen. Solche sind der Kreis der Betroffenen, Reputationsschäden, die Dauer des Vorfalls und seiner Folgen, die geografische Verbreitung und ökonomische Auswirkungen auf das Finanzunternehmen, aber auch den Markt selbst. Beim Vorliegen von zwei oder mehr dieser Kriterien, liegt ein schwerwiegender Vorfall vor, bei nur einem betroffenen Kriterium nicht.[78]

Das Kriterium des Kreises der Betroffenen wird von den ESA in den RTS on classification of incidents (Table 1) wie folgt definiert: Über 100.000 oder über 10% aller Kunden müssen den vom Vorfall betroffenen Dienst nutzen, oder 30% der Finanzpartner des Finanzunternehmen nutzen den betroffenen Dienst, oder 10% der täglichen Transaktionen finden über den Dienst statt oder 10% des Werts der täglichen Transaktionen finden mit dem betroffenen Dienst statt. Diesen starren Grenzwerten wird der Auffangtatbestand zugefügt, dass auch jede relevante Betroffenheit von Kunden oder Finanzpartnern zur Erfüllung des Kriteriums führt.

Zum Reputationsschaden führen die ESA aus, dass negative Auswirkungen auf den Ruf des Unternehmens aus unterschiedlichen Quellen stammen können. Dies kann negative mediale Berichterstattung sein, sich wiederholende Beschwerden in großer Menge, Verletzungen der regulatorischen Anforderungen, der zumindest wahrscheinliche Verlust von Kunden in relevanter Zahl, oder der Verlust von Partnern des Finanzunternehmens in einer Zahl, die den Geschäftsbetrieb beinträchtigen kann. Insgesamt ist die Sichtbarkeit der Auswirkungen des IKT-bezogenen Vorfalls für Außenstehende entscheidend.

[78] Table 1 RTS on classification of incidents, S. 8.

Die Dauer des IKT-bezogenen Vorfalls wird als Kriterium für die Eistufung als schwerwiegend berücksichtigt, wenn sie 24 Stunden am Stück überschreitet oder, bei einem vollständigen Ausfall von kritischen oder wichtigen Systemen, eine Dauer von zwei Stunden. Die Dauer von 24 Stunden läuft ab der Entdeckung des Vorfalls bis zur vollständigen Lösung des Problems. Bei nicht bekanntem Startzeitpunkt des Vorfalls ist dieser zu schätzen. Die Frist beim Ausfall von Systemen startet mit den ersten intern oder extern (Kunden oder andere Unternehmen) wahrnehmbaren Beeinträchtigungen und endet mit der Wiederherstellung des status quo.

Für die geografische Ausbreitung geben die RTS vor, dass mindestens zwei Mitgliedsstaaten betroffen sein müssen. Dies erstreckt sich auf Kunden in zwei Mitgliedsstaaten, aber auch andere Marktteilnehmer und Unternehmen, die mit dem Finanzunternehmen zusammenarbeiten.

Die ökonomischen Auswirkungen werden als Kriterium herangezogen, wenn die Verluste oder die zur Behebung des Vorfalls entstehenden Kosten des Finanzunternehmens in Summe die Marke von EUR 100.000 überschreiten. Diese inkludieren alle direkten Verluste durch Diebstahl, aber auch erhöhte Personalkosten, auch für externe Helfer, Vertragsstrafen, Regressansprüche von Betroffenen, Kosten für die externe Kommunikation und alle direkt mit dem Auftreten des IKT-bezogenen Vorfalls entstandenen Kosten.

Zusätzlich können wiederkehrende IKT-bezogene Vorfälle, auch wenn sie grundsätzlich nicht als schwerwiegend einzustufen wären, trotzdem als Kriterium gelten. Dafür muss innerhalb von sechs Monaten ein IKT-bezogener Vorfall mindestens zweimal auftreten und die gleiche Ursache aufweisen.

Eine Kombination von mindestens zwei dieser Kriterien führt zwingendermaßen zu einer Einstufung des IKT-bezogenen Vorfalls als schwerwiegend, unabhängig von einem tatsächlichen Zugriff auf die Systeme.

2. Meldevorgang

Wurde eine interne Einstufung als schwerwiegender IKT-bezogener Vorfall vorgenommen, ist eine Meldung an die zuständige Behörde erforderlich (Artikel 19 DORA). Der vollständige Meldeprozess kann an einen externen

Dienstleister ausgelagert werden, befreit das Finanzunternehmen jedoch wie in anderen Fällen auch nicht von der Verantwortlichkeit (Artikel 19 Absatz 5 DORA).

a. Erstmeldung

Umgehend nach Entdeckung des Vorfalls hat eine Erstmeldung zu erfolgen (Artikel 19 Absatz 1 Satz 4 DORA). Diese muss einem sachkundigen Dritten den konkreten Sachverhalt verständlich machen können und eine Einschätzung der Schwere des Vorfalls ermöglichen. Auch weitergehende Betroffenheit, etwa die Einbindung eines IKT-Drittdienstleisters, ist mit der Erstmeldung zu kommunizieren. Die zuständige Behörde kann darauf hin aus dem von ihr geführten Informationsregister über die IKT-Drittdienstleister erkennen, ob für andere Kunden des Dienstleisters eine Gefahr durch den Vorfall besteht. Die Stabilität des Marktes wird dadurch abgesichert.

Konkret soll die Erstmeldung umfangreich mitteilen, was passiert ist und welche Dienstleistungen des Finanzunternehmens betroffen sind. Daraus ergibt sich, welche Kunden oder andere Unternehmen betroffen sein könnten. Dazu kommt, ob der Vorfall bereits abgeschlossen ist oder noch andauert. Für letzteres ist eine Prognose abzugeben, wie lange der Vorfall voraussichtlich noch andauert. Auch muss bereits in der Erstmeldung geschätzt werden, ob es sich bei dem Auslöser um einen Defekt oder anderweitigen Fehler im Geschäftsablauf handelt, oder ob kriminelle Vorgänge verantwortlich sind. Ebenfalls ist eine Einschätzung über die Reichweite der Betroffenheit von Kunden und anderen Marktteilnehmern vorzunehmen, auch wenn die zuständige Behörde dies aufgrund der übermittelten Informationen selbst beurteilen wird.

Nach den RTS on major incident reporting[79] hat die Erstmeldung spätestens vier Stunden nach der Klassifizierung des Vorfalls als schwerwiegend zu erfolgen.

[79] Artikel 6 Seite 18: Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents
https://www.eba.europa.eu/sites/default/files/2024-07/6d341d14-0c54-44ff-a849-21561baee157/JC%202024-33%20-%20Final%20report%20on%20the%20draft%20RTS%20and%20ITS%20on%20incident%20reporting.ppd (zuletzt abgerufen am 17.08.2025).

Alternativ ist sie spätestens nach 24 Stunden ab Erkennung des IKT-bezogenen schwerwiegenden Vorfalls abzugeben.

b. Zwischenmeldung

In der Zwischenmeldung müssen detaillierte Informationen und Analysen zum Vorfall an die Behörde übermittelt werden. Die Behörde erstellt daraus ein noch weitreichenderes Lagebild und kann Risiken einschätzen. Auch die Unterstützung in der Bewältigung des Vorfalls baut auf den Stand aus den Zwischenmeldungen auf. Jede signifikante Änderung am Kenntnisstand zum Vorfall bedarf einer erneuten Zwischenmeldung. Die Behörde kann eine weitere Zwischenmeldung jederzeit verlangen, sollten die ihr bekannten Informationen nicht ausreichen. Insbesondere soll die Zwischenmeldung den aktuellen Status des Vorfalls klären, den Status des Geschäftsbetriebes des Finanzunternehmens und die Entwicklung der Auswirkungen des Vorfalls skizzieren, um Planungen für das weitere Vorgehen zu ermöglichen.

Die RTS on major incident reporting sehen eine Zwischenmeldung spätestens 72 Stunden nach der Qualifizierung des Vorfalls als schwerwiegend vor. Alternativ bei einer Normalisierung des Geschäftsbetriebs, wenn die akuten Auswirkungen bereits behoben sind.

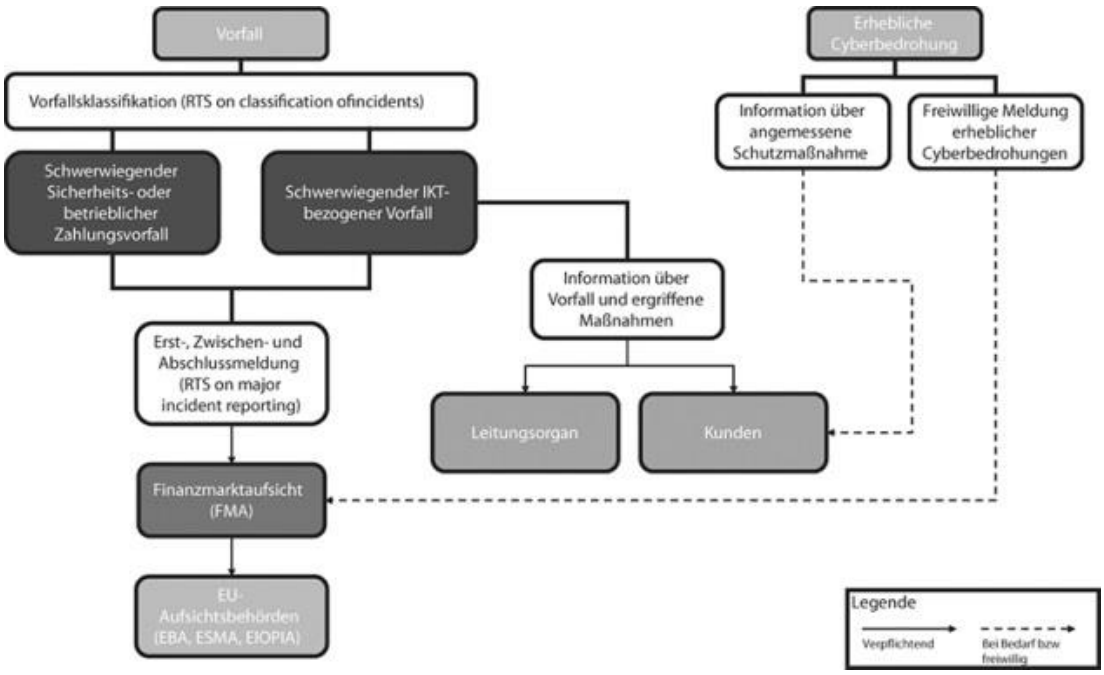
c. Abschlussmeldung

Die umfassendste Meldung an die zuständige Behörde stellt die Abschlussmeldung dar. In dieser sollte das Finanzunternehmen bereits die Ursache des IKT-bezogenen Vorfalls analysiert haben und umfangreich über die getroffenen Maßnahmen und deren Umsetzung und Auswirkung informieren. Auch sollen Kosten und Verluste, die durch den Vorfall entstanden sind, aufgelistet werden. Als Kosten nennen die RTS on major incident reporting Haftungen für Schäden durch Diebstahl, Ersatzkosten und Umsetzungskosten, Personalkosten, Vertragsstrafen, Schadensersatz, Verlust von Einnahmen, Kommunikationskosten und Beratungskosten, die im Zusammenhang entstanden sind.

Spätestens einen Monat nach der Klassifizierung des Vorfalls als schwerwiegend hat der Abschlussbericht bei der zuständigen Behörde einzugehen. Sollte der Vorfall bis

zu dieser Frist noch nicht behoben worden sein, hat der Abschlussbericht am Tag nach der Beendigung zu erfolgen.

Grundsätzlich kann eine Meldung in der ersten Stunde am Folgetag nach einem Wochenende oder Feiertag nachgeholt werden, um die Frist einzuhalten. Ausgenommen von dieser Regelung sind jedoch Vorfälle mit grenzüberschreitender Betroffenheit, als systemrelevant oder signifikant eingestufte Finanzunternehmen und Finanzmarktinfrastrukturen aufgrund des erhöhten Risikos weitreichender Folgen.



