Amtsblatt
der Europäischen Union

DE
Reihe L

2025/295

13.2.2025

DELEGIERTE VERORDNUNG (EU) 2025/295 DER KOMMISSION

vom 24. Oktober 2024

zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Harmonisierung der Bedingungen für die Durchführung von Überwachungstätigkeiten

(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 41 Absatz 2 Unterabsatz 2,

in Erwägung nachstehender Gründe:

(1) Mit dem durch die Verordnung (EU) 2022/2554 geschaffenen Rahmen für die digitale operationale Resilienz im Finanzsektor wird ein Überwachungsrahmen der Union für die gemäß Artikel 31 der genannten Verordnung als kritisch eingestuften Drittdienstleister der Informations- und Kommunikationstechnologie (im Folgenden „IKT-Drittdienstleister“) im Finanzsektor eingeführt.

(2) IKT-Drittdienstleister, die sich dafür entscheiden, einen freiwilligen Antrag auf Einstufung als kritisch zu stellen, sollten der betreffenden Europäischen Aufsichtsbehörde (ESA) alle erforderlichen Informationen zum Nachweis ihrer Kritikalität gemäß den in der Verordnung (EU) 2022/2554 festgelegten Grundsätzen und Kriterien zur Verfügung stellen. Aus diesem Grund sollten die in dem freiwilligen Antrag enthaltenen Informationen hinreichend detailliert und vollständig sein, um eine präzise und umfassende Bewertung der Kritikalität gemäß Artikel 31 Absatz 11 der genannten Verordnung zu ermöglichen. Die zuständige ESA sollte unvollständige Anträge ablehnen und die fehlenden Informationen anfordern.

(3) Die rechtliche Identifizierung von IKT-Drittdienstleistern, die in den Anwendungsbereich dieses technischen Regulierungsstandards fallen, sollte der Kennung entsprechen, die in der gemäß Artikel 28 Absatz 9 der Verordnung (EU) 2022/2554 erlassenen Durchführungsverordnung der Kommission festgelegt ist.

(4) Nachdem die federführende Überwachungsbehörde ihre Empfehlungen an kritische IKT-Drittdienstleister abgegeben hat, sollte sie als Folgemaßnahme deren Einhaltung durch die kritischen IKT-Drittdienstleister überwachen. Im Interesse einer effizienten und wirksamen Überwachung der von den kritischen IKT-Drittdienstleistern im Zusammenhang mit diesen Empfehlungen ergriffenen Maßnahmen oder Abhilfemaßnahmen sollte es der federführenden Überwachungsbehörde möglich sein, die in Artikel 35 Absatz 1 Buchstabe c der Verordnung (EU) 2022/2554 genannten Berichte anzufordern, die als Zwischenberichte über erzielte Fortschritte und Abschlussberichte konzipiert sein sollten.

(5) Für die Zwecke der Bewertung gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2022/2554, wonach die federführende Überwachungsbehörde zu beurteilen hat, ob die von einem kritischen IKT-Drittdienstleister vorgelegte Erklärung ausreichend ist, sollte mit der Mitteilung des kritischen IKT-Drittdienstleisters über seine Absicht, den erhaltenen Empfehlungen Folge zu leisten, eine Beschreibung der Schritte und Maßnahmen, die zur Minderung der in den Empfehlungen dargelegten Risiken ergriffen wurden, einschließlich der entsprechenden Fristen, an die federführende Überwachungsbehörde übermittelt werden. Diese Erklärung sollte in Form eines Plans mit Abhilfemaßnahmen vorgelegt werden.

(6) Da die federführende Überwachungsbehörde die Vereinbarungen der kritischen IKT-Drittdienstleister über die Unterauftragsvergabe bewerten soll, muss eine Vorlage für die Bereitstellung von Informationen über diese Vereinbarungen ausgearbeitet werden. In der Vorlage sollte der Tatsache Rechnung getragen werden, dass kritische IKT-Drittdienstleister anders als Finanzunternehmen strukturiert sind.

