EU-Verordnung

DIGITALE BETRIEBSSTABILITÄT VON FINANZUNTERNEHMEN

cep**Analyse** 11/2021

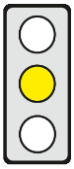
Centrum für Europäische Politik
FREIBURG | BERLIN

KERNPUNKTE

Hintergrund: Die Abhängigkeit der Finanzunternehmen von IKT-Produkten und Dienstleistungen, auch von Dritten, hat zugenommen und schafft neue Risiken für das Finanzsystem. Die Verordnung befasst sich mit diesen Risiken.

Ziel der Verordnung: Die Kommission möchte die digitale Betriebsstabilität von Finanzunternehmen erhöhen.

Betroffene: Finanzunternehmen, IKT-Drittanbieter.



Pro: (1) EU-Maßnahmen zur Stärkung der digitalen Betriebsstabilität von Finanzunternehmen sind sachgerecht, da die von Finanzunternehmen bereitgestellten Produkte und Dienstleistungen oft zentral für das Funktionieren einer Gesellschaft sind.

(2) Meldungen über Cybervorfälle erzeugen einen erheblichen externen Nutzen. Die Meldepflicht ist daher angemessen.

(3) Die Schaffung eines EU-Aufsichtsrahmens für kritische IKT-Drittanbieter kann die digitale Betriebsstabilität von Finanzunternehmen stärken.

Kontra: (1) Dem Verordnungsvorschlag mangelt es an Verhältnismäßigkeit und Zielgerichtetheit.

(2) Die Aufteilung der Aufsichtsaufgaben zwischen EBA, ESMA und EIOPA wirft Bedenken auf. Kritische IKT-Drittanbieter könnten mit widersprüchlichen Aufsichtsansätzen konfrontiert werden.

Die wichtigsten Textstellen sind durch eine Linie am Rand gekennzeichnet.

INHALT

Titel

Vorschlag COM(2020) 595 vom 24. September 2020 für eine **Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors**

Kurzdarstellung

- **Hintergrund und Ziele**
  - Laut dem Europäischen Ausschuss für Systemrisiken (ESRB) können der hohe Grad der Vernetzung von Finanzunternehmen und die gegenseitigen Abhängigkeiten ihrer IKT-Systeme eine „Systemanfälligkeit herbeiführen“. Cybervorfälle können sich schnell von einem Finanzunternehmen auf das gesamte Finanzsystem ausbreiten. [Erwägungsgrund 3]
  - Bestehendes EU-Recht konzentriert sich jedoch hauptsächlich auf die zentralen finanziellen Risiken wie das Kredit-, Markt- oder Liquiditätsrisiko und geht nicht angemessen auf IKT-Risiken ein [Erwägungsgrund 12].
  - Die Verordnung soll daher die bestehenden EU-Vorschriften über IKT-Risiken für Finanzunternehmen konsolidieren und aktualisieren, um ein "hohes gemeinsames Niveau digitaler Betriebsstabilität" zu erreichen [Art. 1, Erwägungsgrund 12].
  - Um dies zu erreichen, sieht die Verordnung insbesondere vor [Erwägungsgrund 12, Art. 1]:
    - Anforderungen an Finanzunternehmen, u.a. zum Management von IKT-Risiken [Art. 4–14] und zur Meldung schwerwiegender IKT-bezogener Vorfälle an Finanzaufsichtsbehörden [Art. 15–21],
    - Anforderungen an Verträge zwischen Finanzunternehmen und IKT-Drittanbietern [Art. 25-27],
    - einen Aufsichtsrahmen für IKT-Drittanbieter, die Dienste für Finanzunternehmen erbringen [Art. 28–39].
- **Geltungsbereich**
  - Die Verordnung gilt für [Art. 2, Art. 3 Abs. 1 Ziff. 15]
    - Banken, Handelsplätze, Investmentfonds, Versicherungen und andere, in Art. 2 genannte Finanzunternehmen,
    - IKT-Drittanbieter, d. h. Unternehmen, die "digitale und Datendienste" wie Cloud Computingdienste anbieten.
  - Finanzunternehmen mit weniger als 10 Mitarbeitern und 2 Mio. € Umsatz und/oder Bilanzsumme ("Kleinstunternehmen") sind von einigen der Vorgaben zum IKT-Risikomanagement befreit [Erwägungsgrund 34, Art. 4–13].
- **Management von IKT-Risiken**
  - Finanzunternehmen müssen über Governance- und Kontrollrahmen verfügen, die geeignet sind, IKT-Risiken in einer "wirksamen und umsichtigen" Weise zu steuern [Art. 4 Abs. 1].

