Amtsblatt
der Europäischen Union

DE
Reihe L

2024/1773

25.6.2024

DELEGIERTE VERORDNUNG (EU) 2024/1773 DER KOMMISSION

vom 13. März 2024

zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards 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

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die 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 ([1]), insbesondere auf Artikel 28 Absatz 10 Unterabsatz 3,

in Erwägung nachstehender Gründe:

(1) Nach dem mit der Verordnung (EU) 2022/2554 geschaffenen Rahmen für die digitale operationale Resilienz im Finanzsektor müssen Finanzunternehmen bestimmte Schlüsselprinzipien für das Management des IKT-Drittparteienrisikos festlegen, die insbesondere dann wichtig sind, wenn Finanzunternehmen zur Unterstützung ihrer kritischen oder wichtigen Funktionen auf IKT-Drittdienstleister zurückgreifen.

(2) Finanzunternehmen müssen im Rahmen ihres IKT-Risikomanagementrahmens eine Strategie für das IKT-Drittparteienrisiko annehmen und regelmäßig überprüfen. Nach Artikel 28 Absatz 2 der Verordnung (EU) 2022/2554 muss diese Strategie eine Leitlinie für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen, die von IKT-Drittdienstleistern bereitgestellt werden. Sie gilt auf individueller und gegebenenfalls teilkonsolidierter und konsolidierter Basis.

(3) Finanzunternehmen unterscheiden sich in ihrer Größe, Struktur und internen Organisation sowie in der Art und Komplexität ihrer Tätigkeiten und Geschäfte erheblich voneinander. Es ist notwendig, dieser Vielfalt Rechnung zu tragen und bei der Ausarbeitung 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 „Leitlinie“), bestimmte grundlegende regulatorische Anforderungen einzuführen, die für alle Finanzunternehmen angemessen sind, und sicherzustellen, dass diese Anforderungen in einer verhältnismäßigen Weise angewandt werden.

(4) Gehören Finanzunternehmen einer Gruppe an, so sollte das Mutterunternehmen, das für die Erstellung des konsolidierten oder teilkonsolidierten Abschlusses für die Gruppe verantwortlich zeichnet, sicherstellen, dass die Leitlinie innerhalb der Gruppe auf konsistente und kohärente Weise angewandt wird.

(5) Bei der Anwendung der Leitlinie sollten gruppeninterne IKT-Dienstleister, einschließlich solcher, die sich im vollständigen oder gemeinsamen Besitz von Finanzunternehmen innerhalb desselben institutsbezogenen Sicherungssystems befinden, als IKT-Drittdienstleister betrachtet werden. Wenngleich die von gruppeninternen IKT-Dienstleistern ausgehenden Risiken möglicherweise anderer Art sind, gelten für sie dieselben Anforderungen nach der Verordnung (EU) 2022/2554. Werden die Dienstleistungen über eine Kette von IKT-Drittdienstleistern bereitgestellt, so sollte die Leitlinie entsprechend auch für Unterauftragnehmer gelten, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon für IKT-Drittdienstleister erbringen.

(6) Das übergeordnete Prinzip, wonach die Verantwortung für das Management des IKT-Risikos eines Finanzunternehmens letztlich beim Leitungsorgan liegt, gilt auch bei der Nutzung von IKT-Drittdienstleistern. Diese Verantwortung sollte sich weiter im kontinuierlichen Engagement des Leitungsorgans bei der Kontrolle und Überwachung des IKT-Risikomanagements niederschlagen, einschließlich bei der Annahme und mindestens jährlichen Überprüfung der Leitlinie.

([1]) ABl. L 333 vom 27.12.2022, S. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(7) Um eine angemessene Berichterstattung an das Leitungsorgan zu gewährleisten, sollten in der Leitlinie die internen Zuständigkeiten für die Genehmigung, das Management, die Kontrolle und die Dokumentation vertraglicher Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden (im Folgenden „vertragliche Vereinbarungen"), einschließlich der IKT-Dienstleistungen, die im Rahmen vertraglicher Vereinbarungen nach Artikel 28 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 erbracht werden, eindeutig spezifiziert und ermittelt werden.

