

Tech Sovereignty in Financial Services: Balancing Risks with Global Competitiveness

This note sets out a risk-based perspective on technological sovereignty in financial services, including external data access and processing, the use of cloud and other emerging technologies. Existing regulatory frameworks, for example DORA, EBA Guidelines and GDPR, at the Union level support a risk-based perspective through financial entities' own governance, risk management and control frameworks. Importantly, established legal frameworks at the Union level should continue to apply to manage risk, adequately consider sovereignty risk, and deliver outcomes - resilience, security and compliance. EBF calls for a balanced strategy that combines financial entities' strategic decisions to bolster their resilience, competitiveness and diversification, with clear regulatory prioritisation.

In the current volatile geopolitical environment, discussions around Europe's sovereignty have multiplied and taken various forms (e.g., technological, operational, payments, monetary, and supply chain). In the context of operational resilience in finance, the focus should remain on retaining a resilient, secure and competitive European economy. This should be supported by the ability for financial entities to make informed, strategic choices about their third-party providers that strengthen their own resilience and support Europe's long-term competitiveness - without introducing additional mandates as sovereignty requirements, which do not account for existing regulatory requirements within the financial sector.

We are concerned to see a paradigm shift in current legal initiatives, such as the proposal for the Cybersecurity Act review (CSA2), away from a primarily technical-operational perspective toward a more pronounced consideration of geopolitical risks. This development is accompanied by structural uncertainties, limited legal clarity, and a role distribution that has not yet been fully clarified.

The EBF advocates for the ability for financial entities to manage the underlying operational, cyber and third-party risks associated with sovereignty considerations, through their existing governance, risk management and control frameworks, consistent

with current regulatory requirements and supervisory expectations. These requirements, such as those set out in DORA's Regulatory Technical Standards, require regulated entities to identify, assess and manage risks arising from their technology and third-party arrangements with a risk-based approach, based on their own risk profile and operating model, taking into account geopolitical risk.

This approach supports innovation by enabling financial entities to leverage global technologies and services (including cloud, AI and quantum) while maintaining robust risk management standards. It also allows financial entities to consider domestic or EU-based solutions where these are available and fit-for-purpose, based on assessments of risk, resilience and operational needs.

Crucially, this flexibility supports the continued development of a technologically advanced and globally competitive European banking sector, by including major actors extending beyond European borders and also by adapting to evolving cyber threats, operational risks and customer expectations.

Financial entities assess and manage their own risk and operational requirements based on their risk profile, operational complexity, business model and cross-border footprint. These decisions must balance regulatory compliance with financial-entity-**specific operational needs such as service availability, technological performance, scalability, cost efficiency and business continuity**. DORA embeds the consideration of geopolitical risk through all of these aspects and should remain the foundation of any financial sector focus on sovereignty.

Therefore, a one-size-fits-all approach for tech sovereignty requirements would undermine both resilience and efficiency.

Constraints without a balance between risk and operational requirements would place **European banks at a competitive disadvantage relative to global peers** and restrict access to cutting-edge technologies that enhance resilience, fraud prevention, innovation and customer experience.

Tech sovereignty, i.e. the ability to make self-determined decisions about the technology used, is a legitimate policy objective; however, as of today, the debate sometimes conflates various concerns and objectives. Legal measures and jurisdictional control are presented as the only protection against unlawful data access, while technical protections may prove more effective in practice. In this context, it is particularly relevant to consider that different risks require different mitigating measures and different objectives may compete with each other.

When it comes to ensuring resilience and data security, additional regulatory interventions that constrain financial entities' strategic investment decisions are not necessary since existing requirements already address underlying risks, including

concentration risk, location of data processing, supply chain risk management, exit planning, business continuity, legal and compliance risk. Existing frameworks should continue to be applied to manage unauthorised data access, cyber threats, operational resilience and concentration risk - and not as a route to introduce new “sovereignty obligations”.

Europe’s integration in the global economy is particularly relevant for cloud, quantum and AI services, where disparities in scale, maturity and functionality persist across markets. Moreover, **many European financial entities serve customers internationally and therefore require solutions that are globally interoperable, scalable and resilient.**

The EBF notes that is not an “either-or” choice between technological sovereignty and openness, but a **balanced, interoperable and risk-based strategy** built on four pillars:

- **Public-private partnership:** Fostering a **transparent, continuous dialogue** between policymakers and the industry is fundamental to facilitate industry’s competitiveness and to maintain operational imperatives like performance, scalability, and resilience.
- **Flexibility to deploy international partnerships:** Cooperation at international level in particular, remains a key driver of innovation and resilience.
- **Foster resilience through diversification:** Supplier and technology diversification enhances resilience without disconnecting Europe from global innovation.
- **Clear prioritization in policy requirements:** Not all dependencies pose equal risks; policy efforts should focus on areas of genuine strategic importance.

Maintaining **flexibility for banks to make technology and sourcing decisions within existing regulatory requirements is essential and aligns with the European Commission objective towards simplification.** Financial entities make long-term technology investments planned over many years. Predictability and regulatory clarity are therefore critical.

An entity-led, risk-based approach, as already implemented by entities that are both regulated and subject to supervisory oversight, remains the most effective way to address sovereignty-related risks. In practice, this is often supported through centralised governance models, common data architectures and globally integrated operating models that strengthen consistency, visibility and operational resilience. Measures that disrupt these established and integrated approaches may create unintended operational resilience trade-offs, while negatively impacting competitiveness and innovation in Europe’s banking sectors.

On the basis of the above, the European Banking Federation calls to consider the following definition of “tech sovereignty”:

“Tech sovereignty: *refers to a legal entity’s ability to preserve decision-making authority over the critical technologies on which it depends and to manage them effectively in order to ensure regulatory compliance, operational resilience and freedom of choice regarding suitable deployment models, physical infrastructure locations and data location within existing regulatory and risk management frameworks. This includes, among others : infrastructure, data, software and supply chains.*

For more information:

Alexandra Maniati

Senior Director - Innovation &
Cybersecurity
a.maniati@ebf.eu

Ingrida Taurina

Senior Policy Adviser - Innovation
& Cybersecurity
i.taurina@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 33 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and