Sie wollen mehr Informationen?
Dann schauen Sie auch in unsere

Wissensdatenbank!

www.wko.at/wissensdatenbank oder www.wko.at/wdb

Fachverband Finanzdienstleister
Bundessparte Information und Consulting
Wirtschaftskammer Österreich
Wiedner Hauptstraße 63 | 1045 Wien
T 05 90 900-4818 | F 05 90 900-4817
E finanzdienstleister@wko.at
W http://wko.at/finanzdienstleister

Datum

19.2.2021

Digital Operational Resilience Act (DORA)
Teil des EU-Rahmenwerks „Digital Finance Package“

Index

1. Digital Finance Package

Fragen:
1. Was regelt das Digital Finance Package?

Die Europäische Kommission hat am 24.9.2020 das „Digital Finance Packages“ vorgestellt, das bisher ungeregelte innovative Bereiche am Finanzdienstleistungsmarkt regeln soll. Es soll einerseits die Wettbewerbsfähigkeit anderseits die Innovation am Finanzsektor fördern und damit auch eine internationale Voreiterrolle darstellen.

Das Digital Finance Package beinhaltet folgende vier Bereiche:

- **Digitale Finance Strategy (Strategie zur Digitalisierung des Finanzsektors):**
  Ziel ist es, eine neuen europäischen Finanzdatenraum zu schaffen, neue Wege zur Bereitstellung von Finanzmitteln für KMU sowie bessere Finanzprodukte für Verbraucher anzubieten.

- **Retail Payments Strategy (Strategie für den Massenzahlungsverkehr):**
  Mit dieser Strategie sollen europäischen Bürgern und Unternehmen sichere, schnelle und zuverlässige Zahlungsdienste zur Verfügung gestellt werden, welche modern, kostengünstig sein sollen (in Form eines vollständig integrierten Zahlungssystems für Privatkunden in der EU, einschließlich sofortiger grenzüberschreitender Zahlungslösungen).

- **Legislativpaket zu Markets in Crypto Assets (MiCA); Legislativvorschläge für einen EU-Rechtsrahmen für Kryptowerte):**
  Dieser Vorschlag soll jene Kryptowerte regeln, die bisher keinen Bestimmungen unterlegen sind, stellt Emittenten unter strenge Anforderungen, und schafft insbesondere Sicherheitsvorkehrungen (Eigenkapitalanforderungen, Verwahrung von Vermögenswerten, Beschwerdeverfahren etc.). Auch ein White-Paper für Kryptowerte wird eingeführt. Zusätzlich ergeht ein Vorschlag für eine Pilotregelung für Marktinfrastrukturen, mit denen angestrebt wird, Transaktionen mit Finanzinstrumenten in Form von Kryptowerten zu tätigen und abzuwickeln.

- **Legislativpaket zu Digital Operational Resilience Act (DORA, Vorschlag für eine Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors):**
  Die Verordnung soll sicherstellen, dass alle Teilnehmer am Finanzsystem über die erforderlichen Sicherheitsvorkehrungen verfügen, um Cyber-Angriffe und andere Risiken zu mindern. Die Risikoanforderungen für Informations- und Kommunikationstechnologie (IKT) im gesamten Finanzsektor sollen konsolidiert und verbessert werden.

Hinweis:
Der folgende Artikel soll einen ersten Überblick auf den Digital Operational Resilience Act (DORA) geben.

2. Legislativpaket zu Digital Operational Resilience Act (DORA)

Fragen:
2. Was ist DORA?
3. Was ist dort geregelt?

Ziel des Vorschlags der Europäischen Kommission für einen „Digital Operational Resilience Act“ (DORA)[1] ist es sicherzustellen, dass alle Teilnehmer am Finanzsystem über die erforderlichen Sicherheitsvorkehrungen verfügen, um Cyber-Angriffe und andere Risiken zu mindern. Die Risikoanforderungen für Informations- und Kommunikationstechnologie (IKT) im gesamten Finanzsektor sollen konsolidiert und verbessert werden.

Nach den vorgeschlagenen Regeln müssen alle Finanzunternehmen strenge gemeinsame Standards einhalten, um sicherzustellen, dass sie IKT-bedingten Störungen und Bedrohungen standhalten können. Dafür sollen folgende Maßnahmen von den Unternehmen ergriffen werden:

- taugliche IKT-Risikomanagementfunktionen,
- harmonisierte Berichterstattung über wichtige IKT-Vorfälle,
- Prüfung der digitalen Betriebsstabilität,
- Management des IKT-Drittrisikos durch Finanzunternehmen,
- Informationsaustausch zwischen Finanzunternehmen.

Vor diesem Hintergrund schlägt die Kommission auch Änderungen der Solvency II-, AIFMD, IORP, MiFID II, PSD II und der CRD IV vor, um bestimmte Bestimmungen in diesen bereits bestehenden Finanzdienstleistungsrichtlinien zu präzisieren. Betreffend IDD werden keine Änderungen vorgeschlagen.

Der Vorschlag für DORA besteht aus den folgenden Kapiteln:

- Kapitel 1 – Allgemeine Bestimmungen (insbesondere Anwendungsbereich, Definitionen)
- Kapitel 2 - IKT-Risikomanagement
- Kapitel 3 – Management, Klassifizierung und Berichterstattung von IKT-Vorfällen
- Kapitel 4 - Regelungen für die Testung der IKT-Systeme
- Kapitel 5 – Risikomanagement von IKT-Drittanbietern
- Kapitel 6 –Informationsaustausch
- Kapitel 7 – zuständige Aufsicht
- Kapitel 8 – Delegierte Rechtsakte
- Kapitel 9 – Übergangs- und Schlussbestimmungen

2.1. Kapitel 1 – Allgemeine Bestimmungen - Anwendungsbereich

Der Entwurf spricht von der Anwendbarkeit auf „Finanzunternehmen“ und „IKT-Drittparteianbietern“.[2] Neben Banken und Versicherungen fallen mehrere Berufsgruppen der Finanzdienstleister unter den Begriff „Finanzunternehmen“, darunter Wertpapierfirmen, Gewerbliche Vermögensberater als Versicherungsvermittler, Schwarmfinanzierungsdienstleister sowie Zahlungsdienstleister.[3] Das heißt, dass diese Berufsgruppen von den Bestimmungen betroffen sind.

[1] Der Link zum Verordnungs-Vorschlag findet sich am Ende des Rechtsartikels.
[2] Art. 2 Abs 2 DORA.
[3] Art. 2 DORA.

2.2. Kapitel 2-4 IKT-Risikomanagement, Berichterstattung und Testung

Hier sind umfangreiche administrative Anforderungen an das Management und die Organisationsstrukturen der Unternehmen geregelt.

Finanzunternehmen sollen über einen „geeigneten Rahmen" an IKT-Risikomanagementwerkzeugen, ausreichend Kapazitäten und Ressourcen verfügen und protokollieren, um den Aufsichtsbehörden darüber zu berichten. Dafür muss im Unternehmen eine eigene verantwortliche Stelle eingerichtet sein.

In regelmäßigen Abständen – mindestens einmal pro Jahr müssen die Systeme anhand des Regelwerks getestet werden, dabei müssen verschiedene mögliche Bedrohungsszenarien simuliert werden was auch umfangreich protokolliert werden muss. Präventionsmaßnahmen sind zu setzen, beispielsweise zur Erkennung und Entdeckung von Bedrohungen sowie Regelungen zu Backupmaßnahmen sind enthalten.

Mögliche Vorfälle bzw Störungen sind in Klassen einzuteilen (wieviele Betroffene, in welchem Gebiet, welche Daten betroffen, etc.)

Die Dokumentation und Berichterstattung soll nach festgeschriebenen Standards erfolgen.

Die Testung der Systeme ist ebenfalls zu klassifizieren und alle drei Jahre müssen größere Tests stattfinden, für die eigene „Tester" benötigt werden.

Im Entwurf ist vorgesehen, dass die meisten Anforderungen für Finanzinstitute aller Größen gelten: vom systemrelevanten Kreditinstitut bis hin zum Gewerblichen Vermögensberater als Versicherungsvermittler. Lediglich für Kleinstunternehmen[4] („microenterprises" – also Unternehmen, die weniger als 10 Personen beschäftigen und deren Jahresumsatz bzw. Jahresbilanz weniger als 2 Mio. EUR beträgt) sind folgende Erleichterungen vorgesehen:

- Ausnahme von der Einrichtung eines eigenen „IKT-Verantwortlichen",[5]
- keine Implementierung von international standardisierten IKT-Managementsystemen und keine Trennung von IKT-Management, Kontrolle und interner Revision,[6]
- keine Risikobewertung für wesentliche Änderungen der Netzwerk- und Informationssysteminfrastruktur und keine mindestens jährliche IKT-Risikobewertung für alle älteren IKT-Systeme,[7]
- keine unabhängige Prüfung des IKT-Notfallwiederherstellungsplans, weniger umfangreiche Test-Szenarien, keine Einrichtung eines eigenen Krisenmanagements und keine Berichterstattung an die Aufsichtsbehörden über die Kosten von IKT-Störungen bzw. Ausfällen,[8]
- keine Meldung an die Aufsichtsbehörde bei Systemänderungen[9].

2.3. Kapitel 5 - Risikomanagement von IKT-Drittanbietern

Hier befinden sich Regelungen zum Risikomanagement von IKT-Dienstleistern, insbesondere auch zur Prüfung der Auslagerungsverträge. Die Verantwortung bleibt jedoch immer beim Finanzunternehmen

[4] Art. 3 Abs 50 DORA *'microenterprise' means a financial entity as defined in Article 2(3) of the Annex to Recommendation 2003/361/EC.*
[5] Art. 4 Abs 3 DORA
[6] Art. 5 Abs 4 und 5 DORA.
[7] Art. 7 Abs 3 und 7 DORA.
[8] Art. 10 Abs 3, 5, 6 und 9 DORA.
[9] Art. 12 Abs 2 DORA.

Im zweiten Teil des Kapitels soll ein europäischer Aufsichtsrahmen für kritische IKT-Drittparteianbieter (wie Big Techs) geschaffen werden, die für Finanzinstitute digitale Dienstleistungen (zB Cloud Computing) erbringen. Zuständig sollen die Europäischen Aufsichtsbehörden EIOPA, EBA und ESMA sein. diese sollen das Recht haben, auf Dokumente zuzugreifen und Vor-Ort-Prüfungen durchzuführen und die Befugnis erhalten, Empfehlungen und Anweisungen auszusprechen, Abhilfemaßnahmen zu verlangen oder Vereinbarungen zu treffen, die sich auf die Stabilität des Finanzunternehmens oder des Finanzsystems auswirken.

Mit diesem Aufsichtsrahmen soll auch ein Mechanismus zur Bestimmung kritischer IKT-Drittparteianbieter eingerichtet werden, der die Dimension und Art der Abhängigkeit des Finanzsektors von Diensten berücksichtigt, die von IKT-Dienstleistern bereitgestellt werden.[10]

2.1. Kapitel 6 – Informationsaustausch

Das Kapitel beinhaltet Regelungen zum Informationsaustausch über Cyber-Bedrohungen und wie Vereinbarungen dazu gestaltet sein müssen[11].

2.2. Kapitel 7 – Zuständige Aufsicht

Für die Durchsetzung des geplanten Regelwerks sollen die Aufsichtsbehörden zuständig sein, die bereits jetzt für die Aufsicht der im Anwendungsbereich befindlichen Unternehmen zuständig sind. In Österreich daher für Wertpapierfirmen die österreichische Finanzmarktaufsicht FMA und für Versicherungsvermittler die Gewerbebehörden.
Den Mitgliedstaaten wird eingeräumt, bei Verstößen gegen die Verordnung neben Verwaltungsstrafen auch gerichtliche Strafen zu normieren. Das lehnen wir ab, da es sich um administrative Maßnahmen handelt, sollen eventuelle Verstöße ausschließlich verwaltungsrechtliche Konsequenzen nach sich ziehen.

2.3. Kapitel 8 - Delegierte Rechtsakte

Der Entwurf enthält zahlreiche Ermächtigungen für delegierte Rechtsakte. Diese technischen Details werden für die Normunterworfenen gerade in der Einhaltung und Umsetzung der künftigen Verordnung entscheidend sein.

3. Kritikpunkte zu DORA

Fragen:
4. Was ist kritisch zu sehen?

Das Ziel des Entwurfs, das IKT-Risikomanagement von Finanzinstituten zu vereinheitlichen, wird grundsätzlich begrüßt. Wir halten die gegenständlichen Inhalte allerdings nicht für geeignet, das Ziel zu verwirklichen.

3.1. Proportionalität

Der Entwurf wirft eine Vielzahl von Fragen auf – insbesondere zur Verhältnismäßigkeit und Risikobasiertheit der umfangreichen administrativen und technischen Vorgaben, deren Einhaltung insbesondere KMU vor signifikante finanzielle, operative und technische

[10] Art. 28ff DORA.
[11] Art. 40 DORA.

Herausforderungen stellen würde und die in der aktuellen Ausgestaltung eine unverhältnismäßige Belastung darstellen.[12.]

Wir setzen uns dafür ein, die Ausnahmen für Kleinstunternehmen sehr stark zu erweitern – oder diese gänzlich aus dem Anwendungsbereich der Verordnung zu streichen. Sollte das nicht möglich sein, so ist jedenfalls die Anwendung der Kapitel drei („Management, Klassifizierung und Berichterstattung von IKT-Vorfällen“) und vier (Regelungen für die Testung der IKT-Systeme) für Kleinstunternehmen praktisch nicht denkbar.

Denkbar wäre eine Differenzierung auf zwei Ebenen: Einerseits sollte die Verordnung eine grundsätzliche Unterscheidung auf Basis unterschiedlicher Verpflichteter bzw. deren Größe vornehmen (vergleichbar mit dem Konzept systemrelevanter Kreditinstitute nach CRD IV) und andererseits sollte die Verordnung eine klare Definition kritischer Dienste/Funktionen enthalten, für die allenfalls ein strengeres Regime gelten soll.

Kritische Dienste könnten etwa anhand unterschiedlicher Kriterien, wie etwa das Halten von Kundengeldern oder sonstiger Assets, oder die (grenzüberschreitende) Verflechtung mit dem Finanzsystem, identifiziert werden. Somit könnten, zusätzlich zur Einstufung von „microenterprises“, weitere Klassifizierungen von Dienstleistern vorgenommen werden und in weiterer Folge eine Teil- bzw. Vollanwendung von (gewissen) Kapiteln oder Einzelbestimmungen für unterschiedliche Dienste bzw. Dienstleister vorgesehen werden.

Wie die Regelungen bezüglich der Drittparteianbieter in der Praxis funktionieren sollen, ist schwer nachvollziehbar: Die Verantwortung für die Sicherheit der IKT Systeme liegt beim jeweiligen Unternehmen, das auch den Dienstleister prüfen muss. Sollen große multinationale IT-Konzerne (wie zB Microsoft, Amazon AWS und Co) durch deren Auftraggeber – in Österreich zumeist kleine Unternehmen - geprüft werden?

3.2. Hoher bürokratischer Aufwand

Insgesamt scheint es, dass den Verfassern eine "Papier-Compliance" vorschwebt, deren ständige Aktualisierung viele Ressourcen in den Unternehmen bindet. Diese Ressourcen fehlen dann bei der praktischen Überwachung und der Verteidigung des Netzwerks und der IT-Systeme. Eine solche Compliance ist gerade für kleine Unternehmen bzw. EPUs, wie zB Gewerbliche Vermögensberater oder Versicherungsvermittler, praktisch nicht bewältigbar.

3.3. Zu viele Delegierte Rechtsakte

Die Verhältnismäßigkeit und Risikobasiertheit des DORA-Regimes sollte soweit wie möglich direkt auf Ebene der Verordnung sichergestellt werden und eine weitere Konkretisierung auf Level-2 und -3 nur in jenen Bereichen vorgenommen werden, wo eine Klarstellung/Definition konkreter technischer Vorgaben unbedingt notwendig ist.

Die technischen Details sollten so weit möglich gleich von Beginn weg klar definiert sein, damit Rechtssicherheit herrscht.

3.4. Fehlende Abstimmung zu anderen Regelungen

In diesem Zusammenhang möchten wir insbesondere festhalten, dass der gegenständliche Entwurf aus unserer Sicht nur unzureichend auf den ebenfalls im Rahmen des „Digital Finance Packages“ vorgestellten Verordnungsentwurf für Market in Crypto-Assets (MiCA), sowohl inhaltlich als auch zeitlich, abgestimmt ist.

[12] Das steht zusätzlich im Gegensatz zur Folgenabschätzung – Zitat von S. 6 des Vorschlag-Dokuments: *The proposal will bring clarity to SMEs on what rules apply, which will reduce compliance costs.*

3.5. Fazit

Zusammenfassend ist zu sagen, dass der gegenständliche Entwurf in der vorliegenden Form seine Ziele verfehlt und daher abgelehnt wird. Der Fachverband Finanzdienstleister wird sich vehement für Verbesserungen einsetzen.

Autor:
Mag. Dagmar Hartl-Frank, Referentin des Fachverbands Finanzdienstleister (WKÖ)

Links

[1] COM(2020) 591 final - Strategie für ein digitales Finanzwesen in der EU
[2] COM(2020) 592 final - EU-Strategie für den Massenzahlungsverkehr (Retail Payments Strategy)
[3] COM(2020) 593 final – Legislativvorschlag zu Markets in Crypto-Assets + Anhang
[4] COM(2020) 594 final - pilot regime for for market infrastructures based on distributed ledger technology
[5] COM(2020) 595 final – legislative proposal on digital operational resilience
[6] COM(2020) 596 final – legislative proposal amending the existing financial services directives with regards to digital resilience