Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

# Stellungnahme

## Digital Finance Package der Europäischen Kommission - Legislativvorschlag „proposal for a regulation on digital operational resilience for the financial sector" (DORA) vom 24.9.2020

Kontakt:

Berit Schimm

Telefon: +49 30 2021-2111

Telefax: +49 30 2021-19 2100

E-Mail: b.schimm@bvr.de

Berlin, 16.10.2020

Federführer:

Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.

Schellingstraße 4 | 10785 Berlin

Stellungnahme **Digital Finance Package der Europäischen Kommission - Legislativvorschlag „**proposal for a regulation on digital operational resilience for the financial sector" (DORA) vom 24.9.2020

## Allgemeine Einschätzung

Eine Harmonisierung der verschiedenen europäischen Regulierungsansätze begrüßen wir grundsätzlich.

Die im vorliegenden Legislativvorschlag enthaltenen Regelungen gehen jedoch deutlich über den von der europäischen Kommission beabsichtigten Harmonisierungsansatz hinaus. Ausnahmen sind an vielen Stellen nur für „Microenterprises" vorgesehen, unter deren Definition Banken aufgrund der geringen Bilanzsummengrenze und/oder üblichen Belegschaftsgröße nicht fallen. Somit kommt das Proportionalitätsprinzip nicht ausreichend zur Anwendung. Dies steht im Gegensatz zum derzeit etablierten Ansatz in Deutschland.

Die aktuellen Regulierungsstandards von EBA und BaFin verfolgen einen Proportionalitätsansatz insbesondere hinsichtlich Risiko und Komplexität der Institute. Zudem ermöglichen Leitlinien der ESAs gegenüber einer unmittelbar anzuwendenden EU-Verordnung den nationalen Aufsichtsbehörden die Berücksichtigung nationaler Besonderheiten. Die prinzipienorientierten Anforderungen dieser Leitlinien lassen aktuell grundsätzlich Handlungsspielraum bei der Umsetzung. Darüberhinausgehende gesetzliche Regelungen sind nicht erforderlich.

Die im Legislativvorschlag enthaltenen Einzelregelungen schaffen hingegen neue Regelungen, die teilweise inkonsistent zu bestehenden aufsichtsrechtlichen Vorgaben sind.

Über die zur Umsetzung der Verordnung vorgesehenen Regulatory Technical Standards der ESAs ist eine noch weitergehende Regelungsdichte und –tiefe zu erwarten. Es sollte keine gesetzliche Methodenfestlegung über RTS erfolgen, da insbesondere im IT-Sicherheitsumfeld eine kurzfristige Anpassungsfähigkeit der Methoden und Praktiken erforderlich ist.

Bereits bestehende Anforderungen der NIS- und die PSD2-Richtlinie würden sich mit den vorgelegten Anforderungen des Legislativvorschlags überlappen, so dass zudem eine Anpassung dieser Richtlinien erforderlich wäre, sofern Punkte in der vorliegenden Form in eine neue Verordnung gefasst werden.

Positiv ist die angedachte Harmonisierung des Meldewesens zu Sicherheitsvorfällen hervorzuheben. Wir begrüßen ferner grundsätzlich die Idee eines neuen Aufsichtsrahmens für kritische europaweit tätige IKT-Dienstleister. Dieser sollte allerdings mit Erleichterungen bei der Überwachung durch die Finanzinstitute verknüpft werden und die Nutzung dieser Dienstleister sollte nicht durch zu limitierende Vorgaben erschwert werden. Daher sehen wir die Notwendigkeit, die vorgeschlagenen Anforderungen in diesem Kapitel, aber auch im Kapitel IKT-Drittanbieter-Risikomanagement allgemein mit Blick auf Notwendigkeit und Zielgerichtetheit genau zu prüfen. Im Fokus sollten aus Sicht der Finanzinstitute insbesondere solche internationalen IKT-Dienstleister stehen, bei denen die Durchsetzbarkeit von Prüfungen auf Ebene des einzelnen Finanzinstituts nicht in ausreichendem Maße gewährleistet werden kann. Für überwiegend national tätige bedeutende IKT-Dienstleister sollte eine Prüfung durch nationale Aufsichtsbehörden erfolgen, da diese die nationalen Gegebenheiten genauestens kennen.

