



# EFR PAPER ON CLOUD OUTSOURCING

## Executive Summary

Financial services providers adopt the cloud to be able to leverage new technological developments and provide innovative solutions to their clients in a secure manner. However, with many regulatory approaches the resulting fragmentation raises hurdles to the use of cloud solutions. This paper presents several considerations of how EU policy makers could develop the cloud services market, increase harmonisation and provide financial institutions with the certainty needed in their digitisation process.

To reach these objectives, the EFR has the following recommendations to EU policymakers:

- Regulatory fragmentation should be tackled by taking harmonised approaches at EU level, while avoiding divergent initiatives at national levels. This implies establishing a framework for mutual recognition of outsourcing agreements approval, and mechanisms to solve frictions related to extraterritorial reach of rules.
- Any supervision of Cloud Service Providers (CSPs) should be undertaken at the CSP level, rather than by financial supervision authorities. In that regard, the EFR considers the EU should adopt an objective, outcomes-based approach, rather than implementing specific requirements. It would indeed give organisations enough flexibility to be agile in reaching the stated outcome while preventing a competitive disadvantage for EU financial services firms operating in other markets.
- The financial services sector is supportive of EU ambitions to foster Europe's own capabilities in cloud computing since it could address current market imbalances by introducing greater competition. CSPs are becoming critical infrastructure and Europe needs to establish capabilities to remain competitive in the long term. However, significant investments in the long run are needed to enable the emergence of European CSPs offering the same level of technologies and services as existing providers. In any case, companies and individuals within the EU should remain able to freely choose cloud services providers.
- Finally, reducing fragmentation at EU-level requires establishing minimum baseline requirements avoiding gold-plating, and consistently harmonising supervisory practices across jurisdictions. To that end, a harmonised European approach proposing minimum requirements for cloud providers based on supplements to the provisions of the GDPR, as well as coordination among national competent authorities will be critical to ensure legal certainty and prevent inconsistencies within the European market.

## 1. Rapid adoption of the financial services regulatory & supervisory framework for cloud outsourcing

The use of cloud can offer a number of advantages such as increased IT resilience, economies of scale, flexibility, operational efficiencies, and access to digital innovation, with a cost-effectiveness and enhanced security that, if managed correctly, are better than for traditional data centers. The cloud is also a key enabler for the adoption of new promising technologies such as Big Data, Artificial Intelligence (AI) or Distributed ledger Technologies (DLTs). Last but not least, many software providers that traditionally offered on-premise solutions have also switched their services to cloud due to the flexibility of these environments.

Several regulatory authorities, whether at national or European level, have published in the past years guidelines or recommendations on cloud outsourcing. While these seek to enable the use of cloud and at the same time ensure adequate security, they also pose challenges, as the current regulatory environment is characterised by fragmentation, ultimately leading to overlapping or redundant obligations for outsourcing institutions. In addition, in a global context, data localisation requirements present a particular challenge in this regard, where significant costs must be incurred for companies operating internationally and may even increase the exposure to cyber and operational risks. This is also key in Europe. It is essential to remove any data localisation requirements allowing companies to store and process data wherever they choose. These restrictions increase operating costs and hinder the scalability of global services. Uncertainty about how different regulations apply globally can also become a discouraging factor, especially given the scale of investments in time and resources involved.

We believe that in order to facilitate the adoption of cloud, regulators across the EU should adopt a transparent and consistent approach and a framework for mutual recognition. This would significantly reduce both fragmentation and redundancies, e.g. with regards to required approvals of cloud outsourcing agreements that are required in some jurisdictions. Also in a more and more connected world, mechanisms to avoid gaps between jurisdictions are needed.

In anticipation of further work at the international level through the FSB (Financial Stability Board), BCBS (Basel Committee on Banking Supervision) and IOSCO (International Organization of Securities Commissions), we encourage EU policy makers to adopt a consistent European approach in order to better influence discussions at global level. This will support Europe's ability to set global rules and also provide the required scale to create globally competitive European CSPs and prevent a competitive disadvantage for EU financial services firms operating in other markets.

As a first step, at European level, there should be a common approach, for example regarding requirements for notifications when outsourcing services. Achieving common criteria is needed to facilitate greater scalability in cloud solutions when operating in several EU Member States, while avoiding an unlevelled playing field.

## **2. Systemic oversight of cloud providers by dedicated European supervisors**

The potential for cloud providers to become critical participants in the financial system is widely recognised. However, this risk is not exclusive to the financial sector; the provision of cloud computing is becoming essential across all sectors, including critical ones such as health care or the government services. While cloud providers do not currently represent a systemic risk to the European financial system, as more financial institutions, directly or indirectly (through the services provided by other third party providers), come to rely on a limited number of CSPs and deploy more critical services to the cloud, the risk that some CSPs become a single point of failure increases. Considering the growing role of this technology, which might also be accelerated by the COVID-19 pandemic, we offer some considerations for EU policy makers.

The cost and benefit of the various possibilities to establish dedicated CSPs supervision should be examined to ensure that concentration risk is properly monitored and managed. In considering whether to regulate cloud providers, we encourage policymakers to take also stock of these companies' role in the wider economy outside of financial services. Many authorities recognise that concentration could pose a risk to the stability of the financial system. But regulation so far (e.g. EBA Outsourcing Guidelines) does not apply to CSPs. And risks originating in cloud services are monitored through financial supervision authorities, which relay to financial entities the obligation to control and report the outsourcing arrangements they have entered into. The focus has been on financial institutions, through an adequate risk assessment, sound governance and risk management of all aspects of CSP relationships. This has led to monitoring and audit requirements for outsourcing financial institutions which are difficult to impose and enforce, while at the same time, there is a lack of supervisory certainty with regards to collaborative approaches, such as the Collaborative Cloud Audit Group (CCAG). However, financial institutions individually do not have the bargaining power to impose conditions on global providers, also lacking the required information to assess the risk to financial stability, or the market as a whole. Authorities are better positioned to monitor risks at system level and to take action in case it is deemed necessary.

Considering the relevance of CSPs for other sectors, it is also clear that relying purely on financial services supervision to achieve wider policy goals could also have severe impacts on the development of a competitive European cloud market for financial services, fragmenting the provision of cloud services in two parallel markets, as CSPs will adapt their offers and prices depending on whether their clients are supervised financial entities or not.

In addition, other initiatives that could also help to manage concentration risk would be the promotion of certification schemes for CSPs — that would avoid each financial institution to repeat the assessment of the same provider

increasing the efficiency of the process — or the definition of standard contractual clauses for cloud arrangements, ensuring a minimum standard for CSPs to facilitate FIs compliance with outsourcing regulation.

Regardless of which model the EU were to choose, any supervision of cloud service providers should be undertaken at the CSP level, once for an entire industry, rather than requiring each individual financial services organisation to perform such checks, reports and controls. Clarifying the reliability of certifications (e.g. relating to data protection or cybersecurity), third party audits (private-or public-sector led) or the results of pooled audits would result in a more business friendly environment and reduce the total compliance burden on EU businesses without reducing the level of supervision or the quality of controls. One additional objective should be to reduce duplication of the compliance burden between firms using cloud service providers. Rules such as the EBA Guidelines which allow for pooled audits are a good step, but the EU will want to consider in time if a more direct regime would be beneficial to the wider economy by focusing compliance on the providers rather than the users.

### **3. Foster the development of a competitive European Cloud Market**

Cloud computing is at the heart of the digital transformation, enabling significant gains in efficiency, innovation, data processing capabilities, and cyber security. As a result, cloud infrastructures and services are a critical sector for the development of the European digital economy and its international competitiveness. Yet on the supply side, the market in Europe (and indeed the world) is dominated by a few Big Tech companies which suggests that further competition is needed. There are very few EU-based service providers and those that exist are not only smaller than the international actors, but they also do not provide the same level of functional richness that is attractive to businesses.

Fostering the development of European CSPs must therefore be a high priority for Europe in order to bolster the strength and competitiveness of both Europe's digital market and the other sectors that rely on it. To support this, there should not be any barrier to the use of CSPs among EU Member States (i.e. Freedom of Services should fully apply). However, although increasing European strength in cloud governance may be possible in the shorter term, it should be stressed a fully competitive offering from a European cloud provider can only be envisaged in the medium to long-term as it would be unrealistic to expect European CSPs to soon provide the same technologies and functionalities as established providers. For that purpose, targeted measures will be essential to foster the investments needed, also very importantly on skills and training programmes, to reach the critical mass and scale required to deliver the sort of features and services expected of a cloud provider and be consistent with the Commission's ambitions of creating a "data agile economy".

European stakeholders would benefit from the emergence of European CSPs in order to increase the number of cloud providers which would allow the development of a more competitive and less oligopolistic market and lead to more innovation, improvement in the pricing of services, and a reduction of concentration risks. The proposed European cloud services marketplace will also help to address the low visibility on the market of smaller European CSPs and uptake by SMEs and the public sector.

As an industry that relies heavily on cloud services, the EFR therefore supports the EU's goals of fostering Europe's own capabilities in cloud computing and addressing imbalances in market power. We consider that any EU policy action should indeed prioritise encouraging competition and the entrance of new providers serving the financial services sector among others. Greater competition is ultimately the best solution, not only in terms of pricing, but also in terms of innovation (either in technology and functionality). In this context, financial institutions, as any other company or individual, should be able to freely choose service providers under commercial and due diligence considerations.

### **4. EU-wide harmonised requirements to set global standards**

In the Commission's Data Strategy, European authorities unveil their ambition to invest in the creation of common data spaces and the setup of a European federation of trustworthy cloud infrastructures, leveraging on existing national cloud federations. Action at European level will help to avoid multiplication of national level initiatives and provide the capacity to achieve the necessary scale. The Memoranda of Understanding planned for Q3 2020 should help to refocus disparate efforts into fewer but more efficient workstreams.

Against this background, it is fundamental to deliver a harmonised European approach to avoid legal uncertainty and prevent inconsistencies that would arise from a disparity of parallel national regulatory initiatives. A proportionate level of regulation must therefore guarantee existing high standards of data protection and security without creating entry barriers for new service providers. Overly burdensome and costly regulatory requirements may ultimately restrict competition and further cement the current oligopolistic market structure. More precisely, there should be a consensus on the essential requirements that this framework must contain, i.e. guaranteeing audit rights, certification

schemes, preventing vendor lock-in effects. Such requirements will help to facilitate financial institutions' secure adoption of cloud services by establishing clear expectations on CSPs.

Current GDPR legislation provides a high level of protection for European customers and clients, who are guaranteed that their data cannot be shared within or outside European borders without their consent. Based on this framework, EU authorities must introduce additional protections. For instance, the GDPR should be accompanied by high standards for availability and data recovery. It must be ensured that cloud service users and clients are able to access their data based on a committed service level agreement. In addition, clients and users need to be able to trust that the level of protection is consistent across the European Union, which will require further harmonisation. Finally, EU authorities should work to address concerns around data protection which have arisen as a result of the extraterritorial reach of legislation in third countries. Therefore, the EFR supports the European authorities' efforts to reach a solution with the authorities in third countries in order to ensure that EU data privacy laws are upheld.

In addition, other initiatives that could also help to manage concentration risk would be the promotion of certification schemes for CSPs – which would alleviate the burden arising from each financial services firm having to repeat the assessment of the same provider, thus increasing the efficiency of the process – or the definition of standard contractual clauses for cloud arrangements, which would ensure a minimum standard for CSPs to facilitate financial institutions compliance with outsourcing regulation. By such standardisation and clarification, this will help to ensure that CSPs adhere to a minimum standard of controls and procedures as expected by the financial industry and provide assurance on the integrity and effectiveness of the CSPs' internal controls and safeguarding the financial institutions' customers' interest.

In addition to a top down harmonised framework of minimum requirements, to avoid fragmentation of regulation along national lines, the EU must harmonise bottom up regulatory and supervisory practices as designed by the EBA and EIOPA guidelines. Consequently, national competent authorities will also have to coordinate towards the convergence of supervisory requirements, such as outsourcing notification or information obligations. Avoiding national fragmentation of supervisory practices will preserve a level playing field and prevent arbitrage that would hinder the emergence of a European "data agile economy".

The European Financial Services Round Table (EFR) was formed in 2001. The Members of EFR are Chairmen and Chief Executive Officers of international banks or insurers with headquarters in Europe. EFR Members believe that a fully integrated EU financial market, a Single Market with consistent rules and requirements, combined with a strong, stable and competitive European financial services industry will lead to increased choice and better value for all users of financial services across the Member States of the European Union. An open and integrated market reflecting the diversity of banking and insurance business models will support investment and growth, expanding the overall soundness and competitiveness of the European economy.