BANK · VERSICHERUNG

Österreichische Finanzmarktaufsicht (FMA)
Otto-Wagner-Platz 5
1090 Wien

**Bundessparte Bank und Versicherung**
Wiedner Hauptstraße 63 | Postfach 320
1045 Wien
T +43 (0)5 90 900-DW | F +43 (0)5 90 900-272
E bsbv@wko.at
W http://wko.at/bsbv

| Ihr Zeichen, Ihre Nachricht vom | Unser Zeichen, Sacharbeiter | Durchwahl | Datum |
|---|---|---|---|
| | BSBV 70/Dr. Egger | 3137 | 22.3.2018 |

**FMA-Leitfaden IT-Sicherheit in Banken**

Sehr geehrte Damen und Herren!

Zum Entwurf eines Leitfadens zur IT-Sicherheit in Banken dürfen wir anmerken, dass wir die Hilfestellung und Konkretisierungen für die Banken sehr zu schätzen wissen. Wir dürfen Ihnen anbei unsere wesentlichen Anmerkungen zum Leitfaden übermitteln.

Generell ist anzumerken, dass nicht klar ist, ob mit dem Leitfaden die IT- oder die Informations-Sicherheit oder beides adressiert werden soll. Oder ist dies als „Sicherheit der IT“ – sohin im Sinne von sicherer Betrieb für die Banken – zu verstehen?
Im gesamten Dokument wird der Begriff „IT“ und „Information“ jeweils mit den dazugehörigen Attributen „Risiko“ und „Sicherheit“ verwendet. Außerdem wird der in den EBA Guidelines herangezogene Begriff „ICT“ – mit Ausnahme eines generellen Hinweises – nicht weiterverwendet bzw. in Betracht gezogen (dies gilt auch zB für die in den EBA Guidelines angeführten Cyber Risiken und dem damit potentiell verbundenen Anstieg der Cyber-Kriminalität). Könnte die vorgesehene Leitlinie in diesem Zusammenhang nicht als Umsetzung der EBA Guidelines zu ICT Risk verstanden werden? Wir ersuchen in diesem Sinne um Klarstellung in Kapitel 1 des Leitfadens.

Im Detail dürfen wir darüber hinaus auf folgende Aspekte hinweisen:

- Seite 3 „Dieser Leitfaden richtet sich primär an Kreditinstitute im Sinne des § 1 Abs. 1 BWG, kann jedoch auch von Zahlungsinstituten, E-Geldinstituten und Sonderkreditinstituten zur Orientierung herangezogen werden.“
  Die Konzession der Betrieblichen Vorsorgekassen ist in § 1 Abs 1 Z 21 BWG geregelt, sie zählen jedoch eindeutig zu den Sonderkreditinstituten. Wir bitten um Klarstellung, dass Betriebliche Vorsorgekassen auch in diesem Zusammenhang zu den Sonderkreditinstituten zählen und die Anwendung des Leitfadens somit fakultativ ist.

- Seite 5, Österreichisches Informationssicherheitshandbuch: hier könnte man als fachspezifische Quelle zB FFIEX für Cybersecurity anführen

- Seite 6: Die Begriffe „Geschäftsleiter“, Geschäftsführung“ und „Unternehmensführung“ werden hier jeweils für den gleichen Aspekt verwendet? Eventuell kann man dies noch einer Vereinheitlichung zuführen bzw. klarstellen, dass

die Begriffe immer die gleiche Zielsetzung verfolgen oder wenn hier unterschiedliche Aspekte angesprochen werden sollen, wäre dies bitte auch entsprechend klarzustellen.

- Seite 6, 4. Absatz („Mit Hilfe der IT-Strategie…"): Die Verankerung von Awareness/Bewusstsein für Informationssicherheit mit Hilfe der IT-Strategie ist unseres Erachtens zu hinterfragen, da uE Sicherheitsbewusstseinsmaßnahmen auch von Instituten geplant, budgetiert und umgesetzt werden müssen. Wir ersuchen den Punkt in diesem Sinne nochmals zu überarbeiten bzw. den Punkt zu streichen.

- Seite 7, Kapitel 3 (IT-Governance), 2. Absatz („Es liegt im Verantwortungsbereich…"): uE stellt eine Trennung Entwicklung/Betrieb nicht unbedingt einen Interessenkonflikt dar. Eine Trennung oder Zusammenlegung ist vielmehr situations- und zielabhängig; teilweise widerspricht dies auch den Prinzipien einer agilen Organisation. Es wird um diesbezügliche Anpassung /Klarstellung ersucht.

- **Seite 9 – Informationssicherheitsmanagement**
  - Im Kapitel 5.1. wird vorgegeben, dass je nach Art, Umfang und Komplexität sowie unter Berücksichtigung der Risikosituation die Funktion eines organisatorisch und prozessual unabhängigen Informationssicherheitsbeauftragten einzurichten ist. Hinsichtlich dieser Anforderung möchten wir darauf hinweisen, dass eine solche Vorgabe den EBA Guidelines nicht zu entnehmen ist. Es ist nicht erkennbar, weshalb diese Funktion (organisatorisch und prozessual) unabhängig zu sein hat. Sensible Bereiche, die in diesem Zusammenhang berührt werden könnten, sind bereits durch entsprechend eingerichtete unabhängige Funktionen geschützt, z.B. der Datenschutzbeauftragte. Gemäß Leitfaden ist diese Funktion im eigenen Institut vor Ort zu etablieren, obwohl der Zugriff auf IT-Dienste nicht ortsgebunden ist.
  - Ad Überwachung der Einhaltung der Informationssicherheitsprozesse und –richtlinien: dies fällt eher in den Verantwortungsbereich eines allfälligen Datenschutzbeauftragten bzw. stellen sich hier – auf Basis der aktuellen Formulierung – entsprechende Abgrenzungsfragen.
  - Ist es zutreffend, dass der Informationssicherheitsbeauftragte (auch) ein Mitarbeiter der IT-Abteilung sein kann, wenn Art, Umfang und Komplexität der betriebenen Geschäfte das zulassen?

- Seite 12, zweiter Absatz: anstelle des Begriffs „vollständig dokumentiert" erscheint uE der Begriff „angemessen dokumentiert" oder „in nachvollziehbarer Weise dokumentiert" sachgerechter bzw. ausreichend. Ziel muss es sein, dass die Änderungen dergestalt erfasst werden, dass auch mit dem Thema bisher nicht im Detail befasste Personen sich in kurzer Zeit einen entsprechenden Überblick über die Änderungen verschaffen können. Eine vollständige Dokumentation von allen möglichen (teilweise kleinsten) Änderungen erscheint in diesem Zusammenhang überzogen.

- Seite 13, Kapitel IT-Betrieb und Datenintegrität: Diesbezüglich ersuchen wir um Klarstellung, wie das Kapitel zu verstehen ist („die Organisationseinheit"), wenn zB die IT zu weiten Teilen ausgelagert ist. Erscheint hier nicht eine Trennung der beiden Begrifflichkeiten sinnvoll zu sein?

- Seite 13, vierter Absatz: Ist hier tatsächlich das Business Continuity Management (BCM) gemeint, oder zielen die IT Spezifika nicht eher auf ein funktionierendes Disaster Recovery (im Sinne einer erfolgreichen Datenwiederherstellung) ab? Es wird um nochmalige Prüfung zu diesem Punkt ersucht.

- **Zu Punkt 8. - IT-Auslagerungen / Faktische Genehmigungspflicht anstelle einer reinen Anzeigepflicht**
  Gemäß § 25 Abs 5 BWG haben KI der FMA die beabsichtige Auslagerungen wesentlicher bankbetrieblicher Aufgaben vor Abschluss einer entsprechenden Vereinbarung schriftlich anzuzeigen.
  Hier ist nach dem vorliegenden Leitfadenentwurf der FMA in Kreditinstituten sodann die Rückmeldung der FMA abzuwarten. Faktisch (und insbesondere gesetzlich) ist das Abwarten der Rückmeldung durch die FMA zwar kein Muss, aber es wäre – vor dem Hintergrund dass die FMA dem Auslagerungsvorhaben nicht zustimmt – eine nachfolgende Vertragsanpassung notwendig; dies führt in der Folge dazu, dass für das KI nicht mehr von einer reinen Anzeigepflicht auszugehen ist, sondern faktisch für jede wesentliche Auslagerung eine Pflicht zur Genehmigung durch die FMA notwendig ist.
  Hier sollte daher zum Ausdruck gebracht werden, dass es sich hierbei um eine Anzeigepflicht handelt und ein Vertrag in jedem Fall abgeschlossen werden kann, ohne dass die Rückäußerung bzw. Zustimmung der FMA notwendig ist. Unbeschadet dessen hat die Aufsichtsbehörde ja ohnehin zu jeder Zeit das Recht, in bestehende Auslagerungen einzugreifen. In zeitkritischen Situationen sollte das KI jedoch nicht durch ein „Überstrapazieren“ gesetzlicher Anzeigepflichten faktische Genehmigungspflichten erhalten bzw. sich zu eigen machen.
  **Fußnote 10 sollte daher gestrichen oder zumindest durch den Zusatz ergänzt werden, dass das KI nicht auf eine (positive) Rückmeldung der FMA für den geplanten Vertragsabschluss warten muss.**
  Alternativ könnte – um hier den Bankbetrieb nicht zu sehr einzuschränken – eine knappe Reaktionszeit der FMA vorgesehen werden.
  Gesetzlich ist hier freilich (da der Gesetzgeber ja von einer reinen Anzeigepflicht und gerade nicht von einer Genehmigungspflicht ausgeht) keine Frist für die Rückmeldung der FMA vorgesehen, sodass im Worst Case von einer Frist von bis zu 6 Monaten (etwa nach allgemeinen Verwaltungsvorschriften) auszugehen sein könnte.
  Da eine derart lange Stillhaltefrist für den Bankbetrieb undenkbar ist, insbesondere da gesetzliche Anforderungen oft kurze Reaktionszeiten erfordern, ist hier eine Maximalfrist für die FMA notwendig. Ergänzend wäre vorzusehen, dass, sollte die FMA innerhalb dieser Frist keine Rückmeldung abgeben, das Auslagerungsvorhaben als gebilligt anzusehen ist. Die Frist, die der FMA als angemessene Bearbeitungsfrist zur Verfügung steht, sollte maximal 2 Wochen bzw. 10 Bankarbeitstage betragen.
  Eine Maximalfrist erscheint vor dem Hintergrund angemessen, dass von der Aufsicht bereits ein einheitliches Excel-File als Vorlage zur Verfügung steht, das ausgefüllt im Detail aufgeschlüsselt bei der Behörde eingereicht wird, und die FMA ohnehin jederzeit in einen bestehenden Vertrag eingreifen kann. Es bedarf hier der Schaffung von hinreichender Rechtssicherheit.
  Weiters ist anzuführen, dass die Materialien zu § 25 Abs 5 BWG lediglich davon ausgehen, dass die auszulagernde Funktion, der beabsichtigte Zeitpunkt des Beginns

der Auslagerung, die wesentlichen rechtlichen Vereinbarungsinhalte und der geplante Vertragspartner hinreichend anzugeben sind.
Das FMA-Excel-Sheet enthält mehr Punkte, die der FMA mitzuteilen sind (z.B. Informationen zur Risikoanalyse im Vorfeld der Auslagerung und Überwachung des Dienstleisters). Eine derart umfangreiche Anzeige geht über die Vorgaben des § 25 Abs 5 BWG hinaus.

- Seite 14, zweiter Absatz: Im Sinne einer besseren Planbarkeit auch für die Kreditinstitute wäre es hilfreich, wenn der Terminus „rechtzeitig“ (im Sinne der Anzeige einer geplanten IT-Auslagerung) eventuell mit einigen Beispielen beschrieben wird, an denen sich die Kreditinstitute orientieren können. Zum Beispiel könnten lediglich Auslagerungen von kleineren Bereichen von gesamthaften Auslagerungen unterschieden werden, ebenso sollte es bei Auslagerungen innerhalb einer KI-Gruppe entsprechende Erleichterungen geben (auch in Bezug auf die „Vorlaufzeit“ einer Anzeige).

- Seite 15, Kapitel 9: Dieses Kapitel vermischt IT-Notfallmanagement und BCM Planung. Nachdem generelle Aspekte im BCM erfasst sind, ersuchen wir in dieser Hinsicht um entsprechende Klarstellung / Überarbeitung.

- Seite 15, letzter Absatz: Der Terminus „Geschäftsfortführungs- und“ ist bitte zu streichen. Durch Business Continuity-Pläne können heute nur mehr sehr wenige Geschäftsprozesse in einer Bank bei einem IT-Ausfall weitergeführt werden. Ausnahmen bilden Teile des Filialgeschäftes und vereinzelt Geschäftstransaktionen. Aber auch in diesen Fällen ist eine IT (zumindest teilweise) erforderlich.

- Seite 16, erster Absatz („Das Notfallmanagement fußt…“): Diese Aussage ist grundsätzlich korrekt, hat aber mit dem IT-Notfallmanagement nur bedingt etwas zu tun bzw. ist eher in generellen BCM Plänen abgedeckt. Aus diesem Grund wäre dieser Absatz daher bitte zu streichen.

- Seite 16, zweiter Absatz „Störfallmanagement- und Eskalationsprozesse“. Dies kann nur den IT-Dienstleister betreffen, aber nicht ein Kreditinstitut, das diese Tätigkeiten ausgelagert hat. Es wird um diesbezügliche Klarstellung / Anpassung ersucht.

- Seite 16, letzter Absatz: Hier stellt sich die Frage, ob dieser Absatz thematisch nicht einem anderen Kapitel (Informationssicherheitsmanagement) zuzuordnen wäre.

Mit freundlichen Grüßen

Dr. Franz Rudorfer
Geschäftsführer
Bundessparte Bank und Versicherung