Europäischer Wirtschafts- und Sozialausschuss

ECO/536
Betriebsstabilität digitaler Systeme

Stellungnahme

Europäischer Wirtschafts- und Sozialausschuss

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014
[COM(2020) 595 final – 2020/0266 (COD)]

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinien 2006/43/EG, 2009/65/EG, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 und EU/2016/2341
[COM(2020) 596 final – 2020/0268 (COD)]

Berichterstatter: **Antonio GARCÍA DEL RIEGO**

Befassung	Europäisches Parlament, 17/12/2020 Rat der Europäischen Union, 22/12/2020
Rechtsgrundlage	Artikel 53 Absatz 1, Artikel 114 Absatz 1 und Artikel 304 des Vertrags über die Arbeitsweise der Europäischen Union
Zuständige Fachgruppe	Fachgruppe Wirtschafts- und Währungsunion, wirtschaftlicher und sozialer Zusammenhalt
Annahme in der Fachgruppe	12/02/2021
Verabschiedung auf der Plenartagung	24/02/2021
Plenartagung Nr.	558
Ergebnis der Abstimmung (Ja-Stimmen/Nein-Stimmen/Enthaltungen)	243/1/4

1. **Schlussfolgerungen und Empfehlungen**

1.1 Der Europäische Wirtschafts- und Sozialausschuss (EWSA) begrüßt den von der Europäischen Kommission vorgelegten Vorschlag für eine Verordnung über die Betriebsstabilität digitaler Systeme (Digital Operational Resilience Act – DORA). Dieser zielt darauf ab, Rechtsklarheit in Bezug auf die Bestimmungen über Risiken im Zusammenhang mit Informations- und Kommunikationstechnologien (IKT) zu schaffen, die regulatorische Komplexität zu verringern, eine Reihe gemeinsamer Standards zur Entschärfung von IKT-Risiken festzulegen und ein harmonisiertes Aufsichtskonzept zu ermöglichen. Gleichzeitig soll für Rechtssicherheit und die notwendigen Schutzmaßnahmen für Finanzunternehmen und IKT-Dienstleister gesorgt werden. Die DORA-Verordnung erhöht nicht nur die Widerstandsfähigkeit des Sektors gegenüber IKT-Risiken, sondern ist auch für eine Reihe von Akteuren wie Kunden, Anleger und Mitarbeiter von Interesse und trägt zur Umsetzung einer nachhaltigen Entwicklung bei.

1.2 Der EWSA empfiehlt, die Wirksamkeit des DORA-Verordnungsvorschlags durch folgende Schritte zu erhöhen:

1.2.1 Einbeziehung aller Anbieter von kritischen Finanzdienstleistungen, die Finanztätigkeiten erbringen, in den Geltungsbereich des DORA-Vorschlags, und Ausnahme von IKT-Dienstleistungen für nicht kritische Funktionen.

1.2.2 Sicherstellung der Kohärenz in Definition und Geltungsbereich zwischen dem DORA-Vorschlag und den Anforderungen in den bestehenden Leitlinien der europäischen Finanzaufsichtsbehörden.

1.2.3 Begünstigung eines Rahmens für einen grundsatz- und risikobasierten Ansatz im IKT-Management, der die Durchführung von Kontrollen erleichtert, die zukunftssicher, flexibel und den Risiken angemessen sind.

1.2.4 Vollständige Angleichung bei IKT-bezogenen Vorfällen an das Instrumentarium des Finanzstabilitätsrats für Gegenmaßnahmen und Wiederherstellung bei Cybervorfällen (Cyber Incident Response and Recovery toolkit).

1.2.5 Berücksichtigung nicht nur der Größe des Finanzinstituts, sondern auch der Komplexität und der kritischen Eigenschaften der Dienstleistungen beim Testen der Betriebsstabilität digitaler Systeme; Vermeidung der obligatorischen Auslagerungen von Tests, die von einer begrenzten Anzahl externer Prüfer durchgeführt werden, und gegenseitige Anerkennung der Testergebnisse.

1.2.6 Konsolidierung der für Auslagerungen geltenden Anforderungen in einem einzigen Regelwerk, um Rechtssicherheit für alle Marktteilnehmer durchzusetzen und die Erwartungen in puncto Aufsicht zuverlässig zu erfüllen.