Grafik: Meldeprozess für die Meldung von schwerwiegenden IKT-bezogenen Vorfällen, Beispiel Österreich[80]

d. Strafmaßnahmen

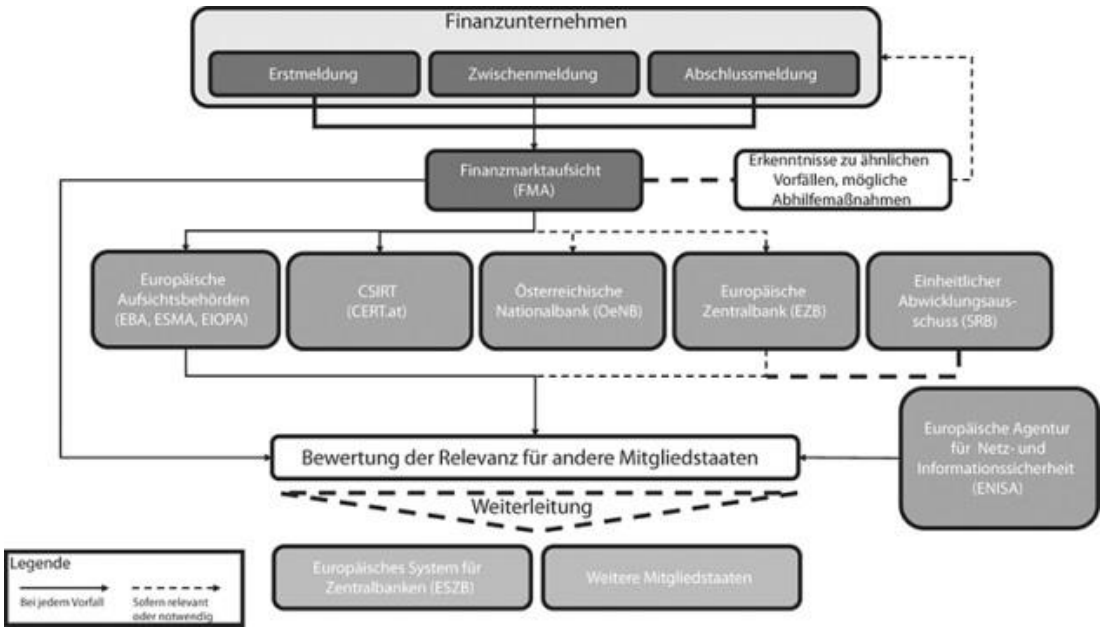
Verstöße gegen die Vorschriften von DORA und damit auch die Meldepflichten können nach dem nationalen Vollzugsgesetzen festgelegt werden. Das österreichische DORA-VG sieht für natürliche Personen Verwaltungsstrafen von bis zu EUR 150.000 vor (§ 7 DORA-VG). Bei juristischen Personen können diese bis zu EUR 500.000 anwachsen oder 1% des jährlichen Gesamtnettoumsatzes

[80] *Hefler*, in Hysek Praxishandbuch DORA, Kapitel 5.4 Seite 120.

ausmachen (§ 8 DORA-VG). Der jeweils höhere Betrag ist entscheidend. Dazu kommt die Veröffentlichung von Verhängten Strafen durch die zuständige Behörde, was öffentlichen Druck bedeutet und das Ansehen des betroffenen Finanzunternehmens in der öffentlichen Wahrnehmung und in der Finanzbranche schmälert.[81]

e. Innerbehördlicher Ablauf

In der zuständigen Behörde werden die übermittelten Meldungen auf ihre Vollständigkeit hin geprüft und die Plausibilität der Angaben gegebenenfalls hinterfragt. Es kann eine Aufforderung zur Nachreichung von Informationen ergehen. Im Anschluss werden die Informationen an die federführende Behörde der Europäischen Union übermittelt. Dies sind insbesondere die EBA, ESMA und die EIOPA. Je nach Vorfall kann auch das CSIRT informiert werden. In der nationalen Ausgestaltung des DORA-VG wird in Österreich auch die Zusammenarbeit mit der Österreichischen Nationalbank gefordert. Dazu kommt bei grenzüberschreitenden Vorfällen die EZB.



Grafik: Informationsfluss nach Meldung an die zuständige Behörde, Beispiel Österreich[82]

[81] *Schmidt*, Digital Operational Resilience Act (DORA) - Behördliche Eingriffs- und Sanktionierungsinstrumente Teil I, WM 2024, 2125, 2132.
[82] *Hefler,* in Hysek Praxishandbuch DORA, Kapitel 5.4.4 Seite 125.

II. Thread-Led Penetration Testing

Die digitale operationale Resilienz soll nach DORA durch regelmäßig stattfindende Thread-Led Penetration Tests (TLPT) überprüft werden und daraus Verbesserungsmaßnahmen abgeleitet werden. Die zuständige Behörde muss deren Durchführung sicherstellen.

1. Entstehung von TIBER

TLPT sind nicht erst mit DORA geschaffen worden, sondern wurden bereits vorher in der Europäischen Union durchgeführt. Diese TLPT beruhen auf dem etablierten TIBER-Standard (Threat Intelligence-Based Ethical Red Teaming). Dieses Modell wurde von der niederländischen Nationalbank maßgeblich entwickelt und erste Tests wurden bereits im Jahr 2016 durchgeführt.[83] Die Durchführung nach dem TIBER-Standard war bislang freiwillig.

Das Besondere an TIBER ist, dass die Sicherheitssysteme des Finanzunternehmens keine Kenntnis von einem bevorstehenden Angriff haben, der als IKT-bezogener Vorfall einzustufen sein wird. Der Angriff wird ausgeführt von einem so genannten Red-Team, welches einem kriminellen Täter gleich vorgeht und die Sicherheitssysteme des Finanzunternehmens realistisch angreift. Durch den vollständigen und realistischen Angriff werden Schwachstellen besonders umfangreich und deutlich offengelegt, sodass Abhilfemaßnahmen besonders zielführend durchgeführt werden können. Ziel ist es nicht, den Angriff zu überstehen, sondern Erkenntnisse zur Verbesserung zu gewinnen.[84]

Damit innerhalb der Europäischen Union einheitliche Standards gelten, hat das Europäische System der Zentralbanken (ESZB) als Zusammenschluss aller Nationalbanken auf Basis des niederländischen Entwurfes das TIBER-EU Rahmenwerk entwickelt. Dieses bedarf noch einer nationalen Umsetzung, um den durchführenden Unternehmen Rechtssicherheit bieten zu können. Die Europäische Union gibt dafür in TIBER-EU die Grundsätze vor, deren Umsetzung aber an nationale Besonderheiten im Rechtssystem oder in der Marktstruktur angepasst werden soll.

[83] *Boss/Herrmann/Richter/Wellischowitsch*, in Hysek Praxishandbuch DORA, Kapitel 6.1.1 Seite 127.
[84] *Boss/Herrmann/Richter/Wellischowitsch*, in Hysek Praxishandbuch DORA, Kapitel 6.1.1 Seite 128.

Angriffe auf IKT-Systeme erfolgen regelmäßig nicht nur national, sondern aufgrund des gemeinsamen Wirtschaftsraumes innerhalb der Europäischen Union auch grenzüberschreitend. Dazu kommt, dass aufgrund der stark verbundenen Marktstruktur ein erfolgreicher Angriff auf ein Finanzunternehmen leicht Auswirkungen auf andere Marktteilnehmer und andere Länder haben kann. Betroffene können ebenfalls in unterschiedlichen Mitgliedsstaaten ansässig sein. Damit eine vertrauensvolle Zusammenarbeit der nationalen zuständigen Behörden und Nationalbanken stattfindet, wurde das TIBER-EU Knowledge Center (TKC) gegründet.[85] Nationale Vertreter tauschen in diesem Forum aktuelle Erkenntnisse über Cyberbedrohungen aus. Die nationalen Umsetzungen von TIBER-EU werden vom TKC begleitet, sodass die Anforderungen erfüllt werden und Neuerungen konsequent nachgehalten werden.

2. Beispiel TIBER-AT

Die genauen Inhalte von TIBER sollen am Beispiel TIBER-AT[86] genauer dargestellt werden. Dies ermöglicht einen Eindruck vom Ablauf von TLPT, wie er von der ESZB vorgesehen ist. TIBER-AT orientiert sich größtenteils am deutschen TIBER-DE[87], beinhaltet aber auch landesspezifische Regelungen, die sich an den nationalen Strukturen orientieren.

a. Akteure nach TIBER-AT

Das Finanzunternehmen als Handlungsort eines Tests nach TIBER-AT ist verantwortlich für die regelmäßige Durchführung des Tests. Die Kosten sind vom Finanzunternehmen zu tragen. Ergebnisse des Tests sind vom Finanzunternehmen auszuwerten und entsprechende Schlüsse daraus zu ziehen. Diese dienen der Mängelbehebung für durch die Tests aufgedeckte Schwachstellen und verbessern somit die digitale operationale Resilienz des Unternehmens.

---

[85] Europäische Zentralbank, TIBER-EU FRAMEWORK, Kapitel 2.2.2 Seite 9 f https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework_2025~b32eff9a10.en.pdf?0309030e5e167a47ca4748370a949064 (zuletzt abgerufen am 17.08.2025).

[86] Österreichische Nationalbank, TIBER-AT Implementation Guide November 2023 https://www.oenb.at/en/financial-market/tiber-at.html (zuletzt abgerufen am 17.08.2025).

[87] Deutsche Bundesbank, Implementierung von TIBER-DE Dezember 2022 https://www.bundesbank.de/resource/blob/842288/d8d656efbb4b961ff3da32bc1092f9a3/472B63F073F071307366337C94F8C870/tiber-implementierung-data.pdf (zuletzt abgerufen am 17.08.2025).

aa. Control Team

Das so genannte Control Team übernimmt die Steuerung des gesamten Testvorgangs im Finanzunternehmen. Alle weiteren Beteiligten werden von diesem angeleitet und koordiniert. Die Mitglieder des Control Teams werden gewählt und setzen sich regelmäßig zusammen aus Vertretern der IT-Sicherheit, einem Vertreter des Vorstands, zuständige Projektmanager und, falls vorhanden, Vertreter von IKT-Drittdienstleistern, die auch betroffen wären. Innerhalb dieses Teams leitet das Control team lead, welches direkten Zugang zur höchsten Entscheidungsebene des Finanzunternehmens hat und damit auch die Reichweite der Abläufe bestimmen darf, das Vorgehen. Die EZB hat die Aufgaben in den TIBER-EU Control Team Guidance[88] näher definiert, um den Finanzunternehmen die Abläufe näher zu bringen und eine einheitliche Umsetzung zu fördern. Das Control Team ist auch verantwortlich für die korrekte Nachbereitung des Tests. Als leitendes Organ wird vom Control Team eine strikte Geheimhaltung erwartet, um die Effektivität des Tests sicherzustellen. Die Reichweite des Tests und des Vorgehens der anderen Beteiligten liegt in der Einschätzung des Control Teams, welches ein möglichst realistisches Szenario erreichen möchte, aber Kollateralschäden und ungewünschte Folgen vermeiden muss.

bb. Blue Team

Im Finanzunternehmen besteht neben dem Control Team auch das Blue Team. Dieses umfasst laut TIBER-AT Vertreter aller Mitarbeiter des Finanzunternehmens, die nicht Teil des Control Teams sind, die also nicht vom Stattfinden eines TIBER-AT-Tests wissen. Sie repräsentieren die normale Belegschaft und sind Teil des Ziels eines simulierten Angriffs sowie in ihrer alltäglichen Tätigkeit die Verteidiger. Aufgrund der vielfältigen Möglichkeiten, IKT-bezogene Vorfälle zu provozieren, sind unterschiedlichste Teile des Finanzunternehmens im Blue Team vertreten. Die

[88] EZB, TIBER-EU Control Team Guidance Januar 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_control_team_2025.en.pdf?5486c57100c723e3caa03d4497fa7136 (zuletzt abgerufen am 17.08.2025).

