EUROPÄISCHE
KOMMISSION

Brüssel, den 24.3.2025
C(2025) 1682 final

DELEGIERTE VERORDNUNG (EU) .../... DER KOMMISSION

vom 24.3.2025

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

(Text von Bedeutung für den EWR)

BEGRÜNDUNG

1. KONTEXT DES DELEGIERTEN RECHTSAKTS

Eines der Ziele der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor besteht darin, die Auslagerungsvorschriften für die indirekte Aufsicht über IKT-Drittdienstleister zu stärken. Mit diesem Ziel sollen die Herausforderungen angegangen werden, vor denen Finanzunternehmen bei der Einhaltung des Rechtsrahmens stehen, wenn bestimmte Funktionen ausgelagert oder weiterverlagert werden.

In diesem Zusammenhang wird den Europäischen Aufsichtsbehörden in Artikel 30 Absatz 5 der Verordnung (EU) 2022/2554 der Auftrag erteilt, einen gemeinsamen Entwurf technischer Regulierungsstandards zur Präzisierung der Aspekte auszuarbeiten, die ein Finanzunternehmen bei der Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen bestimmen und bewerten muss.

Mit dem vorliegenden Entwurf technischer Regulierungsstandards in Form einer delegierten Verordnung wird dem vorgenannten Auftrag entsprochen.

2. KONSULTATIONEN VOR ANNAHME DES RECHTSAKTS

Im Rahmen der Ausarbeitung der in diesem Verordnungsentwurf enthaltenen Standards stellten die Europäischen Aufsichtsbehörden den Entwurf technischer Regulierungsstandards am 8. Dezember 2023 für einen Konsultationszeitraum, der am 4. März 2024 endete, zur öffentlichen Konsultation. Die Europäischen Aufsichtsbehörden erhielten 116 Beiträge von unterschiedlichen Interessenträgern aus dem gesamten Finanzsektor. Ein vollständiger Überblick über die Beiträge der Interessenträger findet sich im Abschlussbericht der Europäischen Aufsichtsbehörden[1].

Die Europäischen Aufsichtsbehörden haben die Antworten aus der öffentlichen Konsultation bewertet und gegebenenfalls Änderungen an dem Entwurf technischer Regulierungsstandards vorgenommen. Die Befragten waren offenbar besorgt über die Verhältnismäßigkeit der Maßnahmen und schlugen vor, dass bei den Anforderungen an die Unterauftragsvergabe ein verhältnismäßigerer Ansatz verfolgt werden sollte, da diese zu aufwendig wären, wenn sie auf die gesamte Kette der IKT-Dienstleistungserbringung angewendet würden. Die Befragten schlugen ferner vor, dass die Verantwortung für die Überwachung der IKT-Unterauftragnehmer in der Verantwortung des IKT-Drittdienstleisters liegen und daher nicht auf das Finanzunternehmen übertragen werden sollte, auch wenn das Finanzunternehmen möglichst sicherstellen sollte, dass der IKT-Drittdienstleister den Unterauftragnehmer überwacht und hinreichend beaufsichtigt. In den Rückmeldungen aus der öffentlichen Konsultation wurde auch auf die Einführung spezifischer Anforderungen für IKT-Drittdienstleister hingewiesen, darunter eine Verantwortung des Drittdienstleisters für die Übermittlung von Informationen an das Finanzunternehmen sowie Anforderungen an die Prüfung und die Zugriffsrechte. Schließlich schlugen die Interessenträger auch einen ausgewogeneren Ansatz zwischen der Vertragsfreiheit und dem gesetzlichen Recht des Finanzunternehmens vor, den Vertrag mit dem Drittdienstleister unter bestimmten Umständen im Falle wesentlicher Änderungen der Unterauftragsvergabe zu kündigen.

[1] https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/operational-resilience/joint-regulatory-technical-subcontracting.

