

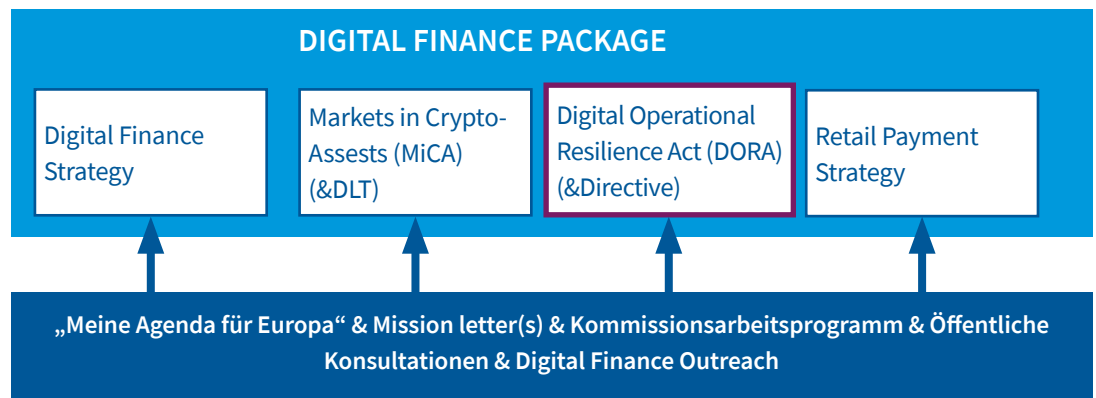
AUF EINEN BLICK

01.2021



DIGITAL OPERATIONAL RESILIENCE (DORA, 2020/0266(COD))

Ende September 2020 hat die Europäische Kommission ihr „Digital Finance Package“ veröffentlicht. Dieses Paket beinhaltet u.a. den Gesetzesentwurf zur Harmonisierung und Verbesserung der digitalen Resilienz im Finanzsektor (Digital Operational Resilience for the Financial Sector, DORA). Über den Legislativvorschlag wird seitdem im Europäischen Parlament und Rat beraten. Eine Beschlussfassung ist noch im Jahr 2021 zu erwarten. Inkrafttreten soll die Verordnung 2022. Im Anschluss ist eine Konkretisierung durch Regulatory Technical Standards (RTS) vorgesehen.



Gesetzesentwurf DORA im Digital Finance Package der EU- Kommission (vereinfachte Darstellung)

Was soll mit DORA erreicht werden?

Mit DORA schlägt die Europäische Kommission eine Harmonisierung der Rahmenbedingungen der digitalen betrieblichen Widerstandsfähigkeit von Banken und Dienstleistern (z.B. Clouddienstleister) im Finanzsektor vor und stellt dabei Anforderungen insbesondere in folgenden Bereichen:

- Risikomanagement bei Informations- und Kommunikationstechnologien (IKT) inkl. Testen der digitalen operationalen Resilienz und Drittparteienrisikomanagement;
- Meldepflichten bei schwerwiegenden IKT-Vorfällen;
- Umgang mit IKT-Drittanbieter-Risiken;
- Aufsichtsrahmen für kritische IKT-Drittdienstleister mit Neuaufstellung der Aufsichtsbehörden.

Mit DORA und der zugehörigen Richtlinie (2020/0268(COD)) sollen insgesamt weite Teile der Europäischen Finanzmarktregulierung überarbeitet werden; es sollen vier Verordnungen (u.a. EMIR), acht Richtlinien (u.a. CRD, MiFID & PSD2) sowie zahlreiche Durchführungsrechtsakte sowie delegierte Rechtsakte abgeändert bzw. erlassen werden.

Unsere Position

Wie bewerten wir DORA?

Grundsätzlich unterstützen wir den Harmonisierungsansatz der Europäischen Kommission. Zugleich gehen wir davon aus, dass in Folge der umfangreichen sowie sehr detaillierten Regelungen von DORA und der geplanten Umsetzung durch die europäischen Aufsichtsbehörden grundlegende strukturelle Änderungen in der Aufsichtsführung und -praxis auf europäischer und nationaler Ebene zu erwarten sind.

Daraus resultierende Auswirkungen auf die Finanzmarktinfrastrukturen und -akteure schätzen wir als grundlegend ein. Hier wird es auf eine proportionale Ausgestaltung der Anforderungen ankommen.

Die Schaffung eines Aufsichtsrahmens und die geplante Beaufsichtigung kritischer IKT-Dienstleister auf Basis einheitlicher Standards und optionaler Zertifizierung können zu einer dringend notwendigen Entlastung von Banken bei der Erfüllung aufsichtsrechtlicher Anforderungen (u.a. durch eine Reduzierung des Aufwands in der Dienstleistersteuerung, dem Management von Drittrisiken und der Reduzierung von Auditpflichten) führen. Insgesamt sollte eine prinzipienbasierte Regulierung erfolgen, die den Umgang mit unterschiedlichen Risikoprofilen ermöglicht und keinerlei Nachjustieren einzelner Regelungen im Zuge von Weiterentwicklungen erfordert.

Wo sehen wir weiteren Handlungsbedarf?

Ausnahmeregelungen für kleine Banken erforderlich

Vergleichsweise geringere Anforderungen an das IKT-Risikomanagement sind nach DORA für sog. „Microenterprises“ (mit bis zu 10 Mitarbeitern) vorgesehen. Kleinere Kreditinstitute fallen somit aktuell nicht unter diese Ausnahmeregelungen. Der Geltungskreis der Ausnahmeregelungen sollte unter dem Aspekt der Verhältnismäßigkeit überprüft und angepasst werden. Dies ist nicht zuletzt auch für einen fairen Wettbewerb unerlässlich.

Verpflichtende Vertragsauflösungen und „Multi-Vendor-Strategie“ bergen hohe Risiken

Vorgesehen sind u.a. verpflichtende Auflösungen von Verträgen mit Dienstleistern unter bestimmten Bedingungen (z.B. bei Verlust der Aufsichtsmöglichkeit). Eine verpflichtende Vertragsauflösung kann mit erheblichen Risiken verbunden sein. Ebenso wenig praktikabel erscheint die vorgesehene Verpflichtung, Alternativen für den Fall eines erforderlichen Dienstleisterwechsels im Rahmen einer „Multi-Vendor-Strategie“ aktiv vorzuhalten. Dies sollte auf mögliche negative Folgen hin überprüft und entsprechend angepasst werden.

Aufsichtsrahmen für IKT-Dienstleister: Fokus auf internationale Dienstleister erforderlich

Mit DORA soll ein europäischer Aufsichtsrahmen für IKT-Drittdienstleister wie Cloud-Diensteanbieter geschaffen werden. Dabei sollten große, international agierende Cloud-Dienstleister im Fokus stehen. Die Prüfung überwiegend national tätiger IKT-Dienstleister sollte weiterhin durch nationale Aufsichtsbe-

hörden erfolgen, da diese die nationalen Gegebenheiten kennen und bewerten können. Das Verständnis zum Gesetzentwurf sollte dahingehend geschärft werden. Wir unterstützen im Zusammenhang eine standardbasierte optionale Zertifizierung von Cloud-Dienstleistern, um die Institute beim Nachweis der Konformität zu gesetzlichen und aufsichtsrechtlichen Anforderungen zu entlasten.

Echte Harmonisierung des Meldewesens ohne Überschneidungen der Regelungen und Meldewege
DORA sieht konkrete Verpflichtungen zur Meldung von schwerwiegenden IKT-Sicherheitsvorfällen vor. Im Gesetzesentwurf sollte sichergestellt werden, dass dies auf Basis einheitlicher Rahmenbedingungen mit abgestimmtem Vorgehen erfolgt. Eine weitergehende Fragmentierung des europäischen Meldewesens sollte unbedingt vermieden werden. Besonders wichtig ist auch, dass im Zuge der Anwendung von DORA als „Lex Specialis“ keine Doppel- oder Mehrfachmeldungen erforderlich sind und Meldungen von Banken oder durch beauftragte IKT-Dienstleister erfolgen können.

Für weitere Informationen oder Rückfragen wenden Sie sich gerne an:

oliver.psyk@voeb.de (+49 30 81 92 204) marcus.scheidl@voeb.de (+49 30 8192 187).

Der Bundesverband Öffentlicher Banken Deutschlands, VÖB, ist ein Spitzenverband der deutschen Kreditwirtschaft. Er vertritt die Interessen von 59 Mitgliedern, darunter die Landesbanken sowie die Förderbanken des Bundes und der Länder. Die Mitgliedsinstitute des VÖB haben eine Bilanzsumme von rund 2.900 Milliarden Euro und bilden damit etwa ein Drittel des deutschen Bankenmarktes ab. Die öffentlichen Banken nehmen ihre Verantwortung für Mittelstand, Unternehmen, die öffentliche Hand und Privatkunden wahr und sind in allen Teilen Deutschlands fest in ihren Heimatregionen verwurzelt. www.voeb.de