1.2.7 Vollständige Durchsetzung der Empfehlungen der federführenden Aufsichtsbehörden und eine klare Festlegung der Rollen und Verantwortlichkeiten der verschiedenen an der Aufsicht über kritische IKT-Drittanbieter beteiligten Behörden.

1.2.8 Sicherstellung des Zugangs zu ausgelagerten Dienstleistungen, die für in Drittländern ansässige IKT-Drittanbieter als kritisch erachtet werden, um die Vertragsfreiheit der Unternehmen und die Fähigkeit, auf die Dienstleistungen von Anbietern besonderer Mehrwertdienste zuzugreifen, nicht einzuschränken.

1.2.9 Aufnahme der Verhältnismäßigkeit in die Sanktionsregelung, um negative Anreize zu vermeiden, aufgrund derer IKT-Anbieter vor der Diensteerbringung für EU-Finanzunternehmen zurückschrecken, und Abkehr von der derzeitigen Bezugnahme auf den weltweiten Umsatz.

1.2.10 Klärung der Fähigkeit von Firmen, Informationen über Cyber-Bedrohungen auszutauschen. Damit soll sichergestellt werden, dass solche Vereinbarungen auf freiwilliger Basis getroffen werden und dass eine ausdrückliche Bestimmung, die den Austausch von personenbezogenen Daten erlaubt, in den DORA-Vorschlag aufgenommen wird.

1.2.11 Die Anhebung der Schwellenwerte für die Ausnahme von Kleinst- und Kleinunternehmen gemäß Definition der Empfehlung der Kommission 2003/361/EG Anhang 1, Artikel 2 Absatz 2 (Unternehmen, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt) sowie die Verringerung der Zahl der Anforderungen für KMU im Verhältnis zum jeweiligen digitalen Risikoprofil könnten erwogen werden.

1.3 Der EWSA begrüßt, dass die federführenden Aufsichtsbehörden zur Durchführung der Prüfungs- und Kontrollverfahren für die kritische IKT-Drittanbieter bevollmächtigt werden und so ein besseres Verständnis für die von den kritischen IKT-Drittanbietern ausgehenden potenziellen Risiken erlangen können. Dies könnte dazu beitragen, die Auslagerungsverfahren der Banken zu straffen.

2. Hintergrund

2.1 Europäische Verbraucher und Unternehmen setzen zunehmend auf digitale Finanzdienstleistungen. Gleichzeitig setzen die Marktteilnehmer immer mehr innovative Lösungen auf der Grundlage neuer Technologien ein. Die digitale Transformation ist der Schlüssel für den europäischen Aufschwung und für die Schaffung einer nachhaltigen und widerstandsfähigen europäischen Wirtschaft.

2.2 Im Einklang mit den Prioritäten der Europäischen Kommission, Europa für das digitale Zeitalter fit zu machen und eine zukunftsfähige Wirtschaft aufzubauen, die im Dienste des Menschen steht, hat die Kommission ein **Paket zur Digitalisierung des Finanzsektors** vorgelegt. Dieses Paket skizziert Maßnahmen, um weitere Digitalisierungspotenziale des Finanzsektors in Bezug auf Innovation und Wettbewerb freizusetzen und zu fördern und gleichzeitig die damit verbundenen Risiken einzudämmen.

2.3 Neben dem Vorschlag zur Betriebsstabilität digitaler Systeme enthält das Paket zur Digitalisierung des Finanzsektors[1] eine neue Strategie zur Digitalisierung des EU-Finanzsektors und einen Vorschlag für eine Verordnung über Märkte für Kryptowerte zusammen mit einem Vorschlag für eine Verordnung über eine Pilotregelung zur Marktinfrastruktur für die Distributed-Ledger-Technologie (DLT)[2].

2.4 Die **Betriebsstabilität digitaler Systeme** ist die Fähigkeit von Unternehmen, sicherzustellen, dass sie allen Arten von Störungen und Bedrohungen im Zusammenhang mit Informations- und Kommunikationstechnologien (IKT) standhalten. Aufgrund der stetig zunehmenden Abhängigkeit des Finanzsektors von Software und digitalen Prozessen sind IKT-Risiken Teil des Finanzwesens. Finanzunternehmen sind zur Zielscheibe von Cyberangriffen geworden, die bei Verbrauchern und Unternehmen zu schwerwiegenden finanziellen Schäden und Rufschädigungen führen. Diese Risiken müssen gut verstanden und gehandhabt werden, insbesondere in Stressphasen.

