Policy Brief:

Digital Sovereignty in Europe

Definition, Status, Policy Options

Version 2

June 1st 2026

Werner Illsinger
Executive Director
4future.institute
werneri@4future.group

Imprint

4future.institute
Graben 17/10 1010 Vienna Austria +43 1 31440-0

4future.institute is part of the 4future.group and a brand of 4future.business GmbH.

Company Register Number: FN 459359 d
Company Court: Vienna Commercial Court
VAT ID: ATU71656745
Majority Shareholder: 4future.foundation

Executive Summary

On almost every issue that matters today, there are more opinions than orientation. More noise than clarity. More interests than arguments.

The 4future.institute was founded to cut through that noise. Not to add another opinion — but to ask: What is actually true here? What are the structural conditions? And above all: Does this make sense — not just economically, but for us as a society, as human beings?

Digital sovereignty is one of three strategic questions the 4future.institute addresses — alongside the future of democracy and the future of work and economic competitiveness in Europe.

Since 1990, Europe's share of global GDP has fallen from 30% to 13%. The United States has remained stable over the same period — while China has grown from 3% to 18%. This trajectory has many causes. One of the structural ones is digital: what Europe generates in data, users and markets becomes value added in American balance sheets. This paper examines the structural causes — and what must change.

Europe's core digital infrastructure — cloud, identity, communications, AI — is almost entirely provided by platforms subject to foreign legal systems, in conflict with European law, and operating in monopolistic market structures.

This creates a structural trilemma: Legally, Europe cannot guarantee compliance with data protection law, because US legislation such as the CLOUD Act and FISA 702 directly conflicts with it. Technologically, the dominance of proprietary multi-tenant architectures prevents auditability and portability. Economically, digital value creation is systematically drained out of Europe.

Developments since the first publication of this paper have sharpened the situation: the PCLOB — the central oversight body of the EU-US Data Privacy Framework — was effectively dismantled by the Trump administration.

FISA Section 702 was extended twice on a short-term basis in April 2026. At the time of publication, the current extension expires within days — and a lasting agreement between the House and Senate remains outstanding. The political standoff between reform conditions and a clean extension illustrates precisely how fragile the legal foundation of transatlantic data transfers is.

The DPF is under legal challenge before the Court of Justice of the European Union. Early industry responses such as the AWS European Sovereign Cloud point in the right structural direction — but do not resolve the underlying problem.

Europe currently lacks legal, technological and economic digital sovereignty.

The path forward requires a systemic approach: an enforceable legal framework, auditable European cloud and AI infrastructures, binding interoperability standards, strategic digital investment and an education system that fosters critical thinking. These measures are not costs — they are an investment in Europe's future viability.

Inhaltsverzeichnis

1 Defining Digital Sovereignty

Digital sovereignty refers to the ability of states, institutions, organisations and individuals to operate digital technologies, data, infrastructures and communications systems independently, in compliance with the law and securely — or to make free and informed decisions about their use. The concept encompasses three core dimensions: legal, technological, and economic-societal sovereignty.

Digital sovereignty does not, however, mean that Europe must manufacture or operate all technologies itself. It is not about autarky.

It is about the ability to determine for ourselves whom we trust, which technologies we deploy, and under what legal conditions they are operated.

Self-determination requires:

- Reliable partners whose organisations operate within a legal framework compatible with European fundamental rights.
- Technical means of control that allow commitments to be verified.
- Plurality over monopoly — because self-determination is impossible when a single provider, even a European one, is effectively the only option.
- Manageable, transparent dependencies that are not imposed through extraterritorial legislation or proprietary lock-in.

Digital sovereignty does not mean isolation or technological autarky.

Europe does not need to build all technologies itself — but it must be free to decide which systems are used, and to ensure that those systems operate within a compatible legal framework, under transparent governance, and without monopolistic dependencies.

Digital sovereignty is therefore not a nationalist or protectionist concept. It is a principle of **legal compatibility, openness to competition, and self-determined choice** of partners.

Digital sovereignty means: freedom of choice, control over the foundations, and certainty about the legal framework — not isolation or closure.