Für die Verordnung sollte generell eine ausreichende Umsetzungsfrist von 36 Monaten nach Inkrafttreten vorgesehen werden (vgl. Artikel 56 - dort wird mit zwei Ausnahmen lediglich eine Frist von 12 Monaten nach Inkrafttreten genannt).

## Zu den Kapiteln im Einzelnen

### Kapitel II ICT risk management

#### Section I Governance und Organisation

Der Geschäftsleitung werden zu viele Aufgaben direkt zugeordnet. Die Geschäftsleitung muss im Rahmen ihrer abschließenden Verantwortung bspw. zwar den Risikoappetit definieren, aber nicht selbst alle Details bestimmen, Überwachungshandlungen und regelmäßige Reviews durchführen.

Die Anforderungen sind absolut formuliert und erlauben keine proportionale am Risiko orientierte Auslegung.

Beispiel:

Abs. 3. fordert die Benennung einer zentralen Rolle zur Überwachung der IKT- Dienstleister auch für kleine, weniger komplexe Institute (außer für „Microenterprises" vgl. allgemeine Einschätzung oben).

## Section II

Viele Anforderungen sind grundsätzlich aus den BAIT und den EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken bekannt. Diese Anforderungen sollten auf Ebene von Leitlinien der ESAs belassen werden, die entsprechend untereinander harmonisiert werden. Die Gesetzgebung sollte den dafür notwendigen Rahmen festlegen.

Auch wenn im Kapitel 1 eine grundsätzliche Absichtserklärung für eine proportionale Anwendung vorangestellt wird, stellen die Anforderungen in diesem Kapitel dennoch Mindestanforderungen für grundsätzlich alle Finanzinstitute dar. Ausnahmen sind wieder nur für „Microenterprises" vorgesehen. Während die heutigen EBA-Leitlinien zukünftig in der Verordnung aufgehen und noch durch zusätzliche Regeln erweitert werden, würden die angedachten Regulatory Technical Standards (RTS) der ESAs das Regelwerk deutlich erweitern (vgl. Artikel 14). Damit geht die Regulierung deutlich über ein Harmonisierungsziel hinaus, Handlungsspielräume werden zugleich eingeschränkt. Neue RTS gemäß Artikel 14 sollten nicht neue Methoden festschreiben, sondern weiterhin auf die Anwendung gängiger Standards abstellen. Dies ist besonders deshalb von Vorteil, da gängige Standards kontinuierlich weiterentwickelt werden.

Beispiele für Anforderungen des vorliegenden Entwurfs, die über die Anforderungen der EBA-Leitlinien hinausgehen:

Beispiele:

- Artikel 5, Abs. 10: Zustimmung der Aufsichtsbehörden erforderlich, wenn Finanzunternehmen die Aufgaben der Überprüfung der Einhaltung der Anforderungen an das IKT-Risikomanagement an Dritte delegieren.
- Artikel 7, Abs. 1: Mindestens jährliche Überprüfung der Klassifizierung der Informationsassets und aller relevanten Dokumentationen. Hier sollte analog zu den bestehenden Regeln eine regelmäßige Überprüfung, die ein nach Risiko abgestuftes Vorgehen erlaubt, ermöglicht werden.
- Artikel 7, Abs. 7.: Jährliche IKT Risiko-Assessments über die Gesamtheit aller bestehenden IKT-Systeme stellen einen hohen Aufwand dar. Auch hier sollte ein risikoorientierter Ansatz gewählt werden, der ein abgestuftes Vorgehen ermöglicht.
- Artikel 9, Abs. 2: Verpflichtung zu einem "automatischen Alarm", d.h. ein automatisiertes SIEM System wird damit für alle Finanzinstitute mandatorisch (entgegen Proportionalitätsansatz).
- Artikel 10, Abs. 2: Umfangreiche detaillierte BCM-Anforderungen, die über die Anforderungen der EBA-Leitlinien sowie die bereits ausführlichen Anforderungen der BAIT-Novelle hinausgehen. Die Verordnung sollte hier Prinzipienorientierung ermöglichen und nicht alle Details gesetzlich regeln.
- Artikel 10, Abs. 9: Kosten und Verluste lassen sich nicht bei jedem (Sicherheits)vorfall unmittelbar zuordnen bzw. berechnen. Auf ein Reporting sollte verzichtet werden.
- Artikel 10-12 umfassen ebenso wie Kapitel III (weitere) Anforderungen zum Umgang mit IKT-Vorfällen.
- Artikel 11, Abs. 5: Für IT-Dienstleister von Zentralverwahrern wird unabhängig von der Risikoeinschätzung von IT-Dienstleistern gefordert, eine redundante Betriebsumgebung bereitzustellen. Diese Forderung ist nicht risikoadäquat.
- Artikel 11, Abs. 6: Es wird zur Bestimmung der Wiederherstellungszeit für jede Funktion eine Auswirkungsanalyse gefordert. Dies sollte auf die geschäftskritischen Funktionen (nach Durchführung einer Business Impact Analyse) beschränkt werden.
- Artikel 12, Abs. 2: Auf dediziertes Reporting von implementierten Änderungen der Business Continuity Policy an die Aufsichtsbehörden sollte verzichtet werden.
- Artikel 13, Abs. 3: Eine aufeinander abgestimmte Kommunikation bei IKT-Vorfällen wird bereits von verschiedenen Instanzen entsprechend ihrer Funktion (operativ, Krisenkommunikation, Pressesprecher etc.) wahrgenommen, ein separater Kommunikationsbeauftragter bei IKT-Vorfällen sollte nicht gefordert werden.

Stellungnahme **Digital Finance Package der Europäischen Kommission - Legislativvorschlag „**proposal for a regulation on digital operational resilience for the financial sector" (DORA) vom 24.9.2020

## Kapitel III ICT-related Incidents

Die Anforderungen in diesem Kapitel in Artikel 15 doppeln sich in Teilen mit den Anforderungen aus Kapitel II, Artikel 12 und 13 erscheinen aber in der Detaillierungsebene vergleichsweise sachgerechter.

Wir begrüßen die Vereinheitlichung des Vorfallreportings in den Kapiteln 16 und 17. Bei der Einführung von Erheblichkeitsschwellen für die Meldung von Vorfällen durch RTS der ESAs sind zu starre Schwellwerte z.B. absolute Werte zu vermeiden. Alternativ empfehlen wir, die Wesentlichkeit auf den eigenen Umfang, das eigene Wirkungsraster und das eigene kritische Dienstleistungsprofil anzuwenden.

Die bestehenden Anforderungen an ein Vorfallreporting u.a. aus PSD2 und der NIS-Richtlinie sind bei der Vereinheitlichung des Reportings zu berücksichtigen und sind durch das neue Reporting vollständig abzudecken.

Bei der Evaluierung für eine zentrale EU-weite Meldestelle für schwerwiegende IKT-Vorfälle („single EU Hub for major ICT-related incident reporting by financial entities) ist das Risiko zu berücksichtigen, dass hierdurch ein Single Point of Compromise entsteht, der Begehrlichkeiten bei Angreifern wecken könnte.

## Kapitel IV Digital operational resilience testing

Die allgemeinen Anforderungen an alle Institute werden in Deutschland grundsätzlich bereits im Rahmen der Umsetzung der EBA-Leitlinie in der BAIT-Novelle aufgegriffen.

Der Legislativvorschlag geht darüber in Teilen hinaus:

- Artikel 21, Abs. 5 fordert ausdrücklich interne Validierungsmethoden von den Instituten, mit denen alle Schwachstellen und Gaps vollständig adressiert werden. Es sollten auch entsprechende Nachweise der IKT-Dienstleister anerkannt werden.
- Artikel 21, Abs. 6 fordert generell mindestens jährliche Tests aller kritischen IKT-Systeme.
- Artikel 22, Abs. 1 fordert die Nutzung der gesamten Breite der Testmethoden, während die EBA-Leitlinien und die BAIT eine Differenzierung nach Turnus, Art und Umfang zulassen. Die Überprüfung sollte sich insbesondere am Schutzbedarf und der potentiellen Angriffsfläche des IT-Systems orientieren.