Die Europäischen Aufsichtsbehörden berücksichtigten die Stellungnahmen der Interessenträger, sofern diese relevant und angemessen waren. Artikel 1, der im Hinblick auf die verhältnismäßige Anwendung des Entwurfs technischer Regulierungsstandards durch Finanzunternehmen zu berücksichtigen ist, wurde präzisiert und an die technischen Regulierungsstandards in Bezug auf den Inhalt der Strategie für die vertragliche Vereinbarung über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von Drittdienstleistern erbracht werden, angepasst. Darüber hinaus wurde klargestellt, dass der Entwurf der technischen Regulierungsstandards nur für IKT-Dienstleistungen gilt, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen und von Unterauftragnehmern erbracht werden, wobei der Schwerpunkt auf Unterauftragnehmern liegt, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen sicherstellen. In diesem Zusammenhang wurde die Überwachungspflicht durch Finanzunternehmen klarer formuliert und ein verhältnismäßigerer Ansatz verfolgt.

Der Ansatz für Ex-ante-Risikobewertungen, die vorgenommen werden, bevor IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, an Drittdienstleister vergeben werden dürfen, wurde beibehalten. Die Anforderungen betreffen die Verpflichtung der Finanzunternehmen, zu ermitteln und zu beschreiben, welche der IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen unter welchen Bedingungen für eine Unterauftragsvergabe infrage kommen, und solche Vereinbarungen zu überwachen, wobei unter anderem im Falle von Änderungen der Unterauftragskette Bewertungen vorzunehmen sind. Die ursprünglich vorgesehene Anforderung, dass der Drittdienstleister die vorherige Genehmigung der Finanzunternehmen einholen muss, um wesentliche Änderungen umzusetzen, wurde in eine Anforderung geändert, dass bis zum Ende einer Mitteilungsfrist eine Genehmigung oder eine Nichtbeanstandung vorliegen muss. Der Artikel über Kündigungsrechte wurde ebenfalls präzisiert.

3. RECHTLICHE ASPEKTE DES DELEGIERTEN RECHTSAKTS

In den Artikeln 1 und 2 sind die Vorschriften über die Verhältnismäßigkeit und die Anwendung auf eine Gruppe festgelegt.

Artikel 3 enthält Vorschriften über die Sorgfaltspflicht und die Risikobewertung in Bezug auf den Einsatz von Unterauftragnehmern, die kritische oder wichtige Funktionen unterstützen.

Artikel 4 enthält die Beschreibung und die Bedingungen, unter denen IKT-Dienstleistungen, die eine kritische oder wichtige Funktion unterstützen, an Unterauftragnehmer vergeben werden dürfen.

Die Artikel 5 bis 7 enthalten die Vorschriften für wesentliche Änderungen an Vereinbarungen über die Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die Bestimmungen über die Beendigung der vertraglichen Vereinbarung sowie die Schlussbestimmungen über das Inkrafttreten.

DELEGIERTE VERORDNUNG (EU) .../... DER KOMMISSION

vom 24.3.2025

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

(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[2], insbesondere auf Artikel 30 Absatz 5 Unterabsatz 4,

in Erwägung nachstehender Gründe:

(1) Die Erbringung von IKT-Dienstleistungen für Finanzunternehmen hängt häufig von einer komplexen Kette von IKT-Unterauftragnehmern ab, wobei IKT-Drittdienstleister eine oder mehrere Unterauftragsvereinbarungen mit anderen IKT-Drittdienstleistern schließen können. Die indirekte Abhängigkeit von IKT-Unterauftragnehmern kann die Fähigkeit eines Finanzunternehmens beeinträchtigen, seine Risiken zu ermitteln, zu bewerten und zu steuern, einschließlich Risiken in Verbindung mit lückenhaften Informationen von IKT-Drittdienstleistern sowie mit der begrenzten Möglichkeit eines Finanzunternehmens, Informationen von IKT-Unterauftragnehmern zu erhalten, die IKT-Dienstleistungen erbringen, welche kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen. In diesem Zusammenhang ist es in Fällen, in denen die Erbringung von IKT-Dienstleistungen für Finanzunternehmen von einer potenziell langen oder komplexen Kette von IKT-Unterauftragnehmern abhängt, von wesentlicher Bedeutung, dass Finanzunternehmen die Gesamtkette der Unterauftragnehmer ermitteln, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen erbringen.