(8) Damit allen möglichen Risiken, die bei der Vergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen entstehen können, Rechnung getragen wird, sollte die Leitlinie die einzelnen Schritte in jeder Hauptphase des Lebenszyklus vertraglicher Vereinbarungen mit Drittdienstleistern nachzeichnen.

(9) Um die ermittelten Risiken zu mindern, sollte in der Leitlinie spezifiziert werden, wie vertragliche Vereinbarungen zu planen sind, einschließlich der Risikobewertung, des Verfahrens zur Erfüllung der Sorgfaltspflicht und des Genehmigungsverfahrens für neue oder wesentliche Änderungen dieser vertraglichen Vereinbarungen. Um die Risiken zu managen, die vor dem Abschluss einer vertraglichen Vereinbarung mit einem IKT-Drittdienstleister entstehen könnten, sollte die Leitlinie ein geeignetes und verhältnismäßiges Verfahren für die Auswahl und die Bewertung der Eignung künftiger IKT-Drittdienstleister enthalten und vorschreiben, dass das Finanzunternehmen eine nicht erschöpfende Liste von Elementen zu berücksichtigen hat, die bei einem IKT-Drittdienstleister gegeben sein müssen. In der Liste sollten insbesondere auch Elemente enthalten sein, die die geschäftliche Reputation der Dienstleister, ihre finanziellen, personellen und technischen Ressourcen, ihre Informationssicherheit, ihre Organisationsstruktur, einschließlich Risikomanagement, und ihre internen Kontrollen betreffen.

(10) Um bei der Bereitstellung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen durch IKT-Drittdienstleister ein solides Risikomanagement zu gewährleisten, sollte die Leitlinie Informationen über die Implementierung, die Überwachung und das Management der vertraglichen Vereinbarungen, gegebenenfalls auch auf konsolidierter und teilkonsolidierter Ebene, enthalten. Dazu gehören auch Anforderungen hinsichtlich der Vertragsklauseln über gegenseitige Verpflichtungen der Finanzunternehmen und IKT-Drittdienstleister, die schriftlich niedergelegt werden sollten. Um eine effiziente Beaufsichtigung zu gewährleisten und die Resilienz im Falle von Änderungen des Geschäftsmodells oder -umfelds zu fördern, sollten in der Leitlinie die Rechte der Finanzunternehmen oder der beauftragten Dritten und der zuständigen Behörden im Zusammenhang mit Inspektionen und dem Zugang zu Informationen gewährleistet und die Ausstiegsstrategien und Beendigungsverfahren genauer festgelegt werden.

(11) Soweit personenbezogene Daten von IKT-Drittdienstleistern verarbeitet werden, lassen die Leitlinie und etwaige vertragliche Vereinbarungen die Verpflichtungen aus der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([2]) unberührt und sollten diese ergänzen, z. B. durch einen schriftlichen Vertrag, in dem beschrieben wird, wie personenbezogene Daten zu verarbeiten sind, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten, und in dem alle anderen nach dieser Verordnung erforderlichen Elemente festgelegt werden.

([2]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Der in Artikel 54 der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates ([3]), in Artikel 54 der Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates ([4]) und in Artikel 54 der Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates ([5]) genannte Gemeinsame Ausschuss der Europäischen Aufsichtsbehörden hat zu diesem Entwurf technischer Regulierungsstandards, auf dem die vorliegende Verordnung beruht, öffentliche Konsultationen durchgeführt, die damit verbundenen Kosten- und Nutzeneffekte analysiert und die Stellungnahme der nach Artikel 37 der Verordnung (EU) Nr. 1093/2010 eingesetzten Interessengruppe Bankensektor, der nach Artikel 37 der Verordnung (EU) Nr. 1094/2010 eingesetzten Interessengruppe Versicherung und Rückversicherung und der nach Artikel 37 der Verordnung (EU) Nr. 1095/2010 eingesetzten Interessengruppe Wertpapiere und Wertpapiermärkte eingeholt.

