LIECHTENSTEINISCHER
BANKENVERBAND

Per Post und E-Mail versandt

Vaduz, 27.09.2022
SIT/ABE

Regierung des Fürstentums Liechtenstein
Herr Regierungschef Dr. Daniel Risch
Ministerium für Präsidiales und Finanzen
Peter-Kaiser-Platz 1
Postfach 684
FL-9490 Vaduz

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

Sehr geehrter Herr Regierungschef Dr. Risch

Mit Schreiben vom 12. Juli 2022 haben Sie uns eingeladen, zum eingangs bezeichneten Vernehmlassungsbericht (VNB) Stellung zu nehmen. Die gegenständliche Vorlage dient der Umsetzung der Richtlinie (EU) 2016/1148 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (nachfolgend: NIS-Richtlinie) in das liechtensteinische Recht sowie der Durchführung der Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren.

Wir danken Ihnen für die Einräumung dieser Möglichkeit und möchten nach Abschluss des verbandsinternen Konsultationsverfahrens zur gegenständlichen Gesetzesvorlage Folgendes ausführen:

I. Generelle Anmerkungen zur Vorlage

Problemstellungen rund um Cybersicherheit gewinnen immer mehr an Bedeutung. In Liechtenstein wurde nunmehr mit der Stabstelle Cyber-Sicherheit eine entsprechende zentrale Stelle im Zusammenhang mit Sicherheitsvorfällen und Cyberattacken etabliert. Zwecks wirkungsvoller Wahrnehmung der gesetzlich verankerten Aufgaben und Kompetenzen ist grundlegende Voraussetzung, dass der Stabstelle auch ausreichend Ressourcen zur Verfügung stehen. Ebenso sollte die Vernetzung und Zusammenarbeit mit dem NCSC (Schweiz) sowie europäischen CERT weiter vorangetrieben werden.

Der Finanzsektor ist ein stark regulierter Sektor mit strengen Sicherheitsstandards in verschiedenen Bereichen, vor allem in Bezug auf Cybersicherheit und Widerstandsfähigkeit. Die Übernahme der Richtlinie (EU) 2016/1148 ins EWR-Abkommen und Umsetzung ins nationale Recht hat sich bereits über mehrere Jahre hinausgezögert. Seither sind bereits andere Rechtsakte im EWR-Abkommen bzw. national in Kraft, die ebenfalls sektorspezifisch Vorgaben im Bereich Cybersicherheit bzw. Incident-Reporting normieren. Zwar enthält Art. 4 Abs. 3 CSG einen lex specialis Vorbehalt. Dennoch regen wir dringend an, die Wechselwirkung der verschiedenen Vorgaben im Hinblick auf den Charakter des CSG als Rahmengesetz nochmals zu prüfen, um Duplizitäten oder abweichende Pflichten zu vermeiden. So enthalten bspw. die

AUSTRASSE 46 · POSTFACH 254 · FL-9490 VADUZ
TELEFON +423 230 13 23 · FAX +423 230 13 24 · INFO@BANKENVERBAND.LI · WWW.BANKENVERBAND.LI

Zahlungsdiensterichtlinie (PSD2) bzw. das ZDG und die zugehörigen technischen Regulierungsstandards zur Strong Customer Authentication (SCA) Vorgaben betreffend wirksame Verfahren zur Aufdeckung, Klassifizierung und Handhabung von Vorfällen einschliesslich schwerer Betriebs- und Sicherheitsvorfälle im Zahlungsverkehr sowie deren Meldung an die FMA. Es ist davon auszugehen, dass schwere Sicherheitsvorfälle i.S.d. Art. 101 f. ZDG in der Regel auch meldepflichtige Sicherheitsvorfälle nach Art. 5 CSG an die Stabsstelle Cyber-Sicherheit begründen.

Ebenso haben die Banken die Leitlinien der Europäischen Bankenaufsichtsbehörde (EBA) zum IKT- und Sicherheitsrisikomanagement (EBA/GL/2019/04) bzw. die entsprechende FMA-Richtlinie 2021/03 einzuhalten inkl. Mindestanforderungen an das Risikomanagement und die aufsichtsrechtlichen Anforderungen an die IT, welche ebenfalls Sicherheitsanforderungen an die Banken, die gleichzeitig Betreiber wesentlicher Dienste i.S.d. gegenständlichen CSG sind, regeln. Darüber hinaus gelten für digitale Zahlungsprodukte, insbesondere für Kartenzahlungen von Kreditkartenunternehmen, internationale Standards wie der Payment Card Industry Data Security Standard (PCI DSS).

Es ist zentral, dass Sicherheitsanforderungen und die Anforderungen an den Mindestinhalt der Meldungen einheitlich geregelt sind, um unnötige Mehraufwände zu vermeiden. Auch ist eine einheitliche Aufsicht bzw. Koordination der zuständigen Behörden, FMA und Stabsstelle Cyber-Sicherheit, sicherzustellen.

Weitere Einzelheiten sind zu Art. 4, Art. 5 sowie Art. 10 und 11 CSG ausgeführt.

Schliesslich ist nicht ohne Weiteres nachvollziehbar, weshalb nach so langer Zeit der Nicht-Umsetzung der NIS-Richtlinie nunmehr der bereits überholte NIS1 Standard übernommen wird. Bereits seit Dezember 2020 ist der Entwurf des NIS2 - Richtlinie verfügbar. Voraussichtlich wird diese noch im Herbst und damit vor Inkrafttreten des CSG verabschiedet werden, welches damit unmittelbar nach Inkraftsetzung wieder revidiert werden muss. Dies ist umso mehr fraglich, als die NIS2-Richtlinie keine reine Änderungsrichtlinie darstellt, sondern die NIS-Richtlinie vollständig ersetzt und aufhebt. Nicht nur der Anwendungsbereich der NIS2-Richtlinie ist deutlich weiter, auch die Anforderungen an das Risiko- und Sicherheitsvorfallmanagement werden erheblich ausgeweitet, so dass unter NIS1 verpflichtete Betreiber wesentlicher Dienste bzw. Anbieter digitaler Dienste nach der Implementierung des CSG unmittelbar erneuten Abgleich- und Anpassungsbedarf haben. Zudem enthält die NIS2 -Richtlinie jene zusätzlichen Bestimmungen, um die Verhältnismässigkeit, eindeutige Kritikalitätskriterien zur Bestimmung der erfassten Einrichtungen und die Abstimmung mit sektorspezifischen Rechtsakten sicherzustellen, die derzeit bei der NIS-Richtlinie bzw. dem CSG fehlen.