(2) Von den Unterauftragnehmern, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen erbringen, sollten sich Finanzunternehmen insbesondere und kontinuierlich auf diejenigen Unterauftragnehmer konzentrieren, die die IKT-Dienstleistung zur Unterstützung kritischer oder wichtiger Funktionen sicherstellen, einschließlich aller Unterauftragnehmer, die IKT-Dienstleistungen erbringen, deren Störung die Sicherheit oder Kontinuität der Dienstleistung beeinträchtigen würde, wie im Informationsregister gemäß Artikel 28 Absatz 3 der Verordnung (EU) 2022/2554 festgelegt.

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

(3) Finanzunternehmen unterscheiden sich in Bezug auf Größe, Struktur, interne Organisation sowie Art und Komplexität ihrer Tätigkeiten erheblich. Um die Verhältnismäßigkeit sicherzustellen, sollten diese Unterschiede berücksichtigt werden, wenn festgelegt wird, welche Aspekte ein Finanzunternehmen bei der Untervergabe von IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, bestimmen und bewerten sollte.

(4) Auch wenn die Finanzunternehmen gemäß Artikel 30 Absatz 2 der Verordnung (EU) 2022/2554 die Nutzung von an Unterauftragnehmer vergebenen IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen durch IKT-Drittdienstleister gestatten, entbindet dies die Leitungsorgane der Finanzunternehmen nicht von ihrer letztendlichen Verantwortung für das Risikomanagement und die Einhaltung ihrer gesetzlichen und regulatorischen Pflichten. Ist die Untervergabe von IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, zulässig, ist es wichtig, dass Finanzunternehmen einen klaren und ganzheitlichen Überblick über die Risiken haben, die mit der Vergabe von Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen an Unterauftragnehmer verbunden sind, damit sie diese Risiken überwachen, steuern und mindern können. Daher sollten sie diese Risiken vor der Untervergabe dieser Dienstleistungen bewerten.

(5) Gruppeninterne IKT-Unterauftragnehmer, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon erbringen, einschließlich gruppeninterner IKT-Unterauftragnehmer, die sich im vollständigen oder gemeinsamen Besitz von Finanzunternehmen innerhalb desselben institutsbezogenen Sicherungssystems befinden, sollten als IKT-Unterauftragnehmer betrachtet werden.

(6) Liegt eine Gruppe von Finanzunternehmen vor, sollte gegebenenfalls deren Mutterunternehmen sicherstellen, dass die Leitlinie über den Einsatz von IKT-Unterauftragnehmern, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder eines wesentlichen Teils davon erbringen, innerhalb der Gruppe auf konsistente und kohärente Weise angewandt wird.

(7) Es ist wichtig, ein umfassendes Management der Risiken sicherzustellen, die entstehen können, wenn IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, an Unterauftragnehmer vergeben werden. Aus diesem Grund sollten Finanzunternehmen die einzelnen Phasen des Lebenszyklus einer vertraglichen Vereinbarung über die Nutzung von IKT-Dienstleistungen, die diese Funktionen unterstützen und von IKT-Drittdienstleistern erbracht werden, verfolgen, auch bei Unterauftragsvereinbarungen. Daher sind Anforderungen an Finanzunternehmen festzulegen, die in ihren vertraglichen Vereinbarungen mit IKT-Drittdienstleistern zum Ausdruck kommen sollten, wenn die Nutzung von IKT-Dienstleistungen, die an Unterauftragnehmer vergeben werden und kritische oder wichtige Funktionen unterstützen, zulässig ist.