(13) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([6]) angehört und hat am 24. Januar 2024 eine Stellungnahme abgegeben —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Gesamtrisikoprofil und -komplexität

In der Leitlinie für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden (im Folgenden „Leitlinie"), werden die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art und der Umfang seiner Dienstleistungen, Tätigkeiten und Geschäfte und die Elemente berücksichtigt, durch die sich deren Komplexität erhöht oder verringert, einschließlich der Elemente, die Folgendes betreffen:

a) die Art der IKT-Dienstleistungen, die Gegenstand der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden (im Folgenden „vertragliche Vereinbarung"), sind;

b) den Standort des IKT-Drittdienstleisters oder den Standort seines Mutterunternehmens;

c) ob die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen von einem IKT-Drittdienstleister in einem Mitgliedstaat oder einem Drittstaat bereitgestellt werden, auch unter Berücksichtigung des Standorts, von dem aus die IKT-Dienstleistungen bereitgestellt werden, und des Standorts, an dem die Daten verarbeitet und gespeichert werden;

d) die Art der Daten, die mit dem IKT-Drittdienstleister ausgetauscht werden;

e) ob der IKT-Drittdienstleister derselben Gruppe angehört wie das Finanzunternehmen, für das die Dienstleistungen erbracht werden;

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

f) die Nutzung von IKT-Drittdienstleistern, die einer Zulassung, Registrierung oder der Beaufsichtigung oder Überwachung durch eine zuständige Behörde in einem Mitgliedstaat oder dem Überwachungsrahmen nach Kapitel V Abschnitt II der Verordnung (EU) 2022/2554 unterliegen, sowie die Nutzung von IKT-Drittdienstleistern, auf die dies nicht zutrifft;

g) die Nutzung von IKT-Drittdienstleistern, die der Zulassung, Registrierung oder der Beaufsichtigung oder Überwachung durch eine Aufsichtsbehörde in einem Drittstaat unterliegen, sowie die Nutzung von IKT-Drittdienstleistern, auf die dies nicht zutrifft;

h) ob die Bereitstellung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen sich auf einen einzigen IKT-Drittdienstleister oder eine kleine Anzahl solcher Dienstleister konzentriert;

i) die Übertragbarkeit der IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen auf einen anderen IKT-Drittdienstleister, auch aufgrund technologischer Besonderheiten;

j) die potenziellen Auswirkungen von Störungen bei der Bereitstellung der IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen auf die Kontinuität der Tätigkeiten des Finanzunternehmens und auf die Verfügbarkeit seiner Dienstleistungen.

Artikel 2

Anwendung auf eine Gruppe

Findet diese Verordnung auf teilkonsolidierter oder konsolidierter Basis Anwendung, so gewährleistet das Mutterunternehmen, das für die Erstellung des konsolidierten oder teilkonsolidierten Abschlusses für die Gruppe verantwortlich zeichnet, dass die Leitlinie in allen Finanzunternehmen, die Teil der Gruppe sind, konsistent umgesetzt wird und für die wirksame Anwendung dieser Verordnung auf allen relevanten Ebenen der Gruppe angemessen ist.

Artikel 3

Governance-Regelungen

(1) Das Leitungsorgan überprüft die Leitlinie mindestens einmal jährlich und aktualisiert sie erforderlichenfalls. Die an der Leitlinie vorgenommenen Änderungen werden zeitnah und sobald dies im Rahmen der einschlägigen vertraglichen Vereinbarungen möglich ist umgesetzt. Das Finanzunternehmen dokumentiert den geplanten zeitlichen Ablauf der Umsetzung.

(2) In der Leitlinie wird eine Methode festgelegt, mit der bestimmt wird, welche IKT-Dienstleistungen kritische oder wichtige Funktionen unterstützen, oder es wird auf eine solche Methode verwiesen. In der Leitlinie ist auch anzugeben, wann eine solche Bewertung vorgenommen und überprüft werden soll.

(3) In der Leitlinie werden die internen Zuständigkeiten für die Genehmigung, das Management, die Kontrolle und die Dokumentation einschlägiger vertraglicher Vereinbarungen eindeutig zugewiesen, und es wird sichergestellt, dass innerhalb des Finanzunternehmens angemessene Fähigkeiten, Erfahrung und Kenntnisse aufrechterhalten werden, damit die einschlägigen vertraglichen Vereinbarungen, einschließlich der im Rahmen dieser Vereinbarungen erbrachten IKT-Dienstleistungen, wirksam überwacht werden können.