Autoren: Dr. Martina Anzini und Philipp Eckhardt eckhardt@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Deutschland | Telefon + 49 761 38693-0 | www.cep.eu

– Finanzunternehmen müssen über einen "soliden, umfassenden und gut dokumentierten" IKT-Risikomanagementrahmen verfügen [Art. 5 Abs. 1]. Ihre Leitungsorgane müssen den Rahmen definieren, genehmigen, überwachen und sind für dessen Umsetzung rechenschaftspflichtig. Dies umfasst die Festlegung [Art. 4 Abs. 2]
  - klarer Zuständigkeiten für IKT-bezogene Funktionen innerhalb des Unternehmens, und
  - die Toleranzschwelle für das IKT-Risiko, das das Unternehmen in Einklang mit seiner Risikobereitschaft als angemessen akzeptiert.
– Der IKT-Risikomanagementrahmen muss alle relevanten physischen Komponenten und Infrastrukturen – z. B. Hardware – sowie alle relevanten Räumlichkeiten und Rechenzentren vor Risiken schützen [Art. 5 Abs. 2]. Er muss einmal jährlich, bei Auftreten schwerwiegender IKT-bezogener Vorfälle, und bei aufsichtsrechtlichen Anweisungen überprüft werden [Art. 5 Abs. 6]. Er umfasst bei Nutzung mehrerer IKT-Anbieter eine Strategie, die Abhängigkeiten von IKT-Drittanbietern aufzeigt und begründet [Art. 5 Abs. 9 lit. g].
– Das IKT-Risikomanagement muss u. a. umfassen
  - die Nutzung und Pflege von aktuellen IKT-Systemen, -Protokollen und -Werkzeugen [Art. 6 Abs. 1];
  - die Identifizierung von IKT-bezogenen Unternehmensfunktionen und Quellen von IKT-Risiken [Art. 7],
  - den Schutz und die Prävention vor IKT-Risiken, einschließlich der Einführung von Strategien und Verfahren, die die "Resilienz, Kontinuität und Verfügbarkeit von IKT-Systemen" und "hohe Standards in Bezug auf Sicherheit, Vertraulichkeit und Integrität von Daten" gewährleisten [Art. 8],
  - die Festlegung einer "IKT-Strategie zur Fortführung des Geschäftsbetriebs", um eine rasche und angemessene Reaktion auf alle IKT-bezogenen Vorfälle zu ermöglichen [Art. 10], und
  - die Festlegung von Kommunikationsplänen, um Kunden, Finanzunternehmen und ggfs. die Öffentlichkeit auf verantwortungsvolle Weise über IKT-bezogene Vorfälle und Anfälligkeiten zu informieren [Art. 13].

► **Meldung von IKT-bezogenen Vorfällen**
– Finanzunternehmen müssen über Verfahren verfügen, um IKT-bezogene Vorfälle zu erkennen, zu bewältigen und zu melden [Art. 15 Abs. 1]. Diese müssen die Verfolgung und Klassifizierung der Vorfälle sowie die Aufteilung der Verantwortlichkeiten für die Ergreifung von Maßnahmen in diesen Situationen umfassen [Art. 15 Abs. 3].
– Finanzunternehmen müssen "schwerwiegende" IKT-bezogene Vorfälle melden an [Art. 17 Abs. 1 und 2]
  - ihre zuständige Finanzaufsichtsbehörde durch die Einreichung eines Vorfallberichts, der alle relevanten Informationen enthalten muss, um die Signifikanz und mögliche grenzüberschreitende Auswirkungen des Vorfalls zu bewerten, und
  - ihre Dienstnutzer und Kunden, wenn die Vorfälle Auswirkungen auf deren finanziellen Interessen haben.
– Die Europäischen Finanzaufsichtsbehörden (ESAs) erarbeiten Entwürfe für technische Regulierungsstandards (RTS), in denen sie Schwellenwerte für die Bestimmung „schwerwiegender“ Vorfälle, sowie den Inhalt und die Form der Berichte festlegen [Erwägungsgrund 22; Art. 16 Abs. 2 und Art. 18].