Zu Artikel 23 „Advanced testing":

Threat led penetration Tests (TLPT) sind ein guter Baustein für einen effektiven Cybersecurity-Schutz und abhängig von der Kritikalität/ Bedeutung der IKT-Systeme zu befürworten, insbesondere für Systeme, die für die Versorgungssicherheit der Bevölkerung bzw. Finanzstabilität notwendig sind. Bei den Tests sollten vor allem die IKT-Systeme und deren Betreiber (z.B. Finanzinstitute, die Dienste für andere erbringen, zentrale IKT-Dienstleister) im Fokus stehen. Die in Abs. 3 aufgeführten Kriterien sind deshalb grundsätzlich nachvollziehbar.

Eine Wiederholung von TLPT in ca. einem 3-Jahresrhythmus gemäß Abs. 1 stellt eine realistische Zeitspanne dar, welche die Umsetzung von Maßnahmen auf Basis der Testergebnisse und den Test der Wirksamkeit dieser Maßnahmen ermöglicht.

Zu Abs. 2: Bei den Tests sollten die Auswirkungen auf die Sicherheit des Unternehmens und das Potenzial für Störungen berücksichtigt werden. Tests auf Live-Produktionssystemen sind kritisch mit Blick auf potenzielle negative Auswirkungen auf den Produktionsbetrieb bzw. können eine direkte Gefährdung des Bankgeschäfts sowie Haftungsrisiken bedeuten. Deshalb sollte das finale Testdesign immer von dem getesteten Unternehmen selbst festgelegt werden, da dieses haftet.

Auch wenn das Testing der relevanten IKT-Dienstleistungen die Teilnahme der entsprechenden Anbieter erfordert, sollte die Verantwortlichkeit dafür nicht bei den Finanzinstituten liegen. Da der tatsächliche Umfang des Testings durch die Aufsichtsbehörden validiert werden muss, besteht hier im Lichte der allgemein fehlenden Proportionalität im Entwurf das Risiko, dass Banken zu Erfüllungsgehilfen der Aufsicht gemacht werden, selbst in Fällen, in denen die IKT-Dienstleistung nicht kritisch für die Erbringung des zu testenden Prozesses ist oder in denen ein Testing Auswirkungen auf eine Vielzahl von Kunden haben könnte (bspw. im Bereich Public Cloud, IaaS / Saas).

Eine zentrale Sammlung von Dokumentationen von Schwachstellen im Detail sowie der etwaigen Maßnahmenpläne bei der Aufsicht oder bei Dritten erachten wir als nicht zielführend, da sich hierdurch das Risiko erhöht, dass Unberechtigte diese nutzen könnten (Risikokonzentration).

Zu Artikel 24 „Requirements for testers":

Eine mittelbare Risikokonzentration bei Red Teaming Dienstleistern sollte vermieden werden. Deshalb sollte auch die Verwendung eigener Red-Team-Ressourcen eines Unternehmens unterstützt werden. Dies würde dazu beitragen, Konzentrationsprobleme von Testexperten zu lösen und auch die Risikoexposition durch externe Tests zu verringern.

## Kapitel V Managing of ICT Third-Party Risk

### Section I Key Principles

Generell sollten die in den EBA-Leitlinien angelegten Erleichterungen zur Auslagerung durch Gruppen sowie Institute, die Mitglieder eines institutsbezogenen Sicherungssystems sind, auch auf das Management von durch Dritten erbrachten IKT-Dienstleitungen übertragen werden und eine zentralisierte operative Überwachung der IKT-Dienstleistungen ermöglicht werden.

Wir unterstützen ein proportionales Vorgehen beim Management der durch Dritte erbrachten IKT-Dienstleistungen wie in Artikel 25, Abs. 2 dargestellt. Die weiteren Anforderungen sollten dieses Prinzip berücksichtigen. Insbesondere sollte bei den Anforderungen unterscheiden werden, ob diese IKT kritische / wesentliche Funktionen unterstützt oder nicht.