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

(7) Nachdem die federführende Überwachungsbehörde ihre Empfehlungen an einen kritischen IKT-Drittdienstleister abgegeben hat und die zuständigen Behörden die betreffenden Finanzunternehmen über die in diesen Empfehlungen ermittelten Risiken in Kenntnis gesetzt haben, sollte die federführende Überwachungsbehörde die Umsetzung der Maßnahmen und der Abhilfemaßnahmen, mit denen der betreffende kritische IKT-Drittdienstleister den Empfehlungen nachkommt, überwachen und bewerten. Die zuständigen Behörden sollten überwachen und bewerten, inwieweit die Finanzunternehmen den in diesen Empfehlungen ermittelten Risiken ausgesetzt sind. Damit bei der Wahrnehmung ihrer jeweiligen Aufgaben die gleichen Voraussetzungen bestehen, sollten sich die zuständigen Behörden und die federführende Überwachungsbehörde über alle wesentlichen Erkenntnisse austauschen, die sie für die Wahrnehmung ihrer jeweiligen Aufgaben benötigen, insbesondere wenn die in den Empfehlungen ermittelten Risiken schwerwiegend sind und bei einer großen Zahl von Finanzunternehmen in mehreren Mitgliedstaaten auftreten. Durch den Informationsaustausch soll sichergestellt werden, dass bei der Rückmeldung der federführenden Überwachungsbehörde an den kritischen IKT-Drittdienstleister über die Umsetzung der Maßnahmen und Abhilfemaßnahmen die Auswirkungen auf die Risiken für Finanzunternehmen berücksichtigt werden und dass die Aufsichtstätigkeiten der zuständigen Behörden auf der Grundlage der Bewertung durch die federführende Überwachungsbehörde durchgeführt werden.

(8) Um einen effizienten und wirksamen Informationsaustausch zu ermöglichen, sollten die zuständigen Behörden im Rahmen ihrer Aufsichtstätigkeiten bewerten, inwieweit die von ihnen beaufsichtigten Finanzunternehmen den in den Empfehlungen ermittelten Risiken ausgesetzt sind. Diese Bewertung sollte verhältnismäßig und risikobasiert erfolgen. Die federführende Überwachungsbehörde sollte die zuständigen Behörden in konkreten Fällen, in denen die in den Empfehlungen dargelegten Risiken schwerwiegend sind und bei einer großen Zahl von Finanzunternehmen in mehreren Mitgliedstaaten auftreten, um Übermittlung der Ergebnisse dieser Bewertung ersuchen. Im Sinne der bestmöglichen Nutzung der Ressourcen der zuständigen Behörden sollte die federführende Überwachungsbehörde bei der Anforderung der Ergebnisse dieser Bewertung stets berücksichtigen, dass der Zweck dieser Auskunftsersuchen darin bestehen sollte, die Umsetzung der Maßnahmen und Abhilfemaßnahmen der kritischen IKT-Drittdienstleister zu bewerten.

(9) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([2]) angehört und hat am 22. Juli 2024 eine Stellungnahme abgegeben.

(10) Die vorliegende Verordnung beruht auf dem Entwurf technischer Regulierungsstandards, der der Kommission von den ESA vorgelegt wurde.

(11) Der Gemeinsame Ausschuss der ESA hat zu dem Entwurf technischer Regulierungsstandards, auf den sich diese Verordnung stützt, offene öffentliche Konsultationen durchgeführt, die damit verbundenen potenziellen Kosten- und Nutzeneffekte analysiert und die Stellungnahmen der nach Artikel 37 der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates ([3]) eingesetzten Interessengruppe „Bankensektor“, der nach Artikel 37 der Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates ([4]) eingesetzten Interessengruppen „Versicherung und Rückversicherung“ und „Betriebliche Altersversorgung“ sowie der nach Artikel 37 der Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates ([5]) eingesetzten Interessengruppe „Wertpapiere und Wertpapiermärkte“ eingeholt —

([2]) 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).

([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).

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Informationen, die IKT-Drittdrittdienstleister im Antrag auf Einstufung als kritisch bereitstellen müssen

(1) Nach Artikel 31 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 übermittelt der Drittdienstleister der Informations- und Kommunikationstechnologie (im Folgenden „IKT-Drittdienstleister“) in einem begründeten Antrag auf freiwillige Einstufung als kritisch gemäß Artikel 31 Absatz 11 der genannten Verordnung folgende Informationen:

a) Name der juristischen Person,

b) Rechtsträgerkennung der juristischen Person,

c) Name der Kontaktperson und Kontaktdaten des kritischen IKT-Drittdienstleisters,

d) Land, in dem die juristische Person ihren Sitz hat,

e) eine Beschreibung der Unternehmensstruktur, die mindestens Angaben zu seinem Mutterunternehmen und anderen verbundenen Unternehmen enthält, die IKT-Dienstleistungen für Finanzunternehmen der Union erbringen. Diese Informationen umfassen gegebenenfalls:

   i) Name der juristischen Personen,

   ii) Rechtsträgerkennung der juristischen Person,

   iii) Land, in dem die juristische Person ihren Sitz hat,

f) geschätzter Marktanteil des IKT-Drittdienstleisters im Finanzsektor der Union und geschätzter Marktanteil nach Art des Finanzunternehmens gemäß Artikel 2 Absatz 1 der Verordnung (EU) 2022/2554 ab dem Jahr des Antrags auf Einstufung als kritisch und für das Vorjahr der Antragstellung,

g) eine Beschreibung aller IKT-Dienstleistungen, die für Finanzunternehmen der Union erbracht werden, einschließlich:

   i) einer Beschreibung der Art der Geschäftstätigkeit und der Art der IKT-Dienstleistungen, die für Finanzunternehmen erbracht werden,

   ii) einer Liste der durch IKT-Dienstleistungen unterstützten Funktionen der Finanzunternehmen, sofern verfügbar,

   iii) Angaben darüber, ob die für Finanzunternehmen erbrachten IKT-Dienstleistungen kritische oder wichtige Funktionen unterstützen, sofern verfügbar,

h) eine Liste der Finanzunternehmen, die die IKT-Dienstleistungen des IKT-Drittdienstleisters in Anspruch nehmen, einschließlich der folgenden Informationen für jedes einzelne Finanzunternehmen, sofern verfügbar:

   i) Name der juristischen Person,

   ii) Rechtsträgerkennung der juristischen Person, sofern dem IKT-Drittdienstleister bekannt,

   iii) Art des Finanzunternehmens gemäß Artikel 2 Absatz 1 der Verordnung (EU) 2022/2554,

   iv) geografischer Standort, von dem aus die IKT-Dienstleistungen für die betreffende juristische Person erbracht werden,

i) eine Liste der kritischen IKT-Drittdienstleister, die in der aktuellsten verfügbaren Fassung der von den ESA gemäß Artikel 31 Absatz 9 der Verordnung (EU) 2022/2554 veröffentlichten Liste dieser Dienstleister aufgeführt werden und die vom Antragsteller erbrachten Dienstleistungen in Anspruch nehmen, sofern verfügbar,

j) eine Selbstbewertung in Bezug auf die folgenden Aspekte:

   i) Grad der Substituierbarkeit für alle vom Antragsteller erbrachten IKT-Dienstleistungen unter Berücksichtigung der folgenden Punkte:

      — Marktanteil des IKT-Drittdienstleisters im Finanzsektor der Union,

— Anzahl der bekannten relevanten Wettbewerber für jede Art von IKT-Dienstleistung oder Gruppe von IKT-Dienstleistungen,

— einer Beschreibung der Besonderheiten der angebotenen IKT-Dienstleistungen, auch in Bezug auf alle proprietären Technologien, oder der besonderen Merkmale der Organisation oder Geschäftstätigkeit des IKT-Drittdienstleisters,

ii) Kenntnis von gleichen IKT-Dienstleistungen, die durch andere als den antragstellenden IKT-Drittdienstleister erbracht werden,

k) Informationen über die künftige Geschäftsstrategie hinsichtlich der Bereitstellung von IKT-Dienstleistungen und -Infrastruktur für Finanzunternehmen in der Union, einschließlich aller geplanten Änderungen in Bezug auf die Gruppen- oder Managementstruktur, die Erschließung neuer Märkte oder Geschäftstätigkeiten,

l) Angaben zu den Unterauftragnehmern des IKT-Drittdienstleisters, die als kritische IKT-Drittdienstleister eingestuft wurden,

m) alle sonstigen Gründe, die für den Antrag des IKT-Drittdienstleisters auf Einstufung als kritisch relevant sind.

(2) Gehört der IKT-Drittdienstleister zu einer Gruppe, so werden die in Absatz 1 genannten Informationen in Bezug auf die von der Gruppe als Ganzes erbrachten IKT-Dienstleistungen zur Verfügung gestellt.

Artikel 2

Inhalt, Struktur und Format der Informationen, die kritische IKT-Drittdienstleister übermitteln, offenlegen oder melden müssen

(1) Kritische IKT-Drittdienstleister stellen der federführenden Überwachungsbehörde auf Anfrage alle Informationen zur Verfügung, die sie benötigt, um ihre Überwachungsaufgaben gemäß den Vorschriften der Verordnung (EU) 2022/2554 wahrzunehmen.

