RICHTLINIE (EU) 2022/2556 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

zur Änderung der Richtlinien 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 und (EU) 2016/2341 hinsichtlich der digitalen operationalen Resilienz im Finanzsektor

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 53 Absatz 1 und Artikel 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme der Europäischen Zentralbank ([1]),

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([2]),

gemäß dem ordentlichen Gesetzgebungsverfahren ([3]),

in Erwägung nachstehender Gründe:

(1) Die Union muss den digitalen Risiken, die sich aus dem verstärkten Einsatz von Informations- und Kommunikationstechnologien (IKT) bei der Bereitstellung und Nutzung von Finanzdienstleistungen ergeben und sämtliche Finanzunternehmen betreffen, angemessen und umfassend begegnen und damit ihren Beitrag zur Realisierung des Potenzials des digitalen Finanzwesens leisten, indem Innovationen vorangetrieben werden und der Wettbewerb in einem sicheren digitalen Umfeld gefördert wird.

(2) Finanzunternehmen sind in ihrem Geschäftsalltag sehr stark auf die Nutzung digitaler Technologien angewiesen. Es ist daher von größter Bedeutung, die operationale Resilienz ihres digitalen Betriebs gegenüber IKT-Risiken sicherzustellen. Dies ist angesichts der Zunahme von bahnbrechenden Technologien am Markt — insbesondere Technologien, die die digitale Darstellung von Werten oder Rechten, die mittels Distributed-Ledger- oder ähnlicher Technologie (Kryptowerte) gespeichert werden, ermöglichen — sowie von Dienstleistungen im Zusammenhang mit Kryptowerten dringender geworden.

([1]) ABl. C 343 vom 26.8.2021, S. 1.
([2]) ABl. C 155 vom 30.4.2021, S. 38.
([3]) Standpunkt des Europäischen Parlaments vom 10. November 2022 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 28. November 2022.

(3) Auf Unionsebene enthalten derzeit die Richtlinien 2009/65/EG ([4]), 2009/138/EG ([5]), 2011/61/EU ([6]), 2013/36/EU ([7]), 2014/59/EU ([8]), 2014/65/EU ([9]), (EU) 2015/2366 ([10]) und (EU) 2016/2341 ([11]) des Europäischen Parlaments und des Rates die Bestimmungen zum Management von IKT-Risiken im Finanzsektor.

Diese Bestimmungen sind uneinheitlich und stellenweise lückenhaft. Das IKT-Risiko wird in einigen Fällen nur implizit als Teil des operationellen Risikos behandelt, während es in anderen Fällen überhaupt nicht behandelt wird. Diese Probleme werden durch die Annahme der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates ([12]) behoben. Um die Kohärenz mit der genannten Verordnung zu gewährleisten, sollten die genannten Richtlinien daher geändert werden. Durch die vorliegende Richtlinie werden eine Reihe von Änderungen vorgenommen, die erforderlich sind, um für Rechtsklarheit und Kohärenz bei der durch die gemäß den genannten Richtlinien zugelassenen und beaufsichtigten Finanzunternehmen erfolgende Anwendung von unterschiedlichen Anforderungen an die digitale operationale Resilienz, die für die Ausführung ihrer unternehmerischer Tätigkeiten und für die Erbringung von Dienstleistungen erforderlich sind, zu sorgen, wodurch das reibungslose Funktionieren des Binnenmarkts gewährleistet wird. Es ist erforderlich, dafür zu sorgen, dass diese Anforderungen in Bezug auf die Marktentwicklungen angemessen sind, und zugleich die Verhältnismäßigkeit — insbesondere in Bezug auf die Größe von Finanzunternehmen und die besonderen für sie geltenden Regelungen — mit dem Ziel zu fördern, die Befolgungskosten zu senken.

(4) Im Bereich der Bankdienstleistungen enthält die Richtlinie 2013/36/EU derzeit nur allgemeine interne Governance-Vorschriften und Bestimmungen für operationelle Risiken, einschließlich Anforderungen an Notfallpläne und Geschäftsfortführungspläne, die implizit als Grundlage zum Angehen von IKT-Risiken dienen. Um IKT-Risiken explizit und klar anzugehen, sollten jedoch die Anforderungen an Notfallpläne und Geschäftsfortführungspläne im Einklang mit den Anforderungen der Verordnung (EU) 2022/2554 geändert werden, damit auch Geschäftsfortführungspläne und Reaktions- und Wiederherstellungspläne betreffend IKT-Risiken aufgenommen werden. Ferner werden IKT-Risiken im aufsichtlichen Überprüfungs- und Bewertungsprozess (Supervisory Review and Evaluation Process, SREP), der von den zuständigen Behörden durchgeführt wird, nur als Teil des operationellen Risikos implizit berücksichtigt, und die betreffenden Bewertungskriterien sind derzeit in den von der Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde, EBA) herausgegebenen Leitlinien für die IKT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses (Supervisory Review and Evaluation process — SREP) festgelegt, die durch die Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates ([13]) eingerichtet wurden. Um Rechtsklarheit zu schaffen und sicherzustellen, dass die Bankenaufsichts-

([4]) Richtlinie 2009/65/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 zur Koordinierung der Rechts- und Verwaltungsvorschriften betreffend bestimmte Organismen für gemeinsame Anlagen in Wertpapieren (OGAW) (ABl. L 302 vom 17.11.2009, S. 32).

([5]) Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II) (ABl. L 335 vom 17.12.2009, S. 1).

([6]) Richtlinie 2011/61/EU des Europäischen Parlaments und des Rates vom 8. Juni 2011 über die Verwalter alternativer Investmentfonds und zur Änderung der Richtlinien 2003/41/EG und 2009/65/EG und der Verordnungen (EG) Nr. 1060/2009 und (EU) Nr. 1095/2010 (ABl. L 174 vom 1.7.2011, S. 1).

([7]) Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338).

([8]) Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 zur Festlegung eines Rahmens für die Sanierung und Abwicklung von Kreditinstituten und Wertpapierfirmen und zur Änderung der Richtlinie 82/891/EWG des Rates, der Richtlinien 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU und 2013/36/EU sowie der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates (ABl. L 173 vom 12.6.2014, S. 190).

([9]) Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. L 173 vom 12.6.2014, S. 349).

([10]) Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35).

([11]) Richtlinie (EU) 2016/2341 des Europäischen Parlaments und des Rates vom 14. Dezember 2016 über die Tätigkeiten und die Beaufsichtigung von Einrichtungen der betrieblichen Altersversorgung (EbAV) (ABl. L 354 vom 23.12.2016, S. 37).

([12]) 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 (siehe Seite 1 dieses Amtsblatts).

([13]) Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 12).

behörden die IKT-Risiken gemäß dem neuen Rahmen für digitale operationale Resilienz wirksam ermitteln und deren Management durch Finanzunternehmen überwachen, sollte der Anwendungsbereich des SREP auch dahingehend geändert werden, dass die in der Verordnung (EU) 2022/2554 niedergelegten Vorgaben explizit genannt und insbesondere die Risiken abgedeckt werden, die durch Berichte über schwerwiegende IKT-bezogene Vorfälle und durch die Ergebnisse der von Finanzunternehmen im Einklang mit jener Verordnung durchgeführten Tests der digitalen operationalen Resilienz aufgedeckt werden.

(5) Die digitale operationale Resilienz ist unverzichtbar, um die kritischen Funktionen und Kerngeschäftsbereiche eines Finanzunternehmens im Falle seiner Abwicklung aufrechtzuerhalten und dadurch Störungen der Realwirtschaft und des Finanzsystems zu vermeiden. Größere betriebliche Vorfälle können die Fähigkeit eines Finanzunternehmens, den Betrieb aufrechtzuerhalten, beeinträchtigen und die Abwicklungsziele gefährden. Bestimmte vertragliche Vereinbarungen betreffend die Nutzung von IKT-Dienstleistungen sind unverzichtbar, um die Aufrechterhaltung des Betriebs sicherzustellen und im Falle der Abwicklung die erforderlichen Daten bereitzustellen. Um die Richtlinie 2014/59/EU mit den Zielen des Unionsrahmens für die operationale Resilienz in Einklang zu bringen, sollte sie entsprechend geändert werden, damit sichergestellt ist, dass Informationen über die operationale Resilienz im Zusammenhang mit der Abwicklungsplanung und der Bewertung der Abwicklungsfähigkeit von Finanzunternehmen berücksichtigt werden.

(6) Nach der Richtlinie 2014/65/EU gelten strengere IKT-Risikovorschriften für Wertpapierfirmen und Handelsplätze, die algorithmischen Handel betreiben. Weniger detaillierte Vorschriften gelten für Datenbereitstellungsdienstleistungen und Transaktionsregister. Außerdem enthält die Richtlinie 2014/65/EU nur wenige Verweise auf Kontroll- und Sicherungsvorkehrungen für Informationsverarbeitungssysteme sowie auf die Nutzung geeigneter Systeme, Ressourcen und Verfahren, um die Kontinuität und Ordnungsmäßigkeit von Dienstleistungen zu gewährleisten. Des Weiteren sollte die genannte Richtlinie in Bezug auf Kontinuität und Ordnungsmäßigkeit bei der Erbringung von Wertpapierdienstleistungen sowie bei der Ausübung von Anlagetätigkeiten, der operationalen Resilienz, der Kapazität von Handelssystemen sowie der Wirksamkeit der Vorkehrungen zur Fortführung der Geschäftstätigkeit und des Risikomanagements mit der Verordnung (EU) 2022/2554 in Einklang gebracht werden.

(7) Die Richtlinie (EU) 2015/2366 enthält spezifische Vorschriften für IKT-Sicherheitskontrollen und Risikominderungsmaßnahmen für die Zwecke der Erteilung einer Zulassung für die Erbringung von Zahlungsdiensten. Diese Zulassungsvorschriften sollten geändert werden, um sie an die Verordnung (EU) 2022/2554 anzugleichen. Darüber hinaus sollten zur Verringerung des Verwaltungsaufwands und zur Vermeidung von Komplexität und doppelten Meldepflichten die Vorschriften für die Meldung von Sicherheitsvorfällen gemäß der Richtlinie (EU) 2015/2366 keine Anwendung auf Zahlungsdienstleister mehr finden, die jener Richtlinie und der Verordnung (EU) 2022/2554 unterliegen, um ihnen den Vorteil eines einheitlichen und vollständig harmonisierten Mechanismus für die Meldung von Vorfällen in Bezug auf alle betrieblichen Vorfälle oder zahlungsbezogene Sicherheitsvorfälle — unabhängig davon, ob ein IKT-Bezug besteht — zu ermöglichen.

(8) Die Richtlinien 2009/138/EG und (EU) 2016/2341 decken IKT-Risiken teilweise in ihren allgemeinen Bestimmungen über Governance und Risikomanagement ab, wobei bestimmte Anforderungen durch delegierte Rechtsakte mit oder ohne spezifische Verweise auf IKT-Risiken festgelegt werden können. Ebenso gelten für Verwalter alternativer Investmentfonds, die der Richtlinie 2011/61/EU unterliegen, und Verwaltungsgesellschaften, die der Richtlinie 2009/65/EG unterliegen, nur sehr allgemeine Vorschriften. Diese Richtlinien sollten daher an die Anforderungen für die Verwaltung von IKT-Systemen und -Tools der Verordnung (EU) 2022/2554 angeglichen werden.

(9) In vielen Fällen wurden weitere IKT-Risikoanforderungen bereits in delegierten Rechtsakten und Durchführungsrechtsakten festgelegt, die basierend auf von der zuständigen Europäischen Aufsichtsbehörde ausgearbeiteten Entwürfen technischer Regulierungs- und Durchführungsstandards angenommen wurden. Da die Bestimmungen der Verordnung (EU) 2022/2554 künftig den Rechtsrahmen für IKT-Risiken im Finanzsektor bilden, sollten bestimmte Ermächtigungen zum Erlass von delegierten Rechtsakten und Durchführungsrechtsakten in den Richtlinien 2009/65/EG, 2009/138/EG, 2011/61/EU und 2014/65/EU geändert werden, um die Bestimmungen zu IKT-Risiken vom Geltungsbereich dieser Ermächtigungen auszuschließen.

(10) Um eine kohärente Anwendung des neuen Rahmens für digitale operationale Resilienz im Finanzsektor zu gewährleisten, sollten die Mitgliedstaaten die nationalen Rechtsvorschriften zur Umsetzung der vorliegenden Richtlinie ab dem Geltungsbeginn der Verordnung (EU) 2022/2554 anwenden.

(11) Die Richtlinien 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 und (EU) 2016/2341 wurden auf der Grundlage von Artikel 53 Absatz 1 oder Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) oder beiden angenommen. Der Gegenstand und die Ziele der in der vorliegenden Richtlinie enthaltenen Änderungen sind miteinander verflochten und wurden daher in einem einzigen Rechtsakt zusammengefasst. Diese Richtlinie sollte daher auf der Grundlage von Artikel 53 Absatz 1 und Artikel 114 AEUV angenommen werden.

(12) Da die Ziele dieser Richtlinie von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, da sie die Harmonisierung von bereits in Richtlinien enthaltenen Anforderungen beinhalten, sondern vielmehr wegen des Umfangs und der Wirkungen der Maßnahme auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Richtlinie nicht über das für die Verwirklichung dieser Ziele erforderliche Maß hinaus.

(13) Gemäß der Gemeinsamen Politischen Erklärung der Mitgliedstaaten und der Kommission zu erläuternden Dokumenten ([14]) vom 28. September 2011 haben sich die Mitgliedstaaten verpflichtet, in begründeten Fällen zusätzlich zur Mitteilung ihrer Umsetzungsmaßnahmen ein oder mehrere Dokumente zu übermitteln, in denen der Zusammenhang zwischen den Bestandteilen einer Richtlinie und den entsprechenden Teilen nationaler Umsetzungsinstrumente erläutert wird. Für diese Richtlinie hält der Gesetzgeber die Übermittlung derartiger Dokumente für gerechtfertigt —

HABEN FOLGENDE RICHTLINIE ERLASSEN:

Artikel 1

Änderungen der Richtlinie 2009/65/EG

Artikel 12 der Richtlinie 2009/65/EG wird wie folgt geändert:

1. Absatz 1 Unterabsatz 2 Buchstabe a erhält folgende Fassung:

„a) über eine ordnungsgemäße Verwaltung und Buchhaltung, Kontroll- und Sicherheitsvorkehrungen für die elektronische Datenverarbeitung, einschließlich in Bezug auf Netzwerk- und Informationssysteme, die im Einklang mit der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*) eingerichtet und verwaltet werden, sowie angemessene interne Kontrollverfahren, zu denen insbesondere Regeln für persönliche Geschäfte ihrer Angestellten und für das Halten oder Verwalten von Anlagen in Finanzinstrumenten zum Zwecke der Anlage auf eigene Rechnung gehören, verfügen muss, durch die zumindest gewährleistet wird, dass jedes den OGAW betreffende Geschäft nach Herkunft, Vertragsparteien, Art, Abschlusszeitpunkt und -ort rekonstruiert werden kann und dass die Vermögenswerte der von der Verwaltungsgesellschaft verwalteten OGAW gemäß den Vertragsbedingungen oder Satzungen dieser Fonds sowie gemäß den geltenden rechtlichen Bestimmungen angelegt wird;

(*) 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 (ABl. L 333 vom 27.12.2022, S. 1).“.

2. Absatz 3 erhält folgende Fassung:

„(3) Unbeschadet des Artikels 116 erlässt die Kommission mittels delegierter Rechtsakte nach Artikel 112a Maßnahmen zur Festlegung:

a) der Verfahren und Regelungen gemäß Absatz 1 Unterabsatz 2 Buchstabe a mit Ausnahme der Verfahren und Regelungen bezüglich Netzwerk- und Informationssysteme;

b) der Strukturen und organisatorischen Anforderungen zur Verringerung von Interessenkonflikten gemäß Absatz 1 Unterabsatz 2 Buchstabe b.“

([14]) ABl. C 369 vom 17.12.2011, S. 14.

Artikel 2

Änderungen der Richtlinie 2009/138/EG

Die Richtlinie 2009/138/EG wird wie folgt geändert:

1. Artikel 41 Absatz 4 erhält folgende Fassung:

„(4) Versicherungs- und Rückversicherungsunternehmen treffen angemessene Vorkehrungen, einschließlich der Entwicklung von Notfallplänen, um die Kontinuität und Ordnungsmäßigkeit ihrer Tätigkeiten zu gewährleisten. Zu diesem Zweck greift das Unternehmen auf geeignete und verhältnismäßige Systeme, Ressourcen und Verfahren zurück, richtet insbesondere Netzwerk- und Informationssysteme ein und verwaltet diese gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*).

(*) 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 (ABl. L 333 vom 27.12.2022, S. 1).“

2. In Artikel 50 Absatz 1 erhalten die Buchstaben a und b folgende Fassung:

„a) die Bestandteile der in den Artikeln 41, 44, insbesondere die unter Artikel 44 Absatz 2 aufgeführten Bereiche, 46 und 47 genannten Systeme mit Ausnahme derjenigen, die das Risikomanagement im Bereich der Informations- und Kommunikationstechnologie betreffen;

b) die in den Artikeln 44, 46, 47 und 48 genannten Funktionen mit Ausnahme der Funktionen im Zusammenhang mit dem Risikomanagement im Bereich der Informations- und Kommunikationstechnologie.“.

Artikel 3

Änderung der Richtlinie 2011/61/EU

Artikel 18 der Richtlinie 2011/61/EU erhält folgende Fassung:

„*Artikel 18*

Allgemeine Grundsätze

(1) Die Mitgliedstaaten legen fest, dass die AIFM für die ordnungsgemäße Verwaltung der AIF jederzeit angemessene und geeignete personelle und technische Ressourcen einsetzen.

Insbesondere schreiben die zuständigen Behörden des Herkunftsmitgliedstaats des AIFM — auch unter Berücksichtigung der Art der von dem AIFM verwalteten AIF — vor, dass der betreffende AIFM über eine ordnungsgemäße Verwaltung und Buchhaltung, Kontroll- und Sicherheitsvorkehrungen für die elektronische Datenverarbeitung, einschließlich in Bezug auf Netzwerk- und Informationssysteme, die im Einklang mit der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*) eingerichtet und verwaltet werden, sowie angemessene interne Kontrollverfahren, zu denen insbesondere Regeln für persönliche Geschäfte ihrer Angestellten und für das Halten oder Verwalten von Anlagen zum Zwecke der Anlage auf eigene Rechnung gehören, verfügt, durch die zumindest gewährleistet wird, dass jedes die AIF betreffende Geschäft nach Herkunft, Vertragsparteien, Art, Abschlusszeitpunkt und -ort rekonstruiert werden kann und dass die Vermögenswerte der vom AIFM verwalteten AIF gemäß den Vertragsbedingungen oder Satzungen der AIF sowie gemäß den geltenden rechtlichen Bestimmungen angelegt werden.

(2) Die Kommission erlässt gemäß Artikel 56 und nach Maßgabe der Bedingungen der Artikel 57 und 58 delegierte Rechtsakte, mit denen die Verfahren und Regelungen gemäß Absatz 1 mit Ausnahme der Verfahren und Regelungen bezüglich Netzwerk- und Informationssysteme festgelegt werden.

(*) 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(ABl. L 333 vom 27.12.2022, S. 1).“

Artikel 4

Änderungen der Richtlinie 2013/36/EU

Die Richtlinie 2013/36/EU wird wie folgt geändert:

1. Artikel 65 Absatz 3 Buchstabe a Ziffer vi erhält folgende Fassung:

„vi) Dritte, auf die die Unternehmen im Sinne der Ziffern i bis iv Funktionen oder Tätigkeiten ausgelagert haben, einschließlich IKT-Drittdienstleister gemäß Kapitel V der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*),

(*) 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 (ABl. L 333 vom 27.12.2022, S. 1).“.

2. Artikel 74 Absatz 1 Unterabsatz 1 erhält folgende Fassung:

„Die Institute verfügen über solide Unternehmensführungsregelungen, wozu eine klare Organisationsstruktur mit genau festgelegten, transparenten und kohärenten Zuständigkeiten, wirksame Verfahren zur Ermittlung, Steuerung, Überwachung und Meldung der tatsächlichen und potenziellen künftigen Risiken, angemessene interne Kontrollmechanismen, einschließlich solider Verwaltungs- und Rechnungslegungsverfahren, Netzwerk- und Informationssysteme, die gemäß der Verordnung (EU) 2022/2554 eingerichtet und verwaltet werden, sowie eine Vergütungspolitik und -praxis, die mit einem soliden und wirksamen Risikomanagement vereinbar und diesem förderlich sind, zählen.“

3. Artikel 85 Absatz 2 erhält folgende Fassung:

„(2) Die zuständigen Behörden stellen sicher, dass die Institute über angemessene Notfall- und Geschäftsfortführungsleitlinien und -pläne verfügen, einschließlich IKT-Geschäftsfortführungsleitlinien und -plänen sowie IKT-Reaktions- und Wiederherstellungsplänen in Bezug auf die von ihnen genutzte Technologie zur Übermittlung von Informationen, und dass diese Pläne gemäß Artikel 11 der Verordnung (EU) 2022/2554 eingerichtet, verwaltet und getestet werden, damit Institute bei einer schwerwiegenden Betriebsunterbrechung geschäftlich tätig bleiben und Verluste in Folge einer solchen Unterbrechung begrenzen können.“

4. In Artikel 97 Absatz 1 wird folgender Buchstabe angefügt:

„d) die Risiken, die bei Tests der digitalen operationalen Resilienz gemäß Kapitel IV der Verordnung (EU) 2022/2554 aufgedeckt werden.“.

Artikel 5

Änderungen der Richtlinie 2014/59/EU

Die Richtlinie 2014/59/EU wird wie folgt geändert:

1. Artikel 10 wird wie folgt geändert:

a) Absatz 7 Buchstabe c erhält folgende Fassung:

„c) Ausführungen dazu, wie kritische Funktionen und Kerngeschäftsbereiche im erforderlichen Umfang rechtlich und wirtschaftlich von anderen Funktionen getrennt werden könnten, um ihre Fortführung und die digitale operationale Resilienz nach einem Ausfall des Instituts sicherzustellen;“;

b) Absatz 7 Buchstabe q erhält folgende Fassung:

„q) eine Beschreibung der wesentlichen Prozesse und Systeme zur Fortführung des Geschäftsbetriebs des Instituts, einschließlich der Netzwerk- und Informationssysteme im Sinne der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*);

(*) 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 (ABl. L 333 vom 27.12.2022, S. 1).“;

c) In Absatz 9 wird folgender Unterabsatz angefügt:

„Gemäß Artikel 10 der Verordnung (EU) Nr. 1093/2010 überprüft und — soweit erforderlich — aktualisiert die EBA die technischen Regulierungsstandards, um unter anderem den Bestimmungen des Kapitels II der Verordnung (EU) 2022/2554 Rechnung zu tragen."

2. Der Anhang wird wie folgt geändert:

a) Abschnitt A Nummer 16 erhält folgende Fassung:

„16. eine Aufstellung der Regelungen und Maßnahmen, die zur Fortführung des Geschäftsbetriebs des Instituts, einschließlich der gemäß der Verordnung (EU) 2022/2554 eingerichteten und verwalteten Netzwerk- und Informationssysteme, erforderlich sind;";

b) Abschnitt B wird wie folgt geändert:

i) Nummer 14 erhält folgende Fassung:

„14. Angaben zu den Eigentümern der in Nummer 13 genannten Systeme, zu entsprechenden Dienstgütevereinbarungen und zu Software, Systemen oder Lizenzen, einschließlich Zuordnung zu den jeweiligen juristischen Personen, kritischen Operationen und Kerngeschäftsbereichen des Instituts, sowie Angaben zu kritischen IKT-Drittdienstleistern im Sinne des Artikels 3 Nummer 23 der Verordnung (EU) 2022/2554;";

ii) Folgende Nummer wird eingefügt:

„14a. Ergebnisse der von Instituten im Einklang mit der Verordnung (EU) 2022/2554 durchgeführten Tests der digitalen operationalen Resilienz;";

c) Abschnitt C wird wie folgt geändert:

i) Nummer 4 erhält folgende Fassung:

„4. inwieweit die vom Institut geschlossenen Dienstleistungsvereinbarungen, einschließlich vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen, solide und im Fall einer Abwicklung des Instituts in vollem Umfang durchsetzbar sind;";

ii) Folgende Nummer wird eingefügt:

„4a. die digitale operationale Resilienz derjenigen Netzwerk- und Informationssysteme, die die kritischen Funktionen und Kerngeschäftsbereiche des Instituts unterstützen, wobei Berichte über schwerwiegende IKT-bezogene Vorfälle und die Ergebnisse der entsprechend der Verordnung 2022/2554 durchgeführten Tests der digitalen operationalen Resilienz zu berücksichtigen sind;".

Artikel 6

Änderungen der Richtlinie 2014/65/EU

Die Richtlinie 2014/65/EU wird wie folgt geändert:

1. Artikel 16 wird wie folgt geändert:

a) Absatz 4 erhält folgende Fassung:

„(4) Eine Wertpapierfirma trifft angemessene Vorkehrungen, um die Kontinuität und Regelmäßigkeit der Wertpapierdienstleistungen und Anlagetätigkeiten zu gewährleisten. Zu diesem Zweck greift sie auf geeignete und verhältnismäßige Systeme, einschließlich gemäß Artikel 7 der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*) eingerichteter und verwalteter Systeme der Informations- und Kommunikationstechnologie (IKT), sowie auf geeignete und verhältnismäßige Ressourcen und Verfahren zurück.

(*) 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 (ABl. L 333 vom 27.12.2022, S. 1).";

b) In Absatz 5 erhalten die Unterabsätze 2 und 3 folgende Fassung:

„Eine Wertpapierfirma muss über eine ordnungsgemäße Verwaltung und Buchhaltung, interne Kontrollmechanismen sowie wirksame Verfahren zur Risikobewertung verfügen.

Unbeschadet der Möglichkeit der zuständigen Behörden, Zugang zu Kommunikation im Einklang mit dieser Richtlinie und mit Verordnung (EU) Nr. 600/2014 zu verlangen, muss eine Wertpapierfirma über solide Sicherheitsmechanismen gemäß den Anforderungen der Verordnung (EU) 2022/2554 verfügen, durch die die Sicherheit und Authentifizierung der Informationsübermittlungswege sichergestellt werden, das Risiko der Datenverfälschung und des unberechtigten Zugriffs minimiert und ein Durchsickern von Informationen verhindert wird, so dass die Vertraulichkeit der Daten jederzeit gewährleistet ist."

2. Artikel 17 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Eine Wertpapierfirma, die algorithmischen Handel betreibt, verfügt über wirksame Systeme und Risikokontrollen, die für das von ihr betriebene Geschäft geeignet sind, um sicherzustellen, dass ihre Handelssysteme entsprechend den Anforderungen in Kapitel II der Verordnung (EU) 2022/2554 belastbar sind und über ausreichende Kapazitäten verfügen, angemessenen Handelsschwellen und Handelsobergrenzen unterliegen sowie die Übermittlung von fehlerhaften Aufträgen oder eine Funktionsweise der Systeme vermieden wird, durch die Störungen auf dem Markt verursacht werden könnten bzw. ein Beitrag zu diesen geleistet werden könnte.

Eine solche Wertpapierfirma verfügt außerdem über wirksame Systeme und Risikokontrollen, um sicherzustellen, dass die Handelssysteme nicht für einen Zweck verwendet werden können, der gegen die Verordnung (EU) Nr. 596/2014 oder die Vorschriften des Handelsplatzes verstößt, mit dem sie verbunden ist.

Die Wertpapierfirma verfügt über wirksame Vorkehrungen zur Fortführung der Geschäftstätigkeiten, einschließlich gemäß Artikel 11 der Verordnung (EU) 2022/2554 aufgestellter IKT-Geschäftsfortführungsleitlinie und -plänen sowie IKT-Reaktions- und Wiederherstellungsplänen, um mit jeglichen Störungen in ihren Handelssystemen umzugehen, und stellt sicher, dass ihre Systeme vollständig getestet sind und ordnungsgemäß überwacht werden, damit die in diesem Absatz festgelegten allgemeinen Anforderungen und die in den Kapiteln II und IV der Verordnung (EU) 2022/2554 festgelegten spezifischen Anforderungen erfüllt werden."

b) Absatz 7 Buchstabe a erhält folgende Fassung:

„a) die Einzelheiten der in den Absätzen 1 bis 6 festgelegten konkreten organisatorischen und nicht mit dem IKT-Risikomanagement zusammenhängenden Anforderungen, die Wertpapierfirmen vorzuschreiben sind, die verschiedene Wertpapierdienstleistungen, Anlagetätigkeiten, Nebendienstleistungen oder entsprechende Kombinationen erbringen bzw. ausüben; in den Präzisierungen zu den organisatorischen Anforderungen gemäß Absatz 5 werden besondere Anforderungen für den direkten Marktzugang und für den geförderten Zugang in einer Weise festgelegt, dass sichergestellt ist, dass die beim geförderten Zugang durchgeführten Kontrollen denjenigen, die beim direkten Marktzugang durchgeführt werden, zumindest gleichwertig sind;".

3. Artikel 47 Absatz 1 wird wie folgt geändert:

a) Buchstabe b erhält folgende Fassung:

„b) um angemessen für die Steuerung seiner Risiken, einschließlich der IKT-Risiken gemäß Kapitel II der Verordnung (EU) 2022/2554, ausgestattet zu sein, angemessene Vorkehrungen und Systeme zur Ermittlung von für seinen Betrieb wesentlichen Risiken einrichtet und wirksame Maßnahmen zur Begrenzung dieser Risiken trifft;";

b) Buchstabe c wird gestrichen.

4. Artikel 48 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Die Mitgliedstaaten schreiben vor, dass ein geregelter Markt seine operationale Resilienz zentsprechend den in Kapitel II der Verordnung (EU) 2022/2554 festgelegten Anforderungen herstellt und erhält, um sicherzustellen, dass seine Handelssysteme belastbar sind und über ausreichende Kapazitäten für Spitzenvolumina an Aufträgen und Mitteilungen verfügen, in der Lage sind, unter extremen Stressbedingungen auf den Märkten einen ordnungsgemäßen Handel zu gewährleisten, vollständig geprüft sind, um zu gewährleisten, dass diese Bedingungen erfüllt sind, und wirksamen Vorkehrungen zur Fortführung der Geschäftstätigkeiten unterliegen, die IKT-Geschäftsfortführungsleitlinie und -pläne sowie IKT- Reaktions- und Wiederherstellungspläne gemäß Artikel 11 der Verordnung (EU) 2022/2554 einschließen, um im Fall von Störungen in seinen Handelssystemen die Kontinuität seines Geschäftsbetriebs zu gewährleisten."

b) Absatz 6 erhält folgende Fassung:

„(6) Die Mitgliedstaaten setzen voraus, dass ein geregelter Markt über wirksame Systeme, Verfahren und Vorkehrungen verfügt, einschließlich der Anforderung, dass Mitglieder oder Teilnehmer gemäß den in den Kapiteln II und IV der Verordnung (EU) 2022/2554 festgelegten Anforderungen angemessene Tests von Algorithmen durchführen und ein Umfeld schaffen, um diese Tests zu vereinfachen, um sicherzustellen, dass algorithmische Handelssysteme keine marktstörenden Handelsbedingungen auf dem Markt schaffen oder zu solchen beitragen, und um etwaige marktstörende Handelsbedingungen, die sich aus algorithmischen Handelssystemen ergeben, zu kontrollieren, einschließlich Systemen zur Begrenzung des Verhältnisses nicht ausgeführter Handelsaufträge zu Geschäften, die von einem Mitglied oder Teilnehmer in das System eingegeben werden können, mit dem Ziel, das Auftragsaufkommen zu verlangsamen, wenn das Risiko besteht, dass seine Systemkapazität erreicht wird, und die kleinstmögliche Tick-Größe zu begrenzen und durchzusetzen, die auf dem Markt ausgeführt werden kann."

c) Absatz 12 wird wie folgt geändert:

i) Buchstabe a erhält folgende Fassung:

„a) um die Anforderungen festzulegen, die sicherstellen, dass die Handelssysteme eines geregelten Markts belastbar sind und über ausreichende Kapazität verfügen; davon ausgenommen sind die Anforderungen in Bezug auf die digitale operationale Resilienz;";

ii) Buchstabe g erhält folgende Fassung:

„g) um dafür zu sorgen, dass angemessene Tests durchgeführt werden, um sicherzustellen, dass die algorithmischen Handelssysteme, einschließlich hochfrequenter algorithmischer Handelssysteme, keine marktstörenden Handelsbedingungen auf dem Markt schaffen können; davon ausgenommen sind Tests der digitalen operationalen Resilienz.".

Artikel 7

Änderungen der Richtlinie (EU) 2015/2366

Die Richtlinie (EU) 2015/2366 wird wie folgt geändert:

1. Artikel 3 Buchstabe j erhält folgende Fassung:

„j) Dienste, die von technischen Dienstleistern erbracht werden, die zwar zur Erbringung der Zahlungsdienste beitragen, jedoch zu keiner Zeit in den Besitz der zu transferierenden Geldbeträge gelangen, wie die Verarbeitung und Speicherung von Daten, vertrauensbildende Maßnahmen und Dienste zum Schutz der Privatsphäre, Nachrichten- und Instanzenauthentisierung, Bereitstellung von Informations- und Kommunikationstechnologie (IKT) und Kommunikationsnetzen sowie Bereitstellung und Wartung der für Zahlungsdienste genutzten Endgeräte und Einrichtungen mit Ausnahme von Zahlungsauslösediensten und Kontoinformationsdiensten;".

2. Artikel 5 Absatz 1 erhält folgende Fassung:

a) Unterabsatz 1 wird wie folgt geändert:

i) Buchstabe e erhält folgende Fassung:

„e) eine Beschreibung der Unternehmenssteuerung und der internen Kontrollmechanismen des Antragstellers einschließlich der Verwaltungs-, Risikomanagement- und Rechnungslegungsverfahren sowie Vereinbarungen über die Nutzung von IKT-Diensten gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*), aus der hervorgeht, dass diese Unternehmenssteuerung und interne Kontrollmechanismen verhältnismäßig, angemessen, zuverlässig und ausreichend sind;

(*) 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 (ABl. L 333 vom 27.12.2022, S. 1).";

ii) Buchstabe f erhält folgende Fassung:

„f) eine Beschreibung der vorhandenen Verfahren für Überwachung, Handhabung und Folgemaßnahmen bei Sicherheitsvorfällen und sicherheitsbezogenen Kundenbeschwerden, einschließlich eines Mechanismus für die Meldung von Vorfällen, der die Meldepflichten des Zahlungsinstituts nach Kapitel III der Verordnung (EU) 2022/2554 berücksichtigt;";

iii) Buchstabe h erhält folgende Fassung:

„h) eine Beschreibung der Vorkehrungen zur Fortführung der Geschäftstätigkeiten, einschließlich klarer Angaben der kritischen Vorgänge, wirksamer IKT-Geschäftsfortführungsleitlinie und -plänen, IKT-Reaktions- und Wiederherstellungsplänen sowie eines Verfahrens für regelmäßige Tests der Angemessenheit und Wirksamkeit dieser Pläne gemäß der Verordnung (EU) 2022/2554;";

b) Unterabsatz 3 erhält folgende Fassung:

„Bei den in Unterabsatz 1 Buchstabe j genannten Sicherheitskontroll- und Risikominderungsmaßnahmen ist anzugeben, auf welche Weise dadurch ein hohes Maß an digitaler operationaler Resilienz entsprechend Kapitel II der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates, insbesondere bezüglich technischer Sicherheit und Datenschutz gewährleistet wird; das gilt auch für Software und IKT-Systeme, die der Antragsteller oder die Unternehmen, an die er den Betrieb oder Teile des Betriebs dieser auslagert, verwenden. Zu diesen Maßnahmen gehören auch die Sicherheitsmaßnahmen gemäß Artikel 95 Absatz 1. Bei diesen Maßnahmen ist den in Artikel 95 Absatz 3 genannten Leitlinien für Sicherheitsmaßnahmen der EBA Rechnung zu tragen, sobald diese vorliegen."

3. Artikel 19 Absatz 6 Unterabsatz 2 erhält folgende Fassung:

„Die Auslagerung wichtiger betrieblicher Aufgaben, einschließlich IKT-Systemen, darf nicht auf eine Weise erfolgen, dass die Qualität der internen Kontrolle des Zahlungsinstituts und die Möglichkeit der zuständigen Behörde, zu überprüfen und zurückzuverfolgen, ob das Zahlungsinstitut sämtlichen Anforderungen dieser Richtlinie genügt, wesentlich beeinträchtigt werden."

4. Dem Artikel 95 Absatz 1 wird folgender Unterabsatz angefügt:

„Unterabsatz 1 gilt unbeschadet der Anwendung von Kapitel II der Verordnung (EU) 2022/2554 auf

a) Zahlungsdienstleister im Sinne des Artikels 1 Absatz 1 Buchstaben a, b und d,

b) Kontoinformationsdienstleister im Sinne des Artikels 33 Absatz 1,

c) Zahlungsinstitute, die gemäß Artikel 32 Absatz 1 ausgenommen sind, und

d) E-Geld-Institute, für die eine Ausnahme gemäß Artikel 9 Absatz 1 der Richtlinie 2009/110/EG gilt;".

5. Dem Artikel 96 wird folgender Absatz angefügt:

„(7) Die Mitgliedstaaten stellen sicher, dass die Absätze 1 bis 5 des vorliegenden Artikels nicht gelten für

a) Zahlungsdienstleister im Sinne des Artikels 1 Absatz 1 Buchstaben a, b und d,

b) Kontoinformationsdienstleister im Sinne des Artikels 33 Absatz 1,

c) Zahlungsinstitute, die gemäß Artikel 32 Absatz 1 ausgenommen sind, und

d) E-Geld-Institute, für die eine Ausnahme gemäß Artikel 9 Absatz 1 der Richtlinie 2009/110/EG gilt."

6. Artikel 98 Absatz 5 erhält folgende Fassung:

„(5) Gemäß Artikel 10 der Verordnung (EU) Nr. 1093/2010 überprüft und aktualisiert die EBA — soweit erforderlich — die technischen Regulierungsstandards regelmäßig, um unter anderem der Innovation und den technologischen Entwicklungen sowie den Bestimmungen des Kapitels II der Verordnung (EU) 2022/2554 Rechnung zu tragen."

Artikel 8

Änderung der Richtlinie (EU) 2016/2341

Artikel 21 Absatz 5 der Richtlinie (EU) 2016/2341 erhält folgende Fassung:

„(5) Die Mitgliedstaaten stellen sicher, dass die EbAV angemessene Vorkehrungen treffen, einschließlich der Entwicklung von Notfallplänen, um die Kontinuität und Ordnungsmäßigkeit ihrer Tätigkeiten zu gewährleisten.

Gegebenenfalls greifen die EbAV zu diesem Zweck auf geeignete und verhältnismäßige Systeme, Ressourcen und Verfahren zurück, richten insbesondere Netzwerk- und Informationssysteme ein und verwalten diese gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*).

(*) 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 (ABl. L 333 vom 27.12.2022, S. 1).“.

Artikel 9

Umsetzung

(1) Spätestens am 17. Januar 2025 erlassen und veröffentlichen die Mitgliedstaaten die Maßnahmen, die erforderlich sind, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Sie wenden diese Maßnahmen ab dem 17. Januar 2025 an.

Bei Erlass dieser Maßnahmen nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten dieser Bezugnahme.

(2) Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten nationalen Maßnahmen mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 10

Inkrafttreten

Diese Richtlinie tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Artikel 11

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Straßburg am 14. Dezember 2022.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident*
R. METSOLA	M. BEK