FMA

Finanzmarktaufsicht
Liechtenstein

Regierung des Fürstentums Liechtenstein
Ministerium für Präsidiales und Finanzen
Regierungsgebäude
Peter-Kaiser-Platz 1
Postfach 468
9490 Vaduz

Einheit Stabsstelle Strategische Grundlagen, Abteilung Recht und Internationale Angelegenheiten
Kontakt Nadja Rossettini
Direkt +423 236 76 19
E-Mail nadja.rossettini@fma-li.li
Vaduz 28. September 2022

Vernehmlassungsbericht der Regierung betreffend die Schaffung eines Gesetzes über Cybersicherheit (Cybersicherheitsgesetz; CSG)

Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Juli 2022 wurde die Finanzmarktaufsicht (FMA) Liechtenstein eingeladen, zu dem im Betreff genannten Vernehmlassungsbericht Stellung zu nehmen.

Die FMA begrüsst und unterstützt die gegenständliche Vorlage und hat diesbezüglich informell bereits Kontakt mit der Stabsstelle Cyber-Sicherheit aufgenommen, um eine enge Abstimmung in diesem Bereich sicherzustellen.

Generell ist anzumerken, dass die gegenständliche Vorlage der Umsetzung der ersten Netz- und Informationssicherheitsrichtlinie, der sogenannten NIS-Richtline 2016/1148 vom 6. Juli 2016, dient, während auf EU-Ebene der Gesetzgebungsprozess für deren Nachfolgerichtlinie, der sogenannten NIS 2-Richtlinie, bereits weit fortgeschritten ist (politische Einigung erzielt). Aus Sicht des Finanzmarktbereichs ist zudem die im EU-Gesetzgebungsprozess kurz vor der Verabschiedung stehende Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (die sogenannte DORA) zu erwähnen. Dies ist deshalb wichtig, weil der EU-Gesetzgeber erst im Rahmen dieser zwei neuen Regelwerke für eine bessere Kohärenz zwischen den Vorschriften sorgt und entsprechende Rechtsklarheit schafft. Im Lichte dessen sollte allenfalls bereits jetzt geprüft werden, inwieweit gewisse, zumindest klarstellende, Elemente aus diesen künftigen EU-Rechtsakten in der gegenständliche Vorlage berücksichtigt werden könnten.

Geltungsbereich (Gegenstand)

Die FMA empfiehlt klarzustellen, dass die Betreiber die Einhaltung der in der Vorlage vorgesehenen Anforderungen auch für den Fall der Liquidation und/oder Abwicklung nach dem Gesetz über die Sanierung und Abwicklung von Banken und Wertpapierfirmen (SAG) sicherzustellen haben, etwa über spezifische Vertragsklauseln. Jüngste Erfahrungen im EWR haben gezeigt, dass in einem solchen Szenario externe IT-Anbieter ihre Dienstleistungsverträge (SaaS) unverzüglich kündigen und eine angemessene IT-Infrastruktur nicht mehr gewährleistet werden kann.

Spezialgesetzlicher Vorrang

Die FMA erachtet es als notwendig, den Wortlaut des Art. 4 Abs. 3 der Vorlage anzupassen. Die Bestimmung in ihrer jetzigen Form ("bleiben unberührt") kann so verstanden werden, dass das CSG und spezialgesetzliche Bestimmungen nebeneinander zur Anwendung kommen. Die NIS-Richtlinie statuiert hingegen in Art. 1(7) einen klaren Vorrang sektorspezifischer Bestimmungen. In Erwägungsgrund (9) der Richtlinie wird dazu insbesondere ausgeführt:

"Wann immer [...] Unionsrechtsakte Bestimmungen enthalten, mit denen Anforderungen in Bezug auf die Sicherheit von Netz- und Informationssystemen oder die Meldung von Sicherheitsvorfällen auferlegt werden, sollten diese Bestimmungen gelten, wenn sie Anforderungen vorsehen, die hinsichtlich ihrer Wirkung [...] mindestens gleichwertig sind. Die Mitgliedstaaten sollten dann die Bestimmungen des betreffenden sektorspezifischen Unionsrechtsakts anwenden [...] und nicht das in dieser Richtlinie festgelegte Verfahren zur Ermittlung der Betreiber wesentlicher Dienste durchführen."

Der Vorrang spezialgesetzlicher, in ihrer Wirkung gleichwertiger Bestimmungen bezieht sich dabei nicht nur auf Sicherheitsvorgaben, sondern auch auf Meldungen von Sicherheitsvorfällen, sodass ein entsprechender spezialgesetzlicher Vorrang auch im Hinblick auf Art. 5 der Vorlage (Meldepflicht für Betreiber wesentlicher Dienste) geprüft werden sollte. Die in den Erläuterungen zu Art. 4 Abs. 3 getroffene Aussage, dass die Meldepflichten vom spezialgesetzlichen Vorrang unberührt bleiben, scheint indessen im Widerspruch zur NIS-Richtlinie zu stehen.

Aus finanzmarktrechtlicher Sicht ist dies insbesondere deshalb wichtig, weil die Regulierung und Aufsicht in den Sektoren der Banken- und Finanzmarktinfrastrukturen durch EWR-Rechtsakte sowie gemeinsam mit den Europäischen Aufsichtsbehörden ausgearbeiteten Normen in hohem Masse harmonisiert sind und von den nationalen Finanzmarktaufsichtsbehörden beaufsichtigt werden. So anerkennt die NIS-Richtlinie in Erwägungsgrund (13) ausdrücklich, dass das operationelle Risiko einen grossen Teil der Aufsichtsvorschriften und der Kontrolle in den Sektoren Banken- und Finanzmarktinfrastrukturen ausmacht, davon sämtliche Tätigkeiten, einschliesslich der Sicherheit, Integrität und Robustheit von Netz- und Informationssystemen, erfasst sind und die Anforderungen oft über die Anforderungen der NIS-Richtlinie hinausgehen. Dem sollen die Mitgliedstaaten Rechnung tragen.

Die NIS-2-Richtlinie und DORA werden dem, wie einleitend erwähnt, besser Rechnung tragen und es ist empfehlenswert zu prüfen, inwieweit dies bereits zum heutigen Zeitpunkt berücksichtigt werden könnte. DORA hält in Erwägungsgrund (16) ausdrücklich fest, dass sie eine *lex specialis* zur NIS-2-Richtlinie darstellt

<u>Meldepflichten</u>

Wie oben erwähnt, statuiert die NIS-Richtlinie einen spezialgesetzlichen Vorrang auch im Hinblick auf die Meldung von Sicherheitsvorfällen. Dies sollte in der Vorlage berücksichtigt werden.

Aus finanzmarktrechtlicher Sicht möchte die FMA in diesem Zusammenhang ausdrücklich auf die FMA-Richtlinie 2021/3 zur Überwachung von Risiken beim Einsatz von Informations- und Kommunikationstechnologie (sogenannte IKT-Richtlinie) hinweisen. Mit der Richtlinie stärkt die FMA die Sicherheit des Finanzsektors und definiert entsprechend den internationalen Standards die Anforderungen, die Finanzintermediäre im Umgang mit IKT-Risiken erfüllen müssen. Die IKT-Richtlinie sieht eine Meldepflicht (einschliesslich eines entsprechenden Meldeformulars) für sämtliche von der FMA beaufsichtigten Finanzintermediäre vor, allerdings nur im Hinblick auf schwerwiegende oder betriebsstörende Cyber-Attacken. Insofern geht das CSG nach dem Verständnis der FMA weiter als die FMA-Richtlinie. Doppelspurigkeiten könnten sich aber für solche Intermediäre ergeben, die sowohl unter die IKT-Richtlinie als auch unter das künftige CSG fallen, soweit es um schwerwiegende oder betriebsstörende Sicherheitsvorfälle geht. Im Hinblick auf die Meldepflicht und das Meldeformular für solche Fälle wäre es aus Sicht der FMA jedenfalls wünschenswert, Doppelspurigkeiten so weit wie möglich zu vermeiden bzw. im günstigsten Fall eine zentrale Meldepflicht bzw. -stelle sowie ein Meldeformat zu schaffen.

Dies wäre auch im Sinne der künftig geltenden DORA, welche zum Ziel hat, Meldungen IKT-bezogener Vorfälle zu straffen und sich überschneidende Meldepflichten zu beseitigen. In Erwägungsgrund (42) der DORA wird dazu explizit angeführt, dass die Meldung IKT-bezogener Vorfälle für alle Finanzunternehmen harmonisiert werden sollte, indem sie verpflichtet werden, nur ihren zuständigen Behörden Bericht zu

erstatten. Die Finanzaufsichtsbehörden sollen diese Informationen sodann an Nicht-Finanzbehörden (u.a. für Netz- und Informationssicherheit zuständige Behörde, nationale Datenschutzbehörde und Strafverfolgungsbehörden im Fall strafrechtlicher Vorfälle) weiterleiten.

Zusammenarbeit, Kontrollen und Informationsaustausch sowie Datenschutz

Angesichts der oben erwähnten potentiellen Überschneidungen und Doppelspurigkeiten ist eine enge Zusammenarbeit und ein enger Austausch zwischen der FMA und der Stabsstelle für Cyber-Sicherheit von grösster Bedeutung. Insofern begrüssen wir grundsätzlich die in Kapitel III der Vorlage diesbezüglich vorgesehenen Bestimmungen. Gleichzeitig lässt die Vorlage die Details und klarere Vorgaben zur Kompetenzverteilung offen, sodass nicht nachvollziehbar ist, wie dies konkret geplant ist. Dies bezieht sich auf den Informations- und Datenaustausch ebenso, wie auf die Frage der Befugnisse gegenüber den Betreibern und der Durchführung von Kontrollen - sei es durch die FMA selbst oder durch die von ihr beauftragten Revisionsstellen. Die FMA geht davon aus, dass dies unter engem Einbezug der betroffenen Behörden, einschliesslich der FMA, auf Verordnungsebene konkretisiert werden wird.

Die FMA bedankt sich für die Möglichkeit der Stellungnahme und steht für weitere Diskussionen und einen Austausch über praktische Fragen der obgenannten Aspekte und Vorbringen gerne zur Verfügung.

Freundliche Grüsse
FMA – Finanzmarktaufsicht Liechtenstein

Mario Gassner
Vorsitzender der Geschäftsleitung

Nadja Rossettini-Lambrecht
Stv. Leiterin Abteilung Recht und Internationale Angelegenheiten