(2) Die in Absatz 1 genannten Informationen umfassen unter anderem:

a) Informationen über die Vereinbarungen, einschließlich entsprechender Vertragsunterlagen in Kopie, zwischen:

i) dem kritischen IKT-Drittdienstleister und den in Artikel 2 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen,

ii) dem kritischen IKT-Drittdienstleister und seinen Unterauftragnehmern, um die technologische Wertschöpfungskette der IKT-Dienstleistungen, die für Finanzunternehmen in der Union erbracht werden, zu erfassen,

b) Informationen über die Organisations- und Gruppenstruktur des kritischen IKT-Drittdienstleisters, einschließlich Angaben zu allen Unternehmen derselben Gruppe, die direkt oder indirekt IKT-Dienstleistungen für Finanzunternehmen in der Union erbringen,

c) Informationen über die Großaktionäre, einschließlich ihrer Struktur und geografischen Verteilung, die den folgenden Kategorien angehören:

i) Unternehmen, die allein oder gemeinsam mit ihren verbundenen Unternehmen mindestens 25 % des Kapitals oder der Stimmrechte des kritischen IKT-Drittdienstleisters halten,

ii) Unternehmen, die berechtigt sind, die Mehrheit der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsorgans des kritischen IKT-Drittdienstleisters zu bestellen oder abzuberufen,

iii) Unternehmen, die aufgrund einer Vereinbarung die Mehrheit der Stimmrechte der Aktionäre oder Gesellschafter des kritischen IKT-Drittdienstleisters kontrollieren,

d) Informationen über den Marktanteil des kritischen IKT-Drittdienstleisters für jede Art von Diensten auf den relevanten Märkten, auf denen er tätig ist,

e) Informationen über die internen Governance-Regelungen des kritischen IKT-Drittdienstleisters, einschließlich der Organisationsstruktur mit den Zuständigkeits- und Rechenschaftspflichten,

f) die Sitzungsprotokolle des Leitungsorgans des kritischen IKT-Drittdienstleisters und aller anderen relevanten internen Ausschüsse, die in irgendeiner Weise mit Tätigkeiten und Risiken bezüglich IKT-Drittdienstleistungen, die Funktionen von Finanzunternehmen in der Union unterstützen, in Zusammenhang stehen,

g) Informationen über die IKT-Sicherheit des kritischen IKT-Drittdienstleisters, insbesondere über relevante Strategien, Ziele, Leit- und Richtlinien, Verfahren, Protokolle, Prozesse, Kontrollmaßnahmen zum Schutz sensibler Daten, Zugangskontrollen, Verschlüsselungsverfahren und Pläne für Reaktionsmaßnahmen bei Vorfällen sowie Informationen über die Einhaltung aller einschlägigen Vorschriften und gegebenenfalls nationalen und internationalen Standards,

h) Informationen über technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes und der Vertraulichkeit von Daten, sowohl bei personenbezogenen als auch nicht personenbezogenen Daten, umgesetzte Kontrollmaßnahmen zum Schutz sensibler Daten, Zugangskontrollen, Verschlüsselungsverfahren, Plan für Reaktionsmaßnahmen bei Datenschutzverletzungen, wenn die Verarbeitung personenbezogener Daten durch den IKT-Drittdienstleister den Rechtsvorschriften von Drittländern unterliegt, auch bei Zugriffsanfragen von Regierungen aus Drittländern, eine Liste der entsprechenden Länder und der geltenden Rechtsvorschriften,

i) Informationen über die Mechanismen für Datenübertragbarkeit, Übertragbarkeit von Anwendungen und Interoperabilität, die der kritische IKT-Drittdienstleister den Finanzunternehmen der Union anbietet,

j) Informationen über den Standort der Rechenzentren und IKT-Produktionszentren, die für die Erbringung von Dienstleistungen für Finanzunternehmen genutzt werden, einschließlich einer Liste aller relevanten Räumlichkeiten und Einrichtungen des kritischen IKT-Drittdienstleisters, auch außerhalb der Union,

k) Informationen über die Erbringung von Dienstleistungen durch den kritischen IKT-Drittdienstleister aus Drittländern, einschließlich Informationen über einschlägige Rechtsvorschriften, die für die vom IKT-Drittdienstleister verarbeiteten personenbezogenen und nicht personenbezogenen Daten gelten,