2.5 Während die Reformen infolge der Finanzkrise 2008 die Widerstandsfähigkeit des EU-Finanzsektors stärkten, wurden IKT-Risiken nur indirekt angegangen. Das Fehlen eines umfassenden Regulierungsrahmens auf europäischer Ebene für die Betriebsstabilität digitaler Systeme führte dazu, dass man sich auf nationale Regulierungsinitiativen verließ. Dies hat jedoch die grenzübergreifende Wirksamkeit eingeschränkt und zu einer Fragmentierung des Binnenmarktes geführt, die die Stabilität und Integrität des EU-Finanzsektors untergräbt. Vor diesem Hintergrund schlägt die Kommission vor, einen umfassenden Rahmen für die Betriebsstabilität digitaler Systeme von EU-Finanzunternehmen zu schaffen.

2.6 Der **Legislativvorschlag zur Betriebsstabilität digitaler Systeme (DORA)[3]** zielt darauf ab, die Durchführung des IKT-Risikomanagements durch Finanzunternehmen zu verbessern und zu straffen, gründliche Resilienztests für IKT-Systeme einzuführen, den Informationsaustausch zu fördern und das Bewusstsein der Aufsichtsbehörden für Cyberrisiken und IKT-bezogene Vorfälle, mit denen Finanzunternehmen konfrontiert sind, zu schärfen sowie Befugnisse für Finanzaufsichtsbehörden einzuführen, um Risiken zu überwachen, die sich für Finanzunternehmen aus der Abhängigkeit von IKT-Drittdienstleistern ergeben. Mit dem Vorschlag soll auch ein einheitlicher Mechanismus zur Meldung von Vorfällen geschaffen werden, der dazu beitragen könnte, den Verwaltungsaufwand für Finanzunternehmen zu verringern und die Wirksamkeit der Aufsicht zu stärken.

2.7 Die Kommission hat auch einen Vorschlag für eine Richtlinie[4], da eine vorübergehende Ausnahme für multilaterale Handelssysteme geschaffen und gewisse Bestimmungen in bestehenden EU-Finanzdienstleistungsrichtlinien geändert oder geklärt werden müssen, um die Ziele des Vorschlags zur Betriebsstabilität digitaler Systeme zu erreichen.

---

1 Siehe in Erarbeitung befindliche EWSA-Stellungnahme ECO/534 – Strategie für ein digitales Finanzwesen in der EU.

2 Siehe in Erarbeitung befindliche EWSA-Stellungnahme ECO/535 – Kryptowerte und Distributed-Ledger-Technologie.

3 COM(2020) 595 final.

4 COM(2020) 596 final.

2.8 Als eine der weltweit größten Branchen wurde der Wert des IKT-Marktes im Jahr 2019 auf über fünf Billionen US-Dollar geschätzt. Dieser Wert soll bis 2022 auf geschätzt über sechs Billionen US-Dollar steigen. Das kontinuierliche Wachstum bestätigt die ständig zunehmende Verbreitung und Bedeutung von Technologien in der heutigen Gesellschaft. Laut Folgenabschätzung zum Legislativvorschlag ist der **Finanzsektor mit einem Anteil von ca. 20 % der gesamten IKT-Ausgaben der größte IKT-Nutzer der Welt**.

2.9 **COVID-19 hat die Verbreitung digitaler Finanzdienstleistungen vorangetrieben,** während die Filialnetze der Finanzinstitute nach wie vor nicht ausreichend ausgelastet sind. Dies wird Investitionen in digitale Selbstbedienungstools, Anwendungen im Bereich Open Finance und Mehrwertdienste anregen. Insgesamt wird die aktuelle Situation Finanzinstitute dazu zwingen, mehr in die IT-Infrastruktur zu investieren, die Migration kritischer Arbeitslasten zu priorisieren und bestehende Anwendungen zu aktualisieren. Der europäische Finanzsektor durchläuft bereits eine große digitale Transformation. Seine Fähigkeit, im globalen Wettbewerb zu bestehen, wird weitgehend von der Fähigkeit der europäischen Institute abhängen, von den fortschrittlichsten Technologien zu profitieren.

3. Allgemeine Bemerkungen

3.1 **Der EWSA begrüßt den von der Europäischen Kommission vorgelegten Verordnungsvorschlag zur Betriebsstabilität digitaler Systeme (DORA)**. Dieser greift viele der vom Finanzsektor angeführten Forderungen auf und zielt darauf ab, Rechtsklarheit in Bezug auf die Bestimmungen über IKT-Risiken zu schaffen, die regulatorische Komplexität zu verringern und den Verwaltungsaufwand zu reduzieren, der sich aus den in der EU bestehenden unterschiedlichen Vorschriften für Finanzunternehmen ergibt. Die DORA-Verordnung wird nicht nur die Widerstandsfähigkeit des Sektors gegenüber IKT-Risiken erhöhen. Sie ist auch für eine Reihe von Interessenträgern, darunter Kunden, Anleger und Mitarbeiter, von Interesse und trägt zur Umsetzung einer nachhaltigen Entwicklung bei.

3.2 Der EWSA sieht im DORA-Vorschlag einen wichtigen Schritt zur Schaffung gemeinsamer Standards, um IKT-Risiken einzudämmen und einen harmonisierten aufsichtsrechtlichen Ansatz zu erleichtern. Dabei ist jedoch darauf zu achten, dass keine zusätzlichen Hürden aufgebaut werden, die die EU-Finanzinstitute daran hindern könnten, am globalen Innovationsprozess teilzunehmen.

3.3 Für den EWSA von vordringlicher Bedeutung, dass die EU-Behörden eine verhältnismäßige und risikobasierte Regelung anstreben. Diese sollte den Aufsichtsbehörden Instrumente an die Hand geben, die ihren Aufgaben gerecht werden, und gleichzeitig Rechtssicherheit und die notwendigen Schutzmaßnahmen für Finanzunternehmen und IKT-Anbieter bieten.

4. Besondere Bemerkungen

4.1 Anwendungsbereich und regulatorische Überschneidungen

4.1.1 Einbeziehung weiterer relevanter Finanzmarktteilnehmer

Der EWSA anerkennt und begrüßt, dass die vorgeschlagene Rechtsvorschrift auf ein breites Spektrum von Finanzmarktteilnehmern abzielt und die einheitliche Anwendung der Vorschriften im gesamten EU-Finanzsektor gewährleisten wird. Er empfiehlt jedoch den politischen Entscheidungsträgern in der EU, auch Finanzmarktteilnehmer einzubeziehen, die nicht als Teil des Anwendungsbereichs dieser vorgeschlagenen Rechtsvorschrift gelten, wie z. B. Hypothekarkreditgeber und Anbieter von Verbraucherkrediten. Alle Anbieter von Finanzdienstleistungen, die identische Tätigkeiten erbringen und die gleichen Risiken eingehen, sollten den gleichen Vorschriften und der gleichen Aufsicht unterliegen, um zum Schutz der Verbraucher und der Finanzstabilität den gleichen Mindestrahmen für die digitale Resilienz zu gewährleisten.

4.1.2 Kohärenz auf internationaler und EU-Ebene, sowie mit bestehenden Regelungen

Es ist von entscheidender Bedeutung, den Unternehmen Klarheit zu verschaffen, insbesondere denjenigen, die grenzüberschreitend tätig sind, indem sichergestellt wird, dass die Definitionen und Begriffe kohärent sind und Doppelungen, Überschneidungen und unterschiedliche Auslegungen darüber, wie ähnliche regulatorische Erwartungen in verschiedenen Rechtsordnungen erfüllt werden sollen, vermieden werden. Der EWSA empfiehlt den politischen Entscheidungsträgern der EU, die Bestimmung des Begriffs der Betriebsstabilität an die Definition des Basler Ausschusses für Bankenaufsicht (BCBS)[5] anzugleichen und sicherzustellen, dass dies die für die EU-Finanzinstitute geltende maßgebliche Regelung ist. Es gilt, die Gefahr von Widersprüchen mit anderen Regelungen zu vermeiden. Außerdem sind viele der in DORA festgelegten Grundsätze und Anforderungen bereits in den bestehenden Leitlinien zu Auslagerungen definiert[6]. IKT-Risiken und Anforderungen an das Sicherheitsrisikomanagement sind ebenfalls bereits in den EBA-Leitlinien definiert. Es ist von entscheidender Bedeutung, in puncto Definition und Geltungsbereich die Kohärenz zwischen DORA und den in den bestehenden Leitlinien festgelegten Anforderungen sicherzustellen, um die Harmonisierung der regulatorischen Anforderungen der EU zu erreichen.

4.1.3 Ebenso empfiehlt der EWSA der Europäischen Kommission, dafür zu sorgen, dass die laufende Überarbeitung der Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS) und der DORA-Vorschlag dieselben Definitionen und Anforderungen an die Meldepolitik für Sicherheitsvorfälle für Finanzunternehmen enthalten.

---

5 Basler Ausschuss für Bankenaufsicht, *Principles for operational resilience*, (Grundsätze für die Betriebssicherheit) 6. November 2020.

6 So z. B. die Leitlinien der EBA, der EIOPA sowie der Entwurf der ESMA-Leitlinien, die sich in der Konsultation befanden.

4.2 **IKT-Risikomanagement**

Einige Elemente des Rahmens sind zu sehr auf die Einhaltung von Vorschriften fokussiert, anstatt darauf, wie Firmen Ergebnisse in einem grundsatz- und risikobasierten Ansatz nachweisen können. Da sie zu präskriptiv und detailliert sind, laufen sie Gefahr, mit der Weiterentwicklung der Cyber- und IKT-Risikolandschaft zu veralten. Der EWSA empfiehlt einen stärker grundsatz- und risikobasierten Ansatz, der die Durchführung von Kontrollen erleichtert, die zukunftssicher, flexibel, verhältnismäßig und den Risiken angemessen sind.

4.3 **IKT-bezogene Vorfälle**

Der EWSA empfiehlt eine vollständige Angleichung zwischen dem kürzlich vom Rat für Finanzstabilität (FSB) bereitgestellten Instrumentarium für Gegenmaßnahmen und Wiederherstellung bei Cybervorfällen (CIRR)[7], das bewährte Verfahren für die Meldung von Vorfällen enthält, und den Vorschlägen in DORA zu Management, Klassifizierung und Meldung von IKT-bezogenen Vorfällen. Es gibt Überschneidungen, die zu regulatorischer Unsicherheit führen und den Verwaltungsaufwand der Unternehmen erhöhen.

4.4 **Prüfung der Betriebsstabilität digitaler Systeme**

4.4.1 Der EWSA begrüßt das europaweite System für bedrohungsorientierte Penetrationstests (TLPT - Threat Led Penetration Testing), da es die Effizienz erhöhen und die Fragmentierung verringern wird. Gleichwohl empfiehlt der EWSA den Behörden, sich nicht nur auf die Größe oder die Reichweite des Finanzinstituts zu konzentrieren, sondern auch auf die Komplexität und Kritikalität des Dienstes. Dabei ist ggf. der Grundsatz der Verhältnismäßigkeit zu berücksichtigen und die Unterscheidung zwischen grundlegenden Prüfungen für alle Finanzinstitute und anspruchsvolleren Prüfungen für bedeutende Finanzinstitute aufzuheben. Es muss sichergestellt werden, dass die Kunden kleinerer Finanzinstitute gleichermaßen geschützt sind und gleiche Wettbewerbsbedingungen für alle Finanzinstitute geschaffen werden.

4.4.2 Der EWSA empfiehlt, die Auslagerung von Prüfungen an externe Prüfer nicht zwingend vorzuschreiben, da die Zahl der externen Prüfer begrenzt ist. Firmen können durchaus ihre eigenen internen Prüfteams haben, die mit der Firmenumgebung vertraut sind und in der Lage sind, anspruchsvollere und gezieltere Prüfungen durchzuführen.

4.4.3 Die Einbeziehung von IKT-Drittanbietern in den Anwendungsbereich des TLPT sollte überprüft werden. Die Tatsache, dass IKT-Drittanbieter möglicherweise eine Reihe von Kunden bedienen, könnte zu erheblichen Doppelprüfungen führen, was wiederum relevante Risiken für den IKT-Drittanbieter und die von ihm betreuten Kunden schaffen könnte.

7 Rat für Finanzstabilität, Final Report on Effective Practices for Cyber Incident Response and Recovery (Abschlussbericht zum wirksamen Umgang mit Cybervorfällen), 19. Oktober 2020.

4.4.4 Darüber hinaus empfiehlt der EWSA, ausdrücklich auf die **gegenseitige Anerkennung von Prüfergebnissen** zu verweisen, da diese zur Risikominderung und zum reibungslosen Funktionieren des Binnenmarktes beiträgt. Zudem lassen sich so Mehrkosten für grenzüberschreitend tätige Finanzunternehmen vermeiden.

4.5 Steuerung des Risikos durch IKT-Drittanbieter und des Überwachungsrahmens für kritische IKT-Drittanbieter

4.5.1 Sicherstellung der Kohärenz mit den bestehenden Leitlinien zu Auslagerungen

Der EWSA begrüßt, dass mit DORA ein gemeinsamer Rechtsrahmen für eine zuverlässige Steuerung des Risikos durch IKT-Drittanbieter für alle Finanzmarktteilnehmer in Europa geschaffen wird. Es wird jedoch von entscheidender Bedeutung sein, eine vollständige Angleichung zwischen dieser gemeinsamen Grundlage, die in den allgemeinen Grundsätzen (Artikel 25, 26 und 27) festgelegt ist, und den bestehenden Vorschriften wie den Leitlinien der europäischen Aufsichtsbehörden zu Auslagerungen sicherzustellen (d. h. die bestehende Dichotomie im Anwendungsbereich zwischen „Auslagerung“ und „Drittdienstleistung“[8] aufzulösen). Darüber hinaus hält der EWSA dies für eine gute Gelegenheit für die EU-Behörden, die Anforderungen an die Auslagerung in einer einzigen Verordnung zu konsolidieren – mit hinreichender Ausführlichkeit, um unterschiedliche Auslegungen zu vermeiden –, die allen Marktteilnehmern Rechtssicherheit bringen und die aufsichtsbezogenen Erwartungen zuverlässig erfüllen könnte.

4.5.2 Anforderungen, die für kritische oder wichtige ausgelagerte Tätigkeiten gelten

Bei der Anwendung von Artikel 25 Absatz 2 der Verordnung muss im Interesse eines risikoorientierten Fokus konkreter darauf eingegangen werden, wie der Grundsatz der Verhältnismäßigkeit angewandt wird, indem die Anforderungen spezifiziert werden, die für kritische oder wichtige ausgelagerte Tätigkeiten gelten würden, und diejenigen, die für die übrigen Tätigkeiten gelten würden[9]. Der EWSA empfiehlt die Nutzung von IKT-Diensten für nicht kritische Funktionen vom Anwendungsbereich von DORA auszunehmen.

4.5.3 Direkter Aufsichtsrahmen für kritische Drittanbieter

Der EWSA begrüßt die Einführung eines direkten Aufsichtsrahmens, der in Ermangelung eines horizontalen, sektorübergreifenden EU-Rahmens eine kontinuierliche Überwachung der Tätigkeiten von kritischen IKT-Drittanbietern durch die Finanzbehörden ermöglicht. In der vorgeschlagenen Verordnung sollten die EU-Behörden anerkennen, dass die Risikoexposition von Finanzinstituten aufgrund der kontinuierlichen Überwachung ihrer Aktivitäten sinkt, wenn

8 DORA bezieht sich nur auf Dienstleistungen von IKT-Drittanbietern in Bezug auf die Grundsätze für eine zuverlässige Steuerung des Risikos durch IKT-Drittanbieter (Kapitel V). Der Anwendungsbereich der EBA-Leitlinien zu Auslagerungsvereinbarungen wiederum basiert auf einer Definition von Auslagerung, bei der die Tätigkeit wiederholt oder laufend erbracht wird (Ziffer 26). Die EBA-Leitlinien enthalten auch eine Liste von Ausnahmen, die nicht als Auslagerung gelten (Ziffer 28.).

9 Auch hier wird es entscheidend sein, die Definition von „kritischen oder wichtigen Funktionen“ in DORA und in den EBA-Leitlinien zu Auslagerungen aneinander anzugleichen. Die EBA-Leitlinien definieren insbesondere die Faktoren, die Finanzinstitute bei der Beurteilung, ob sich eine Auslagerungsvereinbarung auf eine kritische oder wichtige Funktion bezieht, berücksichtigen sollten (Ziffern 29, 30 und 31).

ein kritischer IKT-Anbieter unter diese Aufsicht fällt. Daher sollte dieser neue Aufsichtsrahmen auch dazu beitragen, die Auslagerungs-Verfahren der Banken zu straffen. Ein Teil des Aufwands, dem Finanzunternehmen derzeit ausgesetzt sind, wird verringert, z. B. in Bezug auf die Durchführung von Prüfungs- und Kontrollverfahren bezüglich der als kritisch eingestuften Drittanbieter.

4.5.4 Der EWSA befürwortet die Ermächtigung der federführenden Aufsichtsinstanz zur Durchführung der Prüfungs- und Kontrollverfahren bei den kritischen IKT-Drittanbietern. Denn die federführenden Aufsichtsinstanzen würden ein besseres Verständnis der Risiken erlangen, die von den diesen kritischen Drittanbietern ausgehen können, da sie deren Prozesse und Gegebenheiten aus erster Hand kennen und sich nicht auf die derzeitige Berichterstattung der beaufsichtigten Finanzinstitute verlassen müssten. Die Strategien der Finanzinstitute zu Risikominderung und die entsprechenden gesetzlichen Verpflichtungen sollten beibehalten werden. Werden Kontrollen und Audits jedoch bereits von der federführenden Aufsichtsinstanz durchgeführt, sollten die Finanzinstitute von diesem zusätzlichen Sicherheitsniveau profitieren und diese Kontrollen und Audits nicht erneut durchführen müssen.

4.5.5 **Federführende Aufsichtsinstanz und zuständige nationale Behörden**

Nach Abschluss des Aufsichtsprozesses werden die Empfehlungen der federführenden Aufsichtsinstanz von den zuständigen nationalen Behörden weiterverfolgt, die bei benannten kritischen Drittanbietern ihren eigenen Ansatz zur Umsetzung der Ergebnisse der federführenden Aufsichtsinstanz haben können. Der EWSA empfiehlt, vollständige Klarheit über die Rollen und Zuständigkeiten der verschiedenen Behörden zu schaffen, um eine Situation zu vermeiden, in der sich unterschiedliche Auslegungen je nach zuständiger Behörde unterschiedlich auf die Kunden kritischer Drittanbieter auswirken. Das Risiko einer Fragmentierung soll so verringert werden. Angesichts der derzeitigen Unklarheit von Artikel 37 in Bezug auf ihre Verbindlichkeit sollten diese Empfehlungen auch vollständig durchsetzbar gemacht werden.

4.5.6 **Aussetzung der Nutzung eines kritischen Drittanbieters**

Gemäß Verordnungsvorschlag haben die nationale Finanzaufsichtsbehörden die Befugnis, von Kunden zu verlangen, die Nutzung eines IKT-Anbieters vorübergehend teilweise oder vollständig auszusetzen, bis die in den Empfehlungen ermittelten Risiken behoben sind. Die Forderung nach einer sofortigen Beendigung der Zusammenarbeit mit einem kritischen Drittanbieter würde sich definitiv auf bestehende oder künftige geschäftliche und betriebswirtschaftliche Entscheidungen auswirken (z. B. vor Investitionen in der EU abschrecken) und möglicherweise die Finanzstabilität beeinträchtigen. Bevor solche Entscheidungen getroffen werden, sollten die zuständigen Behörden neben anderen Faktoren sorgfältig die potenziellen negativen Auswirkungen der Beendigung des Dienstes für die Finanzunternehmen abwägen, die diesen speziellen kritischen Drittanbieter in Anspruch

nehmen[10], genaue Kriterien für die Anwendung einer solchen Forderung festlegen und mögliche Korrekturmaßnahmen erwägen.

4.5.7 Sollte eine solche Situation jedoch letztlich eintreten, empfiehlt der EWSA zudem, die Finanzunternehmen rechtzeitig zu informieren und ihnen ausreichend Zeit für den Wechsel einzuräumen.

4.6 Erhalt der globalen Wettbewerbsfähigkeit europäischer Finanzunternehmen

4.6.1 Der neue Rahmen muss die Fähigkeit der europäischen Finanzunternehmen bewahren, mindestens auf die gleichen Technologien zuzugreifen wie ihre globalen Wettbewerber. EU-Finanzunternehmen stehen im globalen Wettbewerb. Der künftige EU-Rechtsrahmen sollte die EU-Unternehmen nicht benachteiligen, indem der Zugang zu den fortschrittlichsten Technologien einschränkt wird, solange die Anbieter dieser Technologien die EU-Standards in puncto Resilienz und Sicherheit erfüllen.

4.6.2 Drittanbieter mit Sitz in Drittländern

Die Möglichkeit der Auslagerung von als kritisch erachteten Dienstleistungen an Drittanbieter mit Sitz in Drittländern sollte durch die Verordnung nicht einschränkt werden. Diese Einschränkung würde die Vertragsfreiheit der einzelnen Unternehmen und die Fähigkeit der europäischen Finanzinstitute massiv einschränken, auf die Dienste von Anbietern mit hohem Mehrwert zuzugreifen, die es in Europa höchstwahrscheinlich nicht in ausreichender Zahl geben wird. Dies ist umso relevanter, als der vorgeschlagene Aufsichtsrahmen auf den Finanzsektor beschränkt ist. Das würde ungleiche Wettbewerbsbedingungen für andere Akteure schaffen, die nicht dieser Regulierung unterliegen, und am Ende die Gefahr einer Konzentration erhöhen, die mit der Verordnung ja gerade vermieden werden soll.

4.6.3 Zwangsgelder auf der Grundlage des globalen Umsatzes

Der Vorschlag sieht Strafzahlungen in Bezug auf den weltweiten Umsatz für IKT-Anbieter vor, wenn diese den Aufforderungen der EU-Finanzaufsichtsbehörden nicht nachkommen. Eine unverhältnismäßige Anwendung solcher Sanktionen könnte globale IKT-Anbieter davon abhalten, EU-Finanzunternehmen zu bedienen. Für EU-Finanzunternehmen könnte dies de facto die Auswahl an Anbietern einschränken. Darüber hinaus würde es nicht kritische IKT-Drittanbieter davon abhalten, sich dem Aufsichtsregime anzuschließen. Es besteht die Gefahr, mit unverhältnismäßigen Bußgeldern bestraft zu werden, weshalb sie den Wettbewerb im vorgelagerten Markt verringern könnten. Der EWSA spricht sich für die Einführung der Verhältnismäßigkeit bei der Sanktionsregelung aus. Dies ist von entscheidender Bedeutung, um zu verhindern, dass IKT-Anbieter, die Dienstleistungen für EU-Finanzinstitute erbringen wollen, abgeschreckt werden.

---

10 Eines der Kriterien, um einen IKT-Anbieter als kritisch zu benennen, ist der Grad der Substituierbarkeit des IKT-Drittanbieters unter Berücksichtigung des Mangels an echten Alternativen oder der Schwierigkeiten, die mit einer teilweisen oder vollständigen Migration der Dienste verbunden wären (Artikel 28 Absatz 2). Wenn dies zutrifft, wäre es für Finanzinstitute schwierig, den Dienst zu einem anderen Anbieter zu migrieren. Darüber hinaus würde die Forderung an exponierte Finanzinstitute, zu einem anderen Dienstleister zu wechseln, letztlich zu einer verstärkten Konzentration auf dem europäischen Markt beitragen. Dies würde jedoch gerade der Intention dieser Verordnung zuwiderlaufen.

4.7 **Vereinbarung über den Austausch von Informationen**

4.7.1 Der EWSA begrüßt Vereinbarungen über den Informationsaustausch über Cyberbedrohungen zwischen Finanzinstituten auf freiwilliger Basis. Denn ein rechtzeitiger Informationsaustausch ist von entscheidender Bedeutung, um Angriffsvektoren wirksam zu ermitteln und potenzielle Bedrohungen zu isolieren und zu verhindern.

4.7.2 Der EWSA empfiehlt ferner, dass die EU-Behörden unter den Bedingungen dieses Vorschlags eine explizite Grundlage für den Austausch personenbezogener Daten (wie z. B. IP-Adressen) vorsehen. Dadurch würde die Unsicherheit verringert und die Fähigkeit der Finanzunternehmen gestärkt, ihre Verteidigungsfähigkeiten zu verbessern, Bedrohungen besser zu erkennen und das Risiko einer Ansteckung untereinander zu verringern. Weitergehende Klarheit ist aufgrund der vertraulichen und sensiblen Natur der Daten erforderlich.

Brüssel, den 24. Februar 2021

Christa SCHWENG
Präsidentin des Europäischen Wirtschafts- und Sozialausschusses