► **Risiken durch IKT-Drittanbieter**
Verträge von Finanzunternehmen mit IKT-Drittanbietern
– Finanzunternehmen, die IKT-Dienstleistungen von IKT-Drittanbietern nutzen, bleiben für die Einhaltung der Verordnung verantwortlich [Art. 25 Abs. 1].
– Im Rahmen ihres IKT-Risikomanagements müssen Finanzunternehmen dem Risiko durch IKT-Drittanbieter unter Beachtung des Verhältnismäßigkeitsprinzips Rechnung tragen und dabei die Relevanz von IKT-bezogenen Abhängigkeiten und das Risiko, das sich aus Verträgen mit IKT-Drittanbieter für die Tätigkeiten und Dienstleistungen des Finanzunternehmens ergibt, berücksichtigen [Art. 25 Abs. 2].
– Finanzunternehmen müssen u. a.,
  - vor Vertragsschluss mit einem IKT-Drittanbieter prüfen, ob dieser eine kritische oder wichtige Funktion abdeckt und ob der Vertrag die IKT-Konzentrationsrisiken erhöhen könnte, z. B. durch Prüfung, ob der Anbieter ersetzbar ist oder mit demselben Anbieter mehrere Verträge abgeschlossen wurden [Art. 25 Abs. 5, Art. 26],
  - sicherstellen, dass Verträge über die Nutzung von IKT-Diensten, z. B. bei Verstößen des IKT-Drittanbieters gegen geltende Gesetze, Verordnungen oder Vertragsbedingungen, gekündigt werden [Art. 25 Abs. 8],
  - Ausstiegsstrategien einrichten, um mit Ausfällen oder einer nicht sachgemäßen Erbringung von Dienstleistungen durch den IKT-Drittanbieter umgehen zu können; diese Strategie muss sicherstellen, dass eine Vertragskündigung die Einhaltung regulatorischer Anforderungen oder die Kontinuität und Qualität der von den Finanzunternehmen für ihre Kunden angebotenen Dienstleistungen nicht beeinträchtigt [Art. 25 Abs. 9].
– Verträge zwischen Finanzunternehmen und IKT-Drittanbietern müssen die Rechte und Pflichten jeder Partei klar zuweisen. Sie müssen enthalten [Art. 27 Abs. 1 und 2]
  - eine Beschreibung der vom IKT-Drittanbieter zu erbringenden Dienstleistungen, einschließlich der Angabe, ob die Vergabe von Unteraufträgen zulässig ist,
  - Verweise auf die Orte, an denen Dienste erbracht und Daten verarbeitet und gespeichert werden,
  - das Recht des Finanzunternehmens, die Leistung des IKT-Drittanbieters zu überwachen.

EU-Aufsicht über kritische IKT-Drittanbieter
– Mit der Verordnung wird ein EU-Aufsichtsrahmen für "kritische" IKT-Drittanbieter geschaffen. [Art. 28 Abs. 1].
– Ihre Kritikalität hängt von mehreren Kriterien ab, darunter [Art. 28 Abs. 2]

- die systemischen Auswirkungen einer potenziellen umfassenden Betriebsstörung des betreffenden IKT-Drittanbieters auf die Stabilität, Kontinuität oder Qualität der Erbringung von Finanzdienstleistungen,
- die systemische Relevanz der Finanzunternehmen, die die Dienste des betreffenden IKT-Drittanbieters nutzen,
- der Grad der Substituierbarkeit des IKT-Drittanbieters.

Die Kommission kann weitere Kriterien durch delegierte Rechtsakte hinzufügen [Art. 28 Abs. 3].

– Der Gemeinsame Ausschuss der ESAs benennt die kritischen IKT-Drittanbieter [Art. 28 Abs. 1].
– Der Gemeinsame Ausschuss legt zudem für jeden kritischen Anbieter entweder die Europäische Bankaufsichtsbehörde (EBA), die Europäische Wertpapieraufsichtsbehörde (ESMA) oder die Europäische Versicherungsaufsichtsbehörde (EIOPA) als federführende Aufsichtsinstanz. Diejenige ESA, die vom Gemeinsamen Ausschuss zu benennen ist, ist diejenige, die die am meisten vertretenen Finanzunternehmen im Kundenportfolio eines kritischen IKT-Drittanbieters. [Art. 28 Abs. 1]
– Die federführende Aufsichtsinstanz muss beurteilen, ob kritische IKT-Drittanbieter die IKT-Risiken angemessen steuern, die sie für Finanzunternehmen darstellen. Sie nimmt für jeden Anbieter jährlich einen detaillierten Aufsichtsplan an. Nach Verabschiedung solcher Pläne dürfen zuständige Finanzaufsichtsbehörden nur in Einvernehmen mit der federführenden Aufsichtsinstanz Maßnahmen gegenüber IKT-Drittanbietern ergreifen. [Art. 30]
– Die federführende Aufsichtsinstanz kann an kritische IKT-Drittanbieter Empfehlungen zur Anwendung bestimmter IKT-Sicherheitsanforderungen oder zum Verzicht auf den Abschluss bestimmter Unterverträge richten. Die Anbieter müssen der federführenden Aufsichtsinstanz binnen 30 Tagen mitteilen, ob sie beabsichtigen, einer Empfehlung zu folgen. [Art. 37 Abs. 1]
– Die zuständigen Finanzaufsichtsbehörden können Finanzunternehmen zwingen, ihre Verträge mit IKT-Drittanbietern auszusetzen, bis diese die in den Empfehlungen genannten Risiken beseitigen. Erforderlichenfalls können sie von den Finanzunternehmen auch verlangen, ihre Verträge zu kündigen. [Art. 37 Abs. 3]
– Finanzunternehmen dürfen keine IKT-Drittanbieter mit Sitz außerhalb der EU nutzen, wenn diese Anbieter als kritisch eingestuft würden, wenn sie in der EU niedergelassen wären [Art. 28 Abs. 9].

Subsidiaritätsbegründung der Kommission

EU-Maßnahmen sind notwendig, um zu vermeiden, dass für Finanzunternehmen unterschiedliche Anforderungen an die digitale Betriebsstabilität gelten, wenn sie grenzüberschreitend tätig sind. Ferner ist ein EU-Aufsichtsrahmen für IKT-Drittanbieter geboten, um den Risiken, die sie für die Solidität des EU-Finanzsektors darstellen, entgegenzuwirken.

Politischer Kontext

Mit dem Vorschlag soll ein sektorspezifisches Regelwerk zur Ergänzung der sektorübergreifenden Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der Union [COM(2020) 823] zu schaffen.

Politische Einflussmöglichkeiten

Generaldirektion:	GD Finanzstabilität, Finanzdienstleistungen und Kapitalmarktunion
Ausschuss des Europäischen Parlaments:	Wirtschaft und Währung (federführend), Berichterstatter: Billy Kelleher (Renew Europe, Irland)
Bundesministerium:	Finanzen (federführend)
Ausschuss des Deutschen Bundestages:	Finanzen (federführend)

BEWERTUNG

Ökonomische Folgenabschätzung

Finanzunternehmen haben ein Eigeninteresse daran, ihre digitale Betriebsstabilität zu schützen, da ein Versagen in diesem Bereich zu erheblichen Umsatzeinbußen und Reputationsschäden führen kann. **EU-Maßnahmen zur Stärkung der digitalen Betriebsstabilität von Finanzunternehmen sind** dennoch **sachgerecht, da die von Finanzunternehmen bereitgestellten Produkte und Dienstleistungen** oft **zentral für das Funktionieren einer Gesellschaft sind** und die Kosten für die Gesellschaft durch auf Finanzunternehmen abzielende Cyberangriffe besonders hoch sind. Da Finanzunternehmen zudem oft stark miteinander vernetzt sind, können größere Cybervorfälle bei einem Finanzunternehmen Systemrisiken für den Finanzsektor hervorrufen und die Finanzstabilität gefährden.

Dem Verordnungsvorschlag mangelt es jedoch in mehrfacher Hinsicht **an Verhältnismäßigkeit und Zielgerichtetheit**. Erstens ist zu bezweifeln, dass nur Finanzunternehmen, die als Kleinstunternehmen eingestuft werden, als unkritisch für die Gesellschaft angesehen werden können. Hier ist ein höherer Schwellenwert geboten, um einen unnötigen Verwaltungsaufwand zu vermeiden. Zweitens sollte sich das IKT-Risikomanagement von Finanzunternehmen auf kritische Elemente konzentrieren, und nicht alle physischen Komponenten, Infrastrukturen, Räumlichkeiten und Rechenzentren abdecken, unabhängig von deren Bedeutung für das operationelle Risiko der Unternehmen. Und drittens beziehen sich die Anforderungen an Verträge zwischen Finanzunternehmen und IKT-Drittanbietern auf jeden Vertrag, unabhängig von der Kritikalität der eingekauften IKT-Dienstleistung. Fazit: Betroffene Parteien müssen einen zu hohen Aufwand für die Umsetzung von Maßnahmen betreiben, die ihre digitale Betriebsstabilität nicht wesentlich erhöhen.

Finanzunternehmen haben angesichts von Meldekosten und potenziellen Reputationsschäden wenig Anreize, Cybervorfälle zu melden. Gleichzeitig helfen **Meldungen über Cybervorfälle** anderen dabei, Sicherheitslücken zu erkennen und zu schließen. Sie **erzeugen** also **einen erheblichen externen Nutzen. Die Meldepflicht** für Finanzunternehmen **ist daher angemessen.** Die Meldepflichten sollten jedoch mit vergleichbaren Anforderungen anderer EU-Gesetze, z.B. der Datenschutzgrundverordnung [DSGVO, 2016/679] oder der vorgeschlagenen NIS-2-Richtlinie [COM(2020) 823], übereinstimmen, um übermäßige Meldungen zu vermeiden, die unnötig Ressourcen zur Bekämpfung von Vorfällen binden.
Finanzunternehmen nutzen zunehmend IKT-Drittanbieter, z. B. für Cloud-Computing-Lösungen. Dies bietet ihnen zwar Zugang zu Innovationen und kann ihre Kosteneffizienz steigern, kann aber auch Governance-, Lock-in- und operationelle Risiken erhöhen. Derzeit fallen die von IKT-Drittanbietern für Finanzunternehmen erbrachten Dienstleistungen jedoch häufig nicht (vollständig) in den Zuständigkeitsbereich der Finanzaufsichtsbehörden. **Die Schaffung eines EU-Aufsichtsrahmens für kritische IKT-Drittanbieter**, der solche neuen Risiken berücksichtigt, **kann** daher **die digitale Betriebsstabilität von Finanzunternehmen stärken**.
Die Aufteilung der Aufsichtsaufgaben zwischen EBA, ESMA und EIOPA, d.h. drei Aufsichtsinstanzen, **wirft** einige **Bedenken auf. Kritische IKT-Drittanbieter könnten mit** unterschiedlichen und **widersprüchlichen Aufsichtsansätzen konfrontiert werden**, z. B. wenn ihre federführende Aufsichtsinstanz wechselt. Zweitens könnte es einer ESA an Expertise mangeln, einen IKT-Drittanbieter angemessen zu beaufsichtigen, der Dienstleistungen für ein Finanzunternehmen erbringt, das nicht in den üblichen Aufsichtsbereich dieser ESA fällt. Dies könnte durch die Einrichtung eines gemeinsamen Gremiums der drei ESAs verhindert werden. Damit könnte Fachwissen konzentriert, die Aufsichtsmaßnahmen gestrafft und eine einzige Anlaufstelle für Finanzunternehmen und kritische IKT-Drittanbieter geschaffen werden.
Die vorgesehene Aufsichtsstruktur ist ferner nicht zielgerichtet genug. Die Aufsicht über kritische IKT-Drittanbieter durch die ESAs sollte sich erstens nur die Dienstleistungen konzentrieren, die die Drittanbietervon gegenüber Finanzunternehmen erbringen und zweitens nur auf Dienstleistungen, die als kritisch für Finanzunternehmen gelten. Andernfalls werden bei den Aufsichtsbehörden und den beaufsichtigten Anbietern zu viele Ressourcen gebunden, ohne dass die digitale Betriebsstabilität von Finanzunternehmen gestärkt wird.
Das Instrumentarium der ESAs sollte sich nicht auf Empfehlungen beschränken, sondern auch direkte Durchsetzungsbefugnisse gegenüber Finanzunternehmen und kritischen IKT-Drittanbieter umfassen. Ohne diese Befugnisse wären Finanzunternehmen und IKT-Drittanbieter regelmäßig mit unterschiedlichen Abhilfemaßnahmen der nationalen Aufsichtsbehörden konfrontiert, selbst wenn die drei ESAs ähnliche Empfehlungen aussprechen. Dies würde Ineffizienzen und Inkohärenzen erzeugen und den Wettbewerb unter Finanzunternehmen und IKT-Drittanbietern verzerren.
Die Pflicht für Finanzunternehmen, Verträge mit einem IKT-Drittanbieter zu kündigen, wenn letzterer gegen geltende Gesetze, Verordnungen oder Vertragsbedingungen verstößt oder wenn es von einer Finanzaufsichtsbehörde dazu gezwungen wird, dürfte die operationellen Risiken eher erhöhen als mindern, etwa wenn kein geeigneter alternativer Anbieter rasch zur Verfügung steht. Anstelle eines Zwangs zur Vertragskündigung sollte die Verordnung in einem ersten Schritt eine enge Abstimmung zwischen den betroffenen Akteuren fordern und dann zumindest Übergangsfristen vorsehen. Eine strikte Vertragskündigungspflicht sollte nur das letzte Mittel sein.
Die Beschränkungen für die Nutzung kritischer IKT-Drittanbieter von außerhalb der EU sind ein starker Eingriff in die Vertragsfreiheit. Sie könnten Finanzunternehmen dazu zwingen, Verträge mit Anbietern abzuschließen, die weniger cybersichere IKT-Produkte und -Dienstleistungen anbieten, und damit die operationellen Risiken erhöhen, aber auch die Auswahl und den Zugang zu innovativen IKT-Lösungen einschränken. Die Ziele der Kommission, Konzentrationsrisiken zu begegnen, insbesondere die Abhängigkeit des Finanzsektors von US-amerikanischen Cloud-Anbietern, und die Fähigkeit der EU sicherzustellen, IKT-Drittanbietern aus Drittländern zu beaufsichtigen, sollten mit anderen Mitteln erreicht werden. Statt die Nutzung kritischer IKT-Drittanbieter aus Drittländern zu verbieten, würde es ausreichen, die Anbieter zu zwingen, rechtliche Einheiten in der EU zu gründen, um Risiken im Zusammenhang mit einem potenziellen Mangel an angemessener Aufsicht zu begegnen.

Juristische Bewertung

Kompetenz

Die Verordnung wird zu Recht auf die Binnenmarktkompetenz (Art. 114 AEUV) gestützt.

Subsidiarität und Verhältnismäßigkeit gegenüber den Mitgliedsstaaten

Unproblematisch.

Zusammenfassung der Bewertung

EU-Maßnahmen zur Stärkung der digitalen Betriebsstabilität von Finanzunternehmen sindsachgerecht, da die von Finanzunternehmen bereitgestellten Produkte und Dienstleistungen oft zentral für das Funktionieren einer Gesellschaft sind. Dem Verordnungsvorschlag mangelt es an Verhältnismäßigkeit und Zielgerichtetheit. Meldungen über Cybervorfälle erzeugen einen erheblichen externen Nutzen. Die Meldepflicht ist daher angemessen. Die Schaffung eines EU-Aufsichtsrahmens für kritische IKT-Drittanbieter kann die digitale Betriebsstabilität von Finanzunternehmen stärken. Die Aufteilung der Aufsichtsaufgaben zwischen EBA, ESMA und EIOPA wirft Bedenken auf. Kritische IKT-Drittanbieter könnten mit widersprüchlichen Aufsichtsansätzen konfrontiert werden.