l) Informationen über Maßnahmen, die zur Bewältigung von Risiken im Zusammenhang mit der Erbringung von IKT-Dienstleistungen aus Drittländern durch den kritischen IKT-Drittdienstleister und seine Unterauftragnehmer ergriffen wurden,

m) Informationen über den Risikomanagementrahmen und den Rahmen für die Behandlung von Vorfällen, insbesondere über die Leit- und Richtlinien, Verfahren, Instrumente, Mechanismen und Governance-Regelungen des kritischen IKT-Drittdienstleisters und seiner Unterauftragnehmer, einschließlich der Auflistung und Beschreibung schwerwiegender Vorfälle mit direkten oder indirekten Auswirkungen auf Finanzunternehmen in der Union, die relevante Einzelheiten enthält, anhand derer die Bedeutung des Vorfalls für Finanzunternehmen bestimmt und potenzielle grenzüberschreitende Auswirkungen bewertet werden können,

n) Informationen über den Rahmen für das Änderungsmanagement, insbesondere über Leit- und Richtlinien, Verfahren und Kontrollen des kritischen IKT-Drittdienstleisters und seiner Unterauftragnehmer,

o) Informationen über den allgemeinen Reaktions- und Wiederherstellungsrahmen des kritischen IKT-Drittdienstleisters, insbesondere über Geschäftsfortführungspläne und damit zusammenhängende Vereinbarungen und Verfahren, die Lebenszyklusstrategie für die Softwareentwicklung, Reaktions- und Wiederherstellungspläne und damit zusammenhängende Vereinbarungen und Verfahren, sowie Vereinbarungen und Verfahren zum Backup,

p) Informationen über die Leistungsüberwachung, die Sicherheitsüberwachung und die Verfolgung von Sicherheitsvorfällen, über Meldemechanismen in Bezug auf die Leistungsfähigkeit der Dienste und die Sicherheitsvorfälle sowie über die Einhaltung der Dienstgütevereinbarungen und vereinbarter Dienstgüteziele oder vergleichbarer Vereinbarungen zwischen kritischen IKT-Drittdienstleistern und Finanzunternehmen in der Union,

q) Informationen über den Rahmen für das IKT-Drittparteienmanagement des kritischen IKT-Drittdienstleisters, insbesondere über Strategien, Leit- und Richtlinien, Verfahren, Prozesse und Kontrollen, mit detaillierten Angaben zur Sorgfalts- und Risikobewertung aller relevanten IKT- und Gegenparteirisiken, die der kritische IKT-Drittdienstleister gegenüber seinen Unterauftragnehmern vor Abschluss einer Vereinbarung und zur Überwachung der Geschäftsbeziehung durchführt,

r) Auszüge aus den Überwachungs- und Scansystemen des kritischen IKT-Drittdienstleisters und seiner Unterauftragnehmer, die unter anderem die Netzwerk-, Server-, Anwendungs- und Sicherheitsüberwachung, die Schwachstellensuche, die Protokollverwaltung, die Leistungsüberwachung, die Behandlung von Sicherheitsvorfällen sowie Messungen anhand von Zuverlässigkeitszielen, wie etwa den Dienstgütezielen, umfassen,

s) Auszüge aus Produktions-, Vorproduktions- und Testsystemen oder -anwendungen, die vom kritischen IKT-Drittdienstleister und seinen Unterauftragnehmern genutzt werden, um direkt oder indirekt Dienstleistungen für Finanzunternehmen in der Union zu erbringen,

t) Konformitätsberichte und verfügbare Prüfungsberichte sowie alle relevanten Feststellungen aus der Überprüfung, auch im Rahmen von Audits, die von nationalen Behörden in der Union und außerhalb der Union durchgeführt werden, wenn Vereinbarungen über die Zusammenarbeit mit den zuständigen Behörden einen solchen Informationsaustausch vorsehen, oder Zertifizierungen, die der kritische IKT-Drittdienstleister oder seine Unterauftragnehmer erlangt haben, einschließlich Berichten interner und externer Revisoren, Zertifizierungen oder Konformitätsbewertungen nach branchenspezifischen Standards; dies umfasst Informationen über alle Arten verfügbarer unabhängiger Tests zur Prüfung der Resilienz der IKT-Systeme des kritischen IKT-Drittdienstleisters, einschließlich aller Arten bedrohungsorientierter Penetrationstests, die vom IKT-Drittdienstleister durchgeführt werden,

