Finanstilsynet

FIDA response to consultation on a new digital finance strategy for Europe / FinTech action plan

FINANS DANMARK

Summary

We fully support the efforts towards the development of technology-neutral legislation that is horizontal and sufficiently flexible to protect all consumers irrespective of new technologies or products that may arise in the market. We recommend a technologically neutral approach to provide clarity to the market regarding applicable requirements for digital innovation. Without such clarity, innovative services/functions will not be implemented by traditional market players.

It is an important principle of financial regulation that the same activity is regulated equally. This ensures that the regulation of an activity is the same, regardless of who provides the service. It is essential that this is also ensured in the future when, for example, new players in the form of big techs are brought into the financial market. This emphasises the need to regulate the activity instead of the actor.

We believe that clear, simple, future-proof and overarching rules, e.g. concerning taxonomy are essential in order to guarantee consumer protection, and to embrace the digitalization of the financial market.

Data sharing can create great opportunities for Europe to increase prosperity for citizens and boost growth for businesses. For the banking industry, data sharing can enable major innovations which help to enhance customer experience, democratize financial services, improve cybersecurity and consumer protection and strengthen risk management. Open Finance can help 'level up' the whole industry in these areas but should then allow industry to develop a self-support ecosystem around them. A level playing field will be an essential component of open finance and an open data economy.

We welcome the initiative of the European Commission to bring forward legislative proposals for fostering the digital operational resilience framework for financial services with a view to harmonise rules across the EU. The interconnectedness of all actors within the financial ecosystem, including third party providers, and

Høringssvar

6. maj 2020

Dok: FIDA-151247800-691966-v1
Kontakt Mette Stürup

the evolution of ICT risks highlight the need for a common level of minimum security for the financial sector as a whole, based on international coordination. Financial institutions already abide by different existing security frameworks that establish measures for ensuring the resilience of the banking system. Any new requirements should be harmonised and also aligned with existing rules at EU and global level, to avoid duplications or overlaps. New rules should follow a risk-based approach. This would ensure that the framework is future-proof and will provide entities the flexibility required to adapt based on the continuously evolving nature of cyber and technology risks.

FIDA response to consultation on a new digital finance strategy for Europe / FinTech action plan

Høringssvar

6. maj 2020
Dok. nr.:
FIDA-151247800-691966-v1

1. **Ensuring a technology-neutral and innovation friendly EU financial services regulatory framework**

We believe that horizontal and sufficiently flexible technology-neutral legislation is key to ensure sound consumer protection in a continuously evolving digital market. More specifically, flexibility would allow legislation to remain relevant, adapt to the changes in technology and ensure consumer protection. The timing of the EU decision-making process in terms of negotiations, implementation, etc, makes continuous adjustment of legislation in response to evolving technologies very difficult. Therefore, ensuring that legislation is technology neutral is necessary to ensure that it remains relevant to future, potentially rapid, technological changes and to ensure consistency in the protection of consumers.
For example, we particularly praise the design of the Distance Marketing of Financial Services Directive, that by being principle-based rather than rule-based, was able to adapt to evolving use of digital devices and continues ensuring a high level of consumer protection. It is important to address regulatory obstacles not to slow down the uptake of new technologies in the financial sector. There is today problems in areas obstacles to use cloud services, AI and Distributed ledger technology (except crypto assets).

Crypto-assets and blockchain/DLT
Finance Denmark supports the work that is being done internationally in terms of identifying the extent to which crypto assets are covered by current EU legislation, whether new legislation is needed in this area and, where appropriate, how to regulate it. It is essential that regulation takes place at European, if not global level, as there may be global players and activities.

In general, Finans Danmark believes that the same rules should apply, whether conventional assets or crypto-assets ("same business, same risks, same rules"). This applies, for example, in relation to anti-money laundering and terrorist financing rules, consumer and data protection, cyber risks and tax. It ensures that the regulation of an activity is the same regardless of who is providing the service (level playing field).

Future regulation of crypto assets and blockchain technology should focus on regulating the activity and not the technology itself, in other words being technology neutral.

In recent years, Danish banks have studied blockchain and DLT. The technology has potential and can hold opportunities for the community. It is therefore important to have the best framework for utilizing the new technologies. Greater regulatory clarity will make a positive contribution in this regard and ensure that traditional banks can actively participate in the development of new asset classes and offer these where commercially attractive.

Furthermore, regulation will need to be able to respond quickly to future, new categories of crypto-assets when they will arise. A classification will help to support these future adaptions, providing a legally certain foundation for regulatory assessments.

Finance Denmark welcome the EU institutions' awareness regarding stable coins and encourage a thorough assessment. Finance Denmark believes that private stable coins initiatives, if used for payment transactions, should face the same scrutiny as any other payment provider, e.g. when it comes to security and customer protection as stipulated in PSD2, data privacy as stipulated in the GDPR as well as requirements related to AML and KYC, so that a level playing field exists between all payment providers.

Open finance

Data sharing can create great opportunities for Europe to increase prosperity for citizens and boost growth for businesses. For the banking industry, this can enable major innovations which help to enhance customer experience, democratize financial services, improve cybersecurity and consumer protection and strengthen risk management.

Regulatory initiatives like PSD2 has been useful in the establishment of the categories of industry participants, the services that they can offer and of an industry body that has been able support dialogue on e.g. API technical standards. These initiatives are the foundation on which a self-supporting ecosystem can then develop through industry-led and voluntary initiatives. Open finance can help 'level up' the whole industry in these areas but should then allow industry to develop a self-support ecosystem around them.

A level playing field will be an essential component of open finance, which also has to be viewed within the broader discussion on creating an open data economy.

The fundamental requirements for efficient open finance are first and foremost to:

- Focus on customer demand and how data can be used to create value added services.
- Distinguish between machine data and personal data
- For both categories it is important to ensure standardization of data and data formats including clarity on the way data can be technically accessed, and in this context ensure that data is shared in real time
- Ensure a level playing field for machine data in general (not personal data) where both data access and data use is either free of charge or based on a cost-based approach (e.g. Long Rund Increment Cost – LRIC+) including no limitations/restrictions in usage of the obtained data.
- In case there is a move towards free of charge machine data, it would be relevant to take a similar approach in the market data space (raw market data) in contrast to the present "Reasonable Commercial Basis" approach in MiFIDII/MiFIR in order to create a level playing field for raw data in general. Years ago, market data was actually free of charge.
- Move away from the principle of PSD2, where banks have to give access to data without a contractual relation and without any fair distribution of value. All market players should be able to benefit and build sustainable business cases.

There is indeed a growing acknowledgment that relevant data from different sectors holds significant potential for financial industry innovation, competition, and consumer empowerment. It can help provide users with enhanced customer experience, better risk management, stronger security and fraud detection, better services, and convenience. The key driver for the use of data should always be the users' interests and empowerment.

Digitalization of public authorities and access to publicly held data is an important enabler for (cross border) digital financial services to develop. Many public registries hold data that are highly relevant for developing digital financial services. To exemplify, digital land registries will allow for a digital customer journey when buying real estate or when re-mortgaging. The Danish digital infrastructure for this serves as a good example.

Similarly, access to tax returns and company accounts, allow banks to access basic financial data for credit assessments. Having access to passport registries would allow banks and payment service providers to improve the quality of customer onboarding and ongoing AML due diligence.

Thus, public data are key for the development of data-enabled financial service offerings, both by updating regulation and sectoral policies to reflect the opportunities provided by data and by ensuring that they are harmonized and standardized across EU Member States.

We have attached a paper on use cases on open data.

Removing fragmentation in the single market for digital financial services facilitate interoperable cross-border solutions for digital on-boarding:
KYC

Implementation of know-your-customer (KYC) rules according to the 4th and 5th Anti-Money Laundering Directives differs significantly across EU Member States. An illustrative example consists of the differing requirements imposed on obliged entities when verifying the information on beneficial owners and the intensity and time allowed to review, periodically, customer information and documents. In this regard, an AML Regulation should be in place to set out clear and uniform rules for harmonising the KYC policy across the EU, making sure it is aligned with international standards and the FATF Guidance. In addition, such rules need to be followed up with clear guidance on how to implement specific provisions and include risk-based KYC requirements for specific topics. A document-based approach to KYC is rapidly becoming unsustainable in an increasingly digital world.

All in all, we welcome a flexible, risk-based approach that would support financial inclusion, as indicated by the FATF guidance on digital identity. As described in the guidance, AML/CTF risks may be mitigated by, for example, limiting the services available to the customer. However, this risk-based approach should have a broader scope beyond financial inclusion, enabling regulated entities to adjust customer due diligence (CDD) processes to the risks of the specific services being offered at onboarding, and develop stronger confidence in the identity of their customers, as they require services of higher risks.

CDD is not a static exercise; this approach would help to reduce onboarding costs for regulated entities while improving customer experience, while at the same time keeping AML/CTF risks under control. In addition, there would be merit in having guidance on the use of digital identity in the onboarding processes of

legal persons, which also shares many of the potential benefits described in the FATF guidance on digital for their use by natural persons.

Innovation

Cross-border coordination within the EU is fundamental to promote the scale-up of technological innovation and to prevent an unlevel playing field or regulatory arbitrage. This is the principle underpinning the EU framework for experimentation. Coordination across EU member states should be enhanced. This would imply at least the possibility for a national authority to rely on the outcome of the testing done by another authority within a national sandbox via a system of mutual recognition.

The EBA should take the role as the central hub, facilitating exchange of information as well as the gathering of legal interpretations of existing regulations by national authorities in order to support the uptake of common approaches. An EU representation should be organised by the EU authorities in any international initiative (e. g. the Global Financial Innovation Network (GFIN)) to ensure that the views of the Union are represented and to allow EU financial entities to be part of any trials across multiple jurisdictions globally. Likewise, any EU framework of experimentation should also keep in mind similar initiatives that are promoted in third countries, as well as the GFIN work, to ensure knowledge sharing and to avoid a regulatory/innovation arbitrage.

For a supervisor to understand how and if to supervise/regulate e.g. an implementation of AI, they need to both understand the applied technology as well as how the AI is intended to support the business model in order to evaluate the relevant risks with regard to consumer protection and financial stability.

AI

Artificial intelligence (AI) has the potential to improve and change many different industries and sectors – among them also the banking industry. Along with the many benefits that will come - to both consumers and business' alike - when applying AI, there is a growing concern among both consumers, industries, regulators and the political level that AI - if unhinged – can be harmful to both consumers, companies and to our open, democratic and free societies. Therefor we see the European Commission's AI -strategy as welcomed and important.

AI can:

- offer contextualised, personalised products and experiences.
- make more accurate credit-worthiness assessments.
- help identify and remove biases in data

- provide better financial advice.
- better protect customers from fraud.

We support the elements and ambition that the white paper is articulating in relation to building an ecosystem of excellence as well as the need for a comprehensive regulatory framework for AI. When that is said it is important that any new European regulation provides trust and a regulatory setup and framework that will avoid unclarity and ensures that both start-ups, small and large business are all encouraged to provide and use AI solutions. If that ambition is meet, then we can strengthen EU in its competition with the US and China and at the same time strengthen the single European digital market as well as building trust in AI.

- It is important to maintain a strong level of customer protection and ensuring customers are empowered and have trust in AI-solutions.
- AI is an evolving technology and it is paramount to ensure that the regulatory environment is promoting innovation and legal certainty.
- A technology friendly legal and regulatory framework will ensure a level playing field for all industries and geographies is will ensure the uptake of AI in the European banking sector.
- The regulatory frameworks must ensure a coherent risk-based approach.
- It is important that the principles of proportionality and flexibility is applied. This will help the adaption of AI by both large and established companies as well as by SMEs and start-ups.
- When designing a risk-based approach based on proportionality and flexibility future horizontal AI-regulation can seek inspiration in the concept of a regulatory perimeter[1]. A regulatory perimeter will also allow small AI-solution with no risk of very low risk to be easily applied. This will support SME's and start-up to engage with AI
- Providers of AI must make sure that artificial intelligence is being monitored and regularly reviewed (risk-based approach). It is important that any future regulation will acknowledges that many future AI-solutions will be delivered through a mix of in-house solutions as well as services delivered by outsourcing partners e.g. through various cloud services.
- When designing the future horizontal legislative framework for AI, one should also carefully consider alignment with the existing GDPR-regulation and thus avoid any possible contradictions in this relation. This is relevant with regards to the data minimisation principle. Large

[1] EBA Report on Regulatory perimeter (July 2019),

amounts of quality training data are important avoid e.g. biases in future AI-solutions.

AI, fraud prevention, cybersecurity and compliance

The cost of fraud associated to non-cash means of payment is increasing. Fraudsters take seek out new system's vulnerabilities, and exploite people's lack of digital awareness. During the Covid-19-crises banks has experienced a proliferation of scams. AI can provide assistance in the detection of fraud. Having more secure systems will help build trust from consumers in digital services. Consumers trust their banks, mortage institutions ect. to protect their confidential data. With the help of AI, financial institutions can detect anomalies which may be pose a threat. Heir data quality and the amount data is important. By applying AI-solutions into their security setup, banks will be able to improve their security.

Machine learning algorithms and AI can help monitor different kind of activities, and hereby handling large number of "alerts" and selecting only the critical ones. This will be helpful with regard to compliance within a wide range of areas such as CRD IV, MiFID II, GDPR AML/CTF and others

Digital operational cyber resilience

We welcome the initiative of the European Commission to bring forward legislative proposals for fostering the digital operational resilience framework for financial services with a view to harmonise rules across the EU.

Financial institutions already abide by different existing security EU frameworks that establish measures for ensuring the resilience of the banking system (e.g. NIS Directive, PSD2, MiFID II, CRD2, e-IDAS, GDPR, EBA Guidelines on ICT and security risk management, BIS CPMI-IOSCO Guidance on Cyber resilience for financial market infrastructures, TIBER-EU, EBA Guidelines on outsourcing, ECB IT risk self-assessment questionnaire), SWIFT CSP and PCI-DSS .Any new requirements should be harmonised and also aligned with existing rules at EU and global level, to avoid duplications or overlaps.

More harmonised EU-wide ICT incident reporting with a strong focus on four elements (taxonomy, templates, timeframe, thresholds). A widely adopted taxonomy should be used, e.g. by ENISA or VERIS. Finance Denmark also advocates for the harmonization of general information requirements.

Sharing of cyber-threat intelligence among industry must be stringent. It could be on cyber threats and attacks, accessing threat intelligence from law enforcement and authorities, delivering high-level guidance as a result of forensics and

incident reporting analysis while maintaining the confidentiality of sensitive data. Information sharing needs to take place on trusted platforms and contribution should be an obligation for all to reach its full potential.

The EU should develop specific plans for critical sectors and at the same time contemplate introducing measures such as sector CERTs (Computer Emergency Response Team), cyber stress tests and mapping of mutual interdependence. The individual critical sectors must hold a strong and continuous obligation to improve the resilience of their sector.

The interconnectedness of all actors within the financial ecosystem, including third party providers, and the evolution of ICT risks highlight the need for a common level of minimum security for the financial sector as a whole, based on international coordination. We welcome the European initiative on developing security standards for it-services and IOT devices and the intention of having providers to state the level security and the intention of enabling consumer transparency through relevant consumer information regarding the intended goal to reach the maturity level of security by design and by default in consumer products and services.

New rules should follow a risk-based approach. This would ensure that the framework is future-proof and will provide entities the flexibility required to adapt based on the continuously evolving nature of cyber and technology risks.
Regarding the implementation of oversight of third party providers, which would preferably be at European level on the basis of international coordination, should also be risk-based according to the type/ criticality of the service and they should target these providers without imposing additional requirements for financial institutes.

Kind regards

Mette Stürup
Direkte: +4527152020
Mail: ms@fida.dk

Høringssvar

6. maj 2020

Dok. nr.:

FIDA-151247800-691966-v1