1.1 Legal Sovereignty

The ability of a state, organisation or operator to ensure that digital systems and data are subject exclusively to the legal frameworks that apply to them by virtue of their geographical, organisational and legal affiliation — without unintended or extraterritorial access powers by foreign states.

- Transparency regarding access by public authorities
- Legal protection for those affected
- Exclusion of extraterritorial access powers by foreign states

1.2 1.2 Technological Sovereignty

The ability to develop, operate or replace digital systems, software and infrastructure independently. This includes:

- Control over architecture, data flows and cryptography
- Interoperability and standardisation
- Avoidance of critical dependencies on individual providers
- Resilience against disruptions or politically motivated measures

1.3 Economic and Societal Sovereignty

The ability of the economy and society to:

- apply digital technologies independently
- understand them
- and develop them further without external constraint

Digital sovereignty is therefore not a purely technical concept. It represents a state and economic capability that underpins the rule of law, competitiveness and security in the digital world.

2 Status of Digital Sovereignty in Europe

The analysis of the current situation reveals deficits across all dimensions of digital sovereignty — legal, technological and economic. These deficits do not arise from individual decisions, but from structural conditions: extraterritorial legal frameworks, proprietary platform architectures and global market concentration. In combination, they prevent Europe from independently controlling core digital functions.

2.1 Legal Status: Conflicting Legal Frameworks and Structural Tensions

Europe finds itself in a systemic conflict arising from three factors:

European data protection law: The GDPR requires European controllers to retain full control over personal data — including protection against unauthorised access by public authorities.

US legislation with extraterritorial reach: Laws such as the CLOUD Act and FISA 702 compel US companies to disclose data — even when that data is physically stored in the EU and subject to European regulations.

The technical architecture of modern cloud systems: Multi-tenant architectures prevent European customers from exercising full technical control, and limit both auditability and isolation.

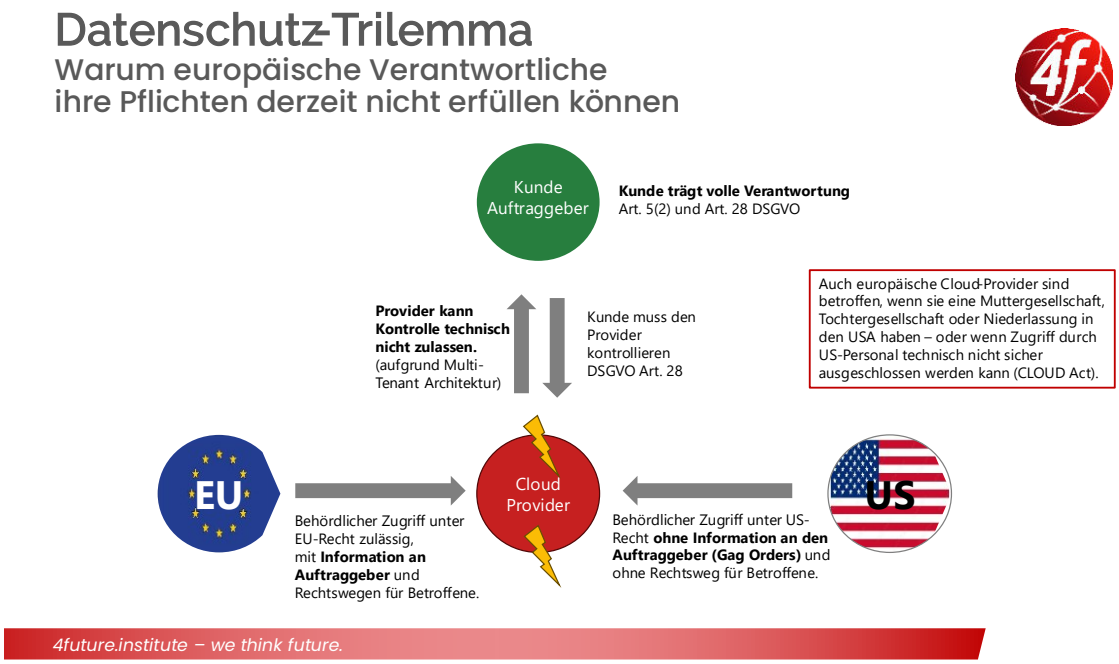
The Court of Justice of the European Union confirmed in Schrems II (C-311/18) that US cloud providers are structurally unable to fully meet GDPR requirements due to the legal situation in the United States.

