FMA

Finanzmarktaufsicht
Liechtenstein

FMA-Merkblatt 2021/2 – Nutzung von Cloud-Dienstleistungen

Orientierungshilfe zur Unterstützung der Finanzdienstleister im Hinblick auf die Nutzung von Cloud-Dienstleistungen.

Referenz:	FMA-MB 2021/2
Adressaten:	Finanzdienstleister in Liechtenstein
Betrifft:	-
Publikationsort:	Website
Publikationsdatum:	13. Dezember 2021
Letzte Änderung:	-

Durch diese Orientierungshilfe werden keine neuen Anforderungen gestellt. Es handelt sich um eine Bereitstellung von Informationen in Bezug auf die Inanspruchnahme von Cloud-Dienstleistungen. Gleichzeitig soll das FMA-Merkblatt den Austausch über die digitale Transformation des Finanzplatzes zwischen den Marktteilnehmern und der FMA anregen.

Die Orientierungshilfe ist weder rechtlich bindend noch ist sie abschliessend.

FMA

Inhalt

1. Allgemeine Ausführungen

1.1 Hintergrund

Eine der wichtigsten Lehren, die aus der 2007 einsetzenden globalen Finanzkrise gezogen wurde, war die Erkenntnis, dass die Informationstechnologie- (IT) und Datenarchitektur vieler Finanzintermediäre für die umfassende Steuerung finanzieller Risiken nicht geeignet war. Seit Jahren entwickelt sich die technische Transformation des Finanzdienstleistungssektors, teilweise getrieben durch verstärkten Wettbewerb durch FinTech-Unternehmen und neuer regulatorischer Vorgaben[1], jedoch rasant. Die den Tätigkeiten der beaufsichtigten Finanzmarktteilnehmer und der Finanzmarktaufsicht zugrundeliegende IT-Infrastruktur zur Unterstützung einer effizienten Erbringung der Finanzdienstleistungen bzw. einer effizienten Aufsicht hat sowohl an Umfang als auch an Komplexität zugenommen.

Ebenso verstärkt sich der Trend zur Nutzung fremder IT-Infrastrukturen über das Internet, wie jene der **Cloud-Dienstleister**, um mit deren Unterstützung dynamisch auf neue technische, geschäftliche oder auch regulatorische Entwicklungen in effizienter und ressourcenschonender Art und Weise zu reagieren.

Die Prominenz der Thematik Cloud-Computing nimmt seit Jahren zu und die verbreitete Nutzung von Cloud-Services ist in vielen Bereichen zum Standard avanciert. Der Finanzsektor ist von dieser Entwicklung nicht ausgenommen, der Einsatz von Cloud-Lösungen wird immer häufiger geprüft und realisiert.

Auch auf dem liechtensteinischen Finanzplatz sind vermehrt Bestrebungen zum Einsatz von Cloud-Lösungen feststellbar. Es bestehen allerdings (rechtliche) Unsicherheiten in Bezug auf die Nutzung von Cloud-Dienstleistungen. Neben einem einleitenden Überblick zu Begrifflichkeiten und technischen Spezifikationen, zeigt das gegenständliche Dokument die geltenden rechtlichen Grundlagen (inkl. möglicher Weiterentwicklungen) auf. Schliesslich wird die Anwendbarkeit der rechtlichen Grundlagen in einem praktischen Wegweiser *(siehe Kapitel 4)* sowie mögliche Anwendungsbeispiele an Hand von Erfahrungen aus der Praxis dargelegt *(siehe Kapitel 5.1)*.

1.2 Adressaten

Das gegenständliche Merkblatt richtet sich an alle in Liechtenstein tätigen Finanzdienstleister.

1.3 Rechtshinweis

Dieses Merkblatt hat keinen Anspruch auf Vollständigkeit und ist ohne jegliche Rechtsverbindlichkeit. Normative Vorgaben, etwa aus Gesetz, Verordnung oder Richtlinie (z.B. «FMA Richtlinie 2021/3 zur IKT-Sicherheit») gelten ungeachtet der im Merkblatt getroffenen Aussagen, Erwartungshaltungen oder Empfehlungen. Auch sonstige europäische Konvergenzinstrumente, wie etwa Leitlinien und Empfehlungen der ESA, gelten ungeachtet der vorliegenden Auslegeordnung.

[1] Siehe unter anderem *BCBS*, Principles for effective risk data aggregation and risk reporting (BCBS 239).

2. Grundlagen «Cloud»

2.1 Begrifflichkeit Cloud-Computing

Es gibt verschiedene Definitionen für den Begriff Cloud-Computing. Eine allgemeingültige Auslegung hat sich bislang nicht durchgesetzt. Häufig wird die Definition der US-amerikanischen Standardisierungsstelle NIST (National Institute of Standards and Technology) verwendet:

"Cloud-Computing ist ein Modell, das es erlaubt bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z.B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können." [2]

Gemäss NIST-Definition zeichnet sich Cloud-Computing durch fünf Eigenschaften aus:

- **On-demand Self Service:** Der Cloud-Nutzer kann automatisch und ohne Interaktion mit dem Service Provider Ressourcen (z.B. Rechenleistung, Speicher) beziehen.
- **Broad Network Access:** Die Cloud-Services sind mit Standard-Mechanismen über das Netz verfügbar und können von unterschiedlichsten Endgeräten (z.B. Mobiltelefon, Tablet, stationärer PC) verwendet werden.
- **Resource Pooling:** Die angebotenen Ressourcen (z.B. Speicher, Verarbeitung, Netzwerkbandbreite) werden in einem Pool vorrätig gehalten und können von vielen Cloud-Nutzern gleichzeitig bezogen werden (Multi-Tenant Modell). Dabei wissen die Nutzer jedoch nicht, wo sich die Ressourcen befinden.
- **Rapid Elasticity:** Die Cloud-Services können bedarfsbezogen und schnell zur Verfügung gestellt werden. Daher scheinen für den Anwender die Ressourcen auch unendlich zu sein.
- **Measured Services:** Zwecks Optimierung kann die Ressourcennutzung automatisch gemessen und überwacht werden.

Weiters spricht das NIST grundsätzlich von drei Varianten der Cloud-Nutzung:

- **Software as a Service (SaaS):** Der Kunde nutzt Software, die bei einem externen IT-Dienstleister betrieben wird. Dabei muss sich der Kunde nicht um die darunterliegende IT-Infrastruktur und deren Betrieb kümmern, er braucht lediglich ein internetfähiges Gerät für die Nutzung.
- **Platform as a Service (PaaS):** Hier wird dem Kunden eine komplette Infrastruktur zur Software-Entwicklung bereitgestellt. Dabei handelt es sich um schnell einsetzbare Tools, Bibliotheken und Services, die vom Anbieter bereitgestellt werden. Der Vorteil für den Kunden liegt neben der Skalierbarkeit darin, dass er einen geringen administrativen Aufwand hat und die darunterliegende Hard- und Software nicht anschaffen muss.
- **Infrastructure as a Service (IaaS):** Bei diesem Service bezieht der Kunde je nach Bedarf IT-Ressourcen wie z. B. Rechenleistung, Datenspeicher oder Netze. Diese Services sind hochgradig standardisiert und virtualisiert und somit schnell verfügbar. Der Kunde kann darauf sein Betriebssystem und seine Anwendungen betreiben.

