



Digital Council Position on European Technological Sovereignty

Introduction

Digital Council welcomes the European Union's efforts to strengthen its technological capacity, resilience and competitiveness. The emerging European technological sovereignty framework, including the Chips Act 2.0, the Cloud and AI Development Act (CADA), the EU Open Source Strategy and the link between digitalisation, AI and energy policy, can help reduce critical dependencies and create new opportunities for European companies.

For the Czech Republic as an open and export-oriented economy, however, it is essential that **technological sovereignty is not equated with technological self-sufficiency, localisation or isolation.**

In Digital Council's view, the Czech position should be based on the principle of **open technological sovereignty**: Europe should strengthen its own technological capabilities and its ability to manage critical dependencies while preserving an open market, competition and cooperation with trusted international partners.

1. Sovereignty should be based on verifiable safeguards, control and resilience

The Czech Republic should support a concept of technological sovereignty based primarily on **effective control, verifiable security safeguards, interoperability and freedom of choice.**

Corporate origin, ownership structure, personnel nationality or the geographic location of data may be relevant in narrowly defined high-risk cases, but should not automatically substitute for an assessment of actual legal, technical and operational risks.

Security, privacy and resilience depend primarily on **how data and systems are protected**, including through strong encryption, privacy and security by design, robust governance, strict access controls, auditability and trusted cross-border data-transfer mechanisms.

The Czech Republic should therefore oppose **discriminatory or unnecessarily restrictive sovereignty requirements for ordinary cloud and AI services**, including requirements based on local ownership, corporate origin, personnel nationality or



blanket immunity from the application of third-country law. Such requirements risk excluding leading global providers from the European market, narrowing customer choice and slowing digital transformation without necessarily delivering corresponding security benefits.

More stringent requirements may be justified for genuinely critical workloads, but should be based on a specific risk assessment and remain proportionate to the public-order or security interest at stake.

Where sovereignty restrictions are applied, they should therefore be limited to systems or workloads that meet a **specific and clearly defined public-order, security or equivalent criticality test**. The Czech Republic should also support appropriate exemptions for covered or trusted trading partners from country-screening requirements, including under Article 18, where equivalent safeguards are ensured.

2. Sovereignty requirements must remain proportionate

The Czech Republic should support the development of European cloud, AI and data-centre infrastructure and a common European framework that reduces fragmentation between Member States.

At the same time, requirements for reaching Union Assurance Levels under Title IV should be proportionate to the actual risks involved. Applying broad sovereignty requirements to baseline public procurement could unnecessarily narrow the supplier pool, increase costs for public authorities and taxpayers and slow down cloud and AI adoption.

Stricter requirements may be justified for genuinely critical systems, including certain defence, security or critical-infrastructure functions. They should not, however, apply indiscriminately to routine public administration or standard commercial services.

The Czech position should therefore support a **risk-based and proportionate approach**, mutual recognition of audits and certifications and avoidance of duplicative or overlapping regulatory requirements.



3. Data localisation should not be the default

The Czech Republic should oppose blanket data-localisation requirements as a baseline instrument of technological sovereignty.

The physical location of data does not in itself determine security, privacy or resilience. Strong encryption, customer-controlled keys, access controls, governance, auditability and robust cross-border transfer mechanisms may provide stronger protection than geographic restrictions alone.

Mandatory localisation may also reduce resilience by limiting geographic redundancy, disaster-recovery options and access to globally distributed cybersecurity infrastructure and expertise. It can also increase costs and reduce access to advanced cloud and AI services without necessarily producing a corresponding security benefit.

Localisation requirements should therefore be reserved for **narrowly defined cases where a concrete security, public-order or criticality risk justifies them**, rather than applied systematically to ordinary public procurement or commercial services.

4. Stronger European capabilities without protectionism

The Czech Republic should support investment in European capabilities in semiconductors, cloud, AI, software, research and digital infrastructure.

European technology policy should not, however, be based on broad preferences linked to provider origin or on excluding trusted non-European technologies.

This is particularly important in relation to the concept of “**Union added value**”. The Czech Republic should support a definition based on objective, transparent and non-discriminatory indicators.

The assessment should take a holistic view of a provider’s actual contribution to the European economy and technology ecosystem, including both:

- **direct contributions**, such as infrastructure investment, R&D, intellectual property, skilled employment and participation of European startups and SMEs; and



- **indirect contributions**, including technological platforms and services that enable European businesses to innovate, scale and compete globally.

A provider's place of establishment, ownership structure or nationality should not in itself determine whether it creates value for Europe.

European policy should aim to **strengthen Europe's position within global technology value chains**, not disconnect Europe from them.

5. Open source as a tool, not a mandatory model

The Czech Republic should support wider use of open source, open standards and interoperable technologies as tools for reducing vendor lock-in and increasing technological control.

Digital Council supports the principle:

Open source first, not open source only.

Open source should not be automatically preferred regardless of security, functionality, maintenance or total cost of ownership.

At the same time, **open-source software is not inherently more secure than proprietary software**. Its security depends on the quality of development and governance, timely vulnerability management, secure dependencies, robust access controls and effective software supply-chain security.

The Czech position should therefore emphasise that Europe needs not only open-source development, but also **long-term professional maintenance, security auditing, vulnerability management, software supply-chain security and sustainable governance**.

Open standards, interoperability, portability and the ability to switch providers are ultimately more important for technological sovereignty than a particular licensing model.



6. Semiconductors: resilience rather than autarky

The Czech Republic should support strengthening the European semiconductor ecosystem, but not through an attempt to achieve complete European self-sufficiency across every part of the value chain.

The priority should be **diversification of critical supplies and investment in areas where Europe and Czechia can create genuine competitive advantage**.

For the Czech Republic, this includes in particular links to the automotive sector, industrial applications, research, chip design, advanced manufacturing and skilled employment.

Trusted international partnerships should remain an integral part of European semiconductor policy. **Diversification is generally more resilient than autarky**.

Public support should focus on clear technological and economic additionality and avoid creating permanent subsidy competition between Member States.

7. Energy and infrastructure are conditions for digital competitiveness

The development of AI, cloud and data centres cannot be separated from energy and infrastructure policy.

The Czech Republic should therefore support closer integration of technological and energy policy, with a focus on:

- development of electricity grids;
- availability and transparency of connection capacity;
- faster and more predictable permitting;
- demand-side flexibility and energy storage;
- effective use of waste heat;
- high-capacity connectivity;
- use of digital technologies and AI to improve energy-system efficiency.

Sufficient energy and grid capacity are becoming fundamental conditions for both European and Czech digital competitiveness.



Key priorities for the Czech position

Digital Council recommends that the Czech Republic promote:

1. **technological sovereignty based on verifiable safeguards, effective control, resilience and freedom of choice rather than provider origin, ownership or localisation;**
2. **rejection of discriminatory or unnecessarily restrictive sovereignty requirements for ordinary cloud and AI services;**
3. **stricter sovereignty requirements only where justified by a concrete public-order, security or criticality risk;**
4. **a proportionate approach to Union Assurance Levels that preserves supplier choice and avoids unnecessary costs for public buyers;**
5. **data localisation only where justified by a specific risk, rather than as a baseline procurement requirement;**
6. **objective, transparent and non-discriminatory criteria for Union added value, reflecting both direct and indirect contributions to the European economy;**
7. **interoperability, portability, open standards and the ability to switch providers;**
8. **the principle “open source first, not open source only”, combined with robust cybersecurity, software supply-chain security and long-term professional maintenance;**
9. **stronger European semiconductor and technological capabilities while preserving cooperation with trusted international partners;**
10. **limiting regulatory duplication and disproportionate burdens, particularly for startups and SMEs;**
11. **linking technology strategy with energy, connectivity and physical infrastructure.**



Conclusion

The Czech Republic has a clear interest in a stronger and more resilient Europe that is better able to manage critical technological dependencies and develop globally competitive technologies.

European technological sovereignty should therefore increase **Europe's capacity to act and its freedom of choice**, not create new dependencies through localisation, protectionism or unnecessarily narrow supplier markets.

Europe does not need technological isolation. It needs stronger capabilities of its own, verifiable security safeguards, genuine freedom of choice and an open ecosystem of trusted partners.

