

Outsourcing Cloud Services for Financial Entities: Opening the PanDORA's Box?

Dr. Dimitris Tsibanoulis, Senior & Managing Partner | Tatiana Kyttaroudi, Associate
02 April 2025

The increasing reliance of financial institutions on cloud outsourcing has raised significant regulatory, operational and cybersecurity concerns. Financial entities are progressively outsourcing critical services to a small number of third-party cloud providers, mostly based outside the EU, which often results in vendor lock-in, complex supply chains and heightened data protection risks. Financial institutions face challenges in ensuring compliance with EU regulatory frameworks, particularly the recent Digital Operational Resilience Act (DORA) and the emblematic General Data Protection Regulation (GDPR). These concerns have been further exacerbated by the extraterritorial implications of the US CLOUD Act, which may allow non-EU authorities to access financial data stored by US-based cloud providers.

To address the challenges that technology poses specifically for the financial sector, the EU introduced DORA to establish a harmonized framework for managing ICT risk. Under DORA, financial institutions must conduct rigorous pre-outsourcing risk assessments, ensuring that only cloud providers with robust security controls are contracted. The ECB has also issued a draft Guide on Cloud Outsourcing, which unambiguously states that institutions remain fully responsible for ICT risks and must implement comprehensive risk management frameworks, continuous monitoring and compliance safeguards.

A key question in this developing threat to the digital financial ecosystem is whether there are alternatives to the current cloud outsourcing model, in particular whether financial institutions can reduce their dependency on non-EU providers. Initiatives such as GAIA-X and European cloud solutions, including OVHcloud and Deutsche Telekom Cloud, were explored as potential pathways to enhance regulatory alignment and data sovereignty.

Multi-cloud and hybrid cloud strategies were also discussed as practical solutions for reducing concentration risks and enhancing operational resilience.

Proactive risk mitigation strategies from financial institutions are also imperative. Several measures can be adopted after careful deliberation, including clear exit planning, contractual safeguards, enhanced cybersecurity protocols and continuous regulatory compliance monitoring. These strategies are essential in ensuring that financial institutions can maintain resilience while benefiting from the efficiency and scalability that cloud solutions offer.

The financial sector faces a critical decision regarding the future of cloud outsourcing. Institutions must determine whether they will continue to rely on US-based cloud giants, despite the compliance and data protection challenges this presents, or shift towards European cloud solutions that align more closely with EU regulatory requirements. As regulatory scrutiny intensifies and financial entities navigate the evolving digital landscape with the introduction of AI-driven solutions, it is imperative to engage specialised and experienced legal professionals in Financial and IT Law, as well as data protection, in the drafting of company policies, protocols and procedures, data processing agreements and compliance training programs. In this way, the adoption of a strategic, risk-conscious and robust approach to cloud outsourcing will be achieved.

The discussion on cloud outsourcing and financial resilience will remain at the forefront of regulatory and business agendas. Financial institutions must stay ahead of regulatory developments and strengthen their internal risk management frameworks to ensure compliance and long-term sustainability.

Key contacts



Dr. Dimitris Tsibanoulis
Senior & Managing Partner
d.tsibanoulis@tsibanoulis.gr



Tatiana Kyttaroudi
Associate
t.kyttaroudi@tsibanoulis.gr

Tsibanoulis & Partners Law Firm

18 Omirou St.
106 72 Athens | Greece
T: +30 210 3675 100
W: tsibanoulis.gr



Disclaimer: This insight is for informational purposes only and does not constitute legal or other professional advice or services. It is not intended to be relied upon as a substitute for professional advice, nor should it be used as the basis for any decision or action that may affect you or your business. Before making any decision or taking any action that may affect you or your business, you should seek advice from a qualified professional advisor. We remain available should you require any further information or clarification in this regard.