

# Ensuring European Tech Sovereignty Through Resilience, Choice and Trust

*A policy perspective from Mastercard*

## Executive Summary

Europe's ambition to strengthen its technological sovereignty is both legitimate and necessary. Ensuring that critical digital systems are resilient, trusted, and aligned with European values is vital for economic stability, security, and competitiveness.

As the European Commission prepares to publish its Tech Sovereignty Package, Mastercard welcomes the focus on strengthening capacity, reducing systemic risks, and increasing Europe's long-term ability to shape its digital future. At the same time, it is essential that sovereignty policies are designed in a way that **reinforces both security and resilience, preserves innovation, and avoids unintended risks**, particularly in systemically important sectors such as payments and financial market infrastructure.

This paper sets out **principles and considerations** to help ensure that Europe's sovereignty objectives are met through **outcomes-based, risk-driven policies** rather than prescriptive technological constraints.

## Sovereignty Should Be Defined by Outcomes, Not Origin

Technological sovereignty is best achieved when Europe can **control outcomes** – security, resilience, continuity, and trust – rather than by focusing narrowly on the geographic origin of technology suppliers.

Risk-based approaches that assess:

- operational control,
- auditability and transparency,
- security, resilience and recoverability,
- and the ability to switch providers or architectures,

offer a more robust and future-proof path to sovereignty than static criteria based on company nationality or headquarters location. Such an approach ensures Europe remains open to innovation, attractive to investment, and resilient in the face of rapidly evolving technology landscapes.

In addition, companies with **deep and lasting economic footprints in Europe** – through substantial employment, infrastructure, R&D, compliance, and taxation – should benefit from a **presumption of operational security and resilience, and economic embeddedness**,

irrespective of the location of their ultimate parent company. Such firms are structurally intertwined with Europe's economic fabric and already subject to robust EU regulatory, supervisory, security and resilience frameworks. Treating these actors as inherently "non-sovereign" risks overlooking the practical realities of risk management, accountability, and control exercised within the EU. A footprint-based approach strengthens European resilience by rewarding long-term investment, diversification, and compliance, rather than relying on formal ownership or headquarters location alone.

## Preserving Security and Resilience in Critical and Regulated Infrastructure

Payments systems and financial market infrastructures form part of Europe's **critical economic backbone**. As such, they are already subject to some of the most stringent resilience, security, and oversight frameworks globally.

Any future sovereignty-related measures affecting these systems should:

- build on existing operational security and resilience frameworks,
- reinforce diversity and redundancy in supply chains,
- and avoid unintentionally increasing concentration risk.

Resilience in critical infrastructure depends not on reliance on a single category of supplier, but on **diversified, well-governed ecosystems** with clear exit and contingency options. Similarly, security of critical infrastructure depends on **objective metrics of security**, regardless of origin.

## Technology Neutrality Enables Stronger Sovereignty

Sovereignty and technology neutrality are not in conflict. On the contrary, **technology-neutral policies are often the most effective way to strengthen sovereignty** over time.

Frameworks that allow organisations to **choose the most appropriate technologies** – subject to clear resilience, security, and governance requirements – enable better risk management, faster innovation, and more sustainable digital ecosystems. Technology implementations should also be **modular and multi-vendor**, with emphasis on interoperability and vendor diversity, ensuring no single provider controls the entire stack.

Prescriptive approaches risk constraining choice, creating vendor lock-in, and slowing adaptation in areas where technology evolves faster than legislation can.

## Procurement as a Proportionate and Targeted Instrument

Public procurement can play an important role in shaping markets and supporting sovereign capabilities. However, procurement-based mechanisms should remain:

- proportionate,
- transparent,
- and tailored to clearly defined public-interest use cases.

In particular, procurement preferences should not become de facto mandates, **criteria should reflect lifecycle cost, interoperability, and exit options**, and private operators in regulated markets should not be indirectly constrained by public-sector procurement rules.

Used carefully, **procurement can encourage resilience and innovation without distorting competition or undermining security**.

## Open-Source as an Enabler

Open-source technologies make an important contribution to interoperability, auditability, and innovation across the digital economy. Mastercard recognises their value as part of a broader sovereignty and resilience strategy.

At the same time, open-source should be assessed on the basis of governance, maintenance, and security, and it should not be assumed to be inherently more or less sovereign than proprietary alternatives.

Policies that encourage consideration of open solutions – while preserving **freedom of design and accountability for outcomes** – strike the right balance between openness and responsibility.

## Avoiding Fragmentation Across Member States

Europe's strength lies in its Single Market. Sovereignty initiatives should therefore aim to **minimise divergent national interpretations, avoid fragmented implementation, and provide clarity and predictability to operators across borders**.

Uncoordinated national approaches risk increasing complexity, cost, and systemic risk—particularly for infrastructures that operate pan-European or global networks.

## A Constructive Partnership Approach

Mastercard operates trusted, secure payment networks that support consumers, businesses, and public authorities across Europe. As a systemically important payment system, the company is fully aligned with Europe's objectives to safeguard resilience, ensure operational continuity, and protect financial stability.

We stand ready to:

- engage constructively with EU institutions and Member States,
- share experience from operating critical global infrastructure,
- and support policies that enhance Europe's technological autonomy while preserving openness and innovation.

\*\*\*