The diagram below illustrates the structural problem clearly: Under Articles 5(2) and 28 of the GDPR, the controller (the customer) bears full responsibility for ensuring that personal data is processed in compliance with the law. The controller must both ensure and be able to demonstrate that the cloud provider engaged meets all GDPR requirements.

To fulfil this responsibility, the controller would need to be able to technically audit the provider. In practice, however, this is not possible in modern multi-tenant cloud environments: a technical audit would inevitably expose systems in which other customers' data is also being processed. No provider can permit that.

The only available alternative is a Data Processing Agreement (DPA), in which the provider commits to complying with all relevant GDPR obligations and to preventing unauthorised access. However, providers subject to US law cannot give such an assurance with legal force — because they are bound by US legislation, such as the CLOUD Act, that directly conflicts with it.

This creates an irresolvable conflict: the customer remains fully liable, yet is demonstrably unable to fulfil their legal obligations — because the provider can neither be audited nor provide the required guarantees with binding legal effect.



Developments since the first publication of this paper have further deepened the legal uncertainty described above.

In January 2025, the Trump administration dismissed the Democratic members of the Privacy and Civil Liberties Oversight Board (PCLOB) — the independent US oversight body responsible for monitoring compliance with data protection commitments made to the EU. The European Commission had explicitly cited the PCLOB 31 times in its adequacy decision on the EU-US Data Privacy Framework (DPF), as a central pillar of institutional safeguarding. Without a functioning PCLOB, that pillar has effectively ceased to exist.

The EU-US Data Privacy Framework itself is under legal challenge: an initial court challenge was dismissed by the EU General Court in September 2025 — however, the appeal before the Court of Justice of the European Union remains pending. That same court has already invalidated both predecessor frameworks: Safe Harbour in 2015 and Privacy Shield in 2020.

There is a further complication: FISA Section 702 is again set to expire in June 2026. The reauthorisation debate in the US Congress remains unresolved — with uncertain implications for the scope of future surveillance powers.

These developments confirm the structural analysis of this paper: transatlantic data transfers rest on a legally fragile foundation that depends on political decisions in Washington — not on stable statutory guarantees.

Conclusion: Europe does not currently have legal digital sovereignty, as long as critical data is processed by companies subject to foreign legal systems.

2.2 Technological Status: Dependence on Non-European Platforms

European public administration, business and research rely almost entirely on non-European digital platforms in key areas — platforms that are largely incompatible with the European legal framework, and for which few alternatives exist:

Cloud infrastructure: AWS, Microsoft Azure and Google Cloud hold a combined market share of approximately 65%

Collaboration & communications: Over 90% usage of Microsoft 365 or Google Workspace

Software development: GitHub (Microsoft) as the globally dominant platform

Identity management: Strong dependence on Azure AD / Entra ID

AI models & APIs: Predominantly US-based models and training infrastructures

These systems are proprietary, deeply integrated and only partially portable. This creates an additional layer of structural vendor lock-in, making any switch or exit technically and economically prohibitive.

Early industry responses are emerging — with considerable differences in substance and seriousness.

In January 2026, AWS launched a European Sovereign Cloud, structured as a fully independent European legal entity with no direct operational connection to the US parent company. This approach addresses the underlying problem more seriously than previous market solutions: it attempts to block the extraterritorial reach of the CLOUD Act through complete corporate separation — rather than contractual assurances. The structural residual risk nevertheless remains: the CLOUD Act operates at the level of the parent company, regardless of operational separation. Whether this approach will withstand legal scrutiny remains open — and will set a precedent for the entire industry.

