Strengthening digital sovereignty

Priorities for Europe's capacity to act and a resilient industrial base

The global economic order is increasingly characterised by geopolitical tensions. Technologies are becoming a strategic power factor, whether through their potential for change, their relevance to security policy or dependencies on monopolised markets. Europe has recognised that technological dependencies can jeopardise its own capacity to act as well as its economic and social stability. Digital sovereignty must fundamentally be approached from a European perspective.

The European debate on digital sovereignty has so far been conducted primarily defensively, as a reaction to dependencies. However**,** a **proactive approach based on Europe's industrial strengths** is needed**.** Europe should **not** be playing **catch-up** but must focus on the **next generation of digital technologies** in the fields of industrial AI, microelectronics, robotics, advanced materials, secure infrastructures, cybersecurity and sovereign data spaces. European competitiveness cannot be achieved solely through the "Buy European" concept. Instead, the legal framework must be further developed in such a way that globally competitive corporate structures can also emerge in the internal market.

For the electro and digital industry, digital sovereignty **does not** mean **isolation**, but rather **the ability to operate in open markets** on the basis of innovation, resilience and international cooperation.

The electro and digital industry provides the basic technologies that will shape Europe's digital future, from microelectronics, industrial AI and cybersecurity to energy and communications infrastructures and automation. With its high level of innovation and value creation, it is the driving force **and foundation of digital sovereignty** – especially through **the interplay between hardware and software and the convergence of IT and OT.**

To strengthen digital sovereignty, ZVEI and FIEEC recommend focusing on the following areas:

- **Strengthen Industrial AI**
  Industrial artificial intelligence is the key driver of productivity, competitiveness and sustainability in European industries. The focus should therefore not be solely on large language models; instead, Europe must systematically build on its existing strengths across the entire industrial AI ecosystem (e.g. edge AI, agentic AI).

  Specifically, we propose:
  - Integrating industrial AI as a priority in national and European innovation strategies and funding initiatives (Apply AI strategy, AI Gigafactories, German High-Tech Agenda) focusing on AI deployment in industrial sectors.
  - Avoid double regulation of industrial AI under the AI Act and other EU legislation like MDR or Machinery Regulation and link the transition period to the availability of standards

- **Establishing open and secure data spaces**
  European industrial data is characterised by high quality, depth and reliability. Interoperable and trustworthy data spaces such as Manufacturing X allow production and process data to be exchanged securely across company boundaries without losing control over one's own data. These data spaces must be consistently developed further in order to promote innovation and digital business models and strengthen technological leadership roles. A mandatory requirement to share data is contrary to European sovereignty since sovereignty also requires robust legal protection of trade secrets.

Specifically, we propose:
- Further promote sovereign data spaces such as Manufacturing X
- Ensure an adequate protection of trade secrets and postpone the application of chapters 2, 3, 4, and 5 of the Data Act at least until September 12, 2026, in order to give companies the time they need to reorganize and prepare for compliance

- **Strategically promote cybersecurity**
  Digital sovereignty depends crucially on the ability to ward off threats in cyberspace independently and in a coordinated manner. Strategic security solutions along critical value chains, post-quantum cryptography and public-private partnerships strengthen resilience and trust. Only strong European champions are capable of scaling technologies and keeping them internationally competitive. At the same time, the cybersecurity regulatory framework must remain proportionate, clear, and free of overlapping obligations. Cybersecurity should simultaneously serve as a pillar of sovereignty, protection, and industrial competitiveness.

  Specifically, we propose:
  - Promoting cybersecurity as a strategic technology field while ensuring that cybersecurity requirements are proportionate
  - Expanding public-private partnerships and establishing information and exchange formats with partner countries
  - Ensure coherence of European cybersecurity legislation (NIS 2, RED DA, CRA, CSA) to avoid double regulation.
  - Adress inconsistencies and overlaps between regulations in the Digital Omnibus

- **Creating the right legal framework for a competitive industrial and innovation ecosystem**
  In order to encourage the use of AI and data-driven business models, Europe needs a clear, practical legal framework. Industrial applications should be exempt from the AI Act to avoid double regulation. GDPR and Data Act requirements must also be designed in an innovation-friendly manner in order to protect trade secrets.

  Specifically, we propose:
  - Stop the clock for digital regulation such as the AI Act, Data Act and Cyber Resilience Act in order to fundamentally reduce and revise and avoid double regulation

- **Further develop the microelectronics ecosystem**
  Without competitive products and services in strategic parts of the microelectronics supply chain, Europe will remain heavily dependent on supply from third country players. Therefore, the further development of a strong, resilient and innovative semiconductor ecosystem (from design and manufacturing to system integration) and strategic cooperation must be given the highest priority in industrial and security policy. Other regions have recognised this and are investing heavily.

  Specifically, we propose:
  - Promoting the entire microelectronics ecosystem (chip design, front-end and back-end manufacturing, testing, printed circuit board and electronics manufacturing) through Chips Act 2.0 and national support programmes.
  - Reforming the IPCEI framework and overcoming the "first-of-a-kind" approach

- **Creating powerful, competitive and resilient infrastructure**
  A powerful, resilient and networked digital infrastructure is crucial for industrial AI and digital sovereignty. In addition to the targeted establishment of AI gigafactories and data centres in Germany, France and Europe, the focus must also be on connecting them. Europe should continuously integrate its own technologies and rely on domestic hardware suppliers and providers for its cable infrastructure. Energy policy is an often-underestimated factor for industrial AI. High electricity prices and inadequate energy infrastructure are hampering the development of the necessary computing capacity.

Specifically, we propose:

- Measures to accelerate and simplify the permitting process of data center projects and their connection to the grid.
- Focus on connecting data centres (data centre interconnect)
- A level playing field for domestic suppliers of digital infrastructure components
- Competitive electricity prices
- Promoting the strategic importance of energy-efficient equipment

- **Establish a strategic raw materials and trade policy**
  A strategic raw materials and trade policy is also crucial for a sustainable industrial base. Access to critical materials such as rare earths, permanent magnets and semiconductor materials must be secured in the long term, to support the energy transition, electrification, and digitalisation of European industry. This can be achieved through resilient international partnerships, diversified supply chains, and a strong European industrial base for processing, refining, and recycling. Securing critical materials must go hand in hand with the development of European value chains, particularly in key sectors such as, for example for batteries, inverters and semiconductors.

  Specifically, we propose:
  - Expanding strategic partnerships with Australia, Southern American countries, ASEAN countries, Korea, Japan and India to secure access to markets, expertise and raw materials
  - Working on European processing and recycling capacities, including through investment incentives and an adapted regulatory framework.
  - Targeted local content requirements for narrowly and clearly defined areas
  - Integrate critical raw materials security into EU trade and industrial policy, ensuring coherence between environmental, competitiveness, and sovereignty objectives.

- **Advancing standardisation**
  Technical standards are the basis for interoperability and markets. French, German and European industry must be actively represented in international committees in order to help shape the technological basis. This requires the promotion of companies that are involved in standardisation. In addition, open and established industry standards such as the Asset Administration Shell (AAS) and the IEC/ISA 62443 series of cybersecurity standards for industrial automation systems should be consistently used and promoted internationally as the basis for data exchange, digital twins, digital product passports, and cybersecurity. Their application can contribute significantly to interoperability and global connectivity as well as the dissemination of European technologies.

  Specifically, we propose:
  - Introduction of tax incentives for companies active in standardisation (similar to tax incentives for research and development)
  - Use and promotion of open and established standards such as the Asset Administration Shell and IEC/ISA 62443 suite of standards.

- **Increased support for industrial innovation in Europe**
  European strategic autonomy and industrial sovereignty cannot be decreed: they must be financed. The European Union already has powerful instruments at its disposal that must be mobilized strategically: Horizon Europe, the Connecting Europe Facility, InvestEU, etc. Financial support for innovation must be strengthened and a framework must be put in place to enable industrial companies to scale up in Europe.

  Specifically, we propose:
  - Accelerate the establishment of the Capital Markets Union (CMU) to secure the necessary funding to finance innovations.
  - Support the creation of European Digital Innovation Hubs that help companies in adopting data, AI, and cybersecurity technologies.
  - European Union must strengthen and support public-private partnerships. These forms of cooperation are the most effective way to accelerate technology transfer, pool risks and mobilise greater funding.
  - Strengthen the industry pillar in the next European Framework Programme (FP 10)

Contact
Jochen Reinschmidt • Director • Digitalisation & Law
Tel.: +49 30 306960-23 • Mobile: +49 174 9414-164 • Email: jochen.reinschmidt@zvei.org

ZVEI e. V. • Electro and Digital Industry Association • Charlottenstr. 35/36 • 10117 Berlin
Lobby register no.: R002101 • EU Transparency Register ID: 94770746469-09 • www.zvei.org

Aridge Khayati • Public Affairs Officer and responsible for Digital regulations
Tel.: +33 1 45 05 70 56 • Mobile: +33 6 74 92 95 01 • Email: akhayati@fieec.fr

FIEEC • Fédération des Industries Electriques Electroniques et de Communication • 11 rue de l'Amiral Hamelin 75116 Paris
EU Transparency Register ID : 36474004071-38• www.fieec.fr

Date: 13.11.2025