ÖSTERREICHISCHE FMA·FINANZMARKTAUFSICHT

Digitalisierung am österreichischen Finanzmarkt

Call for Input: Ergebnisse

April 2022

INHALTSVERZEICHNIS

Im vorliegenden Bericht wird aufgrund der leichteren Lesbarkeit 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. Die rechtlichen Grundlagen bleiben durch diesen Bericht unberührt. Über die gesetzlichen Bestimmungen hinausgehende Rechte und Pflichten können aus diesem Dokument nicht abgeleitet werden. Trotz sorgfältiger Aufbereitung und Recherche übernimmt die FMA keine Haftung für die Richtigkeit und Vollständigkeit der Daten und Inhalte in diesem Bericht.

EINLEITUNG

Analyse der FMA zur Digitalisierung am österreichischen Finanzmarkt

Die digitale Transformation verändert grundlegend die Rahmenbedingungen am Finanzmarkt, bringt neue Chancen, aber auch Auslegungsschwierigkeiten und Risiken und stellt die Aufsichtstools auf den Prüfstand. Die FMA ist deshalb daran interessiert, bei der Digitalisierung am Ball zu bleiben und Treiber, Trends und mögliche künftige Entwicklungen richtig einzuschätzen. Wir haben deshalb im Jahr 2021 unsere Analyse zur Digitalisierung am österreichischen Finanzmarkt fortgeführt. Bei einer beinahe vollständigen Marktabdeckung in fast allen Sektoren des Finanzmarkts und einer hohen Mitwirkung der beaufsichtigten Unternehmen konnten wir aktuelle Erkenntnisse zum Stand der Digitalisierung und den Einsatzbereichen digitaler Technologien am österreichischen Finanzmarkt gewinnen.

Um eine breitere Diskussion anzustoßen und den Dialog zu den Implikationen der Digitalisierung zu intensivieren, hat die FMA außerdem die Stakeholder – die Kunden der beaufsichtigten Unternehmen, ihre Interessensvertretungen, Branchenverbände sowie die interessierte Öffentlichkeit eingeladen, die im Bericht zur Digitalisierung am österreichischen Finanzmarkt skizzierten Erkenntnisse und Schlussfolgerungen kritisch zu hinterfragen und um ihre Erfahrungen, Ansichten und Lösungsansätze anzureichern.

Ergebnisse des Call for Input

Verschiedenste Stakeholder sind diesem Call for Input gefolgt und haben im Februar 2022 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 (zB Fragen des Datenschutzes, Umgang mit Haftungen für Risiken, die mit der Digitalisierung verbunden sind, und Risiken einer bloß flüchtigen und nicht mehr nachvollziehbaren Kommunikation bei der Forcierung sozialer Medien).
- Mehrere Stakeholder machen rechtspolitische Anregungen und Vorschläge de lege ferenda (so wird etwa vorgeschlagen, Vorsorge dafür zu treffen, dass der Digitalisierung zugrundeliegende Algorithmen diskriminierungsfrei sind und eine analoge Mindestinfrastruktur verpflichtend aufrecht erhalten bleibt, damit Dienstleistungen nicht in Richtung ausschließlicher Digitalisierung transformiert werden).

Die FMA bedankt sich für die umfangreichen Stellungnahmen und wird diesen wertvollen Input in ihre strategische Planung bzw. in die Festlegung der Aufsichtsschwerpunkte entsprechend einfließen lassen.

I. STRATEGIEN

In welchen Bereichen werden disruptive Entwicklungen aus Ihrer Sicht mittel- bis langfristig erwartet? Welche Chancen und Risken der Digitalisierung sind für den österreichischen Finanzmarkt entscheidend? Was sind die Erfolgsfaktoren, um den digitalen Wandel optimal bei der Weiterentwicklung der Geschäftsmodelle in den einzelnen Sektoren des Finanzmarktes zu nutzen? 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:

Die Auswirkungen der Digitalisierung auf den österreichischen Finanzmarkt werden insgesamt positiv eingeschätzt. Digitalisierung fördert Innovationen und unterstützt Finanzmarktteilnehmer dabei, Kunden besser zu verstehen und Geschäftsmodelle sowie Finanzprodukte auf deren Bedürfnisse auszurichten.

- Die Auswirkungen der Digitalisierung beschränken sich nach Ansicht der Stakeholder nicht bloß auf Effizienzsteigerungen und Kosteneinsparungen. Neue Mitbewerber und neue Geschäftsmodelle zwingen bestehende Branchen zu **Innovation und Agilität**. Im Zuge der digitalen Transformation werden **Marktanteile völlig neu aufgeteilt**.
- Besonders starken Einfluss wird der Digitalisierung auf **weniger beratungsintensive Produkte und Services** beigemessen: Vor allem im Zahlungsverkehr wird weiterhin mit einer starken Veränderung der Prozesse durch die Digitalisierung gerechnet. Zunehmend betroffen werden aber auch Kreditgeschäfte mit kleineren Summen, Transaktionsprozesse und das Wertpapiergeschäft. Erwartet wird, dass sich die Bearbeitung der Kunden- und Vertriebsfelder zwischen analoger und digitaler Welt abspielen wird. Dabei entstehen neue Dienstleistungsfelder, während alte verschwinden. Wichtig bleibt idZ die Möglichkeit zur relevanten Kontaktherstellung für diese Beratungssituationen.
- Kritisch wird gesehen, dass die IT-Abteilung einer der Haupttreiber der Transformation ist. Denn es wird befürchtet, dass die **Digitalisierung rein der Technik wegen vorangetrieben** wird und somit die Bedürfnisse am Markt nur unzureichend widerspiegelt.
- Angeregt wird, den Fokus auch auf die Chancen der Digitalisierung zu legen, anstatt vornehmlich auf die Risiken. Dies geschieht unter dem Blickwinkel, dass **risikoscheue Unternehmen bei der Transformation mehr Schwierigkeiten** erfahren und so leichter durch branchenfremde oder ausländische Marktteilnehmer „erobert“ werden.
- Die Auswirkungen der Digitalisierung wären auch für die **Beschäftigten** spürbar und zwar in dem Sinne, dass sich die benötigten Kompetenzen maßgeblich ändern. Die zunehmende Digitalisierung würde sich auch in Form von sukzessivem Personalabbau bemerkbar machen. Von einem Stakeholder wird daher eine weitergehende Beleuchtung dieses Aspekts gewünscht.

In den nächsten drei Jahren wird keine Disruption im Kerngeschäft der beaufsichtigten Unternehmen erwartet. Allerdings ist man davon überzeugt, dass die Veränderungen in den nächsten fünf Jahren näher an einer Disruption als an einer Evolution sein werden.

- Die großen Veränderungen sind bisher ausgeblieben oder wurden von der Finanzindustrie **bereits als state of the art** übernommen. Wahrscheinlich ist deshalb eher die „schleichende“ Veränderung: Lediglich die Art, wie (bestehende) Produkte betrieben und angeboten werden, wird weiter digitalisiert, um diese dem Kunden besser zugänglich zu machen. Die Überführung von bereits vorhandenen Produkten in das digitale Zeitalter wird hier von einigen Stakeholdern als relevante Herausforderung gesehen.

- Eine weitere Herausforderung resultiert aus der **Zunahme von Kooperationen**, die für eine stärkere Vernetzung der Finanzmarktteilnehmer untereinander sowie mit finanzmarktfremden Teilnehmern sorgt. Durch die Zunahme an Kooperationen sieht man die Entstehung von Ökosystemen gegeben. Diese könnten sich insofern **als disruptiv erweisen**, als dass ein etabliertes Ökosystem zahlreiche Kunden anziehen, sie an sich binden und somit den Markt komplett verändern könnte.
- Die Digitalisierung wird zwar durch den Eintritt neuer digitaler Mitbewerber vorangetrieben, auf Grund der kooperativen Ausgestaltung ist aber mit weniger disruptiven Entwicklungen zu rechnen. Ein Stakeholder befürchtet idZ, dass rasche technologische Änderungen für viele Bevölkerungsgruppen **zu rasch und zu wenig partizipativ** erfolgen.
- Mittel- bis langfristig wird eine **disruptive Entwicklung** in den Bereichen Wertpapier-Management, Zahlungsverkehr, Instant-Loan und Embedded Finance antizipiert. Durch ein rasches und agiles regulatorisches Rahmenwerk wird ebenfalls im Bereich der Kryptoassets, deren Bedeutung weiter wachsen wird, eine tiefergreifende Veränderung erwartet.
- Teilweise wird eingeräumt, dass **komplexe Regularien** am österreichischen Finanzmarkt **disruptive Entwicklungen erschweren**.

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

- Im Hinblick auf **regulatorische Hindernisse**, die einer Digitalisierung im Wege stehen, werden folgende Aspekte genannt:
  - die Inhomogenität der Regularien auf EU- sowie nationaler Ebene (hier werden etwa unterschiedliche Rechte, Pflichten und Vorgehensweisen beim Abschluss von verschiedenen Finanzprodukten oder Services angeführt);
  - der Umstand, dass sich viele rechtliche Anforderungen auf veraltete Technologien beziehen (zB Kommunikationsgesetz);
  - uneinheitliche nationale und internationale Schnittstellen;
  - der Trend zum „Know-your-customers-Prinzip“ in der Regulierung wird kritisch eingestuft und sollte nach Ansicht einiger Stakeholder Aufgabe der Behörden sein.
- Als maßgebliche Hürde der Digitalisierung werden auch die **Organisation eines Unternehmens** (hier erscheint ein Experte in der Vorstands-Reihe angebracht) und die **Unternehmenskultur** (hier erscheint es wichtig, dass die Transformation durch ein Change-Management und Kultur-Management begleitet wird) gesehen.
- Als größtes Risiko bzw. Hindernis wird teilweise gesehen, dass **die Trends** der Digitalisierung **nicht (rechtzeitig) erkannt werden**. So werden etwa auch „best practices“, welche sich über Jahrzehnte etabliert haben, als Hindernisse bezeichnet. Wie der Erneuerung in der Vergangenheit begegnet wurde, sollte demnach nicht als Vorlage dienen.
- Auch eine stark fragmentierte und veraltete **IT-Landschaft** und Kern-Infrastruktur wird als Hürde für die Digitalisierung beschrieben. Lösungen und Vorgaben für entsprechende adaptive Schnittstellen und simplifizierte Anbindungsmöglichkeiten (wie API-Schnittstellen) werden gefordert. Auch eine einfache und sichere Erreichbarkeit des Kunden außerhalb des eigenen Applikationsuniversums sollte gegeben sein.
- Das **Kundenverhalten** wird nicht als Hindernis, sondern allenfalls als Herausforderung gesehen. Aus Kundensicht werden aber **Betrugsfälle** thematisiert. Betrugsmethoden würden immer gefinkelter und selbst für sorgfältige Konsumenten immer öfter nicht mehr durchschaubar. Dennoch blieben die Konsequenzen immer wieder an den Kunden hängen (zB unseriöse oder gar betrügerische Investmentplattformen).

Entscheidende Erfolgsfaktoren der Digitalisierung reichen von der laufenden Anpassung der Unternehmensstrategie über das Schaffen einer entsprechenden technologischen Basis bis hin zu ausreichend Know-how in Form von personellen Ressourcen.

- Die erfolgreiche Transformation steht und fällt mit der Einsicht, dass sich die Unternehmenskultur und Organisationsstruktur an das dynamische Marktumfeld anpassen müssen (Vision und die dazugehörige Umsetzung und laufende Anpassung der **Unternehmensstrategie**). Wichtig ist das Verstehen, dass Transformation elementar ist und nicht bloß beiläufig. Einerseits muss das traditionelle Kerngeschäft einer Transformation unterworfen werden, andererseits muss das Geschäftsmodell durch Innovationen weiterentwickelt werden. Dies wird als kritisch angesehen, um die Markstellung zu schützen und ausbauen zu können.
- Wichtig erscheint ebenfalls eine **Fokussierung**, da entscheidende Erfolgsfaktoren oftmals gleichzeitig Engpassfaktoren darstellen. Somit sollten kritische Erfolgsfaktoren jedenfalls erkannt werden, um dann in weiterer Folge bei genau diesen mit der Digitalisierung anzusetzen.
- Aufbauend auf der Strategie sollte auch die entsprechende technologische Basis geschaffen werden. Dazu zählen auch Anpassungen der **IT-Infrastruktur** und die bessere Nutzung von Daten. So können Transaktionen vereinfacht und Beratungsprozesse digitalisiert bzw. mit AI optimiert werden. Die IT sollte sich in diesem Bereich auf Erfolgsfaktoren konzentrieren, anstatt bei Standardleistungen zu verharren.
- Eine laufende Weiterentwicklung und die Integration von guten Ideen (zB durch eine Kooperation mit Techs) wird als hilfreich für eine erfolgreiche Digitalisierung angesehen. Erfolgsentscheidend ist, dass **in den Führungsetagen** ausreichend **Know-how** für die anstehenden Herausforderungen in Form personeller Ressourcen vorhanden ist. In diesem Zusammenhang werden „Generalisten und Visionäre“ sowie die Eingliederung eines „Chief Digital Officer“ in der Vorstandsreihe als wichtige Faktoren bei der Umsetzung erachtet.
- Entsprechend **qualifiziertes Personal** sowie eine laufende Weiterbildung werden überdies als entscheidende Erfolgsfaktoren genannt. Außerdem wird auf die Wichtigkeit der **Einbindung der Beschäftigten** sowie deren Interessenvertretungen hingewiesen.

Es wird erwartet, dass die **neuen digitalen Mitbewerber** die bestehenden Unternehmen zu einer fortlaufenden Weiterentwicklung drängen werden. Die Zunahme der Produkt- und Servicevielfalt wird positiv gesehen, bedacht werden sollten jedoch Bevölkerungsgruppen, für die technologische Änderungen zu rasch erfolgen könnten.

- Die Implikationen des Eintritts neuer digitaler Mitbewerber in den Finanzmarkt werden positiv gesehen, da
  - diese in Form von Kooperationen den bestehenden Teilnehmern helfen, die digitale Transformation zu meistern;
  - dadurch neue Entwicklungen vorangetrieben werden und die Produkt- und Servicevielfalt der Marktteilnehmer zunimmt.
- Negativ wird gesehen, dass rasche technologische Änderungen für viele Bevölkerungsgruppen zu rasch und zu wenig partizipativ erfolgen.
- Neuen Marktteilnehmern mangelt öfters technisches sowie rechtliches Wissen und Erfahrung. Als Markteintrittsbarriere für neue digitale Mitbewerber wird somit auch die **Regulatorik** – welche selbst BigTechs vor größere Herausforderungen stelle – gesehen. Als Konsequenz würden sich neue Mitbewerber **einzelne Geschäftsfelder** suchen, die technisch und regulatorisch einfacher „in den Griff“ zu bekommen sind.

Neue Marktteilnehmer und bestehende Akteure sind nicht nur Konkurrenten, oft ergänzen sie sich gegenseitig durch Kooperationen. Eine deutliche Zunahme solcher Kooperationen wird beobachtet.

- 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.
- Als Kehrseite der kooperativen Beziehungen wird der Umstand genannt, dass allfällige Effizienz-, Preis- bzw. Spesenvorteile nicht bei den Konsumenten ankommen würden.
- Als **Konkurrenten** werden eher industriefremde Unternehmen (insb. „BigTechs“) gesehen, die die Übernahme von Start-ups für einen Markteintritt nutzen. Zu nennen wären hier Unternehmen, die sich auch bereits einen Anteil in der Finanzdienstleistung gesichert haben, zB Alphabet/Google.
- Als **Geschäftsbereiche**, in denen neuen Playern innerhalb der nächsten drei Jahre wesentliche Bedeutung zukommen könnte, werden genannt: Zahlungsdienstleistungen, Instant-Loan, Wertpapiertransaktionen/beratung in bestimmten Segmenten, Debit- und Kreditkartengeschäft, Krypto-Asset Manager, Mikrokredite und cash loans.
  - Kreditinstitute sieht man weniger als Ganzes bedroht, vielmehr seien sie einer Vielzahl kleinerer, spezialisierter neuer Marktteilnehmer ausgesetzt. Gerade kleinere, als Universalbank aufgestellte Kreditinstitute mit einem breiten Leistungsspektrum werden so vor besondere Herausforderungen gestellt.
  - Es werde etwa auch vernachlässigt, dass Versicherungen Wettbewerb im eigenen Haus drohe, da Rückversicherer mitunter die Hauptfinanziers der Start-up-Szene sind und zahlreiche Kooperationen mit FinTechs/InsurTechs unterhalten.

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. In diesem Zusammenhang ist zum einen eine frühzeitige Präzisierung der Regulatorik wichtig, um für notwendige Stabilität zu sorgen. Zum anderen ist es essentiell, dass die FMA sektorübergreifend und agil agiert.

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

- Durch die Aufsicht sollte ein **Level Playing Field** gewährleistet werden. Wichtig sei es dabei,
  - den **Finanzplatz als Ganzes** im Auge zu haben und für alle Marktteilnehmer ein Level Playing Field sicherzustellen,
  - dass die Aufsicht **neue Verflechtungen** in der Risikosicht antizipiert,
  - dass die FMA aktiv die **Harmonisierung innerhalb der EU** begleitet, wobei insbesondere die uneinheitlichen nationalen und internationalen Schnittstellen und „Open Insurance“ aufgegriffen werden sollten, um zu verhindern, dass sich der vorhandene Wildwuchs in Europa fortsetzt,
  - auch beim Bezug und der Nutzung von digitalen Werkzeugen (zB Software, Cloud-Lösungen) europäische Chancengleichheit herzustellen; so ist etwa Datenschutz im Detail unterschiedlich geregelt.
- Hervorgehoben wird die Wichtigkeit der frühzeitigen **Präzisierung der Regulatorik**, um nicht zu viel Entwicklung in undefinierte Richtungen zu treiben. So soll in einem an sich volatilen Umfeld zumindest im regulatorischen Bereich die notwendige Stabilität in Form von konsistenter Auslegung, die über längere Zeit Konstanz aufweist, geschaffen werden.

- Die Transformation im Zuge der Digitalisierung erfordert auch, dass die Aufsichtsbehörden **agiler und iterativ handeln** sollten.
  - Die Aufsicht sollte angesichts des tiefgreifenden Strukturwandels im Bankensektor den **Dialog mit den Sozialpartnern** suchen, gerade was die Entwicklung von nachhaltigen Geschäftsmodellen betrifft. Der kollektive Konsumentenschutz sollte aktiv und umfassend wahrgenommen werden, wobei auch auf umfassende Resilienz der Unternehmen im Hinblick auf die Digitalisierung zu achten wäre.
  - Es würde verbindlicher Regelungen von **Haftungsfragen** in der Mensch-Maschine-Kommunikation bzw. beim Einsatz von Algorithmen zur Entscheidungsfindung bedürfen. Gerade auf diese Abgrenzungsthematik in Haftungsfragen sollte die FMA künftig mehr Augenmerk legen.
  - Eine der zentralen Fragen sollten die Auswirkungen der digitalen Transformation des österreichischen Finanzmarktes auf die **Finanzmarktstabilität** bilden.
- Schließlich ist es wichtig, die eigene Weiterentwicklung bzw. den **Aufbau eigener digitaler Kompetenz** bei der Aufsicht sicherzustellen, um der rasanten Entwicklung folgen zu können, sowie der Struktur und Qualifikation der Beschäftigten eine größere Rolle beizumessen. Im Hinblick auf die zunehmenden Social Engineering Attacken sollte die Bewusstseinsbildung und Sensibilisierung stärker forciert werden.

II. PRODUKTGESTALTUNG

Welche Hindernisse erschweren die Entwicklung von neuen digitalen Finanzprodukten? Teilen Sie die Einschätzung der FMA zu den Chancen und Risiken, die mit den Auswirkungen der Digitalisierung auf das Bank- und Versicherungsgeschäft verbunden sind? 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 aktuell keiner weiteren regulatorischen Vorgaben bedarf. Wichtig ist, dass es zu keiner Ungleichbehandlung kommt, die einem fairen Wettbewerb und fairen Rahmenbedingungen für alle Marktteilnehmer im Wege stehen würde.

- Anstatt einer Ausweitung regulatorischer Vorgaben sollten bestehende Regularien **harmonisiert** und **vereinfacht** werden.
- Problematisch gesehen werden Formerfordernisse, die **digital nicht dargestellt** werden können und verhindern, dass Prozesse in der Kundenbetreuung end-to-end digital durchgeführt werden können, wie etwa
  - eine handschriftliche Unterschrift im Zuge eines Unterschriftenprobenblatts,
  - der Umstand, dass gewisse Angaben eines Kunden nur von diesem selbst und ebenfalls handschriftlich erfolgen müssen (steuerliche Selbstauskünfte), wodurch weiterhin ein Zwang zu physischen Prozessen besteht und solche Prozesse nicht digital abgewickelt werden können.
- Wichtig ist, dass die Regulatorik in allen wesentlichen Bereichen **in nationales Recht** umgesetzt wird, um kleine Änderungen nicht jedes Mal auf Ebene der EBA bestreiten zu müssen.
- Ein weiterer Aspekt ist die **Ungleichbehandlung** zwischen Kreditinstituten und FinTechs. Als konkretes Beispiel wird die PSD 2 RTS angeführt. Durch die PSD 2 wurden Kreditinstitute strikt dazu verpflichtet, die starke Kundenauthentifizierung zum 14.9.2019 umzusetzen. Seitens der Aufsicht wurden unmittelbar danach Prüfungen in den Kreditinstituten bzgl. der korrekten Umsetzung vorgenommen. Hingegen wurden anderen Finanzdienstleistern im eCommerce-, sowie im Kartenbereich, Aufschiebungen und Übergangsfristen gewährt. Dies führte dazu, dass die Kreditinstitute aus Anwendersicht in der Bedienerfreundlichkeit wesentlich ins Hintertreffen gerieten. Es wäre deshalb künftig stärker darauf zu achten, bei gleichartigen Geschäften alle Marktteilnehmer gleich zu regulieren.
- Ein Stakeholder fordert, dass digitale Prozesse und Algorithmen als „Prüfungsmaterie" einen eigenen Platz bekommen.

Hindernisse der Digitalisierung werden nicht nur in der Regulierung, sondern auch in der teilweise fragmentierten und veralteten IT-Landschaft und in der Kundenakzeptanz gesehen:

- Zu den **regulatorischen Hindernissen**, die der Digitalisierung im Wege stehen, zählen bestehende Regularien, die nicht mehr zeitgemäß seien, wie etwa
  - die Vorgaben, wonach auf dem ausgedruckten Unterschriftsprobeblatt die einzelnen Zeichnungsberechtigten ihre Unterschriftsproben im Original zu leisten haben,
  - der Umstand, dass digitale Produkte nicht „nahtlos", „medienbruchfrei" und ohne Verzögerungen abgeschlossen werden können,

- die schwere Umsetzbarkeit der Datenschutzgrundverordnung in der Praxis und der Umstand, dass Datenschutz in Österreich im Vergleich zu den Rahmenbedingungen der europäischen Mitbewerber sehr eng gefasst ist,
- der Zwang, immer striktere Risikovermeidungsansätze zu implementieren, welche die Möglichkeiten für die Entwicklung von neuen digitalen Finanzprodukten einschränken,
- das Fehlen einer regulatorischen Gleichstellung mit großen Anbietern wie Google und Amazon (etwa iZm Geldwäschevorgaben und ZaDiG).

- Die teilweise alte und behäbige Kern- und **IT-Infrastruktur** des gesamten Kapital- und Finanzmarktes wird nach wie vor als Hindernis der Digitalisierung gesehen. Hier braucht es Lösungen und Vorgaben für entsprechende adaptive Schnittstellen und simplifizierte Anbindungsmöglichkeiten (API-Schnittstellen).
- Ein weiteres Hindernis sieht man in der bestehenden Kundenstruktur bzw. **Kundenakzeptanz**, da immer noch eine erhebliche Anzahl von Kunden nach wie vor eine direkte Kundenbetreuung vor Ort wünscht. Gerade durch eine einfache Gestaltung und geringe Komplexität sollen solche Hürden abgebaut werden. Ein standardisiertes, vereinfachtes und rechtssicheres Verfahren zur Legitimation der Kunden könnte hier Abhilfe schaffen.

Als positive Entwicklungen werden insbesondere die steigende Transparenz von Produkten und der bessere Kundenservice wahrgenommen. Aber auch Kostenersparnisse werden vielfach genannt.

- Positiv hervorgehoben werden die **steigende Transparenz und Einfachheit** von Produkten sowie Innovationen, mit denen der Kunde etwa einen **besseren Service** erhält und die „Consumer Convenience“ (Stichwort „rund um die Uhr“) dadurch erhöht wird.
- Der stärkere Einsatz der Digitalisierung ermöglicht auch schnellere Anpassungen des Geschäftsmodells und ein breiteres Angebot.
- Durch Prozessautomation kommt es zur **Kostenersparnis**; auch Auslagerungen, welche durch die intensivere Zusammenarbeit mit Drittanbietern genutzt werden können, begrenzen Kosten. Auch ein neues/größeres Angebot führt zu einem besseren Kostenverhältnis.
- Ein Anstieg an Innovationsgrad und Ideenaustausch ist zu beobachten.

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

- Negativ betrachtet werden Bemühungen, bestehende Produkte **einfach nur „digital“** zu machen. Digitale Transformation sollte anders aussehen. Individuelle Kundenlösungen und die bedarfsorientierte Beratung würden dadurch zurückgedrängt.
- 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 **iZm „beratungslosen“ Angeboten** kritisch zu sehen. Ähnliche Risiken werden auch beim Thema „embedded insurance“ gesehen, sofern hier auf intransparente Art und Weise unnütze oder nicht benötigte Versicherungen oder Finanzprodukte dem Endkunden angediehen werden.
- Als Risiko wird auch der durchschnittliche Verbraucher selbst gesehen, der – im Fall einer mangelnden Finanzbildung – gute Beratung benötigt, welche unterstützt werden sollte.
- Das Erfordernis einer erhöhten IT-Sicherheit bringt **steigende IT-Kosten** mit sich.
- Die Aufspaltung der Wertschöpfungskette birgt Risiken, insbesondere bei einer hohen **Abhängigkeit von externen Dienstleistern**.
- Der persönliche Kontakt zum Kunden und die damit einhergehende Kundenbindung reduzieren sich, wodurch das Unternehmen austauschbar wird.

- Eine Zunahme an (branchenfremden) Marktteilnehmern wird erwartet. Durch die fehlende regulatorische Gleichstellung wird eine Benachteiligung befürchtet.
- Ein Stakeholder thematisiert im Detail die von der FMA angeführten kritischen Aspekte der digitalisierten Finanzprodukte (zB Risiko, dass Scheinkorrelationen hergestellt werden oder Parameter zum Einsatz kommen, die nicht zur Gänze in der Kontrolle der Kunden liegen) und stellt die Frage nach dem realen Mehrwert von technologiegetriebenen Innovationen für den Kunden.

Die Erwartungshaltung an die Rolle der Aufsicht ist durchaus vielschichtig: Während einerseits gefordert wird, dass die Aufsicht die gleichen Aufgaben wie bei „analogen" Finanzprodukten übernimmt, werden andererseits auch Anpassungen begrüßt.

- Die Risiken digitaler Produkte sollten zum einen im Sinne des **Konsumentenschutzes** wahrgenommen, geprüft und allenfalls beanstandet werden. Vor diesem Hintergrund sollte es auch nicht zu einer nahezu vollständigen Digitalisierung der Geschäftsmodelle kommen, ohne die Wünsche und Bedürfnisse vieler Konsumenten zu berücksichtigen. Andernfalls bestünde das Risiko der „Financial Exclusion". Weiterhin und noch verstärkt sollten auch betrügerische Aktivitäten am Markt verfolgt und konsequent unterbunden werden, um Konsumenten einen umfassenden Schutz zu bieten.
- Es sollte aber auch für **Wettbewerbsgleichheit** gesorgt werden, nach dem Grundsatz „Gleiche Tätigkeit, gleiches Risiko, gleiche Regeln". Der Finanzplatz als Ganzes sollte so im Auge behalten werden und in diesem Sinne geeignete Rahmenbedingungen geschaffen werden. Auch **Rechtssicherheit** und ein stabiles Fundament werden als zwingend erforderlich angesehen.
- Gefordert wird ein aufsichtlicher Rahmen im Sinne eines **iterativen und agilen** Ansatzes, der die aktuellen Entwicklungsgeschwindigkeiten des Finanzmarktes hinreichend reflektiert.
- Grundsätzlich wird die **Notwendigkeit für einen Diskurs** gesehen.
  - Der Grundsatz sollte lauten „gleicher Preis, für gleiche Risiken". Insbesondere sei es etwa bei Versicherungen gut möglich, dass neben einem risikogerechten, fairen und bezahlbaren „Basispreis", für diejenigen, die risikobewusster und risikovermeidender leben, ein Discount gerechtfertigt und möglich sein sollte.
  - Ebenfalls wird zu bedenken gegeben, dass kein Erfordernis bestünde, dass der Markt in jedem Fall und immer in der Lage sein muss, alle Risiken abzudecken. Eventuell ist dann auch der Staat gefragt, eventuell bestehende „Super-Risiken" zu tragen bzw. auf das gesamte Kollektiv (Einwohner) zu verteilen.
  - Analog zur Prüfung interner Modelle sollte es auch iZm der Digitalisierung Prüfprozesse geben, um sicherzustellen, 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 Vorreiterrolle der Aufsicht bei einem Diskurs um ethische Grenzen wird teilweise als fragwürdig eingestuft. Hier sind vorrangig Gesellschaft und Politik gefragt. Die Aufsicht sollte notwendige diesbezügliche Diskussionen lediglich anstoßen und moderieren.

III. 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? 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. Es wird dafür plädiert, dass der Beratungs- und Abschlussprozess für alle Beteiligten einfacher und schneller – ohne Medienbruch und Wartezeiten – erfolgen kann. Die Interaktion mit dem Kunden sollte den heutigen technisch möglichen Standards entsprechen dürfen. Bei automatisierten Prozessen müsse aber auch darauf geachtet werden, dass die zugrundeliegenden Parameter transparent, nachvollziehbar und nichtdiskriminierend sind.

- Gewünscht werden **die gleichen Regeln** für online und physische Schnittstellen. Dies inkludiert Informations- und Dokumentationspflichten sowie Pflichten im Bereich der Geldwäscheprävention und iZm der Legitimationsprüfung bei Vertragsabschluss.
- Betont wird hinsichtlich der digitalen Kommunikation auch die Wichtigkeit der **Wahlfreiheit** von Konsumenten bezüglich der Kommunikationsformen. Es wird als positiv erachtet, dass etwa im Versicherungsbereich die elektronische Kommunikation ausdrücklich und mittels einer gesonderten Erklärung vereinbart werden muss. Kunden sollten weder faktisch noch aus Kostengründen Technologien aufgezwungen werden. Zustimmungserfordernisse müssen für Kunden transparent dargestellt werden und dürfen die „Usability" nicht negativ beeinflussen. Vorgeschlagen werden für die Umsetzung der beiden letztgenannten Punkte Mindeststandards und Zustimmungserfordernisse, die auf Umsetzbarkeit ausgerichtet sind.
- Bei automatisierten Prozessen müsse darauf geachtet werden, dass die zugrundeliegenden Parameter **transparent, nachvollziehbar und nichtdiskriminierend** sind. Konkret könnten zB im Robo-Advice verwendete Algorithmen eine „Blackbox" darstellen, für deren Einsatz es Regeln braucht. Genannt werden idZ: Auskunftsrechte, Erläuterungspflicht, Kennzeichnungspflicht, Einsichtnahme und Prüfung durch Experten sowie Regeln und technische Standards.
- Weiters erscheint eine Regulierung von **Vergleichsportalen und Vertriebsplattformen** sinnvoll: Dem Nutzer sollte transparent gemacht werden, in welcher Relation Betreiber und Produktanbieter stehen, welche Gebühren und Provisionen an den Betreiber gehen und zum Beispiel auch nach welchen Kriterien das vorgelegte Ranking erzeugt wurde. Zudem sollte es Vorgaben für den Umgang mit Interessenskonflikten für Vergleichsportale und Vertriebsplattformen geben.
- Neben der Regulatorik, welche als Hindernis die digitale Kommunikation erschweren könnte, wird auch das Fehlen von flächendeckendem **Highspeed-Internet** erwähnt. Es sei schwierig, Kunden über alle Kanäle entsprechend transparent und zeitgerecht hinsichtlich der vorgeschriebenen Aufzeichnungspflichten zu informieren.

Positiv im Hinblick auf den digitalen Vertrieb wird unter anderem die größere Interaktion mit den Kunden gesehen. Auch in Krisensituationen könne so die Kommunikation aufrecht erhalten werden. Auch habe die Akzeptanz digitaler Strukturen deutlich zugenommen.

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

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

- Durch die Digitalisierung wird die Produktlandschaft uneinheitlicher. Daraus ergibt sich ein **erhöhter Beratungsbedarf**. Der Verkauf von Finanzdienstleistungen ohne Beratung könnte einen überhasteten und unüberlegten Kauf zur Folge haben. Skepsis herrscht jedenfalls bei komplexen Angeboten ohne jegliche Beratung. Dies berge das Risiko einer Fehlauswahl.
- Die Forcierung **sozialer Medien** wird ebenfalls kritisch beäugt; sie berge das Risiko einer flüchtigen und nicht nachvollziehbaren Kommunikation. Befürchtet wird ein Netzwerk-Marketing, bei dem das Strukturvertriebsprinzip zu Massenschäden führen könnte, wie die Anlageskandale der Vergangenheit zeigen. Auch deshalb sei eine umfassende, kompetente Beratung durch qualifizierte Mitarbeiter im Finanzbereich essentiell.
- Es wird auch vorgeschlagen, dass beim Einsatz von **Algorithmen** diese der Aufsicht vorgelegt werden sollten, um die Einhaltung von Wohlverhaltensregeln und Diskriminierungsfreiheit evaluieren zu können. Denn Anleger können die Qualität der Robo-Advice-Programme sowie die ihnen zugrundeliegenden Parameter kaum einschätzen und bewerten.
- 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.
- Moniert wird, dass es bezüglich der eID keine klaren Vorgaben gebe und, dass Standards nicht ausreichend vorhanden seien (so etwa bei ich.app versus ID Austria). Außerdem weise die Video-Legitimation technische Schwachstellen und mangelnde Kundenakzeptanz auf. Bank-Ident-Verfahren könnten von Banken nicht verwendet werden. Auch die Foto-ID sei noch nicht freigegeben. Hinsichtlich digitaler Signaturen hält man die Akzeptanz der digitalen Signatur auch beim Grundbuch für dringend notwendig.
- Die Aufsicht sollte auf **einheitliche Wettbewerbsbedingungen in der EU**, zB in Bezug auf die Videoidentifikation, hinwirken. Kritisch beäugt wird auch das noch fehlende Level Playing Field etwa im Hinblick auf die Offenlegungspflichten der Onlinebanken.
- 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. In Bezug auf das Ranking wird auch dargelegt, dass die Unabhängigkeit bei digitalen Vertriebsplattformen nicht gewährleistet sei. Zudem sollte es Vorgaben für den Umgang mit Interessenskonflikten für Vergleichsportale und Vertriebsplattformen geben.

IV. 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 Kostensenkungspotential und in Effizienzgewinnen sowie in der Reduktion von operationellen Risiken gesehen. Die damit einhergehende Automatisierung sei parallel dazu jedoch mit diversen **Nachteilen** verbunden: Die Möglichkeit für ein manuelles Eingreifen müsse gewahrt bleiben. Zudem wäre es gefährlich, wenn ein Anbieter mit einem signifikanten Marktanteil aufgrund eines automatischen Triggers Kapitalanlagen transferieren und den Markt dadurch beeinflussen könnte. Negativ wird weiters von manchen Stakeholdern der Anlagetrend in Richtung Kryptoanlageformen gesehen.

Als Hindernis für die Automatisierung werden fehlendes Know-how und die vorherrschende Datenlandschaft identifiziert.

- **Positiv** wird erachtet, dass es bereits viele Produktlösungen (zB Robo Advisor) gibt, welche vollautomatisiert Anlageentscheidungen treffen können.
  - Als nützlich erweist sich, dass komplexe Beratungsprozesse und damit einhergehende regulatorische Anforderungen einfach und schnell abgearbeitet werden können. Die Digitalisierung hilft überdies gegen manuelle Datenmanipulation als Hauptfehlerquelle.
  - Auch KI-Systeme für einen zielgerichteteren Research und die Entwicklung der Blockchain-Technologie werden positiv wahrgenommen.
  - Wenngleich automatisierte Prozesse von Vorteil seien, müsse auch ein manuelles Eingreifen möglich sein. Ein Stakeholder weist diesbezüglich auf den Einsatz von Machine Learning in einem konkreten Anwendungsfall hin: Dabei werden grundlegende Marktallokationen errechnet, sodass Allokationsentscheidungen nicht durch traditionelle fundamentale Analyse, sondern durch quantitative Analyse unter Nutzung von Machine Learning unterstützt werden. Die Umsetzung in konkrete Transaktionsentscheidungen obliegt jedoch ausdrücklich weiterhin dem zuständigen Fondsmanager.
- Als **Hindernis**, um die Asset-Management-Prozesse zu automatisieren, wird gesehen:
  - das fehlende Know-how in den einzelnen Unternehmen und das Fehlen einer standardisierten Aus- und Weiterbildung im Bankensektor,
  - die vorherrschende Datenlandschaft (so sind die Daten in vielen verschiedenen Systemen und oft nicht „bereinigt“ und „konsolidiert“; eine breite Datenbasis und Historie sind aber für die Techniken des Data Science essentiell; zudem gibt es keine rechtlichen Leitfäden für den Zugang und die Verarbeitung von Daten).

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

- So wird angeregt, die **automatische** und oft risikobasierte **Vermögensverwaltung** („Robo Advisory“ oder „WealthTech“) separat und explizit in die Digitalisierungsstudie aufzunehmen. Begründet wird dies damit, dass es europaweit bereits über 100 Anbieter, einige davon mit einem verwalteten Vermögen von mehr als 1 Mrd. EUR, gibt. Obwohl dies einerseits im Nützlichen mit Kosteneffizienz und Bequemlichkeit einhergeht, kann dies auf der anderen Seite dann gefährlich sein, wenn ein Anbieter einen signifikanten Marktanteil bekommt und er aufgrund eines automatischen Triggers in der Fläche Kapitalanlagen (ETFs, Aktien) in einem großen Stil transferiert und damit den Markt stark beeinflusst.

- Es wird auch die Meinung vertreten, dass die Aufsicht die Rolle als **Prüfungsinstanz** der digitalen und automatisierten Prozesse (zB RPA), vor allem in den Mid- und Back Office Abteilungen wahrnehmen sollte.
  - Auch eine Regulatorik im Umgang mit automatisierten Orderprozessen wird als notwendig erachtet.
  - Ein institutioneller Rahmen für die übergeordnete Steuerung und Überwachung Künstlicher Intelligenz in Österreich soll das Einhalten von Regeln, Maßnahmen und die Verteilung von Kompetenzen kontrollieren (KI Governance).
  - Regulatorische Vorgaben sollte es im Bereich der Kontrolle und Überwachung von **Datenanbietern**, wenn diese unter die Aufsicht der FMA fallen, geben.
- Zusätzlich soll die Aufsicht ad-hoc **Informationsgeber** zu aktuellen Entwicklungen sowie **Sparringpartner** für nationalen Austausch zum Thema Digitalisierung sein.
- Eine Förderung von **Aus- und Weiterbildung** im Bereich Digitalisierung, da User IT-Verständnis im Umgang mit alternativen Techniken brauchen, wird gewünscht.

V. 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? Welche konkreten positiven, aber auch negativen Entwicklungen bezüglich der IT-Systeme sind in den einzelnen Sektoren zu beobachten?

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 ist, dass durch eine breite Nutzung das Niveau der IT-Sicherheit in der Anwendung und damit auch bei den Nutzern gehoben werden könne. Zusätzlich kommt es zu einer **Kostenreduktion** und einer **Vereinfachung der Zusammenarbeit**. Außerdem könnte in den Zentren mehr Personal und Geld in die IT-Sicherheit fließen, als dies bei einer verteilten Struktur in kleinere Einheiten möglich wäre.
- Nachteilig ist, dass die zentralen Systeme oder Provider ein ungleich attraktiveres Ziel für potentielle Angreifer darstellen und somit die Wahrscheinlichkeit eines Angriffs steigt. Sollte es zu einer Kompromittierung und zu Ausfällen kommen, wären Auswirkung auf eine große Anzahl von Kunden und somit uU auch **weitreichende systemische Auswirkungen** auf Unternehmen im Finanzsektor die Folge. Sind mehrere Finanzdienstleister betroffen, ist die Koordination einer einheitlichen Reaktion komplex und schwierig. Ebenfalls nachteilig wird die reduzierte Möglichkeit der Steuerung der großen Dienstleister gesehen.

Bezüglich der **IT-Systeme** ist neben positiven Entwicklungen auch ein Anstieg von Cyber-Risiken und Konzentrationsrisiken zu beobachten. Die Finanzmarktteilnehmer sollten sich diesen bewusst sein.

- Der **Trend zu agiler Entwicklung** nimmt stark zu. Der Einsatz von agilen Methoden bringt neben vielen Erleichterungen aber auch einige Risiken. Zusätzlich wird dies durch Cloud-Services und der damit einhergehenden Vernetzung von Anwendungen verstärkt. Als Folge daraus steigt das Risiko für die Gesamtfunktionalität. In vielen Bereichen ist allerdings der Einsatz agiler Methoden nur eingeschränkt möglich. Durch die stärkere Verbreitung von Open-Banking Plattformen können vermehrt agile Methoden zum Einsatz kommen und somit ihre Vorteile und Stärken ausspielen.
- **Cyber-Risiken** steigen an. Getroffenen Maßnahmen in den Unternehmen sollten daher überprüft und angepasst werden.
- Die Fokussierung auf wenige große Anbieter führt zu **Konzentrationsrisiken**, die häufig nicht als solche erkannt und damit auch nicht entsprechend behandelt werden. Große Anbieter bieten mitunter volle Funktion ihrer Produkte nur an, wenn sie in ihrer Cloud betrieben werden. Damit verbunden seien meist Zugeständnisse in der technischen Umsetzung der Netzwerkanbindung und wenig Bereitschaft für Sonderwünsche.
- Es erfolgt die schrittweise **Modernisierung der IT-Systeme** hin zu Open-Banking Plattformen; die Ablöse von bestehenden Systemen wird teilweise verzögert. Auf Grund der Komplexität und Größe der bestehenden Systeme verursacht dies enorme Kosten und dauert einige Jahre. Somit kommt es zu einem sich aufbauenden Investitionsstau.

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

- Die Konformität von IT-Systemen mit der österreichischen Gesetzeslage sollte von der Aufsicht **zertifiziert** werden. So sollte eine Analyse und Bewertung von IT-Systemen hinsichtlich der Eignung zum Einsatz am Finanzmarkt sowie eine Listung von IT-Systemen, die für den Einsatz am Finanzmarkt geeignet sind, erfolgen. Jene Aspekte, die für die Bewertung der IT-Systeme herangezogen werden (Verschlüsselung, Protokollierung, IT-Security, Userverwaltung, Historisierung, …), sollten in regulatorischen Vorgaben enthalten sein. Somit sollte eine zunehmend detailliertere Prüfung der IT-Systeme/Prozesse stattfinden.
- Eine **Sensibilisierung** von Unternehmen wird auch in Bezug auf die Revisionssicherheit der Systeme als wichtig empfunden. Von der Aufsicht sollte dies theoretisch (Prüfung der Dokumentation) sowie praktisch (Vorortprüfung) überwacht werden. Insbesondere Banken sollten die Risiken weltweiter Wertschöpfungsketten bewusstgemacht werden.
- Hervorgehoben wird auch das Thema **Business Continuity Management** (BCM). Diesbezüglich wünscht man sich von der Aufsicht Mindestanforderungen an das BCM.
- IT-Systeme werden mittlerweile weitgehend redundant ausgelegt – beim **Personal**, das diese Systeme bedienen soll, ist dies auf Grund des Kostendrucks und der beschränkten Verfügbarkeit von kompetenten Mitarbeitern nicht der Fall. Daher wird gewünscht, diesbezüglich Awareness bei Ministerien für entsprechende Initiativen zu schaffen.
- Konkrete regulatorische Vorgaben in Form von **Vorgaben zur Mindestausstattung von IT-Abteilungen** seien begrüßenswert. Außerdem wünscht man sich im Bereich Konzentrationsrisiken durch große IT-Dienstleister eine europaweite Regulierung/Limitation.

VI. IT-VERFLECHTUNGEN

Welche Aufgaben soll die FMA iZm den Verflechtungen zwischen den beaufsichtigten Unternehmen und den IT-Dienstleistern wahrnehmen? In welcher Form sollen diese Aufgaben übernommen werden? Welche konkreten regulatorischen Vorgaben sind iZm den Verflechtungen am österreichischen Finanzmarkt notwendig? Welche positiven und negativen Entwicklungen bezüglich der Vernetzung mit IT-Dienstleistern sind in den einzelnen Sektoren zu beobachten?

Die in der Digitalisierungsstudie genannten Aspekte ergänzen die Stakeholder um folgenden Input:

In Bezug auf die steigende Vernetzung mit IT-Dienstleistern wird es als wichtig erachtet, dass die FMA den Überblick über die Vernetzungen behält und bei Konzentrationen von kritischen Dienstleistungen die kritischen Dienstleister hinsichtlich ihrer Business Continuity überwacht werden.

- **Positiv** werden folgende Entwicklungen gesehen:
  - Der Umstand, dass IT-Dienstleister aus einem gemeinsamen Sektor kommen, wird positiv gesehen, da dann der Vorteil besteht, dass Sicherheitsrichtlinien in einer abgestimmten Form eingefordert und umgesetzt werden können.
  - Ebenfalls positiv sei der aktive Informationsaustausch.
  - Auch die verstärkte Nutzung von innovativer Standardsoftware vom Markt anstelle von Eigenentwicklungen und Auslagerungen von „Standarddienstleistungen“ sei vorteilhaft.
- Hingegen **negativ** werden das steigende Risiko (zB Cyber-Fraud) sowie der steigende Aufwand zur Erfüllung der regulatorischen Anforderungen eingestuft.
- Ein Stakeholder merkt an, dass noch nicht klar sei, ob eine homogene Landschaft und eine Marktkonzentration bei IT-Systemen das Ziel von einheitlichen Schnittstellen eher leichter oder schwerer machen.

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

- Eine **Aktualisierung der Dienstleisterliste** im Hinblick auf einen Überblick über wichtige Dienstleister und Subdienstleister wird angeregt.
- Die FMA sollte überdies eine **Koordination von gepoolten Audits** bzw. Prüfungen der Dienstleister durch beaufsichtigte Unternehmen übernehmen. IdZ ist auch die Akzeptanz von Ergebnissen von Pool-Audits zumindest als Basis für die von den Beaufsichtigten dann noch individuell durchzuführende Prüfung essentiell.
- Die FMA sollte außerdem durch die von den Beaufsichtigten gemeldeten Aus- und Weiterverlagerungen den **Überblick über die Vernetzung** behalten. Bei Konzentrationen von kritischen Dienstleistungen für den Finanzmarkt sollten diese Dienstleister hinsichtlich ihrer Business Continuity überwacht werden.
- Neben der Wichtigkeit, Verflechtungen im Gesamtblick zu haben, wird auch die Vereinheitlichung von Zertifizierungen als Aufgabe, welche die Aufsicht wahrnehmen sollte, genannt. Im Zusammenhang mit regulatorischen Vorgaben wünscht man sich hierbei die Schaffung von Transparenz im Hinblick auf die Verflechtungen und Abhängigkeiten sowie die Verhinderung von Monopolen. Auch wird angemerkt, dass durch die Ausbreitung von Ökosystemen die Zunahme der Verflechtungen von IT-Systemen auch branchenübergreifend sein wird. Somit wird auch die Frage nach einer **branchenübergreifenden** (IT) **Regulierung** und Aufsicht gestellt.
- Die aktuellen regulatorischen Vorgaben werden als weitgehend ausreichend betrachtet. Eine **Präzisierung** der Vorgaben für den Umgang mit weit verbreiteten Dienstleistern (zB MS 365, AWS, Azure sowie den Datenleitungslieferanten A1, Drei) wird als wünschenswert erachtet.

VII. DIGITALE TECHNOLOGIEN

Sollen entsprechend Ihren Erfahrungen bzw. Ihrer Einschätzung 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 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 Finanzmarkts?

Die am Call for Input teilnehmenden Stakeholder bekräftigen im Wesentlichen die Schlussfolgerungen der FMA hinsichtlich der neuen digitalen Technologien und ergänzen diese um folgende Einschätzungen:

Die Einschätzung bezüglich der **Chancen** und **Risiken** der einzelnen Technologien wird großteils geteilt und um ein paar Anmerkungen ergänzt.

Weitere wesentliche Risiken bestehen im Druck der globalen Player auf den Finanzmarkt und in möglichen Konzentrationen bei einzelnen Clouddienstleistern.

- Großes Potential wird in der besseren Nutzung der eigenen Daten mit **Big Data** gesehen. Die Datenqualität muss in vielen Bereichen bis auf Einzeldatensatzebene regulatorischen Anforderungen genügen. In Big Data sollte daher kein statistisch signifikantes Datenqualitäts-Problem auftreten.
- **Robotics** sei nach Ansicht einiger Stakeholder nicht langfristig für die Prozessautomatisierung geeignet.
  - Eine Verwendung sollte nur dann erfolgen, wenn keine Service-Schnittstellen möglich sind, womit Robotics nur als Zwischenschritt zu einer Service-Integration gesehen werden sollte. Stattdessen wären serviceorientierte Integrationen über Unternehmensgrenzen hinaus anzustreben.
  - Mit Robotics können auch APIs von Applikationen angesprochen werden, um auf Daten zuzugreifen. Dies hilft in der Komplexität der Zugriffe.
- Bei **Machine Learning** könnte noch die Subkategorie Decision Intelligence hervorgehoben werden. Es wird auch darauf hingewiesen, dass Machine Learning und die Problematik des Black-Box-Effekts zu Erklärungsproblemen bzw. falschem Bias führen können.
- **Open source-Software** sei sicherer als dedizierte Software und sollte dementsprechend auch behandelt und verwendet werden (dürfen).
- Ein Stakeholder sieht verstärkte Einsatzmöglichkeiten neuer Technologien insbesondere im Bereich der Compliance (Stichwort „know your transaction“).
- Angemerkt wird auch, dass die in der Digitalisierungsstudie von der FMA erwähnten „ethisch problematischen Schlussfolgerungen“ ausführlicher behandelt werden könnten, da diese vermutlich in der Breite bei den Marktteilnehmern noch nicht präsent sind.
- Als wesentliches Risiko wird auch das inhärente **technische Risiko** (Prozesse ohne Zwischenschaltung/Überprüfung eines Menschen) ergänzt.
- Als weiteres wesentliches Risiko wird der **Druck der globalen Player** auf den Finanzmarkt (gemeint sind globale Technologiekonzerne wie etwa Google, Apple, Amazon) beschrieben: Wenn deren Dienste ausgeweitet werden, bestünde die Gefahr, dass die Geschäftsfelder der Banken beschnitten würden.
- Als zusätzliches Risiko werden mögliche **Konzentrationen** bei einzelnen Cloud-Dienstleistern, die das Klumpenrisiko erhöhen, genannt.

Rechtsunsicherheiten in Verbindung mit neuen digitalen Technologien beziehen sich vor allem auf Cloud-Dienste und Outsourcing.

Die **Erwartungshaltung an die Aufsicht** richtet sich auch in dieser Hinsicht primär an die Harmonisierung regulatorischer Rahmenbedingungen.

- Es sollten **gleiche regulatorische Bedingungen** für alle Marktteilnehmer (Banken, FinTechs, BigTechs) herrschen. Derzeit seien vor allem Banken einer sehr starken Regulatorik ausgesetzt, wohingegen BigTechs kaum erfasst seien. Die Erwartungshaltung an die Aufsichtsbehörden ist zudem, dass die Aufsicht grundsätzlich im Hinblick auf die wesentlichen Regulierungsziele **technologieneutral** agiert, jedoch die Besonderheiten der jeweiligen Dienstleistung (und Art der Dienstleistungserbringung) berücksichtigt.
- Der **Einsatz von Cloud-Diensten** sei mit einer Abgabe der vollständigen Kontrolle über Daten verbunden. Große Anbieter würden die rechtlichen Vereinbarungen ohne eine Möglichkeit von Anpassungen vorgeben. Damit seien regulatorisch (Outsourcing) bereits heute extrem hohe Aufwände verbunden. Parallel dazu seien Bedingungen, die sich aus der DSGVO und dem problematischen Amerikabezug (Schrems-Urteil) ergeben, zusätzliche große Hürden. Mehr Klarheit zu diesen Aspekten ist gefragt.
- Rechtsunsicherheit sieht man auch in den Bereichen **Machine Learning** und **Big Data**: Hier besteht das Risiko, dass es zu diskriminierenden Prozessen kommt. Digitalisierung wird nur dann einen Mehrwert kreieren können, wenn sie diskriminierungsfrei gestaltet und reguliert wird.
- Ebenfalls sei mehr Klarheit bezüglich der **Verwendung von Kryptotechnologien** wünschenswert. Die Aufsicht sollte für die Sicherstellung eines rechtlichen Rahmens für digitale Währungen sorgen.
- Häufige **Änderungen in der Produktgestaltung**, der Art der Kommunikation und Laufzeit (zB digitale Produkte mit „on“- und „off“-Modus) machen viele vertragliche bzw. zivilrechtliche Änderungen notwendig. Zudem bestünde das Risiko, dass Haftungsrisiken zum Nachteil der Konsumenten gestaltet werden.
- Hervorgehoben wird, dass die Aufsicht mit ausreichend Ressourcen ausgestattet sein sollte, um eine aktive Rolle bei der digitalen Transformation des österreichischen Finanzmarktes einnehmen zu können.

VIII. CYBER RISIKEN

Mit welchen Maßnahmen bzw. Initiativen könnte die FMA zur Erhöhung der Cybersicherheit am Finanzmarkt konkret beitragen? Welche Cyber-Bedrohungsszenarien könnten in Zukunft für den österreichischen Finanzmarkt besonders relevant 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? 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 Cyberrisiken und ergänzten diese um folgende Einschätzungen:

Als für den österreichischen Finanzmarkt besonders relevante **Cyber-Bedrohungsszenarien** werden etwa Hacking-Angriffe auf sensible Daten identifiziert. Zu weiteren Bedrohungen zählen Cyberbetrug, Angriffe auf elektronische Zahlungssysteme, Angriffe via Supply-Chain, Angriffe auf Lieferketten, Angriffe auf Endverbraucher, staatlich motivierte Angriffe, „künstliche Intelligenz“ gestützte Angriffe, Folgeangriffe im Zuge eines Blackouts, Angriffe im Bereich Brute-Force sowie offene, noch nicht bekannte Schwachstellen (analog Log4J).

Auch Cyber-Angriffe über **Social Engineering** werden häufiger beobachtet: Bei Privatkunden kann ein hoher Anstieg der Betrugsfälle (Anlagebetrug, Kauf-/Verkaufsbetrug, Identitätsdiebstahl, Phishing, Debitkartenbetrug, Diebstahl von Digital Wallets, Kreditbetrug, Bedrohungen und Nötigung sowie Call-Bots) beobachtet werden. Dabei müssen technische Sicherheitsmaßnahmen von den Hackern nicht umgangen werden, da der Finanzdienstleistungskunde selbst instrumentalisiert wird.

- Allgemein lässt sich festhalten, dass das erforderliche Skillset für Cyberangriffe sinkt und die **Qualität der Angriffe steigt**. Eine bessere Sprache und gut nachgebaute Fake-Seiten vermitteln eine verführerische Korrektheit. Gleichzeitig steigt die für Einzelne nicht mehr erfassbare Komplexität in der Digitalisierung. Die Bedrohung steige dabei mit Art und Umfang der verarbeiteten Daten sowie Transaktionen und den möglichen Auswirkungen. Je breiter die Finanzdienstleistung aufgestellt sei, desto größer sei die Bedrohungslage. Bankinstitute mit ihren Onlineangeboten und der Möglichkeit, auf kurzem Weg Zahlungen anzustoßen, stünden naheliegend speziell für Phishing-Attacken im Fokus.
- Zur Verbesserung der IT-Sicherheit sollte der Bereich **User-Awareness prioritär verstärkt** werden. Neben allen technischen Maßnahmen bzgl. Internetsicherheit ist die Schulung der Mitarbeiter in Bezug auf Awareness ein wichtiger Faktor. Weiters sollte größere Priorität auf tatsächliche Cyber-Resilienz im Zusammenspiel sämtlicher Unternehmensabteilungen gesetzt werden. IT-Sicherheit hängt nicht ausschließlich von technischen Parametern ab. Cyber-Angriffe erfordern vielmehr auch ein reibungsloses Zusammenspiel von technischen Abteilungen, Unternehmenskommunikation und Rechtsabteilung.
- Zusätzlich sollte **Informationssicherheit** bei IT-Beschaffungen verstärkt berücksichtigt werden. Auch die Etablierung von Systemen zur raschen Reaktion und Prävention (zB SIEM-SOC) wird genannt.
- Von den Unternehmen sollten jedenfalls **weitere Maßnahmen zur künftigen Abwehr** von Cyber-Attacken gesetzt werden.
  - Neben diversen Übungen und technischen Prüfungen sollten Überlegungen darüber angestellt werden, ob im Ernstfall die notwendigen quantitativen und qualitativen Ressourcen sowie trainierte Prozesse zur Verfügung stehen. Aktivitäten zur Prüfung und Verbesserung technischer und organisatorischer Sicherheitsmaßnahmen hinsichtlich Umfang, Aktualität und Wirksamkeit sollten verstärkt werden.
  - Wichtig sei zudem, das Level der eigenen Sicherheit auch bei den Dienstleistern und Subdienstleistern einzufordern, damit keine Sicherheitslöcher entstehen.

Hinsichtlich der **Erwartungshaltung an die Aufsicht** wurden im Bereich der Cyberrisiken folgende Anregungen formuliert:

- Seitens der FMA sollte ein **Informations- und Erfahrungsaustausch** – im Speziellen zu DORA – angedacht werden. Initiativen dahingehend, ob in der **Bildung und Weiterbildung** Grundkompetenzen gefordert werden sollten, könnten überlegt werden. Bei Auslagerungen und Kooperationen besteht die Problematik, dass Dienstleistungsanbieter sich immer noch an den hohen Sicherheitsanforderungen stoßen.
- Dennoch seien die vorhandenen regulatorischen Vorgaben großteils ausreichend. Mit ihnen sollte **durch genauere Messbarkeit des Reifegrades bessere Transparenz** für die Leitungsorgane geschaffen werden. Eine Gesamtreifedarstellung dürfe keine generellen Schwächen in manchen kritischen Bereichen verdecken.
- Für einheitliche Transparenz und Verbesserung der Cyber-Sicherheit könnte die FMA eine Art „**FMA FinCoop Ready**“-Zertifizierung bzw. Selbstzertifizierung anhand der bekannten gesetzlichen und regulatorischen Vorgaben der Finanzdienstleister initiieren.
- Prüfungen sollten mit konkreten Schwerpunkten in Bezug zur aktuellen Bedrohungslage stattfinden, die auch **aktive Angriffssimulationen** enthalten.
- Die Etablierung des mehrfach angedachten **Finanz-CERTs** wird gewünscht.
- Im Hinblick auf die Schwierigkeit der Überprüfung von Cyber-Sicherheitsmaßnahmen wird vorgeschlagen, zumindest **allgemeine Grundsätze ordnungsgemäßer Datenverarbeitung** vorzuschreiben und dann im Einzelfall zu kontrollieren, ob und wie diese eingehalten werden.
- Ein Stakeholder merkt an, dass dieses Thema nur gemeinschaftlich mit anderen betroffenen Bereichen und am besten auch übergeordnet in der EU geregelt werden sollte.

ABKÜRZUNGSVERZEICHNIS

AI	Artificial Intelligence
API	Application Programming Interface
BCM	Business Continuity Management
bzgl.	bezüglich
bzw.	beziehungsweise
DORA	Digital Operational Resilience Act
DSGVO	Datenschutz-Grundverordnung
EBA	European Banking Authority
etc.	et cetera
ETF	Exchange Traded Fund
EU	Europäische Union
idR	in der Regel
idZ	in diesem Zusammenhang
insb.	insbesondere
iZm	in Zusammenhang mit
KI	Künstliche Intelligenz
PSD	Payment Service Directive
RPA	Robotic Process Automation
RTS	Regulatory Technical Standards
SIEM	Security Information and Event Management
SOC	Security Operations Center
uU	unter Umständen
va	vor allem
ZaDiG	Zahlungsdienstegesetz
zB	zum Beispiel