Microsoft, by contrast, has so far offered only marketing announcements under labels such as "EU Data Boundary" or "Sovereign Cloud", without altering the underlying legal structure. Microsoft's own legal counsel was compelled to acknowledge before the French Senate in June 2025 that no guarantee against access by US authorities can be given — even for data stored in France.[1]

This distinction is analytically significant: it shows that the market is beginning to differentiate between serious structural responses and pure compliance narratives — even though none of the solutions available to date fully resolves the underlying problem.

Conclusion: Europe does not have technological digital sovereignty — we cannot make autonomous decisions about our own digital infrastructure — as long as core digital functions are operated without alternatives compatible with European law or genuine means of control.

2.3 Economic Status: Loss of Value Creation and Strategic Vulnerability

Europe's economy is heavily dependent, across core value chains, on platforms whose ownership, legal frameworks and decision-making structures are incompatible with European law and values:

- Cloud services
- Communications and collaboration systems
- AI models and training infrastructures
- Developer and deployment platforms
- Identity and security mechanisms

These dependencies result in:

Economic dependence: Value creation and profits flow predominantly to non-EU countries.

Strategic vulnerability: Platforms can be influenced by geopolitical tensions, sanctions or political decisions.

[1] Sénat français, Commission des affaires économiques, Audition du 10 juin 2025 — senat.fr

Limited bargaining power: Prices, technical standards and contractual terms are largely determined by global platform operators.

Risk of economic espionage: Outflow of scientific and industrial research results.

These developments have real consequences for our economy. Since 1990, Europe has fallen from first place — with 30% of global GDP — to third place, at 13%.

This trajectory is neither coincidental nor a temporary weakness. It is the result of structural decisions — and structural failures. Over the past three decades, Europe has systematically outsourced the digital infrastructure on which its economy runs. What has flowed out is not only revenue and tax receipts — it is the capacity to shape digital value creation itself.

The United States built and defended that capacity. China developed it strategically. Europe consumed it comfortably.

As long as that remains the case, the curve will not reverse. The decline will continue.

Conclusion: Europe does not have economic digital sovereignty, as core digital value creation does not take place within its own economic area and geopolitical risks remain beyond its control. This has real and measurable economic consequences.

3 Policy Options for Strengthening Digital Sovereignty

Strengthening digital sovereignty requires a multi-layered policy framework that integrates legal, technical, economic and societal measures. Individual measures can reduce dependencies, but only a coherent European strategic framework can bring about systemic change.

The following sections outline strategic guidelines and concrete operational measures.

3.1 Legal Framework

Clear jurisdictional boundaries and protection against extraterritorial access

European digital sovereignty requires a legal framework that guarantees legal clarity, enforceability and protection against foreign legal systems.

3.1.1 Define Applicable Law Clearly

- Introduction of a European "Digital Jurisdiction Standard" that establishes: which legal system may access which data.
- Prohibition of extraterritorial access to European data spaces by third countries, unless such access is compatible with EU law.

3.1.2 EU-Wide Certification of Cloud and AI Services

Establishment of a binding certification that guarantees:

- Data processing exclusively in countries compatible with the European legal framework (no circumvention of EU law).
- No parent company outside EU jurisdiction (e.g. no CLOUD Act exposure).
- No subsidiaries or affiliated entities outside EU jurisdiction with access to European data.
- Transparency obligations regarding access by public authorities.

Applicable specifically to technical platform providers.

3.1.3 Renegotiation of Transatlantic Agreements

No agreements without:

- Legal protection for EU citizens
- Exclusion of covert access orders (gag orders)
- Technical and legal control mechanisms

The urgency of this demand has become concretely apparent since the first publication of this paper: FISA Section 702 is again set to expire in June 2026 — the reauthorisation debate in the US Congress is ongoing, with active efforts to expand rather than restrict its scope. At the same time, the Trump administration has effectively dismantled the PCLOB — the central oversight body on which the EU-US Data Privacy Framework relies.

These developments illustrate precisely why bilateral agreements based on executive commitments rather than statutory law are structurally unreliable: they can be altered or hollowed out by a new administration with a single decision — without European input, without prior notice.