[2] Abzurufen unter: NIST SP 800-145, The NIST Definition of Cloud Computing (Juni 2021)

Das NIST unterscheidet grundsätzlich vier Bereitstellungsmodelle:

- **Private Cloud:** Die Cloud-Infrastruktur wird nur für ein Unternehmen betrieben. Die Organisation und der Betrieb der Cloud können dabei durch das Unternehmen selbst oder von Dritten ausgeführt werden. Die Cloud kann im eigenen Rechenzentrum oder in einem fremden Unternehmen stehen.
- **Community Cloud:** Hier wird die Cloud-Infrastruktur mehreren Unternehmen, welche gemeine Interessen teilen, zur Verfügung gestellt. Die Cloud wird von einem oder mehreren dieser Unternehmen oder von einem Dritten betrieben.
- **Public Cloud:** Die Cloud-Infrastruktur wird der breiten Öffentlichkeit zur Verfügung gestellt. Der Anbieter kann ein privatwirtschaftliches Unternehmen, eine öffentliche oder akademische Organisation sein – eine Kombination ist auch denkbar.
- **Hybrid Cloud:** Mehrere eigenständige Cloud-Infrastrukturen (Private, Community, Public), welche über standardisierte Schnittstellen gemeinsam genutzt werden.

2.2 Unterschiede zwischen Cloud-Computing und IT-Outsourcing

Beim klassischen IT-Outsourcing werden Arbeits-, Produktions- oder Geschäftsprozesse einer Organisation ganz oder teilweise zu externen Dienstleistern ausgelagert. Dabei wird von einem Kunden die Infrastruktur gemietet und exklusiv genutzt, auch wenn Outsourcing-Anbieter normalerweise noch weitere Kunden haben. Im Regelfall werden Outsourcing-Verträge über längere Zeiträume abgeschlossen.[3]

Cloud-Services sind dem klassischen IT-Outsourcing sehr ähnlich, weisen jedoch einige markante Unterschiede auf: [4]

- Die Teilung einer gemeinsamen Cloud-Infrastruktur durch mehrere Nutzer (Kostenvorteile).
- Cloud-Services sind dynamisch und können dadurch schneller nach oben und unten skaliert werden. Dementsprechend ist eine bedarfsgerechte Nutzung möglich. So können z.B. Belastungsspitzen individuell abgedeckt werden.
- Der Cloud-Nutzer steuert in aller Regel die von ihm genutzten Cloud-Dienste und Ressourcen selbst mittels einer Web-Schnittstelle und ist somit flexibel in seiner Bedürfnisabdeckung. Die Administration erfordert dabei wenig Interaktion mit dem Provider.
- Cloud-Dienste können über verschiedene Standorte verteilt sein (geographisch weit voneinander entfernt).

Bei Cloud-Computing handelt es sich im Regelfall, sobald dieses von einem Cloud-Anbieter für ein Unternehmen erbracht wird, **um eine IT-Auslagerung**, und wird regulatorisch entsprechend behandelt. Die Nutzung von Cloud-Dienstleistungen gilt regulatorisch nicht *per se* als risikoverändernd. Die konkreten Auswirkungen auf das Risikoprofil sind stets im Einzelfall zu beurteilen. Regulatorisch sind jedoch (zumindest) die Vorgaben der Leitlinien der Europäischen Finanzaufsichtsbehörden (ESAs) zusätzlich zu beachten *(siehe Kapitel 3.3)*.

---

[3] Vgl. *BSI*, Cloud Computing Grundlagen, abzurufen unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen_node.html;jsessionid=6C184975094F55E7C6ABFA2D572BB3F3.internet472 (Juni 2021).

[4] Vgl. *BSI*, Cloud Computing, Grundlagen (2021).

3. Rechtliche Rahmenbedingungen im Aufsichtsrecht

3.1 Generelles

Sowohl das liechtensteinische Finanzmarktrecht als auch die liechtensteinische Datenschutzgesetzgebung sind grundsätzlich technologieneutral ausgestaltet. Die Thematik „Cloud“ ist daher im Regelfall legistisch nicht spezifisch geregelt. Bei der Nutzung von Cloud-Diensten sind die von den einschlägigen Gesetzen definierten Grundsätze zu beachten, eine Einzelfallprüfung ist erforderlich. Im Kontext des Finanzmarktrechts sind in Bezug auf die Nutzung von Cloud-Dienstleistungen insbesondere Bestimmungen für die Auslagerung von Funktionen durch beaufsichtigte Finanzmarktteilnehmer relevant. Im Bereich des Datenschutzes stehen die für jegliche Verarbeitung personenbezogener Daten geltenden Grundsätze im Vordergrund. Ein anderer wesentlicher Aspekt ist die Sicherheit von IT-Systemen (Cybersecurity).

Die relevanten Rechtsgrundlagen für die Auslagerung von Funktionen durch beaufsichtigte Finanzmarktteilnehmer ergeben sich aus den in Art. 5 Abs. 1 FMAG (Finanzmarktaufsichtsgesetz) aufgelisteten Spezialgesetzen. Daneben haben die Europäischen Aufsichtsbehörden EBA[5], ESMA[6] und EIOPA[7] (zusammen ESAs) Leitlinien für die Auslagerung von Funktionen an Dritte generell und speziell an Cloud-Dienstleister festgelegt *(siehe sogleich unten)*, wobei spezialgesetzliche Vorschriften zur Delegation von Aufgaben unberührt bleiben. Die Leitlinien richten sich gewöhnlich an die jeweils betroffenen Finanzmarktteilnehmer und die zuständigen Aufsichtsbehörden. Leitlinien sind von der FMA als anwendbar zu erklären, soweit keine berechtigten Gründe dagegensprechen. Diese ESAs-Leitlinien bilden zudem die Grundlage des Punktes 10 «Auslagerung (inkl. Cloud)» der FMA Richtlinie 2021/3 zur IKT Sicherheit in Verbindung mit der FMA-Wegleitung 2021/17 zur Umsetzung der IKT-Sicherheit, welche jeweils am 1. Januar 2022 in Kraft treten werden. Gleichzeitig wird die FMA-Mitteilung 2018/3 zum Umgang mit Cyber-Risiken ausser Kraft gesetzt. Eine besondere Bedeutung kommt den datenschutzrechtlichen Bestimmungen zu.

3.2 Spezialgesetzgebung

3.2.1 Allgemeines

Aus Sicht der Finanzmarktgesetzgebung sind insbesondere die Themenkreise *Auslagerung/Delegation, Datenlagerung/Aufbewahrung* sowie *Datenschutz/IKT-Sicherheit* relevant. Grundsätzlich basieren die Regelungen auf EWR-rechtlichen Grundlagen. In den in Punkt 3.2.2 angeführten Finanzmarktgesetzen finden sich nationale Besonderheiten, deren Überprüfung notwendig werden könnte.

3.2.2 Besondere Bestimmungen

3.2.2.1 Sorgfaltspflichtgesetz (SPG)/Sorgfaltspflichtverordnung (SPV):

Art. 24 Abs. 7 SPG (betrifft die FMA) und Art. 27 Abs. 1 Bst. d SPG (betrifft die von der FMA mit der Durchführung von Sorgfaltspflichtkontrollen beauftragten Wirtschaftsprüfer) bestimmen, dass Unterlagen und Daten von Sorgfaltspflichtkontrollen ausschliesslich im Inland verarbeitet und gelagert werden dürfen. Nach Art.