u) Informationen über alle Bewertungen, die vom kritischen IKT-Drittdienstleister oder in seinem Auftrag durchgeführt werden, um die Eignung und Integrität von Personen, die Schlüsselpositionen innerhalb des kritischen IKT-Drittdienstleisters innehaben, zu beurteilen,

v) Informationen über etwaige Pläne mit Abhilfemaßnahmen zur Umsetzung der Empfehlungen gemäß Artikel 3 und einschlägige Informationen, die die Umsetzung der Abhilfemaßnahmen belegen,

w) Informationen über für Mitarbeiter angebotene Schulungen und Programme zur Sensibilisierung für IKT-Sicherheit, gegebenenfalls einschließlich Informationen über Investitionen, Ressourcen und Methoden des kritischen IKT-Drittdienstleisters für die Schulung seines Personals im Hinblick auf den Umgang mit sensiblen Finanzdaten und die Wahrung eines hohen Maßes an Sicherheit,

x) Informationen über die Geschäftstätigkeiten des kritischen IKT-Drittdienstleisters und Abschlüsse, einschließlich Informationen über die für IKT und Sicherheit vorgesehenen Budgetmittel und Ressourcen.

Artikel 3

Informationen, die kritische IKT-Drittdienstleister nach Abgabe der Empfehlungen bereitstellen müssen

(1) Der kritische IKT-Drittdienstleister legt der federführenden Überwachungsbehörde einen Bericht vor, der einen Plan mit Abhilfemaßnahmen in Bezug auf die Empfehlungen und die Abhilfemaßnahmen enthält, die der kritische IKT-Drittdienstleister umzusetzen beabsichtigt, um die in den Empfehlungen nach Artikel 35 Absatz 1 Buchstabe d der Verordnung (EU) 2022/2254 ermittelten Risiken zu mindern. Der Bericht muss mit den Fristen in Einklang stehen, die von der federführenden Überwachungsbehörde in den einzelnen Empfehlungen vorgegeben wurden.

(2) Damit die Umsetzung der Maßnahmen oder Abhilfemaßnahmen, die der kritische IKT-Drittdienstleister im Zusammenhang mit den erhaltenen Empfehlungen ergriffen hat, überwacht werden kann, übermittelt der kritische IKT-Drittdienstleister der federführenden Überwachungsbehörde auf Anfrage folgende Unterlagen:

a) Zwischenberichte über erzielte Fortschritte und entsprechende Nachweise, aus denen hervorgeht, welche Fortschritte bei der Umsetzung der in dem Bericht des kritischen IKT-Drittdienstleisters an die federführende Überwachungsbehörde beschriebenen Schritte und Maßnahmen innerhalb der von dieser vorgegebenen Fristen erzielt wurden,

b) Abschlussberichte und entsprechende Nachweise, aus denen hervorgeht, welche Maßnahmen der kritische IKT-Drittdienstleister ergriffen oder welche Abhilfemaßnahmen er umgesetzt hat, um die in den erhaltenen Empfehlungen ermittelten Risiken zu mindern.

Artikel 4

Struktur und Format der Informationen, die kritische IKT-Drittdienstleister bereitstellen müssen

(1) Der kritische IKT-Drittdienstleister stellt der federführenden Überwachungsbehörde die angeforderten Informationen über die in ihrem Ersuchen verlangten sicheren elektronischen Kanäle und in der von dieser Behörde vorgegebenen Form zur Verfügung.

(2) Bei der Bereitstellung der Informationen an die federführende Überwachungsbehörde müssen die kritischen IKT-Drittdienstleister

a) die von der federführenden Überwachungsbehörde in ihrem Ersuchen vorgegebene Struktur befolgen,

b) die relevanten Informationen in den eingereichten Unterlagen so angeben, dass sie leicht zu finden sind.

(3) Die Informationen, die die kritischen IKT-Drittdienstleister der leitenden Überwachungsbehörde übermitteln, offenlegen oder melden, müssen in einer in der internationalen Finanzwelt gebräuchlichen Sprache abgefasst sein.

Artikel 5

Vorlage für die Bereitstellung von Informationen über Vereinbarungen über die Unterauftragsvergabe

Ein kritischer IKT-Drittdienstleister, der Informationen über Vereinbarungen über die Unterauftragsvergabe übermitteln muss, stellt der federführenden Überwachungsbehörde die Informationen nach Maßgabe der Vorlage im Anhang zur Verfügung.