(4) Unbeschadet der letztlichen Verantwortung des Finanzunternehmens für die wirksame Beaufsichtigung der einschlägigen vertraglichen Vereinbarungen wird in der Leitlinie vorgeschrieben, dass der IKT-Drittdienstleister laut der Bewertung über ausreichende Ressourcen verfügen muss, um sicherzustellen, dass das Finanzunternehmen alle seine rechtlichen und regulatorischen Anforderungen hinsichtlich der zur Unterstützung kritischer oder wichtiger Funktionen bereitgestellten IKT-Dienstleistungen erfüllt.

(5) In der Leitlinie wird eindeutig angegeben, bei welcher Funktion oder bei welchem Mitglied der Geschäftsleitung die Zuständigkeit für die Überwachung der einschlägigen vertraglichen Vereinbarungen liegt. In der Leitlinie wird festgelegt, wie diese Funktion oder dieses Mitglied der Geschäftsleitung mit den Kontrollfunktionen zusammenarbeitet, es sei denn, die Funktion oder das Mitglied ist Teil der Kontrollfunktionen, und es werden die Berichtspflichten gegenüber dem Leitungsorgan festgelegt, einschließlich der Art der zu meldenden Informationen und der vorzulegenden Dokumentation. Darüber hinaus wird festgelegt, wie häufig diese Berichterstattung erfolgt.

(6) Die Leitlinie gewährleistet, dass die vertraglichen Vereinbarungen mit Folgendem im Einklang stehen:

a) dem in Artikel 6 der Verordnung (EU) 2022/2554 genannten IKT-Risikomanagementrahmen;

b) der in Artikel 9 Absatz 4 der Verordnung (EU) 2022/2554 genannten Informationssicherheitsleitlinie;

c) der in Artikel 11 der Verordnung (EU) 2022/2554 genannten IKT-Geschäftsfortführungsleitlinie;

d) den in Artikel 19 der Verordnung (EU) 2022/2554 festgelegten Anforderungen für die Meldung von Vorfällen.

(7) In der Leitlinie ist vorzusehen, dass IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden, einer unabhängigen Überprüfung unterzogen und in den Auditplan aufgenommen werden.

(8) In der Leitlinie ist ausdrücklich festzulegen, dass die vertraglichen Vereinbarungen

a) das Finanzunternehmen und sein Leitungsorgan nicht von ihren aufsichtlichen Pflichten und Verantwortlichkeiten gegenüber ihren Kunden entbinden;

b) die wirksame Beaufsichtigung eines Finanzunternehmens nicht verhindern und nicht gegen aufsichtliche Einschränkungen für Dienstleistungen und Tätigkeiten verstoßen dürfen;

c) vorschreiben müssen, dass die IKT-Drittdienstleister mit den zuständigen Behörden zusammenarbeiten;

d) vorschreiben müssen, dass das Finanzunternehmen, seine Revisoren und die zuständigen Behörden wirksam Zugang zu Daten und Räumlichkeiten haben müssen, die mit der Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen zusammenhängen.

Artikel 4

Hauptphasen des Lebenszyklus mit Blick auf die Annahme und Nutzung vertraglicher Vereinbarungen

In der Leitlinie werden für jede Hauptphase des Lebenszyklus der vertraglichen Vereinbarung die Anforderungen, einschließlich der Regelungen, Zuständigkeiten und Prozesse, festgelegt, die mindestens Folgendes abdecken:

a) die Zuständigkeiten des Leitungsorgans, gegebenenfalls einschließlich seiner Beteiligung an der Entscheidungsfindung hinsichtlich der Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden;

b) die Planung vertraglicher Vereinbarungen, einschließlich der Risikobewertung, des Verfahrens zur Erfüllung der Sorgfaltspflicht nach den Artikeln 5 und 6 und des Genehmigungsverfahrens für neue oder wesentliche Änderungen vertraglicher Vereinbarungen im Sinne von Artikel 8 Absatz 4;