Die direkte Übernahme des NIS2 Standards mit einer angemessenen Umsetzungsfrist hätte betroffenen Betreibern wesentlicher Dienste bzw. Anbietern digitaler Dienste gegebenenfalls einiges an (unnötigem) Aufwand erspart. Dies gilt für den Sektor Bankwesen auch im Hinblick auf den Digital Operational Resilience Act (DORA) zur Regelung der digitalen Betriebsstabilität im Finanzbereich, dessen Verabschiedung auf EU-Ebene im Herbst erwartet wird und der in weiten Teilen der NIS/NIS 2-Richtlinie für den Bankenbereich als lex specialis vorgehen wird.

Insgesamt regen wir an, seitens der Stabsstelle Cyber-Sicherheit gemeinsam mit der FMA und der Datenschutzstelle vor Einführung des CSG für den Sektor Bankwesen eine Auslegeordnung hinsichtlich der Überschneidungen mit der PSD II (ZDG), eIDAS-VO

AUSTRASSE 46 · POSTFACH 254 · FL-9490 VADUZ
TELEFON +423 230 13 23 · FAX +423 230 13 24 · INFO@BANKENVERBAND.LI · WWW.BANKENVERBAND.LI

(SigVG), DSGVO (DSG), anerkannten (internationalen) Standards (z.B. ISO 27001/27002, NIST, MaRisk/BIAT etc.), den aufsichtsrechtlichen Vorgaben der europ. Bankenaufsichtsbehörde EBA bzw. der FMA im Bereich IKT Sicherheit und Cybersecurity sowie inskünftig NIS2, DORA und der Critical Enteties Resilience Directive (CER), welche die Resilienz kritischer Infrastrukturen ggü. nicht-cyberbedingten Bedrohungen regelt, vorzunehmen.

II. Anmerkungen zu einzelnen Bestimmungen bzw. Erläuterungen des CSG

Sollte die Regierung nach eingehender Analyse bzw. der oben vorgeschlagenen Auslegeordnung am bisherigen CSG-Fahrplan festhalten wollen, erlauben wir uns nachfolgend einzelne Bestimmungen des gegenständlichen Vorschlags zum CSG zu kommentieren und Anliegen bzw. Empfehlungen an die Regierung auszusprechen.

1. Art. 1 – Anwendungsbereich

Gemäss den Erläuterungen S. 12 zum VNB gilt das CSG für die Landesverwaltung nur in jenen Bereichen, in welchen die LLV als Betreiberin wesentlicher Dienste auftritt.

Wir gehen davon aus, dass die Stabsstelle Cyber-Sicherheit als NCC-FL bzw. im Hinblick auf das CSIRT selbst auch als kritische Infrastruktur zu werten ist und bitten um entsprechende Klarstellung in den Materialien.

2. Art. 3 Abs. 1 Ziff. 2 – Sicherheit von Netz- und Informationssystemen

Nach Art. 3 Abs. 1 Ziff. 2 CSG müssen die Betreiber wesentlicher Dienste in der Lage sein, «auf einem bestimmten Vertrauensniveau alle Angriffe abzuwehren […]». Auch wenn die Definition dem Wortlaut der Richtlinie entnommen ist, bitten wir im Hinblick auf das Prinzip der Verhältnismässigkeit um Klarstellung – in der Definition oder zumindest in den Erläuterungen -, dass durch Betreiber wesentlicher Dienste die Sicherheit der Netz- und Informationssysteme derart sicherzustellen ist, dass Angriffe *im Bereich des Zumutbaren und dem jeweiligen Stand der Technik* abgewehrt werden.

3. Art. 3 Abs. 1 Ziff. 4 – wesentlicher Dienst

Art. 3 Abs. 1 Ziff. 4 CSG definiert zwar den Begriff des wesentlichen Dienstes. Jedoch ist es für die betroffenen Unternehmen in den relevanten Sektoren von zentraler Bedeutung, eine einheitliche Methodik sowie handhabbare, objektive Kriterien zur Bestimmung kritischer Infrastrukturen zur Verfügung zu haben. Ausschlaggebend ist stets die Bedeutung für das Funktionieren des Gemeinwesens.

Zunächst wäre überhaupt zu erheben, welche Dienste / Dienstleistungen im Bankensektor erbracht werden, um diese anschliessend im Lichte der Zielsetzung der Richtlinie zu qualifizieren. Aus Sicht eines möglichen Ausfalls und dadurch entstehender Gefährdung für das Gemeinwesen aufgrund von Versorgungsengpässen und Gefährdungen für die öffentliche

AUSTRASSE 46 · POSTFACH 254 · FL-9490 VADUZ
TELEFON +423 230 13 23 · FAX +423 230 13 24 · INFO@BANKENVERBAND.LI · WWW.BANKENVERBAND.LI

Sicherheit sind im Bereich Banken sicherlich die Bargeldversorgung sowie der kartengestützte und konventionelle Zahlungsverkehr von Bedeutung. Inwieweit auch die reibungslose Abwicklung von Wertpapier- und Derivategeschäften einen wesentlichen Dienst i.S.d. Gesetzes darstellt, wäre zu evaluieren.

Zudem erscheint es allenfalls sinnvoll, gewisse Schwellenwerte für einzelne Sektoren zu definieren, bei deren Überschreiten die als potentiell wesentlich identifizierten Dienste auch als solche i.S.v. Art. 3 Abs. 1 Bst. 4 CSG zu werten sind, bspw. Anzahl der dienstleistungsbezogenen Transaktionen.

Wir regen daher an, dringend mit den einzelnen Sektoren und in Abstimmung mit der FMA, welche u.a. die bankenaufsichtsrechtlichen Anforderungen an die Funktionsfähigkeit kritischer Infrastrukturen und deren Sicherheitsanforderungen definiert und überwacht, bzw. den anderen zuständigen Aufsichtsbehörden, im Rahmen von Wegleitungen die Vorgaben aus dem CSG zu konkretisieren.

Im Hinblick auf die Erläuterungen auf S. 15 des VNB gehen wir derzeit davon aus, dass lediglich die drei grössten Banken, LGT, LLB sowie VP Bank als besonders kritische Einrichtungen zu definieren sind. Der Marktanteil am Retailgeschäft sowie den gesicherten Einlagen i.S.d. Gesetzes über die Einlagensicherung und Anlegerentschädigung bei Banken und Wertpapierfirmen vom 27. Februar 2019 (EAG) beträgt rund 90%, ein Grossteil der reinen Zahlungsverkehrstransaktionen wird über diese drei Banken abgewickelt.

4. Art. 3 Abs. 1 Ziff. 5 – Betreiber wesentlicher Dienste

Art. 3 Abs. 1 Ziff. 5 CSG definiert den Betreiber eines wesentlichen Dienstes als den «Erbringer». Gerade im Finanzdienstleistungsbereich werden häufig Dienstleistungen ausgelagert. Dies betrifft teilweise auch die Auslagerung kritischer IT-Dienstleistungen. Wer effektiv Erbringer des Dienstes ist, kann unseres Erachtens nur unter Berücksichtigung der tatsächlichen Umstände und des «beherrschenden» Einflusses auf den betreffenden Dienst bestimmt werden. Dies ist in der Regel jenes Unternehmen, welches die zugrundeliegende Anlage/Infrastruktur betreibt. Bei Auslagerung kritischer IT-Dienstleistungen von Banken und Finanzmarktinfrastrukturen dürfte unter Gesamtschau der Umstände der jeweilige IT-Dienstleister als «Betreiber» des wesentlichen Dienstes anzusehen sein. Aufsichtsrechtlich bleibt die Bank selbstverständlich für die Einhaltung der Sicherheitsanforderungen verantwortlich.

Auch dies (Betreiberbegriff bei Auslagerungen) ist im Rahmen weiterer konkretisierender Vorgaben zu klären.

5. Art. 3 Abs. 1 Ziff. 9 – Sicherheitsvorfall

Wir bitten um weitere Präzisierung des Begriffs des Sicherheitsvorfalls. Die bisher in den Erläuterungen auf S. 17 des VNB zur Verfügung gestellten Beispiele erscheinen zu wenig abgegrenzt. Auch rein technische Probleme bzw. operative Störungen, die die Verfügbarkeit/Erreichbarkeit eines wesentlichen Dienstes betreffen, wären nach der gegebenen Definition erfasst, bspw. vorübergehender Ausfall des E-bankings. Es bleibt auch unklar, ab wann tatsächlich von einer «Beeinträchtigung» des wesentlichen Dienstes auszugehern ist (vgl. dazu auch

AUSTRASSE 46 · POSTFACH 254 · FL-9490 VADUZ
TELEFON +423 230 13 23 · FAX +423 230 13 24 · INFO@BANKENVERBAND.LI · WWW.BANKENVERBAND.LI

Ausführungen unter Ziff. 11 betreffend Meldeschwelle). Aufgrund der weiten Definition wären folgende Beispiele Sicherheitsvorfälle:

- Ein x-fach vorkommender Port-Scan wäre per se schon ein Sicherheitsvorfall
- Jeder Stromausfall, der bereits durch den Energieversorger gemeldet wurde, wird parallel dazu von allen betroffenen Infrastrukturen gemeldet (sofern die Plattform verfügbar ist).
- Ausfall einer externen Netzwerkinfrastruktur (z.B. SWIFT-Netzwerk)
- Ausfall von Outlook / Exchange oder Telekommunikation FL, soweit dies auf die Erbringung wesentlicher Dienste Einfluss hat (bspw. Zahlungsverkehr)

6. Art. 3 Abs. 1 Ziff. 13 – CSIRTs-Netzwerk

Art. 3 Abs. 1 Ziff. 13 CSG übernimmt die Umschreibung des Art. 12 Abs. 2 der Richtlinie (EU) 20216/1148. Im Hinblick auf die besondere Situation Liechtensteins und die Anbindung an das NCSC Schweiz regen wir die Ergänzung der Legaldefinition derart an, dass neben den bereits benannten Vertretern ebenfalls «Vertreter weiterer vertrauenswürdiger Drittstaaten» berücksichtigt werden.

7. Art. 3 – zusätzliche Definition «Unverzüglich»

Entsprechend den Vorgaben der Richtlinie (EU) 2016/1148 wird in zeitlicher Hinsicht wiederholt der Begriff «unverzüglich» im CSG verwendet. Es handelt sich um einen unbestimmten Rechtsbegriff, der in der Richtlinie selbst nicht spezifiziert wird. Wir bitten um Aufnahme einer Legaldefinition in Art. 3 CSG derart, dass unverzüglich nicht die – bereits rein faktisch nicht mögliche – sofortige Vornahme der geforderten Handlung, bspw. Meldung eines Sicherheitsvorfalls, voraussetzt, sondern dass nach einer Erstanalyse rasch möglichst, d.h. ohne schuldhaftes Zögern innerhalb einer nach vernünftigem Ermessen zu erwartenden Frist, die geforderte Handlung vorzunehmen ist.

Die zulässige Frist sollte mit dem aufsichtsrechtlichen Verständnis, insbesondere im Bereich Cybersecurity und IKT Sicherheit, kongruent sein. So sieht die FMA-Mitteilung 2018/3 zum Umgang mit Cyber-Attacken eine Meldung (erst) innert 14 Tagen ab Kenntniserlangung über schwerwiegende und betriebsstörende Cyber-Attacken vor. Eine Abstimmung der Meldefristen wäre zu befürworten.

8. Art. 4 Abs. 1 – Sicherheitsanforderungen und lex specialis Vorbehalt nach Art. 4 Abs. 3

Der lex specialis Vorbehalt des Art. 4 Abs. 3 CSG ist zu begrüssen, betrifft jedoch nur die Bestimmungen über Sicherheitsanforderungen bei Vorliegen sektorspezifischer Rechtsvorschriften. Sektoren, welche bereits stark im Bereich der Cybersicherheit durch lex specialis reguliert sind, unterstehen nicht nur den dort bestehenden Sicherheitsanforderungen und Auflagen, sondern ebenfalls spezifischen Meldepflichten. Um Duplizitäten zu vermeiden, erscheint es aus unserer Sicht wichtig, den horizontalen Vorschlag des CSG noch stärker mit den sektorspezifischen, insbesondere aufsichtsrechtlichen, Vorgaben betreffend Sicherheitsvorgaben für Betreiber wesentlicher Dienste sowie auch dem Incident Reporting (s. dazu

AUSTRASSE 46 · POSTFACH 254 · FL-9490 VADUZ
TELEFON +423 230 13 23 · FAX +423 230 13 24 · INFO@BANKENVERBAND.LI · WWW.BANKENVERBAND.LI

Anmerkungen unter Ziff. 11 zu Art. 5 CSG) abzugleichen. Die Vorgaben der Art. 4 Abs. 1 und Abs. 2 CSG werden für den Banksektor durch die EBA/GL/2019/04 bzw. FMA-Richtlinie 2021/3 und FMA-Mitteilung 2018/03 bereits aufsichtsrechtlich abgedeckt. Ebenfalls bestehen mit der DSGVO bereits Vorgaben zur Verarbeitung von besonders schützenswerten personenbezogenen Daten.

9. Art. 4 Abs. 4 und Art. 5 Abs. 5 – Verordnungskompetenz

Gemäss Art. 4 Abs. 4 bzw. Art. 5 Abs. 5 CSG regelt die Regierung das Nähere zu den Sicherheitsanforderungen für Betreiber wesentlicher Dienste bzw. zur Meldung mittels Verordnung. Aufgrund des engen Praxisbezuges bitten wir um Einbezug des LBV bei der Erarbeitung allfälliger weitergehender Sicherheitsvorgaben im Finanzdienstleistungssektor.

10. Art. 5 und Art. 7 – Umsetzung des lex specialis Vorbehalts des Art. 1 Abs. 7 der Richtlinie (EU) 2016/1148

Wir erlauben uns den Hinweis, dass der lex specialis Vorbehalt des Art. 1 Abs. 7 der Richtlinie (EU) 2016/1148 explizit auch im Bereich der Meldung greift und derzeit nicht in Art. 5 bzw. Art. 7 CSG nachvollzogen ist. Danach gilt:

> «Wird nach Maßgabe eines sektorspezifischen Rechtsakts der Union von den Betreibern wesentlicher Dienste oder den Anbietern digitaler Dienste gefordert, entweder die Sicherheit ihrer Netz- und Informationssysteme oder die Meldung von Sicherheitsvorfällen zu gewährleisten, und sind diese Anforderungen in ihrer Wirkung den in dieser Richtlinie enthaltenen Pflichten mindestens gleichwertig, so gelten die einschlägigen Bestimmungen jenes sektorspezifischen Rechtsakts der Union.»

Wir bitten um Ergänzung des Gesetzeswortlauts.

11. Art. 5 Abs. 1 – Meldeschwelle und Meldefrist

Nach Art. 5 Abs. 1 CSG haben Betreiber jegliche *Sicherheitsvorfälle*, die einen wesentlichen Dienst *betreffen*, an die Stabsstelle zu melden. Gemäss den Erläuterungen, S. 15 spielt es dabei keine Rolle, ob es durch den Sicherheitsvorfall zu einem Schaden oder zu einer anderweitigen Störung gekommen ist. Die Meldeschwelle ist damit deutlich niedriger als die Vorgaben des Art. 14 Abs. 3 der Richtlinie (EU) 2016/1148, welche Meldungen von Sicherheitsvorfällen vorsieht, *die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen bereitgestellten wesentlichen Dienste haben*. Zwar ist das Anliegen hinter der in der Vorlage gewählten Formulierung – vollständige Übersicht über die Sicherheitslage der betroffenen Einrichtung und im Land generell – verständlich. Jedoch dürfte die sehr weite Fassung zu einer Überzahl an nicht relevanten Meldungen führen, welche von der Stabsstelle geprüft und bewertet werden müssten. Dies dürfte angesichts der verfügbaren Ressourcen der Stabsstelle Cyber-Sicherheit nicht zielführend sein. Es kann auch nicht das Ziel sein, zusätzliche aufwändige manuelle Prozesse zu etablieren. Besser erscheint es, klare Kriterien für eine Meldung festzulegen.

AUSTRASSE 46 · POSTFACH 254 · FL-9490 VADUZ
TELEFON +423 230 13 23 · FAX +423 230 13 24 · INFO@BANKENVERBAND.LI · WWW.BANKENVERBAND.LI

Ein Sicherheitsvorfall ist zu unterscheiden von einer Cyberbedrohung oder einem Beinahe-Vorfall. Von Interesse sind wesentliche Sicherheits-/Cybervorfälle, nicht operative Störungen / einfache Vorfälle des Tagesgeschäfts. Es muss sich um in irgendeiner Form schwerwiegende Sicherheitsvorfälle handeln. So verlangt auch die Richtlinie (EU) 2016/1148 nicht, dass durch den Sicherheitsvorfall eine Störung oder ein Schaden eingetreten sein muss, sondern nur, dass die Auswirkungen auf die Verfügbarkeit des bereitgestellten wesentlichen Dienstes *erheblich* gewesen sind. Wann eine derartige Erheblichkeit gegeben ist, wäre durch weitergehende Verwaltungsanweisung zu konkretisieren. Es bedarf klarer Leitlinien, ab wann ein Vorfall relevant und wie dieser zu klassifizieren ist (Fraud Incident, Cyber Angriff, Data Breach, etc.).

Wir regen daher dringend an, die Formulierung des Art. 5 Abs. 1 CSG im Lichte der Richtlinie zu schärfen. Ein Liechtenstein-Finish ist nicht zielführend.

Entsprechend den Richtlinien-Vorgaben hat die Meldung «unverzüglich» zu erfolgen. Wie bereits zu Art. 3 CSG ausgeführt (vgl. Ziff. 7), ist regelmässig erst nach einer Analyse Art und Schwere des Sicherheitsvorfalls feststellbar, weshalb eine Konkretisierung innerhalb der Begriffsbestimmungen wünschenswert wäre.

12. Art. 5 Abs. 1 – zuständige Stelle

Zuständige Meldestelle ist nach Art. 5 Abs. 1 CSG die Stabsstelle Cyber-Sicherheit. In Art. 15 Abs. 1 Bst. a CSG wird die Zuständigkeit intern an das CSIRT weiterverlagert.

Mehrere Banken sind als kritische Infrastrukturen dem NCSC Schweiz angegliedert. Wenn nun das neue nationale CERT oder CSIRT über die EWR Mitgliedschaft in den Verbund des europäischen CERT / CSIRT eingebunden wird, ist für die Banken von grundlegender Bedeutung, dass auch in Zukunft Cyber-Vorfälle bzw. sonstige Sicherheitsvorfälle in Bezug auf Netzt- und Informationssysteme – im internationalen Kontext – nur an eine Stelle zentral gemeldet werden müssen. Auch ist festzuhalten, welche Stelle den Banken anlässlich eines Sicherheitsvorfalls Unterstützung leistet. Ein reines Reporting hilft den Banken bei der Bewältigung einer Cyber-Krise nicht weiter, reduziert aber die wenigen verfügbaren Ressourcen der Spezialisten. Bestehende Kanäle wie zum Schweizer NCSC sollten unter keinen Umständen unterbrochen oder vervielfältigt werden oder parallele Strukturen redundant und mit anderer Periodizität der Berichterstattung bedient werden müssen. Dies ist soweit erforderlich auf zwischenstaatlicher Ebene sicherzustellen (s. dazu auch unter Ziff. 20).

Zudem ist ein Sicherheitsvorfall betreffend einen wesentlichen Dienst in der Regel ein Sicherheitsvorfall, welcher bereits unter spezialgesetzlichen Bestimmungen eine Meldepflicht begründet. Durch die FMA-Mitteilung 2018/03 besteht bereits eine Meldepflicht bei schwerwiegenden oder betriebsstörenden Cyber-Attacken. Ferner besteht aufgrund Art. 33 DSGVO bei Verletzungen des Schutzes personenbezogener Daten eine Meldepflicht an die Datenschutzstelle. Im Zweifelsfall müssen durch den Betreiber des Dienstes mithin mehrere Meldungen an verschiedene nationale Behörden/Stellen abgesetzt werden: Meldung an die Datenschutzstelle (Data Breach), Meldung an FMA (Operational Incident oder auf spezialgesetzlicher Grundlage, bspw. Art. 102 ZDG oder Cyber Incident), Stabstelle Cyber-Security (Cyber Incident).

AUSTRASSE 46 · POSTFACH 254 · FL-9490 VADUZ
TELEFON +423 230 13 23 · FAX +423 230 13 24 · INFO@BANKENVERBAND.LI · WWW.BANKENVERBAND.LI

In Bezug auf die Resilienz wäre eine zentrale nationale Meldestelle (Hub), für alle Arten von Sicherheitsvorfällen und alle betroffenen Marktteilnehmer wünschenswert. Erhielten die dann jeweils zuständigen Behörden mittels Data Pool Zugriff auf dieselben Daten, entstünden keine Redundanzen und das Meldeverfahren könnte einfach und effizient gestaltet werden.

Sollte dies nicht umsetzbar sein, ist gerade für stark regulierte Sektoren wie den Finanzbereich jedenfalls eine klare *Struktur der Zuständigkeiten* zu schaffen. Es erscheint angezeigt, auch die Zusammenarbeit der Behörden untereinander zu intensivieren und daher näher zu regeln, bspw. in einer Art Verständigungsverfahren. Es ist bisher unklar, welche der zuständigen Behörden lead authority ist und wie der allenfalls notwendige grenzüberschreitende Informationsaustausch der verschiedenen Behörden organisiert wird.

13. Art. 5 Abs. 2 – Inhalt der Meldung

Nach Sinn und Zweck des Art. 5 Abs 2 CSG hat eine frühzeitige Meldung Vorrang gegenüber einer vollständigen Meldung (vgl. Erläuterungen, S. 22 des VNB). Dennoch sollte im Hinblick auf Art. 21 Abs. 1 Bst. d CSG klargestellt werden, unter welchen Umständen eine bussgeldbewährte unvollständige Meldung vorliegt. Dem Betreiber des wesentlichen Dienstes müssen Abklärungen und Analysen möglich sein, ohne sich mit einem potentiellen Verstoss gegen Art. 5 Abs. 2 CSG konfrontiert zu sehen. Die Schwere eines Sicherheitsvorfalles lässt sich im Zeitpunkt seines Eintrittes oftmals noch gar nicht bewerten. Im Fokus des Betreibers steht regelmässig zunächst die Behebung bzw. Begrenzung eines erheblichen Sicherheitsvorfalles, die die verfügbaren Ressourcen absorbiert. Auch sind im Zeitpunkt des Eintritts des Sicherheitsvorfalls oftmals noch nicht alle Begleitumstände oder nach Art. 5 Abs. 2 CSG erforderlichen Mindestangaben bekannt.

14. Art. 5 Abs. 3 – Meldeformular / elektronisches Meldeformat

Auch diesbezüglich bitten wir um Abstimmung auf die aufsichtsrechtlichen Erfordernisse. Selbst wenn der materielle Inhalt der Meldungen kongruent ist, begründen bereits formale Unterschiede unnötige Mehraufwände für die Banken. Sollte am bisherigen CSG-Entwurf festgehalten werden, sollten Banken nur eine Meldung (an und unter den Vorgaben der FMA) absetzen müssen. Der Informationsfluss an weitere zuständige Stellen sollte über behördliche Zusammenarbeit sichergestellt werden. Es ist daher zwingend vorzusehen, dass die Verwendung aufsichtsrechtlich aufgrund sektorspezifischer Vorgaben erstellter Meldungen und Meldeformulare auch für Zwecke der Meldung nach Art. 5 Abs. 3 CSG an die Stabsstelle Cyber-Sicherheit zulässig ist, sofern der Mindestinhalt der Meldung nach Art. 5 Abs. 2 CSG abgedeckt ist. Dies sieht bereits der lex specialis Vorbehalt des Art. 1 Abs. 7 der Richtlinie (EU) 2016/1148) vor. Für die Banken bestehen aus verschiedenen Regularien Meldeformate (PSD 2 Incident Reporting, FMA Meldeformular von Cyber-Attacken etc.). Es bedarf hier dringend einer konsistenten Umsetzung.

Ausserdem regen wir an, neben dem elektronischen Meldeformat alternative Kanäle zu erwägen, sollte die Website der Stabsstelle oder das elektronische Meldeformular im Falle einer Störung nicht erreichbar / verfügbar sein (bspw. DDOS Attacke oder Ausfall ISP).

AUSTRASSE 46 · POSTFACH 254 · FL-9490 VADUZ
TELEFON +423 230 13 23 · FAX +423 230 13 24 · INFO@BANKENVERBAND.LI · WWW.BANKENVERBAND.LI

15. Art. 5 Abs. 4 bzw. Art. 7 Abs. 3 - Unterrichtung der Öffentlichkeit

Im Einzelfall kann nach Art. 5 Abs. 4 bzw. Art. 7 Abs. 3 CSG eine Information der Öffentlichkeit über konkrete Sicherheitsvorfälle erfolgen. Nach Art. 7 Abs. 3 kann die Stabsstelle Cyber-Sicherheit neben der Eigeninformation sogar «verlangen, dass der Anbieter digitaler Dienste dies unternimmt».

Offen bleibt hier, auf welcher Grundlage letztlich die Stabsstelle Cyber-Sicherheit entscheidet, ob und durch wen die Öffentlichkeit zu informieren ist. Offen ist auch die Art und Weise der Information, über die Website der Stabsstelle / des Anbieters digitaler Dienste, Printmedien, Radio etc.?

Wir bitten um weitere Ergänzung der Materialien.

16. Art. 6 Abs. 2 Bst. e – Einhaltung internationaler Normen

Wir bitten angesichts der Vielzahl an internationalen Standards und Normen um Präzisierung in den Erläuterungen oder im Gesetzestext zu Art. 6 Abs. 2 Bst. e CSG, dass Anbieter digitaler Dienste selbstverständlich nur die für sie geltenden /relevanten internationalen Normen und Standards einzuhalten haben.

17. Art. 7 Abs. 2 – Meldepflicht von Betreibern wesentlicher Dienste

Wir bitten um Prüfung und Neuverortung des Art. 7 Abs. 2 CSG, welcher die Meldepflicht bei Inanspruchnahme digitaler Dienste durch Betreiber wesentlicher Dienste regelt («Betreiber- bzw. Anbieterkette»). Es handelt sich um die Begründung originärer Meldepflichten für den Betreiber wesentlicher Dienste und ist damit in Art. 5 CSG und nicht innerhalb der Meldepflicht für Anbieter digitaler Dienste zu regeln. Auch sollte nur eine Meldepflicht für relevante/erhebliche Auswirkungen auf die Verfügbarkeit dieser Dienste bestehen (vgl. 2. HS von Art. 7 Abs. 2 sowie Anmerkungen zu Art. 5 Abs. 1 unter Ziff. 11).

18. Art. 10 Abs. 1 Bst. a und b – Überprüfung und Überwachung

In Art. 10 Abs. 1 Bst. a und b CSG wird der Stabsstelle Cyber-Sicherheit eine Überwachungs- und Überprüfungskompetenz für die Einhaltung des CSG durch Betreiber wesentlicher Dienste eingeräumt. Dies macht jedoch nur dort Sinn, wo nicht bereits aufgrund der spezialgesetzlichen Zuständigkeit der Aufsichtsbehörden oder anderer zuständiger Behörden entsprechende Kontrollen durchgeführt werden.

Ist im Rahmen des Gesetzes ein Auditing / Kontrollen seitens der Stabstelle Cyber- Sicherheit für Banken angedacht, ist dies zwingend mit der FMA zu koordinieren, um den Aufwand für die Banken nicht unnötig zu duplizieren. Mit der Schaffung einer neuen Instanz, die ergänzend zu den anderen Behörden Prüfungen anordnen kann, wird nur die Anzahl der Prüfungen und somit der Aufwand erhöht – es ist aber zu bezweifeln, dass dies zu einer Erhöhung der Sicherheit führt. Vielmehr werden die ohnehin schwer verfügbaren Spezialisten für zusätzlichen Administrationsaufwand absorbiert. Wir bitten um Prüfung, inwieweit nicht die Kompetenz zur Überwachung der regulatorischen Anforderungen im Bereich Netz- und Informationssystem-

AUSTRASSE 46 · POSTFACH 254 · FL-9490 VADUZ
TELEFON +423 230 13 23 · FAX +423 230 13 24 · INFO@BANKENVERBAND.LI · WWW.BANKENVERBAND.LI

Sicherheit für Banken zentral bei der FMA liegen sollte (s. dazu auch die weiteren Ausführungen unter Ziff. 22 zu Art. 11 und 13 CSG).

19. Art. 10 Bst. c – CSIRTs

Wir regen die Ergänzung bzw. Änderung des Wortlauts von Art. 10 Abs. 1 Bst. c CSG derart an, dass die Stabsstelle für c) *Einrichtung und Koordination* des Computer-Notfallteams gemäss Art. 15 zuständig ist. Die Stabsstelle «betreibt» dieses nicht im eigentlichen Sinn.

20. Art. 10 Abs. 1 Bst. h - Koordination

Nach Art. 10 Abs. 1 Bst. h CSG obliegt der Stabsstelle Cyber-Sicherheit als NCC-FL die Gesamtkoordination und Schnittstellenfunktion im Cyberbereich. Wir bitten um Konkretisierung dieser Funktion auch im Verhältnis zu den Aufgaben des CSIRT und der Stabsstelle im Allgemeinen. Angesicht der Personalressourcen der Stabsstelle Cyber-Sicherheit erscheint der sehr umfangreiche Aufgaben- und Kompetenzkatalog mehr als ambitioniert.

Um der Schnittstellenfunktion gerecht zu werden, schlagen wir vor, neben der gesetzlich verankerten Möglichkeit des Informationsaustausches der Stabsstelle Cyber-Sicherheit mit anderen staatlichen Stellen (FMA, FIU etc.) sowie anderen CERT, CSIRTs etc. auch explizit eine Rechtsgrundlage für Public Private Partnerships (PPP) im Bereich Cybersecurity zu schaffen. Teil eines solchen PPP könnte bspw. der informelle, vertrauliche Austausch zwischen einzelnen Sektoren und der Stabsstelle Cyber-Sicherheit zu Bedrohungslagen etc. sein.

Zudem erlauben wir uns, an dieser Stelle nochmals auf unser Anliegen aufmerksam zu machen, welches bereits vor über einem Jahr bei der Regierung platziert wurde:

Die Schweizerische Bankiervereinigung (SBVg) hat im Mai dieses Jahres den Verein «Swiss Financial Sector Cyber Security Centre (Swiss FS-CSC)» mit dem Ziel des Informationsaustausches und der Zusammenarbeit unter seinen Mitgliedern und Affiliates zur Verbesserung der Cyberresilienz gegründet. Ein Anschluss einzelner oder aller liechtensteinischen Banken ist aus statutarischen Gründen noch in Abklärung. Die SBVg strebt eine enge Zusammenarbeit mit dem NCSC mit dem Ziel eines PPP an. Dazu gehört auch, dass Behörden und Finanzinstitute gemeinsam unverzüglich eine handlungsfähige Krisenorganisation für die Abwehr von Cyberrisiken aufbauen. Ein Anschluss an das FS-CSC in der Schweiz würde es allen Banken ermöglichen, Zugang zu sektorspezifischen Informationen zu erhalten und die Krisenmanagement- und Vorfallbewältigungsfunktionen des FS-CSC nutzen zu können. Dies hat aber zur Folge, dass Banken grenzüberschreitend sicherheitsrelevante Informationen und Informationen zu Sicherheitsvorfällen bzw. Störungen der Netz- und Informationssystem-Sicherheit (auf privatrechtlicher Basis) austauschen. Wir haben bereits im Juni 2021 darum gebeten zu prüfen bzw. sicherzustellen, dass ein solches Vorgehen mit den geltenden datenschutz- und strafrechtlichen Bestimmungen im Einklang steht.

Fraglich ist auch, auf welcher Grundlage derzeit Meldungen von Sicherheitsvorfällen bzw. der Informationsaustausch mit dem NCSC erfolgen. Nach unserer Kenntnis besteht im Sinne zwischenstaatlicher Vereinbarungen derzeit allein eine Absichtserklärung der Schweiz und

AUSTRASSE 46 · POSTFACH 254 · FL-9490 VADUZ
TELEFON +423 230 13 23 · FAX +423 230 13 24 · INFO@BANKENVERBAND.LI · WWW.BANKENVERBAND.LI

Lichtensteins zur Zusammenarbeit im Cyberbereich. Mit dem CSG wird nunmehr für den behördlichen Austausch in Art. 10 Abs. 1 Bst. l und m CSG eine Rechtsgrundlage geschaffen.

Wir bitten um ergänzende Regelung des grenzüberschreitenden Austausches sicherheitsrelevanter Informationen und Informationen zu Sicherheitsvorfällen zwischen den Betreibern wesentlicher Dienste bzw. Anbietern digitaler Dienste und privatrechtlich organisierten Branchenvereinigungen (bspw. FS-ISAC) bzw. Klarstellung in den Materialien, dass ein derartiger Austausch zulässig ist.

21. Art. 10 Abs. 1 Bst. k und l - SPOC

Es erscheint als Intention der Vorlage, die umfassende und zentrale Kompetenz für Cybersecuritybelange der Stabsstelle Cyber-Sicherheit zuzuweisen. Sie wird damit in gewisser Weise zum SPOC (Single Point of Contact) für Cyber-Sicherheitsvorfälle bzw. sonstige Sicherheitsvorfälle im Zusammenhang mit Netz- und Informationssystemen. Die Banken sind aber teilweise direkt beim Schweizer NCSC oder CERT Österreich akkreditiert. Neben den Kompetenzen und Befugnissen der Stabsstelle ist daher auch zu regeln, wie die Reaktionszeiten der Stabsstelle und Support-Dienstleistungen(-dienstleistungspflichten) aussehen und ob bzw. wann eine Weitergabe der Informationen durch die Stabsstelle Cyber-Sicherheit an das NCSC oder an europ. CERT zu erfolgen hat. Das Verhältnis der Stellen und Behörden untereinander, sowohl international als auch national, muss klar und abschliessend normiert sein.

22. Art. 11 Abs. 1 und Art. 13 Abs. 1 und 2 – Dokumentationspflicht, Kontrollen und Einsichtsrecht

Wir erachten es als kritisch, dass durch Art. 11 und 13 CSG faktisch eine weitere Aufsichtsbehörde für den Finanzbereich geschaffen wird. Alleinige Aufsichtsbehörde für Banken sollte weiterhin die FMA bleiben (s. auch die Ausführungen unter Ziff. 18 zu Art. 10 Abs. 1 Bst. a und b CSG). Die FMA beurteilt bereits sämtliche Aspekte der IKT- respektive Cybersicherheit aus aufsichtsrechtlicher Sicht (vergleichbare Prüfungen zu Art. 11 Abs. 1 und Art. 13 Abs. 1 CSG durch die jeweiligen Revisionsgesellschaften). Insbesondere stellen die Banken den Revisionsgesellschaften bereits die notwendigen Informationen gemäss Art. 11 Abs. 1) a) und b) CSG zur Verfügung. Diese Informationen betrachten wir ebenfalls als besonders schützenswert, die Herausgabe der Informationen birgt in sich selbst wieder ein Sicherheitsrisiko.

Es erscheint zielführender, eine entsprechende Pflicht der zuständigen Aufsichtsbehörde (FMA) zur Information an die Stabsstelle Cyber-Sicherheit über die Überprüfung der Sicherheit der Netz- und Informationssysteme zu normieren. Der lex specialis Vorbehalt des Art. 1 Abs. 7 der Richtlinie (EU) 2016/1148 muss generell gelten, nicht nur betreffend Sicherheitsanforderungen allgemein und Meldepflichten, sondern auch betreffend Überwachung und Kontrolle. Sinn und Zweck des CSG ist die Sicherstellung eines einheitlich hohen Schutzniveaus von Netz- und Informationssystemen, die aber bereits aufsichtsrechtlich und durch spezialgesetzliche Sicherheitsanforderungen für die Banken erreicht wird.

Wir bitten daher um Ergänzung des Gesetzes betreffend Art. 10, Art. 11 und Art. 13 CSG wie folgt: «Werden durch sektorspezifische Rechtsakte anderen Behörden bzw. Stellen Befugnisse für die Überwachung und Kontrolle der Sicherheit von Netz- und Informationssystemen

AUSTRASSE 46 · POSTFACH 254 · FL-9490 VADUZ
TELEFON +423 230 13 23 · FAX +423 230 13 24 · INFO@BANKENVERBAND.LI · WWW.BANKENVERBAND.LI

eingeräumt, die zur Erbringung bzw. Bereitstellung wesentlicher Dienste nach diesem Gesetz oder durch Anbieter digitaler Dienste genutzt werden, so gelten auch für die Überwachung und Kontrolle die einschlägigen Bestimmungen jenes sektorspezifischen Rechtsakts. Die zuständige Behörde / Stelle hat die Stabsstelle Cyber-Sicherheit über die durchgeführten Kontrollen zu unterrichten.»

Jedenfalls erscheint eine derart weitgehende Kompetenz der Stabsstelle, wie sie derzeit in Art. 11 und 13 CSG vorgesehen ist, neben der aufsichtsrechtlichen Prüfkompetenz der FMA fraglich. Die Kontroll- und Einsichtskompetenz kann nur soweit reichen, als im stark regulierten Finanzdienstleistungsbereich überhaupt noch ein Anwendungsbereich des CSG verbleibt. Gemäss Art. 11 Abs. 1 Bst. a CSG kann die Stabsstelle Cyber-Sicherheit von den Betreibern wesentlicher Dienste die Zurverfügungstellung der zur Bewertung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen einschliesslich der dokumentierten Sicherheitsmassnahmen verlangen. Es kann nicht sein, dass die Banken der Stabsstelle sämtliche Dokumentation über Cyber-Risiken aushändigen müssen. Erfasst sein können – wenn überhaupt – lediglich jene Informationen, die sich auf Netz- und Informationssysteme zur Erbringung/Bereitstellung der wesentlichen Dienste beziehen. Wir bitte um entsprechende Ergänzung des Gesetzeswortlauts, sollten Art. 11 und 13 CSG in der vorgeschlagenen Form beibehalten werden.

Wird eine zusätzliche Prüfbefugnis seitens der Stabsstelle Cyber-Sicherheit aus dem CSG bei Banken angenommen, sind für Zutritte zum Bankgebäude bzw. Rechenzentrum jedenfalls die etablierten Sicherheitsprozesse einzuhalten. Bspw. ist Voraussetzung, dass eine Anmeldung und Ausweiskontrolle erfolgt und der Zutritt jederzeit durch Personal der Bank begleitet wird.

Ausserdem regen wir an, diesfalls in Art. 13 Abs. 1 CSG vorzusehen, dass nach Abschluss der Kontrollen sämtliche Unterlagen mit Ausnahme der Abschlussberichte wieder zu vernichten sind.

23. Art. 11 Abs. 2 – unentgeltliche Offenlegung von Betreibern wesentlicher Dienste

Art. 11 Abs. 2 regelt die Pflicht zur unentgeltlichen Offenlegung von statistischen Daten und weitere Angaben. Es ist jedoch nicht verständlich, weshalb allfällige zusätzliche Aufwände der Banken, welche durch die Erhebung/Aufbereitung der Daten, ggf. sogar unter Einbezug externer Stellen/Dienstleister, entstehen, nicht abgegolten werden.

Wir bitten um Ergänzung des Wortlauts von Art. 11 Abs. 2 Satz 2 CSG derart, dass «Die Offenlegung […] unentgeltlich zu erfolgen [hat], sofern dadurch dem Betreiber kein unverhältnismässiger Mehraufwand entsteht.»

24. Art. 12 Abs. 2 – unverzügliche Offenlegung durch Anbieter digitaler Dienste

Art. 12 Abs. 2 CSG sieht die unverzügliche Offenlegung der zur Beurteilung der Sicherheit von Netz- und Informationssystemen erforderlichen Informationen vor. Hier gilt zunächst das zu Art. 11 Abs. 1 CSG Gesagte entsprechend. Die Offenlegungspflicht kann sich nur auf jene Netz- und Informationssysteme beziehen, die zur Bereitstellung digitaler Dienste genutzt werden. Ebenso ist der vorgeschlagene lex specialis-Vorbehalt nachzuvollziehen.

AUSTRASSE 46 · POSTFACH 254 · FL-9490 VADUZ
TELEFON +423 230 13 23 · FAX +423 230 13 24 · INFO@BANKENVERBAND.LI · WWW.BANKENVERBAND.LI

Die Pflicht zur unverzüglichen Offenlegung darf den operativen Betrieb einer kritischen Infrastruktur nicht beeinträchtigen. Hier erscheint Augenmass wichtig sowie angemessene Fristen, um eine Bereitstellung der Informationen in guter Qualität zu ermöglichen.

25. Art. 13 Abs. 2 - Kontrollen

Kontrollen nach Art. 13 Abs. 1 CSG können nach Abs. 2 auch durch beauftragte qualifizierte Dritte wahrgenommen werden. Offen bleibt hier, wer die Kosten der qualifizierten Dritten trägt. Wir bitten um entsprechende Ergänzung.

26. Art. 15 – Aufgaben CSIRT

Art. 15 Abs. 2 CSG regelt umfangreiche Aufgaben eines nationalen CSIRT, insbesondere auch die Unterstützung als Ratgeber bzw. Verbindung zu anderen CSIRTs, welche dann direkt unterstützen (vgl. Art. 15 Abs. 2 Bst c und Erläuterungen S. 38/39 des VNB). Es werden einige Personalressourcen nötig sein, um ein funktionierendes nationales CSIRT zu etablieren. Der Mehrwert eines CSIRT Liechtenstein ist dabei schwierig abzuschätzen. Absatz 4 erlaubt der Stabstelle Cyber-Sicherheit zwar, Tätigkeiten an externe Stellen auszulagern. Bei Banken stellt sich jedoch immer die Frage, inwieweit eine Auslagerung mit den für den Finanzbereich geltenden hohen regulatorischen Anforderungen zu Bankgeheimnis und Datenschutz vereinbar ist.

Ein derart qualifizierter Dritter wären unseres Erachtens auch bestehende Netzwerke / CSIRTs. Es stellt sich daher die Frage, ob ein Anschluss an bestehende Netzwerke (Schweiz, EU) nicht zielführender und realistischer ist.

Wichtig erscheint zumindest, dass Betreiber wesentlicher Dienste sich trotz Art. 15 CSG weiterhin direkt an jene Stellen, Service Provider, Anbieter digitaler Dienste etc., wenden können, von denen Unterstützung im Rahmen eines Sicherheitsvorfalls nicht nur allgemein, sondern spezifisch erhältlich ist (inkl. Shutdown von Domänen etc.).

27. Art. 17 – IKT-Lösungen zur Datenverarbeitung

Die bisher gewählte Formulierung in Art. 17 CSG, nach der die Stabsstelle Cyber-Sicherheit IKT-Lösungen betreiben kann, um Risiken oder Sicherheitsvorfälle frühzeitig zu erkennen (Abs. 1) bzw. IKT-Lösungen betreiben oder nach Einwilligung der betroffenen Einrichtung nutzen kann (Abs. 2), ist unklar und lässt offen, ob die Stabsstelle diese selbst einsetzt oder den Betreibern wesentlicher Dienste auferlegen kann, von der Stabsstelle vorgegebene IKT-Lösungen in ihren Netz- und Informationssystemen zu implementieren bzw. der Stabsstelle Zugang zu eigenen IKT-Lösungen zu gewähren.

Wir bitten um entsprechende Klarstellung, dass die IKT-Lösungen nicht bei den Banken bzw. Betreibern wesentlicher Dienste platziert bzw. betrieben werden dürfen.

AUSTRASSE 46 · POSTFACH 254 · FL-9490 VADUZ
TELEFON +423 230 13 23 · FAX +423 230 13 24 · INFO@BANKENVERBAND.LI · WWW.BANKENVERBAND.LI

28. Art. 21 – Verwaltungsübertretungen

Auch bezüglich der in Art. 21 CSG vorgesehenen Sanktionsmöglichkeiten bitten wir um Sicherstellung, dass es zu keiner Doppelbestrafung kommt, wenn wegen desselben Tatbestands auch aus aufsichtsrechtlicher Sicht eine Sanktionierung erfolgt.

29. Art. 22 - Inkrafttreten

Das Inkrafttreten ist derzeit – evtl. aus legistischen Gründen – auf den Tag nach der Kundmachung festgelegt. Wir bitten jedoch, eine Kopplung an das Inkrafttreten des EWR-Übernahmebeschlusses zur Richtlinie (EU) 2016/1148 vorzusehen (zumindest in den Materialien).

III. Fazit

Der Entwurf des CSG regelt viele wichtige Aspekte im Hinblick auf die Sicherheit von Netz- und Informationssystemen und die Resilienz gegenüber Cyberbedrohungen sowie anderen Sicherheitsvorfällen. Es bedarf jedoch einer zielgerichteten Abstimmung auf bereits bestehende und zeitnah in Kraft tretende sektorale Vorgaben in diesem Bereich, um Duplizitäten zu vermeiden.

Wir möchten daher nochmals den eingangs gemachten Vorschlag einer gemeinsamen Auslegeordnung der zuständigen Behörden vor Einführung des CSG für den Sektor Bankwesen hinsichtlich der Überschneidungen mit der PSD II (ZDG), eIDAS-VO (SigVG), DSGVO (DSG), anerkannten (internationalen) Standards (z.B. ISO 27001/27002, NIST, MaRisk/BIAT etc.), den aufsichtsrechtlichen Vorgaben der europ. Bankenaufsichtsbehörde EBA bzw. FMA im Bereich IKT Sicherheit und Cybersecurity sowie inskünftig NIS2, DORA und CER hervorheben und dessen Notwendigkeit betonen.

Wir danken für Ihre Kenntnisnahme und Berücksichtigung der vorstehenden Ausführungen und stehen Ihnen bei Fragen selbstverständlich gerne zur Verfügung.

Mit freundlichen Grüssen
LIECHTENSTEINISCHER BANKENVERBAND

Simon Tribelhorn
Geschäftsführer

Dr. Anneka Beccarelli
Tax / Legal

AUSTRASSE 46 · POSTFACH 254 · FL-9490 VADUZ
TELEFON +423 230 13 23 · FAX +423 230 13 24 · INFO@BANKENVERBAND.LI · WWW.BANKENVERBAND.LI