---

[5] Europäische Bankenaufsichtsbehörde: www.eba.europa.eu

[6] Europäische Wertpapier- und Marktaufsichtsbehörde: www.esma.europa.eu

[7] Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung: www.eiopa.europa.eu

28 Abs. 5 SPV (betrifft die sorgfaltspflichtigen Finanzintermediäre) sind Sorgfaltspflichtakten an einem jederzeit zugänglichen Ort im Inland aufzubewahren.

3.2.2.2 Vermögensverwaltungsgesetz (VVG)

In Art. 12 Abs. 1 VVG wird einerseits die Delegation von Haupttätigkeiten nach Anhang 1 Abschnitt A MiFID verboten. Andererseits wird nach Abs. 3 die Aufbewahrung von Unterlagen, insbesondere zu personenbezogenen Daten, einschliesslich personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten und andere für die Aufsicht notwendigen Unterlagen im Inland verpflichtend vorgeschrieben.

3.2.2.3 Wirtschaftsprüfergesetz (WPG)

Art. 43 WPG fordert die Aufbewahrung der Abschlussprüfungsberichte im Inland.

3.3 Leitlinien der europäischen Finanzaufsichtsbehörden (ESAs)

Die europäischen Finanzaufsichtsbehörden EBA, ESMA, EIOPA erliessen in ihren jeweiligen Zuständigkeitsbereichen Leitlinien[8] betreffend Auslagerung/Outsourcing (an Cloud-Dienstleister). Die Leitlinien der ESAs adressieren die Thematik Cloud entweder spezifisch (ESMA, EIOPA) oder über die Thematik «Auslagerungen» (EBA). Materiell sind die Leitlinien der ESAs als weitgehend deckungsgleich zu erachten. Da die Leitlinien der ESMA die zeitlich jüngsten Leitlinien sind, dienen diese im Folgenden als Gegenstand der Analyse.

Die **EBA-Leitlinien** zur Auslagerung[9] richten sich an CRR-Institute, Zahlungsinstitute und E-Geld-Institute, wurden seitens EBA im Februar 2019 erlassen und beinhalten u.a. die internen Governance-Regelungen, die Letztere einhalten sollten, sofern sie Funktionen auslagern. Die **ESMA-Leitlinien**[10] richten sich an AIFM und Verwahrstellen von AIF, OGAW-Verwaltungsgesellschaften und Verwahrstellen von OGAW, OGAW, Banken und Wertpapierfirmen im Rahmen der Erbringung von Wertpapierdienstleistungen und der Ausübung von Anlagetätigkeiten, Datenbereitstellungsdienste, Betreiber von Handelsplätzen, Zentrale Gegenparteien (CCP) einschliesslich Tier-2-Drittstaaten CCP, Transaktionsregister, Zentralverwahrer, Ratingagenturen, Verbriefungsregister und Administratoren von Referenzwerten. Soweit es sich um eine Auslagerungsvereinbarung mit Cloud-Anbietern handelt, sind auch Auslagerungen an eine Firma oder einen Dritten umfasst, die bzw. der kein Cloud-Anbieter ist, aber in erheblichen Masse auf einen Cloud-Anbieter zurückgreift, um eine Funktion wahrzunehmen, die die Firma sonst selbst wahrnehmen würde. Die **EIOPA-Leitlinien**[11] richten sich an Versicherungs- und Rückversicherungsunternehmen.

---

[8] Leitlinien der ESAs sind Konvergenzinstrumente, die festlegen, was nach Ansicht der ESAs angemessene Aufsichtspraktiken innerhalb des Europäischen Finanzaufsichtssystems sind bzw. wie das Unionsrecht in einem bestimmten Bereich anzuwenden ist. Die zuständigen Behörden sollten die für sie geltenden Gemeinsamen Leitlinien in geeigneter Weise (z. B. durch eine Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren) in ihre Aufsichtspraktiken integrieren, und zwar auch dann, wenn bestimmte Gemeinsame Leitlinien primär an Institute gerichtet sind

[9] EBA/GL/2019/02, 25. Februar 2019 (anwendbar ab 30 September 2019 für bestehende und neue Verträge, wobei Anpassungen spätestens bis 31. Dezember 2021 sicherzustellen sind);

[10] ESMA50-164-4285, 10. Mai 2021 (anwendbar ab 31.Juli 2021 für bestehende und neue Verträge, wobei Anpassungen spätestens bis 31. Dezember 2022 sicherzustellen sind).

[11] EIOPA-BoS-20-002, 6. Februar 2020 (anwendbar ab 1. Januar 2021);

Die Leitlinien der ESAs finden in Liechtenstein Anwendung.

3.3.1 Wesentliche Regelungsinhalte

Die genannten Leitlinien der ESAs verfolgen im Wesentlichen dasselbe Ziel, die Inhalte sind somit vergleichbar. Im Folgenden werden insbesondere die zentralen Regelungsinhalte der Leitlinien (anhand der Struktur der ESMA-Leitlinie) zusammengefasst und auf prinzipienbasierte Art und Weise dargestellt.[12]

3.3.1.1 Leitlinie 1 – Governance, Kontrolle und Dokumentation

In diesem Kontext ist eine Auslagerungsstrategie zu erstellen, die laufend zu überprüfen und entsprechend anzupassen ist. Die Strategie hat Grundsätze, Verantwortlichkeiten und Prozesse (Dokumentation, Verwaltung und Kontrolle, risikobasierte Überwachung der Cloud-Anbieter) zu definieren, die in allen Phasen eines Outsourcing-Prozesses sowohl auf Ebene des Einzelunternehmens als auch auf Gruppenebene einzuhalten sind. Des Weiteren hat die Auslagerungsstrategie im Einklang mit den internen Weisungen und Reglementen, Strategien und Prozessen, insbesondere in Bezug zu Informations- und Kommunikationstechnologie, Informationssicherheit sowie operationellem Risikomanagement zu sein. Es ist ein Register zu führen, wobei die Auslagerung von kritischen oder wichtigen Funktionen eigens auszuweisen sind. Die Finanzmarktteilnehmer müssen jederzeit über ausreichend Substanz verfügen, um ihren gesetzlichen Pflichten nachzukommen bzw. die Verantwortung dafür tragen und die Kontrolle über alle ausgelagerten Funktionen ausüben zu können.

3.3.1.2 Leitlinie 2 – Risikoanalyse der Auslagerung und Due-Diligence

Im Rahmen der Prüfung einer Auslagerung haben alle betroffenen Finanzmarktteilnehmer entsprechend der Natur, dem Ausmass und der Komplexität ihres Geschäftsmodells (Proportionalität) unter Berücksichtigung der den ausgelagerten Funktionen inhärenten Risiken und des Systemrisikos angemessene Analysen und Vorprüfungen vorzunehmen. Vor Abschluss einer Auslagerungsvereinbarung (mit Cloud-Anbietern) sollten die Finanzmarktteilnehmer Analysen in Bezug auf folgende Fragestellungen vornehmen:

- die Betroffenheit kritischer oder wesentlicher operativer Funktionen/Tätigkeiten;
- einschlägige Risiken der Vereinbarung zu (Cloud-)Outsourcing;
- Due-Diligence Prüfung des potentiellen Dienstleisters;
- Identifikation möglicher Interessenkonflikte.

