ÖSTERREICHISCHE FMA·FINANZMARKTAUFSICHT

Digitalisation in the Austrian Financial Market

Call for Input: Results

January 2020

TABLE OF CONTENTS

Masculine forms are used throughout this document for ease of readability. Such designations should be considered as being gender-neutral. It should in particular be noted that all formulations relating to persons apply equally to women and men.

INTRODUCTION

The FMA's Analysis on Digitalisation in the Austrian Financial Market

Digitalisation is changing the framework of the financial market more quickly and radically than has been the case in decades. From the outset, the FMA has been interested in this transformation process for obtaining current findings about the associated opportunities, trends and threats. In so doing we strictly observe the principle of technology neutrality: the FMA does not supervise any technologies, but primarily focuses on risks. Equal risks require equally high supervisory requirements, irrespective of whether they arise from digital or analogue business models or processes.

In July 2019 we presented intermediate results from our analysis about digitalisation in the Austrian Financial Market. These findings are based on a study launched at the beginning of 2019, and which is based on, among other things, a comprehensive survey of supervised entities. Thanks to the almost full market coverage and the high level of involvement of supervised entities that responded, it was possible to create the most comprehensive and simultaneously most detailed basis in terms of data and information about the topic of digitalisation in the Austrian financial market. This forms a solid basis for the FMA in staying on the ball in relation to digitalisation and to correctly appraise the drivers, trends and potential future developments.

Results of the Call for Input

In order to initiate broader discussion and to intensify the dialogue in the Austrian financial market regarding the implications of digitalisation, the FMA additionally invited stakeholders – investors, savers, insurance policyholders and consumers, public institutions – as well as the interest public to critically scrutinise the findings and conclusions contained in the Report on Digitalisation in the Austrian Financial Market and to add their own perspectives, experiences and approaches for finding solutions.

Eleven stakeholders responded to this Call for Input and submitted statements, in some cases of a very comprehensive nature, in response to the questions that the FMA had formulated as guidance at the end of every chapter in the report.

Generally the conclusions reached by the FMA on the implications of digitalisation were also shared and supported by the participating stakeholders. Some statements also contain supplementary remarks and cite further practical examples (e.g. the increasingly practical significance of aggregators, messengers etc.). Several stakeholders raise remarks of a socio-political nature and *de lege ferenda* suggestions (from the perspective of a participant, care needs to be taken that services are not ultimately transformed towards solely digitalised services due to the risk of exclusion; in this regard the [mandatory] maintaining of at least a minimum level of analogue infrastructure should be considered).

The FMA would like to express its thanks for the comprehensive opinions received and will take this valuable input into account in its agendas as well as for the prioritisation of its supervisory activities accordingly.

I. STRATEGIES

What are the decisive opportunities and threats from digitalisation for the Austrian financial market? What are the success factors for being able to exploit digital transformation optimally for the further development of business models in the individual sectors within the financial market? What is the expectation regarding the role of the supervisor? These were a few of the questions that the FMA asked in its Call for Input.

The participating stakeholders in the Call for Input by and large echoed the FMA's conclusions about the implications of digitalisation, while also adding the following views:

The effects of digitalisation on the financial market are overall considered to be positive. Digitalisation supports financial market participants in understanding customers better, and also tailoring business model as well as products to the needs of their customers.

- **Market shares will change completely** as a result of digital transformation. New competitors and new business models will force existing sectors to embrace **innovation and agility.** The processing of data will become ever more significant; with **new role profiles** being sought– banks will be considered as "data-driven entities".
- With regard to increasing levels of cooperation, digitalisation will ensure an **increasing networking** of financial market participants as well as non-financial market participants.
- Digitalisation will have a particularly strong influence on **less advice-intensive products and services**: in particular in the field of payments, it is assumed that digitalisation will dramatically change current processes. Digitalisatio is becoming increasingly prominent in lending business involving smaller amounts, general asset management as well as tailored insurance products.
- In general, changes arising as a result of digitalisation are to be expected considerably earlier in relation to **retail business** than for wholesale business.

For the foreseeable future (within the next three years) no disruption is expected in the core business of supervised entities. However, a belief exists that current business models will need to be adapted in the long term and that the changes over the next five to ten years will be closer to disruption than to evolution.

- According to one stakeholder, disruption is already conceivable before then. It **often lies in the hands of the regulator** and the supervisor whether development occurs in an evolutionary or disruptive manner.
- To a certain extent, it is conceded that **complex regulations** in the Austrian market **impede disruptive developments**. However, disruptive developments remain plausible in the following areas:
  - in areas where there are a large number of repetitive steps in a procedure
  - in areas where digitalisation makes enormous leaps in quality in terms of convenience for customers
  - certain business areas may taper off in the next few years due to the emergence of new market participants.
  - A disruption as a consequence of digitalisation could be a potential future scenario in light of the introduction of the private currency Libra and an associated global payment network.

Impediments to digitalisation are not only observed in connection with regulation, but also with regard to the corporate culture and the IT landscape.

- One the one hand, “over-regulation” in general, and on the other hand certain specific regulations (e.g. Article 37a BWG and Article 3 para. 2 no. 2 SVG) are perceived as **regulatory impediments**, which hamper digitalisation. It is suggested that the Regulatory Sandbox is also used for scrutinising/demonstrating impediments to digitalisation.

  Specific need for action is seen as existing in the following areas:

  - Regulation (banking secrecy, data protection, the Telecommunications Act (TKG), the Financial Markets Anti-Money-Laundering Act (FM-GwG) etc.) should be designed in such a way that **purely digital business processing** is enabled without requiring the physical presence of the customer. Especially in relation to the prevention and combating of fraud, a corresponding degree of cross-linking in communication with the authorities as well as between the financial institutions is desired, in order to ensure a rapid reconciliation or exchange – subject to the observance of regulations under data protection law (e.g. with regard to the checking of identification documents).
  - In a first step formal requirements should be set out in the respective material legal acts in the same manner as in Article 1b of the Insurance Policy Act (VersVG; Versicherungsvertragsgesetz) that **differentiate between declarations in written form and the necessity to use the written form**. “In written form” (*in Schriftform*) means that the declaration must be signed by hand. A contractual declaration that is e.g. sent by e-mail does not therefore meet the requirements of being drawn up in written form. In contrast, where “the written form” (*Erfordernis der geschriebenen Form*) is necessary, a physical signature or qualified electronic signature is not required. The legal declaration must in this case merely consist of a text made in characters, from which the person making the declaration is also apparent. Legal declarations may in this case also be submitted for example by e-mail or SMS (WhatsApp) in a legally effective manner.
  - Extension of applicability of electronic identities and proof of identity/legitimate forms of ID: an option for identity verification by digital means using digital certificates (qualified certificates) would provide several advantages, e.g. in the areas of authentication for AML purposes, declarations of creditworthiness. Doing so could permit a **digital identity** to not just be used in the form of a digital signature towards authorities, but also **in the form of a qualified certificate** between private legal and natural persons.
  - Use of **signature pads** (U-Pads / Unterschriften-Pads) for observing legal formal requirements in releasing elderly customers from banking secrecy requirements; exemption from banking secrecy requirements is already possible in accordance with Article 38 para. 6 BWG by means of strong customer authentication, but elderly bank customers often do not often make use of this option.
  - The regulation about the **nature and manner for electronic submission of applications for repayment of savings and loan premiums** (*Bausparprämien*) stipulated in the BSpkV (Bausparkassengesetzverordnung) should be amended to reflect the current state of digitalisation.
  - Comprehensive **recordings of telephone conversations** pursuant to Article 33 WAG 2018
  - Video-based advice ought also to be considered as **on-site presence** as defined in Article 52 WAG 2018.

- In relation to **using personalised websites as “durable media”** it was remarked that in accordance with the case law of the CJEU a website only fulfils this requirement, if every possibility for the unilateral modification of the content of the website is excluded for the payment service provider or for an administrator assigned with the task of administering the website. It is considered doubtful whether these requirements are currently met in practice. According to the case law of the Austrian Supreme Court (OGH), the mere possibility of being

able to store items via a website including a mailbox does not lead to a durable medium being considered to exist.

- The **organisational structure of a company** with all its "ivory towers" and "allotments" is also seen as a material obstacle for digitalisation. Similarly the general "mindset", especially that of the directors of established entities in the Austrian financial market is viewed similarly (tending to be cautious, having a negative general disposition towards change over the course of time and the market as well as towards digitalisation in general).
- Some consider the largest risk or obstacle to be that **trends** in relation to digitalisation **are not recognised (in time)**.
- Strongly fragmented and out-of-date **IT landscapes** as well as a lack of interfaces across sectors are considered as obstacles for the interaction with customers and cooperation partners (e.g. distribution channels).

Decisive factors for the success of digitalisation range from the development of a minimum viable product (MVP) through to the designing of an attractive working environment and talent management:

- Successful transformation is dependent on the insight that the world is changing at an ever increasing speed, and that **corporate cultures** and organisational structures must adapt to this new and dynamic market environment (the vision and the accompanying implementation and constant adaptation of the **corporate strategy**).
- Decisive success factors are the expectations of financial market participants towards digital change as well as becoming active in the right direction at the right time (e.g. **the development of a minimum viable product**).
- A decisive factor for success is managerial level employees having adequate **know-how** in terms of human resources required for the challenges ahead.
- Designing an **attractive working environment,** as well as **talent management** to obtain the right staff for the job; flexibility, openness, **curiosity regarding new technologies**, which will also require a rethink in relation to the recruiting of staff members.
- **Agility** is a factor that is critical for the prospects of success for transformation in light of the high speed of change. Agility means that staff members are also deployed inter alia based on their personal competence.
- Adaptations to the **IT infrastructure** as well as better usage of data.

Transformation during the digitalisation process should be accompanied by the supervisor from the perspective of the stakeholders. The role of the supervisor is particularly considered as one for ensuring a level playing field, without acting as a "competition regulator" or as a "protector" for existing institutions. The FMA could define a set of "Guidelines for digital transformation processes" within the scope of its monitoring of digital transformation.

Expectations regarding the role of the supervisor affect several areas:

- A **level playing field** should be ensured by the supervisor. In so doing, it is important
  - to consider the **financial market as a whole** and to ensure a level playing field for all market participants
  - to ensure a transparent system of supervision with independent authorities and
  - to ensure its own further development or to ensure that a **digital competence is built up** at the supervisor, to keep pace with the rapid speed of development.
- The transformation during the course of the digitalisation should **be accompanied by the supervisor**, in order to gauge the potential for supervised entities within the confines of the regulatory limits.
- Quick **clarification about whether a licence is necessary** for FinTechs wishing to cooperate with licensed entities.

- The FMA should **not act as a "competition regulator"** or "protector" for existing institutes.
- The supervisor should strive for **dialogue with social partners** in relation to the far-reaching structural change in the banking sector, especially in relation to the development of sustainable business models.
- The supervisor should ensure that the business models of (large) Austrian banks are **increasingly focussed on sustainability**.
- The supervisor may define **"Guidelines for digital transformation processes in banks"** as part of the monitoring of digital transformation, which also envisage the role of a "Chief Digital Officer".

II. NEW PROVIDERS - FINTECHS / INSURTECHS

Digital transformation has opened up the financial market to new competitors. FinTechs / InsurTechs have solutions, offerings and business models at their disposal that allow traditional processes and services in many areas to be more efficiently designed, or even to render them obsolete. It was therefore important for the FMA to also use the Call for Input to obtain the opinion of the stakeholders about implications of the entry of new digital competitors into the financial market.

The stakeholders taking part in the Call for Input by and large echoed the FMA's opinion regarding the new players and also added the following remarks:

New digital competitors will force existing companies to make continuous further developments. The biggest changes are expected in the retail, payments investment advice and self-service sectors (processing of claims, submission of applications for benefits).

- In some companies, **in parallel to existing classic IT, new agile areas** are being built up that focus more strongly on modern technologies.
- The implications of the entry of new competitors into the financial market are seen positively, since they place **pressure on existing participants to adapt** and set an additional benchmark for entities.
- Digital competitors with new business models may improve pricing transparency as well as increasing **pricing pressure** on established financial services.
- Customers, who hold products from several providers, may in the future be able to see all contracts in a single portal by means of **aggregators**. It might for example be difficult for insurers to tie customers to their own portals exclusively by means of insurance. Distribution will also be threatened by comparison portals and niche providers.

New market participants and existing market players are not only competitors, but may also mutually complement one another by means of cooperation.

- FinTech/InsurTech sector start-ups known as digital competitors are primarily considered as cooperation partners of established market participants. Many new players look to cooperation with established players to be able to profit from their access to the market. Established entities seek partnerships with new players in order to profit from their innovative strength.
- Small innovative banking institutions ("challenger banks") use new technologies and provide products and services that have previously not existed, which to a large extent are digital and personalised, and thereby increasingly challenge large universal banks.
- Consideration is also neglected that insurance companies are threatened by competition within their own company, as re-insurers are among the main financiers of the start-up scene, who have many cooperations with FinTechs/InsurTechs.

The concept of the “sandbox” is generally welcomed for the trialling of new business models. Financial market participants are able to establish more quickly about how and which regulatory standards need to be observed thanks to regulatory transparency. However, in doing so, the reputation and confidence in the financial market must also be ensured. Therefore, it is necessary to firstly ensure that all regulatory requirements are met before involving end customers.

III. PRODUCT DESIGN

What specific regulatory standards are still necessary due to the digitalisation of the financial sector? What impediments make the development of new digital financial products more difficult? Do you share the FMA’s assessment about the opportunities and threats associated with their impact on banking or insurance? What specific positive and negative developments regarding “digital” financial products can be observed from your perspective? What duties should the FMA perform in relation to the protection of investors, insured persons and creditors with regard to “digital” financial products? These were a few of the questions that the FMA asked in its Call for Input.

The participating stakeholders by and large confirm the FMA’s estimation about the effects of digitalisation on the product landscape as well as adding the following remarks:

General consensus prevails that apart from possible requirements for dealing with cyber risks there are currently no requirements for further regulatory standards.

- With regard to **data protection** it is clear that
  - a large and correct step has been taken with the European General Data Protection Regulation (GDPR) based on initial experiences which have made it possible to check how the new standard has proven itself, as well as whether extensions/adaptations are necessary.
  - it should be scrutinised whether data protection standards have long since been overtaken by consumers’ actual conduct (terms of use, in which technology providers are allowed to collect far-reaching personal information, are being accepted without any further verification).
  - where the value creation chains are becoming more complicated, there are also more interfaces that could be problematic from a data protection law perspective.
- One stakeholder states that the **management of cyber risks** should be afforded the utmost priority in the digital financial market. While a supervisory authority may not be able to protect the entire financial system from cyber attacks, it remits part of the FMA’s remit to ensure that the necessary awareness is raised about the problem.
  - The supervisor could, for example, define **specifications for handling of cyber risks.** A further mechanism could be to introduce an option for **penetration testing**, where supervised entities allow their systems to be attacked (for test purposes). Potential vulnerabilities may be discovered and rectified by means of regular testing. In this area the FMA should cooperate with renowned partner companies and – while observing the legal framework – simulate attacks and test the cyber resilience of supervised entities.
  - To ensure a high level of security in networks and information systems, the introduction of centralised **incident reporting** is also a sensible step. Based on the Network and Informations Systems Act (NISG; Netz- und Informationssystemsicherheitsgesetz) compulsory IT strategies could be drawn up for supervised entities, a partnership established with the relevant computer emergency response team (CERT.at, sector-specific CERTs and GovCERT) and entities obliged to have appropriate security measures in place as well as to report major incidents. **Awareness training** events held on a regular basis to increase awareness of vulnerabilities would also be recommended.

Barriers to digitalisation are considered not only to exist due to the regulatory environment, but also to some extent as a result of the to some extent fragmented and out-of-date IT environment, due to customer conduct, as well as due to the digital competence of customers.

- **Regulatory impediments**, which hamper digitalisation, include existing regulations, that are not befitting of the era of digitalisation, such as:
  - the obligation of credit institutions to make certain documents available in paper form
  - the compulsory requirement of a signature on the information document for depositors (Article 37a BWG) hampers the introduction of new and innovative on-boarding processes
  - the barriers for conclusion of a contract in a fully digital manner: buzzwords in this regard include “seamless / end-to-end” and “without media discontinuity” as well as occurring without delays.
- The **IT infrastructure** of Austrian financial sector institutions is by and large very out-of-date and very fragmented. The development of digital financial products requires a certain degree of flexibility in IT terms, which doesn’t exist. Some entities consider there to also be need for catching up with regard to their **willingness to radically change IT systems** – especially in the area of continuous integration. Furthermore, it would be more advantageous to work on harmonised methods for a holistic, integrated IT financial infrastructure. While many entities remain committed to their existing individual IT solutions, only very few deploy a methodological consistency across departments.
- Furthermore, **customer behaviour** in Austria has a somewhat “wait-and-see” attitude in the field of digital products. This results in Austria not being a “first mover” in the development of digital products.
- Generally increasing the **digital competence of the population** should not be overlooked. The focus should be on building up in basic competences in relation to mobile Internet usage as well as special training and qualification offers.
- Actively redesigning **corporate culture** is often underestimated as a basis of any change process within the scope of digitalisation. An appropriate system of values, scope for shaping, promoting and supporting staff members are significant measures towards increased customer focus, and an appropriate process design.
- The following were also named as obstacles to digitalisation:
  - lack of a regulatory sandbox
  - thinking in too small dimensions (market size)
  - lack of financial means for research and development

Increasing transparency of products and better customer service are perceived especially as positive developments.

- **Increasing transparency and simplicity** of products as well as innovations which mean that the customer receives, for example, an **improved service** are mentioned in a positive light.
- The creation of new business lines is also perceived positively.
- A small number of IT providers as the exclusive point of contact and a centralised security access is more efficient and has a positive effect on IT security. **Professional IT security management** of big players may reduce the probability of an attack, although the potential damage is much higher.
- The BMF’s **FinTech-Beirat** (FinTech Advisory Board) is also cited as a positive example, since it allows experts from banks, insurance companies, FinTech start-ups as well as other stakeholders to discuss together with experts from the FMA and the BMF about new issues, such as ICOs, the tokenisation of assets, synchronisation of KYC data and regulatory sandboxes.

The mere “digitalisation” of existing products as well as modular products in conjunction with “advice-free” products is considered in a negative light.

- A few providers efforts of making existing products **“digital only”** is considered in a negative light. Digital transformation should have a different appearance.
- **Modular products** are also viewed critically, where the total amount for all the selected components is ultimately significantly more expensive than existing products covering all components. This is particularly to be viewed in a critical light in conjunction with **“advice-free” offerings**.
- Retail business is dominated by a **small number of market participants** (as a rule global technology groups). Due to the increasing concentration on a select few IT providers (e.g. cloud service providers), **concentration and contagion risks** arise, which affect IT security in a negative manner (spillover effects). On the other side, there are a small number of IT providers that are the sole point of contact, and the central security access point is more efficient and also has positive aspects in IT security terms. Professional IT security management of big players may reduce the probability of an attack, although the potential damage is much higher.
- One stakeholder additionally also addressed various critical aspects about the financial products mentioned in the FMA Study (e.g. the risk that spurious correlations are established, or parameters are used, which are not entirely within the control of the customers, etc.) and also questions where cyber risk in reality should in fact be borne by the providers of the technologies used, in a similar way to a provider of baked goods being liable for ensuring the there is no risk for the health of customers emanating from the baked goods.

There is a multi-layered expectation regarding the role of the supervisor: It is suggested that technical standards should be defined for areas like robo advice and that the supervisor monitors technical processes that are intended to ensure in entities that no decision-making parameters are used that are discriminatory and/or contravene data protection law. Compulsory regular inspection, rejection of and modernisation of out-of-date IT systems should form part of the FMA’s duties and demands. The analysis of cyber risks, workshops and simulations in this regards are explicitly welcomed.

- Digitalisation shall **not** be allowed to lead to any **breaking down of protection of investors, insured persons and creditors.** One of the FMA’s most important duties is considered to be making **consumer information** available.
- To ensure a level playing field, the organisational requirements that are applicable for the sector should also be observed in the case of digital business models.
- In the same way as for the auditing of internal risk modules, in relation to the supervisor’s conduct supervision, compulsory rules should also be draw up in relation to **technical processes**. Such audit processes should ensure that no parameters for decision-making are used that are discriminatory and/or illegal in data protection terms. **Technical standards** should be draw up for example for **robo advice**, which should be subject to an ex ante audit as well as ad hoc ex post audits.
- The compulsory **regular inspection, rejection of and modernisation of out-of-date IT systems** should belong to the FMA’s duties and standards in relation to the deployment of IT systems. The analysis of cyber risks, workshops and simulations in this regard are explicitly welcomed. This is especially significant as entities to some extent do not adequately understand the risks and challenges entailed with regard to the IT financial architecture.
- Several institutions mentioned the necessity of a **discourse on ethical limits**. One stakeholder explicitly welcomes the supervisor taking a pioneering role in this discussion. However, at the same time society and politics are also in demand. The overthrowing of the solidarity principle shall not be allowed to be a consequence of using “Big Data”.

IV. DISTRIBUTION / CUSTOMER INTERFACE

What duties should the FMA perform with regard to the protection of investors, insured persons and creditors in relation to the digitalisation of the interfaces to the customers? What specific regulatory standards are still necessary due to the digitalisation of the financial sector? Do impediments exist in Austria that hinder digital communications? What specific positive as well as negative developments regarding "digital" distribution can be observed from your perspective? These were a few of the questions that the FMA asked in the Call for Input.

The stakeholders participating in the Call for Input supplemented the FMA's perspective with the following statements:

The feeling is more or less unanimous that **regulatory standards** still do not adequately reflect digital transformation. On the one hand a plea is made for regulation (especially banking secrecy requirements, data protection, the Telecommunications Act (TKG) and the Financial Markets Anti-Money Laundering Act (FM-GwG)) that should enable the purely digital settlement of transactions without requiring the physical presence of the customer in the interests of customer convenience. On the other hand one stakeholder advocates that digitalisation must continue to allow consumers to communicate in paper form – or receive pre-contractual or contractual information in this form, and that such a form of communication should not be allowed to be penalised by additional fees being charged. Consumers should neither be forced de facto to use technologies nor for to use them for cost reasons. Furthermore, it was criticised that data protection law regulations have been kept general and do not suffice for answering customers' sector-specific data protection questions.

- **Data protection rules:** While the EU's General Data Protection Regulation (GDPR) is a step in the right direction, there is nevertheless a strong divergence in opinion about how effective it is: on the one hand, it is suggested to wait and see how the new standard proves itself before checking whether or not extensions or adaptations are necessary. On the other hand its implementability in relation to the real added value for the customer and the effect on the banks is questioned or criticised with its standards being very general and were not adequate for answering sector-specific data protection questions of some importance for consumers. Where there is room for manoeuvre for clarification in the GDPR, the Austrian legislator should use this room for manoeuvre for detailed sector-specific rules. This would affect, for example, creditworthiness assessments, which are inadequately addressed in the Commercial Code (GewO; Gewerbeordnung) in relation to data protection and various categories of addressees, or the automatic taking of decisions and the profiling of customers by financial services. Alternatively it would be necessary to push for the European Data Protection Board (EDPB) to issue practical guidelines.
- **Digital Communication:** It would be desirable in the interests of customer convenience for regulation (especially banking secrecy requirements, data protection, the Telecommunications Act (TKG), the Financial Markets Anti-Money Laundering Act (FM-GwG) etc.) to be designed in such a way that enables a purely digital conclusion of business without the necessity of the physical presence of the customer. The expansion of interconnection technology should in any case keep up with the expected expansion in data volume for digital communication. In the area of payment services, during the implementing of regulation of strong customer authentication in accordance with Article 87 ZaDiG 2018, some credit institutions were beset by uncertainty. Consequently, users were forced to change to using a smartphone app for authentication purposes, instead of the established process of using an SMS-TAN. Some banks even inaccurately informed their customers in writing about the replacement of the SMS-TAN procedure "due to legal regulations".
- In drawing-up any further regulations, the principle of "one in, one out" should be observed, in order to avoid further reaching over-regulation. The definitive implementation of the already existing legal acts is in particular required, e.g. The PRIIP Regulation, PSD II, MiFID II, before considering any new legal standards.

The increased availability of banking products, the fact that advisory services are not being replaced and quick decision-making paths at the point of sale are perceived as **positive developments** with regard to the digital distribution. For wholesale customers the direct connection of the online banking platform to their ERP systems in particular is an enormous advantage; in the case of special enquiries, however, the customer advisor cannot be replaced by digitalised distribution.

Complex offerings without any form of advice as well as modular products, for which the total cost of all components is ultimately significantly more expensive when selected individually than for existing products covering all components, are viewed **negatively**.

Scepticism is also raised about the closing of physical bank branches, since by doing so classical banks lose their USP (of direct contact with the customer) over classical online banks.

The **expectations of the supervisor** are complex and cover the following suggestions:

- The process of advice and conclusion of service should be conducted more simply and quickly for all parties concerned (i.e. without media discontinuity and waiting times). As the term “advice” is defined in law, the supervisor should ensure that where there is a mention of “advice” that there is actually **advice** provided.
- Where **algorithms** are used, then they should be submitted and presented to the supervisor in relation to the observance of rules of conduct and freedom from discrimination. Investors are after all barely able to assess and evaluate the quality of robo advice programmes as well as their underlying parameters. It is not possible to automatically avoid conflicts of interest with robo advice systems; moreover the danger exists that the lack of transparency will be further increased by recommendations.
- Digital distribution should **ensure traceability.** Whether such a demand is able to be satisfied for example by chats conducted on Facebook remains highly doubtful. In any case, irrespective of the delivery channel, **conclusion and termination should be able to occur symmetrically**, i.e. channels that may be used to establish continuing obligations should also be able to be used to close them again.
- The **maintaining of banking secrecy and data protection requirements** constitute a particular challenge for all interfaces and should be subjected to a special inspection by the supervisor. The same rules should apply for digital interfaces to the customer as for offline interfaces. This also applies for information and documentation requirements as well as the know your customer (KYC) process.
- The supervisor should contribute towards a harmonised **level playing field** in the EU, e.g. in relation to video-based identification. The continuing lack of a level playing field is viewed critically in particular in relation to the disclosure obligations that apply to online banks.
- **Misleading publicity** should also be prevented, and the approval of the customer obtained in a manner that is correct under data protection law.
- The regulation of **comparison portals** appears sensible. It should be apparent to the customer about the relationship that exists between the operator and the product provider, which fees and commissions are passed onto the operator and the criteria used for drawing up the ranking shown. Practical experience shows, that a large number of market providers are not listed in the popular comparison portals, which leads to significant doubt about how representative for the market. Portal operators should therefore be obliged to disclose in a clear and unambiguous manner, in particular about listed providers, as necessary including the figures about their respective market shares, in order to not falsely give the impression of completeness or a particular level of representativeness for the market.
- In conjunction with the used of **personalised websites** the largest challenge is that the information saved about customers is permanently available and permanent access to the website is possible.

- **Social media** could pose a risk, in that firstly communications are of a passing nature and then are no longer traceable. Secondly, it may be observed that structures are nurtured from network marketing, which demonstrate the character of networking marketing. The network marketing principle could however cause enormous mass claims.
- The trend towards **mobile apps** could lead to other communications channels being deliberately neglected, or to some extent associated with higher charges (or other comparative disadvantages). It is also viewed critically if entities encourage their customers to exclusively save their access information or other contract information on an end device that might be used as a gateway for fraud/abuse.
- Replacing advisors with **chatbots** (instead of e-mails) is not in the interest of many consumers, who want personal advice in the case of complex financial products. Chatbots should complement personal advice, but should not serve as a substitute for it. Replacing e-mail communications is to be viewed critically, since communications processes can be traced in terms of the point of time, content and the addressees of the communication.

V. ASSET MANAGEMENT

From your perspective, what duties should the FMA perform with regard to digitalisation in asset management? What impediments exist to automate the asset management processes and facilitate the extension of alternative technologies like AI, deep learning and machine learning? During the consultation period the following input was received about these issues:

The **advantages** of digitalisation in the field of asset management are considered in relation to the potential to reduce costs and in increasing efficiency as well as in reducing operational risks.

Ensuing automation is at the same time also associated with various **disadvantages**: Reduction in number of jobs, while at the same time a shortage of suitable experts exists for extending the IT infrastructure and for the management of interfaces, as financial services providers as a rule only offering solutions for certain sub areas (e.g. the provision of information, trading, funds accounting), high one-off expenses, dependency on external providers and automated processes.

The **expectations of the supervisor** also cover various remarks in this area:

- **technology-neutral supervision** is desired, which neither prefers nor disadvantages technology-savvy entities. Equal standards should apply for all market participants.
- A **focus on IT security** could occur in the future.
- New business models as part of digitalisation may have the consequence of **amendments being made to existing regulations**:
  - In the case of crypto assets as an asset class opportunities for diversification for a portfolio must be taken into consideration appropriately. Furthermore, a requirement could arise for the need for provisions in relation to investment.
  - Adaptations might be necessary in the field of money laundering.
  - It needs to also be regulated under supervisory law, regarding when, in the case of crypto assets, a security actually exists.
  - A competitive advantage is expected for alternative products like crypto currencies, since they are subject to less strict regulations under supervisory law.
- A digitalisation of processes including the valuation of investments is expected in the investment process. **Minimum standards** should be introduced in this case.

VI. ACCOUNTING

Digitalisation also has effects for accountancy and accounting. This in particular takes into account the accounting frameworks and financial reporting, the depiction of digital innovations (e.g. cryptocurrencies) in accounting and in the auditing of the financial statement.

Stakeholders expressed the following remarks about this topic:

Advantages of digitalisation in accountancy are seen in terms of gains in efficiency (which however are by and large outset by a greater information requirement of stakeholders/regulators alike) as well as information being more quickly available as well as an improvement in feasibility checks and valuations by using digital instruments.

The digitalisation of accounting processes also has various **drawbacks**: high investment costs and retaining experts in innovation projects, feasibility and assessments nonetheless require professional competences and the expertise of auditors; the challenge for controllers will be tracing and understanding the interaction of complex software systems, the underlying logic of the analysis as well as the findings of comprehensive and powerful data analyses, and therefore to be able to arrive at relevant implications for the audit findings.

The **expectations for the supervisor** consist of various suggestions:

- Using digital instruments leads to a certain extent to massive changes of the accounting process – from receipt, through analysis, to controlling. The development of accounting standards - especially international accounting standards - shows a massive trend towards allowing future estimations and expectations from various financial phenomena in accounting to flow more strongly into the approaches used for the items in the annual financial statement. The supervisor's duty within the regulatory framework will be **to continue to ensure the quality of audits**. The audit competences of controllers of the internal control system or the auditing of the annual financial statement are to be expanded to focus more strongly on the functioning of audit systems as well as the use of digital instruments.
- The supervisor must in particular bring the possession of the necessary knowledge, skills and expertise further to the fore in relation to the **Fit & Proper requirements**.
- The **digitalisation of communications** between banks and the supervisor should be extended further, especially with regard to reporting and the exchanging of other information that is of supervisory relevance.
- The **physical retention requirements** for documents should be harmonised across the various respective laws, to make it possible for them to be retained in electronic formats or as scans across the board.

VII. IT INFRASTRUCTURE

What duties should the FMA perform in relation to the IT systems used in the Austrian financial market? What specific regulatory standards are necessary in relation to the use of IT systems in the financial sector? What positive and negative aspects exist for IT security in relation to the increasing concentration of the financial market towards only a small number of IT providers? Are the material advantages and potential disadvantages of agile approaches duly captured?

During the consultation the following input was received about these issues in particular:

The increasing **concentration** of the financial market **on a small number of IT providers** is simultaneously advantageous and disadvantageous:

- It should be viewed positively that the **complexity of the interfaces** between different solutions is **decreasing**. Furthermore solutions may emerge that are able to be used for gaining knowledge as well as for security functions. Moreover, the concentration towards a few IT providers would also lead to harmonised or at least **similar process workflows**. Staff members who change employer within the sector, would therefore frequently be familiar with the IT systems used. Furthermore, harmonised systems could also lead to security vulnerabilities being detected and remedied more quickly.
- It is disadvantageous that the concentration on a few IT providers could have **far-reaching systemic effects** on entities in the financial sector **in the event of an outage** of such a provider of services. This would be particularly critical when such an outage affects several providers of material services. It is therefore essential that such providers are checked during the due diligence process.

The **use of agile methods** is not only accompanied by many simplifications, but also by some risks, which financial market participants should make themselves aware of:

- It should viewed positively that agile approaches are being used in almost all areas during the course of modernisation, in order to be able to **implement the requirements of the market in a timely manner**, and to improve the time-to-market by having shorter iteration cycles. Also for IT architecture it would also be advantageous to be able to develop components independently of one another; with a focus on a large number of microservices rather than large monoliths.
- Often, however, not all developers are satisfied or familiar with the method. In addition an increased testing outlay may exist, which would require resources. It may often be **difficult to estimate project costs at the outset**, and being able to do so may only improve during the course of a project. Increased levels of communication between different departments may now be necessary, which was hitherto not usually the case. Furthermore, modernising IT architectures does not always lead to the consolidation or simplification of the application landscape. Such problems are multiplied in light of a lack of consistency in the decommissioning of specific legacy systems. This leads to **permanent redundancy**.

Regarding the **role of the regulator and the supervisor,** the following comments were made with regard to area:

- **Clear legal frameworks** are considered necessary regarding the use of IT systems in the financial sector (e.g. SREP/ISO2700x – the more specific, the better). CROE may be a good example for concrete measures.
- Furthermore, a **control instance for the systems deployed** would have to exist with regard to security, sourcing and governance.
- The FMA should ensure that supervised entities are "**fit & proper in the area of IT"**, to ensure competitiveness and to prevent against crowding-out effects.

VIII. CYBER RISKS

Using which measures or initiatives might be FMA be specifically able to contribute to increasing cyber security in the financial market? Which cyber threat scenarios may be particularly relevant for the Austrian financial market in the future? Which core areas of IT security should be strengthened by undertakings in the Austrian financial markets as a priority? Should further measures be deployed by undertakings to defend against cyber attacks in the future? From your perspective is there a balanced level of threats between the different sectors of the financial market, or are some areas particularly highly exposed? What lack of legal clarity, opportunities and threats do you see in relation to cyber insurance?

The participating stakeholders in the Call for Input by and large echoed the FMA's conclusions regarding cyber risks, while also adding the following views:

Particularly relevant **cyber threat scenarios** for the Austrian financial market have been identified at cloud providers such as data loss or data theft in relation to cloud computing and threats from "shadow IT" (lack of transparency in the IT infrastructure). Further threats include malware, blackmail, crypto attacks, zero day exploits as well as insider fraud.

- The **strengthening** of the following **areas should be prioritised** to improve IT security: awareness, identity and access management, privileged access management, asset management, cloud security, secure software / system development, incident management, third party risk management, investigative technologies and BCM. An overview for defending against cyber attacks should be created by centrally managing security incidents, and a clear approach should be developed in relation to cyber blackmail. It is important to optimise the early detection of attacks and security incidents (e.g. SIEM/SOC). Software products provided by third party manufacturers should be more strictly controlled.
- Within the banking sector the level of threat is generally pretty uniform. The decisive factor for the level of threat is the presence of the bank's own brand, which receives more interest as a result of marketing. Additionally, (poor) dealing with customers and security researchers might lead to a dramatic increase of the level of threat. The more an undertaking exposes itself via web portals and publicly available interfaces, the more vulnerable it makes itself to attacks.

Regarding cyber attacks the increased information exchange (IOCs, Tools etc.) primarily by CERTs or other international governmental organisations is seen as being a **positive development**. Furthermore, in relation to its security focus, the product landscape is continuing to develop very positively.

The **negative developments** include that politics is again showing interest that cryptographic procedures are being diluted (government Trojans (Bundestrojaner), Hack-back, the Australian "Assistance and Access bill"). In addition the focus of ransomware seems to be changing from private persons to companies and government institutions.

Regarding the **role of the regulator and the supervisor,** the following comments were made with regard to cyber risks:

- In the case that attacks are detected and reported that are relevant for other institutions in the sector, then **warnings and recommendations** should be issued. By doing so, the added value of reporting security incidents risks for institutions.
- **A far-reaching inspection** would be desirable, primarily in relation to governance, operational and organisational structure, skills, modern identification methods, security strategy as well as inspections about new topics like cloud technology, IAM, agile development as well as awareness in the management board and supervisory board.
- It would be helpful, fn an allocation were to be drawn up between existing regulatory standards of the FMA and the standards of the EBA, ECB, regulatory requirements and best practices (e.g. ISO/IEC 27001). Consequently compliance with these requirements may be able to be checked and assessed more easily.
- A **stronger formulation** is desired, like, e.g., in the CROE for different levels for ambition as well as focus on cloud technology, IAM, detective security technologies and incident response.
- Data protection and therefore also **privacy in the banking and insurance sector** could be examined in greater detail. It may also be interesting to establish what is being done on a proactive basis in this area. Data protection and data security must be taken into account in the case of software and applications from Austria.

IX. DIGITAL TECHNOLOGIES

Based on your personal experiences or your estimation should other digital technologies or opportunities for deployment be considered in the observation of the implications of digitalisation on the Austrian financial market? What lack of legal clarity are associated with the deployment of new digital technologies from your perspective? Do you share the FMA's opinion in relation to the opportunities and threats of the individual technologies? Which additional material risks could also be relevant from your perspective for the individual sectors in the future? What is your expectation with regard to the role of the supervisor in the individual sectors of the financial market?

The stakeholders participating in the Call for Input generally echo the FMA's conclusions regarding new technologies that are establishing themselves in the financial markets and in addition also mentioned the following:

- It is essential to remain firmly on the pulse in an environment that is permanently changing. In the future **further-reaching analyses of the opportunities and threats** for the financial market may therefore be necessary.
- Regarding the IoT, the **process of the generation of the data in the device** itself is not legally regulated, which is why a lack of legal clarity might often exist in this regard.
- A lack of legal clarity is seen with regard to **robo advisors** in relation to the issue of liability. Clarifications would be required under what conditions the manufacturers and when providers have to assume liability.
- The supervisor would have to **set standards** in advance and share such standards **with supervised entities in the form of a coaching event**. In many issues, banks are currently still in the phase of experimenting and in the first instance pay attention to increased turnover and profit.
- A **regulatory sandbox** would be welcomed for the deployment of new digital technologies, in which technological solutions might be put through their paces from a regulatory perspective, and thereby could arrive at technological solutions more quickly within the scope of (consequently more quickly) adapted regulatory frameworks.
- The opportunities arising from the blockchain are generally correctly depicted. However, in particular the **execution of contracts** (smart contracts) **without a default risk**, could in particular lead to significant **opportunities** in the financial market.

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
AIFMG	Alternative Investment Fund Managers Act
API	Application Programming Interface
B2C	Business-to-Customer
BDA	Big Data Analytics
BWG	(Austrian) Banking Act
CI	credit institution
CROE	Cyber Resilience Oversight Expectations
DLT	Distributed Ledger Technology
EBA	European Banking Authority
EC	European Commission
ECJ	European Court of Justice
e.g.	for example
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Union Agency for Cybersecurity
ESMA	European Security Markets Authority
etc.	et cetera
EU	European Union
FMABG	Financial Market Authority Act
FSB	Financial Stability Board
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
IAM	Identity Access Management
IDD	Insurance Distribution Directive - Directive (EU) 2016/97
IEC	International Electrotechnical Commission
IFRS	International Financial Reporting Standards
IFs	investment service providers and investment firms
IoT	Internet of Things
ISO	International Standards Organization
IU	Insurance undertaking
KYC	Know your Customer
MIs	market infrastructures
MiFID	Markets in Financial Instruments Directive
OGH	(Austrian) Supreme Court of Justice
OPFs	Occupational provision funds
ORSA	Own Risk and Solvency Assessment
PaaS	Platform as a Service
PKs	Pensionskassen
PHI	Private health insurance
P2P	Peer-to-Peer
PRIIP	Packaged Retail Investments and Insurance Products
PSD	Payment Services Directive
RPA	Robotic Process Automation
(R)IUs	(Re)insurance undertakings
SaaS	Software as a Service
SIs	significant institutions
SME	small and medium-sized enterprise
SREP	Supervisory Review and Evaluation Process
VAG	Insurance Supervision Act 2016
VersVG	Insurance Policy Act
ZaDiG	(Austrian) Payment Services Act