Beispiele:

- Artikel 25, Abs. 4: Das geforderte Reporting an die Aufsichtsbehörden zu jeglichen Vereinbarungen mit IKT-Dienstleistern stellt ein neues Meldeverfahren dar. Dieses sollte angemessen umgesetzt werden, um unverhältnismäßig hohe Aufwände zu verhindern.
- Artikel 25, Abs. 5 und Artikel 26: Für einen Bezug von einmaligen, geringfügigen bzw. erkennbar unkritischen Dienstleistungen dürfen keine umfangreichen Bewertungen erforderlich sein.
- Artikel 25, Abs. 7: Bei Verträgen, denen keine kritischen IKT-Dienstleistungen zugrunde liegen, sollten nicht zwingend vertragliche Inspektions- und Auditbefugnisse vereinbart werden müssen.
- Artikel 25, Abs. 8: Die Vorschriften zur Vertragsbeendigung scheinen absolut und gehen über die Vorgaben aus den aktuell umgesetzten EBA Leitlinien hinaus. Insbesondere die Anforderungen an Finanzinstitute, Vertragsbeziehungen bei Verstößen gegen vertragliche Vereinbarungen zu beenden - ohne jede Wesentlichkeitsgrenze - erscheint als unverhältnismäßiger Eingriff in die Vertragsfreiheit. Nach unserem Verständnis muss hier gemeint sein, dass die Institute sicherstellen müssen in den gegebenen Fällen die Vertragsbeziehung ohne negative Konsequenzen beenden zu können. Grundsätzlich sollte in Absprache mit den betroffenen Instituten Mindestfristen vorgesehen werden, um eine Vertragsbeendigung vorzunehmen.
- Auch in den anderen genannten Fällen sollte berücksichtigt werden, wie wesentlich das Risiko ist und ob das auslagernde Institut u.U. mitigierende Maßnahmen implementiert hat, die das Risiko aus bspw. einer Ordnungswidrigkeit auf Seiten des IKT-Dienstleisters adressieren.
- Artikel 27: Vorgaben für Vertragsklauseln sollten nach Risikogehalt abgestuft werden. Die vorgelegten Anforderungen sollten nur für kritische IT-Dienstleistungen vollumfänglich zugrunde gelegt werden.

Zu Artikel 26 ICT concentration risk:

Eine Multi-Vendor-Strategie ist grundsätzlich weder notwendig noch zielführend, um Konzentrations- oder Lock-in-Risiken zu adressieren. Eine verpflichtende Multi-Vendor-Strategie birgt je nach Ausgestaltung das Risiko, dass insbesondere kleine Unternehmen, nicht in der Lage sein könnten, IKT-Dienstleister zu nutzen. Dieses Problem wird dadurch verstärkt, dass viele der Services, die extern bezogen werden, stark auf die individuellen Bedürfnisse des Finanzinstitutes zugeschnitten sind. Weiterhin sollte die Integration des Dienstleisters in das auslagernde Institut/Institutsgruppe berücksichtigt werden.

Unabhängig davon, ob die IKT-Dienstleistungen intern oder extern bezogen werden, erhöht insbesondere die Vorgabe eine Multi-Vendor-Strategie auf Ebene der Legaleinheit einzurichten, die Komplexität in Konzernen und reduziert den Mehrwert von zentralen Auslagerungsfunktionen in Institutsgruppen.

Deutlich zielführender wäre eine stärkere Fokussierung auf Standardisierung von Schnittstellen zwischen Dienstleistern um einen Wechsel zu erleichtern, falls und wo dieser notwendig und sinnvoll ist. Auf keinen Fall sollte die Verpflichtung für Finanzinstitute geschaffen werden, für jeden Service mehrere Anbieter parallel verpflichten zu müssen.

Eine entsprechend postulierte Multi-Vendor-Strategie in bestimmten Kernbereichen der IT würde andere, je nach Ausgestaltung auch deutlich höhere Risiken mit sich bringen. Zudem führt die Komplexität heutiger bankfachlicher Prozesse auch zu einer so hohen IT-Komplexität, die nur noch wenige IT-Dienstleister im Stand sind, jederzeit und skaliert für alle Instituts-Dimensionen effizient zu bewältigen. Aufgrund niedriger und qualitativ eingeschränkter Angebotsalternativen würde das Konzentrations-Problem nicht gelöst werden können, sondern neue Konzentrationsrisiken entstehen. Insgesamt würde sich das Gesamtrisiko-Portfolio deutlich erhöhen.

In Deutschland haben in den Finanzgruppen organisierte Banken und Sparkassen die Entwicklung und den Betrieb der IT zu großen Teilen an zentrale IT-Dienstleister der jeweiligen Finanzgruppe ausgelagert, die durch die Banken/Sparkassen gesteuert werden. Es handelt sich hierbei nicht um „klassische" Drittdiensteanbieter, vielmehr besteht eine funktionierende und resiliente Arbeitsteilung in der Digitalisierung. Diese Dienstleister sind direkt bzw. indirekt im Besitz der Banken und Sparkassen, so dass die Banken ihre Anforderungen über standard-vertragliche Formen hinausgehend geltend machen können. Auch wenn die Auslagerung relevanter Bereiche der IT auf einen Dienstleister eine Konzentration mit sich bringt, bringt diese Auslagerung an einen Full-Service-Dienstleister immer auch Vorteile wie Erhöhung des Standardisierungsgrads, der technischen Professionalität und damit einhergehende Risikominderung. Die Umsetzung des Legislativvorschlags darf nicht die Strukturen der Sparkassen- und genossenschaftlichen Finanzgruppe gefährden, da dies erhebliche negative Folgen für die nationale Finanzmarkstabilität hätte.

## Section II Oversight Framework of Critical ICT Third-Party Service Providers

Der Legislativvorschlag sieht eine hauptverantwortliche Aufsichtsinstanz für jeden kritischen IKT-Drittdiensteanbieter vor. Es handelt sich um einen komplett neuen Ansatz zur Beaufsichtigung von IT-Dienstleistern. Im Fokus sollten aus Sicht der Finanzinstitute insbesondere solche internationalen IKT-Dienstleister stehen, bei denen die Durchsetzbarkeit von Prüfungen auf Ebene des einzelnen Finanzinstituts in ausreichendem Maße nicht gewährleistet werden kann. Insgesamt muss dies mit Erleichterungen bei der Überwachung und Nachweiserbringung aufsichtsrechtlicher Anforderungskonformität dieser IKT-Dienstleister durch die Finanzinstitute verknüpft werden und die Nutzung dieser Dienstleister sollte nicht durch zu limitierende Vorgaben erschwert werden. Daher sehen wir die Notwendigkeit, die vorgeschlagenen Anforderungen in diesem Kapitel, aber auch im Kapitel IKT-Drittdienstanbieter-Risikomanagement allgemein mit Blick auf die Notwendigkeit und Zielgerichtetheit genau zu prüfen.

Als Kriterium für eine Beaufsichtigung durch eine europäische Aufsichtsbehörde sollte als Mindestbedingung gelten, dass der IKT-Dienstleister in mehreren Mitgliedstaaten für Finanzinstitute gemäß Kriterien aus Artikel 28, Abs. 2 tätig ist. Für überwiegend national tätige bedeutende IKT-Dienstleister sollte weiterhin eine Prüfung durch nationale Aufsichtsbehörden erfolgen, da diese die nationalen Gegebenheiten genauestens kennen.

Der folgende Aspekt aus dem Oversight Framework birgt erhebliche Risiken für die Finanzinstitute:

Zu Artikel 37, Abs. 3: Die Aufforderung durch Aufsichtsbehörden, Verträge zwischen Finanzinstituten und IKT-Dienstleistern vorübergehend vollständig oder teilweise zu suspendieren, bzw. vollständig oder teilweise zu beenden, erfordert eine enge vorangehende Abstimmung mit den betroffenen Finanzinstituten. Vorrangig sollte in Betracht gezogen werden, ob Sicherheits- und Risikoreduzierungsmaßnahmen durch die betroffenen Finanzinstitute installiert werden können, die die bestehenden Risiken adressieren. Darüber hinaus ist ein ausreichender zeitlicher Vorlauf für die betroffenen Institute notwendig.