Die Risikoanalyse der Auslagerung und Due-Diligence-Prüfung des Cloud-Anbieters stehen unter dem Aspekt der Verhältnismässigkeit in Bezug auf Art, Umfang und Komplexität der auszulagernden Funktion und deren inhärenten Risiken. Soweit kritische oder wesentliche Funktionen betroffen sind insbesondere auch die Risiken betreffend die IKT-Sicherheit, Informationssicherheit, Fortführung der Geschäftstätigkeit oder operationelle Risiken zu beurteilen. Die Due-Diligence sollte in solchen Fällen eine Bewertung der Eignung des Cloud-Anbieters (z.B. Reputation, Qualifikation, IT-Ressourcen, finanzielle Mittel, Organisation, Zulassung/Registrierung) beinhalten und diese laufende überprüfen.

[12] Im konkreten Anlassfall ist jedenfalls die für den jeweiligen Finanzintermediär geltende Leitlinie zu konsultieren.

3.3.1.3 Leitlinie 3 – Zentrale Bestandteile des Vertrags

Rechte und Pflichten der Vertragspartner sind klar und verständlich in einem schriftlichen Vertrag mit Beendigungsmöglichkeit festzulegen. Im Fall der Auslagerung von kritischen oder wichtigen Funktionen sind insbesondere folgende Inhalte im Vertrag zu regeln:

- eine klare Beschreibung der ausgelagerten Funktion sowie gegenseitige Rechte und Pflichten («Rollenverteilung»);
- Beginn und Ende der Vereinbarung sowie eine gegenseitige Kündigungsregelung;
- Zulässigkeit der Inbezugnahme von Subunternehmern;
- das anwendbare Recht (Gerichtsstandklausel);
- die gegenseitigen finanziellen Pflichten;
- eine Regelung über das Recht zu Unter-Auslagerungen;
- den Ort (Region, Land) der Dienstleistungserbringung, der Datenspeicherung und -verarbeitung inklusive der Anforderungen an einen Wechsel des Ortes durch den Cloud-Dienstleister;
- Regelungen betreffend den Zugang, die Verfügbarkeit und die Sicherheit aller Daten;
- das Recht des jeweiligen Finanzmarktteilnehmers zur laufenden Kontrolle der Cloud-Dienstleistungserbringung;
- die vereinbarte Dienstleistung/Service Level unter Angabe qualitativer und quantitativer Ausführungsziele;
- die Berichtspflichten des Cloud-Dienstleisters;
- die Möglichkeit bzw. Pflicht zum Abschluss einer Haftpflichtversicherung seitens des Dienstleistungsanbieters;
- die Erstellung von Geschäftskontinuitäts- und Notfallplänen sowie unverzügliche Meldepflicht von Störfällen;
- die Angabe ob, und wenn ja in welchem Ausmass, der Cloud-Dienstleister für bestimmte Risiken eine Versicherung abzuschliessen hat;
- die Anforderung an den Dienstleister, dem jeweiligen Finanzmarktteilnehmer, seinen Aufsichtsbehörden und etwaigen anderen benannten Personen (z.B. Revisionsstellen), uneingeschränkte Zugangs- und Prüfungsrechte in Bezug auf alle relevanten Geschäftsräume inkl. aller einschlägiger Einrichtungen, Systeme, Netzwerke etc., die für die Ausführung der ausgelagerten Funktion von Relevanz sind, einzuräumen;
  die Gewährleistung des Zugangs zu allen Daten, die im Auftrag des Finanzmarktteilnehmers verarbeitet oder gespeichert werden sowie deren Aussonderung im Insolvenzfall;
- die Gewährleistung, dass die Daten, die der Cloud-Anbieter im Auftrag der Firma verarbeitet oder speichert, bei Bedarf abgerufen, wiederhergestellt und an die Firma zurückgegeben werden können.

3.3.1.4 Leitlinie 4 – Informationssicherheit

Finanzmarktteilnehmer sollten die geltenden Informationssicherheitsbestimmungen und -prozesse im Auslagerungsvertrag festschreiben und deren Einhaltung in regelmässigen Abständen überprüfen. Diese Anforderung gilt auch für vertrauliche, persönliche oder sonstige sensible Daten. Im Falle der Auslagerung von kritischen oder wichtigen Funktionen ist – bei Berücksichtigung der geltenden Datenschutzbestimmungen – zumindest Folgendes zu regeln:

- Informationssicherheitsorganisation: Klare Rollen- und Verantwortlichkeitszuordnung zwischen den Vertragsparteien in Bezug auf Bedrohungserkennung, Notfallmanagement etc.;

- Identitäts- und Zugriffsmanagement: starke Authentifizierungsmechanismen und Zugangskontrollen, die den gegenseitigen Zugriff einschränken;
- Verschlüsselung und Schlüsselmanagement: Verwendung angemessener Verschlüsselungstechnologien für die Übermittlung, Speicherung etc. von Daten;
- Betriebs- und Netzwerksicherheit: Gewährleistung von ausreichender Netzwerkverfügbarkeit, Netzwerktrennung und Verarbeitungsumgebungen;
- Anwendungsprogrammierschnittstellen (API): Sicherstellung von Mechanismen für die Integration der Cloud-Dienstleistungen;
- Geschäftskontinuitäts- und Notfallwiederherstellung: entsprechende Pläne und Kontrollen sicherstellen;
- Datenspeicherort: risikobasierte Auswahl eines Standorts;
- Einhaltung und Überwachung: kontinuierliche Überprüfung der Einhaltung der Informationssicherheitsstandards durch den Cloud-Dienstleister.

3.3.1.5 Leitlinie 5 – Ausstiegsstrategien

Die Finanzmarktteilnehmer sollten in der Lage sein, einen bestehenden Auslagerungsvertrag ohne unzumutbare Beeinträchtigung der Geschäftstätigkeiten und der Dienstleistungen gegenüber den Kunden sowie ohne Verletzung von Aufsichtspflichten, Verschwiegenheitspflichten und der Datenintegrität zu beenden. Zu diesem Zweck sind tragfähige Ausstiegspläne mit Regelungen zu Übergangslösungen und zur ordnungsgemässen Rückführung sämtlicher Funktionen zu erstellen. In diesem Zusammenhang sind folgende Punkte relevant:

- die Definition umfassender, überprüfter und regelmässig aktualisierter Ausstiegspläne;
- die Definition der Kriterien, die den Ausstieg bedingen, insbesondere die Vertragsbeendigung oder grobe Fehlleistungen;
- die Durchführung einer Auswirkungsanalyse entsprechend der ausgelagerten Funktion;
- klare Rollen- und Verantwortlichkeitszuteilung für die Durchführung des Ausstiegs;
- die Prüfung der Angemessenheit der Ausstiegsstrategie unter Verwendung eines risikobasierten Ansatzes;
- die Definition von Erfolgskriterien der Rückabwicklung.

3.3.1.6 Leitlinie 6 – Zugangs- und Prüfungsrecht

Sowohl das auslagernde Unternehmen als auch die zuständige Aufsicht sollen nach angemessener Vorankündigung uneingeschränkt Zugang zum Cloud-Anbieter haben und Prüfungen durch qualifiziertes Personal vornehmen können. Wenn für die Umgebung des Cloud-Anbieters bzw. für einen seiner Kunden damit ein Risiko verbunden sein sollte (z.B. Vertraulichkeit, Integrität und Verfügbarkeit von Daten) ist dies klar zu begründen und es sind alternative Zugangs- und Prüfrechte anzubieten. Zur Effizienzsteigerung können auch Zertifizierungen Dritter oder externe oder interne Prüfberichte vom Cloud-Anbieter angeboten werden oder Sammelprüfungen vorgenommen werden. Bei kritischen oder wesentlichen Funktionen sollte auf externe oder interne Zertifizierungen nur zurückgegriffen werden, wenn:

- die Schlüsselsysteme des Cloud-Anbieters (z.B. Prozesse, Anwendungen, Infrastruktur, Rechenzentren), die zentralen Kontrollen und die Einhaltung der relevanten Rechtsvorschriften abgedeckt wird;
- eine regelmässige Prüfung solcher Zertifizierungen erfolgt und diese nicht veraltet sind und die Zertifizierung eine gute Qualität aufweist;

- angemessene Standards eingehalten werden;
- das vertragliche Recht vorbehalten wird, nach eigenem Ermessen einzelne Vor-Ort-Prüfungen der ausgelagerten Funktionen vorzunehmen.

3.3.1.7 Leitlinie 7 – Sub-Auslagerung

Bei der Auslagerung von kritischen oder wesentlichen Funktionen an Subunternehmer ist vom Cloud-Dienstleister für sich eine angemessene Kontrollmöglichkeit sicherzustellen und folgendes in der schriftlichen Vereinbarung vorzusehen:

- von der Sub-Auslagerung nicht betroffene Funktionen;
- allfällige Bedingungen für eine Sub-Auslagerung;
- Festlegung der Verantwortlichkeit des Cloud-Dienstleisters;
- Informationspflicht für Cloud-Dienstleister gegenüber der auslagernden Firma und Gewährleistung eines Widerspruchsrechts bzw. Beendigungsrechts.

3.3.1.8 Leitlinie 8 – Information an die zuständigen Behörden

Die zuständigen Behörden sollten über beabsichtigte Auslagerungsvereinbarungen betreffend kritische oder wesentliche Funktionen informiert werden. Finanzintermediäre sollten jederzeit in der Lage sein, zumindest folgende Informationen jederzeit vorlegen zu können:

- Datum des Beginns, der Verlängerung oder Beendigung des Vertrags;
- Kurzbeschreibung der ausgelagerten Funktion;
- Kurzzusammenfassung der Gründe für die Auslagerung;
- Name des Cloud-Anbieters, Sitz, LEI, Registrierungsnummer;
- Anwendbares Recht, ggf. Wahlgerichtsstand;
- Bereitstellungsmodell der Cloud-Dienste;
- Datum der letzten Bewertung der Kritikalität oder Wesentlichkeit der ausgelagerten Funktionen;
- Datum der letzten Risikoanalyse und Due-Diligence;
- Entscheidungsträger betreffend der Auslagerungsvereinbarung;
- ggf. Namen von Subunternehmern.

3.3.1.9 Leitlinie 9 – Überwachung von Auslagerungsvereinbarungen mit Cloud-Anbietern

Die Aufsichtsbehörden haben im Rahmen ihres Aufsichtsverfahrens eine Risikoeinschätzung zu den Cloud-Vereinbarungen der betroffenen Firmen vorzunehmen. Der Fokus ist dabei auf die Auslagerung kritischer oder wichtiger operativer Funktionen oder Tätigkeiten zu legen. Die Aufsichtsbehörden haben risikobasiert zu prüfen, ob die Finanzmarktteilnehmer über die entsprechende Unternehmensführung, die Ressourcen und die betrieblichen Prozesse verfügen, um in angemessener Weise Auslagerungsverträge in die Cloud einzugehen und die damit verbundenen Risiken verwalten zu können. Konzentrationsrisiken sollen jedenfalls vermieden werden. Die zuständigen Behörden haben sich zudem zu vergewissern, dass eine wirksame Aufsicht sichergestellt ist.

3.4 Sonstige Bestimmungen

Die europäische **Datenschutz**-Grundverordnung (DSGVO) findet – neben dem liechtensteinischen Datenschutzgesetz (DSG) – in Liechtenstein Anwendung. Auch diese Rechtsgrundlagen sind technologieneutral formuliert und es gelten für die Inanspruchnahme von Cloud-Dienstleistungen die generellen Grundsätze in Bezug auf den Umgang und die Verarbeitung personenbezogener Daten. So werden Anbieter von Cloud-

Dienstleistungen im Regelfall einen Auftragsverarbeitungsvertrag abzuschliessen und angemessene technische und organisatorische Massnahmen einzuhalten haben.

Besonders schützenswerte Daten in diesem Zusammenhang sind unter anderem genetische, biometrische und (sonstige) Gesundheitsdaten (Art. 9 Abs. 1 DSGV). Bei Angaben zu Einkommens- und Vermögensverhältnissen (z.B. betreffend MiFID Angemessenheits-/Eignungstest) handelt es sich im Regelfall zwar um Personendaten, diese gelten aber nicht als besonders schützenswert (vgl. Art. 9 DSGV: wirtschaftliche Aspekte sind in der Definition nicht aufgeführt). Neben den Bestimmungen der DSG bestehen spezialgesetzliche Vorschriften, z.B. Finanzmarktgesetze (Berufs-/Bankgeheimnis), die neben dem DSG zwingend zu beachten sind.

Im Weiteren kann im Hinblick auf die zu beachtenden Datenschutzbestimmungen bei der Nutzung von Cloud Services auf die Webseite der Datenschutzstelle (www.datenschutzstelle.li) verwiesen werden.

Im Hinblick auf die **IKT-Sicherheit** kann hingegen auf die Verordnung (EU) 2019/881 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik verwiesen werden. Sie wird für Cloud Dienstleistungen eine IKT-Sicherheitszertifizierung vorsehen, um das Vertrauen in die Cloud im Rahmen der Nutzung für Finanzdienstleistungen und durch Regulierungsbehörden zu stärken. Daneben werden auch andere EU-Rechtsakte, die sich mit der **Sicherheit von Netz- und Informationssystemen** (z.B. NIS-Richtlinie (EU) 2016/1148) und der Betriebsstabilität digitaler Systeme im Finanzsektor (z.B. Vorschlag Verordnung C(2020) 595; DORA), die Cloud-Dienstleister betreffen, in Liechtenstein nach deren Übernahme in das EWR-Abkommen bzw. Umsetzung ins nationale Recht anwendbar und künftig bei Inanspruchnahme von Cloud-Dienstleistungen zu beachten sein.

Auslagerungen, auch an Cloud-Dienstleister, dürfen nicht dazu führen, die Unternehmenssubstanz, z.B. bezogen auf die inländische Hauptverwaltung, auszuhöhlen. Gesetzliche bzw. allfällige Vorgaben der FMA sind jederzeit zu beachten.

3.5 Fazit

- Die europäischen und liechtensteinischen Finanzmarktrechtsakte sind **grundsätzlich technologieneutral** und sehen, abgesehen von den in Kapitel 3.2.2 genannten besonderen Bestimmungen, keine spezifischen bzw. einschränkende Bestimmungen für die Nutzung von Cloud Dienstleistungen vor;
- Für die Nutzung von Cloud-Dienstleistungen bedarf es einer **Einzelfallprüfung** – relevant sind insbesondere Bestimmungen zu Auslagerung/Delegation, Datenschutz und -Lagerung sowie IKT-Sicherheit;
- Die **Leitlinien der ESAs** betreffend Auslagerungen geben einen Rahmen für die Nutzung von Cloud-Dienstleistungen durch Finanzmarktteilnehmer und die diesbezügliche Aufsicht durch die zuständigen Behörden vor. Diese Leitlinien sind für Liechtenstein relevant;
- Die aktuellen europäischen Regulierungsinitiativen (Digital Finance Package (MICA, Pilotregime, DORA etc.) sowie Cybersecurity- und NIS-Regulierungen) sind zu beobachten bzw. zu implementieren, da die Rechtsakte Cloud-relevante Aspekte beinhalten;
- Die liechtensteinischen Finanzmarktgesetze sind weiterhin auf deren Aktualität laufend zu überprüfen und gegebenenfalls spezifisch anzupassen.

4. Praktischer Wegweiser

4.1 Cloud-Migration

Die Entscheidung, unternehmensinterne Daten- und Infrastrukturen in eine Cloud zu migrieren, sollte erst nach einer umfassenden Risikoanalyse getroffen werden. Dabei sollte berücksichtigt werden, welche Risiken mit einer mangelhaften Erbringung oder (teilweisen) Ausfall der Cloud-Dienstleistungen einhergehen. Die Risikoanalyse sollte ebenso die in Betracht kommenden vertraglichen Laufzeiten und den Zeithorizont nach dem potentiellen Auslaufen der Verträge mit dem Anbieter erörtern. Ebenso sollte in der Risikoanalyse dokumentiert werden, welche Auswirkungen die Migration auf die kritischen Funktionen des Unternehmens generiert und ob es sich um eine wesentliche Auslagerung handelt. Hat sich ein Unternehmen nach einer umfassenden Risikoanalyse dazu entschlossen, Systeme teilweise oder vollständig in eine oder mehre Clouds zu migrieren, so stellen sich zahlreiche Folgefragen, angefangen von der Auswahl des optimalen Cloud-Anbieters bis hin zu Sicherheitsaspekten und internen sowie externen Kontrollmöglichkeiten. Es bietet sich zu diesem Zeitpunkt an, zumindest die FMA und die Datenschutzstelle über das Projekt zu informieren.

4.2 Selektion des Cloud-Anbieters

Die Auswahl eines Cloud-Anbieters sollte erst nach Durchführung eines entsprechenden Due-Diligence-Prozesses (Innovationsgrad, Bewertung der Leistungen nach Risk-Return, Sicherheitsaspekte, Einhaltung aufsichtsrechtlicher Bestimmungen, politische Aspekte bei Anbieter aus Drittstaat) vollzogen werden. Die Verantwortlichkeiten für den Due Diligence-Prozess sollten klar und schriftlich geregelt sein und sollten vorsehen, dass die verantwortlichen Personen fachlich ausreichend geeignet sind, um die Dienstleistungen des Anbieters sowie deren Auswirkungen auf das Unternehmen, unter anderem in Hinblick auf die Einhaltung aufsichts- und datenschutzrechtlicher Anforderungen, bewerten zu können. Unternehmensintern ist hier auch auf etwaige Interessenskonflikte Bedacht zu nehmen. Im Zweifelsfall bietet es sich an, die Meinung eines unabhängigen Dritten einzufordern. Der Prozess sollte angemessen und für einen fachkundigen Dritten nachvollziehbar dokumentiert werden.

4.3 Internes Kontrollsystem

Noch vor Migration der Systeme in die Cloud sollten Unternehmen ihr internes Kontrollsystem („IKS“) umfassend evaluieren und beurteilen, ob Anpassungen im Zuge der Migration notwendig und/oder sinnvoll sind. Dabei sollten insbesondere die Vorgaben der ESAs zu „Auslagerungen/Outsourcing“ berücksichtigt werden. Besondere Beachtung sollten Einsichtsmöglichkeiten durch externe Stakeholder geschenkt werden, z.B. durch Revisionsstellen und Behörden. Im Allgemeinen hat das Unternehmen darauf Acht zu nehmen, dass die Inanspruchnahme von Cloud-Dienstleistungen eine wirksame Aufsicht durch die FMA nicht gefährdet (z.B. durch besondere Zugriffsrechte, rechtliche oder technische Einsichtssperren). Daneben sollte das Unternehmen evaluieren, ab welchem Zeitpunkt eine Information an Stakeholder (Investoren, Kunden, Behörden) stattfinden sollte.

4.4 Lokalität der Cloud-Infrastruktur

Unternehmen sollten darauf achten, sicherzustellen, dass der Cloud-Anbieter die geographische Lokalität der Standorte, an denen sich die relevanten Cloud-Infrastrukturen befinden (Daten- und Betriebszentren), dem Unternehmen rechtzeitig bekannt gibt, inklusive eventueller Änderungen während der Laufzeit des Vertrags. Unternehmen sollten zeitnah beurteilen, ob bei Verlagerung in Drittstaaten (Nicht-EWR-Staaten) eine erneute, zumindest partielle Angemessenheitsprüfung zum Anbieter («Due-Diligence») sowie Anpassungen

des IKS notwendig sind. Die Unternehmen sollten zudem sicherstellen, dass der Cloud-Anbieter vertraglich verpflichtet ist, das Unternehmen regelmässig über wesentliche Änderungen in den Gesetzen der jeweiligen Jurisdiktion zu informieren.

4.5 Zugriffskonzepte und Datenklassifizierungen

Unternehmen sollten interne Verfahren implementieren, um die mittels der Cloud-Dienstleistungen bearbeiteten Informationen, die unter Geheimnisschutzpflichten fallen, angemessen zu klassifizieren und hervorzuheben. Die Klassifizierung der Daten ist derart granular vorzunehmen, dass diese eine effektive Erleichterung bei der Filterung und Aufarbeitung seitens des Unternehmens und des Cloud-Anbieters bewirkt. Bei der Verarbeitung von besonders schützenswerten Daten (z.B. Gesundheitsdaten) sollte eine spezifische Risikoanalyse, insbesondere für den Fall von Datendiebstahl («Leaks»), vorgenommen und angemessene Notfallpläne dokumentiert werden. Es bietet sich an, diese Massnahmen mit einem umfassenden Zugriffskonzept, das mit dem allgemeinen IKS in Einklang ist, zu flankieren.

4.6 Datenbereitstellung

Unternehmen sollten ihr IKS derart ausrichten, dass Daten rechtzeitig bereitgestellt werden können. Dies gilt nicht für interne Kontrollmechanismen (z.B. Compliance und interne Revision), sondern auch in Bezug auf Daten, die extern angefragt wurden, z.B. durch die FMA. In diesem Zusammenhang hat das Unternehmen darauf zu achten, dass keine rechtlichen (vertraglichen) oder faktischen (technischen) Hindernisse zur Herausgabe an die Behörde bestehen. Erkennt das Unternehmen potentielle Hindernisse, so sollte sie die Behörde präventiv informieren und sich bemühen, die Hindernisse zeitnahe zu beseitigen. Der Cloud-Anbieter sollte das Unternehmen rechtzeitig vor einer Herausgabe der Daten an Dritte (z.B. Behörden, Wirtschaftsprüfer), insbesondere wenn es sich um gesetzlich geschützte Daten handelt, informieren.

4.7 Kontrolle

Die Einhaltung der vertraglichen Verpflichtungen durch den Cloud-Anbieter (insbesondere bezüglich Auslagerung, Datenschutz und Informationssicherheit) sollte regelmässig geprüft werden. Eine Prüfung sollte durch das Unternehmen selbst (z.B. interne Revision), seine Revisionsstelle oder durch unabhängige Dritte vorgenommen werden. Das Unternehmen sollte vertraglich dafür sorgen, dass der Cloud-Anbieter zur Mitwirkung an diesen Prüfungen verpflichtet ist. Eine Vor-Ort-Kontrolle der zur Erbringung der Cloud-Dienstleistungen eingesetzten IT-Infrastrukturen ist regelmässig nicht erforderlich, da im Falle von Cloud-Lösungen die Einrichtung eines logischen Zugriffs im Grundsatz als ausreichend erachtet werden kann. Im Falle von Spezialthemen (z.B. Datensicherheit) sollte das Unternehmen darauf achten, dass der Cloud-Anbieter zur unabhängigen Zertifizierung verpflichtet ist und die diesbezüglichen Belege einfordern.

5. Fallkonstellationen

5.1 Neue Technologien

Cloud-Lösungen bieten die Möglichkeit, neue Technologien wie beispielsweise künstliche Intelligenz ohne das Vorhalten eigener spezifischer Soft- und Hardware zu nutzen. Zudem wird die Rechenleistung für die Unternehmen erhöht, womit Unternehmen in die Lage kommen, Big Data kostengünstig in Echtzeit zu verarbeiten. Auf der einen Seite unterstützt dies die Finanzintermediäre dabei, dem Kunden das optimale Finanzprodukt anzubieten, auf der anderen werden die Aggregationskapazitäten für Risikodaten, sowie deren Berichterstattung an interne und externe Stakeholder gestärkt.[13] Dies fördert sowohl die Leistungsfähigkeit und Effizienz von Markt- (Front) als auch von Marktfolgeeinheiten (Back) des Finanzintermediärs.

Als Anwendungsbeispiel ist vor allem die Migration eines Kernbanksystems (oder anderer Back-End-Systeme, die tägliche Finanztransaktionen verarbeiten und Aktualisierungen an Konten und anderen Finanzdaten verbuchen) in die Cloud inklusive der Schnittstellen zum regulatorischen Meldewesen zu nennen. Gerade bei datenintensiven Tools zur Verhinderung von Marktmissbrauch, im Zahlungsverkehr sowie im Falle von Transaktionsmeldungen können Unternehmen via Cloud-Lösungen ihre Ressourcen effizienter nutzen und mit anderen Technologien (z.B. künstliche Intelligenz[14] oder Blockchain) verknüpfen. Auch bedeutende Akteure der Finanzinfrastruktur, wie z.B. Zentrale Gegenparteien und Zentralverwahrer, nutzen Cloud-Lösungen zum Einsatz neuer Technologien, wie beispielsweise künstliche Intelligenz. Cloud-Lösungen unterstützen damit die Datenarchitektur und IT-Infrastruktur in einem hohen Ausmass.

Erfahrungen aus der Praxis

Zwecks Erhebung von Praxiserfahrungen im Zusammenhang mit Cloud-Lösung führte die FMA im Februar 2021 ein Interview mit einem unter Aufsicht stehenden Finanzintermediär. Als Diskussionsgrundlage dienten FMA-interne Vorarbeiten zur Zukunftsvision eines cloudbasierten und durch künstliche Intelligenz (KI) unterstützten Datenintegrationsmodells.

Gemäss Interviewpartner zeigt die aktuelle Entwicklung, dass es im Zusammenhang mit der Thematik Cloud verschiedene Kombinationen mit KI gibt:

Varianten der KI-Nutzung in einer «Cloud»

Im Interview wies der Finanzintermediär auf zwei grundlegende Varianten beim cloudbasierten Einsatz künstlicher Intelligenz («KI») hin:

1. Cloud-Lösungen, bei denen die KI „vorgelagert" ist:

Als konkretes Beispiel nannte der Finanzintermediär das gemeinsame Projekt einer Europäischen Aufsichtsbehörde mit Wirtschaftsprüfern und einer bekannten Artificial Intelligence Platform. Dabei wurde mit Hilfe von KI eine Datenbank in einer Cloud erstellt. Maschinell eingelesene pdf-Dokumente werden durch die KI

[13] Vgl *BCBS*, Principles for effective risk data aggregation and risk reporting (BCBS 239).

[14] Beachte: Von der EU-Kommission wurde am 21. April 2021 ein Vorschlag für eine Verordnung für harmonisierte Regelungen über künstliche Intelligenz (COM(2021) 206 final, vorgestellt.

erkannt, aufgearbeitet und in der Cloud strukturiert abgelegt. Für die weitere Auswertung/Analyse dieser Daten werde bis anhin allerdings keine KI eingesetzt.

2. Cloud-Lösungen, bei denen die KI „nachgelagert" ist:

Als Beispiel wurde ein italienisches KI-Unternehmen, das seit Jahren im Markt etabliert sei und zu seinen Kunden u.a. das FBI und die CIA zählen könne, erwähnt. KI-basierte Lösungen dieses Unternehmens könnten auch zur Auswertung/Analyse von bestehenden Cloud-Datenbanken verwendet werden. Es werden hierbei folgende Beispiele erwähnt:

•Sinnerkennung eines Textes: Nach Einlesen eines mehrseitigen Textes wird innerhalb weniger Sekunden eine perfekte Zusammenfassung auf einer Seite erstellt.

•Aufsichtstätigkeit: Ein Outsourcing-Vertrag sowie eine Aufsichts-Richtlinie zum Outsourcing werden eingelesen. Das System kann innerhalb weniger Sekunden beurteilen, ob der Vertrag die Vorgaben der Richtlinie einhält.

Der Finanzintermediär betonte allerdings, dass die Entwicklung solcher Lösungen enorm aufwendig, insbesondere Ressourcen- und zeitintensiv wäre. Selbst würde der Finanzintermediär eine sehr einfache Form einer Cloud-Lösung betreiben, bei der die KI «vorgelagert» sei. Dabei würden die verschiedenen Arten der eingetroffenen Korrespondenz (Beschwerde, Antrag Neukunden, Stornierungen etc.) durch KI klassifiziert und den zuständigen Mitarbeitern in einer Datenbank/Cloud zur Bearbeitung zur Verfügung gestellt. Der Finanzintermediär wies darauf hin, dass es sich dabei um eine thematisch eng umrissene Lösung handeln würde, bei der relativ einfache, wiederkehrende Prozesse automatisiert und somit effizient gestaltet werden. Der Initialaufwand (Datenmodellierung der KI) sei sehr hoch gewesen, würde sich nach Einschätzung des Unternehmens aber langfristig jedenfalls auszahlen.

Herausforderungen

Der Finanzintermediär wies im Zusammenhang mit Cloud-Lösungen insbesondere auf folgende Herausforderungen hin:

Vielfach sei der Datenbestand in einer Cloud sehr heterogen und facettenreich (Kundendaten, Finanzdaten, allgemeine Marktdaten, Informationen zur Governance, FMA-Dokumente etc). Zudem können die entsprechende Auswertung, Darstellung und der Adressatenkreis ebenfalls sehr unterschiedlich sein. Aus aktueller Sicht würden sich Cloud-Lösungen, insbesondere in Kombination mit KI, nur für eng umgrenzte Problemfelder eignen und seien insbesondere in «wiederkehrenden» Prozessen sinnvoll.

Die Erstellung von Cloudlösungen, welche KI-unterstützt sind, könne zudem sehr aufwendig, zeitintensiv und teuer sein. Im Beispiel von Cloud-Lösungen, bei denen die KI vorgelagert ist, müsse die Datenaufarbeitung zuerst manuell durch das Unternehmen vorgenommen werden. Die daraus abgeleitete Erfahrung könne in Muster festgehalten werden, welche Grundlage für die KI-Modellierung seien. Ein solcher Initialaufwand könne sehr gross sein. Das Beispiel des italienischen Anbieters würde zeigen, dass insbesondere auch Cloud-Lösungen, bei denen die KI nachgelagert ist, sehr aufwendig und zeitintensiv sein können. Dieser Aufwand steige exponentiell mit der Komplexität der Aufgabe. Falls komplexe, facettenreiche Gebiet (Aufsichtstätigkeit, Führung eines Finanzintermediärs etc.) in diesem Sinn als Gesamtheit in einer Cloud realisiert werden sollten, wäre dies aus heutiger Sicht mit enorm hohen Kosten verbunden.

Lösungsvorschläge

Unternehmen, welche die verstärkte Nutzung von Cloud-Lösungen und KI ins Auge fassen, wird empfohlen, sich insbesondere zu Beginn in kleinen Schritten voranzutasten: Das cloudbasierte und KI-unterstützte Datenintegrationsmodell sollte in einem ersten Schritt fokussiert für einige wenige, ausgewählte, eng umrissene und repetitive Aufgaben eingesetzt werden. Empfehlenswert wäre es, sich dabei erst einmal auf eine Cloud-Lösung zu konzentrieren, bei denen die KI «vorgelagert» ist. Dies kann so festgehalten werden, da das «Füttern» einer Cloud mit Daten im Charakter genau diesen relativ eng umrissenen und repetitiven Aufgaben entspricht. Mit zunehmendem Erfahrungsschatz kann der Scope solcher Anwendungen entsprechend vergrössert werden. Eine Projektplanung zur Implementierung von Cloudlösungen sollte im Kern diese Vorgehensweise widerspiegeln.

Die technologische Weiterentwicklung kann zu reduzierten Kosten und einem höheren technologischen Potential führen, was den Anwendungsbereich von KI-unterstützten Cloud-Lösungen in der Praxis erweitern und die Akzeptanz für diese Technologie erhöhen dürfte. Im weiteren Verlauf des Projektes sollte deshalb die Anwendung von KI-unterstützten Cloudlösungen fortlaufend an die technologische Entwicklung angepasst werden. Es sind verantwortliche Personen innerhalb des Unternehmens zu bestimmen, welche sich laufend über entsprechende Entwicklungen informieren und realitätsnahe und ökonomisch sinnvolle Vorschläge zur Weiterentwicklung der implementierten Cloudlösung geben.

Aufgrund der hohen Projektkomplexität und der potentiell hohen Kosten ist für Finanzintermediäre in Liechtenstein zudem der Austausch und die Zusammenarbeit mit vergleichbaren Marktteilnehmern im Rahmen der Projektplanung- und Durchführung sinnvoll. Dadurch können die Projektkosten und die Erfahrung bei der Implementierung und der Reife einer Cloudlösung geteilt werden. Ein vorausschauender Aufbau eines Netzwerkes möglicher Lieferanten und langfristiger Partner ist empfehlenswert. Liechtensteiner Finanzintermediäre, die Teil einer Gruppe sind, könnten entsprechende Entwicklungen frühzeitig intern anstossen und von den entsprechenden Gruppenressourcen profitieren. Nicht zuletzt sollten die Liechtensteiner Verbände eine zentrale Rolle bei der Koordinierung und beim Aufbau solcher Netzwerke spielen und Basis für einen Austausch und eine Zusammenarbeit zwischen den Finanzintermediären bieten.

5.2 Risikocontrolling und Compliance

Durch Cloud-Lösungen können Unternehmen auch komplexe interne Compliance- und Risikocontrolling-Prozesse automatisieren und mit anderen Technologien verknüpfen. Denkbar wäre etwa der Cloud-basierte Einsatz künstlicher Intelligenz in internen Kontrollverfahren zur Aufdeckung von Betrug oder im Kunden-Onboardingprozess („Know Your Customer“). Die Cloud-unterstützte künstliche Intelligenz könnte interne und externe Datenquellen verknüpfen interpretieren und effizient schnelle Ergebnisse zu den eingebrachten Informationen, wie auch Handlungsempfehlungen, generieren. Daneben können Cloud-Lösungen und die dahinterstehe Rechenleistungen auch tägliche Stresstestdaten mit aktuellen Marktdaten liefern. Dies fördert nicht nur die Homogenität der Datenstruktur, sondern auch deren Qualität und Aktualität.

5.3 Community Clouds

Community Cloud-Lösungen im Finanzsektor bieten noch weitergehende Lösungen. So wären zentral verwaltete, gemeinsame Datenbanken und/oder Plattformen in der Cloud zum Zwecke des Informationsaustausches in Echtzeit denkbar. Dies gilt insbesondere für Finanzmarktinfrastrukturen wie Handelsplätze, zentrale Gegenparteien und Zentralverwahrer. Wird auch die Aufsichtsbehörde ein Teil der Community-Cloud, so könnte diese die Daten direkt aus dem System ziehen ohne ad-hoc-Anfragen an die Unternehmen stellen zu

müssen. Dasselbe gilt für die Wirtschaftsprüfung und Ratingagenturen. Zu diesem Thema (Stichwort: «data sharing for the public interest») wurde seitens der Europäischen Kommission im Jahr 2020 der Endbericht der High-Level Expert Group on Business-to-Government Data Sharing veröffentlicht.[15]

***

[15] Abzurufen unter https://digital-strategy.ec.europa.eu/en/news/commission-appoints-expert-group-business-government-data-sharing (Juni 2021).

FMA

Abkürzungsverzeichnis

AIF	Alternativer Investmentfonds
AIFM	Alternativer Investmentfonds Manager
EBA	European Banking Authority, Europäische Bankenaufsichtsbehörde
EIOPA	European Insurance and Occupational Pensions Authority, Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung
ESA(s)	European Supervisory Authorities, Europäische Aufsichtsbehörden
ESMA	European Securities and Markets Authority, Europäische Wertpapier- und Marktaufsichtsbehörde
FMAG	Finanzmarktaufsichtsgesetz
IKS	Internes Kontrollsystem
IT	Informationstechnologien
IKT	Informations- und Kommunikationstechnologie
KI	Künstliche Intelligenz
NIST	National Institute of Standards and Technology
OGAW	Organismus für gemeinsame Anlagen in Wertpapieren
SPG	Sorgfaltspflichtgesetz
SPV	Sorgfaltspflichtverordnung