TIBER-EU Blue Team Test Report Guidance[89] bieten Anhaltspunkte für die Wertungsmaßstäbe des Blue Teams in seinem Bericht im Anschluss an den Angriff.

cc. Threat Intelligence Provider

Der Threat Intelligence Provider kundschaftet das Finanzunternehmen vor der Durchführung des TLPT aus. Es werden Schwachstellen identifiziert, über die der Testangriff erfolgen soll.[90] Als externer Dienstleister im Auftrag des Finanzunternehmens übergibt der Threat Intelligence Provider seine Ergebnisse an dieses, bleibt aber oft weiter in der konkreten Durchführung des TLPT involviert. Auch wird er regelmäßig die Ergebnisse beratend mit auswerten. Bereits die Informationen, wie die Schwachstellen gefunden wurden, ist für die Reaktion auf das Testen der Resilienz relevant. In der Durchführung des eigentlichen Tests ist der Dienstleister jedoch nicht eingebunden. Das Auskundschaften wird strikt vom Angriff getrennt, um den Angreifern eine freie Auswahl der Methoden zu überlassen. Eine Vielzahl von Szenarien soll dadurch ermöglicht werden.[91] Der Threat Intelligence Provider steht somit weder auf Seiten des Finanzunternehmens, noch auf Seiten der Angreifer. Er dient primär als Informationsbeschaffer und kommt nur in der Vorbereitung und Nachbereitung des TLPT zum Einsatz.

dd. Red Team Tester

Die Red Team Tester sind die Angreifer im TLPT. Sie sind interne oder, spätestens bei jedem Dritten Test, externe Hacker, die nach ethischen Grundsätzen im Auftrag des Control Teams und mit Informationen des Threat Intelligence Provider das Finanzunternehmen attackieren. Der Anführer der Red Team Tester ist der einzige Kontakt zu den anderen Gremien des TIBER-Angriffs. Er verantwortet sich gegenüber diesen und stellt die Kompetenz der weiteren Red Team Tester sicher. Diese müssen fachliche Erfahrung vorweisen können. Aufgrund des realen Angriffs müssen sie aber auch Integrität mitbringen, was die gewonnenen Erkenntnisse angeht. Der

[89] EZB, TIBER-EU Blue Team Test Report Guidance, Januar 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_blue_team_test_report_2025.en.pdf (zuletzt abgerufen am 17.08.2025).
[90] EZB, TIBER-EU Targeted Threat Intelligence Report Guidance, Januar 2025 https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_targeted_threat_intelligence_report_guidancg_2025.en.pdf?0ab97721477f47729fca39ce45d1ab15 (zuletzt abgerufen am 17.08.2025).
[91] *Boss/Herrmann/Richter/Wellischowitsch*, in Hysek Praxishandbuch DORA, Kapitel 6.2.2 Seite 131.

umfassende Test der IKT-Sicherheitssysteme des Finanzunternehmens kann virtuell, aber auch physisch erfolgen. Es sollen realistische Angriffsszenarien genutzt werden, wie sie auch von Kriminellen genutzt werden. Die Angriffe sollen möglichst lange unentdeckt bleiben, teilweise werden explizit weitere Ziele gesetzt. Dies kann der Zugriff auf einen bestimmten Geschäftszweig sein oder ein bestimmtes Ausmaß des Angriffs. Der Angriff ist die Hauptphase des TIBER-Tests, verlangt vom Finanzunternehmen jedoch am wenigsten Eigenleistung.

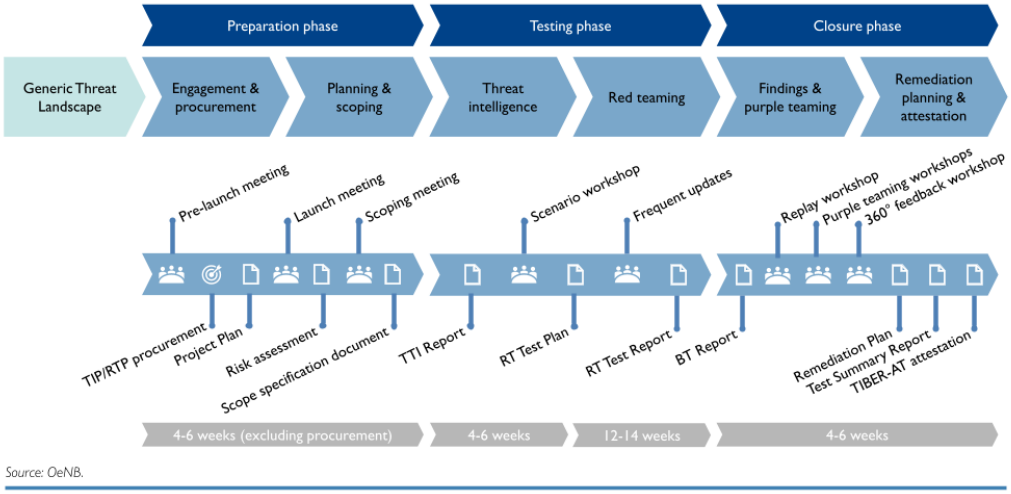
ee. Purple Team

Die Kombination aus blau und rot ist lila. Das Purple Team besteht aus Verantwortlichen des Finanzunternehmens, die im Blue Team sind und den Angriff im Rahmen ihrer Aufgaben abzuwehren versucht haben und dem Anführer der Hacker von den Red Team Testern.[92] Gemeinsam mit dem Control Team wird der vergangene IKT-bezogene Vorfall, der Angriff, analysiert. Es werden Maßnahmen erarbeitet, die das IKT-Sicherheitsmanagement nachhaltig verbessern und durch den Test aufgedeckte Schwachstellen schließen sollen.

ff. TIBER Test Manager

Der TIBER Test Manager ist ein von der zuständigen Behörde entsandter Spezialist, Mitglied des bei der österreichischen Nationalbank sitzenden TIBER Cyber Team Austria, dem nationalen Kompetenzzentrum für die Umsetzung von TIBER-AT bei der österreichischen Nationalbank. Er steht dem Finanzunternehmen während des gesamten Testvorgangs als Ansprechpartner der zuständigen Behörde zur Seite.[93] Außerdem prüft er die Einhaltung aller Anforderungen von TIBER-AT. Die vom Finanzunternehmen angestrebte Validierung der Durchführung des TIBER-Tests wird vom Test Manager vorgenommen. Als Bindeglied ist der Test Manager zwar zwischen Behörde und Finanzunternehmen geschaltet, steht aber im Lager der Behörde und nimmt nicht gestaltend Einfluss auf den Prozess des TIBER-Test.

[92] *Boss/Herrmann/Richter/Wellischowitsch*, in Hysek Praxishandbuch DORA, Kapitel 6.2.2 Seite 132.
[93] Österreichische Nationalbank, TIBER-AT Implementation Guide, Kapitel 3.6 Seite 7 https://www.oenb.at/finanzmarkt/tiber-at.html (zuletzt abgerufen am 17.08.2025).



Grafik: Schematische Darstellung des Ablaufs eines TIBER-AT Test[94]

b. Anpassungen mit DORA

Mit dem Inkrafttreten von DORA am 17. Januar 2025 wird Threat Led Penetration Testing für umfasste Finanzunternehmen verpflichtend. Artikel 26 Absatz 11 DORA verweist für die Durchführung des TLPT auf das TIBER-EU Rahmenwerk. Ergänzt werden soll dies durch die regulatorischen technischen Standards (RTS on TLPT), die von den ESA herausgegeben wurden.[95] Die bestehenden TIBER-EU und TIBER-AT müssen an DORA und die zugehörigen RTS on TLPT in einzelnen Fällen angepasst werden, um mit der Durchführung der Tests die neuen Anforderungen erfüllen zu können.

Artikel 27 DORA stellt hohe Anforderungen an die Hacker, die den Test als Teil des Red Team durchführend. Diese sind umfassender, als bisher in TIBER-AT. Da eine formale Zertifizierung im Sinne von Artikel 27 Absatz 1 lit c DORA bisher nicht vorgesehen ist[96], wird den formalen Verhaltenskodizes oder ethischen Rahmenregelungen in der Praxis viel Gewicht zukommen. Weiter ist der Einsatz von internen Testern in Artikel 26 Absatz 8 DORA vorgesehen.[97] Nur bei jedem dritten TLPT müssen externe

[94] Österreichische Nationalbank, TIBER-AT Implementation Guide, Kapitel 6.2 Seite 20.
[95] ESA, Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554 https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-29_-_Final_report_DORA_RTS_on_TLPT.pdf (zuletzt abgerufen am 17.08.2025).
[96] *Boss/Herrmann/Richter/Wellischowitsch,* in Hysek Praxishandbuch DORA, Kapitel 6.2.2 Seite 138.
[97] Siehe auch: ESA, RTS on TLPT Artikel 13.

Tester herangezogen werden. Beide Arten von Testern müssen für einen Einsatz im Red Team entsprechende technische Erfahrung mitbringen.[98]

Der Einsatz des Purple Team wird seit DORA und den RTS on TLPT verpflichtend vorausgesetzt, während es vorher bei TIBER-AT freiwillig Teil des Prozesses war. Dies dient einer gesteigerten Sorgfalt bei der Auswertung des Tests und damit eine erhöhte Effizienz bei den daraus abgeleiteten Maßnahmen.

Finanzunternehmen können gemeinsame TLPT durchführen, wenn sie derselben Unternehmensgruppe angehören. Auch IKT-Dienstleister können darin integriert werden, wenn sie zur selben Unternehmensgruppe gehören. Eine Durchführung von einzelnen Tests ist damit nicht mehr erforderlich. Dies senkt nicht nur die Kosten, sondern spiegelt auch den sich wandelnden Aufbau von Unternehmen wider, die IKT-Dienstleistungen immer weiter auslagern.

DORA hat die Regulierung auf IKT-Drittdienstleister erweitert. Dies war bisher nicht in TIBER-AT vorgesehen. Auch mit diesen Drittdienstleistern können gebündelte TLPT durchgeführt werden. Jedoch sind die Voraussetzungen hier besonders streng. Der IKT-Drittdienstleister hat regelmäßig auch weitere Kunden, die nicht Teil des TLPT werden sollen oder negative Auswirkungen davon erfahren dürfen. Die zuständigen Behörden legen durch den Test Manager für diesen Fall ein führendes Finanzunternehmen fest, welches sich um die Koordination bemühen muss und verantwortlich ist.[99]

Aufgrund der Umsetzung von TIBER-EU in den einzelnen Mitgliedsstaaten waren die Vorgaben nur national anwendbar, auch wenn sie starke Ähnlichkeiten zu nachbarstaatlichen TIBER aufwiesen. Mit DORA wird der Rahmen europäisiert, sodass auch grenzüberschreitende TLPT möglich sind. Dies trägt den multinationalen Akteuren des Binnenmarktes der Europäischen Union Rechnung. Die zuständige Behörde ist bei einem grenzüberschreitenden Test im Regelfall die des Mutterkonzerns. Sollten unterschiedliche Einstufungen bestehen und nur das Tochterunternehmen zur Durchführung von TLPT verpflichtet sein, der

[98] ESA, RTS on TLPT Artikel 5.
[99] ESA, RTS on TLPT Artikel 6 f.

Mutterkonzern nicht einbezogen sein, ist die zuständige Behörde im Mitgliedsstaat des Tochterunternehmens zu finden.[100]

TIBER-AT wurde damit bereits an DORA angepasst. Auch die TIBER-EU werden auf DORA angepasst, was gegebenenfalls zu weiteren Anpassungen in TIBER-AT und den weiteren nationalen Rahmenwerken zu TLPT führen wird. Auch fordert der rasante Wandel in der digitalen Welt und deren Vernetzung mit der Finanzbranche regelmäßige Anpassungen an technische und strukturelle Fortschritte.

III. Sanktionen aus DORA

DORA ist auf eine erkennbare Stärkung der digitalen operationalen Resilienz ausgelegt. Um diese effektiv zu erreichen, sieht DORA bei Nichteinhaltung ein strenges Sanktionsregime vor. Dieses wird umgesetzt von der zuständigen nationalen Behörde. In Österreich ist dies gemäß § 2 DORA-VG in Verbindung mit Artikel 46 DORA die Finanzmarktaufsicht. Solche können verwaltungsrechtlicher Art sein und die zuständige Behörde muss das Mindestmaß der Befugnisse aus Artikel 50 DORA erhalten. Ebenso können die Sanktionen strafrechtlicher Natur sein. Dies bedarf einer expliziten gesetzlichen Regelung durch die Mitgliedsstaaten. In Österreich hat der Gesetzgeber von dieser Möglichkeit keinen Gebrauch gemacht, sodass die FMA mit den Verwaltungsstrafen, im DORA-VG geregelt, der Hauptakteur im Sanktionsregime ist.