c) die Einbeziehung von Geschäftsbereichen, internen Kontrollen und anderen relevanten Organisationsbereichen in Bezug auf vertragliche Vereinbarungen;

d) die Umsetzung, die Überwachung und das Management vertraglicher Vereinbarungen nach den Artikeln 7, 8 und 9, gegebenenfalls auch auf konsolidierter und teilkonsolidierter Ebene;

e) die Dokumentation und die Erstellung von Aufzeichnungen unter Berücksichtigung der für das Informationsregister nach Artikel 28 Absatz 3 der Verordnung (EU) 2022/2554 geltenden Anforderungen;

f) die Ausstiegsstrategien und Beendigungsverfahren nach Artikel 10.

Artikel 5

Ex-ante-Risikobewertung

(1) Nach der Leitlinie muss vor Abschluss einer vertraglichen Vereinbarung der Geschäftsbedarf des Finanzunternehmens bestimmt werden.

(2) In der Leitlinie ist vorzusehen, dass auf Ebene des Finanzunternehmens und gegebenenfalls auf konsolidierter und teilkonsolidierter Ebene eine Risikobewertung durchzuführen ist, bevor eine vertragliche Vereinbarung geschlossen wird.

Bei der Risikobewertung werden alle einschlägigen Anforderungen der Verordnung (EU) 2022/2554 sowie die geltenden sektorspezifischen Rechtsvorschriften der Union berücksichtigt. In der Leitlinie werden insbesondere die Auswirkungen der Bereitstellung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen durch IKT-Drittdienstleister auf das Finanzunternehmen sowie alle Risiken berücksichtigt, die mit der Bereitstellung dieser IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen durch IKT-Drittdienstleister verbunden sind, darunter

a) operationelle Risiken,

b) rechtliche Risiken,

c) IKT-Risiken,

d) Reputationsrisiken,

e) Risiken im Zusammenhang mit dem Schutz vertraulicher oder personenbezogener Daten,

f) Risiken im Zusammenhang mit der Verfügbarkeit von Daten,

g) Risiken im Zusammenhang mit dem Standort, an dem die Daten verarbeitet und gespeichert werden,

h) Risiken im Zusammenhang mit dem Standort des IKT-Drittdienstleisters,

i) IKT-Konzentrationsrisiken auf Unternehmensebene.

Artikel 6

Sorgfaltspflicht

(1) In der Leitlinie wird ein angemessenes und verhältnismäßiges Verfahren für die Auswahl und Bewertung der künftigen IKT-Drittdienstleister festgelegt, wobei zu berücksichtigen ist, ob es sich bei dem IKT-Drittdienstleister um einen gruppeninternen IKT-Dienstleister handelt, und verlangt wird, dass das Finanzunternehmen vor Abschluss einer vertraglichen Vereinbarung bewertet, ob der IKT-Drittdienstleister

a) über die geschäftliche Reputation, hinreichende Fähigkeiten, Fachkenntnisse und angemessene finanzielle, personelle und technische Ressourcen, Informationssicherheitsstandards, eine angemessene Organisationsstruktur, ein angemessenes Risikomanagement und angemessene interne Kontrollen sowie gegebenenfalls über die erforderlichen Zulassungen oder Registrierungen verfügt, um die IKT-Dienstleistungen zur Unterstützung der kritischen oder wichtigen Funktion zuverlässig und professionell erbringen zu können;

b) in der Lage ist, einschlägige technologische Entwicklungen zu überwachen und führende Praktiken im Bereich der IKT-Sicherheit zu ermitteln und sie gegebenenfalls zu implementieren, damit er über einen wirksamen und soliden Rahmen für die digitale operationale Resilienz verfügt;

c) IKT-Unterauftragnehmer nutzt oder zu nutzen gedenkt, um IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon zu erbringen;

d) in einem Drittstaat lokalisiert ist oder die Daten in einem Drittstaat verarbeitet oder speichert und, falls dies der Fall ist, ob diese Praxis die operationellen Risiken, Reputationsrisiken oder das Risiko erhöht, von restriktiven Maßnahmen, einschließlich Embargos und Sanktionen, betroffen zu sein, die sich auf die Fähigkeit des IKT-Drittdienstleisters, die IKT-Dienstleistungen zu erbringen, oder die Fähigkeit des Finanzunternehmens, diese IKT-Dienstleistungen zu empfangen, auswirken können;