(8) Um Risiken im Zusammenhang mit der Vergabe von Unteraufträgen zu mindern, müssen die Bedingungen festgelegt werden, unter denen IKT-Drittdienstleister Unterauftragnehmer für die Erbringung von IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, in Anspruch nehmen können. Zu diesem Zweck sollten in vertraglichen IKT-Vereinbarungen zwischen Finanzunternehmen und IKT-Drittdienstleistern entsprechende Bedingungen festgelegt werden, einschließlich der Planung von Unterauftragsvereinbarungen, der Risikobewertungen, der Sorgfaltspflicht und des Genehmigungsverfahrens für neue IKT-

Unterauftragsvereinbarungen für IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon. Gleiches gilt für wesentliche Änderungen an bestehenden Vereinbarungen, die vom IKT-Drittdienstleister vorgenommen werden.

(9) Um Risiken zu ermitteln, die entstehen könnten, bevor ein Finanzunternehmen eine Vereinbarung mit einem IKT-Unterauftragnehmer schließt, sollten IKT-Drittdienstleister die Eignung potenzieller Unterauftragnehmer auf der Grundlage der vertraglichen IKT-Vereinbarungen, die der IKT-Drittdienstleister mit dem Finanzunternehmen geschlossen hat, angemessen und verhältnismäßig bewerten. Diese vertraglichen IKT-Vereinbarungen sollten daher vorschreiben, dass der IKT-Drittdienstleister oder gegebenenfalls das Finanzunternehmen direkt die Ressourcen des potenziellen Unterauftragnehmers bewertet, zum Beispiel seine Fachkenntnisse und die Frage, ob er über angemessene finanzielle, personelle und technische Ressourcen verfügt, seine Informationssicherheit und seine Organisationsstruktur, einschließlich des Risikomanagements und der internen Kontrollen, über die der Unterauftragnehmer verfügen sollte.

(10) Um Schwachstellen und Bedrohungen, die Risiken für ihre IKT-Systeme und -Vorgänge darstellen können, zu mindern, sollten Finanzunternehmen in der Lage sein, die Leistung der IKT-Dienstleistung zu überwachen und über alle relevanten Änderungen innerhalb ihrer IKT-Unterauftragskette unterrichtet zu werden, wenn diese Änderungen kritische oder wichtige Funktionen betreffen.

(11) Damit Finanzunternehmen die Risiken im Zusammenhang mit Unterauftragsvereinbarungen oder wesentlichen Änderungen daran bewerten können, sollten IKT-Drittdienstleister die Finanzunternehmen, für die sie IKT-Dienstleistungen erbringen, über alle derartigen neuen Vereinbarungen oder Änderungen rechtzeitig vor deren Inkrafttreten informieren. Aus demselben Grund sollten Finanzunternehmen das Recht haben, den Vertrag mit dem IKT-Drittdienstleister zu kündigen, wenn das Ergebnis ihrer Risikobewertung zeigt, dass die neuen Vereinbarungen oder wesentlichen Änderungen ein Risiko bergen, das ihre Risikotoleranz übersteigt.

(12) Die Europäischen Aufsichtsbehörden haben zu dem Entwurf der technischen Regulierungsstandards, auf den sich diese Verordnung stützt, eine öffentliche Konsultation durchgeführt, die damit verbundenen potenziellen Kosten- und Nutzeneffekte analysiert und nach Artikel 37 der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates[3], Artikel 37 der Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates[4] und Artikel 37 der Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates[5] Empfehlungen der Interessengruppen der Europäischen Aufsichtsbehörden eingeholt.