Artikel 6

Bewertung der in den Empfehlungen der federführenden Überwachungsbehörde dargelegten Risiken durch die zuständigen Behörden

(1) Im Rahmen der Beaufsichtigung von Finanzunternehmen bewertet die zuständige Behörde die Auswirkungen der vom kritischen IKT-Drittdienstleister auf der Grundlage der Empfehlungen der federführenden Überwachungsbehörde ergriffenen Maßnahmen auf die Finanzunternehmen entsprechend dem Grundsatz der Verhältnismäßigkeit.

(2) Bei der Durchführung der in Absatz 1 genannten Bewertung berücksichtigt die zuständige Behörde alle folgenden Elemente:

a) die Angemessenheit und Kohärenz der von den Finanzunternehmen umgesetzten Korrektur- und Abhilfemaßnahmen, um die in den Empfehlungen ermittelten Risiken zu mindern,

b) die von der federführenden Überwachungsbehörde vorgenommene Bewertung über die Einhaltung der im Bericht enthaltenen Maßnahmen und Schritte durch den kritischen IKT-Drittdienstleister, sofern sich dies auf die Exposition der in ihren Zuständigkeitsbereich fallenden Finanzunternehmen gegenüber den in den Empfehlungen ermittelten Risiken auswirkt,

c) die Stellungnahmen aller anderen zuständigen Behörden, die gemäß Artikel 42 Absatz 5 der Verordnung (EU) 2022/2554 konsultiert wurden,

d) ob die federführende Überwachungsbehörde die vom kritischen IKT-Drittdienstleister umgesetzten Maßnahmen und Abhilfemaßnahmen als angemessen erachtet hat, um die Exposition der in ihren Zuständigkeitsbereich fallenden Finanzunternehmen gegenüber den in den Empfehlungen ermittelten Risiken zu mindern.

(3) Auf Anfrage der federführenden Überwachungsbehörde legt die zuständige Behörde die Ergebnisse der Bewertung nach Absatz 1 innerhalb einer angemessenen Frist vor. Bei der Anforderung der Ergebnisse dieser Bewertung berücksichtigt die federführende Überwachungsbehörde den Grundsatz der Verhältnismäßigkeit und das Ausmaß der in den Empfehlungen dargelegten Risiken, einschließlich der grenzüberschreitenden Auswirkungen dieser Risiken, wenn sie sich auf Finanzunternehmen auswirken, die in mehr als einem Mitgliedstaat tätig sind.

(4) Die zuständige Behörde fordert gegebenenfalls die Finanzunternehmen auf, alle Informationen bereitzustellen, die für die Durchführung der in Absatz 1 genannten Bewertung erforderlich sind.

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. Oktober 2024

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG

VORLAGE FÜR DIE ÜBERMITTLUNG VON INFORMATIONEN ÜBER VEREINBARUNGEN ÜBER DIE UNTERAUFTRAGSVERGABE

Informationskategorie	Wesentliche Informationen
Allgemeine Angaben	— Name des kritischen IKT-Drittdienstleisters. — Rechtsträgerkennung des kritischen IKT-Drittdienstleisters. — Name der Kontaktperson und Kontaktdaten des kritischen IKT-Drittdienstleisters. — Datum der Übermittlung der Vorlage.
Überblick über die Vereinbarungen über die Unterauftragsvergabe	— Erfassung der Vereinbarungen über die Unterauftragsvergabe, einschließlich einer kurzen Beschreibung des Zwecks und des Umfangs des Vertragsverhältnisses mit Unterauftragnehmern (einschließlich Angaben zum Grad der Kritikalität oder zur Bedeutung der Vereinbarungen über die Unterauftragsvergabe für den kritischen IKT-Drittdienstleister). — Spezifikation und Beschreibung der Arten von IKT-Dienstleistungen, die an Unterauftragnehmer vergeben werden, und ihrer Bedeutung für die IKT-Dienstleistungen, die für Finanzunternehmen erbracht werden, nach Maßgabe der gemäß Artikel 28 Absatz 9 der Verordnung (EU) 2022/2554 erlassenen technischen Durchführungsstandards. — Bitte bei der Spezifizierung der Arten von IKT-Dienstleistungen die Liste in Anhang IV der gemäß Artikel 28 Absatz 9 der Verordnung (EU) 2022/2554 erlassenen technischen Durchführungsstandards verwenden.
Angaben zu Unterauftragnehmern	— Name und Angaben zur juristischen Person (einschließlich Rechtsträgerkennung) für jeden einzelnen Unterauftragnehmer. — Kontaktdaten der Mitarbeiter, die in der Verwaltungsstruktur des kritischen IKT-Drittdienstleisters für die einzelnen Unteraufträge zuständig sind. — Überblick für jeden einzelnen Unterauftragnehmer über die Fachkenntnisse, die Erfahrung und die Qualifikationen im Zusammenhang mit den in Auftrag gegebenen IKT-Dienstleistungen.
Beschreibung der von Unterauftragnehmern erbrachten Dienstleistungen	— Detaillierte Beschreibung der einzelnen IKT-Dienstleistungen, die von den einzelnen Unterauftragnehmern erbracht werden. — Aufschlüsselung der Zuständigkeiten und Aufgaben, die Unterauftragnehmern übertragen werden, durch Angabe der verschiedenen Aufgaben in den verschiedenen Phasen der IKT-Prozesse. — Informationen über den Umfang des Zugangs von Unterauftragnehmern zu personenbezogenen oder anderweitig sensiblen Daten oder Systemen bei der Erbringung von IKT-Dienstleistungen für Finanzunternehmen. — Informationen über die Standorte, von denen aus die Unterauftragnehmer ihre Dienstleistungen erbringen, und über die Maßnahmen, die zur Bewältigung von Risiken, die mit außerhalb der Union erbrachten Dienstleistungen einhergehen, ergriffen wurden.
Governance und Überwachung der Unterauftragsvergabe	— Beschreibung des bestehenden Vertrags- und Governance-Rahmens für die Verwaltung von Unteraufträgen, einschließlich Klauseln für die Einschränkung der Nutzung sensibler Daten. — Erläuterung der Verfahren für die Auswahl, Beauftragung und Überwachung von Unterauftragnehmern. — Überblick über Leistungsparameter, Dienstgüteziele und -vereinbarungen sowie zentrale Leistungsindikatoren, die zur Bewertung der Leistung und zur Überwachung der Zuverlässigkeit des Unterauftragnehmers herangezogen werden.
Risikomanagement und Einhaltung der Vorschriften	— Bewertung der Risikoprofile des Unterauftragnehmers und der potenziellen Auswirkungen auf die IKT-Dienstleistungen, die für Finanzunternehmen erbracht werden. — Erläuterung der Risikominderungsmaßnahmen, die zur Bewältigung von Risiken im Zusammenhang mit der Unterauftragsvergabe umgesetzt wurden. — Detaillierte Angaben zur Einhaltung der einschlägigen Vorschriften, einschließlich der Datenschutz- und Branchenstandards, durch den Unterauftragnehmer.

Informationskategorie	Wesentliche Informationen
Geschäftsfortführung und Notfallplanung	— Überblick über die Geschäftsfortführungspläne und die Reaktions- und Wiederherstellungspläne des Unterauftragnehmers. — Beschreibung der getroffenen Vorkehrungen, um die Aufrechterhaltung der Dienste im Falle von Störungen oder der Kündigung des Unterauftragnehmers zu gewährleisten. — Häufigkeit der von den Unterauftragnehmern durchgeführten Tests der Geschäftsfortführungspläne und der Reaktions- und Wiederherstellungspläne, Datum der letzten Tests in den letzten drei Jahren und Angaben dazu, ob der kritische IKT-Drittdienstleister an diesen Tests beteiligt war.
Berichterstattung	— Beschreibung der Meldesysteme und der Häufigkeit der Berichterstattung zwischen dem kritischen IKT-Drittdienstleister und seinen Unterauftragnehmern.
Abhilfemaßnahmen und Behandlung von Vorfällen	— Überblick über die Verfahren für die Behandlung von Sicherheitsvorfällen und -verletzungen oder Verstößen in Verbindung mit dem Unterauftragnehmer.
Zertifizierungen und Audits	— Informationen über Zertifizierungen, unabhängige Audits oder Bewertungen, die bei Unterauftragnehmern durchgeführt wurden, um ihre Sicherheitskontrollen, Qualitätsstandards oder Einhaltung der Rechtsvorschriften zu validieren. — Datum und Häufigkeit der vom kritischen IKT-Drittdienstleister vorgenommenen Audits der Unterauftragnehmer.