EUROPEAN COMMISSION
Directorate-General for Financial Stability, Financial Services and Capital Markets Union

Financial services policy and International affairs

ANNEX

Detailed summary of individual responses to the 'Public Consultation on FinTech: a more competitive and innovative European financial sector'

This document provides a factual overview of the contributions to the 'Public Consultation on FinTech: a more competitive and innovative European financial sector. The content should not be regarded as reflecting the position of the European Commission.

Contents

QUESTIONS BY CONSULTATION CHAPTER

SECTION 1 - FOSTERING ACCESS TO FINANCIAL SERVICES FOR CONSUMERS AND BUSINESSES

Question 1.1 – What type of FinTech applications do you use, how often and why? In which area of financial services would you like to see more FinTech solutions and why?

Total respondents to this question	160

Almost all respondents provided a positive or neutral sentiment on FinTech applications, with the vast majority expressing a positive attitude. The use of FinTech applications was referred to as regular, all the time or daily. Only a few respondents indicated not using FinTech applications. Predominant reasons for using FinTech across all categories of respondents were enhanced customer experience, competition, convenience, efficiency and lower cost. Responses covered both specific technologies and the use of these technologies in specific financial services applications.

Organizations, companies and users emphasised the use of new technologies and applications in their particular line of business. Payments related activities featured very often. Taken together respondents noted the use of FinTech applications in a very wide range of market segments such as payments, factoring, insurance and reinsurance, lending, financial and investment advice, asset management, FX and accounting and activities such as claims handling, underwriting and pricing, remote identification, trading and post-trading, risk management, product development, client management, customer service and marketing, Know Your Customer requirements and profiling and credit scoring. Also regulatory compliance was regularly mentioned as a field of application. Also a number of authorities mentioned this latter point.

Technologies most often referred to were authentication and e-identification, big data, biometrics, artificial intelligence and machine learning and data science more generally, mobile technology, distributed ledger technology, cryptocurrencies, either referring to current use or as areas where respondents liked to see more FinTech solutions. Some stakeholders, mostly representing established financial institutions and intermediaries, noted that FinTech solutions cover all layers of their activities be it at the front/customer experience end, the middle-office or the back office. They also noted the co-operation with and integration of FinTech solutions into broader financial services activities, whereas a few stakeholders from the user side observed that more integration so as to avoid the need to use many different applications would be desirable.

Some respondents referred to services provided by alternative providers, though a large majority of responses made no distinction between financial technology used and applied by traditional financial services providers and alternative providers.

Question 1.2 - If there is evidence that automated financial advice reaches more consumers, firms, investors in the different areas of financial services, at what pace does this happen? And are these services better adapted to user needs? Please explain.

Total respondents to this question	164
Yes	**117**
No	9
Do not know	38

Almost all responders agreed that the automated advice was still at early stage of development and is not equally widespread across the three sectors or across EU. Moreover, it emerged clearly that automated financial advice has not penetrated the EU market sufficiently enough to cite reliable data, while potential successful examples come from outside EU, primarily United States. More than half of respondents are of the view that automated financial advice has the potential to reach a greater number of clients, thus stimulating financial inclusion through digital innovations, reducing the cost of advice and helping customers make sound financial decisions. This is seen as having the potential "to democratize" investment advice. It is expected that some customer groups, such as millennials, were likely more adaptive to new automated tools, whilst some customer groups might rely on personal advice.

However, for some respondents it was too early to determine whether automated financial advice solutions may increase the customer base in reality. From the responses, several stakeholders were convinced that the human factor is likely to remain an important element in the distribution process, and the importance of personalised and adapted advice provided by intermediaries should not be underestimated. According to some, most applications are for single purposes and their current stage of development does not provide comprehensive solutions to complex situations. On the other hand, the automated approach could allow for a more standardised experience by removing the potential for differences due to human interpretation and provided the higher level of transparency about the costs and the risks involved. Some stakeholders noted that the notion of automated advice may be interpreted in different ways across the Member States and asked the Commission to intervene in order to clearly define '*advice*' at the EU level and to make a clear distinction between '*tailored advice'*, '*guidance'* and '*recommendations'* prior to developing any regulation which may allow passporting rights for this activity across Europe. Some responders called for the European and national law to be reviewed to correspond to digital-related transformation and development of automated advice.

Interestingly, a large majority of stakeholders considered that efforts of platforms to provide information using language that is suitable for very niche and fragmented categories of customer could bring about long-term financial literacy benefits; automated financial advice could therefore be effective in promoting financial inclusion and improving financial literacy. For some stakeholders automation/algorithms used by robo-advisors has the potential to become a source of systemic risks.

Question 1.3 - Is enhanced oversight of the use of artificial intelligence (and its underpinning algorithmic infrastructure) required? For instance, should a system of initial and ongoing review of the technological architecture, including transparency and reliability of the algorithms, be put in place? What could be effective alternatives to such a system?

Total respondents to this question	162
Yes	**80**
No	51
Do not know	31

Almost half of all respondents supported the idea of enhanced oversight of artificial intelligence (AI)-enabled algorithms, while a sizeable minority thought this was not necessary, while, a clear differentiation between the three groups of respondents (private individuals, organisations/companies, public authorities) did not emerge. For example, of those national competent authorities/public authorities responding to the consultation, six were for whilst four were against enhanced oversight. One concept put forward was the setting up of a *'regressive oversight regime'*, imposing progressively less stringent oversight requirements on supervised entities corresponding to the development stage of the technologies and the increased experience of the regulators.

Some respondents who were sceptical of the need for enhanced oversight considered AI a nascent and burgeoning technology where regulatory control could stifle innovation. Others said that fully-fledged AI was a utopia that was so far away that no special regulation was needed at this stage as several comprehensive rules, such as GDPR, Solvency II, MiFID II are already in place. Rather than devising a new regulatory regime, AI should be regulated by these existing rules. In this context, it was also considered important to develop best practices, codes of conduct and other self-regulatory actions. Some stakeholders preferred such soft law options to a fully-fledged, hard oversight regime. While AI offers benefits such as a more bespoke client service and efficiency gains, the risks associated with this technology such as herding/bubbles and unfair discrimination of customers should not be neglected either, according to some stakeholders. Especially when it comes to unfair discrimination of customers, it is often not the algorithm that is the problem, but the underlying data with which the algorithm was trained. In this context, some stakeholders thought that there needs to be a differentiation between profiling algorithms and quantitative management algorithms, with profiling algorithms indeed requiring oversight.

A sizeable minority of stakeholders described AI-enabled algorithms as black boxes, making it difficult even for the most sophisticated financial market authorities to understand what is going on inside. For this reason, it was considered important by some stakeholders that financial market authorities should develop a solid understanding of artificial intelligence. Some stakeholders believed that there were no control mechanisms available to take into account the dynamic nature of self-learning algorithms and this could be a particular problem for the auditability of such algorithms. One idea put forward was to create systems where algorithms could fail in a safe way (circuit breakers, guardrails) instead of trying to make sure up front that algorithms were safe, a task considered to be challenging given the dynamic nature of AI-enabled algorithms.

Others claimed that a clear set of rules and spot checks could be a way forward, and again others toyed with the idea of deploying surveillance algorithms to monitor and audit other algorithms.

A sizeable minority of stakeholders thought that devising appropriate testing environments and regulatory sandboxes was very important and considered this a key task for any enhanced oversight regime. One idea tabled by a few stakeholders was to check the outputs rather than the algorithms themselves and infer from the outputs whether the algorithm did what it was intended to do. Different algorithms could also be fed the same data and the results could then be compared.

To avoid regulatory arbitrage, very few stakeholders called for global solutions and questioned whether EU regulation can make a difference. While a sizeable minority of respondents thought that more transparency was crucial, some also pointed out that greater transparency would probably lead to the disclosure of sensitive company secrets and assets.

Question 1.4 - What minimum characteristics and amount of information about the service user and the product portfolio (if any) should be included in algorithms used by the service providers (e.g. as regards risk profile)?

Total respondents to this question	130

The dominant view amongst all respondents pointed to the need for technologically-neutral approaches and compliance with already existing requirements in sectorial regulation –e.g. MiFID II, AMLD, PRIIP – as minimum benchmarks for algorithmic-enabled decision-making. Consequently, a large share or respondents signalled a need for an assessment of minimum characteristics and information for each type of service and/or algorithm.

Respondents from all sectors also pointed to the applicability of the GDPR's provisions for customer data, including requirements for user consent and right to explanation for algorithmic decisions. Data minimisation was a central point especially in the responses of public authorities and civil society organisations and some called for the possibility for human assistance and explanation at every step in the decision-making or advice process.

Some respondents, especially from the banking and FinTech sectors, were sceptical as to the utility of minimum information requirements all together, observing that access to more data would also lead to better services, or that the volume of information collected needs to be proportional to the level of risk assessed. They thought prescribing through regulation e.g. types of user-data could stifle innovation in the sector and suggested instead flexible and dynamically-adapted, sector-specific guidelines.

Organisations representing citizens' interest supported the technology-neutral approach to the collection of customer's data, but also requested for all information to be made clear, in an accessible, non-specialist language, to the customer before the signature of the contract and upon request, e.g. when additional advice is necessary beyond default investment options. They requested for algorithms to be tested and 'calibrated' before the 'production' stage, and that the customer can ask for explanations from a human at any stage in the process. Some civil society respondents called upon authorities to further investigate specific types of data which might act against consumers' and societal interests, leading to discrimination and ethically unsafe decisions. Only seven individuals replied to this question, calling for clarity of decisions/advice and consent-based input of data.

Public authorities in the EU Member States who have replied to the consultation also pointed repeatedly that rules and regulations need to be technology-neutral and the same benchmark should be applied to human and machine-supported decisions. The requirements should, in this regard, follow the MiFID II regulation. In addition, some pointed that the information necessary would vary depending on the specific type of service, but also that personal data is concerned in many instances and the treatment of such data should follow the existing rules on personal data protection, also in terms of transparency and right to explanation for the automatic decision-making.

While industry views, including banks, called for a product/service-specific analysis of minimum characteristics and information requirement, and strongly pleaded for a technology-neutral approach, applying existing regulation to algorithmically-enabled processes. Banks considered necessary general information for investment services to include risk acceptance of the customer, investment timeframes and goals, suitability tests, risk profiles, financial status, etc. Some banks pointed to the need for some level of governance to prevent errors, potentially through standard definitions of quality of outcome measurements. FinTech organisations also nuanced a risk-based approach to the use of artificial intelligence, arguing that audits from regulated entities with IT

expertise could potentially certify risk levels in compliance with the general regulatory provisions.

Most industry organisations, FinTech organisations, payment services and sole traders who responded to this question encouraged flexible, performance-based regulatory framework, arguing that any prescriptive regulatory approach to the information requirements would be a major obstacle to innovation in the sector.

Governance proposals from investment advisors included general transparency requirements on the purpose of the algorithm, the products prioritised, the timing of updates and changes to the algorithm, as well as contingency actions for unsatisfactory algorithmic decisions. Some respondents even asked for regulatory monitoring of the use and impacts of algorithms, while pointing to a need for further investment in skills and technical capability for regulatory authorities.

Amongst the very few technology providers who have responded to the consultation, some called for a governance of algorithms where safeguards for ethical and accurate functioning could be monitored through an accepted standard as well as through some level of regulatory oversight. More in detail, one respondent raised the issue of digital identity and secure authentication both for users and for bots. Some trade unions and industry associations also highlighted the challenges for the personnel developing products and services, and emphasised the need for better training, clarity of responsibilities and multidisciplinary skills required.

Finally, some answers from the academia pointed to existing research which could operationalise checks e.g. for peer to peer lending or asset management, and others called for a university-led certification mechanism of the algorithms used.

Question 1.5 – What consumer protection challenges/risks have you identified with regard to artificial intelligence and big data analytics (e.g. robo-advice)? What measures, do you think, should be taken to address these risks/challenges?

Total respondents to this question	152

The vast majority (74%) of respondents were organizations or companies, followed by public authorities or international organisations (11%) and by private individuals (6%). Overall, there were three main risk factors which represented the minimum common denominator across the three categories of respondents: risks associated to cybersecurity and issues linked to systems/algorithms, risks associated to data protection and risks associated to the liability regime. Concerning the first point, the main issues identified by a large majority of the organisations or companies related to errors in the design of the algorithms leading to the sale of unsuitable financial instruments to consumers, potential hacking of data, information asymmetry, wrong data input and lack of transparency (i.e. how the advice was developed). Main possible solutions identified by companies or organisations were: a robust cybersecurity, reasonably designed trading activities, strong data encryption and performance of adequate risk profile for consumers. Some companies and organisations argued that the risk of mis-selling would tend to increase in a scenario of pure automated models (i.e. errors might be discovered only after a certain number of incorrect advices) and expressed their preference for a hybrid model based on human supervision on robo-advice.

The issue of consumers' data protection was a recurrent theme for organisations and companies, particularly relating to privacy and ownership of personal data, access to personal information present on social networks and the selling of customer data to competitors and/or third parties. Amongst the suggested measures to address these challenges, special consideration was given to fostering financial education for investors (including the correct use of artificial intelligence in the field of investment products), maintaining adequate controls in the use of data, ensuring high level of privacy and extending to the robo-advice the same consumer protection requirements applied to human advisors. Concerning the field of legislation, most organisations and companies agreed on the necessity to have adequate legislative framework in place along with regulators carefully monitoring the developing FinTech sector and intervening whenever necessary. Some respondents made a reference to the GDPR which is considered an effective legislation.

The definition of a clear liability regime in the event of legal disputes for economic damages linked to advice received via fully automated tools was also an overarching issue identified by companies and organisations. The remaining two categories of respondents, namely private individuals and public authorities and international organisations shared almost all concerns raised by companies and organisations relating to cybersecurity, consumers' data protection, transparency, and liability issues. Concerning the latter, one authority noted that companies approved by the authorities remain fully responsible for the activities for which they are supervised, regardless of the potential outsourcing of some of these activities to external companies. The European Supervisory Authorities (ESAs) identified the following additional issues compared to the ones raised by companies and organisations: risk of undermining market integrity or investor protection triggered by the use of big data, risks related to price discrimination, financial exclusion or non-transparent credit scoring and decision-making, concerns that that the financial benefits deriving from operational efficiencies remain within the FinTech companies.

Question 1.6 - Are national regulatory regimes for crowdfunding in Europe impacting on the development of crowdfunding? Please elaborate on your reply to whether there are national regulatory regimes for crowdfunding in Europe impacting on the development of crowdfunding. Explain in what way, and what are the critical components of those regimes.

Total respondents to this question	157
Yes	**86**
No	6
Do not know	65

Almost all respondents answered that national regulatory regimes for crowdfunding in Europe had an impact on the sector's development. This belief was shared across the board by all types of respondents (private individuals, private organisations, public authorities and international organisations). Almost half of the respondents who expressed an opinion on the matter believed that national regulatory regimes hindered cross-border crowdfunding activity and that harmonisation at the EU level was required. These respondents regretted the fact that the European market was fragmented due to divergences in the regimes adopted by different Member States. Some argued that hindering cross-border activity by juxtaposing national regulations impeded real competition, and made it difficult for platforms to scale up and reach the necessary size to be profitable in the longer term. A few also mentioned detrimental effects on consumer/investor protection, resulting from different treatment of users across Europe and uncertainty concerning rules that applied for investor protection in cross border transactions. When calling for more harmonisation at the EU level, a few respondents explicitly referred to the creation of a EU framework and passporting rights for crowdfunding platforms, while others stressed the need to identify and promote national best practices across the continent. A wide range of potential areas for harmonisation was cited by the different respondents, and included platforms' disclosure requirements, registration requirements, consumer/investor protection rules, monitoring systems, reporting obligations, minimal safeguards for financial stability, data privacy, and prevention of money laundering.

Only a couple of respondents rejected the idea of a EU level harmonisation, arguing that the sector was already fully regulated, that MiFID already provided a framework for passporting, and that the existence of lighter national regimes did not require European-level action. A few others warned about the risks of unclear, heavy regulations, or regulating too early. At the same time, a sizeable minority of respondents explicitly referred to national regulatory regimes as having a positive impact on the development of the sector at the national level. Most of them cited enhanced consumer/investor protection and confidence as key elements explaining the positive impact of national laws on the local development of the market. The creation of better calibrated, lighter regimes was also mentioned as a critical component of national regimes to foster the crowdfunding national markets. A few respondents explained that national regimes had had to be adopted precisely because the EU did not put a harmonised framework in place, creating a risk of insufficient investor protection. In addition, only a couple of respondents believed that national regimes had a negative impact on the local development of crowdfunding.

Question 1.7 – How can the Commission support further development of FinTech solutions in the field of non-bank financing, i.e. peer-to-peer/marketplace lending, crowdfunding, invoice and supply chain finance?

Total respondents to this question	142

Regulatory fragmentation was one of the main issues identified as creating obstacles hindering the development of a EU crowdfunding market.

As possible solution identified, the large majority of respondents, over all types of stakeholders, proposed pan-European framework aimed at balancing the dynamics of the industry and the protection of investors. The framework should be simple, proportionate and introduce a joint terminology and provide a provide for a pan-European license/passporting. However, there were diverging opinions on whether this should be a new instrument or whether existing legislation (e.g. MiFID II, AIFMD, PSD2, CRD V, prospectus, CCD, MCD) should be adapted. The majority of stakeholders also stressed the importance of introducing *regulatory sandboxes*, while a sizeable minority argued that solutions developed in a sandbox would be exportable to other member states. Moreover, the need to set up a EU register of crowdfunding and peer-to-peer operators was also raised. A few stakeholders proposed to put in place tax incentives or stimulus packages to stimulate and/or facilitate the market. A sizeable minority mentioned the necessity to foresee the provision of guarantees or counter guarantee schemes and a robust framework to protect investors in case of a bankruptcy. Some respondents mentioned the importance of improving public awareness about the alternatives offered by FinTech (platforms in this case) as this is would contribute significantly to the growth of alternative finance markets. The vast majority of banks stressed the importance of ensuring a level playing field, where regulation should be technology neutral and based on the same activities, same risk, same rules and same supervision principle.

Two challenges were highlighted with regard to the implementation of the suggested solutions: (i) the lack of harmonisation of corporate law and fiscal practices and interpretation of directives; (ii) no full dematerialisation of financial instruments - Full dematerialisation would enable a fully automated (primary and secondary) trading in such instruments and ensuring that rights in such instruments are exercised (both property and corporate rights) in a way currently available mainly for public securities.

Question 1.8 - What minimum level of transparency should be imposed on fund-raisers and platforms? Are self-regulatory initiatives (as promoted by some industry associations and individual platforms) sufficient?

Total respondents to this question	133

Almost all stakeholders agreed that the transparency is instrumental to the credibility and development of crowdfunding as a real alternative of business financing. Many of them were of the opinion that that self-regulatory initiatives have proven to be very efficient in creating and maintaining consumer confidence and that a high degree of transparency has already been integrated in the processes. Part of respondents opposed to the need for additional regulatory intervention while others insisted that even though self-regulatory initiatives have been working well, minimum level of disclosures, traceability, and controls had to be put in place to guarantee that the platforms operate in the best interest of the customer.

Some respondents, mainly representing consumers, expressed their high scepticism about self-regulation and referred to some negative examples especially with regard to the misleading presentation of costs and charges. Several stakeholders stated that due to the digital nature of the services, and their associated cross-border potential, a targeted initiative at EU level was necessary to create a pan-European framework that harmonizes the regulatory environment while guaranteeing consumer protection standards.

Some stakeholders asked that the disclosure regime should be inspired by recent EU-level retail disclosure rules (Key Investor Information Document, PRIIPs and UCITS style) and referred to examples of regimes at the national level. Yet, some of these regimes would need to adapt to the technology. According to some respondents, the level of transparency imposed on fund-raisers and on the related platforms should guarantee a level playing field with other competitors. The principle "same activities, same risk, same rules and same supervision" should have applied. On the other hand, some stakeholders stated that expected disclosure for start-up companies differs clearly from that expected from mature companies. Blockchain decentralized network solutions to be used for transparency regime purposes were considered by some as the most appropriate technology for ensuring transparency.

Some stakeholders stressed the need that any specific legislation in the field of FinTech (e.g. new licensing regimes for FinTech activities) should be underpinned by a thorough feasibility and impact assessments should ensure that cost savings stemming from the application of new technologies are passed on to consumers. Finally, one authority addressed the issue of ethical implications of big data changes in the financial services market. The proposed solution was to incorporate ethics into the governance structure of the firm using data.

Question 1.9 – Can you give examples of how sensor data analytics and other technologies are changing the provision of insurance and other financial services? What are the challenges to the widespread use of new technologies in insurance services?

Total respondents to this question	103

Respondents identified a wide range of applications for homes, transportation, agriculture, health, logistics and energy. Examples of locations of connectedness devices (hence known as - IoT Internet of Things) identified were domestic infrastructure, cars, smartphones, wearable devices including health sensors as well as physically remote sensors such as drones, weather stations and satellites. Some respondents also identified that data can also be gathered from social networking sites and credit history, although these are not sensors as such.

Some respondents cited several potential advantages deriving from the use of sensor-based data in the insurance sector. Most examples identified the advantages to insurers including the improved ability to appreciate underwriting risk, customisation of product, accuracy of pricing and product innovation. Some other respondents pointed potential advantages to consumers including better pricing through greater competition and in specific cases the ability to get cover for previously uninsurable risks.

With regard to the challenges to the widespread use of new technologies in insurance services, most respondents pointed out to the risk of exclusion and unaffordable pricing. A consumers' association pointed out the correlation between poverty and the status of health and that poor consumers may be completed excluded from accessing financial products. Many respondents identified that customised insurances based on sensor data, were contrary to the traditional concept of solidarity and risk mutualisation in insurance. Surprisingly, one mutual association opined that customisation can coexist with the principle of solidarity. Some respondents highlighted the increase in cyber risk due to increased connectivity and significant volumes of data collected. Some private individuals felt that individuals may be led to believe the need to share more data than necessary, whilst others recognised that citizens may not be aware of the data collection. Data ownership and sharing came across as a key area of concern besides the expectations on the ethical use of data collected by insurers and others (e.g. car manufacturers).

Many respondents do not consider a policy intervention to be necessary. However, the most important areas where the EU could play a role were identified as (1) ethical use of data and (2) addressing the risk of exclusion of citizens due to the information asymmetry between citizens and insurers.

Question 1.10 - Are there already examples of price discrimination of users through the use of big data? Please provide examples of what are the criteria used to discriminate on price (e.g. sensor analytics, requests for information, etc.).

Total respondents to this question	125
Yes	**28**
No	21
Do not know	76

To the question whether there are already examples of price discrimination of users through the use of big data, few respondents contributed and those respondents provided mixed views. The vast majority of respondents mainly referred to the insurance sector to provide for examples of price discrimination of users through the use of big data.
According to most respondents from the categories of private individuals and public authorities and international organisations, the use of big data might allow insurance companies to achieve a more efficient risk pooling, better differentiation and premium optimization based on the behaviour of the insured person (for example, "pay as you drive" car insurances). However, whereas this might bring financial benefits to consumers in terms of lower premiums paid, there was also a general concern that certain categories of consumers might be discriminated because of sex, age, location and risk profile resulting in higher premiums and in extreme cases even leading to exclusion. Hence, adequate legislative and regulatory frameworks need to be in place to prevent excessive tariff discrimination.
Within the category of companies and organisations, the large majority of respondents expressed similar opinions in terms of potential advantages and disadvantages and provided several examples of price discrimination and criteria used to discriminate on price associated to the use of big data:

- Pay as you use insurance policies;
- Telematics tariffs based on sensor data (car insurance: telematics devices which measures various aspects of how, when and where a car is driven; health insurance: wearable devices which measure the healthiness of the life style, e.g. minutes of activity throughout the day, hours and quality of sleep; home insurance: several home connected devices which help reducing the probability of the insured event to happen and reducing the loss in case the insured event happens);
- Pricing and service differentiation for clients tiered based on information available (e.g. trading clients differentiated based on their relationship and business size);
- Retailers (for example travel sites) changing prices due to usage of end devices, time and geo-location.
- Price setting for insurances based on factors such as gender and wealth;
- Credit card companies assigning a higher credit default risk to consumers who use their card for marriage counselling or therapy;
- Insurance companies taking individual online shopping habits or perceived tolerances for price changes into account when setting premiums;
- Customized marketing and better targeting of financial products and services, improved "know your customer" (KYC) process, improved intelligence on cyber risks;
- Risk-based pricing of loans.

Key issues identified by respondents relating to the impact of the use of big data, concerned the reduction on risk pooling, which might fundamentally alter the structure of the insurance industry (i.e. granular segmentation based on big data might undermine the mutualisation of risks and put in danger the economic and social usefulness of insurance), the weak level of transparency in risk profiling, the risk of privacy unravelling (e.g. consumers obliged to pay higher premiums because unwilling to disclose personal private information) and the aforementioned exclusion risk.

The main solution identified by respondents is to ensure that adequate regulation is in place to protect consumers. European General Data Protection Regulation (GDPR) and MIFIDMIFID were quoted as examples by some stakeholders.

Question 1.11 - Can you please provide further examples of other technological applications that improve access to existing specific financial services or offer new services and of the related challenges? Are there combinations of existing and new technologies that you consider particularly innovative?

Total respondents to this question	127

Many respondents provided answers similar to the answer they provided on question 1.1 on what FinTech applications they used, confirming that in addition to enhanced customer experience, competition, convenience, efficiency and lower costs, improved access to financial services is one of the reasons why respondents use FinTech. A number of respondents noted that these technologies would contribute to financial inclusion.

FinTech is seen by the large majority of respondents as contributing to improving access. Technologies and applications most often mentioned in this respect were mobile devices and applications running on them, robo-advice, machine learning, data aggregation, distributed ledger technology and cloud computing.

Many respondents referred to the potential of technology to remotely identify customers or counterparties as an important advantage. At the same time remote identification and identity verification and management, in particular in a cross-border context, was referred to as an important challenge. FinTech required digital on-boarding. Technologies exist and are being developed to implement such on-boarding, but requirements governing identification such as Know Your Customer and Anti Money Laundering requirements were most regularly referred to as challenges.

SECTION 2 - BRINGING DOWN OPERATIONAL COSTS AND INCREASING EFFICIENCY FOR THE INDUSTRY

Question 2.1 - What are the most promising use cases of FinTech to reduce costs and improve processes at your company? Does this involve collaboration with other market players?

Total respondents to this question	141

The majority of responses mentioned Distributed Ledger Technology (DLT) or blockchain as a promising technology in conjunction with a broad swathe of use cases, such as integrating KYC and identity management into DLT networks, improving asset management and trading processes through smart contracts and confirmations, use of smart contracts for automated management of claim procedures and related payments, escrow, timelock, data protection and data immutability, cryptographic data lineage tracking, system automation through smart contracts, potentially bringing enhanced transparency, making it much easier for issuers and regulators to identify shareholders, bondholders and other investors; Internet of Things, autonomous payments on the blockchain, tokenisation, programmable money, improving post trade infrastructure, increasing security and efficiency while lowering costs, managing the settlement of start leg repo transactions, recordkeeping and managing financial agreements, transfers of assets between parties without depending on a trusted intermediary to provide centralization of data or workflows, ensuring transaction integrity and acting as a common framework for management of collateral across multiple CCPs and bi-lateral engagements, freeing up unused collateral; minimizing the need for reconciliation and improving audit accessibilities, updating and replicating data in real time, and automatized travel insurance. DLT/Blockchain was described as a solution for Know Your Customer (KYC) and Anti Money Laundering (AML) compliance challenges, including controlling KYC costs by identity management enabled by a blockchain, and to enable client and investor on-boarding.

RegTech was frequently mentioned, as were systems for reporting and/or exchange of information between market participants and public authorities. New API (Application Programming Interface) technologies can also ease relevant IT savings. Many respondents mentioned cloud services, including for cost-effective access (scalability) to greater computing power leading to increased availability of data and faster data processing. Robo advisers, robotics, machine learning and artificial intelligence, cognitive automation, automated advice, advanced data analysis techniques and robo investing were referred to by respondents, including for regulatory surveillance. The potential of FinTech for the insurance industry was highlighted. Big data and data analytics for detecting fraud were cited. A challenge identified was that a basic infrastructure for DLT has not materialised. Respondents stated that placing existing infrastructure or processes on blockchain enabled platforms and ecosystems is a complicated, uncertain and expensive process given the nascent state of the technology.

It was stated that the EU could play a vital role in defining standards in the areas of: identity, payment messages, account and transaction information exchange, credit standards, development innovative technologies and products. Several respondents claimed that collaboration among market participants is necessary to develop standards aimed at fostering interoperability. The Internet Engineering Task Force (IETF) was cited as an example of positive cooperation on technical standards to ease interoperability.

For the respondents collaboration between FinTech Start-ups and the financial industry is already underway and the case of FinTech partnering with banks often emerged. The role of incubators was mentioned. A need for collaboration with other market players was stated. DLT's potential for collaboration with other market players and public authorities, including competent authorities under financial regulations was signalled, as was DLT / Blockchain in conjunction

with APIs enabling the possibility of increasing communication and services between various sizes of enterprise. Collaboration with other market players was said to be indispensable to achieve major cost reduction and efficiency gains. The potential of FinTech to increase financial inclusion was also mentioned. Human –AI Collaboration: a respondent stated that artificial intelligence can help monitor market movements more efficiently and be used in making recommendations. However, human intervention will still be needed, making judgement calls.

Public Authority or International Organisation RegTech innovations, Compliance and Disclosure, CDD and client on-boarding through the use of shared CDD facilities, product advice tools developed for financial advice for increased efficiency were cited by respondents. An example was given of a Ministry of Finance automating the issuance of treasury loans through a smart contract, storing relevant data in a blockchain. Work on a framework for a national regulatory sandbox was cited. Obtaining financial information about entities under investigation for tax evasion and for official receivers to obtain financial information about property of companies in liquidation were named as use cases.

Private individuals saw AI , cloud, Big Data and DLTs/blockchains as promising and signalled possibilities for voluntary collaboration and cost savings in relation to eID, Anti Money Laundering (AML) , data protection, and open API and partner integration, and rethinking business processes.

Question 2.2 - What measures (if any) should be taken at EU level to facilitate the development and implementation of the most promising use cases? How can the EU play its role in developing the infrastructure underpinning FinTech innovation for the public good in Europe, be it through cloud computing infrastructure, distributed ledger technology, social media, mobile or security technology?

Total respondents to this question	149

Respondents put forward a great many varied ideas about the different ways the EU could play a role in facilitation and development of FinTech innovations.

On the one hand, a number of respondents cautioned against premature regulation, arguing that further assessment of the nature of new risks emerging from FinTech is required. They viewed the primary role of the European Commission as responding to issues, rather than instigating or devising new technical solutions. On the other hand, there were also calls for the EU to develop a harmonised, market-driven, lighter, proportionate and more flexible regulation, with lower entry barriers, adjusted to fit the new digital reality, technologically neutral and sufficiently future-proof for the digital age. Many respondents stressed the importance of ensuring a level playing field across potential competitors or sectors, and ensuring appropriate investor and consumer protection so as to ensure a sufficient degree of trust.

Concrete suggestions for regulatory actions included:

- The development of a FinTech passport to allow FinTech companies to implement their business models that do not necessarily fit into existing regulatory frameworks;
- Fostering the development of start-ups by establishing calibrated rules to encourage new entrants;
- Developing a definition of "Digital Assets" in EU law to clarify how digital assets would embody counterparty obligations, facilitate individual transfers of title and constitute ownership in the court of law.
- A dedicated pan-European peer-to-peer lending and equity crowdfunding legislation

Considerable support was expressed by many stakeholders for sandboxes/innovation networks - a framework of experimentation where products and services can be tested, allowing regulators to understand practically how regulation needs to change, and calls to clarify the discretionary power of Member States under the current EU regulatory framework. There was also a suggestion that the EU should encourage competent authorities to exchange information and experiences with new regulatory tools aimed at supporting innovation and calls for global cooperation between regulators.

Many respondents raised issues related to distributed ledger technology (DLT), with calls for EU level coordination and clarification about where supervisors deem the use of DLT to be acceptable. It was also suggested to further elaborate how certain EU rules (e.g. Financial Collateral Directive, Settlement Finality Directive, etc.) are applied to new digital assets such as ‘crypto-securities’, or that the EU could envisage the use of DLT for regulatory reporting, or that smart contracts could be fostered, backed by legal recognition when opposed to third party interests.

A number of stakeholders wished to see the EU play a leadership role to develop common standards, in particular for DLT, but also e.g. the streamlining of procedures for security incident reporting (cybersecurity). It was suggested that the EU could promote operability, or an EU-wide standard (Open Banking APIs) to enable an infrastructure to support innovation in the financial services sector; or defining the rules for segregation of access, network security, data protection, incident response, portability across providers, etc..

There were suggestions from a number of stakeholders of a role for ESA's, for example monitoring financial innovation to guard against unnecessary burdens. Several stakeholders mentioned EBA work to analyse current supervisory cyber security practices in Member States, as well as the upcoming EBA recommendations on outsourcing to cloud service providers, with calls to harmonize regulations on outsourcing of financial processes and the underlying technology.

With respect to AML/KYC, several stakeholders supported EU action: suggestions included clarification by supervisors about the interpretation of requirements in current legislation and facilitation of full digitisation and simplification of on-boarding procedures, notably through the use of e-Authorization and e-Recognition and KYC portability.

There were a number of suggestions about how the EU could provide funding in the area of FinTech, for example through a cross-sectoral, collaborative and multi-stakeholder approach, including universities, research centres, large, small companies and start-ups to better transform innovative ideas into market ready solutions; funding academic and industry collaboration on cyber-security at EU level; or employing EFSI funds to build the underlying infrastructure for cloud computing and distributed ledger technology.

With respect to EU data protection rules, some stakeholders called for uniform application of the GDPR and clarification of solutions which are compliant with EU rules (e.g. guidelines on anonymization and pseudonymisation)/need for data to be located within the EU/allowing the possibility share to sensitive information related to fraud & cyber-attacks). Also raised was the need to address risks resulting from open data, and the need to establish clear principles with respect to the roles and responsibilities of each individual participant in a chain.

In the area of payments, it was suggested that the EU should look to update, and improve access to vital payment infrastructures and ensure the interoperability of SEPA payment solutions to allow cross-border financial retailers to adopt a single standard across the EU.

Question 2.3 - What kind of impact on employment do you expect as a result of implementing FinTech solutions? What skills are required to accompany such change?

Total respondents to this question	131

Most respondents expected an impact of FinTech solutions on employment in the financial services sector although there is no agreement on its magnitude. The outlook of the impact is expected to be overall negative in the mid-term but it will also create new jobs and could thus turn to positive in the longer term. Several respondents point to the fact that the impact of FinTech solutions is not envisaged to be different from previous technological revolutions.

Job losses are foreseen to be mostly due to process automation and a strong decrease in traditional front- and back-office jobs and operations in financial services. Other job profiles such as those providing specialised advice are expected not to suffer job losses. Job creation is envisaged to happen due new products serving currently unmet needs but also less expensive and thus more affordable services. Digital technology allows a better understanding of customers and reach, increased productivity and lower barriers to entry.

Many respondents expect that the advent of FinTech induces a strong change in the tasks, roles and thus the required skills of employees. There is a massive need to re-train and up-skill the workforce. As one respondent put it: "*FinTech is redefining the job of a banker*". A new set of skills are needed for the workforce of the future but also for those managing the transition. The combination of technology and human e.g. using a mix of automated advice and human advice will require that staff learns to make the best use of software, artificial intelligence and digital technology more generally.

The job profiles of the future in this sector will require a higher level of digital skills for all employees and also result in an increasing need for digital experts such as software developers, cyber security and social media experts, big data analysts. But also many new sector-specific job profiles will emerge. Several respondents highlighted that these changes are not only a matter of skills but also of attitudes and mindsets. In this vein, it is important to understand clients' expectations, to assist and guide customers and to be able to adapt the offers accordingly. These actions require human interaction, flexibility and capacity to react, critical thinking, innovativeness, creativity and autonomy. Also managers need to be able to "think and act digital" to be sufficiently agile to respond to the disruption of their businesses and initiate the re-skilling of their staff.

Finally, several respondents point out that the automation of certain routine tasks can also lead to more fulfilling jobs. Some respondents also expect an increase in less stable and contract-based working relationships whereas others point to the possible benefits of more flexible working arrangements.

Question 2.4 - What are the most promising use cases of technologies for compliance purposes (RegTech)? What are the challenges and what (if any) are the measures that could be taken at EU level to facilitate their development and implementation?

Total respondents to the open question	143

A large majority of private sector organisations or companies noted that the most promising uses of RegTech lay in ways to reduce compliance costs and make internal risk management and compliance systems more efficient regarding requirements for anti-money laundering, know-your-client, fraud and market abuse detection etc. For example, big data, biometric technology and artificial intelligence (AI) could help identify high risk clients. Supervisory reporting could also be streamlined and real-time oversight facilitated via applications using Distributed ledger technology (DLT), cloud and APIs, but this prospect was acknowledged by many firms to be further off. Several respondents also pointed to the use of some technologies to improve risk-modelling and make it more predictive for the purposes of prudential requirements. A few stakeholders mentioned the use of technology for internal compliance training purposes and as a way to limit the need for physical on-site supervision by authorities.

Among public authorities, the majority welcomed the prospective uses of RegTech in terms of automating areas of reporting and compliance and scaling and generating new regulatory uses from bigger data sets including AI and big data as a way to improve overall efficiency, improve user-confidence in the long-run, and reduce costs. However, some noted that this should not be at the expense of regulatory aims such as prudential safety or investor protection. The few private individuals who replied noted the use of AI in improving oversight and the prospect of more efficient KYC procedures from the application of various RegTech solutions.

In terms of challenges which possible EU measures could address, a large majority of private sector organisations said that policymakers should adopt a supportive approach to RegTech as a way to encourage take-up by industry and to improve efficiency and reduce costs. A large majority urged policymakers to work towards an enhanced pan-EU electronic identification framework and towards greater harmonisation of reporting requirements and standardisation e.g. of identifiers for all financial instruments. A sizeable minority were in favour of setting up regulatory fora to discuss the uses of RegTech between incumbents, RegTech companies and authorities, while some stakeholders urged going further in the shape of setting up a European innovation lab or RegTech sandbox hub. Some stakeholders recommended that authorities design machine-readable one-stop-shop databases, e.g. based on a taxonomy developed together with industry, and containing all up-to-date regulation which firms have to comply with. A few stakeholders suggested that authorities issue guidelines for when RegTech solutions e.g. for outsourced-functions are considered to be fully compliant or that they certify RegTech solutions as compliant with the rules. Very few stakeholders mentioned that supervisors should develop and use algorithms to carry out oversight as a way to cut on-site supervision costs while some others suggested to improve sharing of information on cyber threats between private and public bodies.

The majority of public authorities welcomed an open dialogue on RegTech with industry to encourage uptake and to coordinate with other authorities to ensure a consistent attitude towards the use of RegTech-solutions for compliance purposes. Some saw merit in opening a discussion on whether increasing reliance on RegTech should mean that they should fall within the perimeter of regulation. Some authorities noted that reliance on RegTech does not absolve the regulated entity of its compliance requirements. Some saw a potential risk in a future marked by excessive reliance on a few RegTech providers, in terms of their vulnerability to cyber threats or a concentration of outsourced compliance functions from a wide range of firms, including if these RegTechs were based in third countries.

Question 2.5 – (2.5.1) What are the regulatory or supervisory obstacles preventing financial services firms from using cloud computing services? (2.5.2) Does this warrant measures at EU level?

(The assessment of the responses is provided based on the two sub questions of question 2.5 – respectively 2.5.1 and 2.5.2)

(2.5.1)

Total respondents to this question	120

(2.5.2)

Total respondents to this question	129
Yes	**60**
No	18
Do not know	51

(2.5.1) The vast majority of respondents expressed concerns about:

- the lack of certainty and guidance regarding the use of cloud services in financial services;
- the fragmentation and lack of harmonisation between national rules or in the interpretation of EU rules by national regulators/supervisors;
- almost all those who expressed concerns mentioned various issues around data: for a large majority, concerns related to: the handling of personal data and fragmentation in interpreting regulation (GDPR), data localisation restrictions for both personal and other data (some mentioned explicitly data ownership), and a sizable minority also addressed data issues arising at international level (e.g. international agreement with US / safe haven was questioned by a few respondents as being no longer relevant). Respondents also stressed the sensitive aspects (if not secret) of data handled by banks or insurance firms (while the main Cloud Service Providers (CSPs) are based in US).
- for the majority (but less compared to respondents highlighting data issues), strong concerns about security were raised: the risk of data-breach was perceived as the main obstacle preventing the use of cloud services by financial institutions. A few stakeholders (including CSPs) noted that security may be better ensured through cloud rather than traditional IT services.

A significant number of respondents called for guidelines, certification, or standardisation of contractual conditions to ease partnerships/contracts with cloud service providers. The need to ensure audit imposed by regulation was stressed as a specific and complex issue hampering the use of cloud services. Respondents (sizeable minority) expected a more pro-active and flexible attitude of CSPs to take into account the specific regulatory constraints of financial institutions (e.g. data localisation, audit obligation) and considered CSPs could adapt their offer and contractual conditions in that context. Some respondents noted the improvements already made by CSPs in this respect. The market concentration of Cloud service providers (with US predominance) was noted as another source of risk or of lack of flexibility authorities should address.

(2.5.2) Some respondents were more in favour of a rather light intervention at EU level, while others called for stronger intervention to ensure legal certainty and harmonisation in using cloud services. Suggested measures ranged from (i) clarity on risk management (but allowing market

participants to focus on appropriate control and process); (ii) overarching principles/ generic obligations to be done at EU level, but real guidance to come from supervisors in each MS; (iii) minimum guidance on cloud services implementation; treating cloud services arrangement like typical outsourcing ones; (iv) ESAs to develop an approach for requirements for cloud services, that should become standards for international cloud computing agreements.

It was also proposed to define a clear minimum set of contractual obligations for each regulatory requirement at EU level, to guarantee security and confidentiality measures contractually (in particular with warranties and responsibility insurance and protection), to remove data localisation restrictions or to ensure that data localisation rules are not disproportionate or unjustified (enshrining the principle of free flow of data), to strike the right balance between data protection for citizens and business opportunities, in particular for new FinTech firms. Companies must be allowed to request or provide data localisation.

One CSP called for a harmonised approach to obligations contractually imposed on CSPs (auditing, reporting and reversibility of services but also to move away from overly prescriptive rules), and for financial Institutions to make their own informed decisions on outsourcing.

Other suggestions included:

- Audit/certification/labelling process for Cloud services warranting conformity with EU regulation (going a step further for liability – FS firms could not be held responsible for regularity breach when using a certified power);
- A "reverse" regulatory approach (i.e. Cloud services providers would have to get a licence for offering services);
- Standardisation efforts should be supported regarding contractual clauses for cloud services.

For others, a consistent supervisory/regulatory approach should be proposed with harmonisation of implementation schemes, notably to cover cyber security (ensuring that the implementation of the NIS directive will not impose diverging obligations for CSPs in different MS), data protection, physical security, business continuity. It was suggested that ECB should play a role for the homogenisation of requirements and assessment criteria. It was also considered that an EU central policy should be established with no extra requirement imposed at MS level.

The need to speed up cloud adoption in Europe and stimulate competition between CSPs (to ensure possible migration and avoid single point of failure) was underlined, as well as the need to develop expertise in regulatory supervisory bodies. It was suggested to revise through an omnibus directive NIS / MIFID and the ENISA mandate to facilitate the use of cloud services. Moreover, it was noted that there is a lack of international sanctions to counter foreign intelligence and that the EC should reinforce agreements regarding data protection in trade negotiation; it was also suggested that a research group be created to look into "virtual ongoing supervision".

Question 2.6 – Do commercially available cloud solutions meet the minimum requirements that financial service providers need to comply with? Should commercially available cloud solutions include any specific contractual obligations to this end?

(The assessment of the responses is provided based on the two sub questions of question 2.6 – respectively 2.6.1 and 2.6.2)

(2.6.1)

Total respondents to this question	126
Yes	**39**
No	24
Do not know	63

(2.6.2)

Total respondents to this question	121
Yes	**51**
No	20
Do not know	50

This was considered as an important question with no large majority able to express a clear answer to it. A sizable minority considered that commercially available cloud solution meet such minimum requirements. A majority considered they do not or only partially, noting at the same time the lack of clarity on what those requirements are, and the good progress made by Cloud Service Providers (CSPs) to adapt their offer. Respondents praise the role of public/competent authorities to help clarifying the conditions for using cloud services.

A majority of respondents showed interest in using cloud services, but stressed that many uncertainties remain regarding: concrete list of requirements, the lack of harmonisation across Europe, the lack of certification schemes and pro-active attitude of CSPs to cover all requirements. Therefore, using cloud services was considered by to still depend too much from the capacity of CSPs to adjust to specific conditions, with explicit doubt expressed by some stakeholders.

Divergences in the offer of CSPs was also noted, not all CSPs were consider to be on the same level of elaboration concerning cloud offers for Financial services), as well as the difficulty (regarding resources and expertise) to ensure that all requirements are met by CSPs. Some respondents stressed the importance of being able to ensure competition and to change (easily) of CSPs and that the concentration of offer around a few CSPs was a concern. Some stakeholders explained their interest to go now for hybrid approaches (part of services still in house and the use of public cloud solution to be tested for services representing limited risks).

Security was noted as an important concern but some highlighted that CSPs are better equipped than financial institutions to address security challenges. The main issue expressed by a majority concerned data, and their location. The fact that data and servers would be located outside Europe and the implications regarding the lack of compliance with EU rules, which rules would apply and on how to ensure access to data to national supervisors, was underlined. A few stakeholders explicitly praise the need of having a European cloud offering. The case of audit was also a subject for clarification, with progress expected to be achieved through work on certification or standardised clauses in contract with CSP.

A sizable minority considered that existing requirements are sufficient to use cloud services and that the offer is good enough, but it is up to the financial institutions which are under direct supervision to ensure that CSP solutions are compliant with those requirements. Reference were made to a few working schemes (e.g. the Trusted German Insurance Cloud)

CSPs (representing a few of the respondents), noted that not all the requirements are listed, stressed provisions already existing in their contracts to ensure compliance with prudential rules, considered that GDPR and NIS would bring a higher and more harmonised level of protection and that CSPs would help notably through existing solution to facilitate reporting for compliance. They noted also progressed towards certification (Reference to ISO27001)

The majority of respondents answered affirmatively to the second part of the question. The minority who was not in favour on including any specific contractual obligations regarding minimum requirements that financial services providers need to comply with insisted on the need to comply with data and rules through agreements with CSP. For a few stakeholders, a non-clear distinction emerged between standard contractual obligations and specific contractual obligations.

A large majority of stakeholders stressed that attention needed to be paid to data and data protection rules. Security-issues emerged as concerns, but comparatively lesser than data issues. Some stakeholders insisted on the compulsory need that data and cloud servers should be located in the EU (or EEA). The need to properly ensure audit was highlighted.

A large majority of respondents considered that CSPs should guarantee the proper implementation of data, security as well as transparency rules, facilitate audit and regulatory compliance or reporting; a sizable minority reminded that in any case the regulated financial institutions had to remain liable vis à vis supervisory authorities.

Some considered that existing outsourcing rules and regulation are sufficient for guiding the contractual conditions required for cloud services.

The CSPs (representing just a few of respondents), with a few other stakeholders, considered that "*Many of the issues being considered in this area are already covered by existing legislation on security requirements and data protection. Standard contractual rules cannot be seen as a silver bullet, many of the solutions are already provided by CSPs who are thoroughly covered by both financial outsourcing rules and legislation such as the NIS Directive and the GDPR*". Flexibility is more important than standard contractual obligations. CSPs also invited FIs to work on checklists that could be used for ensuring that all requirements are taken into account for making their own decision when using cloud services.

References were made to existing works and guidelines were made for IT, UK, US, HK and Singapore.

Question 2.7 – Which DLT application are likely to offer practical and readily applicable opportunities to enhance access to finance for enterprises, notably SMEs

Total respondents to this question	122

The overwhelming majority of respondents to this question were from an organisation or company, and most were convinced that DLT offered opportunities in many different areas (not only in relation to enhancing access to finance for enterprises). While many respondents pointed to the fact that the technology is still at a very early stage of development, some respondents pointed to projects that have already been tried out (e.g. registering instruments used in start-up financing transaction, or facilitation of the first-ever blockchain issuance of securities between an investor and issuer).

Among the advantages cited by stakeholders were: the potential to accelerate, decentralise, automate and standardise data-driven processes and therefore to alter the way in which assets are transferred and records are kept; immutability of data - with enormous potential for trust, efficiency and legal certainty; increased data security, enhanced reporting, and real-time auditability.

Among the potential use cases, respondents provided many concrete examples under development or contemplated across many different sectors of financial services, such as:

- **Securities**: issuance; trading e.g. use of blockchain for the transmission and representation of certain financial securities; development of a secondary market for non-MiFID financial instruments, such as projects published on crowdfunding platforms; smart contracts which can automate the post-trade workflow of OTC derivatives trades. Every single step of the post-trade lifecycle can be coded into smart contracts: matching, confirmation, valuation, netting, collateral management, compression, payments and even default management.
- **Unlisted securities** markets have parts that are small enough to be used to start tests on an EU scale: business is very paper intensive and could benefit from full automation.
- **Payments**: crypto currencies, whereby digital currencies and tokenized assets can facilitate payments and contracting across borders with low transaction costs; automated international payments within territories which are not part of the SEPA; micropayments.
- **Insurance**: DLT could facilitate the creation of new products with very low operational costs, enable new models for sharing, distributing and funding risk - coupling DLT with smart contracts; and automated claims handling.
- **AML/KYC**: automation of simple processes such as recording client data for Know Your Customer and AML purposes. A widely accepted KYC registry leveraging blockchain may make it easier and simpler for SMEs to get access to financial services.
- **Record-keeping**, particularly for unlisted companies which tend to keep records manually.
- **Reporting:** DLT could be beneficial for reporting officers, risk managers and regulators: by posting information to a DLT and providing regulator access, regulatory reporting activities could be eliminated, thereby placing control over data enquiry directly in the hands of the regulator.
- **Trade finance** - providing advantages in terms of time reduction, costs and trust of the system.
- **Initial Coin Offerings (ICOs)** – DLT can enable a new way of raising capital, whereby issuers sell stakes in start-up projects to investors in exchange for relatively liquid crypto-currency. These crypto-currencies may then be converted to fiat currency to finance operations.
- **Crowdfunding**: raising seed or venture capital via online platforms may improve efficiency (by disintermediating banks and/or VC funds). It would be possible to tokenise the

investments into companies via a platform, allowing for quicker, more efficient access to capital for enterprises (including SMEs).

- **Security**: the distributed nature of DLT has the potential to reduce the single point-of-failure risk, if a node is inoperable the other nodes can continue the processing of transactions; encryption protocols also offer higher degrees of security.
- **Central bank money**: central banks might be part of some ledgers, issuing central bank money and allowing settlement in central bank money within the DLT.
- **Digital identities**: DLT could be used for the management of digital identities based on already existing global standards, such as the Legal Entity Identifier (LEI).

Specifically in relation to SME/enterprise funding, the example of a consortium of European financial institutions which is exploring the development of a post-trade blockchain infrastructure for SMEs in Europe with the aim to improve SMEs' access to capital markets while facilitating secure and transparent post-trade operations, was cited several times.

A number of other opportunities for SMEs offered by DLT were also mentioned:

- Improved access to liquidity and strengthened investment flows into SMEs.
- Providing SMEs with an easier way to register their securities and the opportunity to follow in almost real-time their shareholder base, since DLT offers the opportunity to develop a decentralised security registrar potentially accessible directly to issuers and investors;
- Enhanced attractiveness of SMEs towards investors by reducing transaction costs through the simplification of the transaction processing chain.
- A single source of information where SMEs can share their financial data (in compliance with existing regulation, starting from GDPR) in order to help financial institutions to better assess their credit risk and thus make it easier to access banking services.
- Interesting applications for SMEs in trade-finance and invoice prepayments.

Question 2.8 - What are the main challenges for the implementation of DLT solutions (e.g. technological challenges, data standardisation and interoperability of DLT systems)?

Total respondents to this question	133

Half of the respondents answered this question. Even if DLTs are considered as a breakthrough, most stakeholders think that, in practice, their introduction will be evolutionary rather than revolutionary.

A vast majority of the respondents identified (data) standardisation and interoperability of DLT (among each other and with the legacy infrastructure, running both systems in parallel) as a challenge, regardless of the category of respondents. Scalability to achieve high volume processing and low latency are among the most common challenges, notably mentioned by a majority of private sector stakeholders (banking and insurance industry, market infrastructure stakeholders).

Development and legal enforceability of smart contracts (and the definition of a general legal framework) are widely mentioned, as well as compliance with EU laws, especially GDPR. Some stakeholders highlighted the complexity of the DLT world and its overall acceptance (by market parties and users) and a number questioned its user-friendliness beyond digital currencies. The early-stage development phase (and limited functionalities of DLT) was mentioned as a possible impediment to a quick uptake.

Public authorities, regulators and supervisors offered consistent views on the challenges, considering that a lack of regulation (especially for DLT interfaces with the real world use cases), legal validity of smart contracts and tokens, liability and rights of the participants, (lack of) governance frameworks and adequate agreements regarding maintenance and obligations of the DLT networks, confidence in the cyber resilience of DLT and compliance (especially with the GDPR and KYC) are the main challenges.

One regulator suggested that the Commission should follow up on the work on standardisation (ISO TC 307). Interoperability between DLT and with legacy systems has to be supported. One supervisor proposed that national and European regulators should carefully assess potential impacts that DLT may have on consumer protection schemes, in particular on data protection obligations, in order to limit negative consequences arising from this technology on consumers . Another supervisory authority believes that DLT could bring a number of benefits to securities markets, for instance by facilitating the issuance of securities by SMEs or the record of ownership of unlisted securities. No major impediments in the existing EU regulatory framework have been identified.

Identity and authentication are crucial elements for DLT to become a trusted source of immutable and authenticated data; the recognition of ownership/proof of existence (probatory value) will need global alignment, as well as territoriality issues. The ENISA paper was mentioned several times especially in relation to cybersecurity problems (key management, cryptography, vulnerabilities in the code, sidechains, Distributed Denial of Services) and for AML and anti-fraud tools to combat illegal activity, at the possible demand from supervisors.

A particular challenge will be to find a business model where the technology would prove to be considerably cheaper or bring sufficient benefits, including security and effectiveness (new applications bringing additional value), which would justify investments.

Several stakeholders shared their views and recommendations on how DLT is likely to impact financial services. In particular, it was felt that DLT could hold the benefit to facilitate the collection, consolidation and sharing of data for reporting. In the future, a coordinated roll out of DLT by a market infrastructure provider would ensure adoption by a large number of participants

simultaneously, allowing for network effects of DLT. Moreover, as standards would not be established in time, market-based solutions may include a commitment to the general necessity of interoperability. There is a need for extensive cooperation between financial institutions, tech companies and regulators. With regard to personal data, it was pointed out that DLT provides a fairly secure way of storing and managing information, which should enable the building of a truly effective framework for the protection of personal data.

With regard to the role that the EU can play, the EU could clarify the legal treatment of DLT technologies, opening up for speedier recognition of various solutions across the Member States and ensuring more rapid RegTech development. Moreover, discussion with and guidance from regulators regarding privacy options and solutions, guidelines for reversibility in case of error or fraud in a DLT environment, clarification about the nature and interpretation of digital tokens as well as the choice of the DLT, their consensus and their cryptology elements are all needed. Regulators will have to consider adapting the existing regulatory framework. Respondents also called for an 'experimentation sandbox' which relaxes some of the existing rules and regulations with respect to KYC, privacy and data security principles (of course with the explicit consent of the customer and in full transparency). EU authorities should have a key role in encouraging standards and driving collaboration, ensuring coordination within and between jurisdictions; increasing awareness about the need for harmonized technology standards and best practices; addressing the issue of who will establish and govern those standards; and enabling the creation of shared technical operational standards that are compliant with the various national regulations. Otherwise, different priorities from individual countries will limit the effectiveness and the establishment of shared standards and regulations (e.g. digital identity, sandbox and cyber security).

Question 2.9 - What are the main regulatory or supervisory obstacles (stemming from EU regulation or national laws) to the deployment of DLT solutions (and the use of smart contracts) in the financial sector?

Total respondents to this question	128

Most private individuals identified divergent national laws as an obstacle to DLT. Examples given include tax legislation or the enforceability of smart contracts.

Public authorities identified various issues, among which the question of the validity of smart contracts was raised, together with the classification of tokens exchanged on DLT – and suggesting the European Commission should define DLT-related terms. Standardisation and data protection were also cited by one public authority. In addition, some stakeholders, though recognizing this was rather a medium-term concern, indicated that some legislation may have to adapt in the future: CSDR, EMIR, SFTR, MiFIR. Finally, one public authority pointed to regulators'/supervisors' capacity to address new challenges brought by emerging technologies and called for *"new multidisciplinary teams with judicial, analytical and information technology skills"*

A large majority of organisations or companies provided similar views as previous categories of stakeholders and cited securities law, GDPR (right to be forgotten), enforceability of smart contracts, liability rules, standardisation, validity of blockchain elements, regulators understanding of the technology, but also governance of DLT networks as issues that should be addressed. Some stakeholders also referred to jurisdictions' diverging laws which created regulatory uncertainty: *"As DLTs have no specific location, each node in the network may be subject to different legal requirements"*. On the other hand, a sizeable minority of respondents acknowledged that DLT was still at an early stage of development and some stakeholders specifically referred to ESMA's report and conclusions that any regulatory measure on DLT would be premature in the short-term.

Independent from their category, some stakeholders spontaneously referred to regulatory sandboxes as a useful tool to overcome the identified issues and help regulators keep up with change.

Question 2.10 - Is the current regulatory and supervisory framework governing outsourcing an obstacle to taking full advantage of any such opportunities? - Please elaborate on your reply to whether the current regulatory and supervisory framework governing outsourcing is an obstacle to taking full advantage of any such opportunities.

Total respondents to the closed question	131
Yes	**58**
No	28
Do not know	45

The majority of private sector organisations considered that the current outsourcing rules are too rigid, time-consuming and constitute an obstacle to reaping the full benefits of outsourcing functions to FinTech firms (and RegTech firms). Specifically, the most common concern was that the rules are not up-to-date as regards the outsourcing of functions to the cloud, creating uncertainty and cost-inefficiencies as opportunities for providers to scale their services are missed. Several stakeholders also noted that Member States require different levels of reassurance over the effective control of the financial entity over the outsourced functions, while some noted that that supervisors' access to the company operating the outsourced functions is another layer of burden.

Some stakeholders also noted that the question of legal liability in case of problems with an outsourced function should be further clarified. However, many private sector organisations disagreed and argued that the current rules achieve the right balance in terms of permitting functions to be outsourced while ensuring that financial entities retain full regulatory responsibility for these operations. Among them, some noted that outsourcing in the FinTech area should not be treated any differently than for other types of business services. The vast majority of private sector stakeholders, on both sides of the argument, agreed that it would be useful for the EU/ESAs to update and clarify the relevant frameworks for outsourcing e.g. through guidance and in this respect several welcomed the recent EBA consultation on outsourcing to the cloud.

In contrast, almost all respondents among public authorities considered that the current framework was adequate and did not consider far-reaching changes to be necessary. However, several among them noted that updating existing guidelines made sense and some noted that new guidance could be developed for example to clarify specific questions of legal liability (e.g. use of Big data and misplaced advice).

Question 2.11 - Are the existing outsourcing requirements in financial services legislation sufficient? Who is responsible for the activity of external providers and/or increase their efficiency and of the related challenge?

Total respondents to the closed question	125
Yes	**58**
No	27
Do not know	40
Total respondents to the open question	104

A large majority of private sector organisations considered that the existing requirements were sufficient, stressing that there was little need to add to them. Several noted that GDPR and PSDII were two recent up-to-date developments which will bolster the objective of the requirements, even if they lack detail in some areas. Some private sector stakeholders welcomed that certain aspects of the functioning of the existing requirements could helpfully be clarified, e.g. as regards the division of legal liability in case of problems, the best means of access of supervisors and clients to cloud service providers, as well as the degree to which some external service providers who are closely entwined with financial institutions could fall within the regulatory perimeter.

However, a sizeable minority of private sector stakeholders commented that the problems in the existing outsourcing rules mentioned in reply to Q2.10 should be addressed, and that the requirements are therefore not sufficient. This was noted to concern e.g. the disparities in the way Member States apply the requirements, the absence of up-to-date rules regarding external cloud and other FinTech providers, and the fact that the rules are not sufficiently tailored to account for the different types of services which can be outsourced. Some consumer organisations noted that the chain of liability of external providers should be clarified and that the responsibility of the firm should not be diluted.

The vast majority of respondents from among public authorities and private individuals also considered the existing rules to be sufficient. One public authority noted that the rules for banks lagged behind those for insurance and securities companies. One individual commented that the requirement that supervisors authorise outsourcing arrangements could be lifted for non-core services.

Question 2.12 - Can you provide further examples of financial innovations that have the potential to reduce operational costs for financial service providers and/or increase their efficiency and of the related challenges?

Total respondents to this question	93

The vast majority of respondents that replied to this question expressed a positive attitude towards the potential of technology to reduce operational costs or increase efficiency. Some respondents expressed neutral attitudes whereas only a few answers contained negative sentiments.

The technologies and financial innovations most referred to as having the potential to reduce operational costs or increase efficiency were cloud computing, robotisation and machine learning, application programming interfaces, distributed ledger technology and remote identification technologies.

Many respondents referred to the fact that any technology or application that removed the need for paper based communications, that allowed customers to 'self-service' and that supported straight through processing and avoided the need to reconcile accounts or require manual/human intervention were of a nature to reduce operational costs and/or increase efficiency. Some respondents did, however, also caution that full automation can have high initial investment and maintenance costs and that automated tools can have functional limitations. Hybrid approaches combining automation with human intervention were presented by some respondents as the best or most likely way forward.

Some respondents also referred to advantages or opportunities of technology related to regulatory compliance and the ability to reduce operational costs through automated compliance processes. Also enhanced fraud detection and analytics were referred to as advantages that reduce operational costs.

Very few respondents referred to particular challenges. Where this was the case the subjects most mentioned were trusted e-identification and Know Your Customer requirements.

SECTION 3 - MAKING THE SINGLE MARKET MORE COMPETITIVE BY LOWERING BARRIERS TO ENTRY

Question 3.1 – Which specific pieces of existing EU and /or Member State financial services legislation or supervisory practices (if any), and how (if at all), need to be adapted to facilitate the implementation of FinTech solutions?

Total respondents to the open question	151

According to regulators and supervisors, the current financial services legislation is overall and should remain technology-neutral and activity-based, hence ensuring a proper level playing field between market participants. However, further work may be necessary in certain areas without challenging these principles. First, some pieces of legislation may not be fully technology neutral since some current provisions could require paper disclosure, handwritten signatures or physical presence limiting therefore digital developments. Harmonised on-line identification processes, in line with AML requirements, should also be available across Europe. The scope of the Directive on Distance Marketing of consumer financial services could also be reviewed in light of FinTech developments. On licensing regimes, competent authorities underlined that the existing legislation is generally sufficient to cover existing activities and business models, but licensing regimes and supervisory practices in this respect could need to be further harmonised across Europe. One of the ESAs mentioned the on-going work on these issues for banking and payment activities. Some supervisors also spotted that the need to combine multiple authorisations to cover new business models could be very complex and such cases would need to be properly identified an discussed. On crowdfunding, some competent authorities reported that the absence of an EU framework could limit possibilities of development of a Single Market. Finally, it would also be useful to screen the current European legislation in view of upcoming developments for disruptive technologies such as DLT, AI and big data, and assess whether it is still technology-neutral. A number of supervisors also praised the innovation hubs and sandboxes set up at national levels.

A few consumers only responded to this question and mainly underlined the need to further harmonise rules and supervisory approaches across Europe. AML rules, but also disclosure requirements and marketing rules were mentioned.

On the industry side, many respondents underlined the broad scope of the question. As a result, a wide number of legislations were mentioned in the various contributions. First of all, the industry insisted that legislation and supervisory practices must be based on the "same activity, same rules" principle to respect the level playing field. On the technology-neutral principle, many respondents identified cases whether clarifications or even amendments may be necessary.

Clarifications are requested on a number of horizontal legislations, in particular on data, in view of the upcoming GDPR. Respondents raised issues in particular on the consistency between GDPR and PSD2 provisions. Many respondents also called for clearer and more harmonised rules regarding digital KYC processes, possibly leveraging on e-IDAS regulation as well as clearer guidelines on outsourcing to cloud providers. A few stakeholders called for a more harmonised approach as regards virtual currencies at EU level.

Regarding sectoral legislation, the industry respondents spotted a number of provisions which are not technology-neutral mainly regarding digital disclosure or handwritten signatures (e.g. IDD). On CRD/CRR, representatives from the banking industry called for changes on the prudential treatment of software as well as on the rules on remuneration. A number of respondents also referred to MiFID 2 provisions (e.g. suitability test, advice) and underlined that such provisions could not fit with some recent digital developments.

Question 3.2 – (3.2.1) What is the most efficient path for FinTech innovation and uptake in the EU? (3.2.2) Is active involvement of regulators/supervisors desirable to foster competition or collaboration, as appropriate, between different market actors and new entrants. If so, at what level?

(The assessment of the responses is provided based on the two sub questions of question 3.2 – respectively 3.2.1 and 3.2.2)

(3.2.1)

Total respondents to this question	139

(3.2.2)

Total respondents to this question	145
Yes	**108**
No	11
Do not know	26

With reference to the first sub question (3.2.1), the following 3 tools were mentioned most frequently:

- A significant minority of firms, organisations, and public authorities noted that key is to ensure open discussions and collaboration between the industry and regulators/supervisors;
- A significant minority of firms called for a level playing field, i.e. same activity, same rules, while taking into account risks proportionately;
- A significant minority of firms also asked for more ability to experiment (sandboxes). Very few respondents noted that testing should be regulated at EU level but delivered at national level. One firm suggested testing for policy making.

Very few stakeholders also noted that more harmonisation is needed at EU level, e.g. for AML and data protection (more regulations and less derogations). While others thought that regulators should really focus on prudential and consumer protection issues and not intervene in technology to avoid creating barriers to development. Very few thought that industry collaboration and market-led initiatives are in fact the best tools. Very few also discussed the need for a special regulatory regime for FinTech (e.g. a modular or tiered regulation) but very few were also specifically against this approach. There were also very few calls for principle-based, proportionate and technology neutral regulation and emphasising the importance of interoperability and open source. Importance of an ecosystem, infrastructure, VC funding and tax incentives were also mentioned.

108 stakeholders responded to the second part of the question (3.2.2). They found that active involvement of regulators and/or supervisors is desirable to foster competition or collaboration between different market actors and new entrants. 11 respondents disagreed and 26 had no opinion. When elaborating, very few public authorities, individuals and a few firms and organisations emphasised again the importance of open communication with regulators (e.g. through Innovation Hubs; one regulator had an interesting example) and facilitation of collaboration between all parties (e.g. through forums). A few firms asked for more space for testing, more harmonisation and co-operation between national authorities. Very few respondents emphasised the importance of consumer protection and 'same rules, same risk' approach. Very few firms also noted that an update of regulators skills is necessary. Certain authorities emphasised the conflict between fostering innovation and ensuring market integrity and consumer protection, and found fostering competition by them inappropriate.

Question 3.3 - What are the existing regulatory barriers that prevent FinTech firms from scaling up and providing services across Europe? What licensing requirements, if any, are subject to divergence across Member States and what are the consequences? Please provide details.

Total respondents to this question	135

Some respondents consider that there is no real obstacle for FinTech services to scale up their services across the EU. They reckon that current regulatory and supervisory practices are based on common principles applicable to all participants irrelevant to the fact whether such applicants are start-ups or not. If proportionality principle is applied, various factors such as size, complexity or systemic importance are primarily used in the current legislation. Other respondents also indicated that the Regulation should ensure a level playing field for companies engaging in similar activities, with similar risks, in any European countries. As a consequence, they consider that there should be no exception in favour of FinTech companies in the banking, insurance or capital markets regulations because this could contradict the objectives of the Single Market.

Different respondents underlined the challenges faced by crowdfunding platforms to grow cross-border. Some respondents underlined that equity crowdfunding platform can operate on a cross-border basis if such a platform are authorised under MiFID. However, they also highlight that some Member States consider that platforms must be authorised under their bespoke regimes to operate as equity crowdfunding platforms irrespective of the fact that they may have a MIFID passport. Regarding lending-based crowdfunding platforms, some respondents recalled that platforms need to obtain authorisation from the local authorities, if they want to provide their services in host Member States (as the EU passport under the Payment Service Directive (PSD) can never cover the full range of services provided by those platforms). Some respondents also mentioned that some obstacles can also stem from divergent interpretations of EU acts (such as Anti-money laundering – 'AML'- requirements and MiFID on investor classification and appropriateness test). Finally, different stakeholders also highlight that some barriers come from national rules (obligation for crowdfunding issuers to issue specific instruments such as subordinated loans, obligation for investors to create a specific tax number, obligation to draft loan contracts in a written form…). As regards crowdfunding, several stakeholders suggest the creation of an EU passport.

AML was often cited by respondents as a hurdle. Some respondents noted that the national implementing legislation and regulatory practice of the authorities with regard to cross-border activities is different from one MS to another. For instance, the documents to be collected are different and digital processes are difficult to implement in certain Member States. Finally, some respondents underscored that AML registration regimes vary a lot across the EU.

As regards MIFID II, one respondent indicated that some FinTech companies would like to use multi-tied agents. However, this solution would not be available if they are providing a MiFID regulated service.

Respondents expressed mixed views about the PSD regime. Some respondents highlight that PSD 1 has not been transposed uniformly into national law and favoured PSD 2 that should establish a level playing field for the payment industry. At the contrary, other respondents consider that PSD I allowed for national discretion as regards small payment institutions, while PSD2 would harm innovations in this field. Finally, one respondent argued that, with the ongoing innovation in the payment area, the frontier between e-money and payment services is blurred and raised interpretation issues when licensing such services. As a consequence, this respondent was in favour of merging PSD 2 and the Electronic Money Directive.

Some respondents also mentioned barriers arising from EU regulation, outside the financial sector. For instance, some respondents indicate that while the eIDAS regulation harmonises the notion of qualified electronic signature, it leaves the identification methods to Member States, which can give rise to divergence. Some respondents underline that there is a need for greater consistency in the application of rules relating to data governance and management of electronic data. Some respondents also mentioned the lack of harmonisation of regulatory approaches to cloud computing and to the existing regulatory gaps in the data filed (portability, accessibility and free flow).

Question 3.4 - Should the EU introduce new licensing categories for FinTech activities with harmonised and proportionate regulatory and supervisory requirements, including passporting of such activities across the EU Single Market? If yes, please specify in which specific areas you think this should happen and what role the ESAs should play in this. For instance, should the ESAs play a role in pan-EU registration and supervision of FinTech firms.

Total respondents to this question	152
Yes	**83**
No	45
Do not know	24

A few authorities responded to this question and these respondents had mixed views. Some authorities believed that there is no need for new licensing regimes specific to FinTech firms and underlined that the regulatory framework should remain activity-based and should not be linked to the type of entity or to the way of offering the service. Two financial markets authorities identified however the need for new licensing regimes for investment services. Together with a number of firms and consumer organisations, these authorities suggested that crowdfunding may require a more harmonised EU framework, including the possibility of passporting such activities. Besides, other gaps were mentioned such as digital asset managers, P2P lending, aggregators, comparators, brokers, invoice and supply chain finance.

On the industry side, many respondents highlighted the need for more harmonised rules and passporting regimes to enable European FinTech to scale across Europe. A number of firms noted that the regulatory landscape is already quite granular and therefore they do not see the need for new categories of financial services licenses. Others explained that they are not in favour of generic licenses which would de facto contradict the activity-based principle. The responses varied however depending on sectors.

The banking industry clearly underlined the need to guarantee a proper level playing field for all market participants through a true activity-based, technology-neutral and proportionate legislation. If the services provided are comparable to banking services, FinTech firms should be requested to get a full banking license. Some banks also noted that incumbents should also benefit from fast-track framework while trying to develop digital solutions on the market. Finally, banks underlined the need for all FinTech providers, whether banks or non-banks, to comply with same rules for consumer protection, data protection and cybersecurity. Payment service providers reported in general that current payment activities are well covered by PSD2, EMD and AML rules. On the insurance side, one respondent mentioned the possible need for new licensing regime to cover advice and intermediation including passporting rights. But most gaps seem to be concentrated in the investment services and non-bank lending activities. A number of firms, consumer organisations and national authorities favoured the establishment for a clear EU legal framework for crowdfunding. Besides, other licenses may be necessary to cover other currently unregulated activities and were mentioned in the consultation for instance aggregators, comparators, brokers.

Regarding the role ESAs could play, a number of respondents reported that ESAs may play a role in setting an EU-wide register of FinTech start-ups and supervising these new entrants. The ESAs could also promote the harmonisation of national regimes, issue guidelines on how certain new activities or business models can fit under existing regime and investigate the need for new licensing regimes to operate across Europe.

Question 3.5 – (3.5.1) Do you consider that further action is required from the Commission to make the regulatory framework more proportionate so that it can support innovation in financial services within the Single Market? (3.5.2) If you do consider that further action is required from the Commission to make the regulatory framework more proportionate so that it can support innovation in financial services within the Single Market, please explain in which areas and how should the Commission intervene.

(The assessment of the responses is provided based on the two sub questions of question 3.5 – respectively 3.5.1 and 3.5.2)

(3.5.1)

Total respondents to this question	150
Yes	**102**
No	17
Do not know	31

(3.5.2)

Total respondents to this question	78

The majority of the respondents were in favour of more proportionality in the regulatory framework for financial services and some of them suggested criteria that could reflect this proportionality (such as the business model, size, systemic significance as well as the complexity and cross-border activity of the regulated entities). Some respondents also indicated that the Commission must ensure that the current legal framework is technology neutral.

However, some respondents (notably from the banking industry) were more cautious about introducing more proportionality in the current EU regulation. They recall that firms providing the same services and thus entailing the same risks should be subject to the same rules and level of supervision, in order to preserve a level playing field among competitors. Other respondents also underlined that in some areas, such as data protection, anti-money laundering, investor protection and cybersecurity, the rules must be the same for all the market players. Finally, several respondents considered that sandboxes as a useful tool that can offer certain regulatory flexibility without jeopardising investor protection.

A few number of respondents actually mentioned areas in which the Commission should intervene. Few of them consider that some aspects (e.g. as regards prepaid instruments) of the Anti-money Laundering Directive ('AMLD') should be changed to make it more proportionate. For instance, one stakeholder underlines that e-money is considered (by the AMLD4's supranational Risk Assessment – SNRA) as 'high risk', in terms of exposure to money laundering and terrorist financing, while the real risk depends on several factors (such as anonymity, type of payment system…). Another respondent indicate that several Member States do not have the same approach in terms of identification procedure under AMLD 4 and ALMD5, which can cause distortion across the EU and create a competitive advantage for market players located in the less restrictive jurisdictions.

Few respondents also mentioned that the Capital Requirements Regulation is not favourable to FinTech operating in the banking sector or incumbent players using digital technologies. They consider that investments in software are penalized for banks in general, but especially in the case of institutions based in the EU, where the accounting treatment of software as an intangible asset causes it to be fully deducted from core equity when calculating the capital requirements.

Few respondents indicated that the Payment Services Directive II ('PSD2') could also be framed in a more proportionate manner, notably as regards the Strong Customer Authentication (SCA)

provisions. According to those respondents, the blanket application of SCA, regardless of the actual security risk of the service provided, would introduce undue friction.

One respondent also reckoned that more proportionality should also be introduced in the Solvency II framework for insurance companies. Some provisions would be too complex for smaller players operating in the insurance sector. This stakeholder calls for a review to examine whether insurers (with a simple risk profile and business model) could apply less complex requirements (notably as regards the governance system, the Own Risk and Solvency Assessment, outsourcing, review of the balance sheets and the qualitative and quantitative reporting requirements).

Question 3.6 - Are there issues specific to the needs of financial services to be taken into account when implementing free flow of data in the Digital Single Market? Please elaborate on your reply to whether there are issues specific to the needs of financial services to be taken into account when implementing free flow of data in the Digital Single Market, and explain to what extent regulations on data localisation or restrictions on data movement constitute an obstacle to cross-border financial transactions.

Total respondents to this question	133
Yes	**71**
No	14
Do not know	48

The overwhelming majority of respondents who expressed an opinion agreed that there are issues specific to financial services that need to be taken into account in the implementation of the principle of free flow of data in the Digital Single Market. Respondents, mostly those representing organisations/companies, considered that the main restrictions on data movement arise from administrative preferences, certification/accreditation, procurement policies, regulatory guidance, national legal requirements related to archival processes, company record laws and national security and law enforcement activities. Other national data localisation requirements hindering the free flow of data concern bank secrecy laws, use of cloud computing services, use of data for creditworthiness assessment purposes and personal data protection. On the last point, the majority of companies and about half of the public authorities considered that while the upcoming General Data Protection Regulation will address some of the existing problems by further harmonising the rules applicable to personal data and thereby strengthening the principle of free movement of personal data, there is a pressing need for further clarification of those rules. Some companies referred specifically to specific legislation such as MiFIR transaction requirements and MiFID or guidance by regulators' such as EBA's 2006 Outsourcing guidelines mandating audit and effective access rights to regulators as measures creating data localisation obstacles in the financial sector. European Supervisory Authorities' responses do not mention any restrictions to the free flow of data. However, one of them noted the existence of operational risks to the functioning of companies and to NCAs ability to effectively supervise the provision of financial services (in particular when the service provider is located outside the EU) arising from the outsourcing of certain company's functions. Some public authorities informed of not having identified any cases of data localisation regulations and a sizeable minority of companies considered that some restrictions to the free flow of data could be justified by Member States law enforcement and national security interests. A large majority of companies considered that the impact of national data localisation regulations on the Single Market is significant as it creates costs for businesses and entry barriers for new players, limits access to data and new technologies (e.g. cloud services), adds red tape, creates legal uncertainty, hampers the delivery of cost-efficient services to consumers and stymies innovation. The majority of companies in particular, considered that the further development of cloud computing in financial services and the technological innovation associated with it, is severely hindered by national laws setting restrictions on the geographical location of cloud services providers' infrastructures as well as by financial supervisors' criteria when approving cloud projects. Some respondents noted that restrictions on use of cloud services is often based on the misconception that storage of data in the cloud is less secure than in-house storage while the opposite is true.

Specific suggestions to improve the above situation and overcome restrictions to the free flow of data included:

- Implementation of the EU "Free flow of data in the Digital Single Market" initiative;
- Review and harmonisation of financial rules and financial supervisors criteria related to outsourcing and cloud projects;

- Improvement of cooperation between financial supervisors and data protection authorities;
- Request for legislative instrument requiring Member States to change their procurement policies;
- Promotion of EU wide standard on use of data for creditworthiness assessment purposes;
- Bank secrecy regulations: apply Art. 9(4) EMIR for all regulatory reporting requirements;
- Provide PSD2-like standardisation for accounting data and for data from the public sector

Question 3.7 - Are the three principles of technological neutrality, proportionality and integrity appropriate to guide the regulatory approach to the FinTech activities?

Total respondents to this question	158
Yes	**138**
No	5
Do not know	15

Out of 158 total responses, 138 respondents agreed with the three guiding principles. 5 disagreed. The importance of "technological neutrality" was emphasised many times. However, there were very few who noted that it is difficult to achieve. And, one supervisor and one firm cautioned that occasionally we may come across existing rules that may prevent or restrict sensible development of truly disruptive technologies (e.g. if DLT solutions do not fit the existing regulatory environment). Very few organisations and public authorities warned that the 'proportionality' principle should not become a loophole out of otherwise applicable regulation; and a race to the bottom. An ESA noted that integrity should include responsibility and accountability (clear allocation of responsibility). A public authority asked for clarity about the hierarchy among the 3 principles in case the conflict.

A few ideas for additional principles were also suggested, e.g.:

- A sizeable minority of organisations and companies and one individual suggested that 'level playing field' or 'same services, same risk, same rules' principle should be added;
- Some companies and a public authority called for more standardisation/uniformity in deployment of rules in the EU to be a principle to enable firms to scale up across the EU;
- A sizeable minority of public authorities and a few firms found that consumer/investor protection and empowering consumers should form a separate principle;
- Very few organisations and companies and two public authorities emphasised that activities-based regulation should be a principle. Very few companies also suggested that the EU should strive for future-proof and principles-based regulation; and
- Very few organisations and companies advocated for an inventory of EU laws to ensure they are not discriminatory to FinTech and innovation – 'do no harm' principle.

Other ideas mentioned once or twice were e.g. retention of supervisors' monitoring and response capacity; transparency; cyber security; security when outsourcing; data privacy; ensuring AML/CTF are guaranteed, decreasing administrative burden, etc. It was also suggested that regulation should be flexible, agile and complemented by the development of non-regulatory instruments. A horizontal approach to consumers and the financial system as a whole was recommended. One public authority suggested "test and learn initiatives". Very few respondents noted that these guiding principles should apply to over-all policy making.

Question 3.8 – (3.8.1) How can the Commission and the European Supervisory Authorities best coordinate, complement or combine the various practices and initiatives taken by national authorities in support of FinTech (e.g. innovation hubs, accelerators or sandboxes) and make the EU as a whole a hub for FinTech innovation? (3.8.2) Would there be merits in pooling expertise from the ESAs?

(The assessment of the responses is provided based on the two sub questions of question 3.8 – respectively 3.8.1 and 3.8.2)

(3.8.1)

Total respondents to this question	136

(3.8.2)

Total respondents to this question	127
Yes	**78**
No	9
Do not know	40

(3.8.1) This question received a number of interesting contributions and proposals from competent authorities and firms regarding the role that the ESAs and the Commission could play in the future.

On the ESAs role, vast majority of respondents underlined the need for a clearer definition and terminology of the different innovative tools set up at national level (e.g. sandbox, innovation hub), more coordination between national hubs, more transparency on the national initiatives (e.g. scope and functioning of the tools established as well as first assessment) and sharing best practices. A number of competent authorities also insisted on the necessity to further enhance the cross-sectoral dimension of ESAs work (e.g. Joint Committee) since FinTech developments are taking place more often across sectors (e.g. digital platforms requiring a combination of authorisations and licensing regimes from different sectoral legislation). Also, some competent authorities argued that ESAs could in particular look into the cross-border challenges faced by FinTech while trying to scale up across Europe. A few respondents asked to include an international dimension in the scope of this coordination work: getting in contacts with hubs outside-EU jurisdictions is key to get a proper assessment of FinTech developments worldwide. EU organisations representing FinTech called for a central point of information at ESA level, gathering for instance the status of regulatory needs across Europe, bringing therefore legal certainty for innovative solutions providers. Finally, a respondent form the industry also argued that ESAs coordination work could include closer links with Data protection authorities.

Views are more heterogeneous on the role the European Commission could play vis à vis national initiatives taken so far. Competent authorities are overall highly supportive of innovation hubs set at national level, in particular to provide direct support to innovative solutions providers and help them navigate the EU legislative framework. Views however differ regarding sandboxes. A number of authorities strongly support regulatory sandboxes where entrepreneurs can test innovative services or business models without having to comply with all legal requirements. Such initiatives are seen as reducing time-to-market for innovative firms, and could bring more benefits than innovation hubs focused on tailored and personalised advice. On the other hand, other supervisors considered that sandboxes could foster discord rather than enhance harmonisation within the Single Market. Sandbox regimes could easily conflict with EU law and therefore would need a new legal basis to define amendments on the level of the directives. Some authorities clearly warned that a race to the bottom due to regulatory arbitrage should be avoided. European supervisors underlined that one should be cautious about supervising FinTech in a different manner and recalled the importance of ensuring a level playing field for participants

while acknowledging at the same time that FinTech start-ups may benefit from additional guidance as offered by current innovation hubs. Based on these diverging views, competent authorities remain quite cautious about the role that the European Commission could indeed play.

On the industry side, most respondents reported they would support an EU sandbox. However, it is not always clear what they mean under EU sandbox. A number of respondents referred to sandboxes established in the UK or in Singapore as best examples. In such cases, the respondents expressed the need for setting up testing and learning capacity at national level, thanks to agile and proportionate regulation. Firms participating in the sandbox should not incur immediately normal regulatory burden of engaging in the activity in question. Going a step further, these respondents called for more harmonised practices at EU level and therefore asked the Commission to issue guidelines or high-level principles where the various criteria regarding the sandbox would be established (e.g. entry criteria, investor/consumer protection rules, duration of testing, exit criteria and transfer of business models into "normal" regulation). Respondents however did not explain how possible waivers to EU or national laws would be specified in such guidelines as well as the level of details on these issues. Other representatives from the industry called for a clear EU framework in this area to avoid regulatory arbitrage and competition among different national authorities. One respondent called for a cross-border EU regulatory sandbox under the umbrella of the ESAs, with the aim of fostering true pan-EU services. Others explicitly referred to testing and learning capacities in specific areas such as DLT, AI or big data. Finally, a couple of respondent explained they do not see the merit of creating regulatory sandboxes creating potentially and uneven level playing field and increasing regulatory arbitrage across Europe. Other initiatives that could be launched by the Commission include: increase EU funding with an open call to establish for-profit FinTech incubators like in Israel or Singapore, organise hackathons and duplicate the FinTech forum set up by some national authorities at EU level.

(3.8.2) The vast majority of respondents to this question thought that there would be merit in pooling expertise in the ESAs. National competent authorities clearly mentioned a number of areas where stronger expertise would be most useful: cloud computing services, big data and cybersecurity. At the same time, some respondents also underlined in certain areas the quality and usefulness of the work already carried out by the Joint Committee.

On the industry side, majority of respondents agreed that ESAs should be able to bring together and coordinate the necessary technological expertise and skills in the future. Small competent authorities, who may not have proper resources to get this expertise internally, also mentioned they would benefit from such centralised expertise at EU level. A number of respondents also stressed that the sectoral specialisation of ESAs may no longer be appropriate, and at least, ESAs should enhance cross-sectoral work since FinTechs cannot be assigned to a specific sector. Respondents from the Insurance industry however underlined the specificities of the insurance sector and the need to keep independent insurance supervisors. A couple of respondents insisted on a strong supervisory convergence in this area to avoid a patchy network of national initiatives. Additional comments were done as regards the need to clarify terminology used by national supervisors for innovative tools such as innovation hubs or sandboxes.

Question 3.9 - Should the Commission set up or support an "Innovation Academy" gathering industry experts, competent authorities (including data protection and cybersecurity authorities) and consumer organisations to share practices and discuss regulatory and supervisory concerns? If you think the Commission should set up or support an "Innovation Academy" gathering industry experts, competent authorities (including data protection and cybersecurity authorities) and consumer organisations to share practices and discuss regulatory and supervisory concerns, please specify how these programs should be organised.

Total respondents to this question	152
Yes	**118**
No	9
Do not know	25

Almost all respondents were very supportive of an "innovation hub" established by the Commission, especially on issues having a cross border impact. Different approaches were suggested: (i) the private model of accelerators or incubators, (2) the European Post trading Forum, (iii) the LabCFTC, (iv) the CAPSSI EU Project. Initiatives at national level were also mentioned as sources of inspiration: the FinTech Forum in France and the Payment Strategy Forum in UK.

The concrete solutions suggested by the respondents on how these programs should be organised - with a different degree of detail and pervasiveness - include the following:

Goals – According to several respondents the academy should convey and share knowledge among the different actors about the possible implications of the new technologies also in areas such as financial crime prevention, data protection or cyber-risks which are common to all financial innovations; for this purpose the Academy could serve also as repository of documents which would be made publicly available. Some stakeholders favoured more ambitious goals such as:

- offer faster, cheaper and easier-to-use services - through advanced systems and processes – including, among others, legal support in the interpretation and application of the regulatory framework, provision of substantial computing resources and organisation of training sessions and workshops for all participants;
- offer an environment to test new technologies and start businesses such as start-up incubators, co-working spaces, and tech office;
- establish learning mechanisms providing guidance for future projects.

Composition - Many respondents highlighted that stakeholders are to be correctly represented: all industry sectors and all types of companies (few mentioned that access to this Innovation Academy should not be limited to start-ups), consumer representatives, academic researchers and financial authorities but also other technologies related authorities, from EU and non EU jurisdictions.

Organisation - Some respondents suggested arranging the HUB in different committees or subgroups (topic/area/field of expertise), even coordinated by the ESAs. One of them also indicated the need to have hubs in each Member States.

Methods – Few respondents remarked on the need for innovative interaction systems (an open platform rather than a representation of local supervisors or associations), solution oriented methods and techniques (design-thinking, prototyping).

Question 3.10 – (3.10.1) Are guidelines or regulation needed at the European level to harmonise regulatory sandbox approaches in the MS? Please elaborate on your reply to whether guidelines or regulation are needed at the European level to harmonise regulatory sandbox approaches in the MS? (3.10.2) Would you see merits in developing a European regulatory sandbox targeted specifically at FinTechs wanting to operate cross-border? If you would see merits in developing a European regulatory sandbox targeted specifically at FinTechs wanting to operate cross-border, who should run the sandbox and what should be its main objective?

(The assessment of the responses is provided based on the two sub questions of question 3.10 – respectively 3.10.1 and 3.10.2)

(3.10.1)

Total respondents to this question	136
Yes	**75**
No	37
Do not know	24

(3.10.2)

Total respondents to this question	128
Yes	**68**
No	32
Do not know	28

(3.10.1) The vast majority of competent authorities opposed to an EU sandbox. In their view, national authorities are best equipped to deal with differences in markets and national legislations and to interact timely with FinTech companies. Creating new rules for entities wanting to operate cross-border that do not comply with all regulatory rules would essentially mean opening up the issue of revising existing European rules. In addition, if the more moderate regulatory requirements were established only for FinTech, this would violate the principle of neutrality. Few mentioned also that the proportionality principle, provided in the European framework, already ensures the promotion of innovation while at the same time preserving financial stability and consumer protection. The Commission should rather encourage a future coordinating role by the ESAs to ensure cooperation between different national Sandbox initiatives and sharing information on best practices. Those competent authority in favour of sandboxes pointed out that a EU 'licence' based on the application of EU rules would ensure the level playing field and help avoid legal and regulatory arbitrage, granting credibility to FinTech operators.

On the industry side, the vast majority of respondents claimed that they would support a common regulatory EU framework opposed to national solutions. Some of them called on EU rules harmonising Member States' regulatory sandbox approaches in order to reduce the regulatory obligations in the early stage of business, ease the running of such "sandbox" experiments on a cross border basis, reduce regulatory arbitrage and fragmentation in financial markets, and strengthen competitiveness. However, maintaining local NCAs as the pivotal point for the day-to-day interaction with local market participants was stressed as being important by some respondents. On the other hand, several respondents suggested the development of EU level guidelines, high-level principles or recommendations setting out best practices either in parallel to the EU sandbox, to quicken the process as a full harmonization may take too long, or as a preferable alternative approach. Coordination with international bodies on FinTech-focused policies such as IOSCO and the G-20 was also welcomed. Some respondents remarked that, while defining a set of common European rules, it is important to be very precise as to the scope and functioning of a "sandbox" setup in a highly regulated financial industry. Consumer organisations highlighted that a key element of sandboxes is safety for consumers and that they

should only be open to professional consumers who are well aware of the risks involved. Alignment of entry and exit criteria for sandboxes was considered as being a key milestone.
A sizeable minority of the respondents from industry opposed to an EU sandbox on the ground that it may be perceived as a short-cut to avoid regulation. They insisted on the need to allow experiences at Member State level to be carried out first, given that current regulatory sandboxes are still in their early phase and the national competent authorities are best placed to run the solution that works best for their market. Other initiatives could be launched by the Commission to support digital innovation at EU level directed to ensure that the existing regulatory framework is digital-friendly, technologically neutral and sufficiently future-proof to be fit for the digital innovation. Some respondents called for a wider participation that only small companies or early stage companies.

(3.10.2) A large majority of the respondents, independently from their background, favoured the development of an EU wide approach to sandboxes i.e. harmonised criteria for entry, simple and transparent authorisation process and exit and transition strategy. One respondent pointed out that a sound regulatory regime for experimentation and testing might foster innovation when the innovative project cannot fit within the existing regulatory framework. Some stakeholders suggested that EU level Guidelines, developed by the EU Commission and/or the ESAs, could be developed faster than heavier regulatory approach and help anyway avoid fragmentation. Among those calling for an EU sandbox, some mentioned that it should be run by the European Commission with the participation of all Member States. It was also mentioned that the ECB could run a special regulatory sandbox for cross-border innovations within the SSM. A future development might be to allow non-EU entities to access sandboxes.

As for its objective, a few respondents perceived an EU sandbox as a waiver to regulatory requirements for start-up companies. Others pointed out that a regulatory sandbox should aim to examine the underlying business models of new innovative products and monitor their development to assess if they might be problematic for consumers and/or for the markets. It could also provide advice to firms intending to operate cross-border as well as a testing facility. Measures should be established to mitigate consumer detriment based on a thorough risk assessment of the innovative projects.

Few respondents suggested that the EU Fin-Tech sandbox should be created for all types of FinTechs (including banks) willing to operate on a cross-border basis while others opposed to an EU sandbox targeted specifically at FinTech only. Few of them highlighted also that it must be accessible for all types of innovators, not just start-ups.

Question 3.11 - Are guidelines or regulation needed at the European level to harmonise regulatory sandbox approaches in the MS? Please elaborate on your reply to whether guidelines or regulation are needed at the European level to harmonise regulatory sandbox approaches in the MS?

Total respondents to this question	88

A vast majority of all ideas were only mentioned once. There were however a few themes arising:

- Measures needed so firms would be able to use the EU as one market; ideas included e.g.
  - More co-operation and less inconsistencies between supervisory authorities
  - Register of local irregularities and differences in regulation
  - Need for better knowledge on bankruptcy code and shareholder rights in other MS
  - Reinforcing links between EU and third countries
- Measures needed to improve financial and digital education; ideas included e.g.
  - Financial education programme for potential FinTech developers
  - Adopting measures on financial literacy based on FinTech tools
  - Call for more digestible and harmonised regulation, more outreach to coming firms
- Measures needed to help firms with their funding; ideas included e.g.
  - Start-up loans with a realistic pay back plan
  - Financing accelerators for disruptive initiatives
  - Allowing tax incentives for start-ups or other types of state aid
  - Dedicated investments by European strategic investment fund into FinTech projects
  - Pan-European equity incentive scheme
- Regarding sandboxes, there were those asking for EU guidelines and/or coordination for sandboxes but leaving the implementation to NCAs. Others were opposed to the whole idea. One idea was for the Commission to open projects with authorities and industry (e.g. for e-ID). An EU Industry Sandbox for non-live testing was also suggested.

Other ideas for supporting innovative firms included, an EU Innovation Hub to advise firms; regulatory waivers; fiscal harmonisation of crypto-currencies; a framework for a privileged relationship for FinTech firms with fast authorisation and continuous monitoring and support; creating a 'data roaming regime' to manage the risk of increased data transfer costs; and EU-wide programme for for-profit FinTech incubators (e.g. models used in Israel or Singapore); publishing views on where innovations represent a major opportunity; proportionate and modular licensing scheme with passporting; Commission support to start-ups when engaging with NCAs; actively attracting innovative companies abroad to set up an EU presence; change in the accounting treatment of software investment in CRR. Some firms however urged not to take any further action at EU level at this time and very few emphasised again the 'same service, same rules' principle.

Question 3.12 – (3.12.1) Is the development of technical standards and interoperability for FinTech in the EU sufficiently addressed as part of the European System of Financial Supervision? Please elaborate on your reply to whether the development of technical standards and interoperability for FinTech in the EU is sufficiently addressed as part of the European System of Financial Supervision. (3.12.2) Is the current level of data standardisation and interoperability an obstacle to taking full advantage of outsourcing opportunities?

(The assessment of the responses is provided based on the two sub questions of question 3.12 – respectively 3.12.1 and 3.12.2)

(3.12.1)

Total respondents to this question	122
Yes	32
No	**43**
Do not know	47

(3.12.2)

Total respondents to this question	116
Yes	**32**
No	29
Do not know	55

Most stakeholders, who expressed an opinion to question 3.12.1, responded negatively, i.e. held that the technical standards and interoperability are not sufficiently addressed as part of the ESFS. Stakeholders who responded negatively, called for further efforts. One respondent stressed that authorities should foster and support standardisation initiatives by market players and focus on solving overlaps between different regulations. A few stakeholders highlighted areas where standardization is insufficient such as the post –trade area, payment services - and notably lack of technical specifications for open banking (to increase competition) as well as lack of reliance between stakeholders under the AML Directive.

Many of the positive respondents recognized, however, the importance of increased standardization and interoperability in order to develop new technologies and solutions to and in order to increase competition, including the use of outsourcing. Also one respondent highlighted that standardization would facilitate compliance. In most of the respondents' views standardization should be left to market participants and the industry, where supervisors should act as catalysts. Standardization could also, according to one respondent, prevent innovation. A few respondents highlighted that standard setting initiatives can be slow processes. Although fragmented standards can initially impair market efficiency, this may deliver faster integration over time.

A few stakeholders considered that common standards could be useful in "FinTechs". According to one respondent, the issue of interoperability may accrue raised attention when DLT initiatives start operating. Common platforms may then be needed to ensure interoperability and the harmonizing of contracts for different processes. According to one stakeholder, common standards for data sharing between financial incumbents and both IoT providers and FinTechs could save the industry from investing in short term solutions and would lower the barriers for partnering with FinTechs. One respondent noted that some of the standards that FinTechs might be using are not specific for the financial sector only. For example, the standardization work of block chain is carried out at ISO.

In the view of one respondent, if the EU would adopt common technical standards and interoperability within the ESFS, this could help the European standards to become global standards. Many respondents, indeed, stressed the benefits of adopting global standards instead of national or regional. The ECB stated that the European Commission and the ESFS should look at promoting and in some cases mandating the adoption of global standards, such as ISO before considering jurisdiction based standards.

With reference to question 3.12.2, several stakeholders highlighted problem areas where, in their opinion, interoperability is insufficient. Some respondents mentioned regulatory restrictions or interpretations by the competent authorities' nationally (for example regarding the deployment of ICT services abroad or stringent security and liability requirements) or lack of appropriate definitions and legal framework. One respondent highlighted that crowdfunding platforms have their own standards. Some respondents suggested that the framework of the PSD2 could be enhanced to allow more competition.

Several respondents highlighted by various examples that better interoperability and better access to data would reduce so called vendor –locks. To this end, several respondents mentioned that it is difficult and costly to move data between cloud service providers (CSP's) and between or from legacy systems.

One respondent stressed strongly reference data to be an important area of harmonization and standardization. In its view, currently, there exists much ambiguity in the interpretation of reference data across multiple sources which potentially lead to differences in the various aspects of servicing of the financial instruments from trade execution, to settlement, accounting and valuation. One stakeholder suggested that the creation of a globally accepted digital identity would foster innovation and interoperability for FinTech in the EU.

A few stakeholders, although responding negatively, acknowledged that standards regarding cybersecurity, data safety issues and ICT reporting mechanisms could be useful in order to facilitate interoperability. Some stakeholders mentioned also, like under question 13.2.1, that global standards would be more useful than regional ones or standards just confined to the financial sector, and that any regulatory action by the EU should be kept to a minimum in order to allow innovation. The ECB stated that the ISO processes are able to address the issues of data standardization and interoperability in a sufficient satisfactory manner.

Question 3.13 - In which areas could EU or global level standards facilitate the efficiency and interoperability of FinTech solutions? What would be the most effective and competition-friendly approach to develop these standards?

Total respondents to this question	98

A fair amount of stakeholders have the opinion that in the context of FinTechs, the objectives of efficiency and interoperability can only be enabled by standards if they are developed at a global level, in a transparent manner, and technology agnostic. Some precised that standards adoption should be done on a voluntary basis and that regulation could stifle innovation if not technology neutral. A majority of respondents expressing an opinion on the standards development process think that standards development should be led by the industry or market stakeholders (through international standards development organisations such as ISO, European Standards Organisations, fora, or consortia), some of them thinking that the EU and public authorities should play an active role in it, while one respondent thinks that public private cooperation on standards development is important for their success.

Others expressed the idea that standards established by regulators, such as ESMA, should be

- done through a cooperation between private and public organisations, with all stakeholders (incumbents and FinTech services providers) being represented,
- consistent with global standards given that FinTech solutions develop across borders
- done in close contact with international bodies to debate and agree on such standards.

A few respondents reminded that interoperability can also be reached through an open source model.
A fair amount of respondents specifying areas where standardisation should occur mentioned API (Application Programming Interface), Blockchain/DLT and identity. Other mentioned different areas: regulatory reporting, corporate financial data, payments (PISP, XS2A), peer to peer lending/payment/investment, analytical credit dataset, EU single merchant identifier, data protection and cybersecurity, artificial intelligence, cloud, big data.
Some standards and Standard Setting Organisations were mentioned: ISO, IEEE, ITU X.509/ISO/IEC 9594-8:2005, ISO 17422, W3C, LEI, AnaCredit initiative, Financial Stability Board (FSB), IOSCO.

Question 3.14 - Should the EU institutions promote an open source model where libraries of open source solutions are available to developers and innovators to develop new products and services under specific open sources licenses? Please elaborate on your reply to whether the EU institutions should promote an open source model where libraries of open source solutions are available to developers and innovators to develop new products and services under specific open sources licenses, and explain what other specific measures should be taken at EU level.

Total respondents to this question	125
Yes	**57**
No	27
Do not know	41

The rationale behind this question is that by offering open-source libraries would be possible to boost interoperability and competitiveness.

Most stakeholders supported the promotion of an open source model.

The majority of the positive answers underlined how the promotion of open source models can help to create innovative solutions with smaller costs (lowering the barriers to enter in the market, encouraging reusability and facilitating cross-platform interoperability) and with enhanced level of security. The support to open source is also seen as an enabler for data portability and access, as well as accountability and auditability.

Among the stakeholders supporting the need for an EU action on Open Source, emerge however some differences which can be categorised on the basis of the type of stakeholder: while private individuals and representatives of the "civil society" express themselves generally in favour to a similar initiative without any precondition, identifying the adoption of open source practices as a milestone toward data and market transparency, company and industry representatives, put quite often the stress on the following points:

- Need to incentive standardisation before open-source (to avoid the un-coherent explosion of the number of open-source platforms), to support an effective interoperability
- Need to better clarify the intellectual property aspects

Some responders from the business domain clearly expressed a positive support underlying however how the initiative should not go in the direction of a mandatory obligation which might put in danger company investments.

Some responders suggested also that the Open Source initiative should concentrate mainly on the so called *Deep libraries* (network, security etc.), on the *Interoperability* aspects and on *Open Banking Models.*

A responder suggested also that within this scheme should also be establish a financial compensation program to reward the adoption of an open source approach, while another pointed out that while the initiative is welcome, a potential barrier could come from the actual regulatory frameworks in place in some MS where national regulators impose the use of proprietary solutions.

Analysing the negative answers instead, it is possible to identify the following main lines of reasoning: (1) EU should not have any role in this domain as the market should be left free to decide the direction to take (2) an Open Source initiative could put in danger the investment done by the business in the FinTech technologies, hence threatening the innovation (no business model = no founds = no innovation).

Some respondents seem to identify in the use of Open Source libraries a threat against cyber-security and Data Protection.

Two respondents expressed their negative opinion as an open-source initiative might distract attention from the cyber-security and privacy priorities.

Question 3.15 - How big is the impact of FinTech on the safety and soundness of incumbent firms? What are the efficiencies that FinTech solutions could bring to incumbents? Please explain.

Total respondents to this question	118

Almost half of the respondents to this question reported that the impact of FinTech solutions on incumbents very much depends on the extent to which they complement, complete or compete with the establish market players. Almost half of the companies foresaw a huge impact of FinTech solutions as these may touch upon the entire financial services value chain. Two main variables determined the impact: the degree to which processes and operations have changed as a result of technological innovation and the developments in the regulatory framework (PSDII, GDPR). Increased competitiveness in different financial services areas as well as the effects on consumers' expectations and preferences where other dimensions of the impact that new FinTech entrants had on traditional market players. Almost half of the responding authorities considered FinTech solutions impact as neutral with a negative outlook as there might consequences on the prudential framework, on liquidity and capital positions and there might be negative incentives on business conduct as result of diminished margins and reduced profitability. Very few companies stated that the impact on incumbents was either limited or not clear at that stage and that further assessment analysis is needed. Overall, the impact of FinTech solutions on incumbents is perceived as a positive driver to improve consumer experience and to foster financial inclusion. Possible drawbacks were seen in the increase level of competitiveness, which could lead to reduced profitability.

Almost half of the respondent authorities and companies considered FinTech as a key driver improving the efficiency in almost every area of financial. FinTech solutions played a key role in reducing inefficiencies boosting higher levels of automation, which have led to more efficient back office activities, higher levels of transparency, operational resilience and significant cost-reduction. Almost half of the respondents saw positive effects as FinTech solutions in the risk mitigation area (reduced counterparty risk exposure, liquidity and operational risk). FinTech solutions have also led to significant efficiencies in trading and post-trading activities by facilitating, among others, clearing and settlement operations, collateral management audit processes and they have also had positive effects in limiting information asymmetries.

Notwithstanding the positive effects of FinTech solutions, very few companies considered that the irruption of new players could make incumbents less profitable, which, in turn, could push incumbents to take more risk. A few stakeholders pointed out the risk that some of the FinTech activities could expand at shadow banking, therefore evading unwelcomed regulation and alerted that a non-regulated development of FinTech may generate bubble-risk. Some companies underlined the need to ensure a level playing field as well as consumers and investor protection .

SECTION 4 - BALANCING GREATER DATA SHARING AND TRANSPARENCY WITH DATA SECURITY AND PROTECTION NEEDS

Question 4.1 - How important is the free flow of data for the development of a Digital Single Market in financial services? Should service users (i.e. consumers and businesses generating the data) be entitled to fair compensation when their data is processed by service providers for commercial purposes that go beyond their direct relationship?

Total respondents to this question	123

A small number of respondents interpreted the question on "Free Flow of Data" in line with the terminological definition applied in Communication "Building a European Data Economy" (COM(2017)9) of 10 January 2017. Under this definition, "Free Flow of Data" means that Member States should refrain from imposing unjustified data localisation restrictions on companies so that they can store their data at any location of their choice inside the EU. For all respondents, enforcing this principle was very important.

The vast number of respondents, on the other hand, understood the question to mean whether it would be beneficial in a Digital Single Market if economic operators had the best possible access to data resources, including data held by other operators, in order to improve operations or quality of services. All those respondents agreed fully to this statement. Two respondents speaking on behalf of portfolio managers made a specifically strong plea for "unrestricted" and "open" access to financial market data, as this would lead to better and more informed decisions.

Banking organisations called for a level playing field in terms of regulation framing data processing and sharing, both between banks and non-banks and between EU and non-EU firms.

On the question of compensation of sharing, a significant number of respondents questioned the assumption that it would be possible to determine "fairness" in this respect. The value of data varies greatly, dependent from the intended use, making abstract assessments impossible. Also, individual data points have very little value. For big data, only having access to large volumes of data is relevant. This makes compensating individual contributors to such data volumes difficult.

Stakeholders also point to the importance of maintaining trust in the handling of data, including personal data, which had been a key selling proposition of banks. Such standards should not be compromised in return for more data sharing.

On the question of compensating consumers for use of personal data, the vast majority of respondents believe that this is already addressed by the General Data Protection Regulation (GDPR) and that no additional rules where necessary. No respondent called into question in any way the rules of the GDPR. A respondent on behalf of the Channel Islands (outside the EU Treaties) noted that while the GDPR may contain restrictions that result in significant barriers to market entry, such rules where necessary to obtain consumer trust in data processing and that for this reason the Channel Islands would adopt legislation akin to GDPR rules.

All respondents agree that the consumer should be compensated in some form and that there should be utmost transparency with respect to processing of personal data. Almost all respondents specified that such compensation should not be in monetary rewards, but come through improved, personalised services and/or cheaper service provision. A few number of respondents cited a recent opinion of the European Data Protection Supervisor taking the view that against the human rights nature of data protection law, it would be problematic to consider personal data as a form of payment for services. Some respondents also note that the individual is free to withdraw his/her consent for the data processing at any time, which makes it difficult to

come to some sort of contractual agreement binding both sides that would be the necessary basis for any compensation.

A smaller number of respondents addressed the question of enhanced access to non-personal data held by other companies. They pointed to the strategic value of such data for a company. Also, maintaining a high quality of data has a clear cost. Consequently, companies should remain free to decide whether to share data, the kind of data they want to share and with whom. Protection rights on such data in this respect are a necessary element.

A small number of respondents call for "data marketplaces" as dedicated intermediaries for exchanging data.

A small number of respondents came from the insurance industry. They note a concentration in the market with respect to consumer information. Data monopolisation in their view is harmful as it makes access to data relevant for tailoring products and similar very difficult.

Responses from the very few consumer rights organisations pointed to the dangers linked to the processing of inaccurate or wrong data, e.g. having unjustified negative impacts on credit scoring. They also remarked that using consumer preference data in the asset management industry may only be used in order to improve sales strategies than provide objectively superior products.

Question 4.2: To what extent could DLT solutions provide a reliable tool for financial information storing and sharing? Are there alternative technological solutions?

Total respondents to this question	113

Almost all respondents underlined the advantages of DLT compared to other more mature technologies. Whilst other technological solutions are available, DLT shows a potential that cannot be matched. DLT is a very promising tool for reliable storing and sharing of financial and non-financial information. Through the establishment of new financial services infrastructure and processes, it provides benefits such as decentralization, flexibility, transparency and immutability that are superior to a classic technological approach. In addition, by sharing the existence of data across a network, DLT mitigates the incentive to attack one central owner of valuable data and reduces systemic risk around single points of failure. Security does not seem to be a problem, given that users can be selected and restricted. Cybersecurity measures, cryptography and encryption mechanisms are to be put in place. One respondent pointed out that security could be further enhanced by using DLT solutions to only store corresponding hash values of data inside the DLT and not the data itself. Many financial processes and services could benefit from DLT: customer data, pre contractual information, contract information, market data and events, ownership rights, information related to transactions settlement and transactions reporting – are some examples of the information that could be stored in a distributed ledger.

Some Competent Authorities deemed it premature to address this topic today, given that the technology itself is not yet feasible. They highlighted that there is still room for improvement with regard to: (i) the protection of the information in the DLT (ii) the legal uncertainty concerning the identification of persons responsible (iii) the governance model. It was also emphasised that DLTs are not designed for data storage but are best suited for storing digital footprints (hashes). Several stakeholders from industry underlined that DLT is a new technology and therefore we are still faced with challenges for DLT to scale up: (i) interfaces and standards have to be provided for storing and sharing; (ii) digital identity and data ownership issues cannot be solved directly, but only in combination with other technologies; (iii) once records are approved, changing stored information, if errors are found in the records or potential voting /approval abuse is discovered, may prove difficult. A dispute resolution mechanism is needed to address these challenges; (iv) a strong governance model would be necessary to ensure interoperability and resilience.

Alternative technological solutions to DLT, which could achieve the same purpose, were suggested: traditional databases operated by central authorities (CCP's, regulators, FMI's, etc.), APIs, microservices, service-oriented architecture, Public Key Infrastructures, Interplanetary File System, cloud computing, modular cryptographic solutions, etc.. These solutions nonetheless lack some built-in capabilities of DLT.

Question 4.3 – Are digital entity frameworks sufficiently developed to be used with DLT or other technological solutions in financial services?

Total respondents to this question	126
Yes	17
No	**62**
Do not know	47

A large majority of respondents (as well as within each category) stated that there is no mature digital identity framework at the moment to be used with DLT or other technical solutions in financial services. While, according to some stakeholders, promising frameworks are emerging, they are not yet fully ready to meet the demands of many potential DLT use cases. Improvements are needed and it remains to be seen how they will develop.

Some stakeholders recommended that digital identity frameworks be further promoted, since they are one the most important enablers of the FinTech and for successful DLT adoption.

Some organisations and companies referred to the eIDAS Regulation and recommended that Member States embrace the regulatory opportunity created by it. It was stated that EIDAS and similar identity verification schemes have the potential to revolutionise FinTech, and greatly bring barriers and costs of conducting financial transactions and KYC/CDD checks down. Only a few respondents expressed scepticism as to whether the eIDAS framework would be able to provide a sufficient solution for the private sector, at least in the mid-term.

- Issues/problems identified by respondents:
  - There are still inconsistencies between eIDAS and the AML Directive. The revision of the AMLD IV should guarantee that existing and future processes and services outside the scope of eIDAS can be accepted under the revised AMLD, at least when they are approved by the competent authority.
  - The implementation and importance of data security is poorly understood, and poorly implemented;
  - There is a need to clarify the regulatory framework with respect to the liability of data sharing;
  - Interoperability between existing systems is a challenge that remains to be resolved;
  - There is a lack of standards characterising which items constitute a valid digital identity;
  - There is a lack of usability of eID solutions ;
  - AML/CDD/KYC requirements are not yet drawn up in such a way that sufficiently covers the potential of DLT and other technological solutions in financial services.

- Some possible solutions were identified by respondents:
  - A key factor for the success of the Digital Single Market Strategy will be to ensure that as rapidly as possible the questions surrounding the implementation of the eIDAS Regulation, the transposition of the revised AML Directive and the implementation of the GDPR are resolved, and that the private sector is confident to be able to access and use the eIDAS framework in the same way as the public sector.
  - Common digital identity-enabling eKYC should be introduced in EU.
  - Electronic identification under eIDAS could be with the LEI in order to have a legally valid sequence between the digital ID and the real ID world for corporates and financial market participants.
  - Associating the digital identity with a qualified electronic signature scheme can enable a person to perform any kind of transaction within the digital single market.

Question 4.4 - What are the challenges for using DLT with regard to personal data protection and how could they be overcome?

Total respondents to this question	110

The vast majority of respondents to this question considered that there were significant challenges for using DLT with regard to personal data protection:

Right to be forgotten - The immutable nature of blockchain, with their full availability of historical transactions, was feared to be being incompatible with the right to be forgotten and the principle of storage limitation under the GDPR by a sizeable minority of respondents. Immutability also raised challenges in the event of individuals exercising broader control, for example needing to modify or correct previous transactions (right to rectification).

Confidentiality - A sizeable minority of respondents also raised the challenge of ensuring personal data confidentiality, especially over the long term. Although encryption and private keys could be used to limit access to personal data, the development of more powerful decryption techniques risks future confidentiality, particularly for public ledgers. One respondent also raised traceability, where the identity of a market participant may be inferred from his/her trading patterns.

Cybersecurity - A number of respondents identified the risk of data breaches, including maintaining the secret nature of private keys and cryptographic data, which would depend upon the strength of protocols and agreements for data generation, storage, distribution, revocation and destruction.

Other issues also noted in responses included:

- The nature of DLT makes it difficult to identify a data controller responsible for processing and for ensuring the exercise of data subjects' rights;
- The current pre-General Data Protection Regulation (GDPR) data protection regulatory fragmentation poses challenges where cross-border DLT solutions are adopted
- The difficulty in complying with data protection rules on international transfers; and
- The difficulty of complying with existing data localisation requirements.

Some stakeholders expressed confidence, at this early stage, that solutions could be found, stressing the importance of clarifying the circumstances under which personal data can be processed safely and securely, with proposals including:

- Deployment of strong encryption through permission-based block chains in which only authenticated individuals have access to personal data. This could potentially form part of a layered approach, in which other elements are accessible more widely.
- Recourse to trusted third parties within the ledger for the management of personal data;
- Storing personal data outside the blockchain, but with proof of the data held inside the DLT e.g. deploying zero knowledge proof protocols.
- Pruning, in which the processing of personal data is gradually restricted over time.
- Ensuring data protection by design so DLT conception and operation minimises risks to personal data from the outset.
- Ensuring that regional regulatory frameworks are aligned to reduce fragmentation

One trade body requested the Commission to consider reducing the personal information that is required to be included in transactions, for example under MiFID II, to reduce the risk of compromising personal data.

Some technical solutions under development, for example zkSNARKs and R3 Corda, could help to address some of these challenges, although some stakeholders noted that these seem to be still expensive and resource intensive.

Of the respondents expressing a view, the majority considered that the GDPR provides an adequate framework for the development of DLT, with one trade body emphasising the need to swiftly increase adequacy decisions for third countries. However, two organisations considered a bespoke regulatory framework is required. Another organisation argued that this would be contrary to the Commission's objective of being technology neutral.

Question 4.5 - How can information systems and technology-based solutions improve the risk profiling of SMEs (including start-up and scale-up companies) and other users?

Total respondents to this question	95

The following key aspects were identified as creating opportunities for profiling solutions:

- Access to SMEs bank account data could give reliable data on creditworthiness of SME. Risk profiles of SMEs should, arguably, be complemented by risk profiling of owners/managers to adjust the risk profile of SMEs.
- Scoring engines, big data (behaviour, geography, device, etc.), IoT advances, network analysis, process distribution techniques, data aggregation and visualisation and machine learning tools have proven very successful in precise risk profiling and risk pricing. Such scoring engines will improve with the availability of even larger data pools.
- Support for real time accounting and cash flow estimates, which take into account all listed and unlisted shares.
- New innovative technologies are not only improving risk profiling and credit-scoring tools but also improve customer knowledge, customisation of services and developing preventive tools. These tools will have the capacity to enhance preventive action and risk management in SMEs that often lack the financial means to institute costly risk-management procedures.
- Risk-profiling techniques should be cross-linked with official tax databases, with the customer's permission, and bank payment data to understand business dynamics and business flows, apart from traditional ratings. This approach enhances credit-scoring tools.
- The risk the SME takes as it conducts its own business of selling goods and services. Technology and data science creates a material improvement in assessing the risk and underlying nature of the business, the creditworthiness of the SME and the future potential products and services to provide to it.
- Substantial revenue opportunities by increasing capital allocations to areas previously excluded and Better customer servicing (consumers and SME's) due to providing a broader range of products (comparative tools & product aggregators), tailoring products and advice (e.g. improved credit scoring, in-creasing product suitability) and reducing risks (e.g. rigorous audits trails). In this connection, data quality and reliability is critical.

A few respondents highlighted that regulations aimed at rating agencies pose a substantial challenge for alternative providers to provide risk profiling solutions and data processing tools for SMEs scoring. A few respondents noted that SMEs are intrinsically very difficult to profile from a risk perspective due to an absence of data, and a lack of data sharing. Lack of data standardisation and divergence of accounting formats results in higher burden and divergences in inter-comparability of SMEs. Big data and common APIs and XS2A under PSD2 can offer some solutions. Big Data tools rely on aggregating confidential data on a company and its members from different sources, possibly without their knowledge, and should not, in the view of the respondent, be permissible. There are extensive new requirements under the GDPR.

For some stakeholders, risk profiling can become a routine operation with access to common datasets across the region. It has been argued by one respondent that at the time of application for a financial service, the provider should know in a matter of seconds all the information for assessing applicant's history and profile without operational friction and delays. It has been argued that today's AML, CDD and KYC rules are way too slow and fraud laden. One respondent argued that very wide and varied types of Big Data are used collectively (up to 15,000 data points in credit scoring algorithm), which makes it difficult to explain the rationale for adverse decisions – e.g. denied SME credit. Use for Big Data for calculating credit scores for SMEs should be subject to the SME's explicit consent and SMEs should be able to choose the types of data they are willing to have included in their credit assessment.

It has been suggested by a few respondents to revisit regulations aimed at rating agencies that poses a substantial challenge for alternative providers to provide risk profiling solutions and SME scoring tools. A few respondents proposed to standardise data and formats and resolve the problem of divergence of accounting standards. One of the proposed solutions was developing common centralised solutions for assessment of risks, centralised risk-scoring and common APIs. In some Member States, only traditional banking and financial lenders can arguably contribute credit data to CRAs, thus preventing a wider and cross-sector level playing field. It has hence been argued by one respondent that CRAs should be given a role in credit scoring SMEs (including start-up and scale-up companies) and other users (i.e. unscored clients). This would arguably solve information asymmetry between borrowers and lenders and unlocking the value of vast data-sets of information, including alternative data. One respondent was advocating for opening small enterprise data to official tax filings and opening up bank transfers (cash-flows). That respondent argued that it is critical that regulators and supervisors allow banks to test these solutions, starting at low scale and scaling them up. Another respondent has proposed to create an open data bank pooling information on SMEs risk profiling. Moreover risk profiling of SMEs is combining public and private data sources. Unfortunately, no conclusive or specific recommendations were made. A few respondents have strongly encouraged the EC to investigate the Dutch PPP approach called Standard Business Reporting (SBR) project aimed at standardisation of primary data and developing machine-2-machine exchange protocols for reporting purposes to the Dutch state authorities. It has been proposed to consider EU equivalent of SBR and its uses.

Question 4.6 - How can counterparties that hold credit and financial data on SMEs and other users be incentivised to share information with alternative funding providers? What kind of policy action could enable this interaction? What are the risks, if any, for SMEs?

Total respondents to this question	92

In relation to sharing SME credit and financial data with alternative funding providers, most respondents identified the upcoming GDPR and PSD2 as the most important recent developments to take into consideration. According to some respondents from the industry, data protection and customer confidentiality requirements restrict financial services firms from sharing information about their customers with third parties; besides, banking secrecy laws prohibit the sharing of financial data. Other respondents underlined that the implementation of PSD2 will be key. Under PSD2, sharing data through the use of APIs covers the accessibility of transactional data. If the right to share data is introduced, the access and portability should however apply only to raw data. Other respondents argued that SMEs should control their data sharing; any regulation should ensure that SME data is shared only when they agree to this. SMEs should decide at their full discretion which information, at what level of detail, when and to whom can be shared (this view was shared by several participants). Data protection and cybersecurity standards should be consistently applied to any party accessing the data, regardless of entity type, to protect SME data.

According to the banking industry, much has been done in terms of policy action with the adoption of PSD2 and GDPR and no additional provision are needed until these regulations are fully in place. In their view, the data creator (banks) is to decide whether to share its data and under what conditions as it owns its internal rating systems and their results. The access to data and transfer of data are crucial for FinTech innovation so the EC initiative on 'Building a European Data Economy' should be supported. Restrictions on data localisation should be removed.

Some respondents suggested adopting common standards to facilitate the sharing of data and establish a set of standard agreements to clarify the legal framework necessary to protect against the unintended use of credit-related information. There was also support for the exchange of best practices on sharing SME credit and financial data.

Some respondents proposed to create public data repositories / public credit registries governed by strict data protection rules and in line with the GDPR proportionality rules, and to ensure access to these and existing pubic registers and databases to stimulate cross-border investment. Other respondents advocated for the use of reciprocity agreements between holders of SME credit and financial data and alternative funding providers and SMEs to incentivise the latter to share more of their information. The need to compensate the data owner for sharing SME information was also underlined by some respondents.

The main risks to data sharing listed by respondents included the following: data and cybersecurity incidents, particularly if information is to be shared cross-border; SMEs or other users not being aware of the data shared; risk profiling of SMEs resulting in undue exclusion; confidentiality concerns of SMEs and potential lack of transparency in relation to the technology and algorithms which may have been applied by the counterparty in assessing credit information; sharing of information that gives only part of the picture of an SME's credit risk, leading to less favourable lending rates.

Question 4.7 - What additional (minimum) cybersecurity requirements for financial service providers and market infrastructures should be included as a complement to the existing requirements (if any)? What kind of proportionality should apply to this regime?

Total respondents to this question	125

The broad message from the vast majority of the stakeholders that replied to this question was that there is no need for additional requirements, given that the EU regulatory framework (e.g. the GDPR, NIS, PSD2, etc.) already provides a comprehensive set of requirements on cyber security. However, respondents from the banking industry pointed to the need to extend and/or update the existing requirements to include all financial market players besides banks. The banking industry suggested that the IT and cyber security requirements for financial institutions should also apply to FinTechs where appropriate and proportional (e.g. the principle "same services, same risks, same rules, same supervision") in order to ensure a level playing field. There was a common view from public authorities, firms and private individuals that the existing requirements should be thoroughly enforced, otherwise there is no point in setting them.

Given the existence of multiple guidance on cyber risk management, many public authorities supported the case for an EU level harmonisation including "minimum horizontal cyber security standards" and the potential strengthening of the legal basis of its application. A wide array of industry respondents gave concrete examples of best practices, as well as practical recommendations and measures for increasing the cyber resilience of financial market participants: appropriate mapping of the IT infrastructure and critical assets, control of administrative and privileged access, ongoing training for employees, ongoing reassessment of the firm's cyber resilience, end-to-end encryption of transmission channels, encryption of "data in transit" as well as "data at rest", segregation of applications and systems, harmonising critical infrastructure penetration testing, increasing information sand intelligence sharing, etc.

However, in developing such guidance, a vast majority of the stakeholders claimed that a prescriptive "one-size-fits-all" approach to regulating cyber risks will not work. They argued that the dynamic nature of cyber threats (and its increase with greater digitalisation) requires cyber security standards to continue being principle and risk based rather than prescriptive rules. They referred to existing cyber security standards in other jurisdictions (e.g. the NIST framework in the US) and called on the EU to leverage and promote the G7 Fundamental Elements of Cybersecurity for the Financial Sector and the CPMI-IOSCO guidance on cyber resilience for financial market infrastructures. Respondents have also suggested more global and cross-border coordination to address any cyber threats. Many public authorities believe there is also a need for flexibility and proportionality, and although minimum cyber security standards are set out, financial market participants should be allowed to "comply or explain". Such deviations could be justified based on the evaluation of risk and impact. A trade union from the financial sector claimed that cyber security requirements for all banks (irrespective of their size) should be the same as it concerns the safety of the individual investor.

In the case of cyber security incidents, many companies and industry associations have raised concerns regarding the overlapping reporting requirements to a variety of authorities (e.g. the GDPR competent authority, the NIS competent authority, the SSM) and have suggested a "one shop stop" for notifications and harmonized reporting formats and procedures. They have also called for a clarification on the definition of "major incident".

The banking industry also claimed that third party vendors and third parties accessing their infrastructures should be certified as secure and regularly audited and supervised, as in many instances these third parties lack very basic security measures.

One respondent has suggested that regulatory and supervisory authorities should increase the security of their systems and their providers, as they hold by far a greater volume of sensitive data than any individual regulated firm.

Question 4.8 - What regulatory barriers or other possible hurdles of different nature impede or prevent cyber threat information sharing among financial services providers and with public authorities? How can they be addressed?

Total respondents to this question	98

All respondents, independently from their background agreed that better information sharing is a necessity to achieve a higher level of cybersecurity.

A few private individuals together with some companies and few public authorities considered the nature and the structure of the financial service sector, the confidentiality issue, the possible reputational damages and the lack of trust as the most relevant non-legal hurdles preventing the information sharing. Very few stakeholders (small dimensions) saw in the limited technical skills and infrastructure capacities the hurdles limiting the development of the flow of information. Mistrust in supervisory authorities to ensure/protect data and confidentiality seemed to be a significant obstacle affecting the development of these practices.

Some industry stakeholders and a few public authorities clearly highlighted concerns regarding the processing of personal data (GDPR in particular), which were considered as the main regulatory barriers impeding the development of the information sharing among markets participants and among markets participants and regulators. The interpretation/implementation of EU law at national level was also pointed at by some stakeholders as a potential issue once GDPR comes into force in 2018 - this has yet to be assessed.

Overall, the vast majority of the respondents consider the EU intervention as necessary to strengthen the cooperation on cybersecurity. On the basis of the responses, a few companies and some public institutions called in favour of the need of the establishment of a central authority in charge of coordinating the information sharing – also mentioning similar but diverging requirements such as the ones in PSD2, NIS and GDPR. In particular, some respondents suggested that ESAs should be empowered to be central authorities for coordination on cybersecurity issues and act as intermediary for information sharing. Some stakeholders underlined the need for more legal clarity to harmonise incident reporting requirements. One asked for "liability carve outs" for companies sharing information. Very few stakeholders called for national CERTs to be recognised as the national hub for information sharing, while a few companies called for a better coordination among national and EU supervisors and with the European Data Protection Board.

A few companies/organisations and stakeholders highlighted the significant role of the industry in facilitating the information sharing through the creation of sharing mechanisms (platforms or cyber threats observatories), and called for best practices and guidelines to support these initiatives. Some stakeholders supported the view that the EU should coordinate the work towards the development of standards and principles on information sharing. The EU was invited to take into account the work done at international level by certain international standard setting bodies and consider the ISO27032 as a good starting point to develop best practices. A few stakeholders called supervisors to adopt a risk-based approach to harmonising cybersecurity requirements.

Question 4.9 - What cybersecurity penetration and resilience testing in financial services should be implemented? What is the case for coordination at EU level? What specific elements should be addressed (e.g. common minimum requirements, tests, testing scenarios, mutual recognition among regulators across jurisdictions of resilience testing)?

Total respondents to this question	94

Many respondents highlighted that providers of financial services, and in particular those that hold customer data, should be ready to support cyber security resilience testing and be able to implement business continuity tests in order to guarantee service continuity. They have also emphasised that most mature financial services providers already have regular penetration and resilience testing policies. At the same time, a significant number of respondents from both the public and private sector highlighted that supervisory and national competent authorities are already conducting resilience testing in financial services, and such tests should continue. Respondents made reference to the CBEST vulnerability testing framework in the UK, the Threat Intelligence Based Ethical Red teaming (TIBER) tests in the Netherlands, the penetration testing as part of the on-site supervisory inspections in France, the Financial Sector Operational Robustness forum (FSOR) initiative in Denmark, and pointed that such initiatives could serves as inspiration for future European actions. A couple of respondents suggested desktop cyber exercises as a useful tool to increase the level of alertness among financial market participants. Industry players have also pointed out that the testing should be tailored to the particular circumstances of the firm.

A vast majority of the replies from both the public authorities and the industry insisted on the need for coordination, cooperation and cross-border collaboration across the EU, but also globally. Stakeholders were generally supportive for penetration and resilience testing, and suggested that a European harmonisation could lead to creating a minimum level of cyber security in financial services across the EU and it should be built on one of the existing national initiatives of the Member States.

Some of the stakeholders were of the opinion that the testing should be performed by external parties (e.g. authorised and recognised third parties), while others suggested that the tests should be performed by the institutions themselves in partnership with the regulatory community and applying frameworks such as those developed by AFME, GFMA, CPMI-IOSCO, etc.. A vast majority of respondents from the industry associations argued that tests that meet comparable standards should be recognised across borders (i.e. mutual recognition), which would contribute to increase the efficiency and effectiveness of the cybersecurity measures.

Industry representatives called for a level playing field in the penetration and resilience testing and suggested testing to be extended to FinTech companies, by respecting the principle of proportionality according to their risk profile, size, operating jurisdictions, etc.

Respondents from the industry suggested that the testing requirements should consider the entire chain of service providers in order to determine the resilience of the different parties involved, while others were more specific by calling for a non-compulsory but incentivised certification or labelling framework for software developers and suppliers of financial services.

Question 4.10 – (4.10.1) What other applications of new technologies to financial services, beyond those above mentioned, can improve access to finance, mitigate information barriers and/or improve quality of information channels and sharing? (4.10.2) Are there any regulatory requirements impeding them?

(The assessment of the responses is provided based on the two sub questions of question 4.10 – respectively 4.10.1 and 4.10.2)

(4.10.1)

Total respondents to this question	83

(4.10.2)

Total respondents to this question	100
Yes	**18**
No	13
Do not know	69

Only about 16% of the respondents expressed a view on question 4.10.1. For the subsequent question about whether there were any regulatory requirements impeding other applications of new technologies to financial services to improve access, mitigate information barriers and/or improve quality of information channels and sharing only few respondents expressed an opinion.

Many respondents referred to previous replies. Among the few respondents that provided a response to these questions, the technologies or applications of technology that were mentioned most often were data sharing, universal or standardised data formats, secure identification and authentication technologies (e.g. biometry), robotics, machine learning and distributed ledger technology.

In terms of regulatory requirements that may impede the use of these applications, among the small number of replies, some respondents referred to rules governing data sharing/GDPR and access to data more generally, even if data portability requirements were also seen as positive and facilitating switching between providers. The need for open standards and APIs was also referred to. Some respondents also referred to heavy authorization and licencing requirements and entry barriers and the fact that supervisors could take a restrictive approach that slowed down innovation or a supportive one. The (lack of) recognition of digital KYC processes and cryptocurrencies as legal tender were also referred to by specific respondents.