---

[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

(13) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates konsultiert und hat am 20. August 2024 eine Stellungnahme abgegeben —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1
Gesamtrisikoprofil und Komplexität

Finanzunternehmen berücksichtigen ihre Größe und ihr Gesamtrisikoprofil sowie die Art, den Umfang und die Aspekte erhöhter oder verringerter Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte, einschließlich der Aspekte, die sich auf Folgendes beziehen:

a) die Art der IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die unter die vertragliche Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister fallen;

b) die Art der IKT-Dienstleistungen, die unter die vertragliche Vereinbarung zwischen dem IKT-Drittdienstleister und seinen Unterauftragnehmern fallen;

c) den Standort des IKT-Unterauftragnehmers, der IKT-Dienstleistungen erbringt, die kritische oder wichtige Funktionen oder einen wesentlichen Teil davon unterstützen, oder den Standort seines Mutterunternehmens;

d) die Länge und Komplexität der vom IKT-Drittdienstleister genutzten Kette von Unterauftragnehmern, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon erbringen;

e) die Art der Daten, die an IKT-Unterauftragnehmer weitergegeben werden, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon erbringen;

f) die Frage, ob die IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, von Unterauftragnehmern erbracht werden, die ihren Sitz in einem Mitgliedstaat oder in einem Drittland haben, einschließlich des Standorts, von dem aus die IKT-Dienstleistungen tatsächlich erbracht werden, und des Standorts, an dem die Daten tatsächlich verarbeitet und gespeichert werden;

g) die Frage, ob die IKT-Unterauftragnehmer, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon erbringen, derselben Gruppe angehören wie das Finanzunternehmen, für das diese Dienstleistungen erbracht werden;

h) die Frage, ob die IKT-Unterauftragnehmer, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon erbringen, einer Zulassung, einer 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;

i) die Frage, ob die IKT-Drittdienstleister, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, einer Zulassung, einer Registrierung oder der

---

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).

Beaufsichtigung oder Überwachung durch eine Aufsichtsbehörde in einem Drittstaat unterliegen;

j) die Frage, ob sich die Erbringung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon auf einen einzigen Unterauftragnehmer eines IKT-Drittdienstleisters oder eine kleine Zahl solcher Unterauftragnehmer konzentriert;

k) die Frage, ob sich die Vergabe von Unteraufträgen für IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile unterstützen, auf die Übertragbarkeit dieser IKT-Dienstleistungen auf einen anderen IKT-Drittdienstleister auswirken würde;

l) die potenzielle Auswirkung von Störungen auf die Kontinuität und Verfügbarkeit der IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen und vom IKT-Drittdienstleister erbracht werden, wenn ein Unterauftragnehmer eingesetzt wird, der IKT-Dienstleistungen erbringt, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen.

Artikel 2
Anwendung auf eine Gruppe

Findet diese Verordnung auf teilkonsolidierter oder konsolidierter Basis Anwendung, so trägt das Mutterunternehmen, das für die Erstellung des konsolidierten oder teilkonsolidierten Abschlusses für die Gruppe verantwortlich zeichnet, dafür Sorge, dass die Bedingungen für die Vergabe von Unteraufträgen für die Nutzung von IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen – sofern eine solche Unterauftragsvergabe nach den vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zulässig ist – in allen Finanzunternehmen, die Teil der Gruppe sind, konsistent umgesetzt werden und für die wirksame Anwendung dieser Verordnung auf allen relevanten Ebenen angemessen sind.

Artikel 3
Sorgfaltspflicht und Risikobewertung in Bezug auf den Einsatz von Unterauftragnehmern, die kritische oder wichtige Funktionen unterstützen

(1) Bevor ein Finanzunternehmen eine vertragliche Vereinbarung mit einem IKT-Drittdienstleister schließt, muss es entscheiden, ob dieser IKT-Drittdienstleister eine IKT-Dienstleistung, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützt, an Unterauftragnehmer vergeben darf. Das Finanzunternehmen darf eine solche vertragliche Vereinbarung nur dann schließen, wenn es festgestellt hat, dass alle folgenden Bedingungen erfüllt sind:

a) Durch die im Rahmen der Sorgfaltspflicht durchgeführten Verfahren in Bezug auf den IKT-Drittdienstleister wird sichergestellt, dass dieser in der Lage ist, potenzielle IKT-Unterauftragnehmer, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon erbringen sollen, auszuwählen und deren operative und finanzielle Fähigkeiten zu beurteilen, auch indem er auf Verlangen des Finanzunternehmens an Tests der digitalen operationalen Resilienz gemäß Kapitel IV der Verordnung (EU) 2022/2554 teilnimmt;

b) der IKT-Drittdienstleister ist in der Lage, alle Unterauftragnehmer, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder

wesentlicher Teile davon erbringen, zu ermitteln, um das Finanzunternehmen über diese Unterauftragnehmer zu benachrichtigen und zu informieren, und ist in der Lage, dem Finanzunternehmen alle Informationen zur Verfügung zu stellen, die für die Bewertung der Bedingungen nach diesem Artikel erforderlich sein könnten;

c) der IKT-Drittdienstleister stellt sicher, dass die vertraglichen Vereinbarungen mit den Unterauftragnehmern, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon erbringen, es dem Finanzunternehmen ermöglichen, seine eigenen Verpflichtungen aus der Verordnung (EU) 2022/2554 und den geltenden Rechtsvorschriften der Union und der Mitgliedstaaten zu erfüllen;

d) der Unterauftragnehmer räumt dem Finanzunternehmen und den zuständigen Behörden und Abwicklungsbehörden die gleichen vertraglichen Zugangs- und Inspektionsrechte wie der IKT-Drittdienstleister ein;

e) unbeschadet der letztendlichen Verantwortung des Finanzunternehmens für die Einhaltung seiner rechtlichen und regulatorischen Pflichten verfügt der IKT-Drittdienstleister selbst über ausreichende Fähigkeiten, Fachkenntnisse und angemessene finanzielle, personelle und technische Ressourcen, um die IKT-Risiken auf der Ebene der Unterauftragnehmer zu überwachen, unter anderem durch die Anwendung geeigneter Informationssicherheitsstandards und durch die Einrichtung einer angemessenen Organisationsstruktur, eines entsprechenden Risikomanagements und interner Kontrollen sowie durch die Meldung von Vorfällen und die Reaktion darauf;

f) das Finanzunternehmen verfügt über ausreichende Fähigkeiten, Fachkenntnisse und angemessene finanzielle, personelle und technische Ressourcen, um die IKT-Risiken im Zusammenhang mit der Dienstleistung zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon, die an Unterauftragnehmer vergeben wurde, zu überwachen, unter anderem durch die Anwendung geeigneter Informationssicherheitsstandards und durch die Einrichtung einer angemessenen Organisationsstruktur und eines angemessenen Risikomanagements sowie durch Reaktionsmaßnahmen bei Vorfällen, ein Geschäftsfortführungsmanagement und interne Kontrollen;

g) das Finanzunternehmen hat die Auswirkungen eines möglichen Ausfalls eines Unterauftragnehmers, der IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder eines wesentlichen Teils davon erbringt, auf die digitale operationale Resilienz und die finanzielle Solidität des Finanzunternehmens bewertet;

h) das Finanzunternehmen hat die Risiken bewertet, die mit dem Standort der potenziellen Unterauftragnehmer in Bezug auf die vom IKT-Drittdienstleister erbrachten IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder eines wesentlichen Teils davon verbunden sind;

i) das Finanzunternehmen hat die IKT-Konzentrationsrisiken auf Unternehmensebene gemäß Artikel 29 der Verordnung (EU) 2022/2554 bewertet;

j) das Finanzunternehmen hat geprüft, ob es Hindernisse für die Ausübung der Prüfungs-, Inspektions- und Zugangsrechte durch die zuständigen Behörden,

die Abwicklungsbehörden oder das Finanzunternehmen, einschließlich der von ihnen benannten Personen, gibt.

(2) Finanzunternehmen, die IKT-Drittdienstleister nutzen, welche IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon an Unterauftragnehmer vergeben, führen regelmäßig die in Absatz 1 Buchstaben f bis j genannte Risikobewertung in Bezug auf mögliche Veränderungen in ihrem Geschäftsumfeld durch, auch mit Blick auf Veränderungen bei den unterstützten Geschäftsfunktionen, einschließlich Risikobewertungen der IKT-Bedrohungen, IKT-Konzentrationsrisiken und geopolitischen Risiken.

(3) Der Rückgriff auf die Ergebnisse der Risikobewertung, die ihre IKT-Drittdienstleister für ihre Unterauftragnehmer im Hinblick auf die Erfüllung der in diesem Artikel festgelegten Pflichten durchgeführt haben, entbindet die Finanzunternehmen nicht von ihrer letztendlichen Verantwortung für die Erfüllung ihrer rechtlichen und regulatorischen Pflichten gemäß der Verordnung (EU) 2022/2554.

Artikel 4

Bedingungen, unter denen IKT-Dienstleistungen, die kritische oder wichtige Funktionen einen wesentlichen Teil davon unterstützen, an Unterauftragnehmer vergeben werden können

(1) In der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister wird festgelegt, welche IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, für eine Unterauftragsvergabe infrage kommen und unter welchen Bedingungen. In diesem Vertrag wird festgelegt,

a) dass der IKT-Drittdienstleister für die Erbringung der von den Unterauftragnehmern erbrachten Dienstleistungen verantwortlich ist;

b) dass der IKT-Drittdienstleister verpflichtet ist, alle an Unterauftragnehmer vergebenen IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, zu überwachen, um sicherzustellen, dass seine vertraglichen Verpflichtungen gegenüber dem Finanzunternehmen jederzeit erfüllt werden;

c) welche Überwachungs- und Berichtspflichten der IKT-Drittdienstleister gegenüber dem Finanzunternehmen in Bezug auf Unterauftragnehmer hat, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon erbringen;

d) dass der IKT-Drittdienstleister alle Risiken zu bewerten hat, die mit dem Standort der derzeitigen oder potenziellen Unterauftragnehmer, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon erbringen, und ihres Mutterunternehmens sowie mit dem Standort, von dem aus die betreffende IKT-Dienstleistung erbracht wird, verbunden sind;

e) an welchem Ort die Daten vom Unterauftragnehmer gegebenenfalls verarbeitet oder gespeichert werden;

f) dass der IKT-Drittdienstleister in seinem Vertrag mit seinen Unterauftragnehmern die Überwachungs- und Berichterstattungspflichten

dieses Unterauftragnehmers gegenüber dem IKT-Drittdienstleister und, sofern vereinbart, gegenüber dem Finanzunternehmen festzulegen hat;

g) dass der IKT-Drittdienstleister die Kontinuität der IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, entlang der gesamten Kette von Unterauftragnehmern sicherstellen muss, wenn ein IKT-Unterauftragnehmer seinen vertraglichen Verpflichtungen nicht nachkommt;

h) dass die vertragliche Vereinbarung zwischen dem IKT-Drittdienstleister und seinen Unterauftragnehmern die in Artikel 30 Absatz 3 Buchstabe c der Verordnung (EU) 2022/2554 genannten Anforderungen an Geschäftsfortführungspläne enthält und die von den IKT-Unterauftragnehmern in Bezug auf diese Pläne zu erfüllende Dienstleistungsgüte vorschreibt;

i) dass die vertragliche Vereinbarung zwischen dem IKT-Drittdienstleister und seinen Unterauftragnehmern die IKT-Sicherheitsstandards und alle zusätzlichen Sicherheitsanforderungen nach Artikel 30 Absatz 3 Buchstabe c der Verordnung (EU) 2022/2554 vorschreibt;

