Martina Isabelle Lipke

EU-weite regulatorische Vorgaben im Bereich der Digitalisierung für Finanzunternehmen

Implikationen des Digital Operational Resilience Act, der Financial Data Access Regulation und des AI Act

Cuvillier Verlag Göttingen
Internationaler wissenschaftlicher Fachverlag

EU-weite regulatorische Vorgaben im Bereich der Digitalisierung für Finanzunternehmen

Implikationen des Digital Operational Resilience Act, der Financial Data Access Regulation und des AI Act

EU-weite regulatorische Vorgaben im Bereich der Digitalisierung für Finanzunternehmen

Implikationen des Digital Operational Resilience Act, der Financial Data Access Regulation und des AI Act

von

Martina Isabelle Lipke

Impressum
Titel des Werkes: EU-weite regulatorische Vorgaben im Bereich der Digitalisierung für Finanzunternehmen –Implikationen des Digital Operational Resilience Act, der Financial Data Access Regulation und des AI Act
Autor/in: Martina Isabelle Lipke
Cuvillier Verlag GmbH
Nonnenstieg 8
37075 Göttingen
Telefon: 0049-551-547240
Webseite: www.cuvillier.de
E-Mail: info@cuvillier.de

Bibliografische Informationen der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

1. Auflage, Göttingen. 2026

Gedruckt auf umweltfreundlichem, säurefreiem Papier aus nachhaltiger Forstwirtschaft.

ISBN 978-3-68952-466-1
eISBN 978-3-68952-467-8
ORCID 0009-0005-5326-7344
DOI 10.61061/ISBN_9783689524661

Vorwort

Diese Masterarbeit ist im Studiengang Informationsrecht (LL.M.) an der Carl von Ossietzky Universität Oldenburg entstanden und befasst sich mit den EU-weiten regulatorischen Vorgaben im Bereich der Digitalisierung für Finanzunternehmen, insbesondere den Implikationen des Digital Operational Resilience Act (DORA), der Financial Data Access Regulation (FIDA-E) und des AI Act.

Mein besonderer Dank gilt meiner Erstgutachterin Prof. Dr. Sarah Rachut sowie meinem Zweitkorrektor Prof. em. Dr. Bernd Holznagel für ihre wertvolle Unterstützung.

Ebenso danke ich dem Studiengang Informationsrecht für die hervorragende fachliche Grundlage und das inspirierende Umfeld, das maßgeblich zur Ausarbeitung dieser Arbeit beigetragen hat.

Frankfurt am Main, Februar 2026

Martina Isabelle Lipke

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Bedeutung
AI Act	EU-Verordnung zur Regulierung von Künstlicher Intelligenz
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAIT	Bankaufsichtliche Anforderungen an die IT
BCM	Business Continuity Management
BNetzA	Bundesnetzagentur
DOR	Digital Operational Resilience
DORA	Digital Operational Resilience Act
DSGVO	Datenschutz-Grundverordnung
EBA	European Banking Authority
EIOPA	European Insurance and Occupational Pensions Authority
ESA	European Supervisory Authorities (EBA, EIOPA, ESMA)
ESG	Environmental, Social and Governance
ESMA	European Securities and Markets Authority
ErwG	Erwägungsgrund
EU	Europäische Union
EZB	Europäische Zentralbank
FDSS	Financial Data Sharing Schemes
FIDA	Financial Data Access Regulation

FIDA-E	Entwurf der Financial Data Access Regulation
FinmadiG	Finanzmarktdigitalisierungsgesetz
FISP	Financial Information Service Provider
GPAI	General-Purpose AI
GwG	Geldwäschegesetz
IKT	Informations- und Kommunikationstechnologie
ISB	Informationssicherheitsbeauftragter
ITS	Implementing Technical Standard
KAIT	Kapitalverwaltungsaufsichtliche Anforderungen an die IT
KMU	Kleine und mittlere Unternehmen
KWG	Kreditwesengesetz
LLM	Large Language Model
MaRisk	Mindestanforderungen an das Risikomanagement
MiCA	Markets in Crypto-Assets Regulation
ML	Maschinelles Lernen
MÜVO	Verordnung über Marktüberwachung und die Konformität von Produkten
PSD	Payment Services Directive
PSR	Payment Services Regulation
RPA	Robotic Process Automation bzw. robotergesteuerte Prozessautomatisierung
RTS	Regulatory Technical Standard
RTS RMF	RTS zur Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und des vereinfachten IKT-Risikomanagementrahmens

RTS SUB	RTS zur Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen
RTS TPPol	RTS zur Spezifizierung des detaillierten Inhalts der Leitlinie für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden
TLPT	Threat-led Penetration Testing
VAIT	Versicherungsaufsichtliche Anforderungen an die IT
xAIT	Zusammenfassend für BAIT, ZAIT, VAIT und KAIT
ZAG	Zahlungsdiensteaufsichtsgesetz
ZAIT	Zahlungsdiensteaufsichtliche Anforderungen an die IT

1. Einleitung

Die Digitalisierung hat in den letzten Jahren auch vor der Finanzbranche keinen Halt gemacht. Mit der zunehmenden Abhängigkeit von digitalen Technologien und den damit verbundenen Cyberrisiken ist die Notwendigkeit von robusten regulatorischen Rahmenbedingungen unerlässlich geworden. Die Europäische Kommission hat hierauf mit verschiedenen Regulierungen reagiert, darunter der Digital Operational Resilience Act (im Folgenden: DORA), der Entwurf der Financial Data Access Regulation (im Folgenden: FIDA-E) und der AI Act. Im Gegensatz zu DORA und FIDA-E sind die Adressaten des AI Act nicht nur Finanzunternehmen. Dennoch enthält der AI Act einige gesonderte Regelungen für Finanzinstitute und ist daher Gegenstand dieser Masterarbeit. Die aufgezählten Regulierungen zielen darauf ab, die digitale Resilienz, den offenen Zugang zu Finanzdaten und die verantwortungsvolle Nutzung von Künstlicher Intelligenz (im Folgenden: KI) in Finanzunternehmen zu gewährleisten, und stellen diese vor die Herausforderung, zahlreiche neue Vorgaben umzusetzen und im Zuge dessen gegebenenfalls sogar neue organisatorische Strukturen zu schaffen.

1.1 Hintergrund und Relevanz der EU-weiten regulatorischen Vorgaben im Bereich der Digitalisierung für Finanzunternehmen

1.1.1 Digital Operational Resilience Act

DORA zielt darauf ab, die digitale Widerstandsfähigkeit von Finanzunternehmen zu stärken. Die Verordnung legt u. a. Anforderungen an das Risikomanagement, die Meldung von Vorfällen und die Prüfung der digitalen operationalen Resilienz fest. Ziel ist es, sicherzustellen, dass Finanzunternehmen in der Lage sind, ihre Dienstleistungen auch bei erheblichen Störungen der Informations- und Kommunikationstechnologie (im Folgenden: IKT) aufrechtzuerhalten.

1.1.2 Financial Data Access Regulation

Der Entwurf zu FIDA stellt einen Schritt in Richtung Open-Finance dar und schafft einen Rahmen für den verantwortungsvollen Zugang zu Daten von Einzel- und Geschäftskunden über eine breite Palette von Finanzdienstleistungen hinweg. Der vorgeschlagene Rahmen zielt darauf ab, einen sicheren und offenen Zugang zu Kundendaten zu gewährleisten, und stellt dabei die Interessen der Verbraucher, den Wettbewerb und die Datensicherheit in den Mittelpunkt. FIDA-E baut auf dem bereits bestehenden Open Banking-Ansatz der EU auf und

erweitert diesen um eine breitere Palette von Finanzdienstleistungen.

1.1.3 AI Act

Der AI Act zielt darauf ab, die Entwicklung und Nutzung von KI in der EU zu regulieren. Er legt Anforderungen an die Transparenz, Sicherheit und ethische Nutzung von KI-Systemen fest. Der AI Act soll sicherstellen, dass KI-Modell und -Systeme sicher und vertrauenswürdig konzipiert und genutzt werden und keine diskriminierenden oder schädlichen Auswirkungen haben.

Zusammen bilden diese Regulierungen einen Rahmen, der die digitale Transformation der Finanzbranche unterstützen und gleichzeitig die Sicherheit, Resilienz und ethische Nutzung digitaler Technologien gewährleisten soll. Sie sollen nicht nur sicherstellen, dass Finanzunternehmen in der Lage sind, digitale Technologien effektiv zu nutzen, sondern auch, dass diese Technologien sicher und im besten Interesse der Verbraucher eingesetzt werden.

1.2 Fragestellungen und Zielsetzung

Das Ziel dieser Masterarbeit ist es, die Implikationen der drei im Fokus stehenden EU-weiten regulatorischen Vorgaben für Finanzunternehmen zu untersuchen. Dabei sollen insbesondere die folgenden Fragestellungen beantwortet werden:

1. Welche Anforderungen stellen DORA, FIDA-E und der AI Act an Finanzunternehmen?

2. Welche Auswirkungen haben diese Regulierungen auf die digitale Resilienz und den Datenzugang in der Finanzbranche?

3. Welche Herausforderungen und Chancen ergeben sich aus der Implementierung dieser Regulierungen für Finanzunternehmen?

1.3 Hypothesen

Hypothese 1: DORA erhöht die digitale Resilienz von Finanzunternehmen, indem es strenge Anforderungen an das Risikomanagement und die Meldung von Vorfällen stellt.

Hypothese 2: FIDA-E fördert die Innovation und den Wettbewerb im Finanzsektor durch den sicheren und offenen Zugang zu Kundendaten, während gleichzeitig die Kontrolle und der Schutz der Daten durch die Verbraucher gewährleistet wird.

Hypothese 3: Der AI Act stellt sicher, dass KI-Systeme in der Finanzbranche sicher, transparent und ethisch genutzt werden, was das Vertrauen der Verbraucher in diese Technologien stärkt.

Hypothese 4: Einige in den Verordnungen enthaltene Regelungen bestanden schon nach der bisherigen Rechtslage bzw. in vergleichbaren Gesetzen und basieren auf allgemeinen Prinzipien, die sich in den Verordnungen überschneiden. Durch entsprechende Synergien können bei der Umsetzung der Vorgaben mehrere Ziele auf einmal erreicht werden.

Hypothese 5: Im Zuge der Umsetzung der Vorgaben werden in den Unternehmen neue organisatorische Bereiche und Stellen geschaffen werden müssen. Auch in dieser Hinsicht sind Synergien möglich, sofern keine Interessenkonflikte bestehen.

Hypothese 6: Die Umsetzung der Vorgaben bindet Ressourcen und ist mit hohen Kosten verbunden. Die aktuelle angeschlagene Wirtschaftslage erschwert die Umsetzung und führt zu Frustrationen bei allen Adressaten der Regulierungen.

2. Digitalisierung und ihre Regulierung in der Finanzbranche

2.1 Überblick über die Digitalisierung in der Finanzbranche

Die Digitalisierung ist seit vielen Jahren in der Finanzbranche ein zentrales Thema. Ähnlich wie in anderen Branchen versprechen sich auch die Finanzmarktakteure durch den Einsatz von neuen Technologien nicht nur die Schaffung innovativer und effektiver Geschäftsmodelle, sondern auch die Erleichterung unternehmensinterner (administrativer) Arbeit.

2.1.1 Einsatz Künstlicher Intelligenz

Im Finanzsektor wird zunehmend KI, insbesondere generative KI, eingesetzt, wobei sich laut dem Bericht zu Risiken im Fokus 2025 der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)[1] viele Initiativen noch in der Testphase befinden. Dem Bericht zufolge werden vor allem große Sprachmodelle (LLM) als Unterstützungssysteme genutzt, beispielsweise in Form von internen Chatbots und Dokumentenbearbeitungssystemen. Ebenso sollen KI-basierte Chatbots vermehrt im Kundenkontakt eingesetzt werden.

---

[1] „Risiken im Fokus der BaFin 2025“, https://www.bafin.de/ref/19792518 (zuletzt abgerufen am 29.05.2025).

Traditionellere Formen der KI und des Maschinellen Lernens (ML) werden laut der BaFin bereits von Banken und Versicherungen zur Erkennung von Geldwäsche und Betrug sowie in Backoffice-Prozessen eingesetzt, wie etwa in der Dunkelverarbeitung von Versicherungsleistungen. Im Risikomanagement kommen KI und ML zunehmend zur Datenaufbereitung und Validierung von Risikomodellen zum Einsatz. In der Wertpapierbranche dienen sie vor allem der Optimierung von Prozessen im algorithmischen Handel, in der Anlageberatung, im Risikomanagement und im Bereich Compliance.[2]

2.1.2 Open Finance / Austausch von Finanzdaten

Eine grundlegende Bedeutung haben nach wie vor Daten. Sie stellen die Basis für die Digitalisierung dar. Die Förderung der Integration und des Austauschs von Finanzdaten zwischen verschiedenen Dienstleistern im Rahmen der sog. Open-Finance-Initiative soll die Entwicklung innovativer, datenbasierter Dienstleistungen stärken, die insbesondere den Kunden zugutekommen sollen. So soll es Dienstleistern durch einen umfassenderen Zugang zu Finanzdaten ermöglicht werden beispielsweise den Kunden zu helfen, ihre Kredite besser zu verwalten, indem sie Übersichten über alle Kredite und Hinweise auf günstigere Produkte bereitstellen.[3]

---

[2] „Risiken im Fokus der BaFin 2025, a.a.O.; Möslein/Omlor: Digitalisierung der Finanzmärkte, ZRP 2025, 44 (46).

[3] Europäische Kommission, Financial data access and payments package, Juni 2023, https://finance.ec.europa.eu/publications/financial-data-access-and-payments-package_en (zuletzt abgerufen am 29.05.2025);

2.1.3 Digitaler Zahlungsverkehr

Die Weiterführung der Digitalisierung des Zahlungsverkehrs beschäftigt vor allem Zahlungs- und E-Geldinstitute. Der Markt für Massenzahlungsdienste hat sich nach den Erwägungsgründen des Entwurfs der EU-Zahlungsdiensterichtlinie PSD3 durch die zunehmende Nutzung von Karten und anderen digitalen Zahlungsmitteln, die abnehmende Verwendung von Bargeld und die zunehmende Präsenz neuer Akteure und Dienste, einschließlich digitaler Brieftaschen und kontaktloser Zahlungen, erheblich verändert. Treiber dieser Entwicklung waren insbesondere die COVID-19-Pandemie und der damit einhergehende Wandel im Hinblick auf Konsum- und Zahlungspraktiken, die dazu geführt haben, dass sichere und effiziente digitale Zahlungen immer wichtiger geworden sind.[4]

2.1.4 Digitaler Euro

Der verstärkt digitale Zahlungsverkehr beschäftigt auch die Europäische Zentralbank (EZB). Sie plant die Einführung des digitalen Euro. Der digitale Euro soll die digitale Form von Bargeld darstellen, die für alle digitalen Zahlungen im Euroraum genutzt werden kann. Ziel ist, dass er allgemein

---

Dreisigacker-Sartor/Ritter-Döring: Mit FIDA von Open Banking zu Open Finance, RdZ 2024, 5 (7); Möslein/Omlor: Digitalisierung der Finanzmärkte, ZRP 2025, 44 (45).

[4] ErwG 1 des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste und E-Geld-Dienste im Binnenmarkt, zur Änderung der Richtlinie 98/26/EG und zur Aufhebung der Richtlinien (EU) 2015/2366 und 2009/110/EG, 2023/0209 (COD).

zugänglich, sowohl online als auch offline verfügbar, und die grundlegende Nutzung kostenlos ist.[5]

Der digitale Euro soll den Euroraum stärken, die strategische Autonomie und geldpolitische Souveränität Europas unterstützen und die Wettbewerbsfähigkeit der europäischen Zahlungsverkehrslandschaft gegenüber nicht-europäischen Zahlungsdienstleistern erhöhen. Zudem soll er die Grundlage für weitere Innovationen privater Zahlungsdienstleister schaffen.[6] Derzeit werden verschiedene Ansätze und Technologien in der Entwicklung eines digitalen Euro analysiert, wobei noch keine Entscheidung für ein Produktivsystem getroffen wurde.[7] Die EU entwickelt zudem einen Rechtsrahmen für den digitalen Euro, dessen Gesetzesentwurf 2023 von der EU-Kommission vorgelegt wurde.[8] Der Entwurf befindet sich weiterhin im Gesetzgebungsverfahren.[9]

---

[5] Deutsche Bundesbank, https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/digitaler-euro/stand-der-dinge/stand-der-dinge-903502 (zuletzt abgerufen am 01.06.2025).

[6] Deutsche Bundesbank, FAQ zum digitalen Euro, https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/digitaler-euro/faq-digitaler-euro (zuletzt abgerufen am 01.06.2025).

[7] Deutsche Bundesbank, FAQ, a.a.O.

[8] Deutsche Bundesbank, FAQ, a.a.O.

[9] Möslein/Omlor: Digitalisierung der Finanzmärkte, ZRP 2025, 44 (46).

2.1.5 Kryptowährungen

Die Popularität von Kryptowährungen und Blockchain-Technologien ist exponentiell gestiegen. Bei Kryptowerten handelt es sich um digitale Darstellungen von Werten oder Rechten, die unter Verwendung der sog. Distributed-Ledger-Technologie oder einer ähnlichen Technologie elektronisch übertragen und gespeichert werden können.[10] Kryptowährungen bieten innovative Möglichkeiten für neue Geschäftsmodelle und Wirtschaftstätigkeiten, und dienen vor allem kleinen und mittleren Unternehmen (KMU) als alternative Finanzierungsquellen. Zudem können sie als Zahlungsmittel grenzüberschreitende Transaktionen kostengünstiger und schneller gestalten, da die Anzahl der Intermediäre begrenzt wird.[11] Unter den mittlerweile zahlreichen Kryptowährungen ist die wohl bekannteste Kryptowährung der Bitcoin.[12]

Laut der BaFin beruhen alle Kryptowerte auf einer neuartigen Technologie, die durch die bestehenden regulatorischen und rechtlichen Vorgaben noch nicht vollständig abgebildet

---

[10] Art. 3 Abs. 1 Nr. 5 der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 (MiCA).

[11] ErwG 2 MiCA.

[12] Niedernhuber in: Wabnitz/Janovsky/Schmitt WirtschaftsStrafR-HdB, 6. Aufl. 2025, 16. Kap. Rn. 21.

wird und daher risikobehaftet ist, insbesondere in Zusammenhang mit drohenden Hacker-Angriffen.[13] Erste einheitliche Aufsichts- und Marktstandards bezüglich Kryptowerten für Primär- wie Sekundärmärkte wurden mit der EU-Verordnung über Märkte für Kryptowerte (MiCA) geschaffen.[14]

Die Digitalisierung in der Finanzbranche bringt zahlreiche Themen und Herausforderungen mit sich, denen mit gezielter Regulierung begegnet werden kann. Die bestehenden und geplanten Regelungen, wie MiCA, FIDA-E, der AI Act, PSD3 und DORA stellen Schritte dar, um die Chancen der Digitalisierung zu nutzen und gleichzeitig die Stabilität und Sicherheit der Finanzmärkte zu gewährleisten. Die Harmonisierung dieser Regelungen auf nationaler und europäischer Ebene soll einen effektiven und wettbewerbsfähigen Finanzmarkt schaffen. Um den Rahmen nicht zu sprengen, beschränkt sich diese Arbeit im Folgenden auf die Regulierungen DORA, FIDA-E und den AI Act.

[13] BaFin, Entwurf eines Rundschreibens 2025 zu Pflichten von Verwahrstelle und Kapitalverwaltungsgesellschaft bei in Kryptowerte investierenden Investmentvermögen, I. Präambel/Einleitung, Ziff. 2.
[14] Möslein/Omlor, ZRP 2025, 44.

2.2 Vorstellung der Regulierungen DORA, AI Act und FIDA-E

2.2.1 Die Verordnungen als Ausprägungen der EU-Digitalstrategie

Die Digitalstrategie der EU, wie sie in der Mitteilung der EU-Kommission vom 9. März 2012[15] dargelegt ist, verfolgt das Ziel, Europa in die digitale Dekade zu führen und eine digitale Gesellschaft zu schaffen, die Menschen und Unternehmen in ihrer Handlungskompetenz stärkt, damit sie sich die Chancen einer auf den Menschen ausgerichteten, nachhaltigen und florierenden digitalen Zukunft zunutze machen können. Diese Strategie ist im Digitalen Kompass 2030 verankert und basiert auf vier Kernpunkten, die die digitale Transformation in der EU leiten sollen. Einer dieser Kernpunkte beinhaltet den digitalen Umbau von Unternehmen.[16] Danach sollen bis 2030 75 % der europäischen Unternehmen Cloud-Computing-Dienste, Big Data und KI nutzen und über 90 % der KMU sollen eine grundlegende digitale Intensität erreichen.

Ein weiterer Teil der Digitalstrategie ist das Paket zur Digitalisierung des Finanzsektors, das die EU-Kommission bereits

---

[15] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen v. 9.3.2021, COM (2021) 118 final, Digitaler Kompass 2030: der europäische Weg in die digitale Dekade (im Folgenden: Digitaler Kompass 2030).

[16] Ziff. 3.3 Digitaler Kompass 2030.

2020 angenommen hat.[17] Mit dem Paket sollen im EU-Raum die Wettbewerbsfähigkeit und Innovationen im Finanzsektor gefördert werden, Verbraucherinnen und Verbraucher sowie Unternehmen eine größere Auswahl an Finanzdienstleistungen und modernen Zahlungslösungen erhalten und sowohl Verbraucherschutz als auch Finanzstabilität gewährleistet werden. Das Paket umfasst neben Strategien für ein digitales Finanzwesen und für den Massenzahlungsverkehr Gesetzgebungsvorschläge zu Kryptowerten (MiCA) und zur Stabilität digitaler Systeme (DORA).[18]

DORA, FIDA-E und der AI Act sind maßgebende Regulierungen für die Finanzbranche im Rahmen der Umsetzung der Digitalstrategie der EU, da sie die Rahmenbedingungen schaffen, um die digitale Transformation im Finanzsektor zu unterstützen und gleichzeitig die Sicherheit, Transparenz und ethischen Standards zu gewährleisten, die für das Vertrauen der EU-Bürger in digitale Technologien von großer Bedeutung sind. Sie sind Teil eines umfassenden Ansatzes, der darauf abzielt, Europa als führenden Akteur in der digitalen Welt zu positionieren und eine nachhaltige und resiliente digitale Gesellschaft zu fördern.

---

[17] Europäischer Rat zum Digitalen Finanzwesen, https://www.consilium.europa.eu/de/policies/digital-finance/#strategy (zuletzt abgerufen am 18.07.2025).

[18] Europäischer Rat zum Digitalen Finanzwesen, a.a.O.

2.2.2 Digital Operational Resilience Act

2.2.2.1 Hintergrund

DORA ist seit dem 16. Januar 2023 in Kraft und gilt seit dem 17. Januar 2025.[19] Unabhängig von der Digitalstrategie der EU ist der Einsatz von Informations- und Kommunikationstechnologien heutzutage fester Bestandteil des Betriebs komplexer Systeme und hat eine essenzielle Bedeutung für die Stabilität des Finanzsektors. Die fortschreitende Digitalisierung hat zu einer stärkeren Vernetzung und Abhängigkeit von IKT-Systemen geführt, was das Risiko von Cyberbedrohungen und Störungen erhöht. Besonders die Finanzbranche ist gefährdet, da IKT-Vorfälle schnell auf das gesamte System ausstrahlen können.[20]

Trotz der bisherigen Anstrengungen von internationalen und nationalen Regulierungsbehörden zur Stärkung der digitalen Resilienz bleibt das IKT-Risiko eine Herausforderung für die operationale Stabilität des Finanzsektors. Die EU hat verschiedene Maßnahmen ergriffen, um die digitale operationale Resilienz zu verbessern, jedoch mangelte es laut ErwG 9 DORA bislang an einer einheitlichen Harmonisierung der

[19] Art. 64 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (DORA).
[20] ErwG 1 DORA.

Vorschriften. Unterschiedliche nationale Ansätze würden Hindernisse für den Binnenmarkt schaffen und die grenzüberschreitenden Aktivitäten von Finanzunternehmen erschweren.[21]

DORA hat das Ziel, diese Lücken zu schließen und einen einheitlichen Rahmen für das IKT-Risikomanagement zu etablieren, um die Stabilität und Integrität des Finanzmarktes zu sichern und das Vertrauen von Anlegern und Verbrauchern zu stärken.[22]

2.2.2.2 Adressaten und zuständige Aufsicht

Adressaten der Verordnung sind zum einen nach Art. 2 Abs. 1 lit. a bis t DORA Finanzunternehmen, wie beispielsweise Banken und Versicherungen, E-Geldinstitute, Wertpapierfirmen sowie größere Versicherungsvermittler, und zum anderen nach Art. 2 Abs. 1 lit. u DORA IKT-Drittdienstleister, also Unternehmen, die IKT-Dienstleistungen für Finanzunternehmen bereitstellen.[23] Zu IKT-Dienstleistungen zählen laut der Definition in Art. 3 Nr. 21 DORA digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung

---

[21] ErwG 4 ff. DORA

[22] ErwG 11 f. DORA.

[23] Zum zweiseitigen personellen Anwendungsbereich siehe auch Siglmüller, ZfPC 2023, 221 (223).

durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste.

Der Großteil der Verpflichtungen nach DORA richtet sich an die Finanzunternehmen. Die IKT-Drittdienstleister werden lediglich in Art. 30 DORA in Zusammenhang mit den wesentlichen Vertragsbestimmungen in Hinblick auf vertragliche Vereinbarungen zwischen Finanzunternehmen und IKT-Drittdienstleistern direkt angesprochen.

Den Europäischen Aufsichtsbehörden (European Supervisory Authorities, im Folgenden ESAs) obliegt es nach Art. 31 Abs. 1 lit. a DORA zu bestimmen, welche IKT-Drittdienstleister als kritisch einzustufen sind. Kritisch sind solche IKT-Dienstleister, von denen verstärkt IKT-Risiken ausgehen. Jene kritischen IKT-Drittdienstleister unterliegen nach Art. 33 Abs. 1 und 2 DORA der direkten Überwachung der ESA, die als federführende Überwachungsbehörde nach Art. 31 Abs. 1 lit. b DORA ernannt wird. Die federführende Überwachungsbehörde wird die Aufgabe haben, Prüfungen vor Ort durchzuführen und Handlungsempfehlungen an die kritischen IKT-Dienstleister abzugeben.

Die Ermittlung der kritischen IKT-Drittdienstleister nehmen die ESAs anhand der Auswertung der durch die Finanzunternehmen übermittelten Informationsregister vor. Gemäß ErwG 65 DORA sind die Finanzunternehmen verpflichtet, ein Informationsregister (Art. 28 Abs. 3 DORA) mit allen vertraglichen Vereinbarungen betreffend die Nutzung von IKT-

Dienstleistungen, die von IKT-Drittdienstleistern bereitgestellt werden, zu führen. Finanzunternehmen müssen auf Grundlage von Art. 28 Abs. 3 UAbs. 4 DORA jährlich ihre Informationsregister an ihre zuständige Aufsichtsbehörde übermitteln.[24] Neben der gesetzlichen Verpflichtung nach Art. 30 DORA zur Integrierung gewisser Mindestvertragsinhalte erhöht das Vorgehen zur Ermittlung und Überwachung den Druck bei kritischen IKT-Drittdienstleistern, die sie betreffenden DORA-Vorgaben tatsächlich umzusetzen.

Auf EU-Ebene bilden die European Banking Authority (EBA), die European Securities and Markets Authority (ESMA) sowie die European Insurance and Occupational Pensions Authority (EIOPA) die zuständige Aufsicht (zusammen ESAs). Diese sind beispielsweise nach Art. 19 Abs. 6 lit. a DORA bei schwerwiegenden IKT-bezogenen Vorfällen durch die national zuständigen Behörden zu informieren. In Deutschland sind die BaFin sowie die Deutsche Bundesbank die maßgeblichen nationalen Aufsichtsbehörden für Finanzunternehmen, die laut Finanzmarktdigitalisierungsgesetz (FinmadiG) mit Befugnissen rund um die Einhaltung der DORA-Vorgaben ausgestattet sind.[25]

---

[24] BaFin, Informationsregister und Anzeigepflichten, Stand 01.07.2025, https://www.bafin.de/DE/Aufsicht/DORA/Informationsregister_und_Anzeigepflichten/Informationsregister_und_Anzeigepflichten_node.html (zuletzt abgerufen am 20.07.2025).

[25] Beispielsweise nach dem durch das FinmadiG neu eingeführten § 47a KWG; Art. 3 Nr. 1 lit. c FinmadiG, Bundesgesetzblatt Jahrgang 2024 Teil I Nr. 438.

2.2.2.3 Kritische oder wichtige Funktionen

Um den Einstieg in die Verordnung zu erleichtern, sollte man sich zunächst mit dem zentralen Begriff der *kritischen oder wichtigen Funktion* befassen, da sich dieser immer wieder durch DORA zieht. Nach Art. 3 Nr. 22 DORA ist unter „kritische oder wichtige Funktion“ eine Funktion zu verstehen, deren Ausfall die finanzielle Leistungsfähigkeit eines Finanzunternehmens oder die Solidität oder Fortführung seiner Geschäftstätigkeiten und Dienstleistungen erheblich beeinträchtigen würde oder deren unterbrochene, fehlerhafte oder unterbliebene Leistung die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen eines Finanzunternehmens oder seiner sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht erheblich beeinträchtigen würde.

Bei der Bewertung von Funktionen als kritisch oder wichtig ist zu beachten, dass diese methodisch und inhaltlich nicht deckungsgleich mit einer Wesentlichkeitsbestimmung bei Auslagerungen ist.[26] Im deutschen Auslagerungsregulierungsregime wird beispielsweise nach § 25b KWG oder § 26 ZAG zwischen (wesentlicher) Auslagerung und sonstigem Fremdbezug von IT-Dienstleistungen unterschieden. Diese Regelungen werden neben DORA auch weiterhin gelten.[27]

---

[26] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 6.1.

[27] Bernau/Lutterbach, BKR 2023, 506 (508).

Allerdings haben Finanzunternehmen nun zu beachten, dass nicht nur hinsichtlich Dienstleistungen, die bisher zu den (wesentlichen) Auslagerungen zählten, strenge regulatorische Vertragsanforderungen zu erfüllen sind, sondern auch hinsichtlich solcher Dienstleistungen, die bislang unter den Begriff des *sonstigen Fremdbezugs* von IT-Dienstleistungen fielen.[28]

Daher ist es für Finanzunternehmen notwendig, eigene geeigneten Kriterien zur Einstufung der Kritikalität zu entwickeln.[29] Zu der Festlegung einer entsprechenden Methode sind Finanzunternehmen auch nach Art. 3 Abs. 2 der Delegierten Verordnung zur Spezifizierung des detaillierten Inhalts der Leitlinie für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden (im Folgenden: RTS TPPol)[30], verpflichtet.

[28] Bernau/Lutterbach, aaO; BaFin-Präsentation „DORA für IKT-Drittdienstleister“ vom 29. Februar 2024, 21.

[29] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 6.1.

[30] Delegierte Verordnung (EU) 2024/1773.

2.2.2.4 IKT-Risikomanagement

Die Anforderungen an das IKT-Risikomanagement innerhalb eines Finanzunternehmens sind in den Artt. 5 bis 16 DORA geregelt.

Bereits vor der Einführung von DORA waren deutsche Finanzunternehmen verpflichtet, aufsichtliche Anforderungen an die IT zu erfüllen, nämlich nach den bank-, zahlungsdienste-, versicherungs- und kapitalverwaltungsaufsichtlichen Anforderungen an die IT (BAIT, ZAIT, VAIT und KAIT, zusammen im Folgenden: xAIT).[31] Die xAIT kamen in der Form von BaFin-Rundschreiben daher und stellten einen praxisnahen Rahmen für die technisch-organisatorische Ausstattung der Finanzunternehmen, insbesondere für das Management der IT-Ressourcen, das IT-Risikomanagement und das IT-Sicherheitsmanagement, dar.[32] Wie die Mindestanforderungen an das Risikomanagement (MaRisk) dienten die xAIT als Interpretationsleitfäden, erleichterten die Auslegung unbestimmter Rechtsbegriffe von gesetzlichen Normen

[31] Bomhard/Siglmüller in: Hornung/Schallbruch, IT-Sicherheitsrecht, § 29 IT-Sicherheitsrecht im Finanzsektor Rn. 91.

[32] Deutsche Bundesbank, BAIT / DORA – Aufsichtliche Anforderungen an die IT und die digitale operationale Resilienz, https://www.bundesbank.de/de/aufgaben/bankenaufsicht/einzelaspekte/risikomanagement/bait-dora-598580 (zuletzt abgerufen am 19.06.2025).

und stellten gleichzeitig die Umsetzung internationaler, europarechtlicher wie nationaler Normen[33] dar, hatten dabei jedoch selbst keinen eigenen Rechtsnormcharakter.[34] Als EU-Verordnung findet DORA seit Anfang 2025 unmittelbare Anwendung in Deutschland, mit eigenem Rechtsnormcharakter und mit einer Ausweitung der Anforderungen an die IT auf Informations- und Kommunikationstechnologien. Um eine Doppelregulierung zu vermeiden, hat die BaFin die ZAIT, VAIT und KAIT mit Ablauf des 16. Januar 2025 aufgehoben. Die BAIT werden mit Ablauf des 31. Dezember 2026 vollständig aufgehoben.[35]

Die Frage, ob zukünftig IKT-Risiken oder Informationssicherheit im Fokus der Aufsichtsbehörden stehen, beantwortet die BaFin damit, dass DORA sich auf die Governance des IKT-Risikomanagementrahmens konzentriert, während der Fokus der xAIT auf der Informationssicherheit und damit verbundenen Anforderungen liegt. Diese Akzentverschiebung von der reinen Informationssicherheit hin zum IKT-Risikomanagement stelle eine bedeutende Entwicklung dar, die sowohl Herausforderungen als auch Erleichterungen mit sich bringen würde. DORA enthalte spezifische Anforderungen an eine Richtlinie zur IKT-Sicherheit, die in den xAIT nicht

---

33 Bernau/Lutterbach, BKR 2023, 506 (mwN).

34 Krimphove: Die „neue“ MaRisk (BA) 9/201, BKR 2018, 1 (4).

35 Deutsche Bundesbank, BAIT / DORA – Aufsichtliche Anforderungen an die IT und die digitale operationale Resilienz, a.a.O.

direkt vorhanden seien. Es gebe zwar inhaltliche und kontextbezogene Schnittmengen, Anpassungen würden aber unumgänglich sein.[36]

Aufgaben des Leitungsorgans

Das Leitungsorgan eines Finanzunternehmens muss gemäß Art. 5 Abs. 2 DORA das IKT-Risikomanagement definieren, genehmigen und überwachen. Es trägt die Gesamtverantwortung für die Umsetzung aller Vorkehrungen im Zusammenhang mit dem IKT-Risikomanagementrahmen. Fortbildungspflichten für das Management sind gemäß Art. 5 Abs. 4 DORA vorgesehen, um sicherzustellen, dass die Mitglieder des Leitungsorgans die IKT-Risiken und deren Auswirkungen verstehen und bewerten können.

DOR- und Multi-Vendor-Strategie

Anders als bisher nach den xAIT, in denen sich jeweils im ersten Kapitel Vorgaben zur IT-Strategie fanden, enthält DORA keine Vorgaben zur IT-Strategie. Stattdessen enthält DORA Anforderungen an die Strategie für die digitale operationale Resilienz (im Folgenden: DOR-Strategie)[37], deren Regelungen sich in Art. 6 Abs. 8 DORA finden. In der DOR-

---

[36] BaFin Mitteilung vom 07.10.2024, https://www.bafin.de/SharedDocs/FAQs/DE/DORA/IKT_Risikomanagement/03.html (zuletzt abgerufen am 20.06.2025).

[37] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 1.

Strategie sind Methoden festzuhalten, IKT-Risiken anzugehen und spezifische IKT-Ziele zu erreichen. Dies beinhaltet u. a. eine Erläuterung, wie der IKT-Risikomanagementrahmen die Geschäftsstrategie und die Ziele des Finanzunternehmens unterstützt (lit. a), die Festlegung klarer Ziele für die Informationssicherheit, einschließlich der wesentlichen Leistungsindikatoren und der wesentlichen Risikokennzahlen (lit. c), und die Darlegung einer Kommunikationsstrategie für IKT-bezogene Vorfälle (lit. h). Nach Art. 5 Abs. 2 lit. d DORA trägt das Leitungsorgan die Gesamtverantwortung für die Festlegung und Genehmigung der DOR-Strategie.

Im Zusammenhang mit der DOR-Strategie können Finanzunternehmen nach Art. 6 Abs. 9 DORA eine ganzheitliche Strategie zur Nutzung mehrerer IKT-Anbieter auf Gruppen- oder Unternehmensebene (im Folgenden: Multi-Vendor-Strategie) festlegen, in der wesentliche Abhängigkeiten von IKT-Drittdienstleistern aufgezeigt und die Gründe für die Nutzung verschiedener IKT-Drittdienstleister erläutert werden. Eine Multi-Vendor-Strategie ist insbesondere für größere Institute mit komplexen Auslagerungen empfehlenswert, um Systemabhängigkeiten besser zu erkennen.[38]

[38] Clausmeier: Die neue Verordnung des europäischen Parlamentes und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA), WM 2022 Heft 39, 1861 (1863).

IKT-Geschäftsfortführungsleitlinie (BCM) und IKT-Reaktions- und Wiederherstellungspläne

Zum Verantwortungsbereich des Leitungsorgans zählen gemäß Art. 5 Abs. 2 lit. d DORA außerdem die Genehmigung, Überwachung und Überprüfung der Umsetzung der IKT-Geschäftsfortführungsleitlinie (auch bekannt als *Business Continuity Management* bzw. *BCM*[39]) und der IKT-Reaktions- und Wiederherstellungspläne, die jeweils als eigenständige spezielle Leitlinie, die integraler Bestandteil der allgemeinen Geschäftsfortführungsleitlinie des Finanzunternehmens und seines Reaktions- und Wiederherstellungsplans ist, verabschiedet werden können. Die IKT-Geschäftsfortführungsleitlinie fußt auf den Identifizierungsanforderungen des Art. 8 DORA.[40]

Die IKT-Geschäftsfortführungsleitlinie hat gemäß Art. 11 Abs. 2 DORA spezielle, angemessene und dokumentierte Regelungen, Pläne, Verfahren und Mechanismen für den Fall von Störungen oder Notfällen zu enthalten, die darauf abzielen, die Fortführung der kritischen oder wichtigen Funktionen des Finanzunternehmens sicherzustellen (lit. a), auf alle IKT-bezogenen Vorfälle rasch, angemessen und wirk-

[39] Glos/Hildner in: Schäfer/Omlor/Mimberg, ZAG, 2. Aufl. 2025, ZAG § 53 Rn. 69.

[40] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 4.1.

sam zu reagieren (lit. b), unverzüglich spezielle Pläne zu aktivieren, die Eindämmungsmaßnahmen, Prozesse und Technologien für alle Arten IKT-bezogener Vorfälle ermöglichen und weitere Schäden vermeiden, sowie maßgeschneiderte Verfahren zur Reaktion und Wiederherstellung zu aktivieren (lit. c), vorläufige Auswirkungen, Schäden und Verluste einzuschätzen (lit. d) und Kommunikations- und Krisenmanagementmaßnahmen festzulegen, die gewährleisten, dass allen relevanten internen Mitarbeitern und externen Interessenträgern aktualisierte Informationen übermittelt werden, und die Meldung an die zuständigen Behörden sicherstellen (lit. e).

Nach Art. 11 Abs. 3 DORA sind IKT-Reaktions- und Wiederherstellungspläne zu implementieren, die einer unabhängigen internen Revision zu unterziehen sind, sofern es sich bei dem Finanzunternehmen nicht um ein Kleinstunternehmen handelt.

Weitere Vorgaben zur IKT-Geschäftsfortführungsleitlinie und zu den IKT-Reaktions- und Wiederherstellungsplänen finden sich in den Artt. 24-26 der Delegierten Verordnung zur Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und des vereinfachten IKT-Risikomanagementrahmens (im Folgenden: RTS RMF).[41]

[41] Delegierte Verordnung (EU) 2024/1774.

Die DORA-Vorgaben in Zusammenhang mit der IKT-Geschäftsfortführungsleitlinie und den IKT-Reaktions- und Wiederherstellungsplänen sind vergleichbar mit den bisherigen Vorgaben zum IT-Betrieb (jeweils Kapitel 8) und zum IT-Notfallmanagement (jeweils Kapitel 10) der xAIT, gehen jedoch noch weiter.[42] So liegt der Fokus der DORA-Vorgaben auf der IKT-Geschäftsfortführungsleitlinie, und die Anzahl der zu berücksichtigenden Szenarien ist höher als in den xAIT (z. B. Auswirkungen im Zusammenhang mit Klimawandel und Umweltzerstörung, Terroranschläge, Angriffe durch Insider, politische und soziale Instabilität).[43] Auch die Zuständigkeit des Leitungsorgans hinsichtlich der Überprüfung des IKT-Geschäftsfortführungsmanagements und die Häufigkeit dieser Überprüfungen ist in den xAIT nicht derart spezifiziert.[44]

Budgetmittel, Ressourcen und Programme zur Sensibilisierung für IKT-Sicherheit, Schulungen und IKT-Kompetenzen

Laut ErwG 46 DORA geht der Grundsatz der uneingeschränkten und letztlichen Verantwortung des Leitungsor-

---

[42] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 4.

[43] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, a.a.O.; Art. 26 Abs. 2 RTS RMF.

[44] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, a.a.O.

gans für das Management der IKT-Risiken des Finanzunternehmens mit der Notwendigkeit einher, einen bestimmten Umfang von IKT-Investitionen und ein Gesamtbudget sicherzustellen, die das Finanzunternehmen in die Lage versetzen, ein hohes Niveau an digitaler operationaler Resilienz zu erreichen. Art. 5 Abs. 2 lit. g DORA verpflichtet das Leitungsorgan dazu, angemessene Budgetmittel zuzuweisen und diese regelmäßig zu überprüfen, um den Anforderungen des Finanzunternehmens an die digitale operationale Resilienz in Bezug auf alle Arten von Ressourcen gerecht zu werden, einschließlich einschlägiger Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz sowie IKT-Kompetenzen für alle Mitarbeiter.

So hat das Leitungsorgan nicht nur für persönliche Ressourcen angemessene Budgetmittel zuzuweisen, sondern auch nach Art. 7 lit. c DORA i. V. m. Art. 9 RTS RMF für stets auf dem neuesten Stand zu haltende IKT-Systeme, -Protokolle und -Tools, die mit ausreichenden Kapazitäten ausgestattet sind, um die Daten, die für die Ausführung von Tätigkeiten und die rechtzeitige Erbringung von Dienstleistungen erforderlich sind, genau zu verarbeiten und Auftragsspitzen, Mitteilungen oder Transaktionen auch bei Einführung neuer Technologien bewältigen zu können. Weiterhin werden in Art. 12 Abs. 4 DORA redundante IKT-Kapazitäten mit Ressourcen, Fähigkeiten und Funktionen gefordert, die für die

Deckung des Geschäftsbedarfs ausreichend und angemessen sind.[45]

Meldekanäle zur Nutzung von IKT-Dienstleistungen

Art. 5 Abs. 2 lit. i DORA verpflichtet das Leitungsorgan, auf Unternehmensebene Meldekanäle einzurichten, die es ihm ermöglichen, ordnungsgemäß über Folgendes informiert zu werden: (i) mit IKT-Drittdienstleistern geschlossene Vereinbarungen über die Nutzung von IKT-Dienstleistungen, (ii) alle relevanten geplanten wesentlichen Änderungen in Bezug auf die IKT-Drittdienstleister und (iii) die potenziellen Auswirkungen derartiger Änderungen auf die kritischen oder wichtigen Funktionen, die Gegenstand dieser Vereinbarungen sind, einschließlich einer Zusammenfassung der Risikoanalyse, um die Auswirkungen dieser Änderungen zu bewerten, und zumindest über schwerwiegende IKT-bezogene Vorfälle und deren Auswirkungen sowie über Gegen-, Wiederherstellungs- und Korrekturmaßnahmen.

Genehmigung und Überprüfung von Leitlinien und internen IKT-Revisionsplänen

Das Leitungsorgan hat nach Art. 5 Abs. 2 lit. b DORA Leitlinien einzuführen, die darauf abzielen, hohe Standards in Be-

[45] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 3.1.

zug auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten aufrechtzuerhalten. Hierbei handelt es sich um die vier Schutzziele von DORA.[46]

Zu diesen Leitlinien gehören die IKT-Geschäftsfortführungsleitlinie, wie weiter oben bereits näher ausgeführt, sowie die Leitlinie in Bezug auf Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die von IKT-Drittdienstleistern bereitgestellt werden (Art. 5 Abs. 2 lit. h DORA), zu welcher sich zusätzliche Vorgaben im RTS TPPol finden. Eine weitere Leitlinie ist die Informationssicherheitsleitlinie nach Art. 9 Abs. 4 lit. a DORA, in der Regeln zum Schutz der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten und der Informations- und IKT-Assets, ggf. einschließlich derjenigen der Kunden des Finanzunternehmens, festzulegen sind.

Darüber hinaus sind auch die IKT-Sicherheitsrichtlinien nach Art. 9 Abs. 2 DORA i. V. m. Art. 2 Abs. 2 lit. b RTS RMF und die internen IKT-Revisionspläne des Finanzunternehmens, die IKT-Revision und die daran vorgenommenen wesentlichen Änderungen nach Art. 5 Abs. 2 lit. f DORA durch das Leitungsorgan zu genehmigen.

[46] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 1.3.

Festlegung von Aufgaben und Verantwortlichkeiten sowie Governance-Regelungen

Das Leitungsorgan ist nach Art. 5 Abs. 2 lit. c DORA außerdem verpflichtet, klare Aufgaben und Verantwortlichkeiten für alle IKT-bezogenen Funktionen sowie angemessene Governance-Regelungen festzulegen, um eine wirksame und rechtzeitige Kommunikation, Zusammenarbeit und Koordinierung zwischen diesen Funktionen zu gewährleisten. Aus ErwG 38 DORA geht hervor, dass nur Finanzunternehmen, die keine Kleinstunternehmen sind, verpflichtet werden sollten, komplexere Governance-Regelungen einzuführen. Demnach sind größere Finanzunternehmen besser gerüstet, um insbesondere spezielle Managementfunktionen für die Überwachung von Vereinbarungen mit IKT-Drittdienstleistern oder für den Umgang mit dem Krisenmanagement einzurichten, ihr IKT-Risikomanagement nach dem Modell der drei Verteidigungslinien zu strukturieren oder ein internes Modell für Risikomanagement und Kontrolle einzuführen und ihren IKT-Risikomanagementrahmen internen Revisionen zu unterziehen.

Zu beachten ist auch, dass DORA lediglich die Governance des IKT-Risikomanagementrahmens adressiert und die allgemeinen Governance-Anforderungen aus den sektoralen Regelungen bestehen bleiben.[47]

Im Rahmen der Governance des IKT-Risikomanagementrahmens gibt Art. 2 Abs. 2 lit. g und i RTS RMF Finanzunternehmen vor, Regelungen für die Aufgabentrennung nach dem Modell der drei Verteidigungslinien oder gegebenenfalls einem anderen internen Modell für Risikomanagement und Kontrolle zu spezifizieren, um Interessenkonflikte zu vermeiden und die Aufgaben und Verantwortlichkeiten für die Entwicklung, Implementierung und Aufrechterhaltung von Richtlinien, Verfahren, Protokollen und Tools für die IKT-Sicherheit festzulegen.

Das organisationstheoretische Modell der drei Verteidigungslinien (auch bekannt als *Three Lines of Defence*) beschreibt, wer in der Aufbauorganisation eines Unternehmens für bestimmte Aufgaben der Risiko- und Gefahrenabwehr verantwortlich sein soll.[48] Dieses Modell sieht in der ersten Verteidigungslinie die operativen Abteilungen vor, die mit eigenen prozessorientierten internen Kontrollen dafür sorgen, dass ihre Aktivitäten rechtskonform und in Einklang mit der

[47] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 1.2.

[48] Gebauer in: Hopt/Binder/Böcking CG-HdB, 2. Aufl. 2020, § 10. Rn. 36.

Risikostrategie durchgeführt werden. Die zweite Verteidigungslinie wird u. a. von dem Risikocontrolling und der Compliance-Funktion repräsentiert. Die zweite Linie ist nicht operativ tätig, sondern ist für die Einhaltung rechtlicher Anforderungen zuständig und überwacht prozessbegleitend die Funktionsfähigkeit der implementierten Kontrollen. Die dritte Verteidigungslinie wird von der Internen Revision mit ihren nachgelagerten prozessunabhängigen Kontrollen repräsentiert. Die Interne Revision überprüft die internen Verfahren der ersten beiden Verteidigungslinien, insbesondere in Hinblick auf konsequente Anwendung und Wirksamkeit.[49]

Weitere DORA-Schlüsselfunktionen

Neben den bereits nach den xAIT bestehenden Fachabteilungen und Funktionen sieht DORA die Einführung der Krisenmanagementfunktion, Funktion zur Überwachung der mit IKT-Drittdienstleistern über die Nutzung von IKT-Dienstleistungen geschlossenen Vereinbarungen und der IKT-Risikokontrollfunktion vor.

Kleinstunternehmen sind von der Verpflichtung der Einführung dieser Funktionen ausgenommen (ErwG 43).

Krisenmanagementfunktion

Nach Art. 11 Abs. 7 DORA haben Finanzunternehmen eine Krisenmanagementfunktion einzurichten, die bei Aktivierung

[49] Gebauer in: Hopt/Binder/Böcking CG-HdB, 2. Aufl. 2020, a.a.O; Bürkle in: Moosmayer/Lösler Corporate Compliance, 4. Aufl. 2024, § 52. Rn. 77.

der IKT-Geschäftsfortführungspläne oder IKT-Reaktions- und Wiederherstellungspläne u. a. klare Verfahren für die Abwicklung interner und externer Krisenkommunikation festlegt.

Im Krisenfall sollen alle relevanten internen Mitarbeiter und externe Interessenträger entsprechend informiert werden (Art. 11 Abs. 2 lit. e i. V. m. Artt. 14 und 19 DORA; Art. 24 Abs. 1 lit. a Ziff. iv und lit. b Ziff. vi RTS RMF). Hierzu braucht es nach Art. 14 Abs. 2 DORA Kommunikationsstrategien und -leitlinien, die die Informationsbedürfnisse der Mitarbeiter, die an Reaktion und Wiederherstellung beteiligt sind, und des weiteren zu informierenden Personals berücksichtigen.[50]

Dem BSI-Standard 200-4 zufolge ist das Krisenmanagement eng mit dem Geschäftsfortführungsmanagement verknüpft.[51] Bei einer Krise handelt es sich nach dem BSI-Standard um ein Schadensereignis, das sich in erheblicher Weise negativ auf die Institution auswirkt und dessen Auswirkungen auf die Institution nicht im Normalbetrieb bewältigt werden können. Krisen können unmittelbar auftreten oder aus einer Störung oder einem Notfall heraus eskalieren.[52] Da das Ge-

[50] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 4.4.

[51] BSI-Standard 200-4, Bonn 2023, 14.

[52] BSI-Standard 200-4, Bonn 2023, 21.

schäftsfortführungsmanagement aufgrund seines Steuerungs- und Überwachungscharakters über die Risikomanagementfunktionen der ersten Verteidigungslinie Teil der zweiten Verteidigungslinie ist[53], liegt es nahe, die Krisenmanagementfunktion aufgrund der engen Verknüpfung ebenfalls in der zweiten Verteidigungslinie zu verorten.

Funktion zur Überwachung von IKT-Drittdienstleistungsvereinbarungen

Art. 5 Abs. 3 DORA schreibt Finanzunternehmen vor, eine Funktion einzurichten, die dafür zuständig ist, die mit IKT-Drittdienstleistern über die Nutzung von IKT-Dienstleistungen geschlossenen Vereinbarungen zu überwachen. Alternativ kann auch ein Mitglied der Geschäftsleitung benannt werden, das für die Überwachung der damit verbundenen Risikoexposition und die einschlägige Dokumentation verantwortlich ist. Die Funktion ist laut der BaFin mit dem (zentralen) Auslagerungsbeauftragten[54] bzw. mit dem Auslagerungsmanagement oder im Fall von Versicherungen mit dem Ausgliederungsbeauftragen bzw. -management vergleichbar.

---

[53] BSI-Standard 200-4, Bonn 2023, 76.

[54] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 6.6.

Aufgrund des Überwachungscharakters ist eine Einordnung der mit der Überwachung von IKT-Dienstleistungsvereinbarungen betrauten Funktion in der zweiten Verteidigungslinie naheliegend. Nach Art. 3 Abs. 5 RTS TPPol ist in der Leitlinie für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen eindeutig anzugeben, bei welcher Funktion oder bei welchem Mitglied der Geschäftsleitung die Zuständigkeit für die Überwachung der einschlägigen vertraglichen Vereinbarungen liegt. In der Leitlinie ist festzulegen, wie diese Funktion oder dieses Mitglied der Geschäftsleitung mit den Kontrollfunktionen zusammenarbeitet, es sei denn, die Funktion oder das Mitglied ist Teil der Kontrollfunktionen. Dieser Vorgabe zufolge ist eine Verortung der Funktion zur Überwachung von IKT-Drittparteienrisiken auch in der ersten Verteidigungslinie denkbar. Geht man vom Standpunkt der BaFin aus, dass die Funktion mit dem (zentralen) Auslagerungsbeauftragten vergleichbar ist, ist die Verortung in der zweiten Verteidigungslinie zu bevorzugen, da der Auslagerungsbeauftragte bzw. das Auslagerungsmanagement nach den allgemeinen Governance-Anforderungen aus den sektoralen Regelungen regelmäßig Teil der zweiten Verteidigungslinie ist.[55]

[55] Ahmad/Kirschbaum in: Riediger Auslagerungen/Dienstleister-Steuerung, Rn. 364.

IKT-Risikokontrollfunktion

Nach Art. 6 Abs. 4 DORA sind Finanzunternehmen dazu verpflichtet, eine Kontrollfunktion zu etablieren, die für das Management und die Überwachung des IKT-Risikos zuständig ist und über ein angemessenes Maß an Unabhängigkeit verfügt, um Interessenkonflikte zu vermeiden. Detaillierte Vorgaben zum IKT-Risikomanagement finden sich im RTS RMF.

Der BaFin zufolge ähnelt die Funktion im Hinblick auf die Stellung und Unabhängigkeit dem aus BAIT/VAIT bekannten Informationssicherheitsbeauftragten (ISB), ist jedoch nicht identisch ausgestaltet.[56] Die IKT-Risikokontrollfunktion beinhaltet eine Ausweitung von der Wahrnehmung der Belange der Informationssicherheit auf das Management und die Überwachung des IKT-Risikos. Aufgrund von inhaltlichen Überschneidungen ist es denkbar, dass der bisherige ISB auch die Aufgaben der IKT-Risikokontrollfunktion übernimmt.[57]

[56] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 2, 2.2.

[57] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 2.2.

Als klassische Kontroll- und Überwachungsfunktion ist auch die IKT-Risikokontrollfunktion in der zweiten Verteidigungslinie einzuordnen.

Kommunikationsbeauftragte Person(en) für IKT-bezogene Vorfälle

Nach Art. 14 Abs. 3 DORA ist mindestens eine Person mit der Umsetzung der Kommunikationsstrategie für IKT-bezogene Vorfälle beauftragt, die zu diesem Zweck die entsprechende Aufgabe gegenüber der Öffentlichkeit und den Medien wahrnimmt. Bei einer bereits im Unternehmen vorhandenen Kommunikationsabteilung ist die Bestimmung einer oder mehrerer Personen innerhalb der Kommunikationsabteilung denkbar, die mit externer Kommunikation vertraut ist bzw. sind.

2.2.2.5 Umgang mit IKT-bezogenen Vorfällen

Die Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle sind in den Artt. 17 bis 23 DORA geregelt und werden ergänzt durch den RTS zur Festlegung der Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen[58], den RTS zur Festlegung des Inhalts und der Fristen für die

[58] Delegierte Verordnung (EU) 2024/1772 der Kommission vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen, der Wesentlichkeitsschwellen und der Einzelheiten von Meldungen schwerwiegender Vorfälle.

Erstmeldung[59] und den ITS zu Standardformularen, Vorlagen und Verfahren für Meldungen von schwerwiegenden IKT-bezogenen Vorfällen.[60] Finanzunternehmen müssen nach diesem Abschnitt

- einen Prozess für die Behandlung IKT-bezogener Vorfälle bestimmen, einrichten und anwenden, um solche zu erkennen, zu behandeln und zu melden (Art. 17),
- IKT-bezogene Vorfälle klassifizieren und deren Auswirkungen bestimmen (Art. 18) und
- schwerwiegende IKT-bezogene Vorfälle an die zuständige Behörde melden und können auf freiwilliger Basis erhebliche Cyberbedrohungen melden (Art. 19).

[59] Delegierte Verordnung (EU) 2025/301 der Kommission vom 23. Oktober 2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung des Inhalts und der Fristen für die Erstmeldung, die Zwischenmeldung und die Abschlussmeldung schwerwiegender IKT-bezogener Vorfälle sowie des Inhalts der freiwilligen Meldung erheblicher Cyberbedrohungen.

[60] Durchführungsverordnung (EU) 2025/302 vom 23. Oktober 2024 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates im Hinblick auf Standardformulare, Vorlagen und Verfahren für Finanzunternehmen zur Meldung eines schwerwiegenden IKT-bezogenen Vorfalls oder einer erheblichen Cyberbedrohung.

Artt. 20 bis 23 DORA enthalten Vorgaben für die ESAs und die national zuständigen Aufsichtsbehörden. Während die ESAs für die Erarbeitung von Standards und Berichterstattung zuständig sind (Art. 20 und 21), regelt Art. 22 Abs. 1, wie die national zuständigen Aufsichtsbehörden Rückmeldungen auf Meldungen ausgestalten. Art. 23 stellt klar, dass die Anforderungen hinsichtlich der IKT-bezogenen Vorfälle auch für zahlungsbezogene Betriebs- oder Sicherheitsvorfälle – auch schwerwiegender Art, wenn sie Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister und E-Geld-Institute betreffen – gelten.

2.2.2.6 Testen der digitalen operationalen Resilienz

Die Anforderungen an das Testen der digitalen operationalen Resilienz sind in den Artt. 24 bis 27 DORA geregelt und werden durch den RTS zur Durchführung von bedrohungsorientierten Penetrationstests (TLPT)[61] ergänzt. Zu beachten

[61] Delegierte Verordnung (EU) 2025/1190 der Kommission vom 13. Februar 2025 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Kriterien für die Bestimmung der Finanzunternehmen, die zur Durchführung von bedrohungsorientierten Penetrationstests verpflichtet sind, der Anforderungen und Standards für den Einsatz interner Tester, der Anforderungen hinsichtlich des Testumfangs, der Testmethodik und des Testkonzepts für jede einzelne Phase des Testverfahrens sowie der Ergebnisse, des Abschlusses und der Behebungsphasen der Tests sowie der Art der aufsichtlichen und sonstigen relevanten Zusammenarbeit, die für die Umsetzung von bedrohungsorientierten Penetrationstests und die Erleichterung der gegenseitigen Anerkennung dieser Tests erforderlich ist.

ist, dass je nach Größe und Bedeutung des Finanzunternehmens abgestufte Anforderungen gelten. Es ist in dem Zusammenhang zwischen folgenden Arten von Finanzunternehmen zu unterscheiden:

- Finanzunternehmen, die keine Kleinstunternehmen sind (Art. 24 und 25 Abs. 1),
- Kleinstunternehmen (Art. 25 Abs. 3),
- Zentralverwahrer und zentrale Gegenparteien (Art. 25 Abs. 2) und
- von zuständigen Behörden ermittelte Finanzunternehmen, die TLPT durchzuführen haben (Art. 26 Abs. 8 UAbs. 3).

Finanzunternehmen, die keine Kleinstunternehmen sind

Finanzunternehmen, die keine Kleinstunternehmen sind, müssen nach Art. 24 DORA ein umfassendes Programm zur digitalen operationalen Resilienz erstellen, pflegen und regelmäßig überprüfen, um Schwächen und Lücken zu identifizieren und Korrekturmaßnahmen umzusetzen. Dieses Programm umfasst verschiedene Bewertungen, Tests und Methoden, die auf einem risikobasierten Ansatz beruhen und spezifische IKT-Risiken sowie die Kritikalität von Informations-Assets und ggf. weitere relevante Faktoren berücksichtigen, welche in Verfahren und Leitlinien festzulegen sind.

Kleinstunternehmen, Zentralverwahrer und zentrale Gegenparteien

Kleinstunternehmen treffen in Hinblick auf Tests weniger umfangreiche Pflichten. Sie sind nach Art. 25 Abs. 3 DORA lediglich dazu verpflichtet, Tests durchzuführen, wie sie in Art. 25 Abs. 1 DORA beschrieben sind, beispielsweise Open-Source-Analysen oder Netzwerksicherheitsbewertungen.

Zentralverwahrer und zentrale Gegenparteien werden nach Art. 25 Abs. 2 DORA verpflichtet, Schwachstellenbewertungen durchzuführen, bevor sie Anwendungen und Infrastrukturkomponenten sowie IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, einsetzen oder wieder einsetzen.

Von zuständigen Behörden ermittelte Finanzunternehmen, die TLPT durchzuführen haben

Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT nach Art. 26 DORA sind jenen Finanzunternehmen vorbehalten, die nach den in Art. 26 Abs. 8 UAbs. 3 DORA dargelegten Kriterien von den zuständigen

Behörden ermittelt werden. Hierbei handelt es sich um systemrelevante Finanzunternehmen.[62]

2.2.2.7 Management des IKT-Drittparteienrisikos

Das Management des IKT-Drittparteienrisikos ist in zwei Abschnitte unterteilt.

Der erste Abschnitt, bestehend aus den Artt. 28 bis 30 DORA, enthält Vorgaben für das Drittparteienrisikomanagement innerhalb von Finanzunternehmen. Ergänzt werden die Vorgaben durch den ITS zur Erstellung einer Standardvorlage für das Informationsregister (im Folgenden: RTS ROI)[63], den RTS TPPol und den RTS zur Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen.[64]

---

[62] Bomhard/Siglmüller in: Hornung/Schallbruch, IT-Sicherheitsrecht, § 29 IT-Sicherheitsrecht im Finanzsektor Rn. 31.

[63] Durchführungsverordnung (EU) 2024/2956 der Kommission vom 29. November 2024 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates im Hinblick auf Standardvorlagen für das Informationsregister.

[64] Delegierte Verordnung (EU) 2025/532 der Kommission vom 24. März 2025 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Präzisierung der Aspekte, die ein Finanzunternehmen bei der Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen bestimmen und bewerten muss.

Im zweiten Abschnitt (Artt. 31 bis 44 DORA) geht es um die Einstufung von IKT-Drittdienstleistern als kritische IKT-Drittdienstleister und um den Überwachungsrahmen dieser kritischen Dienstleister durch die ESAs.

Informationsregister

Finanzunternehmen sind nach Art. 28 Abs. 3 DORA verpflichtet, ein Informationsregister zu führen und zu aktualisieren, das alle relevanten Informationen über den Bezug von IKT-Dienstleistungen von Drittdienstleistern enthält. Das Register sorgt für Transparenz und ermöglicht den Finanzunternehmen eine effektive Überwachung über Drittparteienrisiken.

In Deutschland ist das Informationsregister auf Grundlage von Art. 28 Abs. 3 UAbs. 4 DORA jährlich zum 31. März über die Melde- und Veröffentlichungsplattform (MVP) an die BaFin zu übermitteln.[65] Nach Art. 28 Abs. 3 UAbs. 5 DORA müssen Finanzunternehmen ihre Informationsregister der Aufsichtsbehörde auch auf deren Verlangen zur Verfügung stellen.

[65] BaFin: Informationsregister und Anzeigepflichten, geändert am 18.07.2025, https://www.bafin.de/DE/Aufsicht/DORA/Informationsregister_und_Anzeigepflichten/Informationsregister_und_Anzeigepflichten_node.html (zuletzt abgerufen am 05.09.2025).

Due Diligence und Risikoanalyse

Vor Abschluss einer vertraglichen Vereinbarung über die Nutzung von IKT-Dienstleistungen müssen Finanzunternehmen eine Vielzahl an Punkten berücksichtigen und bewerten. Diese ergeben sich aus Art. 28 Abs. 4 und 5 und Art. 29 DORA sowie aus Artt. 5 und 6 RTS TPPol und stellen Vorgaben für eine Due Diligence und Risikoanalyse dar.

Die meisten Finanzunternehmen waren bereits im Rahmen des bisherigen Auslagerungsregimes zur Durchführung von Due Diligences und Risikoanalysen verpflichtet, beispielsweise nach AT 9 Ziff. 2 MaRisk. Die DORA-Vorgaben erhöhen nun den Umfang der bisherigen Anforderungen an Due Diligences und Risikoanalysen, insbesondere mit Blick auf Dienstleistungen, die kritische oder wichtige Funktionen unterstützen.[66] Während sich die Vorgaben für Dienstleistungen, die keine kritischen oder wichtigen Funktionen unterstützen, auf jene aus Art. 28 Abs. 4 und 5 DORA beschränken, gelten für Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, zusätzliche Vorgaben aus Artt. 5 und 6 RTS TPPol und Art. 29 DORA. Hierzu gehören etwa Erwägungen zur Reputation des IKT-Drittdienstleisters oder die Erfüllung von ESG-Anforderungen (Art. 6 Abs. 1 RTS TPPol). Ebenso sollten IKT-Drittdienstleister, deren Dienstleistungen kritische oder wichtige Funktionen unterstützen,

[66] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 6.4.

zu einer engen Kooperation bereit sein, da im Rahmen der Due Diligence vor Vertragsabschluss auch Prüf- oder Assessmentergebnisse des IKT-Drittdienstleisters heranzuziehen sind (Art. 6 Abs. 3 lit. a und b RTS TPPol).[67]

IKT-Drittdienstleister-Audits

Nach Art. 30 Abs. 3 lit. e DORA haben Finanzunternehmen mit IKT-Drittdienstleistern in Zusammenhang mit dem Bezug von Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, vertraglich das Recht zu vereinbaren, die Leistungen des IKT-Drittdienstleisters fortlaufend zu überwachen, wozu uneingeschränkte Zugangs-, Inspektions- und Auditrechte gehören.

In Hinblick hierauf haben die Finanzunternehmen nach Art. 28 Abs. 6 DORA auf der Grundlage eines risikobasierten Ansatzes vorab die Häufigkeit von Audits und Inspektionen sowie die zu prüfenden Bereiche zu bestimmen, indem allgemein anerkannte Auditstandards im Einklang mit etwaigen Aufsichtsanweisungen für die Anwendung und Einbeziehung solcher Auditstandards eingehalten werden. Art. 8 Abs. 3 RTS TPPol stellt ergänzend klar, dass sich Finanzunternehmen längerfristig nicht nur auf Zertifizierungen oder Auditberichte der IKT-Drittdienstleister verlassen dürfen.

[67] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 6.4.

Ausstiegsstrategien

Ebenfalls nur in Bezug auf vertragliche Vereinbarungen zu IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, haben Finanzunternehmen nach Art. 28 Abs. 8 DORA Ausstiegsstrategien einzurichten. Ergänzend dazu gibt Art. 10 RTS TPPol u. a. vor, dass die Ausstiegspläne realistisch und durchführbar sein, auf plausiblen Szenarien und vernünftigen Annahmen beruhen und einen Durchführungszeitplan enthalten müssen, der mit den in den vertraglichen Vereinbarungen festgelegten Ausstiegs- und Beendigungsbedingungen vereinbar ist.

Wesentliche Vertragsbestimmungen und Unterauftragsvergabe

Art. 30 Abs. 1 und 2 DORA geben die Mindestvertragsinhalte für vertragliche Vereinbarungen über den Bezug von IKT-Drittdienstleistungen vor. Bei Bezügen von IKT-Drittdienstleistungen, die kritische oder wichtige Funktionen unterstützen, sind zusätzlich noch die in Art. 30 Abs. 3 DORA genannten Mindestvertragsinhalte zu berücksichtigen. Weitere Konkretisierungen zu den vertraglichen Vereinbarungen, die kritische oder wichtige Funktionen betreffen, sind im RTS TPPol und im RTS zur Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen (im Folgenden: RTS SUB) zu finden.

Der RTS SUB enthält umfassende Regelungen zur Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, was eine signifikante Erweiterung der Regulierungsbreite und -tiefe darstellt.[68]

Finanzunternehmen sind u. a. nach Art. 3 Abs. 1 RTS SUB verpflichtet, sorgfältig zu prüfen, ob der IKT-Drittdienstleister in der Lage ist, geeignete Unterauftragnehmer auszuwählen und diese angemessen zu überwachen.[69] Diese Anforderung ist entscheidend, um sicherzustellen, dass die Qualität und Sicherheit der Dienstleistungen, die durch Unterauftragnehmer erbracht werden, den gleichen Standards entsprechen wie die des Hauptdienstleisters. Darüber hinaus enthält Art. 6 RTS SUB zusätzliche Vorgaben zu Kündigungsrechten in Zusammenhang mit Unterauftragsvereinbarungen.

Nach Art. 29 Abs. 2 UAbs. 4 DORA haben Finanzunternehmen im Fall von Unterauftragsvergaben zudem zu bewerten, ob und wie sich potenziell lange oder komplexe Ketten der Unterauftragsvergabe auf ihre Fähigkeit auswirken können, die vertraglich vereinbarten Funktionen vollständig zu überwachen, und ob die zuständige Behörde in dieser Hinsicht in

---

[68] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 6.3.

[69] BaFin, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024, Abschnitt II. Nr. 6.3.

der Lage ist, das Finanzunternehmen wirksam zu beaufsichtigen. Die Unterauftragsvergaben sind auch ins Informationsregister einzutragen (Art. 3 Abs. 2 lit. b ITS ROI).

2.2.2.8 Vereinbarungen über den Austausch von Informationen

Art. 45 DORA enthält Regelungen zu Vereinbarungen über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen. Der Austausch kann Informationen zu Indikatoren für Beeinträchtigungen, Taktiken, Techniken und Verfahren sowie Cybersicherheitswarnungen umfassen und soll dem Zweck dienen, die digitale operationale Resilienz zu stärken, das Bewusstsein für Cyberbedrohungen zu schärfen und die Verteidigungsfähigkeiten der Unternehmen zu unterstützen.[70]

Der Austausch hat innerhalb vertrauenswürdiger Gemeinschaften von Finanzunternehmen zu erfolgen und ist durch Vereinbarungen zu regeln, die den sensiblen Charakter der Informationen schützen.[71] Diese Vereinbarungen müssen sicherstellen, dass Geschäftsgeheimnisse und personenbezogene Daten gemäß der Datenschutz-Grundverordnung (im Folgenden: DSGVO) gewahrt bleiben (Art. 45 Abs. 1 lit. c DORA).

---

[70] ErwG 32 DORA.

[71] ErwG 34 DORA.

Zusätzlich müssen die Vereinbarungen die Teilnahmebedingungen und die Einbindung staatlicher Behörden sowie IKT-Drittdienstleister festlegen. Finanzunternehmen sind verpflichtet, den zuständigen Behörden ihre Beteiligung an diesen Austauschvereinbarungen mitzuteilen, sobald die Beteiligung bestätigt oder beendet wird (Art. 45 Abs. 3 DORA).

2.2.3 AI Act

2.2.3.1 Hintergrund

Die Verordnung über Künstliche Intelligenz[72] (im Folgenden: AI Act) verfolgt mehrere zentrale Ziele. Zunächst soll die Verordnung das Funktionieren des Binnenmarkts verbessern, indem ein einheitlicher Rechtsrahmen für die Entwicklung, das Inverkehrbringen und die Verwendung von KI-Systemen geschaffen wird, und zwar in Einklang mit den Werten der EU, um eine menschenzentrierte und vertrauenswürdige KI zu fördern und gleichzeitig ein hohes Schutzniveau für Gesundheit, Sicherheit und Grundrechte zu gewährleisten.[73]

Die Verordnung soll auch sicherstellen, dass KI-Systeme sicher und vertrauenswürdig sind, um eine Fragmentierung des Binnenmarkts zu vermeiden.[74] KI-Technologien sollen in verschiedenen Bereichen der Wirtschaft und Gesellschaft ei-

[72] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

[73] ErwG 1 AI Act.

[74] ErwG 3 AI Act.

nen erheblichen Nutzen bringen, können jedoch auch Risiken für öffentliche Interessen und Grundrechte mit sich bringen.[75]

Um ein hohes Schutzniveau zu gewährleisten, sind insbesondere für Hochrisiko-KI-Systeme gemeinsame Vorschriften erforderlich, die nichtdiskriminierend sind und mit internationalen Handelsverpflichtungen der Union übereinstimmen.[76] Die Verordnung zielt darauf ab, die Entwicklung und Verwendung von KI im Binnenmarkt zu fördern, während gleichzeitig die Grundrechte, einschließlich des Datenschutzes, gewahrt bleiben.[77]

Insgesamt soll der AI Act einen klaren und robusten Rechtsrahmen schaffen, der Innovationen unterstützt und gleichzeitig die Rechte und Sicherheit der Bürger schützt. Bei dem AI Act handelt es sich global um den ersten Rechtsrahmen für KI, der sich mit den Risiken der KI befasst und Europa in die Lage versetzen soll, weltweit eine führende Rolle zu übernehmen.[78]

---

75 ErwG 4 und 5 AI Act.

76 ErwG 7 AI Act.

77 ErwG 8 und 10 AI Act.

78 EU-Kommission zum AI Act, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (zuletzt abgerufen am 07.09.2025).

2.2.3.2 Adressaten und zuständige Aufsicht

Adressaten

Der AI Act beschränkt sich in seiner Geltung nicht auf einen bestimmten Wirtschaftssektor, sondern richtet sich sektorübergreifend hauptsächlich an alle Anbieter und Betreiber von KI-Systemen.

Ein *KI-System* wird in Art. 3 Nr. 1 AI Act definiert als ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.

Davon zu unterscheiden ist der Begriff des *KI-Modells mit allgemeinem Verwendungsweck* (im Folgenden: GPAI für General-Purpose AI), der sich durch den AI Act zieht, und z. B. im Zusammenhang mit Anbietern nach Art. 3 Nr. 3 AI Act genannt wird. Der Begriff KI-Modell bezieht sich auf den Algorithmus, der durch Training die Denkweise einer KI formt und ihre Arbeitsweise bestimmt, wozu beispielsweise LLMs zählen, die als Grundlage für KI-Systeme wie ChatGPT oder Microsoft Copilot dienen.[79]

[79] Schwenke: Einführung KI-Verordnung: Grundlagen, Begriffe und Pflichtenkatalog, DSB 2024, 205.

Ein *Anbieter* i. S. v. Art. 3 Nr. 3 AI Act ist eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein GPAI entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt, oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich.

Ein *Betreiber* ist nach Art. 3 Nr. 4 AI Act eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet. Zu beachten ist, dass unter den Voraussetzungen des Art. 25 AI Act (Verantwortlichkeiten entlang der KI-Wertschöpfungskette) Betreiber ausnahmsweise als Anbieter behandelt werden.[80]

Abgrenzen lässt sich der Betreiber vom Anbieter maßgeblich dadurch, dass der Betreiber nicht am Entwicklungsprozess des KI-Systems beteiligt ist, sondern es lediglich zu beruflichen Zwecken nutzt.[81]

Weitere Adressaten des AI Acts sind u. a. Einführer (Art. 3 Nr. 6 AI Act), Händler (Art. 3 Nr. 7 AI Act), Produkthersteller und Bevollmächtigte von Anbietern von GPAI (Art. 54 AI

[80] Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 3 Rn. 51.
[81] Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 3 Rn. 51.

Act), auf die im Rahmen dieser Arbeit jedoch nicht weiter eingegangen wird. Zusammen werden sie nach Art. 3 Nr. 8 AI Act als *Akteure* bezeichnet.

Zuständige Aufsicht

Nach Art. 88 Abs. 1 AI Act obliegen die Beaufsichtigung und die Befugnis zur Durchsetzung der Regelungen über GPAI nach Artt. 51 bis 56 AI Act dem *AI Office*. Beaufsichtigt werden in dem Zusammenhang Anbieter von GPAI, da diese die Adressaten der Pflichten aus den Artt. 51 bis 56 AI Act sind.

Daneben wird nach Art. 65 Abs. 1 AI Act ein KI-Gremium, auch bekannt als *AI Board***,** errichtet.[82] Dessen Aufgaben bestehen gemäß Art. 66 AI Act hauptsächlich in der Beratung und Unterstützung des AI Boards, der EU-Kommission und der Mitgliedstaaten.[83]

Zuständige nationale Behörden

Regelungen zu zuständigen nationalen Behörden finden sich in Art. 70 AI Act. Gemäß Art. 70 Abs. 1 AI Act haben die Mitgliedstaaten mindestens eine notifizierende Behörde und mindestens eine Marktüberwachungsbehörde als zuständige nationale Behörden einzurichten oder zu benennen. Die

[82] Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 13 Rn. 22.
[83] Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 13 Rn. 27.

nationale Aufsichtsstruktur soll in Deutschland durch das Gesetz zur Durchführung der KI-Verordnung geregelt werden.[84]

Notifizierungsbehörde (grundsätzlich zuständig vor Inverkehrbringen eines KI-Systems[85])

Die Notifizierungsbehörde ist gemäß Art. 3 Nr. 19 AI Act eine nationale Behörde, die für die Einrichtung und Durchführung der Verfahren zur Bewertung, Benennung und Notifizierung von Konformitätsbewertungsstellen und für deren Überwachung zuständig ist. Regelungen zu notifizierenden Behörden und notifizierten Stellen finden sich in den Artt. 28 bis 38 AI Act. Nach Angaben der Bundesnetzagentur (im Folgenden: BNetzA)[86] bedeutet die Notifizierung die offizielle Mitteilung an die EU-Kommission und die anderen Mitgliedstaaten, dass eine Konformitätsbewertungsstelle geprüft und benannt wurde, denn nur von diesen notifizierten Stellen dürfen Konformitätsbewertungen im Sinne des AI Acts vorgenommen werden.[87] Notifizierte Stellen sind einzubeziehen, um zu

84 Das Gesetz ist bislang noch ein Referentenentwurf (Bearbeitungsstand 11.09.2025).

85 Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 13 Rn. 58.

86 Die BNetzA ist zuständige Notifizierungsbehörde für die in Anhang I Nr. 6 AI Act aufgeführte Richtlinie 2014/53/EU über die Bereitstellung von Funkanlagen auf dem Markt.

87 BNetzA, https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/13_Notifizierung/start.html (zuletzt abgerufen am 08.09.2025).

überprüfen, ob Hochrisiko-KI-Systeme den Anforderungen des AI Acts entsprechen.[88]

Marktüberwachungsbehörde (grundsätzlich zuständig nach Inverkehrbringen eines KI-Systems[89])

Bei der Marktüberwachungsbehörde handelt es sich nach Art. 3 Nr. 26 AI Act um eine nationale Behörde, die die Tätigkeiten durchführt und die Maßnahmen ergreift, die in der Verordnung über Marktüberwachung und die Konformität von Produkten[90] (im Folgenden: MÜVO) vorgesehen sind. Ihre Aufgaben sind in Artt. 72 ff. AI Act und in der MÜVO geregelt. Dazu gehören u. a. die Marktüberwachung und Kontrolle von KI-Systemen nach Art. 74 AI Act i. V. m. der MÜVO.[91] Daneben ist die Marktüberwachungsbehörde Adressatin von Melde- und Berichtspflichten der Akteure.[92]

In Deutschland ist die BNetzA die zentrale Marktüberwachungs- und notifizierende Behörde und gleichzeitig zuständig für die Koordination der Zusammenarbeit mit weiteren Behörden.[93]

---

88 BNetzA, a.a.O.

89 Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 13 Rn. 60.

90 Verordnung (EU) 2019/1020.

91 Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 13 Rn. 62 f.

92 Wendehorst in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 3 Rn. 203.

93 Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 13 Rn. 53.

Für Hochrisiko-KI-Systeme, die Produkte im Sinne der in Anhang I Abschnitt A des AI Acts genannten Harmonisierungsrechtsakte darstellen oder mit solchen Produkten verbunden sind, gelten die für die Marktüberwachung benannten Behörden als Marktüberwachungsbehörden im Sinne des AI Acts.[94]

Nach Art. 74 Abs. 6 AI Act ist für Hochrisiko-KI-Systeme, die mit Finanzdienstleistungen in Verbindung stehen, die zuständige Marktüberwachungsbehörde die für die nationale Finanzaufsicht zuständige Behörde. In Deutschland ist folglich die BaFin in dem Zusammenhang die zuständige Marktüberwachungsbehörde.[95]

2.2.3.3 Einsatz von KI in Finanzunternehmen

Der Einsatz von KI-Systemen in Finanzunternehmen hat in den letzten Jahren erheblich zugenommen und bietet zahlreiche Vorteile, darunter verbesserte Risikobewertungen, personalisierte Kundenservices und effizientere Betrugsbekämpfung. Im Folgenden werden einige Anwendungsbeispiele für KI-Systeme im Finanzsektor aufgezeigt.

---

94 Wendehorst in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 3 Rn. 204.

95 § 2 Abs. 3 Referentenentwurf zum KI-Marktüberwachungsgesetz (Bearbeitungsstand: 11.09.2025); Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 13 Rn. 55.

KI im Bereich der Geldwäsche- und Betrugsprävention

Nach dem Geldwäschegesetz (GwG) Verpflichtete, wie beispielsweise Kredit- und Wertpapierinstitute, haben die Pflicht, über ein wirksames und angemessenes Risikomanagement zu verfügen, um Geldwäsche sowie Terrorismusfinanzierung zu verhindern.[96] Im Rahmen dessen haben sie ein angemessenes Risikomanagement (§ 4 GwG) einzurichten und interne Sicherungsmaßnahmen (z. B. nach § 25h KWG) zu ergreifen.[97] Hierzu gehört die Identifizierung des Vertragspartners bei Begründung der Geschäftsbeziehung (Know-Your-Customer-Prüfung) gemäß §§ 10 ff. GwG, die Identifizierung von wirtschaftlich Berechtigten sowie die kontinuierliche Überwachung der Geschäftsbeziehung einschließlich der durchgeführten Transaktionen.[98] In diesen Bereichen gilt es, große Datenmengen zu analysieren, wobei die heutzutage eingesetzten Prozesse und Systeme mithilfe von KI-Systemen effizienter, schneller und weniger fehleranfällig gestaltet werden können.[99]

---

[96] Kaetzler in: Zentes/Glaab, 4. Aufl. 2025, GwG § 4 Rn. 11.

[97] Schmitz in: IDW Kreditinstitute-WPH, 1. Aufl. 2020, Kap. O Rn. 65.

[98] Bitter in: Hoeren/Sieber/Holznagel MMR-HdB, 62. EL Juni 2024, Teil 15.4 Rn. 9.

[99] Bitter in: Hoeren/Sieber/Holznagel MMR-HdB, 62. EL Juni 2024, Teil 15.4 Rn. 10.

Bislang gibt es in dem Zusammenhang aus der Verwaltungspraxis noch keine speziellen Vorgaben für Big-Data-Anwendungen und KI-Systeme.[100]

KI im Risikocontrolling

Auch im Bereich des Risikocontrollings von Kreditinstituten bestehen Einsatzmöglichkeiten für KI-Systeme. Die Risikocontrollingprozesse müssen nach AT 4.3.2 MaRisk gewährleisten, dass die wesentlichen Risiken frühzeitig erkannt, vollständig erfasst und in angemessener Weise dargestellt werden können. Unter wesentlichen Risiken werden z. B. Liquiditätsrisiken, operationelle Risiken und Marktpreisrisiken verstanden. Die Risikocontrollingprozesse sind regelmäßig sowie bei sich ändernden Bedingungen auf ihre Angemessenheit zu überprüfen und ggf. anzupassen.[101] In diesem Bereich ist es denkbar, die Prozesse mit KI-unterstützter RPA-Technik[102] zu verbessern.[103]

Der inzwischen neu eingefügte Abschnitt AT 4.3.5 MaRisk stellt klar, dass die Anforderungen an das interne Kontrollsystem auch für technologiegestützte Innovation und KI gelten.

---

[100] Bitter in: Hoeren/Sieber/Holznagel MMR-HdB, 62. EL Juni 2024, Teil 15.4 Rn. 10.

[101] AT 4.3.2 Ziff. 5 MaRisk.

[102] RPA = Robotic Process Automation bzw. robotergesteuerte Prozessautomatisierung.

[103] Schalkowski/Ortiz: Roboterisierung im finanzwirtschaftlichen Risikomanagement, BC 2020, 130.

KI in der Internen Revision

Die Interne Revision als dritte Verteidigungslinie ist in regulierten Finanzunternehmen für die Prüfung und Beurteilung aller Aktivitäten und Prozesse des Risikomanagements und des internen Kontrollsystems verantwortlich.[104] Im Rahmen ihrer Tätigkeiten sichtet sie zahlreiche Dokumente und Prozesse, weswegen ihr ein vollständiges und uneingeschränktes Informationsrecht einzuräumen ist.[105]

Auch hier besteht das Potenzial, mithilfe von KI-Systemen schnellere, bessere und aussagekräftigere Prüfungsergebnisse zu erzielen. Aufgrund der großen Datenmengen und eines Mangels an Fachkräften sind oft nur Stichprobenprüfungen möglich, was den Einsatz technologischer Hilfsmittel notwendig macht.[106] KI-Systeme bieten hier vielversprechende Lösungen, da die verfügbaren Rechenkapazitäten und Datenmengen größer geworden sind und KI-Systeme umfangreiche Analysen, frühzeitige Identifikation von Risiken und Anomalien sowie die Automatisierung wiederkehrender Tätigkeiten ermöglichen.[107] Einsatzbereiche von KI-

---

[104] Leupold in: Krimphove/Lüke, 2. Aufl. 2025, R 10/2021 MaRisk und Erläuterungen AT4.4.3 Rn. 23.

[105] Leupold in: Krimphove/Lüke, 2. Aufl. 2025, R 10/2021 MaRisk und Erläuterungen AT4.4.3 Rn. 26.

[106] Ascheberg: Künstliche Intelligenz in der Internen Revision, BC 2025, 416 (417).

[107] Ascheberg: Künstliche Intelligenz in der Internen Revision, BC 2025, 416 (417).

Systemen sind dabei insbesondere in der Prüfungsplanung, -vorbereitung und -durchführung vorstellbar.[108]

KI bei der Kreditvergabe

Vielversprechende Einsatzmöglichkeiten für KI-Systeme bieten sich im Rahmen der Kreditvergabe an, auch wenn diese bereits häufig automatisiert erfolgt, wenn das eingesetzte System auf Basis des Kreditscorings ohne weitere Interaktion mit einem Mitarbeiter abschließend über die Kreditvergabe entscheidet.[109] So kann beispielsweise ein KI-System bei der Auswertung neuer Formen der Kreditwürdigkeitsbeurteilung einbezogen werden, bei denen beispielsweise Daten zum digitalen Fußabdruck eines Verbrauchers mit statistischen Verfahren einfließen.[110]

Zu beachten ist, dass KI-Systeme, die zur Bewertung der Kreditwürdigkeit eingesetzt werden, nach Art. 6 Abs. 2 i. V. m. Anhang III Nr. 5 lit. b AI Act grundsätzlich als Hochrisiko-KI-Systeme gelten.[111]

---

[108] Ascheberg: Künstliche Intelligenz in der Internen Revision, BC 2025, 416 (420).

[109] Bitter in: Hoeren/Sieber/Holznagel MMR-HdB, 62. EL Juni 2024, Teil 15.4 Rn. 17

[110] Langenbucher: Diskriminierung bei der Vergabe von Verbraucherkrediten?, BKR 2023, 205 (206).

[111] Rüsing: Verantwortungsvolle Kreditvergabe in der novellierten Verbraucherkreditrichtlinie, ZBB 2025, 24 (45).

2.2.3.4 Die verschiedenen Risikostufen der KI-Systeme

Der AI Act unterscheidet zwischen vier verschiedenen nach Risikograd abgestuften KI-Systemen, für die unterschiedliche Regelungen gelten. Dabei handelt es sich um Hochrisiko-KI-Systeme, KI-Systeme mit Transparenzrisiko, KI-Systeme mit keinem oder minimalem Risiko und KI-Systeme und Modelle mit allgemeinem Verwendungszweck (GPAI).

Hochrisiko-KI-Systeme

Hochrisiko-KI-Systeme unterliegen insgesamt den strengsten Vorgaben des AI Acts. Regelung zu Hochrisiko-KI-Systemen finden sich in Kapitel III (Artt. 6 bis 49) und in mehreren Anhängen. Bei Hochrisiko-KI-Systemen handelt es sich in der Praxis um eine begrenzte Anzahl von KI-Systemen, die sich potenziell nachteilig auf die Sicherheit der Menschen oder ihre Grundrechte auswirken.[112]

Wann ein KI-System als hochriskant eingestuft wird, ist nach Art. 6 AI Act zu bestimmen. Gemäß Art. 6 Abs. 2 AI Act gelten zusätzlich die in Anhang III genannten KI-Systeme als hochriskant. Dazu zählen z. B. biometrische Fernidentifizierungssysteme, KI-Systeme, die für Entscheidungen, die die Bedingungen von Arbeitsverhältnissen, Beförderungen und Kündigungen von Arbeitsvertragsverhältnissen beeinflussen, und KI-Systeme, die für die Kreditwürdigkeitsprüfung

[112] Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 5 Rn. 28.

und Bonitätsbewertung natürlicher Personen verwendet werden sollen.

KI-Systeme mit Transparenzrisiko

Die Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme sind in Art. 50 AI Act geregelt. In der deutschen Literatur werden sie als „KI-Systeme mit Transparenzrisiko“[113] oder als „KI-Systeme mit begrenztem Risiko“ bezeichnet.[114] Hierbei handelt es sich um KI-Systeme, die direkt mit Menschen interagieren[115] und deren Leistungen menschlichen Fähigkeiten nahe sind, und daher die Gefahr von Manipulation und Verwechslungen bestehen kann.[116] Nach ErwG 27 AI Act bedeutet Transparenz, dass KI-Systeme so entwickelt und verwendet werden müssen, dass sie angemessen nachvollziehbar und erklärbar sind, wobei den Menschen bewusst gemacht werden muss, dass sie mit einem KI-System kommunizieren oder interagieren, und dass die Betreiber ordnungsgemäß über die Fähigkeiten und Grenzen des KI-Systems informieren und die betroffenen Personen über ihre Rechte in Kenntnis setzen müssen. KI-

[113] Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 5 Rn. 42.

[114] Schwenke: Einführung KI-Verordnung: Grundlagen, Begriffe und Pflichtenkatalog, DSB 2024, 205.

[115] Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 5 Rn. 42.

[116] Martini in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 50 Rn. 1.

Systeme, die diese Pflichten betreffen, sind z. B. Chatbots im Kundensupport oder Deepfakes.[117]

KI-Systeme mit keinem oder minimalem Risiko

KI-Systeme mit keinem oder höchstens minimalem Risiko sollen einen Großteil der KI-Systeme darstellen, die in der EU Verwendung finden.[118] Hierunter fallen beispielsweise KI-basierte Videospiele, KI-Anwendungen zur Spam-Erkennung[119] oder Legal Tech AI Systeme[120].

KI-Systeme und Modelle mit allgemeinem Verwendungszweck (GPAI)

Der Definition aus Art. 3 Nr. 66 AI Act zufolge handelt es sich bei einem GPAI-System um ein KI-System, das auf einem KI-Modell mit allgemeinem Verwendungszweck beruht und in der Lage ist, einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen. Das GPAI-Modell wird in Art. 3 Nr. 63 AI Act definiert.

Der AI Act unterscheidet zwischen einfachen GPAI-Modellen und GPAI-Modellen mit systemischem Risiko. Die Kriterien

---

[117] Schwenke: Einführung KI-Verordnung: Grundlagen, Begriffe und Pflichtenkatalog, DSB 2024, 205; Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 5 Rn. 44.

[118] Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 5 Rn. 45.

[119] Schwenke: Einführung KI-Verordnung: Grundlagen, Begriffe und Pflichtenkatalog, DSB 2024, 205; Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 5 Rn. 45.

[120] Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 5 Rn. 45.

zur Einstufung als GPAI-Modell mit systemischem Risiko finden sich in Art. 51 AI Act und die Pflichten für Anbieter von GPAI-Modellen mit systemischem Risiko in Art. 55 AI Act. Die Pflichten für Anbieter von einfachen GPAI-Modellen sind in Art. 53 AI Act geregelt.

Verbotene Praktiken im KI-Bereich

In Art. 5 AI Act werden Praktiken im KI-Bereich aufgezählt, die verboten sind. Hierzu gehören z. B. KI-Anwendungen, die kriminelles Verhalten aufgrund persönlicher Merkmale vorhersagen oder Menschen manipulieren.[121]

2.2.3.5 Governance

Die Anforderungen, die Auswirkungen auf die Aufbauorganisation in einem Finanzunternehmen haben könnten, sind je nach Einsatz von KI-Systemen mit verschiedenen Risikotypen unterschiedlich. Während der AI Act für Hochrisiko-KI-Systeme zahlreiche Anforderungen vorschreibt, sind die Pflichten in Zusammenhang mit den weniger risikoreichen KI-Systemen überschaubar.

Allgemeine KI-Governance

Unabhängig vom Risikograd des jeweiligen KI-Systems sieht die BaFin in ihrer Veröffentlichung zu Big Data und Künstlicher Intelligenz eine klare Verantwortung bei der *Geschäftsleitung* für unternehmensweite Strategien und Leit- bzw.

[121] Schwenke: Einführung KI-Verordnung: Grundlagen, Begriffe und Pflichtenkatalog, DSB 2024, 205.

Richtlinien zum Einsatz von algorithmenbasierten Entscheidungsprozessen.[122] Dies setze ein adäquates technisches Verständnis bei der Geschäftsleitung und in den unabhängigen Kontrollfunktionen voraus.[123]

Um einen gesetzeskonformen Einsatz von KI zu gewährleisten, ist es ratsam, eine unternehmensweite *KI Policy* einzuführen.[124] Die KI Policy sollte neben den Compliance-Anforderungen aus dem AI Act weitere rechtliche Anforderungen wie z. B. branchenspezifische Regelungen sowie Anforderungen aus dem Urheber- und Datenschutzrecht enthalten.[125]

Nach Art. 4 AI Act sind Anbieter und Betreiber außerdem dazu verpflichtet, sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an *KI-Kompetenz* verfügen. Es kann sinnvoll sein, einen betriebsinternen *KI-Beauftragten* zu benennen, wel-

---

[122] BaFin, Big Data und künstliche Intelligenz: Prinzipien für den Einsatz von Algorithmen in Entscheidungsprozessen, Juni 2021, S. 6.

[123] BaFin, Big Data und künstliche Intelligenz: Prinzipien für den Einsatz von Algorithmen in Entscheidungsprozessen, Juni 2021, S. 6; Denga: KI in der Anlageberatung, WM 2024 Heft 49, 2275 (2278).

[124] Sassenberg: AI Governance Framework – Regelungsgegenstand der AI Policy, RDi 2025, 346 Rn. 5.

[125] Sassenberg: AI Governance Framework – Regelungsgegenstand der AI Policy, RDi 2025, 346 Rn. 7.

cher mitunter dafür sorgen könnte, dass die relevanten Personen ausreichend zum Thema KI geschult werden.[126] Weitere Aufgaben könnten in der Überwachung der Einhaltung ethischer Richtlinien und Standards und in der Beantwortung KI-bezogener Fragen liegen.[127]

Für eine strukturierte Steuerung der Planung des Einsatzes von KI sollten Unternehmen einen *Prozess zur Risikoklassifizierung* einrichten und diese Risikoklassifizierung dazu nutzen, um ein *Verzeichnis über die eingesetzten KI-Systeme* aufzubauen, auch wenn dies nicht explizit durch den AI Act vorgegeben wird.[128]

Darüber hinaus wird empfohlen, ein multidisziplinär besetztes *KI-Board* zu etablieren, das die KI-Governance verantwortet, deren Anforderungen definiert und die Kontrolle der Einhaltung der Vorgaben übernimmt.[129]

Governance als Anbieter von Hochrisiko-KI-Systemen

Die Anforderungen an Hochrisiko-KI-Systeme sind in Artt. 8 ff. AI Act geregelt. Dabei sind die Formulierungen allgemein

---

[126] Wendehorst in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 4 Rn. 19.

[127] Wendehorst in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 4 Rn. 18 f; Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 4 Rn. 15.

[128] Sassenberg: AI Governance Framework – Regelungsgegenstand der AI Policy, RDi 2025, 346 Rn. 9 f.

[129] Sassenberg: AI Governance Framework – Regelungsgegenstand der AI Policy, RDi 2025, 346 Rn. 38 (mwN).

gehalten und nennen keinen spezifischen Normadressaten.[130] Aus der Bestimmung in Art. 16 lit. a AI Act ist zu entnehmen, dass der die Anforderungen an Hochrisiko-KI-Systeme betreffende Abschnitt (Artt. 8 bis 15 AI Act) Anbieter verpflichtet. Hieraus lässt sich ableiten, dass Anbieter die primären Adressaten dieser Vorschriften sind.[131] In dem Zusammenhang ist jedoch zu beachten, dass Art. 25 AI Act ergänzend zu Art. 16 AI Act die Verantwortlichkeiten entlang der KI-Wertschöpfungskette regelt. So unterliegen z. B. Betreiber nach Art. 25 Abs. 1 lit. a AI Act auch den Anbieterpflichten, wenn ein Hochrisiko-KI-System mit ihrem Namen oder ihrer Handelsmarke versehen ist oder gemäß Art. 25 Abs. 1 lit. b und c AI Act eine wesentliche Änderung oder Veränderung der Zweckbestimmung an dem Hochrisiko-KI-System vorgenommen wurde.[132] Dies ist häufig der Fall, wenn KI-Systeme von Unternehmen individuell angepasst werden.[133]

Sofern ein Finanzunternehmen selbst als Anbieter agiert oder KI-Systeme als Betreiber anwendet, die so angepasst werden, dass sie zu Hochrisiko-KI-Systemen werden, ist es

---

[130] Gerdemann in: BeckOK KI-Recht, 3. Ed. 1.8.2025, KI-VO Art. 8 Rn. 12.

[131] Gerdemann in: BeckOK KI-Recht, 3. Ed. 1.8.2025, KI-VO Art. 8 Rn. 12; Braun Binder/Egli in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 8 Rn. 31.

[132] Braun Binder/Egli in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 8 Rn. 32.

[133] Braun Binder/Egli in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 8 Rn. 32.

zur Einhaltung der Anforderungen an Hochrisiko-KI-Systeme verpflichtet und hat infolgedessen aus aufbauorganisatorischer Sicht die nachfolgend aufgeführten Punkte zu berücksichtigen.

Risikomanagement

Art. 9 AI Act enthält Vorgaben für das Risikomanagement von Hochrisiko-KI-Systemen. So ist u. a. nach Art. 9 Abs. 1 AI Act ein Risikomanagementsystem einzurichten.

Für Finanzunternehmen sind Risikomanagementvorgaben nicht fremd. Neben den Mindestanforderungen an das Risikomanagement für verschiedene Arten von Finanzunternehmen[134] müssen diese bereits zusätzliche Risikomanagementvorgaben aus Datenschutzgesetzen und DORA einhalten. Sinnvoll wäre daher eine Verzahnung des Hochrisiko-KI-Risikomanagements mit dem bereits bestehenden Informationssicherheits-, Geschäftsfortführungs-, Datenschutz- und IKT-Risikomanagement.[135]

Aufbauorganisatorisch wäre es denkbar, die Überwachung des Hochrisiko-KI-Risikomanagements in den Verantwortungsbereich der IKT-Risikokontrollfunktion i. S. v. DORA zu integrieren, da es sich bei einem KI-System in aller Regel um ein IKT-System handeln dürfte.

---

[134] Wie z. B. die MaRisk für Kredit- und Finanzdienstleister.

[135] Knoblich/Krimphove: Die neue KI-VO im Regelungsdickicht des Aufsichtsrechts, BKR 2024, 843 (845).

Technische Voraussetzungen und menschliche Aufsicht

Für die technischen Aspekte der Entwicklung von Hochrisiko-KI-Systemen, wie z. B. Daten-Governance, technische Dokumentation und Cybersicherheit, enthalten Artt. 10 bis 12 AI und 15 Act spezifische Vorgaben. Diese wären maßgeblich von den an der Entwicklung von Hochrisiko-KI-Systemen beteiligten Fachbereichen zu beachten.

Gemäß Art. 14 AI Act müssen Hochrisiko-KI-Systeme außerdem menschlich beaufsichtigt werden. Die menschliche Aufsicht dient nach Art. 14 Abs. 2 AI Act der Verhinderung oder Minimierung möglicher Risiken für Gesundheit, Sicherheit oder Grundrechte.

Qualitätsmanagementsystem

Art. 17 Abs. 1 AI Act schreibt die Einrichtung eines Qualitätsmanagementsystems vor. Nach Art. 17 Abs. 4 AI Act gilt die Pflicht hierzu zum Großteil als erfüllt bei Finanzunternehmen, die finanzmarktrechtlichen Regelungen oder Verfahren der internen Unternehmensführung unterliegen und diese einhalten.[136] Dennoch haben Finanzunternehmen zusätzlich die Risikomanagementvorgaben nach Art. 9, die Vorgaben zur Beobachtung nach dem Inverkehrbringen nach Art. 72

[136] Henke in: BeckOK KI-Recht, 3. Ed. 1.8.2025, KI-VO Art. 17 Rn. 30 mit weiteren Ausführungen, welche Leitlinien solche Organisationsstrukturanforderungen beinhalten.

und jene hinsichtlich der Verfahren zur Meldung schwerwiegender Vorfälle nach Art. 73 AI Act zu beachten.[137]

Beobachtung nach dem Inverkehrbringen

Anbieter müssen außerdem die Vorgaben nach Art. 72 AI Act zur Beobachtung nach dem Inverkehrbringen durch die Anbieter einhalten, die auf einem Plan für die Beobachtung nach dem Inverkehrbringen für Hochrisiko-KI-Systeme beruhen. Die Erfahrung mit Hochrisiko-KI-Systemen soll von den Anbietern berücksichtigt werden, um ihre Systeme zu verbessern und um etwaige Korrekturmaßnahmen im Konzeptions- und Entwicklungsprozess zu ergreifen.[138]

Pflichten der Betreiber von Hochrisiko-KI-Systemen

Pflichten der Betreiber von Hochrisiko-KI-Systemen nach Art. 26 AI Act

Gemäß Art. 26 AI Act haben Betreiber von Hochrisiko-KI-Systemen mitunter folgende besondere Pflichten zu erfüllen:

- Treffen von geeigneten technischen und organisatorischen Maßnahmen, um die Verwendung des Hochrisiko-KI-Systems entsprechend den beigefügten Betriebsanleitungen zu gewährleisten (Abs. 1),

[137] I. Eisenberger in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 17 Rn. 4.
[138] ErwG 155 AI Act.

- Übertragung der menschlichen Aufsicht über das Hochrisiko-KI-System auf eine qualifizierte und über die nötige KI-Kompetenz verfügende natürliche Person (Abs. 2),
- Sicherstellen, dass die Eingabedaten der Zweckbestimmung des Hochrisiko-KI-Systems entsprechen und ausreichend repräsentativ sind (Abs. 4),
- Informieren der Arbeitnehmer vor der Verwendung von Hochrisiko-KI-Systemen am Arbeitsplatz (Abs. 7),
- Durchführung einer Datenschutz-Folgenabschätzung (Abs. 9),
- Informieren der natürlichen Personen, die von Entscheidungen betroffen sind, die von einem Hochrisiko-KI-System getroffen werden (Abs. 11),
- Zusammenarbeit mit zuständigen Behörden (Abs. 12).

Grundrechte-Folgenabschätzung

Gemäß Art. 27 AI Act sind Betreiber von bestimmten in Art. 27 Abs. 1 AI Act genannten Hochrisiko-KI-Systemen verpflichtet, vor Inbetriebnahme eine Grundrechte-Folgenabschätzung durchzuführen und die Ergebnisse der Marktüberwachungsbehörde mitzuteilen. Diese Pflicht gilt für KI-Systeme, die für die Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher Personen verwendet werden sollen (Anhang III Nr. 5 lit. b AI Act), und solche, die für die Risiko-

bewertung und Preisbildung in Bezug auf natürliche Personen im Fall von Lebens- und Krankenversicherungen verwendet werden sollen (Anhang III Nr. 5 lit. c AI Act).

Ziel der Grundrechte-Folgenabschätzung ist laut ErwG 96 AI Act, dass der Betreiber die spezifischen Risiken für die Rechte von Einzelpersonen oder Gruppen von Einzelpersonen, die wahrscheinlich betroffen sein werden, ermittelt und Maßnahmen ermittelt, die im Falle eines Eintretens dieser Risiken zu ergreifen sind.

Pflichten in Zusammenhang mit KI-Systemen mit Transparenzrisiko

Für KI-Systeme mit Transparenzrisiko haben Anbieter und Betreiber Art. 50 AI Act zu beachten. Für diese KI-Systeme gelten maßgeblich Transparenzpflichten und darüber hinaus keine besonderen Regulierungsanforderungen, da sie keine hohen Risiken für die Grundrechte oder sonstige Schutzbedürfnisse bergen.[139]

KI-Systeme mit Transparenzrisiko müssen grundsätzlich so gestaltet sein, dass natürliche Personen spätestens zum Zeitpunkt der ersten Interaktion oder Aussetzung klar und eindeutig informiert werden, dass sie mit einem KI-System interagieren.

[139] Martini in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 50 Rn. 9.

Bei einem Verstoß gegen die Vorgaben des Art. 50 AI Act drohen Geldbußen von bis zu 15 Mio. EUR gemäß Art. 99 Abs. 4 lit. g AI Act.[140]

2.2.3.6 Meldung von schwerwiegenden Vorfällen

Der Begriff „schwerwiegender Vorfall" wird in Art. 3 Nr. 49 AI Act definiert und meint einen Vorfall oder eine Fehlfunktion bezüglich eines KI-Systems, das bzw. die direkt oder indirekt beispielsweise den Tod oder die schwere gesundheitliche Schädigung einer Person oder die Verletzung von Pflichten aus den Unionsrechtsvorschriften zum Schutz der Grundrechte zur Folge hat.

Nach Art. 73 AI Act sind schwerwiegende Vorfälle den Marktüberwachungsbehörden der Mitgliedstaaten zu melden, in denen der Vorfall stattgefunden hat. Diese Meldepflicht gilt für Vorfälle, die Hochrisiko-KI-Systeme betreffen. Zur Meldung verpflichtet sind primär Anbieter von Hochrisiko-KI-Systemen, subsidiär jedoch auch Betreiber, da diese nach Art. 26 Abs. 5 Satz 3 AI Act die Meldung übernehmen, wenn sie den Anbieter nicht erreichen.[141] Stellen Betreiber ihrerseits einen schwerwiegenden Vorfall fest, informieren sie ge-

[140] Martini in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 50 Rn. 14.

[141] Hilgendorf/Härtlein in: HK-KI-VO/Hilgendorf/Härtlein, 1. Aufl. -1, KI-VO Art. 73 Rn. 2.

mäß Art. 26 Abs. 5 Satz 2 AI Act unverzüglich zuerst den Anbieter und dann den Einführer oder Händler und die zuständigen Marktüberwachungsbehörden über diesen Vorfall.

Nach Art. 73 Abs. 2 AI Act hat die Meldung unmittelbar zu erfolgen, nachdem der Anbieter den kausalen Zusammenhang zwischen dem KI-System und dem schwerwiegenden Vorfall oder die naheliegende Wahrscheinlichkeit eines solchen Zusammenhangs festgestellt hat und in jedem Fall spätestens 15 Tage, nachdem der Anbieter oder ggf. der Betreiber Kenntnis von diesem schwerwiegenden Vorfall erlangt hat.

2.2.3.7 Beobachtung nach dem Inverkehrbringen

Anbieter von Hochrisiko-KI-Systemen müssen nach Art. 72 AI Act ein System zur Beobachtung nach dem Inverkehrbringen einrichten, welches auf einem Plan für die Beobachtung nach dem Inverkehrbringen beruht. Hierbei handelt es sich um eine Produktbeobachtungspflicht, die zur Minimierung von Gefahren dient, die von dem Hochrisiko-KI-System ausgehen.[142]

Nach Art. 3 Nr. 25 AI Act umfasst das System zur Beobachtung nach dem Inverkehrbringen alle Tätigkeiten, die Anbieter von KI-Systemen zur Sammlung und Überprüfung von Er-

[142] Hilgendorf/Härtlein in: HK-KI-VO/Hilgendorf/Härtlein, 1. Aufl. -1, KI-VO Art. 72 Rn. 1.

fahrungen mit der Verwendung der von ihnen in Verkehr gebrachten oder in Betrieb genommenen KI-Systeme durchführen, um festzustellen, ob unverzüglich nötige Korrektur- oder Präventivmaßnahmen zu ergreifen sind.

Die Produktbeobachtung basiert insbesondere auf den von Betreibern bereitgestellten Daten.[143] Datenschutzrechtlich fungiert Art. 72 Abs. 2 AI Act als Rechtsgrundlage im Rahmen des Art. 6 Abs. 1 lit. c DSGVO.[144]

[143] Hartmann in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 72 Rn. 1.
[144] Hartmann in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 72 Rn. 6.

2.2.4 Financial Data Access Regulation

2.2.4.1 Hintergrund

Mit FIDA verfolgt die EU-Kommission das Ziel, den gesamten Finanzsektor weiter ins digitale Zeitalter zu führen und anhand des neuen Open-Finance-Rahmens für einen sicheren und offenen Zugang zu Kundendaten für ein breiteres Spektrum von Finanzdienstleistungen zu sorgen.[145] Im Bereich des Zahlungsverkehrs gibt es bereits das Konstrukt des Open Bankings, bei dem Dritten Zugriff auf Zahlungsdaten gewährt wird, sofern dies vom Kunden gewünscht ist, um Innovationen für Märkte und Kunden zu ermöglichen.[146] Im Rahmen von Open-Finance soll der Ansatz der kontrollierten Datenweitergabe von Zahlungsverkehrsdaten auf weitere Finanzdienstleistungen erweitert werden.[147] FIDA befindet sich noch in der Entwurfsfassung und ist Teil eines übergeordne-

[145] EU-Kommission zu FIDA, https://finance.ec.europa.eu/digital-finance/framework-financial-data-access_en (zuletzt abgerufen am 14.09.2025); zur Übersetzung des Inhalts der Seite wurde das KI-Tool Copilot genutzt und kritisch überprüft.

[146] BaFin zum Open Banking, https://www.bafin.de/EN/Aufsicht/FinTech/Geschaeftsmodelle/OpenBanking_OpenFinance/OpenBanking_OpenFinance_node_en.html (zuletzt abgerufen am 14.09.2025).

[147] ErwG 4 FIDA-E; Denga: Entwurf einer Financial Data Access-Verordnung (FiDA), MMR 2025, 701.

ten Pakets, zu dem auch die Modernisierung des Zahlungsdiensteregimes PSD 2[148] und die Einführung einer Zahlungsdiensteverordnung (Payment Services Regulation – PSR) gehört.[149]

FIDA-E soll im Sinne einer verantwortungsvollen Datenwirtschaft sicherstellen, dass sowohl Verbraucher als auch Unternehmen über eine effektive Kontrolle über ihre Finanzdaten verfügen und die Möglichkeit haben, von offenen und sicheren datengestützten Innovationen zu profitieren.[150] Die EU verfolgt ein politisches Interesse daran, Kunden von Finanzinstituten den Zugang zu ihren Finanzdaten zu ermöglichen, um die Vorteile des Datenaustauschs zu nutzen und datengestützte Finanzprodukte zu entwickeln.[151] So kann beispielsweise der Austausch von Daten über laufende Anlagen Innovationen in der Anlageberatung fördern[152] oder der Austausch von Daten zu Hypotheken, Darlehen und Ersparnissen den Kunden einen besseren Überblick über ihre Finanzen ermöglichen.[153]

---

148 Richtlinie (EU) 2015/2366 über Zahlungsdienste.

149 EU-Kommission zu FIDA, https://finance.ec.europa.eu/digital-finance/framework-financial-data-access_en (zuletzt abgerufen am 14.09.2025).

150 ErwG 1 und 2 FIDA-E.

151 ErwG 3 FIDA-E.

152 ErwG 11 FIDA-E.

153 ErwG 12 FIDA-E.

Daten zu Nichtlebensversicherungen und zur Altersvorsorge sind wichtig, um personalisierte Versicherungsprodukte zu entwickeln und den Kunden zu helfen, ihre Risiken besser zu steuern.[154] Die Daten für die Kreditwürdigkeitsprüfung von Unternehmen sollen ebenfalls in den Anwendungsbereich der Verordnung fallen, um den Zugang zu Finanzmitteln zu verbessern.[155]

Die bisherige Fragmentierung der Finanzdatenwirtschaft in der EU und die bestehenden Hindernisse im Datenaustausch schränken die Möglichkeiten für personalisierte Produkte ein und hindern insbesondere KMU daran, von besseren, bequemeren und automatisierten Finanzdienstleistungen zu profitieren.[156]Für einen nahtlosen Datenzugang sind hochwertige Anwendungsprogrammierschnittstellen erforderlich, die bislang nur wenige Finanzinstitute, die Dateninhaber sind, bereitstellen, was die Nachfrage nach Datenzugang begrenzt.[157] Der künftig optimierte Austausch soll auf der Berechtigung durch die Kunden beruhen, welche die Kunden jederzeit widerrufen können.[158]

[154] ErwG 14 und 15 FIDA-E.
[155] ErwG 16 FIDA-E.
[156] ErwG 6 FIDA-E.
[157] ErwG 7 FIDA-E.
[158] ErwG 10 FIDA-E.

FIDA-E fügt sich in die übergeordnete europäische Datenstrategie[159] ein und unterliegt wie auch weitere Initiativen der europäischen Datenstrategie, zu denen z. B. der Data Act oder der Data Governance Act gehören, den Grundprinzipien für den Datenzugang und die Datenverarbeitung.[160]

2.2.4.2 Adressaten und zuständige Aufsicht

Adressaten

Die Verordnung soll für die in Art. 2 Abs. 2 lit. a bis o FIDA-E genannten Stellen in ihrer Eigenschaft als Dateninhaber oder Datennutzer gelten. Dazu gehören beispielsweise Kreditinstitute, Wertpapierfirmen, Anbieter von Krypto-Dienstleistungen, Versicherungs- und Rückversicherungsunternehmen und Einrichtungen der betrieblichen Altersversorgung. Aus ErwG 23 FIDA-E geht hervor, dass bestimmte Finanzinstitute aus Gründen, die mit ihrer Größe oder den von ihnen erbrachten Dienstleistungen zusammenhängen, die die Einhaltung der FIDA-Vorgaben zu schwierig machen würden, nicht in den Anwendungsbereich der Verordnung fallen.[161]

---

[159] Eine europäische Datenstrategie, EU-Kommission, COM (2020) 66 final (näheres zum gemeinsamen europäischen Finanzdatenraum in Ziff. 5).

[160] Denga: Entwurf einer Financial Data Access-Verordnung (FiDA), MMR 2025, 701 (702).

[161] Dies beinhaltet Einrichtungen der betrieblichen Altersversorgung, die Altersversorgungssysteme betreiben, die insgesamt nicht mehr als 15 Mitglieder haben, sowie Versicherungsvermittler, die Kleinstunternehmen oder KMU sind (ErwG 23 FIDA-E).

Dateninhaber ist nach Art. 3 Nr. 5 FIDA-E ein Finanzinstitut, das kein Kontoinformationsdienstleister ist und die in Art. 2 Abs. 1 aufgeführten Kundendaten erhebt, speichert und anderweitig verarbeitet.

Datennutzer ist nach Art. 3 Nr. 6 FIDA-E eine der in Art. 2 Abs. 2 aufgeführten Stellen, die nach Einwilligung des Kunden rechtmäßigen Zugang zu den in Art. 2 Abs. 1 aufgeführten Kundendaten erhält.

Beim *Finanzinformationsdienstleister* (im Folgenden: FISP für Financial Information Service Provider) handelt es sich nach Art. 3 Nr. 7 FIDA-E um einen Datennutzer, der zum Zwecke der Erbringung von Finanzinformationsdienstleistungen berechtigt ist, auf Kundendaten zuzugreifen.

Bei FISPs besteht die Besonderheit, dass diese zur Erbringung von Finanzinformationsdienstleistungen zugelassen sein müssen. Der Antrag auf Zulassung als FISP ist in Art. 12 und die Erteilung und der Entzug der Zulassung in Art. 14 FIDA-E geregelt. Die EBA wird nach Art. 15 FIDA-E ein zentrales elektronisches Register führen, aus dem ersichtlich sein wird, welche FISPs über eine Zulassung verfügen.

Zuständige Aufsicht

Die Mitgliedstaaten müssen nach Art. 17 Abs. 1 Satz 1 FIDA-E zuständige Behörden benennen, die für die Wahrnehmung der FIDA-Funktionen und Aufgaben verantwortlich sind. Die Befugnisse der zuständigen Behörden sind in Art. 18 FIDA-

E geregelt und beinhalten u. a. das Verlangen von Informationen und Dokumenten sowie die Vornahme von Prüfungen in den Geschäftsräumen. In Deutschland wird voraussichtlich die BaFin als zuständige Behörde benannt werden.[162]

2.2.4.3 Kategorien von Finanzdaten

Der Verordnungsentwurf legt fest, welche Finanzinformationen zwischen Dateninhabern und -nutzern zu teilen sind. Art. 2 Abs. 1 FIDA-E listet die folgenden sechs Datenkategorien auf:

- Hypothekarkreditverträge, Darlehen und Konten, ausgenommen Zahlungskonten im Sinne von PDS2, einschließlich Daten zu Saldo, Konditionen und Transaktionen (lit. a),
- Ersparnisse, Investitionen in Finanzinstrumente, Versicherungsanlageprodukte, Kryptowerte, Immobilien und andere damit verbundene finanzielle Vermögenswerte sowie der wirtschaftliche Nutzen dieser Vermögenswerte; einschließlich Daten, die zur Beurteilung der Eignung und Zweckmäßigkeit gemäß Art. 25 MiFID II[163] erhoben werden (lit. b),

[162] Dies lässt zumindest die Informationsseite der BaFin zum Thema Open Finance vermuten, https://www.bafin.de/DE/Aufsicht/FinTech/Geschaeftsmodelle/OpenBanking_OpenFinance/OpenBanking_OpenFinance_node.html (zuletzt abgerufen am 15.09.2025).

[163] Richtlinie 2014/65/EU über Märkte für Finanzinstrumente.

- Ruhegehaltsansprüche aus betrieblichen Altersversorgungssystemen gemäß Solvency II[164] und der EbAV-II-Richtlinie[165] (lit. c),
- Ruhegehaltsansprüche aus Paneuropäischen Privaten Pensionsprodukten gemäß PEPP[166] (lit. d),
- Nichtlebensversicherungsprodukte gemäß Solvency II, ausgenommen Krankenversicherungsprodukte; einschließlich Daten, die zur Ermittlung der Wünsche und Bedürfnisse des Kunden gemäß Art. 20 IDD[167] erhoben werden, sowie Daten, die zur Beurteilung der Eignung und Zweckmäßigkeit gemäß Art. 30 IDD erhoben werden (lit. e),
- Daten, die zur Beurteilung der Kreditwürdigkeit eines Unternehmens im Rahmen eines Kreditantragsverfahrens oder bei einem Antrag auf Bonitätsprüfung erhoben werden (lit. f).

Gemäß ErwG 9 FIDA-E sollte die Verordnung nicht für Daten im Zusammenhang mit der Krankenversicherung eines Ver-

164 Richtlinie 2009/138/EG betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit.

165 Richtlinie (EU) 2016/2341 über die Tätigkeiten und die Beaufsichtigung von Einrichtungen der betrieblichen Altersversorgung.

166 Verordnung (EU) 2019/1238 über ein Paneuropäisches Privates Pensionsprodukt.

167 Richtlinie (EU) 2016/97 über Versicherungsvertrieb (Insurance Distribution Directive).

brauchers, Lebensversicherungsprodukte eines Verbrauchers[168] und mit der Kreditwürdigkeitsprüfung eines Verbrauchers gelten.[169]

2.2.4.4 Organisatorische Umsetzung

Gemäß Art. 9 FIDA-E sind Dateninhaber und Datennutzer verpflichtet, innerhalb von 18 Monaten nach Inkrafttreten der Verordnung Mitglied eines Systems für den Austausch von Finanzdaten (im Folgenden: FDSS für Financial Data Sharing Schemes)[170] zu werden. In den FDSS sollen Daten- und Schnittstellenstandards sowie gemeinsame standardisierte vertragliche Rahmenbedingungen für den Zugang zu bestimmten Datensätzen und Governance-Vorschriften für den Datenaustausch ausgearbeitet werden.[171] Die Anforderungen an FDSS sind in Art. 10 Abs. 1 FIDA-E geregelt. Demnach sind Mitglieder von FDSS nicht nur Dateninhaber und Datennutzer, sondern auch Verbraucherorganisationen und -verbände (Art. 10 Abs. 1 lit. a FIDA-E).

Art. 10 Abs. 1 lit. h FIDA-E legt fest, dass das Vergütungsmodell für die Zugangsabgeltung nach Art. 5 Abs. 2 FIDA-E

---

168 ausgenommen Lebensversicherungsverträge, die durch Versicherungsanlageprodukte abgedeckt sind.

169 Denga: Entwurf einer Financial Data Access-Verordnung (FiDA), MMR 2025, 701 (702).

170 Denga: Entwurf einer Financial Data Access-Verordnung (FiDA), MMR 2025, 701 (704).

171 ErwG 25 FIDA-E.

auf bestimmten Grundsätzen basieren muss.[172] So soll das Modell u. a. auf einer objektiven, transparenten und nichtdiskriminierenden Methode beruhen, die von den Mitgliedern vereinbart wurde (Art. 10 Abs. 1 lit. h ii) FIDA-E). Für Kleinstunternehmen und KMU darf die vereinbarte Vergütung nach Art. 10 Abs. 1 lit. h UAbs. 2 FIDA-E nicht höher sein als die Kosten, die mit der Bereitstellung der Daten für den Datenempfänger unmittelbar zusammenhängen und dem Auftrag zuzuordnen sind.

Sollte für eine oder mehrere Kundendatenkategorien kein System für den Austausch von Finanzdaten entwickelt werden, sieht Art. 11 FIDA-E vor, dass die EU-Kommission zum Erlass eines delegierten Rechtsakts befugt ist, in dem gemeinsame Standards für Daten und ggf. technische Schnittstellen vorgegeben werden.[173] Die Initiative „Digitaleurope“ spricht sich für FDSS auf EU-Ebene vor solchen auf nationaler Ebene aus, damit der Binnenmarkt nicht weiter fragmentiert wird.[174] In Deutschland hat sich die Initiative „German Open Finance Charta 2025“ (GOFC) zur Förderung eines offenen Finanzdaten-Ökosystems in Deutschland und Europa gebildet. Die GOFC betont die Notwendigkeit strategischer Zusammenarbeit zwischen verschiedenen Akteuren wie

---

[172] Denga: Entwurf einer Financial Data Access-Verordnung (FiDA), MMR 2025, 701 (704).

[173] Ausführliche Erläuterung einzelner Bestimmungen des FIDA-Vorschlags.

[174] Digitaleurope, Building a future-proof open finance ecosystem vom 12.02.2025, 6.

Banken, Versicherern, FinTechs und Technologieunternehmen.[175]

In technischer Hinsicht sind die Akteure verpflichtet, im Rahmen der FDSS Daten- und Schnittstellenstandards zu entwickeln und Koordinierungsmechanismen für den Betrieb von Dashboards für die Zugriffsberechtigung auf Finanzdaten einzurichten.[176]

Somit ergibt sich für Finanzunternehmen neben dem Aufwand, FDSS zu bilden und die vertraglichen Einzelheiten zu Datenaustausch, Vergütung und Haftung auszuhandeln bzw. FDSS beizutreten, weiterer Aufwand auf technischer Ebene in Form der Errichtung von Schnittstellen und Dashboards.

2.2.4.5 Weitere einzuhaltende Pflichten

Dateninhaber und Datennutzer unterliegen unterschiedlichen Verpflichtungen.

Dateninhaber haben Kunden auf Antrag die in Art. 2 Abs. 1 FIDA-E genannten Daten unverzüglich, unentgeltlich, kontinuierlich und in Echtzeit (Art. 4 FIDA-E) und dem Datennutzer auf Antrag des Kunden die Kundendaten für die vom Kunden festgelegten Zwecke (Art. 5 FIDA-E) zur Verfügung

[175] German Open Finance Charta 2025, https://openfinance-charta.de/ (zuletzt abgerufen am 28.09.2025).

[176] Ausführliche Erläuterung einzelner Bestimmungen des FIDA-Vorschlags.

zu stellen. Darüber hinaus haben sie nach den Vorgaben des Art. 8 FIDA-E den Kunden ein Dashboard zur Überwachung und Verwaltung der Zugriffsberechtigungen zur Verfügung zu stellen.

Demgegenüber regelt Art. 6 FIDA-E die Pflichten der Datennutzer in Bezug auf den Erhalt von Kundendaten. Dazu zählt u. a., dass ein Datennutzer nur auf Kundendaten zugreifen darf, wenn er zuvor von einer zuständigen Behörde als Finanzinstitut oder FISP zugelassen wurde (Art. 6 Abs. 1 FIDA-E) und sich der Zugriff auf die bereitgestellten Kundendaten auf die Zwecke beschränkt, denen der Kunde zugestimmt hat (Art. 6 Abs. 2 FIDA-E).

Art. 28 FIDA-E regelt den grenzüberschreitenden Zugang von FISP zu Kundendaten innerhalb der EU. Gemäß Art. 28 Abs. 1 FIDA-E können FISP und Finanzinstitute im Rahmen der Dienstleistungs- oder Niederlassungsfreiheit auf Daten zugreifen, die sich im Besitz von Dateninhabern in anderen Mitgliedstaaten befinden. Vor dem erstmaligen Zugriff müssen FISP nach Art. 28 Abs. 2 FIDA-E ihrem Herkunftsmitgliedstaat bestimmte Angaben übermitteln, etwa zu den Mitgliedstaaten, in denen der FISP Zugang erhalten möchte. Diese Informationen werden innerhalb eines Monats an den Aufnahmestaat weitergeleitet (Art. 28 Abs. 3 FIDA-E).

2.2.4.6 Daten- und Geschäftsgeheimnisschutz

ErwG 30 FIDA-E sieht eine Verpflichtung der Teilnehmer der FDSS vor, die vertragliche Haftung für Datenschutzverletzungen zu vereinbaren und festzulegen, wie potenzielle

Streitigkeiten zwischen Dateninhabern und Datennutzern bezüglich der Haftung beigelegt werden sollen, da die Kunden wissen sollten, welche Rechte sie haben, wenn beim Austausch von Daten Probleme auftreten, und an wen sie sich wenden können, um eine Vergütung zu erhalten. Daher sollte jeder Vertrag Haftungsregeln sowie klare Pflichten und Rechte enthalten, um die Haftung zwischen dem Dateninhaber und dem Datennutzer zu bestimmen. ErwG 10 stellt darüber hinaus klar, dass Datennutzer für die Verarbeitung personenbezogener Daten eine gültige Rechtsgrundlage nach der DSGVO vorweisen müssen. Der Kunde soll das Recht haben, die einem Datennutzer erteilte Berechtigung zum Datenaustausch zu widerrufen.[177]

Der Schutz von Geschäftsgeheimnissen ist in Artt. 5 und 6 FIDA-E geregelt. Sowohl Dateninhaber als auch Datennutzer sind verpflichtet, beim Zugriff auf Kundendaten die Vertraulichkeit von Geschäftsgeheimnissen sowie die Rechte des geistigen Eigentums zu wahren. Art. 5 Abs. 3 lit. e FIDA-E verpflichtet den Dateninhaber dazu, diese Schutzvorgaben bei der Bereitstellung von Daten zu beachten. Art. 6 Abs. 4 lit. b FIDA-E legt dieselbe Pflicht dem Datennutzer auf. Damit soll sichergestellt werden, dass sensible unternehmensbezogene Informationen nicht durch den Datenaustausch gefährdet werden.[178] Finanzunternehmen müssen jedoch da-

[177] ErwG 10 FIDA-E.
[178] ErwG 9 FIDA-E.

mit rechnen, dass Geschäftsdaten wie etwa Angaben zu Tarifen oder zur Prämienberechnung, die sie ihren Kunden im Rahmen der Leistungserbringung offenlegen, an Dritte weitergegeben werden.[179]

[179] Denga: Entwurf einer Financial Data Access-Verordnung (FiDA), MMR 2025, 701 (706).

3. Vergleichende Analyse

Ziel dieser vergleichenden Analyse ist es, die wichtigsten Zielsetzungen, Anforderungen und Herausforderungen der drei Verordnungen DORA, AI Act und FIDA-E herauszuarbeiten. Die Gegenüberstellung soll eine strukturierte Orientierung bieten und die Relevanz der jeweiligen Vorgaben für Finanzunternehmen herausstellen. Besonderes Augenmerk liegt auf den Schnittmengen und Unterschieden, um Handlungsfelder und Synergien zu identifizieren.

3.1 Gegenüberstellung der Zielsetzungen, Anforderungen und Herausforderungen von DORA, AI Act und FIDA-E

3.1.1 DORA

Das Ziel der DORA-Verordnung liegt in der Stärkung der digitalen operationalen Resilienz von Finanzunternehmen durch EU-weite Vorgaben für das Management von IT-Risiken und die Widerstandsfähigkeit gegenüber Cyberbedrohungen.

Die Anforderungen, die DORA an Finanzunternehmen stellt, sind zahlreich: Neben der Umsetzung von Vorgaben zum IKT-Risikomanagement, Umgang mit IKT-Vorfällen, Testen der digitalen operationalen Resilienz und zum Drittparteienrisikomanagement inkl. der Pflege eines Informationsregisters sind Finanzunternehmen zur Einrichtung teils neuer

Funktionen und Erweiterung bestehender Funktionen verpflichtet.

Für kleinere Institute gelten weniger umfangreiche Vorgaben. Dies regelt Art. 16 DORA. Zu dessen Konkretisierung hat die BaFin die Aufsichtsmitteilung zur Umsetzung von DORA mit vereinfachtem IKT-Risikomanagementrahmen und IKT-Drittparteienrisikomanagement veröffentlicht[180], die sich an Institute, die nicht unter die Kapitaladäquanzverordnung[181] fallen, sowie an kleine Einrichtungen der betrieblichen Altersvorsorge (EbAV), kleine Wertpapierinstitute und

[180] BaFin Aufsichtsmitteilung Hinweise zur Umsetzung von DORA mit vereinfachtem IKT-Risikomanagementrahmen (Artikel 16 DORA) und IKT-Drittparteienrisikomanagement, Stand August 2025.

[181] Capital Requirements Regulation – CRR, Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und zur Änderung der Verordnung (EU) Nr. 648/2012. Diese Institute wenden laut der BaFin ab Januar 2027 die Vorgaben zum vereinfachten IKT-Risikomanagementrahmen und IKT-Drittparteienrisikomanagement an, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Aufsichtsmitteilung/2025/neu/aufsichtsmitteilung_2025_08_21_hinweise_artikel_16_dora.html;jsessionid=7232FF81AA80285DD46352CFA82BBCCF.internet992 (zuletzt abgerufen am 12.10.2025).

Versicherungsholdings richtet.[182] Die Adressaten dieser Aufsichtsmitteilung müssen beispielsweise keine DOR-Strategie vorweisen.[183]

Die Verordnung gilt seit dem 17. Januar 2025 (Art. 64 DORA).

3.1.2 AI Act

Der AI Act verfolgt das Ziel, einen einheitlichen Rechtsrahmen zur sicheren und vertrauenswürdigen Entwicklung und Nutzung von Künstlicher Intelligenz in der EU zu schaffen. Aufgrund der umfangreichen Regelungen in Hinblick auf Hochrisiko-KI-Systeme wird der AI Act auch als ein „Produktsicherheitsrecht für KI“ mit bestimmten zusätzlichen Regelungen bezeichnet.[184] Es handelt sich bei der Verordnung um keine klassische Finanzmarktregulierung, sondern um eine mit der DSGVO vergleichbaren übergeordneten Regelung des ethischen Einsatzes von KI, die sektorübergreifend gilt.

Der AI Act verpflichtet zur risikobasierten Klassifizierung von KI-Systemen, enthält spezifische Vorgaben für Hochrisiko-KI

---

[182] BaFin Mitteilung vom 21.08.2025, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Aufsichtsmitteilung/2025/neu/aufsichtsmitteilung_2025_08_21_hinweise_artikel_16_dora.html;jsessionid=7232FF81AA80285DD46352CFA82BBCCF.internet992 (zuletzt abgerufen am 12.10.2025).

[183] Ziff. 2.1 BaFin Aufsichtsmitteilung Hinweise zur Umsetzung von DORA mit vereinfachtem IKT-Risikomanagementrahmen (Artikel 16 DORA) und IKT-Drittparteienrisikomanagement, Stand August 2025.

[184] Hafezi Rachti: Zukunftsfähige Regulierung Künstlicher Intelligenz durch die EU?, EuZW 2025, 26.

sowie Transparenzanforderungen und Nachweis- und Überwachungspflichten. Die Adressaten des AI Act begegnen der Herausforderung, KI-Risiken zu identifizieren und bewerten, Compliance-Vorgaben in bestehende Prozesse zu integrieren und Ressourcenbedarf im Zuge paralleler Transformationsprojekte anzupassen. Ein besonders hoher Umsetzungsaufwand besteht, wenn Finanzunternehmen den Betrieb von Hochrisiko-KI-Systemen beabsichtigen.

Die Verordnung wird ab dem 2. August 2026 vollständig gelten (Art. 113 AI Act). Aufgrund der unannehmbaren Risiken, die mit bestimmten Anwendungen von KI verbunden sind, sind die Verbote sowie die allgemeinen Bestimmungen (Kapitel I und II) bereits am 2. Februar 2025 in Kraft getreten (Art. 113 lit. a AI Act). Zwar entfalten diese Verbote ihre volle Wirkung erst mit der Einrichtung der zuständigen Behörden und der Durchsetzung der Verordnung, doch ist ihre frühzeitige Anwendung entscheidend, um Risiken zu begegnen und auch auf andere Verfahren – etwa im Zivilrecht – Einfluss zu nehmen.[185] Anbieter von GPAI, die vor dem 2. August 2025 in Verkehr gebracht wurden, treffen die erforderlichen Maßnahmen für die Erfüllung ihrer Pflichten bis zum 2. August 2027 (Art. 111 Abs. 3 AI Act).

3.1.3 FIDA-E

Das Ziel von FIDA-E liegt in der Förderung eines sicheren und effizienten Austauschs von Finanzdaten innerhalb der

[185] ErwG 179 AI Act.

EU sowie in der Stärkung der Datenportabilität und des Wettbewerbs im Finanzsektor.

FIDA-E wird Dateninhaber zur Bereitstellung von Kundendaten auf Antrag, zur Einrichtung von Schnittstellen und Dashboards sowie zum Beitritt in ein FDSS verpflichten. Finanzinformationsdienstleister werden eine Erlaubnis bei der zuständigen Aufsichtsbehörde beantragen müssen, sofern sie noch nicht über eine solche verfügen. Die Herausforderungen in der Umsetzung der FIDA-Vorgaben werden hauptsächlich in der technischen Umsetzung der Datenaustauschmechanismen, der Optimierung der Datenqualität sowie in der Abstimmung vertraglicher Details der FDSS liegen.

FIDA-E soll 24 Monate nach Inkrafttreten gelten, wobei zwei zentrale Artikel – Art. 9 (Systeme für den Austausch von Finanzdaten) und Art. 13 FIDA-E (Organisation des Datenzugangs) – bereits 18 Monate nach Inkrafttreten Anwendung finden sollen. Damit wird eine gestaffelte Einführung der Regelungen vorgesehen, um insbesondere die technischen und organisatorischen Voraussetzungen für den Datenaustausch frühzeitig zu etablieren.

3.2 Synergien und Konflikte zwischen den Regulierungen

Im Kontext der betrachteten Regulierungen – DORA, FIDA-E und AI Act – lassen sich sowohl Synergien als auch potenzielle Konflikte erkennen.

3.2.1 Kollaboration und Informationsaustausch

Auf den ersten Blick ist allen drei Verordnungen gemein, dass sie jeweils mindestens ein Element zum Informationsaustausch enthalten. Gerade bei FIDA-E zählt der Datenaustausch zum zentralen Zweck und ist für die Adressaten sogar verpflichtend. Bei DORA und dem AI Act spielt der Informationsaustausch eine eher untergeordnete Rolle.

DORA enthält mit Art. 45 eine Regelung, nach der Finanzunternehmen innerhalb vertrauenswürdiger Gemeinschaften Informationen und Erkenntnisse über Cyberbedrohungen untereinander austauschen können. Darüber hinaus haben Finanzunternehmen jährlich den zuständigen Aufsichtsbehörden ihr aktuelles Informationsregister über den Bezug von IKT-Dienstleistungen zu übermitteln, um eine strategische Überwachung von Drittparteienrisiken zu ermöglichen.[186]

Im AI Act sind Informationsaustauschregelungen in Zusammenhang mit der Meldung schwerwiegender Vorfälle betreffend die Pflichtverletzungen von Unionsrechtsvorschriften zum Schutz der Grundrechte (Art. 73 Abs. 7 AI Act), mit der Marktüberwachung (Art. 74 Abs. 2 AI Act) sowie mit der Entwicklung und Bewertung von Hochrisiko-KI-Systemen ent-

[186] ErwG 65 DORA.

halten. Beim Informationsaustausch hinsichtlich der Meldung schwerwiegender Vorfälle und der Marktüberwachung handelt es sich um einen Austausch zwischen Behörden.

Nach ErwG 68 AI Act sollten für die Entwicklung und Bewertung von Hochrisiko-KI-Systemen bestimmte Akteure wie etwa Anbieter, notifizierte Stellen und andere einschlägige Einrichtungen wie Europäische Digitale Innovationszentren, Test- und Versuchseinrichtungen und Forscher auf hochwertige Datensätze – z. B. innerhalb der von der Kommission eingerichteten gemeinsamen europäischen Datenräume – zugreifen und diese nutzen können. Das Recht auf Datenzugang bzw. auf Datennutzung ist u. a. im Data Governance Act[187] und im Data Act[188] geregelt, welche beide parallel zum AI Act anwendbar sind.[189]

Beim Thema Informationsaustausch ist stets das Kartellrecht im Hinterkopf zu behalten. Nach dem Kartellrecht ist der Austausch wettbewerblich sensibler Informationen zwischen

---

[187] Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt).

[188] Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung).

[189] Braun Binder/Egli in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 10 Rn. 7.

Wettbewerbern unzulässig.[190] Zu wettbewerblich sensiblen Informationen zählen in der Regel Daten zu Preisen und Preisbestandteilen, Kunden oder Produktionskosten, -mengen und -kapazitäten, aber potenziell auch Parameter zu Innovationen oder eingesetzten Technologien.[191] Sofern die auszutauschenden Daten ggf. Aufschluss über die Funktionsweise von betroffenen Produkten und Services geben, ist im Einzelfall wettbewerbliches Konfliktpotenzial denkbar.[192] Kartellrechtlichen Bedenken kann jedoch durch Schutzmaßnahmen bei der Datenbereitstellung und -verwendung begegnet werden, z. B. durch Ansätze wie die Einrichtung von Clean-Teams oder ein Ring-Fencing von Daten, die in der kartellrechtlichen Praxis etabliert und bewährt sind.[193]

3.2.2 Vorfallsmanagement

DORA und der AI Act enthalten eigene Vorschriften zu Vorfallsmeldungen, während FIDA-E in Bezug auf die Handhabung IKT-bezogener Vorfälle auf DORA verweist.[194]

---

[190] Schulz: Datenzugang nach dem Data Act – Überblick und Schnittstellen zum Kartellrecht, NZKart 2024, 426 (432); Müller in: BeckOK Kartell, 17. Ed. 1.7.2025, AEUV Art. 101 Rn. 245.

[191] Schulz: Datenzugang nach dem Data Act – Überblick und Schnittstellen zum Kartellrecht, NZKart 2024, 426 (432).

[192] Schulz: Datenzugang nach dem Data Act – Überblick und Schnittstellen zum Kartellrecht, NZKart 2024, 426 (432).

[193] Schulz: Datenzugang nach dem Data Act – Überblick und Schnittstellen zum Kartellrecht, NZKart 2024, 426 (432), mwN.

[194] ErwG 32 FIDA-E.

DORA regelt die Meldepflicht für schwerwiegende IKT-Vorfälle in Art. 19. Dieser Artikel verpflichtet Finanzunternehmen, Vorfälle mit erheblichen Auswirkungen zu melden.

Art. 5 Abs. 1 RTS zur Festlegung des Inhalts und der Fristen für die Erstmeldung enthält abgestufte Fristen zur Meldung schwerwiegender IKT-Vorfälle. Die Erstmeldung hat spätestens vier Stunden nach der Klassifizierung des Vorfalls als schwerwiegend und spätestens 24 Stunden nach dessen Kenntniserlangung zu erfolgen. In Deutschland agiert die BaFin als zentraler Hub für diese Meldungen.[195] Sie leitet sämtliche Meldungen anschließend gemäß Art. 19 Abs. 6 DORA an alle weiteren zuständigen Behörden weiter.

Art. 73 AI Act regelt die Meldepflichten für Anbieter von Hochrisiko-KI-Systemen bei schwerwiegenden Vorfällen. Anbieter müssen solche Vorfälle den Marktüberwachungsbehörden des Mitgliedstaats melden, in dem der Vorfall stattgefunden hat. Die Meldung muss unmittelbar nach Feststellung eines kausalen Zusammenhangs zwischen dem KI-System und dem Vorfall oder der naheliegenden Wahrscheinlichkeit eines solchen Zusammenhangs erfolgen, spätestens jedoch 15 Tage nach Kenntniserlangung durch den Anbieter oder Betreiber. Bei weitverbreiteten Verstößen oder

[195] BaFin, Die BaFin informiert über Abschnitt II, Kapitel III DORA, geändert am 20.01.2025, https://www.bafin.de/DE/Aufsicht/DORA/Meldewesen_IKT_Vorfaelle/Meldung_schwerwiegender_IKT_bezogener_Vorfaelle_und_erheblicher_Cyberbedrohungen/Meldung_schwerwiegender_IKT_bezogener_Vorfaelle_und_erheblicher_Cyberbedrohungen_node.html (zuletzt abgerufen am 04.11.2025).

besonders schwerwiegenden Vorfällen ist die Meldung unverzüglich, spätestens innerhalb von zwei Tagen, zu erstatten. Im Todesfall muss die Meldung ebenfalls unverzüglich, spätestens innerhalb von zehn Tagen nach Kenntnis erfolgen. Da die BaFin voraussichtlich die zuständige Marktüberwachungsbehörde für in direktem Zusammenhang mit einer regulierten Finanztätigkeit stehende Hochrisiko-KI-Systeme wird, ist damit zu rechnen, dass die Meldungen nach Art. 73 AI Act von Finanzunternehmen gegenüber der BaFin zu erfolgen haben.[196]

Sofern die BaFin über die Meldungen schwerwiegender IKT-Vorfälle nach DORA hinaus auch Adressatin für Meldungen schwerwiegender KI-Vorfälle nach dem AI Act wird, bleibt abzuwarten, ob es ggf. konsolidierte Meldewege für Vorfälle geben wird, die sowohl als KI- als auch als IKT-Vorfälle zu klassifizieren sind.

Jedenfalls werden Finanzunternehmen bei der Umsetzung der Vorgaben für sich einen Weg finden müssen, interne Vorfallsbearbeitungen – ggf. über zentrale interne Meldewege – effizient und fristgerecht zu steuern, denn neben den bisherigen Meldungen von Datenschutzvorfällen kommen nun noch die Meldungen von IKT- und potenziell auch von KI-Vorfällen dazu.

[196] § 2 Abs. 3 Referentenentwurf zum KI-Marktüberwachungsgesetz (Bearbeitungsstand: 11.09.2025).

3.2.3 Datenschutz, Daten- und Vertragsmanagement

DORA enthält mit Art. 12 Anforderungen an Backup- und Wiederherstellungsverfahren für Finanzunternehmen im Rahmen des IKT-Risikomanagements. Danach haben Finanzunternehmen Richtlinien und Verfahren für die Datensicherung zu entwickeln und dokumentieren, wobei der Umfang und die Häufigkeit der Sicherung sich nach der Kritikalität und dem Vertraulichkeitsgrad der Daten richten. Ebenso sind Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung von Daten und Systemen zu definieren.

FIDA-E zielt auf einen sicheren und effizienten Austausch von Finanzdaten innerhalb der EU ab. Da Daten hierbei im Zentrum stehen, ist es essenziell für Finanzunternehmen, für eine strukturierte Datenlage und eine hohe Datenqualität als adäquate Basis zu sorgen. Ein solides Datenmanagementsystem ist hierfür unerlässlich. Denn nach FIDA-E haben Finanzunternehmen u. a. sicherzustellen, dass die im Dashboard des Kunden enthaltenen Informationen klar, richtig und für ihn leicht verständlich und Zugriffsberechtigungen in seiner Nutzerschnittstelle leicht auffindbar sind (Art. 8 Abs. 3 FIDA-E).

Nach dem AI Act gelten sieben unverbindliche ethische Grundsätze für KI, die dazu beitragen sollten, dass KI vertrauenswürdig und ethisch vertretbar ist.[197] Zu diesen sieben

[197] ErwG 27 AI Act.

Grundsätzen gehört u. a. der Grundsatz der Privatsphäre und Daten-Governance. Der Grundsatz bedeutet, dass KI-Systeme im Einklang mit den geltenden Vorschriften zum Schutz der Privatsphäre und zum Datenschutz entwickelt und verwendet werden und dabei Daten verarbeiten, die hohen Qualitäts- und Integritätsstandards genügen.[198] Hierzu gehören hochwertige Trainings-, Validierungs- und Testdatensätze, die geeignete Daten-Governance- und Datenverwaltungsverfahren erfordern.[199] Für Hochrisiko-KI-Systeme sind außerdem Datenschutz-Folgenabschätzungen (Art. 9 AI Act) und ggf. Grundrechte-Folgenabschätzungen (Art. 27 AI Act) verpflichtend.

Eine DSGVO-konforme Verarbeitung personenbezogener Daten setzt alle drei Verordnungen voraus.

DORA schreibt mit Art. 30 Mindestvertragsinhalte für Vereinbarungen mit IKT-Drittdienstleistern vor. Eine große Anzahl von Altverträgen genügt(e) den Anforderungen dieser Vorschrift nicht und war/ist daher entsprechend anzupassen. Allein die Identifikation aller relevanten Verträge stellt einen größeren Aufwand dar[200], der jedoch mit einem gut strukturierten Vertragsmanagement leichter zu bewältigen ist.

Ein solides Vertragsmanagement ist sicherlich auch für die Umsetzung der FIDA-Vorgaben hilfreich, da u. a. Inhalte aus

198 ErwG 27 AI Act.

199 ErwG 67 AI Act.

200 Lipke: Vertragsanpassungen nach DORA, BKR 2025, 253 (258).

Kundenverträgen für den Finanzdatenaustausch maßgeblich sind.

3.2.4 Massive Umsetzungsaufwände

Die vorstehenden Ausführungen zeigen, dass Finanzunternehmen unzählige neue Regulierungsvorgaben umzusetzen haben. Teilweise gehen diese einher mit einer Umstrukturierung bzw. Reorganisation der Aufbauorganisationen. Für jede einzelne Verordnung kann es sinnvoll sein, jeweils ein Implementierungsprojekt – wenn möglich mit externer Unterstützung – aufzusetzen. Dies bindet allerdings Ressourcen und ist außerdem mit hohen Kosten verbunden.

Hinzu kommt noch die zeitliche Komponente: DORA gilt seit dem 17. Januar 2025. Dennoch stecken viele Finanzunternehmen noch in Umsetzungsprojekten. Blickt man zurück auf die Umsetzung der DSGVO in Unternehmen, so zeigt sich, dass nur ein kleiner Teil in der Lage war, die Umsetzung innerhalb der zweijährigen Übergangsfrist zu finalisieren.[201] Der AI Act tritt vollständig am 2. August 2026 in Kraft, mit ersten Verboten bereits seit Februar 2025. FIDA-E sieht eine gestaffelte Einführung vor. Zentrale Artikel gelten bereits 18 Monate nach Inkrafttreten. Finanzunternehmen müssen also

[201] Bitkom, 3 von 4 Unternehmen verfehlen die Frist der Datenschutz-Grundverordnung, https://www.bitkom.org/Presse/Presseinformation/3-von-4-Unternehmen-verfehlen-die-Frist-der-Datenschutz-Grundverordnung.html#:~:text=Berlin%2C%2017.%20Mai%202018%20%2D%20Die%20zweij%C3%A4hrige,Unternehmen%20in%20Deutschland%20ist%20bis%20zum%2025. (zuletzt abgerufen am 05.11.2025).

größtenteils parallel unterschiedliche Umsetzungszeitpläne einhalten, was die Ressourcenplanung und Projektsteuerung erschwert.

4. Synthese und Schlussfolgerung

4.1 Zusammenführung der Erkenntnisse

DORA und der AI Act sind Verordnungen, die Finanzunternehmen dazu veranlassen, Risiken in Zusammenhang mit der Digitalisierung souverän zu begegnen. Sie zielen darauf ab, den Finanzmarkt zukunftssicher zu machen und stabil zu halten. FIDA-E hingegen soll für mehr Innovation im Finanzmarkt sorgen, indem ein sicherer und effizienter Austausch von Finanzdaten in der EU ermöglicht wird. Alle drei Verordnungen enthalten Elemente des Informationsaustauschs, wobei FIDA-E den Datenaustausch ins Zentrum stellt. DORA und der AI Act enthalten jeweils eigene Vorschriften zu Vorfallsmeldungen, die es in interne Prozesse zu integrieren gilt, während FIDA-E in Bezug auf das Vorfallsmanagement auf DORA verweist. Datenschutz und Datenmanagement sind zentrale Querschnittsthemen, die in allen drei Verordnungen adressiert werden.

Die sich zeitlich überschneidenden Einführungen, unterschiedliche Adressatenlogik und technisch-organisatorische Anforderungen erzeugen wiederum ein hohes Maß an Komplexität. Kartellrechtliche Bedenken können beim Datenaustausch entstehen, insbesondere wenn wettbewerblich sensible Informationen betroffen sind. Die parallele Umsetzung

der Verordnungen erfordert außerdem eine sorgfältige Ressourcenplanung und klare Verantwortlichkeiten.[202]

Die massive regulatorische Belastung kann dazu führen, dass die von der EU an sich gewünschte Innovation im Digitalsektor gehemmt wird.[203] Nicht jedes Finanzunternehmen verfügt über eine große Compliance-Abteilung, die die Vorgaben in kürzester Zeit verarbeiten kann. Selbst wenn es Erleichterungen für Kleinstunternehmen wie beispielsweise nach Art. 16 DORA gibt, so sind die Aufwände dennoch hoch. Dies gilt vor allem für Unternehmen, die noch nicht über gut funktionierende Dokumenten- und Vertragsmanagementsysteme verfügen.

4.2 Auswertung der Hypothesen

Hypothese 1: DORA erhöht die digitale Resilienz von Finanzunternehmen, indem es strenge Anforderungen an das Risikomanagement und die Meldung von Vorfällen stellt.

Auswertung: Diese Hypothese lässt sich bestätigen. Durch die Einführung strenger Vorgaben für das Risikomanagement sowie für die Meldung und Behandlung von IKT-Vorfällen werden Finanzunternehmen gezwungen, ihre internen Prozesse und technischen Schutzmaßnahmen umfassend

---

202 Für diese Zusammenfassung wurde das KI-Tool Copilot genutzt. Das Ergebnis wurde kritisch geprüft und entsprechend angepasst.
203 Laude/Daum in: Bernzen/Heinze/Steinrötter, DSRI Herbstakademie 2025, Plattformen und Clouds Eine Überdosis Digitalregulierung – Risiken und Nebenwirkungen für die Europäische Wirtschaft Zusammenfassung.

zu verbessern. Dies führt nicht nur zu einer höheren Widerstandsfähigkeit gegenüber Cyberangriffen und IKT-Ausfällen, sondern erhöht auch die Transparenz und Nachvollziehbarkeit im Umgang mit digitalen Risiken. Allerdings geht diese Stärkung der Resilienz mit einem erheblichen organisatorischen und finanziellen Mehraufwand einher, insbesondere für kleinere Institute ohne ausgereifte Compliance- und IT-Strukturen. Trotz potenzieller Synergien mit bereits bestehenden Regelungen bleibt die parallele Umsetzung verschiedener Vorgaben eine große Herausforderung für viele Finanzunternehmen.

Hypothese 2: FIDA-E fördert die Innovation und den Wettbewerb im Finanzsektor durch den sicheren und offenen Zugang zu Kundendaten, während gleichzeitig die Kontrolle und der Schutz der Daten durch die Verbraucher gewährleistet wird.

*Auswertung***:** Die Förderung von Innovation und Wettbewerb durch FIDA-E ist grundsätzlich plausibel, da der sichere und offene Zugang zu Kundendaten neue Geschäftsmodelle und die Verbesserung von Finanzprodukten ermöglicht. Allerdings hängt die Innovationskraft maßgeblich davon ab, wie effektiv die technische und rechtliche Umsetzung gelingt und inwieweit Kunden ihre Datenfreigaben aktiv steuern.

Hypothese 3: Der AI Act stellt sicher, dass KI-Systeme in der Finanzbranche sicher, transparent und ethisch genutzt werden, was das Vertrauen der Verbraucher in diese Technologien stärkt.

Auswertung: Der AI Act legt einen Rahmen für den ethischen Einsatz von KI fest. Die geforderten Transparenz- und Sicherheitsmaßnahmen können das Vertrauen der Verbraucher stärken. Gleichzeitig stellt die Einhaltung der Vorgaben Finanzunternehmen vor erhebliche Herausforderungen, insbesondere was ihre Rolle in Bezug auf Hochrisiko-KI-Systeme und damit einhergehende Verpflichtungen betrifft.

Hypothese 4: Einige in den Verordnungen enthaltene Regelungen bestanden schon nach der bisherigen Rechtslage bzw. in vergleichbaren Gesetzen und basieren auf allgemeinen Prinzipien, die sich in den Verordnungen überschneiden. Durch entsprechende Synergien können bei der Umsetzung der Vorgaben mehrere Ziele auf einmal erreicht werden.

Auswertung: Die Überschneidungen mit bestehenden Regelungen und allgemeinen Prinzipien führen eher weniger zu Synergien, da die neuen Regelungen wesentlich umfangreicher sind als die bisherigen. Auch aufgrund der unterschiedlichen Zielrichtungen der Regulierungen sind die Synergien zwischen den Verordnungen überschaubar. Ein gemeinsamer Nenner für alle drei Regulierungen ist die hohe Bedeutung einer guten Datenqualität sowie eines soliden Daten- und Vertragsmanagements als Grundlage für die Umsetzung der Vorgaben.

Hypothese 5: Im Zuge der Umsetzung der Vorgaben werden in den Unternehmen neue organisatorische Bereiche und Stellen geschaffen werden müssen. Auch in dieser Hinsicht sind Synergien möglich, sofern keine Interessenkonflikte bestehen.

Auswertung: Die Schaffung neuer organisatorischer Funktionen und Stellen ist angesichts der Vielzahl an Anforderungen wahrscheinlich. Synergien lassen sich dort realisieren, wo Aufgaben und Verantwortlichkeiten klar abgegrenzt und Interessenkonflikte vermieden werden.

Hypothese 6: Die Umsetzung der Vorgaben bindet Ressourcen und ist mit hohen Kosten verbunden. Die aktuelle angeschlagene Wirtschaftslage erschwert die Umsetzung und führt zu Frustrationen bei allen Adressaten der Regulierungen.

Auswertung: Die Umsetzung der Regulierungen bindet erhebliche Ressourcen und verursacht hohe Kosten. Besonders kleinere und mittlere Unternehmen stehen vor großen Herausforderungen. Die angespannte Wirtschaftslage verstärkt diesen Effekt und kann zu Frustration und Verzögerungen führen.

Insgesamt zeigt die Auswertung, dass die Regulierungen zwar wichtige Ziele verfolgen, ihre parallele und sich teilweise überschneidende Umsetzung jedoch einen hohen organisatorischen und finanziellen Aufwand für Finanzunternehmen bedeutet. Die tatsächlichen Effekte auf Innova-

tion, Wettbewerb und Verbraucherschutz werden maßgeblich davon abhängen, wie effizient und koordiniert die Umsetzung innerhalb der Unternehmen gelingt.[204]

4.3 Implikationen und Empfehlungen für die Praxis

4.3.1 Neue Aufgaben für bestehende Funktionen

DORA, der AI Act und FIDA-E bereiten in ihrer Gesamtheit allen voran der Geschäftsleitung und den Compliance-Abteilungen viel Arbeit.

4.3.1.1 Geschäftsleitung / Vorstand

Für die BaFin war bereits vor einigen Jahren absehbar, dass mit der sich rasant entwickelnden Digitalisierung ein hoher Grad an IT-Kompetenz in den Vorständen von Finanzunternehmen vonnöten sein wird. So hat die BaFin schon 2017 die Aufnahme von IT-Spezialistinnen und -Spezialisten in die Geschäftsleitung beaufsichtigter Unternehmen vereinfacht, mit dem Ziel die IT-Kompetenz in den Geschäftsleitungen der Unternehmen weiter zu fördern.[205]

Die Geschäftsleitung verantwortet in Bezug auf DORA und den AI Act unternehmensweite Strategien und Richtlinien für

[204] Für diese Zusammenfassung wurde das KI-Tool Copilot genutzt. Das Ergebnis wurde kritisch geprüft und entsprechend angepasst.

[205] BaFin, Big Data und künstliche Intelligenz: Prinzipien für den Einsatz von Algorithmen in Entscheidungsprozessen, Juni 2021, S. 6.

den Einsatz von KI und Informations- und Kommunikationstechnologien. Darüber hinaus verantwortet sie auch die Definition, Genehmigung und Überwachung des IKT-Risikomanagements sowie die Einführung einer KI Policy.

FIDA-E enthält zwar keine expliziten Aufgaben für die Geschäftsleitung, dennoch sollte sie über diese Verordnung ein Grundwissen besitzen, um entsprechende strategische Maßnahmen mit Blick auf die Implementierung der regulatorischen Vorgaben in die Wege zu leiten und sie zu steuern.

4.3.1.2 Compliance, Recht und Interne Revision

Die Compliance-Abteilungen stehen vor der Herausforderung, die Anforderungen aus DORA, dem AI Act und FIDA-E in bestehende Prozesse zu integrieren oder neue Prozesse zu etablieren, interne Richtlinien zu entwickeln, die Einhaltung zu überwachen und Neuerungen wie beispielsweise Aufsichtsmitteilungen im Blick zu behalten. Der Internen Revision wird die Herausforderung zuteil, die Einhaltung der entsprechenden Maßgaben zu kontrollieren.

Die Rechtsabteilungen sind häufig involviert in Themen rund um das Vertragsmanagement. Nach DORA gilt es, Verträge mit IKT-Drittdienstleistern anzupassen bzw. auf regulatorische Konformität zu prüfen. Im Rahmen von FIDA-E ist eine Einbindung der Rechtsabteilungen in Zusammenhang mit Datenzugriffsvereinbarungen sinnvoll, während sie mit Blick

auf den AI Act vermutlich hauptsächlich Haftungsfragen prüfen, insbesondere beim Einsatz von Hochrisiko-KI-Systemen.[206]

4.3.1.3 IT, Informationssicherheit und Risikomanagement

Die Abteilungen IT, Informationssicherheit und Risikomanagement erfahren durch DORA die stärksten Auswirkungen. Bei ihnen liegt die größte Verantwortung auf dem IKT-Risikomanagement. Dies umfasst nicht nur den Aufbau und die Pflege eines umfassenden IKT-Risikomanagementsystems, inklusive BCM und Krisenmanagement, sondern auch die Durchführung regelmäßiger Tests der digitalen Resilienz.

Nach dem AI Act ist beim Einsatz von Hochrisiko-KI-Systemen gemäß Art. 9 Abs. 1 ein Risikomanagementsystem einzuführen. Sofern also in Finanzunternehmen der Einsatz von Hochrisiko-KI-Systemen geplant wird, wäre eine Integration dieses Risikomanagementsystems in das bereits bestehende IKT-Risikomanagement nach DORA sinnvoll.[207]

In Bezug auf FIDA-E liegt der Fokus dieser Abteilungen auf der Errichtung von Schnittstellen zum Datenaustausch sowie

---

[206] Woesch/Vogt: Die KI-Verordnung – Die digitale Zukunft im Finanzsektor, BKR 2024, 689 (695).

[207] Knoblich/Krimphove: Die neue KI-VO im Regelungsdickicht des Aufsichtsrechts, BKR 2024, 843 (845).

von Dashboards zur Überwachung und Verwaltung von Zugriffsberechtigungen.

4.3.2 Etablierung neuer Funktionen

Nach DORA haben Finanzunternehmen eine IKT-Risikokontrollfunktion, eine Funktion zur Überwachung von IKT-Drittdienstleistungsvereinbarungen und eine Krisenmanagementfunktion einzurichten, sofern sie keine Kleinstunternehmen sind.

Der AI Act schreibt in Art. 4 eine KI-Kompetenz vor, unabhängig vom Risikograd der im Unternehmen eingesetzten KI-Systeme. Damit ist nicht zwingend eine neue Funktion oder die Benennung einer verantwortlichen Person im Unternehmen gemeint.[208] Die Vorschrift wird als „soft-law"-ähnliche Leitnorm interpretiert, die erst durch nachgelagerte Leitlinien, Branchenstandards und interne Policies konkretisiert wird.[209] Um Verantwortlichkeiten und Kompetenzen zu bündeln, wird die Einrichtung einer entsprechenden Funktion empfohlen.[210]

Im FIDA-E findet sich keine Verpflichtung zur Errichtung einer neuen Funktion. Um die aus der Verordnung resultierenden Vorgaben effizient im Unternehmen zu koordinieren,

---

[208] Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 4 Rn. 16.

[209] Bunes in: Bernzen/Heinze/Steinrötter, DSRI Herbstakademie 2025, KI-Regulierung Schlau macht sicher – KI-Kompetenz als Compliance-Faktor 1, 370 f.

[210] Wendt in: Wendt/Wendt Das neue KI-Recht, 2. Aufl. 2025, § 4 Rn. 17.

empfiehlt es sich jedoch zumindest eine Taskforce einzurichten, die aus Stakeholdern relevanter Abteilungen wie z. B. aus der Compliance-, Rechts- und IT-/Informationssicherheitsabteilung besteht.

4.4 Schlussfolgerung

Abschließend lässt sich festhalten, dass die aktuellen regulatorischen Entwicklungen rund um DORA, den AI Act und FIDA-E Finanzunternehmen vor neue Herausforderungen stellen, die über rein technische Anpassungen hinausgehen. Vor dem Hintergrund, dass in der heutigen Zeit nicht nur viele Gefahren online lauern, sondern auch offline bestehen, wie z. B. Umweltkatastrophen, Pandemien oder Kriege, ist es wichtig und auch geboten, präventiv tätig zu werden. Auch KI kann Risiken bergen, vor allem wenn sie auf unethische Weise genutzt wird. Die Erweiterung der Aufgaben von Compliance-, Rechts-, IT-, Informationssicherheits- und Risikomanagementabteilungen sowie die Einrichtung neuer Funktionen oder Taskforces sind teilweise von den Verordnungen gefordert bzw. zumindest geboten, um den Anforderungen adäquat zu begegnen. Durch eine ganzheitliche und interdisziplinäre Kollaboration lässt sich sowohl die digitale operationale Resilienz als auch die Einhaltung der rechtlichen Vorgaben nachhaltig sicherstellen. Dies erfordert nicht nur die Anpassung bestehender Prozesse, sondern auch kontinuierliche Schulungen und Sensibilisierungen im Unternehmen. So wird die Basis gebildet, um etwaigen Krisen wirksam zu begegnen und wirtschaftliche Fortschritte zu schaffen.

Der regulatorische Fokus in Hinblick auf FIDA-E liegt auf der Optimierung der Datenverfügbarkeit und -nutzung, wobei vor allem Schnittstellen zum Datenaustausch eine wichtige Rolle spielen. Finanzunternehmen sind gefordert, – wenn nötig – ihre Datenqualität zu verbessern und entsprechende technische und organisatorische Maßnahmen zu etablieren, um die Transparenz und eine wirksame Kontrolle über Datenflüsse sicherzustellen. Die Schaffung von Taskforces kann dazu beitragen, die Anforderungen von FIDA-E effizient und abteilungsübergreifend umzusetzen.[211]

[211] Für diese Zusammenfassung wurde das KI-Tool Copilot genutzt. Das Ergebnis wurde kritisch geprüft und entsprechend angepasst.

Literatur

Ahmad, Khalid/Kirschbaum, Michael (2025) in: Riediger Auslagerungen/Dienstleister-Steuerung, FCH AG: Heidelberg.

Ascheberg, Celine (2025): Künstliche Intelligenz in der Internen Revision, BC 2025, 416.

BaFin (2025): Aufsichtsmitteilung Hinweise zur Umsetzung von DORA mit vereinfachtem IKT-Risikomanagementrahmen (Artikel 16 DORA) und IKT-Drittparteienrisikomanagement, Stand August 2025.

BaFin (2021): Big Data und künstliche Intelligenz: Prinzipien für den Einsatz von Algorithmen in Entscheidungsprozessen, Juni 2021.

BaFin (2025): Entwurf eines Rundschreibens 2025 zu Pflichten von Verwahrstelle und Kapitalverwaltungsgesellschaft bei in Kryptowerte investierenden Investmentvermögen.

BaFin (2024): Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024.

BaFin (2024): Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024.

BaFin (2024): Präsentation „DORA für IKT-Drittdienstleister“ vom 29. Februar 2024.

Bernau, Timo/Lutterbach, Maike (2023): Digital Operational Resilience Act (DORA), BKR 2023, 506.

Bitter, Philip (2024): Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 62. EL Juni 2024, Teil 15.4, Verlag C.H. Beck oHG: München.

Bomhard, David/Siglmüller, Jonas (2024): Hornung/Schallbruch, IT-Sicherheitsrecht, § 29 IT-Sicherheitsrecht im Finanzsektor, 2. Auflage 2024, Nomos Verlagsgesellschaft: Baden-Baden.

Braun Binder, Nadja/Egli, Catherine (2024): Martini/Wendehorst, KI-VO, 1. Aufl. 2024, Verlag C.H. Beck oHG: München.

Bunes, Florian (2025): Bernzen/Heinze/Steinrötter, DSRI Herbstakademie 2025, KI-Regulierung Schlau macht sicher – KI-Kompetenz als Compliance-Faktor, Verlag C.H. Beck GmbH & Co. KG: München.

BSI-Standard 200-4 (2023), Bonn.

Bürkle, Jürgen (2024): Moosmayer/Lösler Corporate Compliance, 4. Aufl. 2024, Verlag C.H. Beck oHG: München.

Clausmeier, Dirk: Die neue Verordnung des europäischen Parlamentes und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA), WM 2022 Heft 39, 1861.

Denga, Michael (2025): Entwurf einer Financial Data Access-Verordnung (FiDA), MMR 2025, 701.

Denga, Michael (2024): KI in der Anlageberatung, WM 2024 Heft 49, 2275.

Digitaleurope (2025), Building a future-proof open finance ecosystem vom 12.02.2025.

Dreisigacker-Sartor, Charlotte/Ritter-Döring, Verena (2025): Mit FIDA von Open Banking zu Open Finance, RdZ 2024, 5.

Eisenberger, Iris (2024): Martini/Wendehorst, KI-VO, 1. Aufl. 2024, KI-VO Art. 17, Verlag C.H. Beck oHG: München.

EU-Kommission (2020), Eine europäische Datenstrategie, COM (2020) 66 final.

EU-Kommission (2021), Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen v. 9.3.2021, COM (2021) 118 final, Digitaler Kompass 2030: der europäische Weg in die digitale Dekade.

Gebauer, Stefan (2020): Hopt/Binder/Böcking, Handbuch Corporate Governance von Banken und Versicherungen, 2. Aufl. 2020, § 10. Rn. 36, Verlag Franz Vahlen GmbH: München.

Gerdemann, Simon (2025): Schefzig/Kilian, BeckOK KI-Recht, 3. Ed. 1.8.2025, KI-VO, Art. 8, Verlag C.H. Beck oHG: München.

Glos, Alexander/Hildner, Alicia (2025): Schäfer/Omlor/Mimberg, ZAG, 2. Aufl. 2025, ZAG § 53, Verlag C.H. Beck oHG: München.

Hafezi Rachti, Schirin (2025): Zukunftsfähige Regulierung Künstlicher Intelligenz durch die EU?, EuZW 2025, 26.

Hartmann, Sarah (2024): Martini/Wendehorst, KI-VO, 1. Aufl. 2024, Verlag C.H. Beck oHG: München.

Henke, Hannes (2025): Schefzig/Kilian, BeckOK KI-Recht, 3. Ed. 1.8.2025, KI-VO Art. 17, Verlag C.H. Beck oHG: München.

Hilgendorf, Eric; Härtlein, Johannes (2025): Hilgendorf/Härtlein, HK-KI-VO, 1. Aufl. 2025, KI-VO Art. 73, Nomos Verlagsgesellschaft: Baden-Baden.

Kaetzler, Joachim (2025): Zentes/Glaab, 4. Aufl. 2025, GwG § 4, dfv Mediengruppe: Frankfurt am Main.

Knoblich, René/Krimphove, Dieter (2024): Die neue KI-VO im Regelungsdickicht des Aufsichtsrechts, BKR 2024, 843.

Krimphove, Dieter (2018): Die „neue“ MaRisk (BA) 9/201, BKR 2018, 1.

Langenbucher, Katja (2023): Diskriminierung bei der Vergabe von Verbraucherkrediten?, BKR 2023, 205.

Laude, Lennart/Daum, Andreas (2025): Bernzen/Heinze/Steinrötter, DSRI Herbstakademie 2025, Plattformen und Clouds Eine Überdosis Digitalregulierung – Risiken und Nebenwirkungen für die Europäische Wirtschaft Zusammenfassung, Verlag C.H. Beck GmbH & Co. KG: München.

Leupold, Michael (2025): Krimphove/Lüke, MaRisk, 2. Aufl. 2025, R 10/2021 MaRisk und Erläuterungen AT4.4.3, Verlag C.H. Beck GmbH & Co. KG: München.

Lipke, Martina (2025): Vertragsanpassungen nach DORA, BKR 2025, 253.

Martini, Mario (2024): Martini/Wendehorst, KI-VO, 1. Aufl. 2024, KI-VO Art. 50 Rn. 1, Verlag C.H. Beck oHG: München.

Möslein, Florian/Omlor, Sebastian (2025): Digitalisierung der Finanzmärkte, ZRP 2025, 44.

Müller, Christian (2025): Bacher/Hempel/Wagner-von Papp, BeckOK Kartell, 17. Ed. 1.7.2025, AEUV Art. 101, Verlag C.H. Beck: München.

Niedernhuber, Tanja (2025): Wabnitz/Janovsky/Schmitt, Handbuch Wirtschafts- und Steuerstrafrecht, 6. Aufl. 2025, 16. Kap. Rn. 21, Verlag C.H. Beck oHG: München.

Rüsing, Christian (2025): Verantwortungsvolle Kreditvergabe in der novellierten Verbraucherkreditrichtlinie, ZBB 2025, 24.

Sassenberg, Thomas (2025): AI Governance Framework – Regelungsgegenstand der AI Policy, RDi 2025, 346.

Schalkowski, Henrik/Ortiz, André (2020): Roboterisierung im finanzwirtschaftlichen Risikomanagement, BC 2020, 130.

Schmitz, Ralf (2020): IDW Kreditinstitute-WPH, 1. Aufl. 2020, Kap. O, IDW Verlag GmbH: Düsseldorf.

Schulz, Max (2024): Datenzugang nach dem Data Act – Überblick und Schnittstellen zum Kartellrecht, NZKart 2024, 426.

Schwenke, Thomas (2024): Einführung KI-Verordnung: Grundlagen, Begriffe und Pflichtenkatalog, DSB 2024, 205.

Siglmüller, Jonas (2023): Cyber Resilience Act und Digital Operational Resilience Act – Lässt sich IT-Sicherheit rechtlich erzwingen?, ZfPC 2023, 221.

Wendehorst, Christiane (2024): Martini/Wendehorst, KI-VO, 1. Aufl. 2024, KI-VO Art. 3, Verlag C.H. Beck oHG: München.

Wendt, Janine/Wendt, Domenik (2025): Wendt/Wendt, Das neue KI-Recht, 2. Aufl. 2025, Nomos Verlagsgesellschaft: Baden-Baden.

Woesch, Philippe/Vogt, Melanie (2024): Die KI-Verordnung – Die digitale Zukunft im Finanzsektor, BKR 2024, 689.

Internetquellenverzeichnis

BaFin: Mitteilung vom 07.10.2024, https://www.bafin.de/SharedDocs/FAQs/DE/DORA/IKT_Risikomanagement/03.html (zuletzt abgerufen am 20.06.2025).

BaFin: zum Open Banking, https://www.bafin.de/EN/Aufsicht/FinTech/Geschaeftsmodelle/OpenBanking_OpenFinance/OpenBanking_OpenFinance_node_en.html (zuletzt abgerufen am 14.09.2025).

BaFin: zum Thema Open Finance, https://www.bafin.de/DE/Aufsicht/FinTech/Geschaeftsmodelle/OpenBanking_OpenFinance/OpenBanking_OpenFinance_node.html (zuletzt abgerufen am 15.09.2025).

BaFin: zum vereinfachten IKT-Risikomanagementrahmen und IKT-Drittparteienrisikomanagement, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Aufsichtsmitteilung/2025/neu/aufsichtsmitteilung_2025_08_21_hinweise_artikel_16_dora.html;jsessionid=7232FF81AA80285DD46352CFA82BBCCF.internet992 (zuletzt abgerufen am 12.10.2025).

BaFin: „Risiken im Fokus der BaFin 2025“, https://www.bafin.de/ref/19792518 (zuletzt abgerufen am 29.05.2025).

BaFin: Informationsregister und Anzeigepflichten, Stand 01.07.2025, https://www.bafin.de/DE/Aufsicht/DORA/Informationsregister_und_Anzeigepflichten/Informationsregister_und_Anzeigepflichten_node.html (zuletzt abgerufen am 20.07.2025).

BaFin: Informationsregister und Anzeigepflichten, geändert am 18.07.2025, https://www.bafin.de/DE/Aufsicht/DORA/Informationsregister_und_Anzeigepflichten/Informationsregister_und_Anzeigepflichten_node.html (zuletzt abgerufen am 05.09.2025).

BaFin: Die BaFin informiert über Abschnitt II, Kapitel III DORA, geändert am 20.01.2025, https://www.bafin.de/DE/Aufsicht/DORA/Meldewesen_IKT_Vorfaelle/Meldung_schwerwiegender_IKT_bezogener_Vorfaelle_und_erheblicher_Cyberbedrohungen/Meldung_schwerwiegender_IKT_bezogener_Vorfaelle_und_erheblicher_Cyberbedrohungen_node.html (zuletzt abgerufen am 04.11.2025).

Bitkom: 3 von 4 Unternehmen verfehlen die Frist der Datenschutz-Grundverordnung, https://www.bitkom.org/Presse/Presseinformation/3-von-4-Unternehmen-verfehlen-die-Frist-der-Datenschutz-

Grundverordnung.html#:~:text=Berlin%2C%2017.%20Mai%202018%20%2D%20Die%20zweij%C3%A4hrige,Unternehmen%20in%20Deutschland%20ist%20bis

BNetzA: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/13_Notifizierung/start.html (zuletzt abgerufen am 08.09.2025).

Deutsche Bundesbank: BAIT / DORA – Aufsichtliche Anforderungen an die IT und die digitale operationale Resilienz, https://www.bundesbank.de/de/aufgaben/bankenaufsicht/einzelaspekte/risikomanagement/bait-dora-598580 (zuletzt abgerufen am 19.06.2025).

Deutsche Bundesbank: FAQ zum digitalen Euro, https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/digitaler-euro/faq-digitaler-euro (zuletzt abgerufen am 01.06.2025).

Deutsche Bundesbank: https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/digitaler-euro/stand-der-dinge/stand-der-dinge-903502 (zuletzt abgerufen am 01.06.2025).

EU-Kommission: zu FIDA, https://finance.ec.europa.eu/digital-finance/framework-financial-data-access_en (zuletzt abgerufen am 14.09.2025).

EU-Kommission: zum AI Act, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (zuletzt abgerufen am 07.09.2025).

EU-Kommission; Financial data access and payments package, Juni 2023, https://finance.ec.europa.eu/publications/financial-data-access-and-payments-package_en (zuletzt abgerufen am 29.05.2025)

Europäischer Rat: zum Digitalen Finanzwesen, https://www.consilium.europa.eu/de/policies/digital-finance/#strategy (zuletzt abgerufen am 18.07.2025).

German Open Finance Charta 2025, https://openfinance-charta.de/ (zuletzt abgerufen am 28.09.2025).