e) vertraglichen Vereinbarungen zustimmt, mit denen effektiv die Möglichkeit sichergestellt wird, dass das Finanzunternehmen selbst, beauftragte Dritte und zuständige Behörden Audits beim IKT-Drittdienstleister, auch in dessen Räumlichkeiten, durchführen;

f) in ethischer und sozial verantwortlicher Weise handelt, die Menschenrechte und die Rechte des Kindes achtet, einschließlich des Verbots der Kinderarbeit, die geltenden Grundsätze des Umweltschutzes einhält und angemessene Arbeitsbedingungen gewährleistet.

(2) In der Leitlinie wird festgelegt, welches Maß an Sicherheit hinsichtlich der Wirksamkeit des Risikomanagementrahmens von IKT-Drittdienstleistern für IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von einem IKT-Drittdienstleister bereitgestellt werden sollen, gegeben sein muss. In der Leitlinie ist vorzusehen, dass im Rahmen des Verfahrens zur Erfüllung der Sorgfaltspflicht bewertet wird, ob Maßnahmen zur Risikominderung und zur Geschäftsfortführung bestehen und wie deren Funktionsfähigkeit innerhalb des IKT-Drittdienstleisters sichergestellt wird.

(3) In der Leitlinie wird das Verfahren zur Erfüllung der Sorgfaltspflicht festgelegt, anhand dessen die künftigen IKT-Drittdienstleister ausgewählt und bewertet werden, und es wird angegeben, welche der folgenden Elemente mit Blick auf das erforderliche Maß an Sicherheit für die Leistungsfähigkeit des IKT-Drittdienstleisters zu berücksichtigen sind:

a) Audits oder unabhängige Bewertungen, die vom Finanzunternehmen selbst oder in seinem Auftrag durchgeführt werden;

b) Berichte über unabhängige Audits, die auf Verlangen des IKT-Drittdienstleisters erstellt werden;

c) Auditberichte der internen Revisionsfunktion des IKT-Drittdienstleisters;

d) geeignete Zertifizierungen Dritter;

e) andere relevante Informationen, die dem Finanzunternehmen zur Verfügung stehen, oder andere vom IKT-Drittdienstleister bereitgestellte Informationen.

(4) Die Finanzunternehmen gewährleisten unter Berücksichtigung der in Absatz 3 Buchstaben a bis e aufgeführten Elemente ein angemessenes Maß an Sicherheit für die Leistungsfähigkeit des IKT-Drittdienstleisters. Gegebenenfalls ist mehr als eines der unter diesen Buchstaben aufgeführten Elemente zu berücksichtigen.

Artikel 7

Interessenkonflikte

(1) In der Leitlinie werden geeignete Maßnahmen festgelegt, die vor Abschluss einschlägiger vertraglicher Vereinbarungen zu ergreifen sind, um die sich aus der Nutzung von IKT-Drittdienstleistern ergebenden tatsächlichen oder potenziellen Interessenkonflikte zu ermitteln, zu vermeiden und zu managen, und es wird eine kontinuierliche Überwachung solcher Interessenkonflikte vorgesehen.

(2) Werden IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen von gruppeninternen IKT-Dienstleistern bereitgestellt, so wird in der Leitlinie festgelegt, dass Entscheidungen über die Bedingungen für diese IKT-Dienstleistungen, einschließlich der finanziellen Bedingungen, objektiv getroffen werden müssen.

Artikel 8

Vertragsklauseln

(1) In der Leitlinie wird festgelegt, dass die einschlägige vertragliche Vereinbarung schriftlich abzufassen ist und alle in Artikel 30 Absätze 2 und 3 der Verordnung (EU) 2022/2554 genannten Elemente enthalten muss. Die Leitlinie umfasst auch Elemente mit Blick auf die in Artikel 1 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannten Anforderungen sowie gegebenenfalls andere einschlägige Rechtsvorschriften der Union und der Mitgliedstaaten.