j) dass der Unterauftragnehmer dem Finanzunternehmen und den relevanten zuständigen Behörden und Abwicklungsbehörden dieselben Zugangs-, Inspektions- und Auditrechte wie die in Artikel 30 Absatz 3 Buchstabe e der Verordnung (EU) 2022/2254 genannten gewähren muss;

k) dass der IKT-Drittdienstleister dem Finanzunternehmen jede wesentliche Änderung der Unterauftragsvereinbarungen zu melden hat;

l) dass das Finanzunternehmen das Recht hat, den Vertrag mit dem IKT-Drittdienstleister zu kündigen, wenn die in Artikel 6 der vorliegenden Verordnung oder die in Artikel 28 Absatz 7 der Verordnung (EU) 2022/2554 beschriebenen Bedingungen erfüllt sind.

(2) Änderungen, die aufgrund der vorliegenden Verordnung an vertraglichen Vereinbarungen zwischen dem Finanzunternehmen und IKT-Drittdienstleistern, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon erbringen, vorgenommen werden müssen, werden zeitnah und so bald wie möglich umgesetzt. Das Finanzunternehmen dokumentiert den geplanten zeitlichen Ablauf der Umsetzung.

Artikel 5

Wesentliche Änderungen an Unterauftragsvereinbarungen über IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen

(1) Die vertragliche Vereinbarung sieht vor, dass der IKT-Drittdienstleister das Finanzunternehmen rechtzeitig über alle beabsichtigten wesentlichen Änderungen seiner Unterauftragsvereinbarungen informiert, damit das Finanzunternehmen Folgendes bewerten kann:

a) die Auswirkung auf die Risiken, denen er ausgesetzt ist oder ausgesetzt sein könnte;

b) ob solche wesentlichen Änderungen die Fähigkeit des IKT-Drittdienstleisters beeinträchtigen könnten, seinen vertraglichen Verpflichtungen gegenüber dem Finanzunternehmen nachzukommen.

(2) Die vertragliche Vereinbarung muss eine angemessene Mitteilungsfrist enthalten, in der das Finanzunternehmen den Änderungen zustimmen oder sie ablehnen kann.

(3) Der IKT-Drittdienstleister setzt die wesentlichen Änderungen seiner Unterauftragsvereinbarungen erst dann um, wenn das Finanzunternehmen die Änderungen bis zum Ablauf der Mitteilungsfrist entweder genehmigt oder sie nicht abgelehnt hat.

(4) Ist das Finanzunternehmen der Auffassung, dass die in Absatz 1 genannten wesentlichen Änderungen die Risikotoleranz des Finanzunternehmens überschreiten, so muss es vor Ablauf der Mitteilungsfrist

a) den IKT-Drittdienstleister davon in Kenntnis setzen;

b) die Änderungen ablehnen und vor deren Umsetzung Anpassungen verlangen.

Artikel 6

Kündigung des Vertrags zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister

Das Finanzunternehmen hat das Recht, in der vertraglichen Vereinbarung mit dem IKT-Drittdienstleister vorzusehen, dass die vertragliche Vereinbarung in jedem der folgenden Fälle beendet wird:

a) Das Finanzunternehmen hat wesentliche Änderungen der Unterauftragsvereinbarungen zur Unterstützung kritischer oder wichtiger Funktionen abgelehnt und um Anpassungen dieser Änderungen gebeten, doch der IKT-Drittdienstleister hat diese wesentlichen Änderungen dennoch umgesetzt;

b) der IKT-Drittdienstleister hat vor Ablauf der Mitteilungsfrist ohne Genehmigung des Finanzunternehmens wesentliche Änderungen an den Unterauftragsvereinbarungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon vorgenommen;

c) der IKT-Drittdienstleister hat eine IKT-Dienstleistung, die eine kritische oder wichtige Funktion oder einen wesentlichen Teil davon unterstützt, als Unterauftrag vergeben, obwohl eine derartige Unterauftragsvergabe im Vertrag zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister nicht ausdrücklich genehmigt wurde.

Artikel 7

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 24.3.2025

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN