ÖSTERREICHISCHE FMA·FINANZMARKTAUFSICHT

Digitalisierung am österreichischen Finanzmarkt

Call for Input: Ergebnisse

Jänner 2020

INHALTSVERZEICHNIS

Aufgrund der leichteren Lesbarkeit wird in diesem Dokument durchgängig die männliche Form verwendet. Diese Bezeichnungen sind als geschlechtsneutral zu betrachten. Es wird ausdrücklich darauf hingewiesen, dass sich alle personenbezogenen Formulierungen grundsätzlich gleichermaßen auf Frauen und Männer beziehen.

EINLEITUNG

Analyse der FMA zur Digitalisierung am österreichischen Finanzmarkt

Die Digitalisierung verändert die Rahmenbedingungen am Finanzmarkt so schnell und grundlegend wie seit Jahrzehnten nicht mehr. Die FMA ist von Beginn dieses Transformationsprozesses an daran interessiert, aktuelle Erkenntnisse zu den damit verbundenen Chancen, Trends und Risiken zu gewinnen. Dabei gehen wir strikt nach dem Prinzip der Technologieneutralität vor: Die FMA beaufsichtigt keine Technologien, sondern hat primär Risiken im Blick. Gleiche Risiken verlangen gleich hohe Aufsichtsanforderungen, egal ob sie aus digitalen oder analogen Geschäftsmodellen oder Prozessen entstehen.

Einen Zwischenstand der Analyse zur Digitalisierung am österreichischen Finanzmarkt haben wir im Juli 2019 präsentiert. Dieser liegt eine Studie zugrunde, mit der Anfang 2018 begonnen wurde und die sich unter anderem auf eine umfangreiche Erhebung bei den beaufsichtigten Unternehmen stützt. Durch die beinahe vollständige Marktabdeckung und die hohe Mitwirkung der beaufsichtigten Unternehmen konnte die bislang umfassendste und gleichzeitig detaillierteste Daten- und Informationsbasis zum Thema Digitalisierung am österreichischen Finanzmarkt geschaffen werden. Diese bildet für die FMA eine fundierte Basis, um bei der Digitalisierung am Ball zu bleiben und Treiber, Trends und mögliche künftige Entwicklungen richtig einzuschätzen.

Ergebnisse des Call for Input

Um eine breitere Diskussion anzustoßen und den Dialog am österreichischen Finanzmarkt zu den Implikationen der Digitalisierung zu intensivieren, hat die FMA außerdem die Stakeholder – die Investoren, Sparer, Versicherungsnehmer und Verbraucher, öffentliche Institutionen – sowie die interessierte Öffentlichkeit eingeladen, die im Bericht zur Digitalisierung am österreichischen Finanzmarkt skizzierten Erkenntnisse und Schlussfolgerungen kritisch zu hinterfragen und um ihre Sichtweisen, Erfahrungen und Lösungsansätze anzureichern.

Elf Stakeholder sind diesem Call for Input gefolgt und haben zu den Fragen, die die FMA am Ende jedes Kapitels des Berichts als Orientierungshilfe formuliert hat, teilweise sehr umfangreiche Stellungnahmen übermittelt.

Im Allgemeinen werden die Schlussfolgerungen der FMA hinsichtlich der Implikationen der Digitalisierung von den teilnehmenden Stakeholdern grundsätzlich geteilt und bekräftigt. In einigen Stellungnahmen werden ergänzende Hinweise und weitere praktische Beispiele genannt (z. B. zunehmende praktische Bedeutung von Aggregatoren, Messengers etc.). Mehrere Stakeholder machen rechtspolitische Anregungen und Vorschläge de lege ferenda (aus Sicht eines Teilnehmers wäre etwa Vorsorge dafür zu treffen, dass Dienstleistungen nicht zuletzt aufgrund des Exklusionsrisikos nicht in Richtung ausschließlicher Digitalisierung transformiert werden; diesbezüglich soll die [verpflichtende] Aufrechterhaltung einer analogen Mindestinfrastruktur in Erwägung gezogen werden).

Die FMA bedankt sich für die umfangreichen Stellungnahmen und wird diesen wertvollen Input bei ihren Agenden sowie bei der Priorisierung ihrer Aufsichtsaktivitäten entsprechend berücksichtigen.

I. STRATEGIEN

Welche Chancen und Risken der Digitalisierung sind für den österreichischen Finanzmarkt entscheidend? Was sind die Erfolgsfaktoren, um den digitalen Wandel optimal für die Weiterentwicklung der Geschäftsmodelle in den einzelnen Sektoren des Finanzmarktes nutzen zu können? Was ist die Erwartungshaltung hinsichtlich der Rolle der Aufsicht? Das waren einige der Fragen, die die FMA in ihrem Call for Input gestellt hat.

Die am Call for Input teilnehmenden Stakeholder bekräftigten im Wesentlichen die Schlussfolgerungen der FMA hinsichtlich der Implikationen der Digitalisierung und ergänzten diese um folgende Einschätzungen:

Insgesamt werden die Auswirkungen der Digitalisierung auf den Finanzmarkt positiv eingeschätzt. Digitalisierung unterstützt Finanzmarktteilnehmer dabei, Kunden besser zu verstehen und Geschäftsmodelle sowie Produkte auf deren Bedürfnisse auszurichten.

- Im Zuge der digitalen Transformation werden **Marktanteile völlig neu aufgeteilt**. Neue Mitbewerber und neue Geschäftsmodelle zwingen bestehende Branchen zu **Innovation und Agilität.** Die Nutzung von Daten wird immer bedeutender; **neue Rollenprofile** werden gesucht – Bank als „Datenunternehmen".
- Die Digitalisierung sorgt im Hinblick auf die Zunahme von Kooperationen für eine **stärkere Vernetzung** der Finanzmarktteilnehmer untereinander sowie mit marktfremden Teilnehmern.
- Besonders starken Einfluss wird der Digitalisierung auf **weniger beratungsintensive Produkte und Services** beigemessen: Vor allem im Zahlungsverkehr geht man davon aus, dass die Digitalisierung weiter stark die aktuellen Prozesse verändern wird. Auch Kreditgeschäfte mit kleineren Summen, Vermögensverwaltung im Allgemeinen sowie maßgeschneiderte Versicherungsprodukte werden zunehmend digitalisiert.
- Insgesamt werden Veränderungen durch die Digitalisierung **im Privatkundengeschäft** deutlich früher als im Firmenkundengeschäft erwartet.

Auf absehbare Zeit (in den nächsten drei Jahren) wird keine Disruption im Kerngeschäft der beaufsichtigten Unternehmen erwartet. Allerdings ist man davon überzeugt, dass die derzeitigen Geschäftsmodelle langfristig angepasst werden müssen und in den nächsten fünf bis zehn Jahren die Veränderungen näher an der Disruption als an der Evolution sein werden.

- Laut einem Stakeholder kann es durchaus bereits davor zu einer Disruption kommen. Es liegt **oft in der Hand von Regulierung** und Aufsicht, ob eine Entwicklung evolutionär oder disruptiv verläuft.
- Teilweise wird eingeräumt, dass **komplexe Regularien** am österreichischen Markt **disruptive Entwicklungen erschweren**. Disruptive Entwicklungen sind aber in den folgenden Bereichen denkbar:
  - in Bereichen mit einer großen Anzahl an repetitiven Arbeitsschritten
  - in Bereichen, in welchen durch Digitalisierung die Convenience für den Kunden enorme Qualitätssprünge macht
  - Gewisse Geschäftsfelder können innerhalb der nächsten Jahre aufgrund neuer Marktteilnehmer wegbrechen.
  - Aufgrund der Einführung der privaten Währung Libra und eines damit verbundenen weltweiten Zahlungsnetzwerks könnte eine Disruption infolge der Digitalisierung ein mögliches Zukunftsszenario darstellen.

Digitalisierungshindernisse werden nicht nur in der Regulierung, sondern auch in der Unternehmenskultur und der IT-Landschaft gesehen:

- Als **regulatorische Hindernisse**, die einer Digitalisierung im Wege stehen, werden zum einen allgemein die „Überregulierung“ und zum anderen einige konkrete Vorgaben (z. B. § 37a BWG und § 4 Abs. 2 Z 2 SVG) wahrgenommen. Es wird angeregt, dass die Regulatory Sandbox auch zur Prüfung / zum Aufzeigen der Digitalisierungshindernisse genutzt wird.

  Konkret wird in den folgenden Bereichen Handlungsbedarf gesehen:

  - Die Regulatorik (Bankgeheimnis, Datenschutz, TKG, FM-GwG etc.) sollte so ausgestaltet sein, dass eine **rein digitale Geschäftsabwicklung** ohne physische Präsenz des Kunden ermöglicht wird. Gerade mit Blick auf Betrugsprävention und -bekämpfung sei eine entsprechende Vernetzung in der Kommunikation mit den Behörden wie auch zwischen den Finanzinstituten wünschenswert, um hier – unter Einhaltung der datenschutzrechtlichen Vorschriften – einen raschen Abgleich bzw. Austausch sicherzustellen (z. B. hinsichtlich der Prüfung von Ausweisen).
  - In einem ersten Schritt sollte zumindest in den jeweiligen Materiengesetzen nach dem Vorbild des § 1b VersVG bei den Formvorschriften **zwischen Erklärungen in Schriftform und dem Erfordernis der geschriebenen Form unterschieden** werden. „Schriftform“ bedeutet, dass die Erklärung eigenhändig unterschrieben werden muss. Eine rechtsgeschäftliche Erklärung z. B. per E-Mail erfüllt damit nicht die Anforderungen eines Schriftformgebots. Beim Erfordernis der „geschriebenen Form“ ist hingegen keine Unterschrift oder qualifizierte elektronische Signatur erforderlich. Die rechtsgeschäftliche Erklärung muss hier lediglich aus einem Text in Schriftzeichen bestehen, aus dem auch die Person des Erklärenden hervorgeht. Rechtsgeschäftliche Erklärungen können hier z. B. auch per E-Mail oder SMS (WhatsApp) rechtswirksam abgegeben werden.
  - Ausweitung der Anwendbarkeit elektronischer Identitäten und von Identitätsnachweisen/-berechtigungen: Eine Legitimierungsoption auf digitalem Wege durch die Verwendung digitaler Zertifikate (qualifiziertes Zertifikat) würde mehrere Vorteile – z. B. in den Bereichen AML, Authentifikation, Bonitätserklärungen etc. – bieten; damit könnte erreicht werden, dass eine **digitale Identität** nicht nur in Form der digitalen Signatur gegenüber Behörden, sondern auch **in Form eines qualifizierten Zertifikats** zwischen privaten juristischen und natürlichen Personen zum Einsatz gelangen könnte.
  - Verwendung von **Unterschriften-Pads** (U-Pads) zur Erfüllung gesetzlicher Formerfordernisse bei der Entbindung vom Bankgeheimnis für ältere Kunden; die Befreiung vom Bankgeheimnis ist zwar nach § 38 Abs. 6 BWG schon durch die strenge Kundenidentifizierung möglich; über diese Möglichkeit verfügen aber ältere Bankkunden oft nicht.
  - Die Regelung über die **Art und Weise der elektronischen Übermittlung von Anträgen auf Erstattung der Bausparprämien** in der BausparVO sollte an den aktuellen Stand der Digitalisierung angepasst werden.
  - Umfangreiche **Telefonaufzeichnungen** gemäß § 33 WAG 2018
  - Als **Vor-Ort-Verfügbarkeit** iSd § 52 WAG 2018 müsste auch Videoberatung gelten.
- Zur **Verwendung von personalisierten Websites als „dauerhafter Datenträger“** wurde angemerkt, dass nach der Rechtsprechung des EuGH eine Website nur dann diese Anforderung erfüllt, wenn jede Möglichkeit der einseitigen Änderung des Inhalts der Website für den Zahlungsdienstleister oder einen mit der Verwaltung der Website beauftragten Administrator ausgeschlossen ist. Ob diese Anforderungen aktuell in der Praxis erfüllt werden können, sei in Zweifel zu ziehen. Nach der Rechtsprechung des OGH führt auch die reine Möglichkeit der Speicherung im Rahmen einer Website inklusive Mailbox noch nicht dazu, dass ein dauerhafter Datenträger vorliegt.

- Als maßgebliche Hürde der Digitalisierung wird auch die **Organisation eines Unternehmens** mit all seinen „Elfenbeintürmen“ und „Kleingärten“ gesehen. Dazu gehört auch das generelle „Mindset“, vor allem jenes der Führungskräfte etablierter Unternehmen am österreichischen Finanzmarkt (eher vorsichtige, negative Grundeinstellung gegenüber dem Wandel der Zeit und des Marktes sowie allgemein zur Digitalisierung).
- Als größtes Risiko bzw. Hindernis wird teilweise aber gesehen, dass **die Trends** der Digitalisierung **nicht (rechtzeitig) erkannt werden**.
- Auch die stark fragmentierte und veraltete **IT-Landschaft** sowie das Fehlen branchenübergreifender Schnittstellen werden als Hürden für die Interaktion mit Kunden und Kooperationspartnern (z. B. Vertrieben) gesehen.

Entscheidende Erfolgsfaktoren der Digitalisierung reichen von der Entwicklung eines Minimum Viable Product bis hin zur Gestaltung eines attraktiven Arbeitsumfeldes und zum Talentmanagement:

- Die erfolgreiche Transformation steht und fällt mit der Einsicht, dass sich die Welt immer rasanter verändert und dass sich **Unternehmenskulturen** und Organisationsstrukturen an dieses neue, dynamische Marktumfeld anpassen müssen (Vision und die dazugehörige Umsetzung und laufende Anpassung der **Unternehmensstrategie**).
- Entscheidende Erfolgsfaktoren sind die Erwartungshaltung der Finanzmarktteilnehmer gegenüber dem digitalen Wandel und das rechtzeitige Tätigwerden in die richtige Richtung (z. B. **Entwicklung eines Minimum Viable Product**).
- Erfolgsentscheidend ist, dass in den Führungsetagen ausreichend **Know-how** für die anstehenden Herausforderungen in Form personeller Ressourcen vorhanden ist.
- Gestaltung eines **attraktiven Arbeitsumfelds** sowie **Talentmanagement**, um die richtigen Mitarbeiter zu gewinnen; Flexibilität, Offenheit, **Neugier hinsichtlich neuer Technologien**, die auch ein Umdenken beim Recruiting von Mitarbeitern erfordern.
- Im Lichte der hohen Veränderungsgeschwindigkeit ist **Agilität** ein erfolgskritischer Faktor bei der Transformation. Agilität bedeutet unter anderem, dass Mitarbeiter je nach ihrer persönlichen Kompetenz eingesetzt werden.
- Anpassungen der **IT-Infrastruktur** und die bessere Nutzung von Daten.

Die Transformation im Zuge der Digitalisierung sollte nach Ansicht der Stakeholder von der Aufsicht begleitet werden. Die Rolle der Aufsicht wird insbesondere darin gesehen, ein Level Playing Field zu gewährleisten, ohne dabei allerdings als „Wettbewerbsregulierer“ oder „Schützer“ für existierende Institute zu agieren. Im Rahmen der Überwachung der digitalen Transformation könnte die FMA „Leitlinien für digitale Veränderungsprozesse“ definieren.

Die Erwartungshaltung hinsichtlich der Rolle der Aufsicht greift in mehrere Bereiche ein:

- Durch die Aufsicht sollte ein **Level Playing Field** gewährleistet werden. Wichtig ist es dabei,
  - den **Finanzplatz als Ganzes** im Auge zu haben und für alle Marktteilnehmer ein Level Playing Field sicherzustellen
  - ein transparentes Aufsichtssystem mit unabhängigen Behörden und
  - die eigene Weiterentwicklung bzw. den **Aufbau digitaler Kompetenz** bei der Aufsicht sicherzustellen, um der rasanten Entwicklung folgen zu können.
- Die Transformation im Zuge der Digitalisierung sollte **von der Aufsicht begleitet** werden, um die Potenziale für beaufsichtigte Unternehmen im Rahmen der regulatorisch erforderlichen Grenzen auszuloten.
- Rasche **Abklärung von Konzessionserfordernissen** für FinTechs, die mit konzessionierten Unternehmen kooperieren wollen.
- Die FMA soll **nicht als „Wettbewerbsregulierer“** oder „Schützer“ für existierende Institute agieren.

- Die Aufsicht sollte angesichts des tiefgreifenden Strukturwandels im Bankensektor den **Dialog mit den Sozialpartnern** suchen, gerade was die Entwicklung von nachhaltigen Geschäftsmodellen betrifft.
- Die Aufsicht sollte darauf achten, dass die Geschäftsmodelle österreichischer (Groß-) Banken **verstärkt auf Nachhaltigkeit ausgerichtet** sind.
- Die Aufsicht könnte im Rahmen der Überwachung der digitalen Transformation **„Leitlinien für digitale Veränderungsprozesse in Banken“** definieren, die auch die Rolle eines „Chief Digital Officer“ vorsehen.

II. NEUE ANBIETER – FINTECH/INSURTECH

Der digitale Wandel eröffnet am Finanzmarkt Raum für neue Wettbewerber. FinTechs/InsurTechs verfügen über Lösungen, Angebote und Geschäftsmodelle, die traditionelle Prozesse und Dienstleistungen in vielen Bereichen effizienter gestalten oder gar vollständig hinfällig machen. Deshalb war es der FMA wichtig, den Call for Input auch dazu zu nutzen, die Meinung der Stakeholder zu den Implikationen des Eintritts neuer digitaler Mitbewerber in den Finanzmarkt zu erfahren.

Die am Call for Input teilnehmenden Stakeholdern bekräftigten im Wesentlichen die Einschätzung der FMA hinsichtlich der neuen Player und ergänzten diese um die folgenden Hinweise:

Die neuen digitalen Mitbewerber werden die bestehenden Unternehmen zu einer fortlaufenden Weiterentwicklung drängen. Die größten Veränderungen werden in den Bereichen Retail, Zahlungsverkehr, Anlageberatung und Self-Service (Abwicklung von Schäden, Einreichung von Leistungen) erwartet.

- In einigen Unternehmen werden **neben der bestehenden IT neue, agile Bereiche** aufgebaut, die sich stärker den modernen Technologien widmen.
- Die Implikationen des Eintritts neuer Mitbewerber in den Finanzmarkt werden positiv gesehen, da diese **auf bestehende Teilnehmer Anpassungsdruck** ausüben und eine zusätzliche Benchmark für Unternehmen setzen.
- Digitale Mitbewerber können die Preistransparenz verbessern sowie durch neue Businessmodelle den **Preisdruck** auf etablierte Finanzdienstleistungen erhöhen.
- Kunden, die Produkte mehrerer Anbieter haben, können zukünftig über **Aggregatoren** alle Verträge in einem Portal verwalten. Es könnte für etwa Versicherer schwierig werden, Kunden mit reinen Versichungsthemen in den eigenen Portalen zu halten. Auch der Vertrieb wird wohl durch Vergleichsportale und Nischenanbieter in Bedrängnis kommen.

Neue Marktteilnehmer und bestehende Akteure sind nicht nur Konkurrenten; oft ergänzen sie sich gegenseitig durch Kooperationen.

- Die als digitale Mitbewerber bezeichneten Start-ups im Bereich FinTech/InsurTech werden in erster Linie als Kooperationspartner der etablierten Marktteilnehmer gesehen. Viele der neuen Player suchen die Kooperation mit etablierten Playern, um von deren Marktzugang zu profitieren. Etablierte Unternehmen suchen die Partnerschaft mit neuen Playern, um von deren Innovationskraft zu profitieren.
- Kleine, innovative Bankinstitute („Challenger-Banken“) setzen neue Technologien ein und bieten noch nicht dagewesene Produkte und Services an, die in hohem Ausmaß digital und personalisiert sind, und fordern damit große Universalbanken immer mehr heraus.
- Es werde etwa auch vernachlässigt, dass Versicherungen Wettbewerb im eigenen Haus drohe, da Rückversicherer mitunter die Hauptfinanziers der Start-up-Szene seien und zahlreiche Kooperationen mit FinTechs/InsurTechs unterhielten.

Das Konzept der „Sandbox“ für die Erprobung neuer Geschäftsmodelle wird grundsätzlich begrüßt. Durch die Transparenz der Regulatorik können Finanzmarktteilnehmer schneller erkennen, wie und welche regulatorischen Vorgaben zu erfüllen sind. Allerdings müssten dabei die Reputation sowie das Vertrauen in den Finanzmarkt gewahrt werden. Somit müsse zunächst sichergestellt werden, dass alle regulatorischen Anforderungen erfüllt werden, bevor der Endkunde einbezogen wird.

III. PRODUKTGESTALTUNG

Welche konkreten regulatorischen Vorgaben sind durch die Digitalisierung des Finanzsektors noch notwendig? Welche Hindernisse erschweren die Entwicklung von neuen digitalen Finanzprodukten? Teilen Sie die Einschätzung der FMA zu den mit den Auswirkungen auf das Bank- bzw. Versicherungsgeschäft verbundenen Chancen und Risiken? Welche konkreten positiven, aber auch negativen Entwicklungen bezüglich „digitaler“ Finanzprodukte sind aus Ihrer Sicht zu beobachten? Welche Aufgaben soll die FMA im Rahmen des Anleger-, Versicherten- und Gläubigerschutzes bezüglich „digitaler“ Finanzprodukte wahrnehmen? Das waren einige der Fragen, die die FMA in ihrem Call for Input gestellt hat.

Die teilnehmenden Stakeholder bekräftigten im Wesentlichen die Einschätzung der FMA zu den Auswirkungen der Digitalisierung auf die Produktlandschaft und fügten dem Folgendes hinzu:

Einigkeit besteht im Wesentlichen darüber, dass es bis auf allfällige Anforderungen für den Umgang mit Cyberrisiken aktuell keiner weiteren regulatorischen Vorgaben bedarf.

- Im Hinblick auf den **Datenschutz** stellt man fest, dass
  - mit der EU-Datenschutz-Verordnung bereits ein großer und richtiger Schritt gemacht worden ist. Aufgrund der ersten Erfahrungen kann geprüft werden, wie sich der neue Standard bewährt und ob gegebenenfalls Erweiterungen/Anpassungen notwendig sind.
  - zu hinterfragen wäre, ob sich die Vorgaben für den Datenschutz durch das tatsächliche Verhalten von Konsumenten nicht längst überholt haben (Nutzungsbedingungen, in denen insbesondere Technologieanbietern die Sammlung weitreichender personalisierter Informationen gestattet wird, würden ohne weitere Prüfung akzeptiert).
  - wo die Wertschöpfungsketten vielteiliger werden, auch mehr Schnittstellen vorhanden sind, die aus datenschutzrechtlicher Perspektive problematisch sein könnten.
- Ein Stakeholder führt aus, dass das **Management von Cyberrisiken** oberste Priorität im digitalen Finanzmarkt haben sollte. Zwar kann eine Aufsichtsbehörde nicht das gesamte Finanzsystem vor Cyberangriffen schützen, doch gehört es zur Rolle der FMA, für die nötige Sensibilisierung bezüglich der Problematik zu sorgen.
  - Die Aufsicht könnte beispielsweise **Anforderungen für den Umgang mit Cyberrisiken** festlegen. Ein weiterer Mechanismus könnte die Einführung eines **Penetration Testing** sein, wonach die beaufsichtigten Unternehmen ihr System probehalber angreifen lassen. Durch regelmäßiges Testen lassen sich mögliche Schwachstellen ausfindig machen und korrigieren. Hier sollte die FMA mit namhaften Partnerfirmen zusammenarbeiten und – unter Beachtung des rechtlichen Rahmens – Angriffe simulieren und die Cyberresilienz der beaufsichtigten Unternehmen testen.
  - Um ein hohes Sicherheitsniveau von Netz- und Informationssystemen sicherzustellen, ist auch die Einführung eines zentralen **Incident Reportings** sinnvoll. Angelehnt an das Netz- und Informationssystemsicherheitsgesetz (NISG) könnten verpflichtete IT-Strategien für beaufsichtigte Unternehmen erarbeitet, mit den jeweiligen Computer-Notfallteams (CERT.at, sektorenspezifische CERTs und GovCERT) eine Partnerschaft eingegangen und die Unternehmen zu angemessenen Sicherheitsmaßnahmen und der Meldung erheblicher Störfälle verpflichtet werden. Auch kontinuierliche **Awareness-Schulungen**, die für Schwachstellen sensibilisieren, wären zu empfehlen.

Hindernisse der Digitalisierung werden nicht nur in der Regulierung, sondern auch in der teilweise fragmentierten und veralteten IT-Landschaft, im Kundenverhalten sowie in der digitalen Kompetenz der Kunden gesehen:

- Zu den **regulatorischen Hindernissen**, die der Digitalisierung im Wege stehen, zählen bestehende Regularien, die nicht dem Zeitalter der Digitalisierung entsprechen, wie etwa
  - die Pflicht von Kreditinstituten, bestimmte Dokumente in Papierform bereitzuhalten
  - die verpflichtende Unterschriftsleistung eigens auf dem Einleger-Informationsbogen (§ 37a BWG), die die Einführung neuer, innovativer On-Boarding-Prozesse erschwert
  - die Hürden für einen vollständig digitalen Abschluss: Stichworte sind hier „nahtlos“ und „medienbruchfrei“ sowie ohne Verzögerungen.
- Die **IT-Infrastruktur** von österreichischen Instituten in der Finanzindustrie ist großteils sehr veraltet und sehr fragmentiert. Die Entwicklung von digitalen Finanzprodukten setzt IT-seitig ein gewisses Maß an Flexibilität voraus, welche nicht gegeben sei. Einigen Unternehmen wird Nachholbedarf auch hinsichtlich ihrer **Bereitschaft zu einer radikalen Veränderung der IT-Systeme** attestiert – dies insbesondere im Bereich der Continuous Integration. Weiters wäre es vorteilhafter, an einheitlichen Methoden für eine ganzheitliche, integrierte IT-Finanzinfrastruktur zu arbeiten. Während viele Unternehmen an ihren bestehenden individuellen IT-Lösungen festhalten, gibt es nur wenige, die eine bereichsübergreifende Konsistenz der Methoden einsetzen.
- Weiters ist auch das **Kundenverhalten** in Österreich im Bereich der digitalen Produkte eher abwartend. Dies führt dazu, dass man in der Entwicklung von digitalen Produkten kein First Mover ist.
- Generell sollte nicht auf die Hebung der **digitalen Kompetenz der Bevölkerung** vergessen werden. Dabei müssen der Aufbau von Basiskompetenzen in mobiler Internetnutzung sowie spezielle Trainings- und Qualifizierungsangebote im Vordergrund stehen.
- Die aktive Neugestaltung der **Unternehmenskultur** als Basis jeglichen Veränderungsprozesses im Rahmen der Digitalisierung wird oft unterbewertet. Ein passendes Wertesystem, Raum für Gestaltung, Förderung und Unterstützung der Mitarbeiter sind wesentlich auf dem Weg zu mehr Kundenzentriertheit und zu einem passenden Prozessdesign.
- Als sonstige Digitalisierungshindernisse werden auch genannt:
  - Fehlen einer Regulatory Sandbox
  - Denken in zu kleinen Dimensionen (Marktgröße)
  - fehlende finanzielle Mittel für Forschung und Entwicklung.

Als positive Entwicklungen werden insbesondere die steigende Transparenz von Produkten und der bessere Kundenservice wahrgenommen.

- Positiv zu erwähnen sind die **steigende Transparenz und Einfachheit** von Produkten sowie Innovationen, mit denen der Kunde z. B. einen **besseren Service** erhält.
- Die Erschließung neuer Geschäftsfelder wird positiv wahrgenommen.
- Eine geringe Zahl von IT-Anbietern als ausschließliche Kontaktstelle und zentraler Sicherheitszugang ist effizienter und wirkt positiv auf die IT-Sicherheit. Durch **professionelles IT-Sicherheitsmanagement** der großen Player kann die Wahrscheinlichkeit eines Angriffs gesenkt werden, obwohl der potenzielle Schaden ungleich höher ist.
- Als positives Beispiel wird auch der **FinTech-Beirat** des BMF genannt, da hier Experten aus Banken, Versicherungen, FinTech-Start-ups sowie weitere Stakeholder gemeinsam mit den Experten der FMA und des BMF über neue Themen wie ICOs, Tokenisierung von Assets, KYC-Datensynchronisierung und regulatorische Sandboxes sprechen können.

Negativ werden etwa eine bloße „Digitalisierung“ von bestehenden Produkten sowie modulare Produkte in Verbindung mit „beratungslosen“ Angeboten gesehen.

- Negativ betrachtet werden Bemühungen einiger Anbieter, bestehende Produkte einfach nur **„digital“ zu machen**. Digitale Transformation sollte anders aussehen.
- Kritisch werden auch **modulare Produkte** gesehen, bei denen die Summe aller Komponenten bei der Auswahl letztlich signifikant teurer ist als bereits vorhandene Produkte, die alle Komponenten abdecken. Dies ist gerade im Zusammenhang mit **„beratungslosen“ Angeboten** kritisch zu sehen.
- Das Retailgeschäft wird von **wenigen Marktteilnehmern** (idR globalen Technologiekonzernen) dominiert. Durch die zunehmende Konzentration auf wenige IT-Anbieter (z. B. Cloudserviceprovider) entstehen **Konzentrations- und Ansteckungsrisiken**, die sich negativ auf die IT-Sicherheit auswirken (Spill-over-Effekt). Auf der anderen Seite ist eine geringe Zahl von IT-Anbietern als ausschließliche Kontaktstelle und zentraler Sicherheitszugang effizienter und hat positive Aspekte für die IT-Sicherheit. Durch professionelles Sicherheitsmanagement der großen Player kann die Wahrscheinlichkeit eines Angriffs gesenkt werden, der potenzielle Schaden ist aber ungleich höher.
- Ein Stakeholder thematisiert außerdem diverse kritische Aspekte der in der FMA-Studie angeführten Finanzprodukte (z. B. Risiko, dass Scheinkorrelationen hergestellt werden oder Parameter zum Einsatz kommen, die nicht zur Gänze in der Kontrolle der Kunden liegen, etc.) und stellt etwa auch in Frage, ob das Cyberrisiko in Wahrheit nicht der Anbieter der Technologien tragen sollte, so wie ein Anbieter von Backwaren dafür zu haften hat, dass von den Backwaren kein Risiko fur die Gesundheit der Kunden ausgeht.

Die Erwartungshaltung an die Rolle der Aufsicht ist durchaus vielschichtig: Es wird angeregt, dass technische Standards etwa für Robo-Advice festgelegt werden und die Aufsicht technische Prozesse überwacht, die in den Unternehmen gewährleisten sollen, dass keine diskriminierenden und/oder datenschutzwidrigen Entscheidungsparameter verwendet werden. Zu den Aufgaben und Vorgaben der FMA sollte auch die verpflichtende regelmäßige Prüfung, Beanstandung und Modernisierung veralteter IT-Systeme gehören. Die Analyse von Cyberrisiken, diesbezügliche Workshops und Simulationen werden ausdrücklich begrüßt.

- Die Digitaliserung darf zu **keinem Aufweichen des Anleger-, Versicherten- und Gläubigerschutzes** führen. Eine der wichtigsten Aufgaben der FMA wird dement-sprechend in der Bereitstellung von **Verbraucherinformationen** gesehen.
- Um ein Level Playing Field zu gewährleisten, sollten auch bei digitalen Geschäftsmodellen die sektoralen **organisatorischen Anforderungen** eingehalten werden müssen.
- Analog zur Prüfung interner Risikomodule sollten auch im Sinne der Wohlverhaltensregeln der Aufsicht gegenüber die **technischen Prozesse** verpflichtend dargelegt werden. Diese Prüfprozesse sollten sicherstellen, dass keine diskriminierenden und/oder datenschutzwidrigen Entscheidungsparameter verwendet werden. Es sollten **technische Standards** etwa **für Robo-Advice** festgelegt werden, die einer Ex-ante-Prüfung (Audit) und anlassbezogenen Ex-post-Prüfungen unterworfen sein sollen.
- Die **regelmäßige Prüfung, Beanstandung und Modernisierung veralteter IT-Systeme** auf verpflichtender Basis sollte zu den Aufgaben und Vorgaben der FMA im Zusammenhang mit dem Einsatz von IT-Systemen gehören. Die Analyse von Cyberrisiken, diesbezügliche Workshops und Simulationen werden ausdrücklich begrüßt. Dies ist insbesondere von großer Bedeutung, da Unternehmen teilweise kein ausreichendes Verständnis der Risiken und Herausforderungen im Hinblick auf die IT-Finanzarchitektur aufweisen.
- Die Notwendigkeit eines **Diskurses um ethische Grenzen** wird von mehreren Institutionen aufgezeigt. Ein Stakeholder begrüßt ausdrücklich, dass die Aufsicht eine Vorreiterrolle in dieser Diskussion spielt. Gleichzeitig seien hier aber auch Gesellschaft und Politik gefragt. Aus der Verwendung von „Big Data“ darf keine Aushebelung des Solidarprinzips folgen.

IV. VERTRIEB/KUNDENSCHNITTSTELLE

Welche Aufgaben soll die FMA im Rahmen des Anleger-, Versicherten- und Gläubigerschutzes im Hinblick auf die Digitalisierung der Schnittstellen zu den Kunden wahrnehmen? Welche konkreten regulatorischen Vorgaben sind durch die Digitalisierung des Finanzsektors noch notwendig? Bestehen in Österreich Hindernisse, die die digitale Kommunikation erschweren? Welche konkreten positiven, aber auch negativen Entwicklungen bezüglich des „digitalen" Vertriebs sind aus Ihrer Sicht zu beobachten? Das waren einige der Fragen, die die FMA im Call for Input gestellt hat.

Die am Call for Input teilnehmenden Stakeholder ergänzten die Sichtweise der FMA um die folgenden Einschätzungen:

Einigkeit besteht im Wesentlichen darüber, dass **regulatorische Vorgaben** den digitalen Wandel noch nicht ausreichend reflektieren. Zum einen wird dafür plädiert, dass die Regulierung (insbesondere Bankgeheimnis, Datenschutz, TKG, FM-GwG) im Sinne der Customer Convenience eine rein digitale Geschäftsabwicklung ohne physische Präsenz des Kunden ermöglichen sollte. Zum anderen tritt ein Stakeholder dafür ein, dass es Konsumenten weiterhin ermöglicht werden muss, in Papierform zu kommunizieren – bzw. vertragliche und vorvertragliche Informationen zu erhalten – und dass diese Kommunikationsform nicht durch Zusatzentgelte pönalisiert werden darf. Konsumenten sollten weder faktisch noch aus Kostengründen Technologien aufgezwungen werden. Außerdem wird moniert, dass die datenschutzrechtlichen Vorgaben allgemein gehalten seien und nicht zur Beantwortung branchenspezifischer Datenschutzfragen der Kunden ausreichten.

- **Datenschutzvorgaben:** Mit der EU-Datenschutz-Grundverordnung (DSGVO) sei zwar ein richtiger Schritt gemacht worden, die Meinungen über deren Wirksamkeit divergieren jedoch stark: Zum einen möchte man abwarten, wie sich der neue Standard bewährt, bevor geprüft wird, ob gegebenenfalls Erweiterungen/Anpassungen notwendig sind. Zum anderen wird aber dessen Durchführbarkeit im Hinblick auf den realen Mehrwert des Kunden und die Auswirkung auf die Banken hinterfragt oder kritisiert, dass dessen Vorgaben allgemein gehalten seien und nicht zur Beantwortung branchenspezifischer Datenschutzfragen von einiger Tragweite für Konsumenten ausreichten. Soweit die DSGVO Präzisierungsspielraum eröffne, sollte der österreichische Gesetzgeber diesen für branchenspezifische Detailregelungen nutzen. Dies betreffe etwa Bonitätsbewertungen, die in der GewO in Bezug auf den Datenschutz und verschiedene Adressatenkreise unzureichend geregelt seien, oder die automatisierte Entscheidungsfindung und das Profiling von Kunden von Finanzdienstleistungen. Alternativ wäre darauf zu dringen, dass der europäische Datenschutzausschuss entsprechende Leitlinien für die Praxis verabschiedet.
- **Digitale Kommunikation:** Es sei wünschenswert, dass im Sinne der Customer Convenience die Regulatorik (insbesondere Bankgeheimnis, Datenschutz, TKG, FM-GwG etc.) so ausgestaltet ist/wird, dass eine rein digitale Geschäftsabwicklung ohne physische Präsenz des Kunden ermöglicht wird. Auch sollte der Ausbau der Verbindungstechnologie in jedem Fall mit der zu erwartenden Ausweitung der Datenvolumina für die digitale Kommunikation Schritt halten. Im Bereich der Zahlungsdienste sorgten im Zuge der Regulierung der verstärkten Kundenauthentifizierung nach § 87 ZaDiG 2018 einige Kreditinstitute für Verunsicherung. So werde zur Authentifizierung auf die Nutzung einer Smartphone-App statt der Übermittlung von SMS-TAN gedrängt. Manche Banken informierten ihre Kunden unzutreffenderweise sogar schriftlich darüber, dass das SMS-TAN-Verfahren „aufgrund gesetzlicher Vorgaben" abgelöst werde.
- Bei der Schaffung von etwaigen weiteren Regularien sollte der Grundsatz „One in – One out" berücksichtigt werden, um eine weitergehende Überregulierung zu vermeiden. Insbesondere bedürfe es einer abschließenden Umsetzung der bereits bestehenden Rechtsakte wie beispielsweise PRIIP, PSD II, MiFID II, bevor neue gesetzliche Vorgaben angedacht werden.

Als **positive Entwicklungen** im Hinblick auf den digitalen Vertrieb werden insbesondere der Anstieg der Verfügbarkeit von Bankprodukten, kein Ersatz der Beratungsleistungen und rasche Entscheidungswege am Point of Sale wahrgenommen. Für Firmenkunden sei vor allem die direkte Anbindung der Online-Banking-Plattform an ihre ERP-Systeme ein enormer Vorteil; bei speziellen Anfragen könne der Kundenbetreuer allerdings nicht durch den digitalen Vertrieb ersetzt werden.

Negativ betrachtet werden komplexe Angebote ohne jegliche Beratung sowie modulare Produkte, bei denen die Summe aller Komponenten bei der Auswahl letztlich signifikant teuer ist als bei bereits vorhandenen Produkten, die alle Komponenten abdecken.

Skepsis wird auch der Schließung von Bankstellen entgegengebracht, womit die klassischen Banken ihre USP (direkter Kundenkontakt) gegenüber klassischen Onlinebanken verlieren.

Die **Erwartungshaltung an die Aufsicht** ist durchaus vielschichtig und umfasst etwa folgende Anregungen:

- Der Beratungs- und Abschlussprozess sollte für alle Beteiligten einfacher und schneller (ohne Medienbruch und Wartezeiten) vonstattengehen. Da der Begriff „Beratung“ gesetzlich definiert ist, sollte die Aufsicht sicherstellen, dass dort, wo „Beratung“ draufsteht, auch tatsächlich **Beratung** drin ist.
- Dort, wo **Algorithmen** zum Einsatz kommen, sollten diese hinsichtlich der Einhaltung von Wohlverhaltensregeln und Diskriminierungsfreiheit der Aufsicht vor- und darzulegen sein. Denn Anleger können die Qualitat der Robo-Advice-Programme sowie die ihnen zugrunde liegenden Parameter kaum einschätzen und bewerten. Durch Robo-Advice-Systeme können Interessenkonflikte nicht automatisch vermieden werden; vielmehr bestehe die Gefahr, dass die Intransparenz von Empfehlungen noch erhöht wird.
- Digitaler Vertrieb soll **Nachvollziehbarkeit gewährleisten**. Ob diesem Anspruch beispielsweise durch Chats auf Facebook Genüge getan wird, sei allerdings sehr zweifelhaft. Jedenfalls sollten unabhängig vom Vertriebskanal **Abschluss und Kündigung symmetrisch** erfolgen können, d. h., es sollte über die Kanäle, über die ein Dauerschuldverhältnis errichtet werden kann, dieses auch wieder beendet werden können.
- Die **Wahrung des Bankgeheimnisses und des Datenschutzes** stellt eine besondere Herausforderung bei allen Schnittstellen dar und sollte einer gesonderten Überprüfung durch die Aufsicht unterzogen werden. Für die digitalen Schnittstellen zum Kunden sollen die gleichen Regeln wie für die Offline-Schnittstellen gelten. Dies gilt auch für Informations- und Dokumentationspflichten und die Legitimationsprüfung (KYC).
- Die Aufsicht sollte auf einheitliche, **gleiche Wettbewerbsbedingungen** in der EU, z. B. in Bezug auf die Videoidentifikation, hinwirken. Kritisch beäugt wird auch das noch fehlende Level Playing Field etwa im Hinblick auf die Offenlegungspflichten der Onlinebanken.
- Ebenfalls sollte **täuschende Werbung** verhindert werden, und eine Zustimmung des Kunden soll datenschutzrechtlich korrekt eingeholt werden.
- Eine Regulierung von **Vergleichsportalen** erscheint sinnvoll. Dem Kunden sollte transparent gemacht werden, in welcher Relation Betreiber und Produktanbieter stehen, welche Gebühren und Provisionen an den Betreiber gehen und nach welchen Kriterien das vorgelegte Ranking erzeugt wurde. Die praktische Erfahrung zeige, dass in gängigen Vergleichsportalen etliche marktdominante Anbieter nicht gelistet sind, was erhebliche Zweifel an der Marktrepräsentativität aufkommen lässt. Die Portalbetreiber sollten deshalb verpflichtet werden, vor allem die gelisteten Anbieter, gegebenenfalls inklusive der Zahlen zu den Marktanteilen, klar und deutlich offenzulegen, um nicht den Anschein von Vollständigkeit oder einer besonderen Marktrepräsentativität zu erwecken.
- Im Zusammenhang mit dem Einsatz von **personalisierten Websites** ist die größte Herausforderung, dass die abgespeicherten Informationen für Kunden dauerhaft abrufbar sind und ein permanenter Zugriff auf die Webseite möglich ist.

- **Soziale Medien** würden die Gefahr in sich bergen, dass erstens Kommunikation flüchtig und nicht mehr nachvollziehbar ist. Zweitens sei zu beobachten, dass Strukturen von Netzwerk-Marketing aufgezogen werden, die den Charakter von Strukturvertrieben aufweisen. Das Strukturvertriebsprinzip könne jedoch einen gewaltigen Massenschaden verursachen.
- Der Trend zu **Mobile Apps** könne dazu führen, dass andere Kanäle der Kommunikation bewusst vernachlässigt oder zum Teil mit höheren Entgelten (oder sonstigen Nachteilen) belegt werden. Es wird auch kritisch gesehen, wenn Unternehmen ihre Kunden anhalten, ihre Zugangs- oder sonstigen Vertragsdaten ausschließlich auf einem Endgerät zu speichern, das als Einfallstor fur Betrug/Missbrauch verwendet werden könne.
- Der Ersatz von Beratern durch **Chatbots** (statt E-Mails) sei nicht im Interesse vieler Konsumenten, die sich persönliche Beratung bei komplexen Finanzprodukten wünschen. Chatbots sollen als Ergänzung, nicht jedoch als Ersatz für persönliche Beratung dienen. Auch das Ersetzen von E-Mail-Kommunikation sei kritisch zu betrachten, denn durch E-Mails werden Kommunikationsprozesse nachvollziehbar in Bezug auf Zeitpunkt, Inhalt und Adressaten der Kommunikation.

V. ASSET MANAGEMENT

Welche Aufgaben soll die FMA aus Ihrer Sicht bezüglich der Digitalisierung im Asset Management wahrnehmen? Welche Hindernisse bestehen, um die Asset-Management-Prozesse zu automatisieren und den Ausbau von alternativen Techniken wie AI, Deep Learning und Machine Learning zu erleichtern? Zu diesen Themen ist im Rahmen der Konsultation folgender Input eingelangt:

Vorteile der Digitalisierung im Asset-Management-Bereich werden im Kostensenkungspotenzial und in Effizienzgewinnen sowie in der Reduktion von operationellen Risiken gesehen.

Die damit einhergehende Automatisierung sei parallel dazu jedoch mit diversen **Nachteilen** verbunden: Verringerung von Arbeitsplätzen bei gleichzeitigem Mangel an geeigneten Fachkräften für den Ausbau der IT-Infrastruktur und für das Management von Schnittstellen, da Finanzdienstleister in der Regel nur Lösungen für Teilbereiche (Informationsaufbereitung, Handel, Fondsbuchhaltung) anbieten, hohe Einmalaufwendungen, Abhängigkeit von externen Anbietern und automatisierten Prozessen.

Die **Erwartungshaltung an die Aufsicht** umfasst auch in diesem Bereich diverse Anregungen:

- Es wird eine **technologieneutrale Aufsicht** gewünscht, die technologieaffine Unternehmen weder bevorzugt noch benachteiligt. Gleiche Standards sollen für alle Marktteilnehmer gelten.
- Es könnte sich in Zukunft ein **Fokus auf die IT-Sicherheit** ergeben.
- Neue Geschäftsmodelle im Zuge der Digitalisierung können **Adaptionen bestehender Regulierungen** zur Folge haben:
  - Bei Krypto-Assets als Assetklasse müssen Diversifikationsmöglichkeiten für ein Portfolio angemessen berücksichtigt werden. Zudem könnte sich ein Bedarf an Veranlagungs-bestimmungen ergeben.
  - Adaptionen im Bereich der Geldwäscherei könnten notwendig werden.
  - Auch müsse aufsichtsrechtlich geregelt werden, wann bei Krypto-Assets überhaupt ein Wertpapier vorliegt.
  - Es wird mit einem Marktvorteil bei alternativen Produkten wie Kryptowährungen gerechnet, da diese weniger strengen aufsichtsrechtlichen Vorschriften unterliegen.
- Beim Anlageprozess wird eine Digitalisierung von Prozessen inklusive der Bewertung von Anlagen erwartet. Hierfür sollten **Mindeststandards** eingeführt werden.

VI. RECHNUNGSLEGUNG

Die Digitalisierung hat auch Auswirkungen auf Rechnungswesen und Rechnungslegung. Dies betrifft insbesondere die Rahmenbedingungen der Buchhaltung und der Finanzberichterstattung, die Abbildung von digitalen Innovationen (z. B. Kryptowährungen) in der Rechnungslegung und die Abschlussprüfung.

Bei diesem Thema haben die Stakeholder des Call for Input folgende Anmerkungen:

Vorteile der Digitalisierung in der Rechnungslegung werden in Effizienzgewinnen (die jedoch großteils durch einen größeren Informationsbedarf der Stakeholder/Regulatoren kompensiert werden) und einer schnelleren Datenverfügbarkeit sowie in einer Verbesserung von Plausibilisierungen und Bewertungen durch den Einsatz digitaler Instrumente gesehen.

Die Digitalisierung der Rechnungslegungsprozesse berge aber auch diverse **Nachteile**: Hohe Investitionskosten und Bindung von Fachexperten bei den Innovationsprojekten, Plausibilisierung und Bewertungen bedürfen trotz allem professioneller Kompetenzen und des Sachverstands der Prüfer; die Herausforderung von Kontrolleuren werde es sein, das Zusammenwirken komplexer Softwaresysteme, die dahinterliegende Logik der Analyse sowie die Ergebnisse von umfangreichen und mächtigen Datenanalysen nachzuvollziehen und zu verstehen und damit entsprechende Implikationen auf das Prüfergebnis anstellen zu können.

Die **Erwartungshaltung an die Aufsicht** umfasst verschiedene Anregungen:

- Der Einsatz digitaler Instrumente führt teilweise zu massiven Änderungen der gesamten Prozesskette der Rechnungslegung – von der Eingabe über die Analyse bis zur Kontrolle. Die Entwicklung der Rechnungslegung – insbesondere der internationalen Rechnungslegung – zeigt eine massive Tendenz, zukünftige Einschätzungen und Erwartungen von verschiedenen wirtschaftlichen Phänomenen in der Rechnungslegung stärker in die Ansätze der Jahresabschlussposten einfließen zu lassen. Aufgabe der Aufsicht werde es sein, im Rahmen der Regulierung die **Qualität von Prüfungen weiterhin zu gewährleisten**. Auch Prüfkompetenzen von Kontrolleuren des IKS bzw. der Jahresabschlussprüfung seien noch stärker auf das Funktionieren von Prüfsystemen sowie den Einsatz digitaler Instrumente auszuweiten.
- Die Aufsicht müsse insbesondere bei den **Fit-&-Proper-Anforderungen** entsprechende Kenntnisse, Fähigkeiten bzw. Erfahrungen stärker in den Vordergrund rücken.
- Die **Digitalisierung der Kommunikation** zwischen Banken und der Aufsicht, insbesondere im Hinblick auf Meldungen und den Austausch sonstiger aufsichtsrelevanter Informationen, sollte weiter ausgebaut werden.
- Die **physische Aufbewahrungspflicht** von Dokumenten sollte in den verschiedenen Bundesgesetzen vereinheitlicht werden, sodass flächendeckend elektronische Formate bzw. Scans ermöglicht werden.

VII. IT-INFRASTRUKTUR

Welche Aufgaben soll die FMA iZm den am österreichischen Finanzmarkt genutzten IT-Systemen wahrnehmen? Welche konkreten regulatorischen Vorgaben sind iZm dem Einsatz von IT-Systemen im Finanzsektor notwendig? Welche positiven und negativen Aspekte für die IT-Sicherheit hat die zunehmende Konzentration des Finanzmarktes auf wenige IT-Anbieter? Sind die wesentlichen Vorteile und möglichen Nachteile agiler Vorgehenswesen erfasst?

Zu diesen Fragestellungen ist im Rahmen der Konsultation insbesondere folgender Input eingelangt:

Die zunehmende **Konzentration** des Finanzmarktes **auf wenige IT-Anbieter** birgt sowohl Vor- als auch Nachteile:

- Positiv zu bewerten sei, dass die **Komplexität der Schnittstellen** zwischen den unterschiedlichen Lösungen **abnehme**. Es entstünden außerdem Lösungen, die zur Erkenntnisgewinnung und für Sicherheitsfunktionen genutzt werden können. Die Konzentration auf wenige IT-Anbieter führe überdies zu einheitlichen oder zumindest **ähnlichen Prozessabläufen**. Mitarbeiter, die innerhalb der Branche den Arbeitgeber wechseln, seien deshalb häufig mit eingesetzten IT-Systemen vertraut. Zudem könnten durch einheitliche Systeme Sicherheitsschwachstellen schneller erkannt und behoben werden.
- Nachteilig ist, dass die Konzentration auf wenige IT-Anbieter **im Falle eines Ausfalls** eines solchen Diensteanbieters **weitreichende systemische Auswirkungen** auf Unternehmen im Finanzsektor haben könne. Besonders kritisch sei es, wenn es mehrere Betreiber wesentlicher Dienste betrifft. Die Überprüfung dieser Anbieter im Zuge der Sorgfaltspflicht sei deshalb essenziell.

Auch der **Einsatz von agilen Methoden** bringt neben vielen Erleichterungen auch einige Risiken, die sich die Finanzmarktteilnehmer bewusst machen sollten:

- Positiv zu bewerten sei, dass man in fast allen Bereichen im Zuge der Modernisierung auf agile Vorgehensweisen setzt, um **Anforderungen des Marktes zeitnah umsetzen** zu können und die Time-to-Market durch kürzere Iterationszyklen zu verbessern. Auch bei der IT-Architektur sei es von Vorteil, Komponenten unabhängig voneinander entwickeln zu können; anstelle von großen Monolithen steht eine Vielzahl von Microservices im Vordergrund**.**
- Oft seien allerdings nicht alle Entwickler mit der Methode zufrieden bzw. vertraut. Zudem bestehe ein erhöhter Testaufwand, der Ressourcen erfordere. Es sei oft **schwierig, Projektkosten zu Beginn einzuschätzen**, was erst im Lauf eines Projektes besser werde. Erhöhte Kommunikation zwischen verschiedenen Bereichen sei notwendig, was bisher oft nicht üblich war. Bei der Modernisierung der IT-Landschaften kommt es überdies nicht immer zu einer Konsolidierung oder Vereinfachung der Applikationslandschaft. Vielmehr wird diese aufgrund der fehlenden Konsequenz bei der Abschaltung bestimmter Legacy-Systeme vervielfältigt. Dies führt zu einer **dauerhaften Redundanz**.

Hinsichtlich der **Rolle des Regulators und der Aufsicht** wurden in diesem Bereich folgende Anregungen gemacht:

- IZm dem Einsatz von IT-Systemen im Finanzsektor werden **klare rechtliche Rahmenbedingungen** (z. B. SREP/ISO2700x – je konkreter, desto besser) als notwendig erachtet. CROE sei ein gutes Beispiel für konkrete Maßnahmen.
- Es müsse außerdem eine **Kontrollinstanz für die eingesetzten Systeme** im Hinblick auf Security, Sourcing und Governance geben.
- Die FMA sollte dafür sorgen, dass beaufsichtigte Unternehmen **fit & proper im Bereich IT** sind, um die Wettbewerbsfähigkeit zu erhalten und Verdrängungseffekten vorzubeugen.

VIII. CYBERRISIKEN

Mit welchen Maßnahmen bzw. Initiativen könnte die FMA zur Erhöhung der Cybersicherheit am Finanzmarkt konkret beitragen? Welche Cyber-Bedrohungsszenarien könnten in Zukunft besonders relevant für den österreichischen Finanzmarkt sein? Welche Kernbereiche der IT-Sicherheit sollten von Unternehmen der österreichischen Finanzmärkte prioritär verstärkt werden? Sollten von den Unternehmen weitere Maßnahmen zur künftigen Abwehr von Cyberattacken gesetzt werden? Ist die Bedrohungslage zwischen den Branchen des Finanzmarktes aus Ihrer Sicht einheitlich zu sehen, oder sind bestimmte Sparten besonders exponiert? Welche Rechtsunsicherheiten, Chancen und Risiken sehen Sie iZm den Cyberversicherungen?

Die am Call for Input teilnehmenden Stakeholder bekräftigten im Wesentlichen die Schlussfolgerungen der FMA hinsichtlich der Cyberrisiken und ergänzten diese um folgende Einschätzungen:

Als für den österreichischen Finanzmarkt besonders relevante **Cyber-Bedrohungsszenarien** werden etwa Datenverlust oder Datenklau im Zuge von Cloud-Computing und Bedrohungen aufgrund von „Schatten-IT“ (Intransparenz der IT-Infrastruktur) bei Cloud-Anbietern identifiziert. Zu weiteren Bedrohungen zählen Malware, Crypto, Erpressung, Zero Days sowie Insider Fraud.

- Zur Verbesserung der IT-Sicherheit sollten die folgenden **Bereiche prioritär verstärkt** werden: Awareness, Identity and Access Management, Privileged Access Management, Asset Management, Cloud Security, Secure Software / System Development, Incident Management, Third Party Risk Management, detektive Technologien und BCM. Zur Abwehr von Cyberattacken sollte mittels eines zentralisierten Managements von Sicherheitsvorfällen ein Überblick geschaffen werden, und in Bezug auf Cybererpressungen sollte eine klare Vorgehensweise entwickelt werden. Wichtig sei es, die Früherkennung von Angriffen und Sicherheitsvorfällen (z. B. SIEM/SOC) zu optimieren. Von Drittherstellern bereitgestellte Softwareprodukte sollten verstärkt kontrolliert werden.
- Im Hinblick auf die Bedrohungslage sei diese innerhalb des Bankensektors eher einheitlich. Entscheidend für die Bedrohungslage sei die **Präsenz der eigenen Marke**, die durch Vermarktung mehr Aufmerksamkeit erhalte. Zusätzlich könne der (schlechte) Umgang mit Kunden und Security-Researchern zu einer sprunghaften Steigerung der Bedrohungslage führen. Je mehr sich ein Unternehmen durch Web-Portale und öffentlich verfügbare Schnittstellen exponiere, desto mehr mache es sich angreifbar.

Als **positive Entwicklung** im Hinblick auf Cyberangriffe wird der verstärkte Informationsaustausch (IOCs, Tools etc.) vor allem durch CERTs oder andere internationale staatliche Organisationen gesehen. Außerdem entwickle sich die Produktlandschaft mit Security-Fokus sehr positiv weiter.

Zu den **negativen Entwicklungen** zählt, dass die Politik wieder vermehrt Interesse zeige, dass kryptografische Verfahren geschwächt werden (Bundestrojaner, Hack-back, australische „Assistance and Access bill“). Weiters wechsle der Fokus von Ransomware von Privatpersonen auf Unterneh-men und staatliche Einrichtungen.

Hinsichtlich der **Rolle des Regulators und der Aufsicht** wurden im Bereich der Cyberrisiken folgende Anregungen formuliert:

- Wenn Angriffe im Sektor erkannt und gemeldet werden, die für andere Institute relevant sind, sollten **Warnungen und Empfehlungen** ausgesprochen werden. Somit steigere sich der Mehrwert der Meldung von Sicherheitsvorfällen für die Institute.
- **Eine starke Prüfung** vor allem in Bezug auf Governance, Ablauf und Aufbauorganisation, Skills, moderne Erkennungsmethoden, Security Strategy sowie die Prüfung neuer Themen wie Cloud, IAM, agile Entwicklung sowie Vorstands- und Aufsichts-Awareness wären wünschenswert.

- Es wäre hilfreich, wenn eine **Zuordnung zwischen bestehenden regulatorischen Vorgaben** der FMA und Vorgaben von EBA, ECB, regulatorischen Anforderungen und Best-Practices (z. B. ISO/IEC 27001) erstellt werde. Dadurch könnte die Compliance für diese Anforderungen leichter überprüft und bewertet werden.
- Es werden eine **stärkere Ausformulierung** wie z. B. in CROE auf verschiedenen Ambitionsniveaus sowie ein Fokus auf Cloud, IAM, detektive Security-Technologien und Incident Response gewünscht.
- Der Datenschutz und damit **Privacy im Banking-/Insurance-Bereich** könnte ausführlicher betrachtet werden. Es wäre etwa interessant, was in diesem Bereich proaktiv getan werde. Der Datenschutz und die Datensicherheit müssen bei Software und Applikationen aus Österreich berücksichtigt werden.

IX. DIGITALE TECHNOLOGIEN

Sollen entsprechend Ihrer Erfahrungen bzw. Ihrer Einschätzung nach weitere digitale Technologien bzw. Einsatzmöglichkeiten in die Betrachtung der Implikationen der Digitalisierung auf den österreichischen Finanzmarkt einbezogen werden? Welche Rechtsunsicherheiten sind aus Ihrer Sicht mit dem Einsatz neuer digitaler Technologien verbunden? Teilen Sie die Einschätzung der FMA in Bezug auf die Chancen und Risiken der einzelnen Technologien? Welche weiteren wesentlichen Risiken könnten aus Ihrer Sicht für die einzelnen Sektoren künftig relevant sein? Was ist Ihre Erwartungshaltung hinsichtlich der Rolle der Aufsicht in den einzelnen Sektoren des Finanzmarktes?

Die am Call for Input teilnehmenden Stakeholder bekräftigten im Wesentlichen die Schlussfolgerungen der FMA hinsichtlich der neuen Technologien, welche sich auf den Finanzmärkten verbreiten, und ergänzten diese um folgende Einschätzungen:

- In einer sich permanent verändernden Umgebung ist es essenziell, am Puls der Zeit zu bleiben. In Zukunft seien deshalb **tiefergehende Analysen der Chancen und Risiken** für den Finanzmarkt erforderlich.
- Bezüglich IoT sei der **Prozess der Entstehung der Daten im Device** selbst nicht rechtlich geregelt, weshalb in diesem Zusammenhang oft Rechtsunsicherheiten bestünden.
- Im Hinblick auf **Robo-Advisors** werden Rechtsunsicherheiten bezüglich der Haftungsfrage gesehen. Es bedürfe Klarstellungen, unter welchen Voraussetzungen die Hersteller und wann die Anbieter die Haftung zu tragen haben.
- Die Aufsicht müsse bereits im Vorhinein **Standards setzen** und diese in Form eines **Coachings mit den beaufsichtigten Unternehmen** teilen. Banken seien hier bei vielen Themen noch in der Experimentierphase und achteten in erster Linie darauf, Umsatz und Profit zu steigern.
- Es wäre begrüßenswert, wenn es für den Einsatz von neuen digitalen Technologien eine **regulatorische Sandbox** gäbe, in der man technische Lösungen aus regulatorischem Blickwinkel auf Herz und Nieren prüfen könne und somit schneller zu einsetzbaren technischen Lösungen im Rahmen von (dadurch auch schneller) adaptierten regulatorischen Rahmenbedingungen käme.
- Die Chancen der Blockchain seien im Wesentlichen richtig abgebildet. Zu erwähnen sei jedoch insbesondere auch die **Abwicklung von Verträgen** (Smart Contracts) **ohne Ausfallrisiko**, was gerade am Finanzmarkt zu wesentlichen **Chancen** führen könne.

ABKÜRZUNGSVERZEICHNIS

AI	Artificial Intelligence
AIFMG	Alternative Investmentfonds Manager-Gesetz
API	Application Programming Interface
B2C	Business-to-Customer
BDA	Big Data Analytics
BIP	Bruttoinlandsprodukt
BVK	Betriebliche Vorsorgekassen
BWG	Bankwesengesetz
CROE	Cyber Resilience Oversight Expectations
DLT	Distributed Ledger Technology
DSGVO	Datenschutz-Grundverordnung
EBA	European Banking Authority
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Union Agency for Network and Information Security
ESMA	European Security Markets Authority
EK	Europäische Kommission
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FSB	Financial Stability Board
FMABG	Finanzmarktbehördenaufsichtsgesetz
IAM	Identity Access Management
IDD	Versicherungsvertriebsrichtlinie (EU) 2016/97
idR	in der Regel
idZ	in diesem Zusammenhang
IEC	International Electrotechnical Commission
IFRS	International Financial Reporting Standards
IoT	Internet of Things
ISO	International Standards Organization (Internationale Organisation für Normung)
iZm	in Zusammenhang mit
KI	Kreditinstitute / künstliche Intelligenz
KMU	kleine und mittelgroße Unternehmen
KYC	Know your Customer
MI	Marktinfrastrukturen
MiFID	Markets in Financial Instruments Directive
OGH	Oberster Gerichtshof
ORSA	Own Risk and Solvency Assessment
PaaS	Platform as a Service
PK	Pensionskassen
PKV	Private Krankenversicherung
P2P	Peer-to-Peer
PRIIP	Packaged Retail Investments and Insurance Products
PSD	Payment Service Directive
RPA	Robotic Process Automation
(R)VU	(Rück-)Versicherungsunternehmen
SaaS	Software as a Service
SI	signifikante Institute
SREP	Supervisory Review and Evaluation Process
uU	unter Umständen
VAG	Versicherungsaufsichtsgesetz 2016
VersVG	Versicherungsvertragsgesetz
VU	Versicherungsunternehmen
WPF	Wertpapierdienstleister und Wertpapierfirmen
ZaDiG	Zahlungsdienstegesetz
z. B.	zum Beispiel