EUROPÄISCHE
KOMMISSION

Brüssel, den 24.9.2020
SWD(2020) 204 final

Die vorliegende Sprachfassung enthält die Änderungen der am 16.10.2020 unter der Nummer SWD(2020)/204 final/2 veröffentlichten Fassung der EN-Originalversion.

ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN

BERICHT ÜBER DIE FOLGENABSCHÄTZUNG (ZUSAMMENFASSUNG)

Begleitunterlage zum

VORSCHLAG FÜR EINE RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Änderung der Richtlinien 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 und (EU) 2016/2341

{COM(2020) 596 final} - {SEC(2020) 309 final} - {SWD(2020) 203 final}

ZUSAMMENFASSUNG

Folgenabschätzung zum Vorschlag für eine Verordnung über die Betriebsstabilität digitaler Systeme im Finanzsektor

A. Handlungsbedarf

Warum? Um welche Problematik geht es?

Der Finanzsektor ist in hohem Maße auf Informations- und Kommunikationstechnologien (IKT) angewiesen. Vor dem Hintergrund der derzeitigen COVID-19-Pandemie dürfte sich dies angesichts der Vorteile, die sich aus der Gewährleistung eines kontinuierlichen Fernzugangs zu Finanzdienstleistungen ergeben, noch verstärken. Gleichwohl gibt die Abhängigkeit von digitalen Technologien Anlass zur Sorge, da Unternehmen in der Lage sein müssen, potenziellen IKT-Störungen standzuhalten, damit Vorfälle und Bedrohungen im digitalen Bereich angegangen und Dienste aufrechterhalten werden können. Wenngleich es in allen Wirtschaftssektoren Abhängigkeiten von IKT-Technologien gibt, sind in einem stark vernetzten Finanzsektor, der grenzübergreifende, für die Realwirtschaft unentbehrliche Basisdienstleistungen bereitstellt, die Anfälligkeiten infolge der Abhängigkeit von IKT besonders ausgeprägt, da in diesem Bereich 1) IKT intensiv und umfassend genutzt wird und 2) die Folgen eines operativen Vorfalls in einem Finanzunternehmen oder finanziellen Teilsektor rasch auf andere Unternehmen oder Teile des Finanzsektors und letztlich auf die übrige Wirtschaft übergreifen können.

Auch wenn die Markt- und Regulierungsintegration im Finanzsektor sehr weit fortgeschritten ist und der Sektor sich auf einheitliche harmonisierte Vorschriften – das einheitliche Regelwerk der EU – stützt, beruhten die einschlägigen Maßnahmen der EU, mit denen auf den auf horizontaler und sektoraler Ebene gestiegenen Bedarf an Betriebsstabilität reagiert wurde,

- entweder auf einer Mindestharmonisierung, wodurch Spielraum für nationale Auslegungen und Binnenmarktfragmentierung entstand,
- oder sie waren zu allgemein gefasst und nur begrenzt anwendbar, wobei das operationelle Gesamtrisiko in unterschiedlichem Maße angegangen wurde, teilweise einige Aspekte digitaler Betriebsstabilität reguliert wurden (z. B. IKT-Risikomanagement, Meldung von Vorfällen und IKT-Risiken durch Dritte), andere Aspekte (Durchführung von Tests) jedoch unberücksichtigt blieben.

Im Rahmen von EU-Maßnahmen wurde bislang weder das operationelle Risiko in einer Weise angegangen, die Finanzunternehmen ermöglicht hätte, IKT-bedingte Anfälligkeiten abzufedern und entsprechende Gegen- und Wiederherstellungsmaßnahmen zu ergreifen, noch wurden die Finanzaufsichtsbehörden mit einem Instrumentarium ausgestattet, das ihnen ermöglichen würde, ihr Mandat zur Eindämmung der aus diesen IKT-Anfälligkeiten resultierenden finanziellen Instabilität zu erfüllen.

Die derzeitigen Lücken und Inkohärenzen haben zu einer Zunahme von unkoordinierten nationalen Initiativen (z. B. in Bezug auf die Durchführung von Tests) und Aufsichtsansätzen (z. B. bezüglich der Abhängigkeiten von Dritten im IKT-Bereich) geführt, die sich entweder in Überschneidungen, Doppelanforderungen und hohen Verwaltungs- und Befolgungskosten für grenzübergreifend tätige Finanzunternehmen niederschlagen oder zur Folge haben, dass IKT-Risiken nicht erkannt bzw. angegangen werden. Insgesamt sind die Stabilität und Integrität des Finanzsektors nicht gewährleistet, und der Binnenmarkt für Finanzdienstleistungen ist nach wie vor fragmentiert, was den Verbraucher- und Anlegerschutz schwächt.

Was soll mit dieser Initiative erreicht werden?

Das übergeordnete Ziel besteht darin, die Betriebsstabilität digitaler Systeme im EU-Finanzsektor zu stärken, indem bestehende EU-Finanzvorschriften gestrafft und modernisiert und – wenn Lücken bestehen – neue Anforderungen eingeführt werden, um Folgendes zu erreichen:

- Verbesserung der Steuerung von IKT-Risiken durch Finanzunternehmen;
- Erweiterung der Kenntnis der Aufsichtsbehörden von Bedrohungen und Vorfällen;
- bessere Möglichkeiten für Finanzunternehmen, ihre IKT-Systeme zu testen; und
- bessere Überwachung der Risiken, die sich aus der Abhängigkeit der Finanzunternehmen von IKT-Drittanbietern ergeben.

Insbesondere würden mit dem Vorschlag kohärentere und einheitlichere Verfahren für die Meldung von Vorfällen eingeführt, wodurch der Verwaltungsaufwand für Finanzinstitute verringert und die Effizienz der Aufsicht erhöht würde.

Worin besteht der Mehrwert des Tätigwerdens auf EU-Ebene?

Der EU-Binnenmarkt für Finanzdienstleistungen unterliegt einem umfangreichen Regelwerk auf EU-Ebene, das es in einem Mitgliedstaat zugelassenen Finanzunternehmen ermöglicht, mit einem „Europäischen Pass“ Dienstleistungen im gesamten Binnenmarkt zu erbringen. Folglich wären Vorschriften auf nationaler Ebene kein wirksames Mittel, um die Betriebsstabilität von Finanzunternehmen, die den Pass nutzen, zu erhöhen. Darüber

hinaus wurden infolge der Finanzkrise bindende und sehr detaillierte Vorschriften zu eher „traditionellen“ Risiken wie Kredit-, Markt-, Gegenpartei- und Liquiditätsrisiken in das einheitliche Regelwerk der EU aufgenommen, während die bestehenden Bestimmungen zu Risiken für die Betriebsstabilität nach wie vor allgemein gehalten sind. Die Stärkung der digitalen Betriebsstabilität erfordert Anpassungen der Bestimmungen über operationelle Risiken, die bereits auf EU-Ebene festgeschrieben sind und daher nur auf EU-Ebene verbessert und ergänzt werden können.

B. Lösungen

Welche gesetzgeberischen und sonstigen Maßnahmen wurden erwogen? Wird eine Option bevorzugt? Warum?

In der Folgenabschätzung wurden neben einem Referenzszenario, bei dem keine Maßnahmen hinsichtlich der EU-Rechtsvorschriften über Finanzdienstleistungen ergriffen werden, drei Optionen geprüft. Im Einzelnen:

- **Kein Tätigwerden**: Die Regelungen zur Betriebsstabilität würden weiterhin durch die derzeitigen, voneinander abweichenden EU-Vorschriften für Finanzdienstleistungen, zum Teil durch die Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) sowie durch bestehende oder künftige nationale Regelungen vorgegeben.
- **Option 1 – Stärkung der Kapitalpuffer**: Ein zusätzlicher Kapitalpuffer würde eingeführt, damit Finanzunternehmen eventuelle Verluste aufgrund von mangelnder Betriebsstabilität besser ausgleichen könnten.
- **Option 2 – Rechtsakt zur Betriebsstabilität der digitalen Systeme im Finanzsektor**: Ein umfassender Rechtsrahmen auf EU-Ebene würde eingeführt, der Vorschriften zur digitalen Betriebsstabilität für alle beaufsichtigten Finanzinstitute enthält und auf Folgendes abzielt:
  - IKT-Risiken umfassender angehen;
  - Finanzaufsichtsbehörden den Zugang zu Informationen über IKT-bezogene Vorfälle ermöglichen;
  - sicherstellen, dass Finanzunternehmen bewerten, wie wirksam ihre Präventions- und Resilienzmaßnahmen sind und wo ihre IKT-Anfälligkeiten liegen;
  - die Outsourcing-Vorschriften für die indirekte Beaufsichtigung von IKT-Drittanbietern verschärfen;
  - eine direkte Beaufsichtigung der Tätigkeiten von IKT-Drittanbietern ermöglichen, wenn diese Dienstleistungen für Finanzunternehmen erbringen, und
  - Anreize für den Informationsaustausch über Bedrohungen im Finanzsektor schaffen.
- **Option 3 – Rechtsakt zur Betriebsstabilität in Verbindung mit einer zentralisierten Beaufsichtigung kritischer Drittanbieter**: Zusätzlich zu einem Rechtsakt zur digitalen Betriebsstabilität (Option 2) würde eine neue Behörde geschaffen, die Drittanbieter von einschlägigen IKT-Dienstleistungen für Finanzunternehmen beaufsichtigen würde. Außerdem würde der Finanzsektor hierdurch klarer vom Anwendungsbereich der NIS-Richtlinie abgegrenzt.

Option 2 ist die bevorzugte Option. Sie ist – unter Berücksichtigung der Kriterien Effizienz und Kohärenz – im Vergleich zu den anderen Optionen am besten geeignet, die Ziele der Initiative zu erreichen. Diese Option erhielt auch die meiste Unterstützung von den Interessenträgern.

Wer unterstützt welche Option?

Die meisten (privaten und öffentlichen) Interessenträger stimmen darin überein, dass Maßnahmen auf EU-Ebene erforderlich sind, um die digitale Betriebsstabilität von Finanzunternehmen besser zu schützen. Viele sind darüber hinaus der Ansicht, dass Maßnahmen auf EU-Ebene notwendig sind, um den Regelungsaufwand einzudämmen, der Finanzunternehmen durch Doppelanforderungen und die Uneinheitlichkeit der Bestimmungen entsteht, die in der NIS-Richtlinie, den EU-Rechtsvorschriften über Finanzdienstleistungen und den nationalen Regelungen (z. B. für die Meldung von Vorfällen) festgelegt sind. Infolgedessen sprechen sich nur wenige Interessenträger gegen ein Tätigwerden aus. Nur wenige Interessenträger halten es für sinnvoll, die digitale Betriebsstabilität durch höhere Kapitalpuffer zu gewährleisten (Option 1). Im Hinblick auf operationelle Risiken ist dies jedoch der traditionelle Ansatz, insbesondere im Bankensektor; so stützen sich etwa internationale Standardsetzungsgremien auf einen solchen Ansatz. Die in Option 2 beschriebene Art qualitativer Maßnahmen, mit denen die Finanzvorschriften der EU gestrafft und modernisiert und im Falle von Regulierungslücken neue Anforderungen eingeführt würden, während Verzahnungen mit der horizontalen NIS-Richtlinie beibehalten würden, findet breite Unterstützung seitens der Interessenträger, die an der öffentlichen Konsultation teilgenommen haben. Während einige Interessenträger (insbesondere Behörden) die verstärkte Beaufsichtigung von IKT-Drittanbietern im Sinne von Option 3 als sinnvoll erachten, finden die Schaffung einer neuen EU-Behörde zu diesem Zweck sowie die umfassendere Abkopplung vom NIS-Rahmen nur begrenzt Unterstützung bei den Interessenträgern.

C. Auswirkungen der bevorzugten Option

Worin bestehen die Vorteile der bevorzugten Option bzw. der wesentlichen Optionen?

Mit Option 2 würden **IKT-Risiken** im gesamten Finanzsektor angegangen, indem die Fähigkeit von Finanzunternehmen, IKT-Vorfällen standzuhalten, gestärkt würde. Dies würde das Risiko verringern, dass sich ein Cybervorfall rasch über die Finanzmärkte hinweg ausbreitet. Wenngleich es schwierig ist, die Kosten operativer Vorfälle im Finanzsektor zu schätzen (nicht alle Vorfälle werden gemeldet; Kostenumfang ungewiss), geht aus Branchenuntersuchungen hervor, dass sich die Kosten für den EU-Finanzsektor auf 2 bis 27 Mrd. EUR pro Jahr belaufen könnten. Mit der bevorzugten Option würden diese direkten Kosten verringert und alle eventuellen weiterreichenden Auswirkungen schwerwiegender Cybervorfälle auf die Stabilität des Finanzsektors abgefedert. Die Beseitigung sich überschneidender **Berichtspflichten** würde den Verwaltungsaufwand verringern. So könnten die damit verbundenen Einsparungen für einige der größten Banken zwischen 40 und 100 Mio. EUR pro Jahr betragen. Durch eine direkte Berichterstattung ließe sich auch die Kenntnis der Aufsichtsbehörden von IKT-Vorfällen steigern. Durch **harmonisierte Tests** würden unbekannte Anfälligkeiten und Risiken besser erkannt werden. Dies würde auch die Kosten senken, insbesondere für grenzüberschreitend tätige Unternehmen. So könnte der zu erwartende Gesamtnutzen eines gemeinsamen Testansatzes für die 44 größten grenzüberschreitend tätigen Banken bei 11 bis 88 Mio. EUR liegen. Durch die Einführung eines kohärenten Regelwerks für die Steuerung der Risiken **durch Drittanbieter von IKT-Dienstleistungen** erhielten Finanzunternehmen mehr Kontrolle darüber, wie Drittanbieter den Rechtsrahmen einhalten, was Aufsichtsbehörden helfen könnte. Zudem entstünden durch die Beaufsichtigung von IKT-Drittanbietern aufsichtliche Vorteile. Allgemein ist die bevorzugte Option mit weiteren Vorteilen für die Gesellschaft insgesamt verbunden, die sich aus einem stabileren Betriebsumfeld für alle Finanzmarktteilnehmer und einem verstärkten Verbraucher- und Anlegerschutz ergeben.

Welche Kosten entstehen bei der bevorzugten Option bzw. den wesentlichen Optionen?

Die bevorzugte Option würde sowohl einmalige als auch wiederkehrende Kosten verursachen. Die einmaligen Kosten wären auf Investitionen in IT-Systeme zurückzuführen und lassen sich angesichts des unterschiedlichen Zustands der vorhandenen Systeme von Unternehmen nur schwer quantifizieren. Da bislang nicht regulatorisch eingegriffen wurde, haben einige Finanzunternehmen bereits umfassend in IKT-Systeme investiert. Dies bedeutet, dass die Kosten für die Umsetzung der Maßnahmen des vorliegenden Vorschlags für große Finanzunternehmen wahrscheinlich gering ausfallen werden. Bei kleineren Unternehmen dürften die Kosten ebenfalls niedriger ausfallen, da sie ihrem geringeren Risiko entsprechend weniger umfassenden Maßnahmen unterliegen würden. Die europäischen Aufsichtsbehörden haben in Bezug auf Tests ermittelt, dass die Kosten für bedrohungsorientierte Penetrationstests (Threat-Led-Penetration-Tests) zwischen 0,1 % und 0,3 % des gesamten IKT-Budgets der betreffenden Unternehmen betragen. Die mit der Meldung von Vorfällen verbundenen Kosten würden drastisch gesenkt, da es keine Überschneidungen mit den Meldepflichten im Rahmen der NIS-Richtlinie gäbe. Bei den Aufsichtsbehörden werden gewisse Kosten entstehen, da sich ihr Aufgabenfeld erweitern würde; so könnte beispielsweise für Aufsichtsbehörden, die an der direkten Beaufsichtigung von IKT-Drittanbietern beteiligt sind, mit einem geschätzten Anstieg der Zahl der Vollzeitäquivalente von 1 bis 5 VZÄ für die federführende Aufsichtsinstanz und von rund 0,25 VZÄ für die beteiligten Behörden gerechnet werden.

Worin bestehen die Auswirkungen auf Unternehmen, KMU und Kleinstunternehmen?

Die bevorzugte Option würde alle Finanzunternehmen umfassen, um die Betriebsstabilität des Sektors insgesamt zu erhöhen. Angesichts der Verflechtungen im Finanzsektor und der damit verbundenen Notwendigkeit, ein robustes Maß an allgemeiner Betriebsstabilität zu gewährleisten, ist ein weit gefasster Anwendungsbereich wichtig. Bei der Festlegung der Kernanforderungen in den wichtigsten Handlungsbereichen würde jedoch sowohl über alle Teilsektoren hinweg als auch innerhalb jedes Teilsektors der Grundsatz der Verhältnismäßigkeit gelten. Dabei würden etwa Unterschiede bei den Geschäftsmodellen, der Größe, dem Risikoprofil, der Systemrelevanz usw. berücksichtigt. Beispielsweise müssten kleinere Finanzunternehmen weniger umfassende Maßnahmen zur Meldung von Vorfällen und zur Durchführung von Tests ergreifen.

Hat die Initiative nennenswerte Auswirkungen auf die nationalen Haushalte und Behörden?

Nein. Die zusätzliche Beaufsichtigung kann, wie oben dargelegt, ein begrenztes Maß an zusätzlichen Aufsichtsressourcen erfordern, die ganz oder – wenn Aufsichtsgebühren erhoben werden – teilweise aus öffentlichen Haushalten finanziert werden können.

Wird es andere nennenswerte Auswirkungen geben?

Die sozioökonomischen Folgen der COVID-19-Pandemie verdeutlichen, wie wichtig die digitalen Finanzmärkte und deren Betriebsstabilität sind. Mit der bevorzugten Option würde eine solide Grundlage für die Nutzung des

digitalen Wandels geschaffen, indem sichergestellt wird, dass der Binnenmarkt für Finanzdienstleistungen, einschließlich der Banken- und Kapitalmarktunion, eine Betriebsstabilität aufweist und auf gemeinsamen Regeln und Anforderungen beruht, die Sicherheit, Leistung, Stabilität und gleiche Wettbewerbsbedingungen gewährleisten sollen. Dies wird auch die globale Führungsrolle Europas im Finanz- und Digitalbereich stärken – ein Ziel, das die Kommission in ihrer Mitteilung „Gestaltung der digitalen Zukunft Europas“ festgeschrieben hat.

D. Folgemaßnahmen

Wann wird die Maßnahme überprüft?

Die erste Überprüfung würde drei Jahre nach Inkrafttreten des Rechtsinstruments vorgenommen. Die Kommission würde dem Europäischen Parlament und dem Rat einen Bericht über ihre Überprüfung vorlegen. Die Überprüfung könnte gegebenenfalls mit einer öffentlichen Konsultation, Studien, Expertendiskussionen, Umfragen und Workshops unterlegt werden.