1. Tatbestände

Die Verantwortlichkeit für Verstöße gegen DORA richtet sich gemäß § 7 DORA-VG nach den Regelungen des § 9 VStG. DORA hat eine strenge Vorstandshaftung eingeführt, welche mit dem österreichischen Verwaltungsstrafgesetz die verantwortliche Person bestimmt. Es muss sich dabei um eine nach außen vertretungsbefugte Person handeln (§ 9 Absatz 2 VStG). Dies richtet sich wiederum nach der Rechtsform des Finanzunternehmens. Es kann dabei aus dem Kreis der vertretungsbefugten Personen eine einzelne Person ausgewählt werden, die für die

[100] ESA, RTS on TLPT Artikel 14.

Materie von DORA offiziell der Beauftragte ist. Der FMA als zuständige Behörde ist die wirksame Bestellung eines Verantwortlichen mitzuteilen (§ 22 Absatz 5 FMABG).

a. Verstoß gegen Vorgaben des IKT-Risikomanagement

In § 7 Nr. 1 DORA-VG werden sämtliche Verstöße gegen die Vorgaben des IKT-Risikomanagement aus Kapitel 2 DORA als strafbar angesehen. Die Anforderungen von DORA sind umfassend zu erfüllen, mit Ausnahme der von DORA ausgenommenen Unternehmen für ein vereinfachtes IKT-Risikomanagement. Sämtliche Verstöße gelten als Verwaltungsübertretung. Ein Abwägungsspielraum ist nicht vorgesehen, die Strafe ist zu verhängen.

b. Verstoß gegen Vorgaben des vereinfachten IKT-Risikomanagement

Das vereinfachte IKT-Risikomanagement aus Artikel 16 DORA wird im Zuge des Verhältnismäßigkeitsgrundsatz aus Artikel 4 DORA und unter Wahrung sektorspezifischen Unionsrechts auf ausgewählte Finanzunternehmen angewendet. Diesen wird ein geringerer Aufwand im IKT-Risikomanagement zugestanden, welches jedoch trotzdem vollständig zu erfüllen ist. Erfüllt ein Finanzunternehmen mit vereinfachtem IKT-Risikomanagementrahmen die Anforderungen nicht, ist auch hier kein Abwägungsspielraum vorgesehen, trotz der abweichenden Ausgangssituation (§ 7 Nr. 2 DORA-VG). Eine doppelte Abwägung der Verhältnismäßigkeit bei Einstufung und Konsequenzen darf nicht vorgenommen werden.[101]

c. Fehlerhafte Reaktion

Die Reaktion auf einen IKT-bezogenen Vorfall und Cyberbedrohungen müssen gemäß Artikel 17, 18, 19 DORA behandelt werden, andernfalls fällt eine Verwaltungsübertretung an (§ 7 Nr. 3 DORA-VG). Dies umfasst die Reaktion, aber auch die Klassifizierung und die Meldung. Ausgenommen sind Finanzunternehmen, für deren Überwachung nicht die FMA als nationale Behörde zuständig ist, sondern die EZB. Dies ist insbesondere bei gemäß der Verordnung (EU) 1024/2013 als bedeutsam eingestuften Finanzunternehmen der Fall.

[101] *Sedlak/Wagner,* in Hysek Praxishandbuch DORA, Kapitel 13.4.2. Seite 362.

d. Durchführung von TLPT

Gemäß § 7 Nr. 4 DORA-VG ist eine Verwaltungsstrafe vorgesehen, wenn die Durchführung von TLPT nicht den Artikeln 24, 25 DORA entspricht. Die TLPT sind ein gewichtiges Instrument von DORA, mit deren Hilfe ein Überblick über den aktuellen Stand der digitalen operationalen Resilienz erhalten wird und Verbesserungspotenzial identifiziert wird. Unternehmen, die gemäß Artikel 26 Absatz 8 Unterabsatz 3 DORA mit der Durchführung von erweiterten TLPT beauftragt sind, sind gemäß § 7 Ziffer 5 DORA-VG erfasst.

e. IKT-Drittdienstleistermanagement

§ 7 Nr. 6 DORA-VG normiert Verstöße gegen das von den Artikel 28 Absatz 1-8, Artikel 29 und Artikel 30 Absatz 1-4 DORA vorgeschriebene IKT-Drittdienstleistermanagement als Tatbestand für Verwaltungsstrafen. Dass IKT-Drittdienstleister in das IKT-Risikomanagement einbezogen werden, ist eine Neuerung von DORA und erfordert weitreichendes Handeln der Finanzunternehmen. Eine Verwaltungsstrafbarkeit dieser Vorgaben erscheint daher praxisrelevant und fördert die Umsetzung der aufwendigen Neuerungen. IKT-Drittdienstleister, die in einem Drittland außerhalb der Europäischen Union angesiedelt sind, müssen nach Artikel 31 Absatz 12 DORA behandelt werden. Verstöße dagegen sind gemäß § 7 Nr. 7 DORA-VG verwaltungsstrafbar. Das Finanzunternehmen trägt hier teilweise die Verantwortung für das Agieren des Drittdienstleisters.

f. Anordnungen der FMA

Als zuständige Behörde erteilt die FMA gemäß Artikel 42 Absatz 6 DORA Anweisungen gegenüber den Finanzunternehmen. Damit diese unter Druck der Umsetzung stehen und die Rechtsdurchsetzung durch die FMA geschehen kann, fällt gemäß § 7 Nr. 8 DORA-VG eine Verwaltungsstrafe für eine Nichtbefolgung dieser an.

g. Informationsaustausch

Artikel 45 DORA sieht einen umfassenden Informationsaustausch der Finanzunternehmen vor. Dieser kann den vorgeschriebenen Zielen dienen. Ein darüberhinausgehender Austausch, beispielsweise in Form von Marktabsprachen, ist

nicht gestattet und darf nicht mit DORA begründet werden. § 7 Nr. 9 DORA-VG stellt eine Verwaltungsstrafbarkeit für eine Unter- oder Überschreitung dieser Vorgaben fest.

2. Haftung der juristischen Person

Die juristische Person hinter der natürlichen Person des Verantwortlichen kann gemäß § 8 DORA-VG haften. Dies kann der Fall sein, wenn der Verantwortliche in Vertretung der juristischen Person agiert, Entscheidungsbefugnis für die juristische Person übernimmt oder Kontrollbefugnis innerhalb der juristischen Person innehat. Dazu haftet die juristische Person, wenn sie es unterlässt, die Verantwortung eindeutig festzulegen und dadurch Versäumnisse entstehen.

3. Strafbemessung

Die Höhe der Verwaltungsstrafe hängt gemäß § 9 DORA-VG von den dort aufgezählten Faktoren ab. Dabei ist stets der Grundsatz der Verhältnismäßigkeit aus Artikel 4 DORA einzubeziehen.

Wesentlichkeit, Schwere und Dauer des Verstoßes gelten als die gewichtigsten Parameter bei der Strafbemessung.[102] Der Grad der Verantwortung spielt ebenfalls eine wichtige Rolle. Wird die Verantwortung einer natürlichen Person einer juristischen Person zugerechnet, erhöht sich deren Verantwortung entsprechend. Die konkrete Stellung der natürlichen Person ist dabei zu berücksichtigen. Sollte die juristische Person die verantwortliche natürliche Person in ihrem fehlerhaften Verhalten begünstigt haben, verschärft dies den Grad der Verantwortung.[103] Die individuelle Finanzkraft ist bei den Verantwortlichen zu berücksichtigen. Eine finanzielle Überforderung würde dem Verhältnismäßigkeitsprinzip zuwiderlaufen. Sollte durch die Nichteinhaltung der Vorgabe aus DORA ein finanzieller Gewinn erwirtschaftet worden sein oder ein sicherer Verlust verhindert, ist dies ebenfalls zu berücksichtigen. Auch Schäden bei Dritten sind in der Strafbemessung zu berücksichtigen, beispielsweise Kunden des Finanzunternehmens oder andere, unbeteiligte Kunden des IKT-Drittdienstleisters. Die Zusammenarbeit mit der FMA bei

[102] *Sedlak/Wagner,* in Hysek Praxishandbuch DORA, Kapitel 13.6.2. Seite 376.
[103] *Künzel,* in Dellinger, BWG Kommentar § 99e Rn. 19.

wirkt sich strafmildern aus, während sich Wiederholungstaten strafverschärfend auswirken.

Durch diese Bemessungsgrundlagen kann die FMA bei den Verwaltungsstrafen verhältnismäßig vorgehen und den Verantwortlichen eine faire Strafe auferlegen. Diese soll strafend wirken, aber auch präventiv vor Wiederholung warnen und damit eine verbesserte Umsetzung von DORA unterstützen.

IV. Zwischenfazit

DORA billigt der zuständigen nationalen Behörde eine sehr weitreichende Rolle zu, in der diese nicht nur tiefgehende Kompetenzen vor einem Vorfall zukommt, sondern auch während und nach einem Vorfall. Die Beaufsichtigung des IKT-Risikomanagements der Unternehmen, inklusive der Durchführung des TLPT, ist genau vorgeschrieben und durch weitere Regelwerke ausgestaltet. Damit nimmt die Kontrolle der Vorgaben nicht nur in den Finanzunternehmen und deren IKT-Drittdienstleistern viel Zeit und Personal ein, sondern stellt auch für die Behörde einen erheblichen Mehraufwand dar.

D. NIS-2

Zentrales Element des harmonisierten Schutzes von Informationssystemen in der Europäischen Union neben DORA ist die NIS-2-Richtlinie (NIS-2), RL (EU) 2022/2555. Sie stellt eine Verschärfung und Konkretisierung der NIS-Richtlinie RL (EU) 2016/1148 dar und hat ähnliche Ziele, wie DORA.

I. Inhaltsauszug

1. Kapitel I

Die NIS-2-Richtlinie verpflichtet die Mitgliedsstaaten, nationale Cybersicherheitsstrategien zu verabschieden und zuständige Behörden einzurichten und auf die Abläufe anzupassen (Artikel 1 Absatz 2 lit a NIS-2). Dazu sollen klar definierte Unternehmen und Behörden ein Cybersicherheitsrisikomanagement einführen und es soll ein Austausch von daraus gewonnenen Informationen sichergestellt werden (Artikel 1 Absatz 2 lit b, c NIS-2).

NIS-2 gilt für öffentliche und private Einrichtungen, die zu im Anhang I und II der Richtlinie aufgeführten Sektoren gehören oder gemäß Artikel 2 des Anhangs der Empfehlung 2003/361/EG als mittlere Unternehmen gelten oder die erforderliche Schwelle dafür überschreiten. Anhang I nennt Unternehmen aus den Bereichen Energie, Verkehr Gesundheit, Bankwesen und Finanzinfrastruktur, Wasserwirtschaft, digitale Infrastruktur, Verwaltung von IKT-Diensten, öffentliche Verwaltung und Weltraum. Anhang II nennt dazu Postdienstleistungen, Abfallwirtschaft, Produktion und Verarbeitung von Chemikalien, Lebensmitteln und Waren, Anbieter digitaler Dienste und Forschung. Die Wirtschaftszweige sind nicht in ihrer Gänze erfasst, sondern es findet neben dem Kriterium der Größe des Betriebs auch eine Abgrenzung durch den Einbezug einzelner EU-Richtlinien statt. Damit wird der Kreis der betroffenen Einrichtungen spezifiziert. Die Mitgliedsstaaten dürfen den Geltungsbereich im vorgegebenen Rahmen frei definieren. Zusammenfassend kann bei der Vielzahl an erfassten Unternehmen und Einrichtungen auf die Systemrelevanz abgestellt werden, die durch das Überschreiten der festgelegten Schwellenwerte als gegebene angenommen wird. Die Auflagen sollen eine starke Resilienz gegen Cyberattacken sicherstellen und damit eine Fortführung des wirtschaftlichen und öffentlichen Lebens im Fall einer Attacke gewährleisten.

Die betroffenen Unternehmen werden als wesentliche, wichtig oder kritisch bezeichnet. Für den Fall, dass bereits sektorspezifische Unionsrechtsakte auf eine Einrichtung anwendbar sind, gilt NIS-2 nur insoweit, dass diese Regelungen nicht beeinträchtigt werden. Eine doppelte Verpflichtung soll nicht bestehen (Artikel 4 NIS-2). Dazu können die Mitgliedsstaaten eigene, strengere Regelungen erlassen, um das Cybersicherheitsniveau zu erhöhen (Artikel 5 NIS-2).

2. Kapitel II

Es werden umfassende Verpflichtungen für die Mitgliedsstaaten vorgeschrieben, deren Umsetzung es bedarf. Zentral ist die Schaffung einer nationalen Cybersicherheitsstrategie, die sämtliche erforderlichen Maßnahmen beinhaltet und die folgenden Mindestanforderungen aus Artikel 7 Absatz 1 NIS-2 abdeckt:

Ziele und Prioritäten der Strategie, einen umsetzbaren Steuerungsrahmen, einen Mechanismus zur Ermittlung von betroffenen Einrichtungen, Maßnahmen zur

Vorsorge, Reaktionsfähigkeit und Wiederherstellung sowie Kommunikationsaustausch, eine Liste der Verantwortlichen und einen Plan für die Förderung der Sensibilisierung der Bevölkerung zur Cybersicherheit allgemein.

Die nationale Sicherheitsstrategie ist regelmäßig, spätestens alle fünf Jahre, neu zu bewerten und bei Bedarf zu aktualisieren (Artikel 7 Absatz 4 NIS-2). Die Europäische Union unterstützt dies durch die ENISA aktiv, um dem gemeinsamen Ziel näher zu kommen.

Für die Umsetzung der Richtlinie ist eine nationale Behörde als zuständig zu benennen. Die Aufgaben können auch auf mehrere Behörden verteilt werden, eine Kompetenzzuschreibung hat aber eindeutig zu erfolgen. Die zuständige Behörde ist auch die zentrale Anlaufstelle, außer es findet eine Aufteilung der Zuständigkeiten statt. In diesem Fall ist eine eindeutige zentrale Anlaufstelle zu benennen, die die weitere Kommunikation zwischen Behörden und von der Richtlinie betroffenen Einrichtungen koordiniert (Artikel 8 Absatz 3 NIS-2).

Dazu wird eine Behörde geschaffen oder benannt, die für das Cyberkrisenmanagement zuständig ist (Artikel 9 NIS-2). Sie überwacht nicht die Einhaltung der NIS-2-Richtlinie, sondern agiert als Koordinator im Fall eines Cyberangriffs, der weitreichende Auswirkungen hat. Die dafür erforderlichen Ressourcen sind vom Mitgliedsstaat bereit zu stellen.

Als Untereinheit der zuständigen Behörde, oder aber als eigenständige Institution werden Computer-Notfallteams (CSIRTs) eingerichtet (Artikel 10 NIS-2). Sie sind die technischen Ausführer von Kontrollen im Bereich der Cybersicherheit, stellen die Kommunikation um Cyberbedrohungen herum, stellen die Unterstützung für betroffenen Einrichtungen bereit und erheben Daten, um eine Lagebeurteilung ausgeben zu können. Dazu führen die CSIRTs Schwachstellenscans durch und kommunizieren mit anderen Betroffenen und CSIRTs (Artikel 11 Absatz 3 NIS-2). Die zuständige Behörde, die zentrale Anlaufstelle und die CSIRTs müssen, sollten sie nicht ident sein, den Informationsaustausch über Vorfälle, Risiken und anderer Ereignisse untereinander nachhalten, um stets eine umfassende Reaktion zu ermöglichen.

3. Kapitel III

Auch auf Unionsebene werden Kommunikationsforen eingerichtet. Dazu gehört die Kooperationsgruppe, welche aus Vertretern der Mitgliedsstaaten, der Kommission und der ENISA besteht (Artikel 14 Absatz 3 NIS-2). Sie stellt Unterstützung für die zuständigen nationalen Behörden bereit, bietet Beratung an, bezieht falls erforderlich weitere Unionsorgane ein und bietet Hilfe bei der Rechtsauslegung. Dazu kommt die Risikobewertung kritischer Lieferketten, die Koordination von Amtshilfemaßnahmen und allgemeine Beratungstätigkeiten, sowie das Erstellen von zugehörigen Berichten (Artikel 14 Absatz 4 NIS-2). Das CSIRTs-Netzwerk daneben besteht aus Vertretern der nationalen CSIRTs und dient insbesondere dem Informationsaustausch (Artikel 15 NIS-2). Gegenseitige Unterstützung wird ebenfalls über das Netzwerk koordiniert und alle grenzüberschreitenden Sachverhalte werden dort behandelt. Das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) dient zusätzlich der Kommunikation der zuständigen Behörden mit der Kommission (Artikel 16 NIS-2).

4. Kapitel IV

Wichtige und wesentliche Einrichtungen müssen für die Umsetzung der Vorgaben der NIS-2-Richtlinie verantwortlich gemacht werden können. Eine entsprechende Umsetzung durch die Mitgliedsstaaten hat zu erfolgen (Artikel 20 NIS-2). Dazu sind entsprechende Schulungen durchzuführen. Die Führungsverantwortlichen werden direkt adressiert und haben die Umsetzung zu verantworten.

Die Einrichtungen müssen Risikomanagementsysteme etablieren, die die Auswirkungen von Cybersicherheitsvorfällen für den Geschäftsbetrieb und für Dritte verhindern oder möglichst gering halten (Artikel 21 Absatz 1 NIS-2). Der Geschäftsbetrieb muss aufrechterhalten werden können und eine wirksame Backup-Strategie muss implementiert werden. Artikel 21 Absatz 2 NIS-2 nennt zehn konkrete Vorgaben an das Risikomanagement, welche mindestens enthalten sein müssen:

Ein Konzept zur Risikoanalyse, die Bewältigung von Sicherheitsvorfällen, die Aufrechterhaltung des Betriebs sowie das Backup-Management, Sicherheit der Lieferkette, Sicherheit bei Entwicklungen an Informationssystemen, Konzepte zur

Bewertung der Cybersicherheit, Cyberhygiene und Schulungen, Kryptografie, physische Sicherheitsmaßnahmen und die Multi-Faktor-Authentifizierung.

Die Lieferketten ausgewählter Einrichtungen unterliegen der Risikobewertung der Kooperationsgruppe der Europäischen Union (Artikel 22 Absatz 1 NIS-2).

Für den Fall einer Cybersicherheitsverletzung haben betroffenen Einrichtungen gemäß Artikel 23 NIS-2 eine umfassende Berichtspflicht an die zuständige Behörde oder die CSIRTs. Es erfolgt eine dreistufige Meldung über den Beginn des Vorfalls, Aktualisierungen bei geänderter Sachlage und ein Abschlussbericht.

5. Kapitel VII

Die Aufsichts- und Durchsetzungsmaßnahmen sind sehr umfangreich ausformuliert. Es wird zwischen wichtigen (Artikel 3 Absatz 2 NIS-2) und wesentlichen (Artikel 3 Absatz 1 NIS-2) Einrichtungen unterschieden.

Die wirksame Durchsetzung der zuständigen Behörde gegenüber wesentlichen Einrichtungen, die die NIS-2-Vorgaben einzuhalten haben, soll gemäß Artikel 32 NIS-2 gewährleistet werden. Teil der Maßnahmen zur Durchsetzung sind Vor-Ort-Kontrollen, Sicherheitsprüfungen, Informationsanforderungen, Zugang zu Daten und die Anforderung von Nachweisen über das Cybersicherheitsmanagement.

Für wichtige Einrichtungen bestimmt Artikel 33 NIS-2 die Befugnisse der Aufsichtsorgane. Diese ähneln denen der wesentlichen Einrichtungen stark, finden jedoch erst Anwendung, nachdem Nachweise, Hinweise oder Informationen vorliegen, die eine Nichtbefolgung der Vorgaben anzeigen. Bei wesentlichen Einrichtungen hingegen erfolgt die Ausübung der Aufsichtsmaßnahmen ohne Verdachtsfall dauerhaft.

Sowohl bei wesentlichen, als auch bei wichtigen Einrichtungen kann eine Mängelbehebung behördlich angeordnet werden und eine Nichtbefolgung zieht entsprechende Verfahren nach sich. Bei wesentlichen Einrichtungen kann dies zum Entzug von Zertifizierungen oder zur Entmachtung des Verantwortlichen führen (Artikel 32 Absatz 5 NIS-2). Bei wichtigen Einrichtungen sind keine derartig weitreichenden Eingriffe möglich.

Artikel 34 NIS-2 erläutert die Verhängung von Geldbußen. Für Verstöße gegen die Artikel 21, 23 NIS-2, also das Risikomanagement und die Berichtspflichten, werden für wesentliche Einrichtungen eine maximale Geldbuße von mindestens EUR 10.000.000 oder 2% des gesamten weltweiten Umsatzes des vergangenen Geschäftsjahres und für wichtige Einrichtungen eine maximale Geldbuße von mindestens EUR 7.000.000 oder 1,4% des gesamten weltweiten Umsatzes des vergangenen Geschäftsjahres festgelegt.

Die von den Mitgliedsstaaten zu erlassenen Vorschriften über die Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein (Artikel 36 NIS-2).

II. Vergleich zu DORA

DORA und NIS-2 haben ähnliche Ziele, nur stellt DORA lex specialis zu NIS-2 dar[104], indem dort eine genauer abgegrenzte Branche, nämlich Finanzunternehmen, reglementiert werden. Dies kann Unterschiede bei den Anforderungen begründen.

1. Rechtliche Umsetzung

DORA ist als Verordnung der Europäischen Union ausgestaltet. Diese ist gemäß Artikel 288 Absatz 2 AEUV direkt in den Mitgliedsstaaten anwendbar und bedarf keiner weiteren Rechtssetzung.[105] Sie entfaltet ihre Rechtswirkung gegenüber Privaten, sodass die Vorgaben in DORA ausführlich und verständlich dargestellt sein müssen. Nur so ist eine Befolgung durch die Verpflichteten direkt möglich. Die Durchführungsgesetze im Sinne von Artikel 291 Absatz 1 AEUV, beispielsweise das österreichische DORA-VG, dienen nicht der reinen Umsetzung, sondern konkretisieren einzelne Ausführungen der Verordnung. Sie widersprechen der Verordnung zu keinem Zeitpunkt.

Die Richtlinie hingegen bedarf einer nationalen Umsetzung durch die Mitgliedsstaaten (Artikel 288 Absatz 3 AEUV). Die Umsetzung ist dabei dem Mitgliedsstaat überlassen. Dabei ist eine wörtliche Übernahme ausreichend[106], es kann aber auch eine sinngemäße Adaption erfolgen. Entscheidend ist, dass nicht vom

[104] Erwägungsgrund 16 DORA.
[105] Ständige Rechtsprechung: EuGH, Rs. 43/71, Slg. 1971, 1039, Rn. 9 (Politi/Italien); Rs. 93/71, Slg. 1972, 287, Rn. 5 f. (Leonesio/Italienisches Ministerium für Landwirtschaft).
[106] *Calliess/Ruffert*, AEUV Art. 288 Rn. 27.

Inhalt der Richtlinie abgewichen wird und eine fristgerechte Umsetzung erfolgt. NIS-2 ist in Deutschland in das bereits bestehende Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) übernommen worden. Österreich hat bereits für die ursprüngliche NIS-Richtlinie ein Netz- und Informationssystemsicherheitsgesetz erlassen, welches auf NIS-2 angepasst wurde.

Die Umsetzung der NIS-2-Richtlinie lässt den Mitgliedsstaaten Spielräume, beispielsweise bei der Schwerpunktsetzung, den umfassten Einrichtungen oder den Prüfungszyklen. Damit kann es innerhalb der Europäischen Union zu nicht nur unerheblichen Abweichungen kommen. Dies kann wiederum verzerrende Effekte für Einrichtungen mit sich bringen, die ihren Standort frei wählen können. Öffentliche Einrichtungen sind hingegen an ihren Mitgliedsstaat gebunden und können sich nicht nach günstigeren Standortbedingungen ausrichten. DORA als Verordnung hingegen schafft eine Vollharmonisierung, die die Einheit des Binnenmarktes stärkt. Mit DORA werden nicht nur Mindeststandards vorgegeben, sondern einzuhaltende Vorgaben gemacht. Damit ist aufgrund der gleichen Anwendung in allen Mitgliedsstaaten durchsetzungsstärker und dient dem Binnenmarkt, indem es gleiche Standortbedingungen überall schafft.

2. Methodik

Sowohl DORA, als auch NIS-2 bauen auf von den Betroffenen einzurichtende Risikomanagementsysteme. Diese zeichnen sich bei beiden dadurch aus, dass jeweils Verantwortliche benannt werden müssen. [107] Dies sind regelmäßig die Vorstände, es können aber auch andere Personen sein.[108] Die abschließende Festlegung erfolgt in der nationalen Umsetzung von NIS-2.

Beide Systeme sind auf Prävention ausgelegt, sodass vorab Maßnahmen getroffen sind, die den Schutz der Informationssysteme vor Zugriffen Unbefugter zu schützen versuchen. Dafür haben regelmäßige Schulungen zu erfolgen und es bestehen umfassende Dokumentationspflichten, die einer Übermittlung an die zuständigen Behörden bedürfen. Die Kontrollzyklen sind dabei regelmäßig und nehmen Rücksicht

[107] Artikel 20 NIS-2; Artikel 5 Absatz 2 DORA.
[108] *Schiefer/Wieser,* NIS-2-RL: Wer trägt die Verantwortung im Unternehmen? Das "Leitungsorgan" in der NIS-2-RL, ecolex 2023/568, 900, B.

auf neue technische Prozesse. Die gesteigerte Resilienz dient in beiden Fällen dazu, kritische Funktionen der Zivilgesellschaft und des Wirtschaftsraumes auch bei Vorfällen in ihrer Funktion zu erhalten. Als Minimum wird ein Schutz vor Beeinträchtigungen Dritter bezweckt, damit kein Flächenbrand entsteht und ganze Versorgungszweige zusammenbrechen.

Auch wenn DORA genauere Vorgaben bezüglich dieses Systems und seiner Ausgestaltung macht, ist das Ziel beider Rechtsakte, klare Handlungsabläufe zu schaffen, um bei einem Sicherheitsvorfall direkt handeln zu können. Das Fortbestehen des Geschäftsbetriebs, der Schutz von Dritten und die schnellstmögliche Beseitigung der Beeinträchtigung sind bei beiden Rechtsakten oberstes Ziel.

Sowohl DORA, als auch NIS-2 haben strenge Bußgeldvorschriften. Während NIS-2 nur ein Minimum für die Höchststrafe vorgibt, hat DORA keinen klar definierten Rahmen für die Bußgelder. Eine verhältnismäßige Höhe von Bußgeldern ist dabei jedoch unumgänglich. Auch hier erfolgt die Festsetzung der genauen Beträge durch die Mitgliedsstaaten in den Durchsetzungsgesetzen, was ähnliche Abweichungen bedeuten kann, wie bei NIS-2. Mit NIS-2 wird, auch im Vergleich zur ursprünglichen NIS-Richtlinie eine deutliche Verschärfung vorgenommen und ein Bezug auf Unternehmen hergestellt, die mit den finanziellen Strafen besonders adressiert sind.[109]

Bedeutender Unterschied zwischen der Vorgehensweise aus DORA und aus NIS-2 sind die TLPT. Die tiefgehenden und aufwändigen Tests sind nur in DORA vorgeschrieben und damit nur für Finanzunternehmen durchzuführen. Die von NIS-2 umfassten wichtigen oder wesentlichen Einrichtungen müssen keine Tests nach festgelegten Standards durchführen. Der immense Aufwand für TLPT ist einzelnen Unternehmen aufgrund ihrer Struktur nicht zumutbar, jedoch findet auch bei DORA eine Abstufung statt, die kleinere Unternehmen von der Verpflichtung ausnimmt. Damit fehlt NIS-2 ein Instrument, das belastbare Fakten liefert und einen genauen Stand über die Absicherung gegen Cybervorfälle darstellen kann.

[109] *Schiefer/Wieser,* Cybersicherheitsrecht 2.0: Mangelhafte Compliance kommt teuer - Die NIS-2-RL und ihr Pflichtenprogramm für Unternehmen ecolex 2023/622, 1000, D. 1.

3. IKT-Drittdienstleister

IKT-Drittdienstleister unterliegen zwar DORA, ihre Verpflichtungen unterscheiden sich aber von denen der Finanzunternehmen. Sie sind vor allem in ihren vertraglichen Vereinbarungen mit Finanzunternehmen betroffen und dem daraus resultierenden Überwachungsrahmen. Eine direkte Vorschreibung von Risikomanagement für IKT-Drittdienstleister hat DORA nicht, sondern die Finanzunternehmen müssen dies für ihre Dienstleister sicherstellen.

NIS-2 hingegen erfasst den Bereich der digitalen Infrastruktur relevanter Einrichtungen. IKT-Drittdienstleister gelten regelmäßig als wichtige Einrichtung, sodass die Umsetzungsgesetze von NIS-2 für sie anwendbar sind. Artikel 6 NIS-2 nennt Dienstleistungen, die regelmäßig von Finanzunternehmen in Anspruch genommen werden dürften. Dies sind Cloud-Computing-Dienste (Nr. 30), Rechenzentrumsdienste (Nr. 31), Inhaltszustellnetze (Nr. 32), Anbieter verwalteter Dienste (Nr. 39) und Anbieter verwalteter Sicherheitsdienste (Nr. 40). Diese Begriffe sind weit gefasst, sodass eine Doppelbetroffenheit von DORA als IKT-Drittdienstleister und von NIS-2 und den zugehörigen Umsetzungsgesetzen regelmäßig auszugehen ist.[110] Artikel 32 Absatz 8 DORA stellt klar, dass die betreffenden Vorgaben aus DORA neben denen der NIS-2-Umsetzungsgesetze stehen. Eine Befolgung beider Regulierungswerke ist damit parallel erforderlich. Der Verweis auf eine bereits bestehende Überwachung aufgrund von NIS-2 kann nicht als relevant für eine Aufsicht aus einem DORA-Überwachungsrahmen angenommen werden.

4. Behörden

DORA stellt als lex specialis einen sektorspezifischen Rechtsakt gegenüber NIS-2 dar. Damit keine Parallelstrukturen geschaffen werden, sieht Artikel 47 Absatz 1 DORA explizit die Beteiligung der ESA und der zu ständigen nationalen Behörden in der NIS-Kooperationsgruppe vor. Die Behörden können dabei mindestens aufsichtsweise teilnehmen, der Erwägungsgrund 18 DORA spricht jedoch sogar von der aktiven Beteiligung an Diskussionen und eine technische Mitarbeit. Die Erkenntnisse der von DORA betroffenen Finanzunternehmen und der von NIS-2 umfassten Einrichtungen

[110] *Heussler/Spiegel/Zanol*, in Hysek: Praxishandbuch DORA, 11.2.3.4. S. 319.

werden damit ausgetauscht und bieten dem jeweils anderen einen Mehrwert. Die Behörden können sich auf Kenntnisse der jeweils anderen berufen und ihr Handeln daran ausrichten, bevor eigene Unternehmen/Einrichtungen betroffen sind. Insbesondere für IKT-Drittdienstleister, die im Gegensatz zu Finanzunternehmen sowohl von DORA, als auch von NIS-2 betroffen sein können, ist dies eine Erleichterung, um keine doppelten Vorgänge bei Behörden zu haben.

Auch können beide zuständigen Behörden auf die CSIRTs zugreifen. In NIS-2 eingerichtet, verweist Artikel 47 Absatz 2 DORA explizit auf die Nutzung dieser. Es findet gemäß Artikel 19 Absatz 6 lit c DORA ein Austausch zwischen den zuständigen Behörden und den nach NIS-2 zuständigen Behörden bezüglich schwerwiegender IKT-bezogener Vorfälle statt, der einer gesteigerten Sensibilisierung des jeweils anderen dient.[111] Erstmeldungen können neben der zuständigen Behörde auch an die nach NIS-2 zuständige Behörde oder die CSIRTs eingereicht werden müssen, wenn die Mitgliedsstaaten dies vorsehen (Artikel 19 Absatz 1 DORA). Insgesamt hat ein sehr umfangreicher Informationsaustausch zwischen den Behörden stattzufinden. Nach DORA als lex specialis zuständige Behörden arbeitet den zuständigen Behörden aus NIS-2 zu, was Synergieeffekte hervorrufen soll und eine gesteigerte Resilienz schaffen kann. Umgekehrt kann dieser Austausch auch für Finanzunternehmen wichtige Erkenntnisse bringen, insbesondere mit den hohen Pflichten zur Kontrolle von IKT-Drittdienstleistern, die NIS-2 unterliegen können.

Allgemeiner Unterschied bei der Behördenarbeit zwischen NIS-2 und DORA ist, dass bei DORA auch europäische Aufsichtsbehörden als federführende Behörden an der Überwachung teilnehmen, während bei NIS-2 die Überwachung ausschließlich durch die zuständigen nationalen Behörden erfolgt.

5. Zwischenfazit

NIS-2 und DORA haben gemeinsame Ziele, wirken aber in den betroffenen Einrichtungen selbstständig nebeneinander. Neben einzelnen Unterschieden in der Umsetzung und den Anforderungen ist DORA die weiter gehende Maßnahme. Insbesondere die TLPT und der Umgang mit den IKT-Drittdienstleistern sind

[111] Erwägungsgrund 52 DORA.

gravierende Unterschiede, die einen erheblichen Mehraufwand bedeuten. Der Finanzsektor wird vergleichsweise stark in die Pflicht genommen, was dessen Bedeutung für die Europäische Union herausstellt.

E. Critical Entities Richtlinie

Als dritten Rechtsakt zur Stärkung der digitalen Resilienz von Einrichtungen innerhalb des Binnenmarktes hat die Europäischen Union die Richtlinie über die Resilienz kritischer Einrichtungen RL (EU) 2022/2557 (Critical Entities Richtlinie, CER) erlassen.

I. Inhalt

Der Inhalt wird verkürzt dargestellt, soweit er für einen Vergleich zu DORA relevant ist und er Handlungsvorgaben enthält.

1. Kapitel II

Die einzelnen Mitgliedsstaaten haben zum 17. Januar 2026 eine Strategie zur Verbesserung der Resilienz kritischer Einrichtungen zu erlassen (Artikel 4 Absatz 1 CER). Mindestgehalt dieser Strategie muss eine Definition der Ziele und Prioritäten sein, mit denen die Resilienz kritischer Einrichtungen gestärkt wird, die auch sektorübergreifende und grenzüberschreitende Abhängigkeiten des Binnenmarktes ausreichend berücksichtigt. Zuständige Behörden und deren Befugnisse sind eindeutig zu benennen und ein Handlungsrahmen vorzugeben. Die Einstufung der Einrichtungen als kritisch obliegt den Mitgliedsstaaten, das Verfahren ist vorab festzulegen und in der Strategie enthalten. Sämtliche Unterstützungsmaßnahmen horizontaler Art sind in der Strategie zu benennen, darüber hinausgehende Absprachen zwischen kritischen Einrichtungen somit nicht automatisch zulässig. Weiter sind alle an der Steigerung der Resilienz Beteiligten in Listen aufzuführen, um den betroffenen Einrichtungen einen Überblick verschaffen zu können.

Die Mitgliedsstaaten müssen eine Risikobewertung ihrer Einrichtungen durchführen, auf die die Kommission Zugriff hat (Artikel 5 Absatz 1 CER). In der Bewertung müssen von Natur und Mensch verursachte Risiken Einfluss finden, auch sektorübergreifend und grenzüberschreitend. Eine Begrenzung wird nicht vorgenommen, sodass alle in

Betracht kommenden Faktoren berücksichtigt werden müssen. Insbesondere müssen bereits bekannte Sicherheitsvorfälle einberechnet werden (Artikel 5 Absatz 2 lit d CER). Die Bewertung muss auch den betroffenen Einrichtungen zugänglich gemacht werden und daraus resultierende Maßnahmen sind von den Mitgliedsstaaten zu unterstützen.

Die Ermittlung der kritischen Einrichtungen obliegt den Mitgliedsstaaten. Dadurch werden nationale Besonderheiten im Rechtssystem oder der Struktur der Wirtschaft berücksichtigt und es kann eine möglichst umfassende Bewertung der potenziell als kritisch einzustufenden Einrichtungen erfolgen. Kriterien bei der Einstufung sind die Art der von der Einrichtung erbrachten Dienste, ob diese kritisch für die Gesellschaft sind, die Lage der kritischen Infrastruktur im jeweiligen Mitgliedsstaat und die potenziellen Auswirkungen eines erheblichen Vorfalls (Artikel 6 Absatz 2 CER). Der Anhang der CER nennt die Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastruktur, Gesundheit, Wasserwirtschaft, digitale Infrastruktur, öffentliche Verwaltung und den Weltraum, sowie die Arbeit mit Lebensmitteln. Die Liste der kritischen Einrichtungen hat regelmäßig, spätestens aber alle vier Jahre, aktualisiert zu werden.

Eine zu erwartende erhebliche Störung, die aus einem Vorfall einer kritischen Einrichtung resultieren könnte, kennzeichnet sich durch die Zahl der betroffenen Nutzer der Einrichtung sowie weitere von dieser abhängige Akteure. Auch die Dauer der Beeinträchtigung ist relevant, sowie der Marktanteil und das geografische Gebiet, falls abgrenzbar. Die Zahl der zur Verfügung stehenden Alternativen kann eine Einstufung als kritisch ebenfalls beeinflussen (Artikel 7 Absatz 1 lit f CER). Die genauen verwendeten Kriterien, die den Mitgliedsstaaten überlassen sind, müssen der Europäischen Kommission übermittelt werden.

Die zuständige Behörde ist von den Mitgliedsstaaten jeweils zu benennen oder zu schaffen. Sollten mehrere Behörden zuständig sein, wird eine zentrale Anlaufstelle eingerichtet, um den betroffenen Einrichtungen eine erhöhte Übersichtlichkeit zu verschaffen (Artikel 9 Absatz 1 Unterabsatz 3 CER). Ebenfalls für die grenzüberschreitende Zusammenarbeit ist eine solche zentrale Anlaufstelle zu benennen.

Über die zuständigen Behörden unterstützen die Mitgliedsstaaten die kritischen Einrichtungen aktiv bei der Erreichung der Ziele, einer gesteigerten Resilienz. Artikel 10 CER nennt dafür insbesondere Beratung und Schulungen, Leitfäden und Übungen zur Prüfung der Resilienz. Auch zwischen den Mitgliedsstaaten hat eine Zusammenarbeit zu erfolgen (Artikel 11 CER), die grenzüberschreitende kritische Einrichtungen betrifft oder deren Dienstleistungen in einem anderen Mitgliedsstaat angeboten wird.

2. Kapitel III

Die als kritisch eingestuften Einrichtungen müssen eine Risikobewertung durchführen (Artikel 12 Absatz 1 CER). Diese muss erstmalig spätestens nach neun Monaten erfolgen, danach regelmäßig, was mindestens alle vier Jahre bedeutet. Sie hat umfassend alle Faktoren menschlicher und natürlicher Art zu berücksichtigen, wie sie auch die Mitgliedsstaaten bei der Einstufung einfließen lassen.

Die aus der Risikobewertung geschlussfolgerten Maßnahmen müssen gemäß Artikel 13 CER geeignet und verhältnismäßig sein und technischer, sicherheitsbezogener und organisatorischer Art. Es müssen Sicherheitsvorfälle vorab verhindert werden können, physischer Schutz für Räumlichkeiten eingerichtet werden, eine aktive Reaktion auf Vorfälle sichergestellt sein und eine Wiederherstellung bei eingetretenen Auswirkungen. Personal ist zu sensibilisieren und vorzubereiten. Die Maßnahmen sind in einem allgemeinen Plan zu dokumentieren und der zuständigen Behörde zu übermitteln, sodass sie im Bedarfsfall zur Verfügung stehen. Eine Kommunikationsperson wird der Behörde zusätzlich benannt.

Einzelne Personen können auf Antrag auf ihre Zuverlässigkeit hin überprüft werden (Artikel 14 Absatz 1 CER). Die Voraussetzungen dafür legen die Mitgliedsstaaten selbst entsprechend den Mindestvorgaben aus der Richtlinie fest.

Sicherheitsvorfälle sind der zuständigen Behörde unverzüglich gemäß Artikel 15 CER zu melden. Die bedeutet in der Regel innerhalb von 24 Stunden nach Kenntniserlangung. Nach einem Monat hat zusätzlich ein umfassender Abschlussbericht zu erfolgen.

3. Kapitel IV

Als besonders von der Richtlinie betroffen gelten Einrichtungen, die als von besonderer Bedeutung für Europa angesehen werden. Eine solche Einstufung erfolgt gemäß Artikel 17 Absatz 1 CER, wenn die Eirichtung bereits kritisch ist, in sechs oder mehr Mitgliedsstaaten tätig ist und der zuständigen Behörde als solche gemeldet ist.

Die Betreuung dieser kritischen Einrichtung mit besonderer Bedeutung für Europa unterstütz die Europäische Union durch eine Beratungsmission (Artikel 18 CER). Sie setzt sich aus Sachverständigen der von der Einrichtung betroffenen Mitgliedsstaaten und der Kommission zusammen, um die Unterschiede der nationalen Akteure innerhalb der Union berücksichtigen zu können.

4. Kapitel VI

Zur Durchsetzung ist den zuständigen Behörden den kritischen Einrichtungen gegenüber die Möglichkeit von Vor-Ort-Kontrollen einzuräumen (Artikel 21 Absatz 1 lit a CER), sowie Audits durchzuführen (lit b). Auch muss Informationszugang gewährleistet werden und die Umsetzung von Maßnahmen nach der eigenen Risikoanalyse und nach Anordnung der Behörde nachgewiesen werden. Sämtliche Handlungen der Behörden sind objektiv, transparent und verhältnismäßig auszuführen, um den berechtigten Interessen der kritischen Einrichtungen Rechnung zu tragen (Artikel 21 Absatz 4 CER).

Für Verstöße gegen die Vorschriften der Richtlinie oder der zuständigen Behörden haben die Mitgliedsstaaten Sanktionsvorschriften zu erlassen. Diese müssen wirksam, verhältnismäßig und abschreckend sein, sind ansonsten aber nicht näher definiert.

II. Vergleich zu DORA

1. Rechtliche Umsetzung

Die CER-Richtlinie umfasst in ihrer Risikobewertung die Sektoren Bankwesen und Finanzmarktinfrastruktur, wie auch NIS-2 und DORA. Auch hier greift das bereits bei NIS-2 anerkannte Spezialitätsverhältnis, DORA als lex specialis, sodass keine doppelte Inanspruchnahme bei gleichen Vorgaben erfolgt. Die CER erkennt in Artikel 8 diese

Spezialität an und nimmt das Bankwesen, die Finanzmarktstruktur und die digitale Infrastruktur von weiten Teilen der CER aus. In den Bereichen des Risikomanagements und der Meldepflichten unterliegen die betroffenen Einrichtungen somit DORA, nicht der CER.

In seiner Ausgestaltung als Richtlinie, nicht als Verordnung wie DORA, wird deutlich, dass die CER nur die Mindeststandards festlegt. Artikel 3 und Artikel 8 Satz 2 CER weisen die Mitgliedsstaaten ausdrücklich darauf hin, dass strengere nationale Regelungen erlassen werden können, wenn sie den Zielen der CER nicht zuwiderlaufen. Der Grad der Harmonisierung ist dadurch bei der CER geringer, als bei DORA.

Das Ziel der CER ist, wie auch bei DORA und bei der NIS-2, die Stärkung der Resilienz der Unternehmen in der kritischen Infrastruktur. Durch die gestiegene Digitalisierung und die höhere Vernetzung im Binnenmarkt sind die Auswirkungen von Angriffen und Ausfällen für die Bevölkerung weitgehender, als vor diesen Entwicklungen. Die Ansätze betreffen unterschiedliche Einrichtungen, die CER kann auch öffentliche Einrichtungen treffen, nicht nur privatwirtschaftliche. Der möglichst reibungslose Fortbestand der Geschäftstätigkeiten ist jedoch bei allen Betroffenen anzustreben und dafür bedarf es der umfassenden Regulierung durch die Europäische Union.

2. Methodik

Methodisch ähnelt die CER stark den Vorgaben der NIS-2, aber auch DORA. Es wird auf ein eigenverantwortliches Risikomanagement gesetzt, unterstützt durch die Behörden. Diese erhalten umfassende Befugnisse und können Maßnahmen veranlassen. Neu ist bei der CER, dass eine Zuverlässigkeitsüberprüfung einzelner Personen beantragt werden kann. Diese Möglichkeit ist in DORA nicht vorgesehen, wenn auch nicht notwendig, da dort besonders Unternehmen als Struktur im Fokus stehen.

Die Meldepflicht der CER ist etwas weniger streng als bei DORA. Sie ist nur zweistufig, im Gegensatz zum dreistufigen Modell bei DORA und damit weniger umfassend, aber auch weniger aufwändig. Die Meldung erfolgt dabei nur an die zuständige Behörde, die entsprechende Maßnahmen erlässt. Die Information der Öffentlichkeit ist sowohl

bei DORA, als auch bei der CER gegeben. Jedoch sind keine europäischen Aufsichtsbehörden in der CER involviert. Die Bandbreite der betroffenen Einrichtungen lässt dies möglicherweise auch nicht zu, trotzdem agiert hier nur der nationale Gesetzgeber und die nationale Behörde in der Umsetzung.

Im Sanktionsregime hat die CER, wie auch DORA, keine festen Vorgaben. Die Umsetzung der Höhe der Strafen obliegt den Mitgliedsstaaten. Im Gegensatz dazu hat die NIS-2-Richtlinie, ähnlich der DSGVO, sehr hohe Sanktionen festgeschrieben. Sowohl DORA, als auch die CER nehmen damit Rücksicht auf die individuelle Wirtschaftsstruktur der Mitgliedsstaaten. Eine abschreckende Wirkung kann in einzelnen Mitgliedsstaaten schon mit geringeren Beträgen erzielt werden, als in besonders wirtschaftsstarken Mitgliedsstaaten.

Die Strukturen der betroffenen Einrichtungen können einen ähnlichen Ablauf etablieren, wie bei der Umsetzung von NIS-2 und/oder DORA. Es werden klare Handlungsaufträge vergeben und Verantwortlichkeiten sind klar festzulegen und zu benennen. Eine Verantwortlichkeit der Führung ist bei der CER im Gegensatz zu DORA nicht vorgesehen.

3. Zwischenfazit

Die CER scheint im Vergleich zu DORA weniger streng und weniger genau. Dies ist der Umsetzung als Richtlinie geschuldet, spiegelt aber auch die besonders hohe Sorge um den Finanzsektor wider, der durch DORA in der Resilienz gestärkt werden soll. Während die Europäische Union auf anderen Feldern eine gewisse Toleranz hinzunehmen bereit ist, wird mit DORA die Überwachung sehr detailliert geregelt. Der Stabilität des Finanzsektors wird damit eine übergeordnete Priorität eingeräumt.

F. Schluss

Mit DORA wird eine umfassende Regulierung des Finanzsektors in der Europäischen Union erreicht, die erheblich zur Steigerung der digitalen operationalen Resilienz beiträgt. Die Vorgaben lassen den Mitgliedsstaaten trotz ihrer Ausgestaltung als Verordnung einen Spielraum, welcher jedoch nicht groß genug ist, um eine Zersplitterung des Binnenmarktes zuzulassen.

I. Fazit DORA

1. Inhalt

Die inhaltlichen Vorgaben von DORA lassen sich unterteilen in die Vorgaben für Unternehmen und ihre Managementsysteme für das IKT-Risiko, den Umgang mit IKT-bezogenen Vorfällen, das TLPT, das Management der IKT-Drittdienstleister, den Informationsaustausch sowie die Aufgaben der involvierten Behörden.

Ziele von DORA sind klar definiert und auf die gesteigerte digitale operationale Resilienz zugeschnitten. Die inhaltlichen Vorgaben dienen diesen Zielen mit unterschiedlichen Ansätzen. Sie wollen präventiv wirken, indem sie die Finanzunternehmen zu selbstständigem Handeln animieren und die Sensibilität für die Sicherheit im digitalen Raum erhöhen. Damit sind sowohl geschäftliche Strukturen, als auch menschliche Elemente gemeint. Zur Sicherstellung dieser Ziele wird auch auf Kontrollen durch die zuständigen Behörden gesetzt.

Die zuständigen Behörden sind jedoch nicht nur als übergeordnete Kontrollinstanzen zu verstehen, sondern stehen betroffenen Unternehmen unterstützend zur Seite. Dies wird durch die Erlasse der Richtlinien und Leitfäden deutlich, aber auch durch die Verbreitung von relevanten Informationen über Gefahrenquellen und IKT-bezogene Vorfälle in der Finanzbranche. Dazu kommt die Führung von Registern, beispielsweise zu IKT-Drittdienstleistern, auf welche die Unternehmen sich bei der Suche nach Geschäftspartnern stützen können.

TLPT stellt für die meisten Finanzunternehmen einen neuartigen Vorgang dar, der geeignet ist, handfeste Ergebnisse zu liefern, die über eine bloße Lagebeurteilung aufgrund von Statistiken und Leitlinien hinaus geht. Damit wird DORA in der Umsetzung deutlich stärkere Resultate erzielen, als freiwillige Überprüfungen oder behördlichen Aufsichten.

Die informationelle Verbreitung von allen Fakten, die mit dem IKT-Risikomanagement in Zusammenhang stehen, stellt Unternehmen vor die Gefahr, bei Versäumnissen der öffentlichen Meinung ausgesetzt zu sein. Viele Finanzunternehmen sind auf Kunden

aus der breiten Bevölkerung angewiesen und richten ihre Produkte auf diese aus. Die Entscheidung für ein Finanzunternehmen und gegen einen Konkurrenten wird von Verbrauchern auf persönliches Vertrauen aufbauen. Dieses kann bei einem beschädigten öffentlichen Image eines Finanzunternehmens verloren gehen, was einen Verlust an Kundschaft bedeutet und damit sogar existenzielle Bedrohungen mit sich bringen kann.

2. Praxis

DORA stellt bei der Umsetzung die Finanzunternehmen nicht nur vor die Herausforderung, wie die konkreten Maßnahmen auszusehen haben.

Einzelne Punkte von DORA bieten Interpretationsspielraum, welcher nicht nur durch die zuständigen Behörden mit Leitlinien abschließend festgelegt werden kann. Auch gerichtliche Entscheidungen werden bei einzelnen Punkten erforderliche werden und konkretisierende Wirkung entfalten. Dies spätestens dann, wenn ein IKT-bezogener Vorfall schwerwiegende Folgen mit sich bringt und Ansprüche gegen das betroffene Finanzunternehmen geltend gemacht werden. Die schnelle Entwicklung des digitalen Raumes und die wandelbaren kriminellen Energien werden immer wieder zu solchen Folgen führen, die Abwehrmaßnahmen sind Teil eines „Katz-und-Maus-Spiels“. Eine hundertprozentige Sicherheit wird kein IKT-Managementsystem bieten können, sodass sich alle Marktteilnehmer der ständigen Gefahr bewusst sein müssen.

Dazu kommt, dass die Unternehmen mit DORA umfassende Anpassungen vornehmen müssen. Dies ist nicht nur bei internen Abläufen erforderlich, sondern auch bei Beziehungen zu Dritten. In vertragsgestalterischer, aber auch prozessualer Hinsicht werden diese eine „Herkulesaufgabe“[112] sein. DORA stellt einen klassischen Ausbau der Bürokratie für die Unternehmen und die Behörden dar. Effizienz, die Risiko gegen Genauigkeit abwägt, wird durch DORA ausgehebelt. Vielmehr werden personelle Ressourcen auf die Einhaltung von DORA angesetzt werden müssen, was einen finanziellen Mehraufwand bedeutet. Der Einsatz von künstlicher Intelligenz wird in Zukunft eine gesteigerte Rolle bei der Überwachung der Einhaltung der Vorgaben aus DORA spielen. Die Einrichtung einer solchen Überwachung wird regelmäßig auch

[112] *Kreisl*, DORA *ante portas*!, ZFR 2024/252, 578, 583.

durch Drittanbieter erfolgen, welche wiederum als IKT-Drittdienstleister unter die Regulierung von DORA fallen könnten.

Die Dokumentationspflichten stellen eine weit verbreitete Maßnahme der Europäischen Union dar, welche in fast jeder Branche in Vorgaben angewendet wird und regelmäßig für Frustration bei den Betroffenen sorgt. Der wirtschaftliche Aufwand wird dabei dem Nutzen gegenübergestellt und als unverhältnismäßig angesehen. Verkannt wird dabei, dass alle Dokumentationen der Einhaltung der Vorgaben dienen und präventiv schützend wirken sollen. Die Kosten eines Schadens dem gegenüber sind regelmäßig um ein Vielfaches höher, sodass der Aufwand für Dokumentationen der angeordneten Maßnahmen die günstigere Alternative darstellt.

Wettbewerbsnachteile, die durch das Einhalten von DORA möglich wären, können nicht festgestellt werden. Der operative Ablauf eines Finanzunternehmens wird nicht beeinträchtigt. Die möglicherweise entstehenden Mehrkosten sind, wie oben dargestellt, die günstigere Alternative zu massiven, unkontrollierbaren Eingriffen in die Finanzmärkte. Damit stellt DORA als Sicherheitsmaßnahme sogar einen Vorteil gegenüber Märkten ohne eine ausgeprägte Sicherheitsarchitektur aufgrund entsprechender regulatorischer Anforderungen dar. DORA garantiert jedem Marktteilnehmer ein höchstmögliches Maß an digitaler operationaler Resilienz, welches regelmäßig an den aktuellen technischen Stand angepasst wird. Sowohl unternehmen, als auch Verbraucher, können damit bei Finanzdienstleistungen in der Europäischen Union ein besonders vertrauenswürdiges Umfeld erwarten.

II. Fazit NIS-2 und CER

Sowohl NIS-2, als auch die CER haben ähnliche Stoßrichtungen, wie DORA. Sie sind Teil der Digitalstrategie der Europäischen Kommission und sollen den Wirtschaftsraum im digitalen Zeitalter gemeinsam stärken. Auch wenn die Normen unterschiedliche Anwendungsbereiche haben, besteht die Möglichkeit, dass einzelne Unternehmen sich der Regulierung durch mehrere Normen ausgesetzt sehen. Eine Vereinfachung des Compliancemanagements wird dadurch jedoch nicht zu erreichen sein. Doppelstrukturen werden insoweit vermieden, dass Unternehmen, die unter DORA als lex specialis fallen, insoweit nicht unter NIS-2 oder CER fallen. Jedoch

können Maßnahmen nach DORA nicht automatisch Maßnahmen nach NIS-2 oder CER ersetzen und damit obsolet machen. Alle Regulierungsvorgaben um DORA herum sind vollumfänglich einzuhalten, sodass keine Synergieeffekte im Umsetzungsmanagement zwischen dem IKT-Risikomanagement aus DORA und weiteren Richtlinien zu erwarten sind.

Das durch die gesteigerte Sensibilität Vorteile bei DORA nach der Anwendung anderer Richtlinien erwachsen, ist anzunehmen. Dies hängt jedoch von der individuellen Umsetzung der Unternehmen ab. Profiteur sind nicht nur diese selbst, sondern auch Unionsbürger, die sich auf stabilere wirtschaftliche Abläufe verlassen können. Der Schutz des Finanzsektors wird insgesamt dem Vertrauen in staatliche Institutionen zugutekommen und auch das Ansehen der Europäischen Union weiter steigern. Diese darf nicht nur als Bringer von Bürokratie verstanden werden, sondern auch als Garant für Stabilität und Sicherheit, was DORA im Zusammenschluss mit NIS-2 und der CER begünstigt.

Kritisiert wird, dass DORA eine kleinschrittige Regulierung darstelle, die bei anderen Werken, NIS-2 und die CER als Beispiel, vermisst wird. Die Europäische Union solle lieber einheitliche Regulierungswerke schaffen.[113] Damit wird aber die Berücksichtigung marktspezifischer Eigenschaften der Betroffenen nicht ausreichend berücksichtigt. Außerdem würde eine gleichmäßige Regulierung verschiedener Wirtschaftszweige eine Gewichtung bei ihrer Relevanz für den Binnenmarkt und damit der Dringlichkeit einer Regulierung verhindern. Die unterschiedliche Behandlung von größeren und kleineren, abtrennbaren Gruppen von Marktteilnehmern sorgt im Gesamtbild für eine hohe Resilienz dort, wo es zwingend erforderlich ist. Andere Marktteilnehmer hingegen können flexibleren Regelungen und landestypischen Gegebenheiten unterworfen bleiben.

Weitere Regulierungswerke, die auch Teil der Digitalstrategie der Europäischen Kommission sind, werden aufgrund ihres Umfangs und des zu begrenzenden Umfangs dieser Arbeit nicht untersucht. Die Datenschutzgrundverordnung[114] stellt

[113] *Siglmüller*, Cyber Resilience Act und Digital Operational Resilience Act - Lässt sich IT-Sicherheit rechtlich erzwingen? ZfPC 2023, 221, 221.
[114] Verordnung (EU) 2016/67.

beispielsweise ein bekanntes Regulierungswerk dar, welches öffentlich deutlich weitgehender kritisiert wird und einen spürbaren Einfluss auf den Alltag zu haben scheint. Sie steht im Gegensatz zu NIS-2 und CER aber deutlich selbstständiger neben DORA, was bei einem direkten Vergleich wenige Gemeinsamkeiten ergeben würde.

III. Gesamtwürdigung

Mit DORA nimmt sich die Europäische Union zusammen mit weiteren Regulierungswerken der Realität an. Die Bedrohungslage im digitalen Raum wird durch kriminelle und auch staatliche Akteure auf absehbare Zeit nicht sinken. Privatwirtschaftliches Engagement, aber auch öffentliche Einrichtungen werden weiterhin das Ziel von Angriffen bleiben. Besonders der Finanzsektor stellt ein lohnendes Ziel dar, um das Vertrauen der staatlichen Strukturen zu unterminieren und wirtschaftliches Handeln zu erliegen zu bringen. DORA bietet sehr konkrete Ansätze, die digitale operationale Resilienz dieses Bereichs zu stärken und damit das Risiko von Totalausfällen, aber auch kleineren IKT-bezogenen Vorfällen, zu senken. Diese Sicherheit hat ihren Preis im Aufwand, das Vorgehen ist jedoch alternativlos.

Die Einheitlichkeit, die durch DORA geschaffen wird, ist Ausdruck des Glaubens an die europäische Idee mit ihrem gemeinsamen Binnenmarkt. Unterstützt wird die Einheitlichkeit, wenn auch in geringerem Maße, durch die NIS-2 und die CER. Nur wenn alle Märkte der Mitgliedsstaaten gleichermaßen geschützt sind, entsteht kein Einfalltor für bösartige Akteure, das für die gesamte europäische Gemeinschaft zur unkontrollierbaren Gefahr werden würde. Weiterhin müssen die Vorgaben aus DORA, insbesondere die Leitlinien und weitere Empfehlungen der europäischen und der nationalen Behörden, regelmäßig auf ihre Aktualität überprüft werden und bei Bedarf umfangreich angepasst werden. Neue Angriffswege werden immer wieder entdeckt und ausgenutzt werden, sodass DORA keinen einmal zu erreichenden Rechtszustand darstellt, sondern einen kontinuierlichen Prozess, der für weitere Regulierungsmaßnahmen als Vorbild genommen werden kann.