SESSION SUMMARY - BERLIN SEPTEMBER 2020

Is the EU policy approach on cloud and data up to the digital challenges?

1. Progress of cloud adoption in the financial sector

An industry representative stated that Europe is moving in step with the rest of the world in terms of cloud adoption. Many European banks and insurers have moved beyond the testing phase and are fully investing in cloud-based solutions. The same is true more generally for the digitalisation of the financial sector, as demonstrated by the innovations happening in the European fintech space in particular. These evolutions are building on the collective progress that the financial and tech industry and the authorities have been making over the last few years in better understanding how cloud solutions can support the financial industry and adapting the regulation accordingly.

Another industry representative confirmed that cloud usage is progressing in banks, both in terms of the breadth of use cases and in the depth of implementation. Initially experimental, use cases started emerging in areas such as data analytics and artificial intelligence (AI). Their bank, for instance, has its mobile bank, big data analytics and AI capabilities fully on the public cloud. An increasing number of organisations are now moving towards more critical public cloud use cases, such as data centre replacement and the hosting of core products and systems in the public cloud. Banks are however not yet moving their entire operation to the cloud. This trend is due to continue and is dependent on well functioning public cloud services.

A regulator emphasized that European supervisory authorities are very supportive of the digital transformation and the leveraging of data which are happening in the financial sector, as that will help to improve customer service and the competitiveness of the sector. EIOPA for example has been monitoring the digital transformation of the European insurance sector for some time. It is clear that the insurance sector is moving ahead, adopting at a fast pace new types of tools, such as the cloud, which facilitate new developments based on AI and big data analytics. The COVID 19 crisis is likely to further accelerate the pace of digital transformation, requiring close attention from the supervisory and regulatory side. For implementing these new developments, it is essential for the financial institutions to conclude partnerships with specialized third-party providers in order to have access to the highest degree of innovation. This on-going evolution is mutually beneficial to insurers and technology providers such as cloud service providers (CSPs).

An industry representative confirmed the relevance of cloud-based solutions for the insurance industry in particular, which is and has always been, a data business with data being fundamental to how insurers analyse, underwrite and price risk. For this speaker's company, a global insurance company, there has been a significant shift to cloud particularly over the last 5 years.

A policy-maker stated that more broadly the whole financial system is increasingly dependent on the use and development of information and communication technology (ICT). There is a growing demand for digital solutions provided by third party services such as CSPs in the sector, for reducing manual operations, putting in place new remote working processes and facilitating new channels of communication with and amongst stakeholders.

2. Benefits associated with cloud usage in the financial sector

2.1 Supporting product innovation and cost-effectiveness

An industry representative stated that innovation and agility are among the main benefits of the cloud, which helps financial institutions to bring new products to the market and reach out to new customer segments faster and in a more cost-efficient way.

Another industry representative explained that insurers for example are increasingly building their new generations of products using cloud infrastructure, not just because of the cost advantages but also because of the benefits in terms of customer experience. Both traditional players and new fintech players are moving to simpler product designs that are leveraging the data storage and analytics capabilities of the cloud, as well as the capacity to speed up development and marketing processes. A trend that is due to continue particularly on the retail level is the use of parametric triggers[1], offering an entirely new kind of customer experience because contracts using them are quicker and easier to subscribe and underwrite than traditional indemnity-based products and claims can be paid in a matter of minutes.

A regulator agreed that digital transformation supported by the cloud will be fundamental for the insurance industry in a number of new areas, including the internet of things, which may provide the insurance sector with a much higher level of data availability, open insurance concepts, which are likely to develop in the coming years, as well as parametric insurance. These changes are in their infancy but will become increasingly relevant in the coming years. Europe therefore needs an ambitious programme to ensure that cloud solutions develop in a safe way and that they benefit customers as well as the industry in terms of cost efficiency.

[1] Parametric insurance is a type of insurance that covers the probability of a predefined event happening instead of indemnifying actual loss incurred. It is an agreement to make a payment upon the occurrence of a triggering event, and as such is detached from an underlying physical asset or piece of infrastructure.

2.2 Reducing operational risks

An industry representative emphasized the risk reductions offered by cloud technology. Cloud services firstly provide increased stability, reliability and security for financial institutions since the outages that regularly happen with traditional data centres are far less frequent. There are also significantly fewer successful hack attempts that may jeopardise consumers' data. This is due to the fact that CSPs have a core expertise on security because their business model depends on it and they employ large teams of security experts solely focused on cyber protection. Secondly, cloud services provide a means for financial services firms to exit the legacy IT infrastructure that they have been using in some cases for up to 40 years. That sort of old infrastructure creates various risks for financial institutions in terms of safety and business model that public cloud-based solutions can address with improved resilience, costs and scalability.

Another industry representative noted that there was initially a great deal of concern over cybersecurity when the use of cloud was first discussed. Such risks cannot be completely eliminated, but the major CSPs are tackling them in a very effective way, investing in state of the art tools and monitoring capacity at a level that significantly outstrips the ability of any individual financial company.

2.3 Improving fraud detection and facilitating compliance

An industry representative explained that cloud services support dramatically improved fraud detection systems, utilising AI and integrating different data sets for spotting patterns that cannot be identified by manual processes. This allows a significant improvement of detection rates, which are typically under 1% (of fraudulent transactions) when they are conducted manually on separate data sets, and also a decrease of false positive cases.

Another industry representative added that cloud-based compliance tools allow global financial companies to pool easily relevant customer and transaction data on a large scale so that AI can be applied. This supports the tackling of money laundering, international sanction, suitability and fraud-related issues in a much more effective way, which constitutes a game changer for large insurance companies that spend significant resources and time on dealing with these issues.

A regulator agreed that cloud services may play a role in improving risk management, in addition to enhancing process automation and customer service. The ability to deal with data in a much more efficient way supports progress in terms of compliance and fraud detection in the insurance sector and has allowed for example the reduction of the levels of fraud related to motor vehicle insurance claims.

3. Challenges posed by the development of cloud services

3.1 Issues related to the underlying data regimes

An industry representative emphasized that many jurisdictions are increasingly requiring all data to be kept locally for data protection purposes, which could be at odds with one of the objectives of cloud usage, which is to generate benefits from scale. This needs to be considered in future cloud and data regulation developments. There are also many uncertainties concerning who has jurisdiction over cloud data. Contractual provisions to this effect can be overwritten by legislation, which can lead to sovereignty and national security questions. Certainty and clarity in this area would be welcomed by private sector actors. The industry speaker also mentioned the European project (GAIA-X) aiming to develop a cloud infrastructure and data ecosystem in the EU based on European standards. While their firm supports this project which may increase competition in the cloud market, it is important to consider that the cloud market is global and should remain so without geographic segmentation. Global users indeed want to be able to choose from the whole range of providers available at the international level.

A regulator considered that the regulatory approach needs to ensure that consumer data is used in a fair and transparent way, with the highest ethical principles. This needs to be done from inception, because digital transformation must be embraced in a way that best serves consumers and service providers.

An industry representative added that the geopolitical risk related to cloud provision also needs to be considered. There need to be appropriate rules and regulations in place in terms of how data can flow or be used across geographical boundaries. Another aspect is that the ability to perform the administration of assets in the public cloud space could be compromised if the cross-border control infrastructure is unavailable or impeded. This issue has been identified by some of the main public CSPs, who are working on building capabilities to allow for country-based administration. In this area, legislation and policies could potentially speed up and harmonize such developments and hence reduce risk.

3.2 Operational and market structure challenges

A regulator underlined some challenges related to cloud implementation that concern both financial institutions and supervisors. For example, there are difficulties with the cultural changes needed to implement digital solutions, which can be a significant challenge for certain organisations. There is also the question of the appropriate management of the shared responsibility model between the CSPs and financial service companies. Financial services companies also face potential lock-in risks with CSPs, which is why a number of financial companies are deciding to implement multi-cloud approaches and further work is needed on the reversibility of cloud contracts.

The regulator was also concerned by the possible concentration risk in the cloud sector, because an excessive concentration in the market around a few major CSPs could potentially create financial stability and systemic risks.

4. Existing cloud outsourcing guidelines in the EU

A regulator stated that the guidelines issued by the European Supervisory Authorities (ESAs) on the outsourcing to CSPs are an important first step in facilitating the dialogue between supervisors and market stakeholders. The guidelines have also contributed to improving market practices and transparency with a clarification of contractual arrangements for example.

An industry representative confirmed that significant progress is being made with the implementation of these guidelines, which are an adequate basis for further improving the European cloud framework. The work on harmonizing requirements for cloud services in the EU should nevertheless continue, because there are still duplicative or overlapping requirements that need to be eliminated for these measures to remain manageable for the industry. In the definition of guidelines, the right balance also needs to be struck between risk mitigation objectives and ensuring that customers can reap the benefits of the cloud.

Another industry representative stressed that there is a very strong common interest between regulators, cloud users and

the CSPs in getting the approach right on cloud guidelines. Standardisation needs to be improved in the cloud market, but in a pragmatic and progressive way. The guidelines on outsourcing provided by EIOPA and the other ESAs are well thought through and make a very strong basis. There are also many advantages in having a European-level agency that works in close coordination with the local authorities on these issues in order to ensure that harmonisation progresses across Europe. This will simplify the terrain for all the players. One objective of this harmonisation work is to ensure that there is a level playing field between CSPs and their users in the current context where market power is largely concentrated amongst a handful of CSPs. Standards can indeed help users to better negotiate sufficient reversibility of cloud contracts and adequate audit rights for example.

5. Measures proposed for mitigating digitalisation risks

5.1 Proposed Digital Operational Resilience framework

A policy-maker acknowledged that the current financial regulation needs updating and completing in order to take into account the changes brought by digitalisation. A new Digital Finance Strategy for the EU (DFS) will be proposed by the end of September, aiming to ensure that the EU financial sector embraces the opportunities offered by the digital revolution[2]. Concerning the risks associated with digitalisation the Commission proposes adapting the existing financial services legislative framework with respect to consumer protection and prudential rules to the new digital environment and also implementing a new EU framework for strengthening digital operational resilience in order to take into account the new challenges that the increasing dependence on ICT and data are creating[3]. This cannot be done entirely through the existing regulation, and so the Commission is considering some new legislative measures that would allow the enhancement of current cyber-resilience approaches in the financial sector, as well as an oversight mechanism of critical ICT third-party service providers, potentially including CSPs[4].

An industry speaker considered that direct oversight may be an option for addressing some of the challenges associated with a broader adoption of cloud services in the financial sector. Another industry representative however emphasized that direct oversight should not absolve cloud users of their monitoring and auditing responsibilities in the context of cloud arrangements[5]. The first industry speaker also stressed that potential oversight arrangements need to be manageable for all stakeholders and that there needs to be an element of proportionality so that small and medium-sized companies can continue to benefit from cloud services in this new regulatory and supervisory environment.

A regulator stated that the direct oversight over the critical CSPs needs to be undertaken at the European level by a single European supervisor. A fragmented oversight of these providers by different member states would make no sense given the international coverage of CSPs. The regulator also agreed with the importance of proportionality for allowing the small and medium-sized entities to also embark upon the digital transformation.

An official agreed that these issues need to be addressed at the EU level. European approaches also need to have a broader international perspective, because cloud services are an area where Europe can take a lead in embedding the measures proposed globally.

5.2 European data frameworks

A public representative mentioned that the European Commission and the European Parliament are addressing the issues of risk reduction and trust associated with digitalisation also with new proposals regarding data. The new European strategy for data proposed at the beginning of 2020 is due to complete the General Data Protection Regulation (GDPR) and the E-Privacy Directive that have been effective for protecting the data of individuals. However standards concerning access to data do not always seem to be properly applied, because customers in some cases are not able to access in a practical way their own data that is held by some big tech companies. Further consideration needs to be given as to how the data regulations can be applied in a practical way because such issues with access to data potentially undermine consumer trust. In order to achieve a well functioning internal market, there also needs to be a balance in the legislation between the interests of European citizens and of the industry, and the expertise of academics and researchers also needs considering in these innovative areas. The data that financial institutions and digital companies collect from European citizens should be used to their advantage, and not just to the advantage of financial service providers.

This issue led the public representative to comment on the taxation of the profits made with digital services. A strong view of the Parliament is that taxes should be imposed where profits are made, even if tech companies operate globally. Changing tax regulation with regard to digital services in order to make this possible will help to convince European citizens that they are receiving the benefits arising from the usage of their data and that these activities are properly regulated.

---

[2] https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en
This framework pursues 4 main objectives : (i) Tackling the fragmentation of the Digital Single Market for financial services; (ii) Ensuring that the EU regulatory framework facilitates digital innovation in the interest of consumers and market efficiency; (iii) Creating a European financial data space to promote data-driven innovation and (iv) Addressing new challenges and risks associated with the digital transformation.

[3] The increasing level of digitalisation of financial services coupled with the presence of high value assets and (often sensitive) data make the financial system vulnerable to operational incidents and cyber-attacks.

[4] The Commission is proposing a new framework for strengthening digital operational resilience built around five pillars : i) a coherent baseline for ICT risk management requirements, hinging on the cyber-risk management concept and which would be shaped and built upon internationally agreed standards guidance; ii) a cyber resilience testing framework to periodically assess financial institutions' cyber vulnerabilities; iii) a comprehensive framework for reporting cyber accidents, which would improve the flow of information between sectors and between the industry and supervisors; iv) an oversight mechanism of critical ICT third-party service providers, potentially including CSPs and aiming to strengthen outsourcing requirements and provide for a direct oversight of activities at individual levels; and v) the encouragement of financial institutions to share information about cyber threats amongst themselves, as well as, possibly, with the regulators.

[5] In the shared responsibility model used in the context of cloud outsourcing arrangements, security, risk management and compliance responsibilities are shared between the CSP and the financial institution, but the latter institution retains the ultimate liability for its own operational resilience and business continuity.

5.3 Enhancement of the EU cybersecurity framework

A policy-maker stated that a growing reliance on digital processes and third-party providers requires increased cybersecurity and the capacity to adapt to fast evolving risks and challenges.

A public representative explained that the Parliament is constantly working to improve cybersecurity regulation, which is one of the key topics related to digitalisation. Legislators and regulators need to adapt to the speed of development of technology. In order to earn customers' trust, cyber-resilience standards need to be applied both to the financial institutions and the CSPs. To this end, a cybersecurity certification scheme is currently being developed by the European Union Agency for Cybersecurity (ENISA) and should be shortly implemented.

A regulator stressed that standardisation is important in this area. Harmonizing cyber-risk taxonomy and incident reporting at the European, if not at the global level, is essential. The current fragmented system is inadequate because it obliges providers to report incidents to multiple authorities using different sets of requirements. ■