(2) In der Leitlinie ist festzulegen, dass die einschlägigen vertraglichen Vereinbarungen das Recht des Finanzunternehmens auf Zugang zu Informationen, auf die Durchführung von Inspektionen und Audits sowie auf die Durchführung von IKT-Tests vorsehen müssen. In der Leitlinie ist vorzusehen, dass das Finanzunternehmen zu diesen Zwecken — unbeschadet seiner letztlichen Verantwortung — auf folgende Methoden zurückgreifen muss:

a) eigene interne Audits oder Audits eines beauftragten Dritten;

b) gegebenenfalls Sammelaudits und gepoolte IKT-Tests, einschließlich bedrohungsorientierter Penetrationstests, die gemeinsam mit anderen als Auftraggeber auftretenden Finanzunternehmen oder Firmen, die IKT-Dienstleistungen desselben IKT-Drittdienstleisters nutzen, organisiert und von diesen Finanzunternehmen oder Firmen oder einem von ihnen beauftragten Dritten durchgeführt werden;

c) gegebenenfalls Zertifizierungen Dritter;

d) gegebenenfalls Berichte über interne oder von Dritten durchgeführte Audits, die vom IKT-Drittdienstleister zur Verfügung gestellt werden.

(3) Das Finanzunternehmen darf sich längerfristig nicht nur auf die in Absatz 2 Buchstabe c genannten Zertifizierungen oder die in Absatz 2 Buchstabe d genannten Auditberichte verlassen. Nach der Leitlinie ist die Anwendung der in Absatz 2 Buchstaben c und d genannten Methoden nur dann gestattet, wenn das Finanzunternehmen

a) den Auditplan des IKT-Drittdienstleisters für die einschlägigen vertraglichen Vereinbarungen als zufriedenstellend erachtet;

b) sicherstellt, dass der Umfang der Zertifizierungen oder Auditberichte die von ihm ermittelten Systeme und wesentlichen Kontrollen abdeckt und die Einhaltung der einschlägigen rechtlichen Anforderungen gewährleistet;

c) den Inhalt der Zertifizierungen oder Auditberichte laufend gründlich bewertet und prüft, ob die Berichte oder Zertifizierungen nicht obsolet sind;

d) sicherstellt, dass wesentliche Systeme und Kontrollen in künftigen Fassungen der Zertifizierung oder des Auditberichts berücksichtigt werden;

e) die zertifizierende oder prüfende Partei in zufriedenstellendem Maße für geeignet hält;

f) davon überzeugt ist, dass die Zertifizierungen ausgestellt werden und die Zertifizierungen und die Audits nach weithin anerkannten einschlägigen professionellen Standards durchgeführt werden und einen Test der operationalen Wirksamkeit der bestehenden wesentlichen Kontrollen umfassen;

g) das vertragliche Recht hat, in einer aus der Perspektive des Risikomanagements vertretbaren und legitimen Häufigkeit Änderungen des Umfangs der Zertifizierungen oder Auditberichte mit Blick auf andere einschlägige Systeme und Kontrollen zu verlangen;

h) das vertragliche Recht hat, nach eigenem Ermessen Einzel- und Sammelaudits im Zusammenhang mit den vertraglichen Vereinbarungen durchzuführen und diese Rechte in der vereinbarten Häufigkeit wahrzunehmen.

(4) Die Leitlinie stellt sicher, dass wesentliche Änderungen der vertraglichen Vereinbarung in einem schriftlichen Dokument förmlich festgehalten werden, das von allen Parteien datiert und unterzeichnet wird und in dem das Verfahren zur Verlängerung der vertraglichen Vereinbarungen festgelegt ist.

Artikel 9

Überwachung der vertraglichen Vereinbarungen

(1) In der Leitlinie ist vorzusehen, dass in den vertraglichen Vereinbarungen die Maßnahmen und Schlüsselindikatoren festgelegt werden, anhand deren die Leistungsfähigkeit der IKT-Drittdienstleister kontinuierlich überwacht wird, einschließlich Maßnahmen, die dazu dienen, die Einhaltung der Anforderungen für die Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität von Daten und Informationen und die Einhaltung der einschlägigen Strategien und Verfahren des Finanzunternehmens durch die IKT-Drittdienstleister zu überwachen. Darüber hinaus sind in der Leitlinie Maßnahmen zu spezifizieren, die Anwendung finden, wenn Dienstleistungsvereinbarungen nicht eingehalten werden, und gegebenenfalls Vertragsstrafen umfassen.

(2) In der Leitlinie wird festgelegt, wie das Finanzunternehmen bewertet, ob die IKT-Drittdienstleister, die für die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen in Anspruch genommen werden, angemessene Leistungs- und Qualitätsstandards im Einklang mit der vertraglichen Vereinbarung und den Strategien des Finanzunternehmens einhalten. Die Leitlinie muss insbesondere gewährleisten, dass

a) die IKT-Drittdienstleister dem Finanzunternehmen angemessene Berichte über ihre Tätigkeiten und Dienstleistungen vorlegen, darunter regelmäßige Berichte, Berichte über Vorfälle, Berichte über die Erbringung von Dienstleistungen, Berichte über die IKT-Sicherheit und Berichte über Maßnahmen und Tests zur Geschäftsfortführung;

b) die Leistungsfähigkeit von IKT-Drittdienstleistern anhand wesentlicher Leistungsindikatoren, wesentlicher Kontrollindikatoren, Audits, Selbstzertifizierungen und unabhängiger Überprüfungen im Einklang mit dem IKT-Risikomanagementrahmen des Finanzunternehmens bewertet wird;

c) das Finanzunternehmen andere relevante Informationen von den IKT-Drittdienstleistern erhält;

d) das Finanzunternehmen gegebenenfalls über IKT-bezogene Vorfälle und operationale oder sicherheitsbezogene Vorfälle im Zusammenhang mit Zahlungen unterrichtet wird;

e) eine unabhängige Überprüfung und Audits vorgenommen werden, um die Einhaltung der rechtlichen und regulatorischen Anforderungen und Strategien zu prüfen.

(3) In der Leitlinie wird festgelegt, dass die Bewertung nach Absatz 2 zu dokumentieren ist und ihre Ergebnisse verwendet werden müssen, um die Risikobewertung des Finanzunternehmens im Sinne von Artikel 6 zu aktualisieren.

(4) In der Leitlinie werden die geeigneten Maßnahmen festgelegt, die das Finanzunternehmen ergreifen muss, wenn es Mängel beim IKT-Drittdienstleister, einschließlich IKT-bezogener Vorfälle und operationaler oder sicherheitsbezogener Vorfälle im Zusammenhang mit Zahlungen, bei der Erbringung der IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder bei der Einhaltung vertraglicher Vereinbarungen oder rechtlicher Anforderungen feststellt. Ferner wird darin festgelegt, wie die Umsetzung solcher Maßnahmen zu überwachen ist, um sicherzustellen, dass die Maßnahmen innerhalb eines festgelegten Zeitrahmens wirksam eingehalten werden, wobei zu berücksichtigen ist, wie wesentlich die Mängel sind.

Artikel 10

Ausstieg aus und Beendigung von vertraglichen Vereinbarungen

Die Leitlinie enthält Anforderungen an einen dokumentierten Ausstiegsplan für jede vertragliche Vereinbarung sowie Anforderungen, die die regelmäßigen Überprüfungen und Tests des dokumentierten Ausstiegsplans betreffen. Bei der Festlegung des Ausstiegsplans ist Folgendes zu berücksichtigen:

a) unvorhergesehene und anhaltende Unterbrechungen bei der Bereitstellung von Dienstleistungen;

b) eine mangelhafte oder nicht erfolgte Erbringung von Dienstleistungen;

c) eine unerwartete Beendigung vertraglicher Vereinbarungen.

Der Ausstiegsplan muss realistisch und durchführbar sein, auf plausiblen Szenarien und vernünftigen Annahmen beruhen und einen Durchführungszeitplan enthalten, der mit den in den vertraglichen Vereinbarungen festgelegten Ausstiegs- und Beendigungsbedingungen vereinbar ist.

Artikel 11

Inkrafttreten

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

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 13. März 2024

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN