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

Prof. Dr. Joachim Wuermeling

Member of the Executive Board,
Deutsche Bundesbank

Reaping the benefits of going digital without compromising on stability

Cloud computing is a key technology in the digitalisation of the financial industry, promising a boost in computing capacities and software capabilities. As banking supervisors, we want to help smooth the digitalisation process so that the financial sector can reap the full benefits of new technologies. We're open-minded about cloud computing and other technologies. At the same time, driven by our mandate for ensuring financial stability, we will not lose sight of the risks associated with digital transformation.

Benefits of cloud technology

Cloud services open up a wealth of benefits and innovative potential, not least because they enable banks to tap into huge computing capacities and state-of-the-art software capabilities.

Cloud usage can also boost the take-up of fresh technologies like big data analytics and artificial intelligence, especially among small and medium-sized banks. Moreover, cloud service providers can better equip banks to fend off certain types of cybercrime.

Challenges

Needless to say, where there is light, there is also shadow. Cloud technologies introduce risks that require proper management – all the more so when they are deployed in risk-relevant areas such as credit checks, capital planning and money laundering prevention.

At the individual-bank level, IT and cyber risks are typical challenges, of course. But when clouds come into play, there is also the matter of outsourcing risk because cloud services are often provided by third parties. One risk is the weak negotiating position and limited control that banks might have vis-à-vis large, internationally active cloud providers. Then there is the risk of vendor lock-in, which might materialise if a bank cannot easily switch between providers due to technical barriers, prohibitively high switching costs or contractual issues.

There's a golden rule that (prospective) outsourcers to cloud providers need to follow: you can't outsource responsibility. A bank might transfer some of its IT processes to an experienced IT service provider in an outsourcing arrangement, but it can't offload the responsibility. That's why every bank has a duty to monitor and control the risks arising from the outsourcing relationship.

Way forward

Without losing sight of the risks, I regard supervisors as enablers of digitalisation in the banking sector. We will naturally remain within the scope of our supervisory mandate, which provides for technology and market neutrality.

Clear and regular communication of our expectations is crucial. Last year, European supervisors communicated their expectations regarding risk management at banks, in the shape of the revised EBA Guidelines on outsourcing arrangements. These guidelines are an essential step to ensure planning security, and we are currently working on their national implementation.

Furthermore, we encourage banks to make better use of instruments already embedded in the supervisory framework. Joint reviews (pooled audits) of cloud providers are one way in which banks' internal audit units can gain high-quality insights into the interface between bank and third-party services. This can help them assess a cloud service provider's risk management and the internal controls it has put in place more effectively and efficiently.

> *Without losing sight of the risks, I regard supervisors as enablers of digitalisation in the banking sector.*

Of course, supervisors may have to access and check third-party cloud service providers, too. EBA guidelines already stress the importance of having suitable clauses in outsourcing contracts, and we will examine their quality and effectiveness closely.

Further steps are being taken to forge an effective European oversight framework for monitoring the activities of critical third-party providers. In March, the European Commission launched a public consultation on a digital operational resilience framework for financial services, and it will build on this consultation when conducting its ongoing initiative to develop a cross-sectoral financial services act on operational and cyber resilience. We also welcome the European Commission's initiative to set up an EU Cloud Rulebook including standard contractual clauses for cloud use in the financial sector.

Looking ahead, supervisors will continue to strive for close European and global coordination in this field. We are guided by the goal of enabling banks to reap the full benefits of going digital without compromising on financial stability. ●

Joachim Wuest

Head of Financial Services,
Google Cloud Germany

European banks accelerate digital transformation with cloud adoption

Financial services institutions face continued pressures in the race for business transformation. This has never been more apparent than now during the COVID-19 pandemic which made consumers shift to digital banking channels at an unprecedented rate, whilst capital markets firms are dealing with extreme volatility. Cloud technology presents significant opportunities to help financial institutions standardise in multi-cloud or hybrid cloud environments, streamline tasks related to internal risk assessment, compliance and governance, improve visibility through the use of machine learning and data analytics, and minimise complexity with modern collaboration tools.

We see three key areas where cloud technology can help transform the financial services industry for the future:

1. Cloud can help reimagine customer relationships using data and artificial intelligence (AI);
2. Cloud can transform and modernise the use and management of data with the help of machine learning (ML) addressing one of the key challenges faced by financial services institutions;
3. Cloud can help drive operational improvements within core systems.

Whilst financial institutions in Europe were relatively slow to adopt public cloud at first, we are seeing an accelerated trend toward cloud across the Eurozone aimed to redefine and innovate banking services at large. Our recent announcement with Deutsche Bank to form a long-term global partnership to drive a fundamental transformation of banking and enable co-innovation between the two companies to create the next generation of technology-based financial products is a strong example of this type of strategic approach to cloud. This tendency can largely be attributed to the growing understanding of cloud security capabilities, and trust in the industry.

Trust, security and sovereignty

Financial services is an industry that is based on trust, and security and privacy are absolutely critical.
At Google Cloud, we provide a number of technological advances to support our customer privacy and security controls to achieve various strategic autonomy and sovereignty requirements:

- Data Locality Controls are available for various services enabling customers to have sole control on the storage location of all copies of their data including backups;
- Confidential Computing of VMs allows to encrypt customer data also during processing;
- External Key Management enables data encryption keys hosting offsite and air gapped from Google;
- Access Transparency, Access Approval and Key Access Justifications tools enable customers to understand why access for their data is being requested and deny access to their data.

Embracing open standards and multi-cloud approach

We also understand customer and regulator concerns over potential market concentration and systemic risk. We agree it is critical to ensure that proper risk mitigations are in place. Google has a deep commitment to open source, reflected in our contributions to projects like Kubernetes, which has been originally developed by Google, then open-sourced and is now the industry standard in portability and interoperability in the cloud. Another example is TensorFlow, our state-of-the-art AI and ML technology, which we open-sourced to allow the broader, global community of researchers to innovate.

We support openness and the ability for financial firms to freely choose which services and providers will best meet their needs, without being locked into a single vendor. That's why we introduced our cloud-native platform called Anthos that runs in a data center, in one cloud or in multiple clouds to give firms the freedom of choice and workload portability. For example, if a bank is running Kubernetes or open source containerisation, they can use Anthos to support workloads across any cloud, including through local providers in Europe.

We believe in open source technology and an open cloud, and work to support and enable our customers' choice. ●

Christopher P. Buttigieg

Chief Officer Supervision,
Malta Financial Services Authority

Cloud computing and adapting Financial Supervision to the digital era

Cloud computing is a facilitator for enterprise business transformation and has the potential of significantly changing the way financial services are offered to clients. Leaders in financial services and practitioners are progressively acknowledging that cloud computing can facilitate the: [a] storage of data and applications; [b] access of advanced software applications via the internet; and [c] application of advanced analytics for better and more integrated insights.

The paradigm shift in the conduct of financial services through FinTech brings about new risks and challenges, which also require a change to our approach to financial supervision.

This article briefly outlines: [a] the policy and regulatory work being carried out by the European Commission to create a framework for the better use of cloud computing in Europe; [b] the operational and systemic risks which emerge from outsourcing to the cloud service providers ('CSP'); and [c] how these risks are being dealt with by financial supervisors at European level. ▶

▶ The Commission is currently working on projects, which will further reap the benefits from cloud computing at European level. Specifically, the establishment of a European federation of cloud infrastructures and services, a European marketplace for cloud services, and a governance framework that includes an EU cloud rulebook. Largely driven by the Digital Single Market, these projects entail: [a] the free flow of non-personal data; [b] data portability; [c] cybersecurity; [d] data protection in the cloud; [e] standardised cloud service level agreements; [f] cloud use by the financial services sector as pre-empted within the FinTech Action Plan 2018; and [g] a European mapping of data flows.

Outsourcing to CPSs gives rise to governance and oversight challenges, for example the dynamics of the management's oversight and control of data, which is a critical function for every organisation, which must be adapted to the cloud environment. It also brings new dimensions of operational risk, particularly cyber security risk, and possible concentration risk, which must be monitored by prudential supervisors to ensure that these are properly mitigated. In addition, discussions are on-going on the possible systemic risks brought about from outsourcing to the CSPs, above all if financial services firms rely on a handful of dominant CSPs, the failure of which could have a meaningful impact on such firms.

In the field of prudential supervision, the European Banking Authority ('EBA') and the European Insurance and Occupational Pensions Authority ('EIOPA') have both issued guidelines specifically dealing with outsourcing to CSPs. The European Securities and Markets Authority ('ESMA') is also consulting on a set of guidelines in this area. The guidelines, which converge on substance and address cloud outsourcing from a multidisciplinary perspective, are being implemented at national level and monitored by national financial supervisors.

More generally, FinTech presents challenges that are shaping the art and craft of financial supervision, including the methodologies and processes, which today incorporate: [a] data driven solutions and analytics for supervision; and [b] technology whereby supervision is partly carried out on a real time basis.

> *Europe is strategically going forward in closing outstanding gaps, maximising the potential of the cloud, and mitigating substantial risks.*

Europe is strategically going forward in closing outstanding gaps, maximising the potential of the cloud, and mitigating substantial risks. Nonetheless, the fast-moving pace of emerging technologies is increasingly posing challenges to financial supervision, which has to continue keeping abreast and adapting to the emerging new technologies. Ensuring that we are able to supervise the industry is not enough. As outlined in this short article, benefiting from the opportunities which this presents by adopting technology to make supervisory processes more efficient thereby, allowing financial supervisors to optimise resources, and be more effective in achieving supervisory objectives, is equally important. ●

Gabriel Bernardino

Chairman, European Insurance and Occupational Pensions Authority (EIOPA)

Cloud services: challenges and opportunities for the insurance sector

Cloud computing technology is seen as key enabler of agility and data analytics allowing firms to get quick access to new business models and technologies such as Artificial Intelligence and Machine Learning. Given that data processing and data analytics have historically been at the very core of the business of insurance undertakings, the relevance of cloud computing for the sector is no surprise.

Based on EIOPA's thematic review on the use of Big Data Analytics in motor and health insurance, in 2018 cloud computing services were already used by 33% of insurance undertakings, with a further 32% saying they would be moving to the cloud over the next 3 years (i.e. by 2021).

> *Digital finance is an important driver of Europe's financial services.*

At the European Insurance and Occupational Pensions Authority (EIOPA), our view is that we should be able to strike a balance between enhancing financial innovation and ensuring consumer protection and financial stability.

This is also true for cloud services, which are becoming common place in Europe's financial sector. Today, cloud outsourcing services

have become more standardised, allowing services to be provided to a larger number of different customers in a highly automated manner and on a larger scale. ▶

However, although services can offer the insurance sector the advantages of economies of scale, flexibility, operational efficiencies and cost-effectiveness, they also raise challenges. This includes issues related to operational resilience, data protection and location, security issues and concentration risk; large suppliers of cloud services can become a single point of failure when many undertakings rely on them.

Understanding how new technologies and business models drive new risks and opportunities is crucial, as is insurance regulation that is fit for purpose.

Earlier this year, EIOPA issued guidelines for cloud outsourcing with a view to providing clarification and transparency to users of cloud services, to reduce the risk of possible regulatory arbitrage. The guidelines also foster supervisory convergence regarding the expectations and processes applicable in relation to cloud outsourcing.

The guidelines were developed following a public consultation with stakeholders. They are principle-based and cover a number of key areas, such as the pre-outsourcing analysis, covering risk and materiality assessments of outsourcing arrangements and contract clause requirements.

In the area of governance, the guidelines cover documentation requirements, including notification, to supervisory authorities. The guidelines also address the management of access and audit rights, the security of data and systems, sub-outsourcing, monitoring and oversight, and exit strategies.

Looking ahead, and taking into consideration the upcoming Digital Finance Strategy of the European Commission, EIOPA will consider issuing further guidance on outsourcing in other activities / areas of the insurance value chain, with the aim to clarify supervisor expectations in this area, improve the governance of such processes and provide transparency to the market, without lowering standards.

Digital finance is an important driver of Europe's financial services. However, innovation cannot be at the detriment of consumers, nor can it call into doubt the security and resilience of Europe's insurance industry. EIOPA will therefore continue to work with a range of stakeholders to further the European digital agenda and create a Europe fit for a digital age. ●

Tsvetelina Penkova

MEP, Committee on the Internal Market and Consumer Protection, European Parliament

Europe's approach on cloud and data in a post-Covid world

The use of cloud services has proven to be largely beneficial not only for the financial sector but for all economic actors as well as for the consumers in their everyday life. Agile data storage, faster processing, scaling up of operations and cost optimisation are only a few of the benefits that the cloud provides. In order to take full advantage of the technology and to maintain a high level of privacy and security, both financial institutions and cloud service providers in Europe are subject to multiple regulations, some of which have become world standards, like the GDPR.

But beyond the existing (and forthcoming) regulations, it is important to properly implement those that are already in place and to define clear responsibilities in the contractual arrangements between the cloud providers and the financial institutions.

The realisation of the huge potential of the data economy has spurred a number of initiatives in Europe, which aim to boost innovation and technology, starting with the Digital Single Market Strategy and coming to the new European Strategy for Data.

Data sharing requirements, common sectorial data spaces, including for financial services, federalisation of cloud services (like for instance GAIA-X, the newly created Franco-German cloud consortium) are all relevant workstreams evolving in the EU. However, in order for these to work we need incentives for data sharing, interoperability of data systems and clear competition rules, while always accounting of the principle of global convergence.

Another important aspect of cloud is security. Some argue that the cloud provides higher security than in-house infrastructures. While this is true in many cases, it is important that we nurture a robust security practices with the participation of all interested stakeholders, CSPs and users alike. The Cybersecurity Act and the soon-to-be revised NIS Directive are a good basis to achieve this goal and now we await the first cybersecurity certification scheme for cloud services, which is being developed by ENISA.

> *"We need incentives for data sharing, interoperability of data systems and clear competition rules.*

Finally, for our data economy to flourish, we also need adequate resources. The current pandemic situation has imposed additional budgetary challenges for Europe, but we call on the members states to be more ambitious in the upcoming MFF negotiations and remain dedicated to fostering a commensurate Digital agenda for Europe. ●

Patricia Plas

Director of AXA Group Public Affairs - AXA Group

Is the EU policy on Cloud and Data up to the digital challenges?

Since 2016, the European Union (EU) has taken steps to develop a regulatory framework on data with the GDPR, the EU Cybersecurity Act, and the Regulation on the free flow of non-personal data, among others. Against this background, the Commission now aims to make of Europe a trusted digital leader. However, will the new Digital Strategy be adequate to change EU's image of that of a regulatory superpower to an innovation powerhouse? Does this approach have the potential to expand worldwide? How to ensure that EU calls for technological sovereignty do not result in a protectionist approach?

The EU is taking a more assertive approach to digital challenges to differentiate itself on the global stage by reflecting about digital sovereignty, as a mean of promoting Europe's leadership and strategic autonomy. This translates into ambitions to develop data governance rules and sovereign digital infrastructures.

A data governance framework facilitating data collection, processing and sharing should enable the EU to further translate its values and principles into the digital domain and share globally its experience in data protection. Nevertheless, to design a comprehensive digital approach, these key considerations must be balanced with competitive stakes so that EU stakeholders can take full economic advantage of the data economy. For instance, the creation of common data spaces dedicated to financial services or health, should help EU actors to benefit from the raw material of the digital economy that is non-personal data. However, some grey areas regarding the exact scope of these initiatives (e.g. the types of data involved, modalities of access, security safeguards) may act as a brake to a supportive contribution.

Moreover, there is no question that Europe lags far behind Chinese and US firms on several technological and industrial capacities fronts. To date, the EU focus has often been on data protection and security matters but going forward, ramping up capacities of the EU tech industry would be beneficial. One angle would be to boost some competitive edge, among which leveraging industrial data and taking advantage of a more decentralized digital ecosystem, with the rise of the Internet of Things, 5G and edge computing. In this sense the EU aims to develop a secure cloud infrastructure. However, while a European actor could indeed diversify the cloud market and bring the flow and storage of data under greater European control, it is unlikely that it would be able to compete with other cloud providers on the whole supply chain, in the short term.

> *How to enable the EU to further translate its values and principles into the digital domain.*

These ambitions demonstrate that the geography of the cloud matters to the EU. More globally, the reflection on the need for sovereign digital technologies has gained momentum in the past few years. Some EU companies operating globally, and non-European observers are concerned that this approach could result into protectionist measures. Therefore, while Europe's ability to act independently in the digital world should be encouraged to avoid overreliance on non-EU firms and to feed into recovery effort from the covid-19 crisis, it is critical that the EU remains open for businesses operating with foreign technologies as well as for foreign participation in the EU digital market. ●