Renegotiations of transatlantic agreements must therefore proceed on a different basis: binding statutory law rather than executive orders, parliamentary oversight rather than administrative discretion, and genuine legal enforceability for affected EU citizens.

3.1.4 Legal Framework for Critical Digital Infrastructure

- ·Definition of which systems qualify as critical (e.g. identity infrastructure, AI models, government cloud environments).
- Requirement that such systems operate exclusively within sovereign infrastructures.

3.1.5 Establish Global Regulation of Multinational Corporations

International rules are equally necessary to ensure that the power of multinational platforms does not undermine democratic processes. States must collectively establish standards that:

- limit extraterritorial interference,
- make transparency, auditability and interoperability mandatory,
- prevent monopolistic structures,
- ensure fair taxation.

No single state — not even an EU member — can achieve this alone. Only coordinated international regulation can rebalance the structural asymmetry between states and corporations.

Outcome: A legal framework that ensures control, transparency and protection against foreign legal claims.

3.2 Technological Framework: Building European Control Capability

Legal requirements can only take effect if they are technically implementable. Europe therefore needs its own autonomous digital capability — one that ensures core services can be operated, audited and further developed independently of foreign legal systems. Technical control capability is the heart of digital sovereignty — not isolation, but the ability to understand, operate and shape digital infrastructure on its own terms.

3.2.1 Building a European Cloud and AI Infrastructure

Europe needs a federated, scalable and sovereign cloud and AI architecture that operates core digital functions under EU law. This infrastructure must meet the following requirements:

- Operation exclusively under European law — without extraterritorial access by foreign states.
- Auditability at every level — infrastructure, platform, software and AI models must be technically and legally verifiable (open source or disclosed components).
- Interoperability over proprietary dependencies — services must be interchangeable, portable and combinable.

Existing initiatives such as GAIA-X provide a framework, but do not address all technical and organisational requirements. They represent a starting point — not yet a complete operational solution.

3.2.2 Interoperability as a Binding Standard

Interoperability is the prerequisite for competition, portability and long-term cost transparency. It must therefore be anchored as a mandatory standard across Europe — particularly in areas where digital sovereignty is most critical. This covers:

- Communications and collaboration: CalDAV, CardDAV, IMAP
- Documents and data: OpenDocument standards, open metadata, open API specifications
- Identity and access management: OpenID Connect, European Digital Identity Wallet
- Data portability: Fully documented export formats and interfaces

Interoperability creates a market in which European providers can compete — and prevents the emergence of monopolistic structures.

3.2.3 European Identity and Trust Services

Digital identity is one of the central dependencies of modern digital systems. Today, large parts of European public administration, business and education rely on proprietary US identity services (e.g. Azure AD / Entra ID).

A European, publicly anchored identity and trust infrastructure is therefore needed — one that:

- functions as a basic public service, comparable to energy or communications networks,
- is equally accessible to citizens, businesses and public authorities,
- operates fully under European legal norms,
- is federated, security-certified and interoperable,
- is not dependent on individual technology providers.

A sovereign European identity infrastructure is the necessary foundation for all digital innovation — from AI and e-government to cloud services.

3.2.4 European Security Architecture

Security-critical digital infrastructure in Europe must be verifiable, transparent and free from hidden access mechanisms. This requires:

- Promotion and prioritisation of European open-source solutions in cybersecurity, cryptography, network services and identity management.
- Mandatory disclosure of security-relevant components by providers serving critical infrastructure.
- Common European standards for security audits, penetration testing and Software Bills of Materials (SBOM).
- European certification of security-critical software with clear requirements for transparency, protocols and architecture.

Security is not achieved through opacity — it is achieved through verifiability and control.

Outcome:

Technological sovereignty does not arise from isolation — it arises from control capability. A European cloud and AI infrastructure, interoperable open standards, a sovereign identity architecture and a verifiable security foundation will enable Europe to operate and develop digital systems independently. This creates a stable digital core that makes legal, economic and security policy measures effective in practice.

3.3 Economic Framework: Reshaping Market Mechanisms

Digital sovereignty requires an economic framework that enables alternatives and corrects market failures.

3.3.1 Strategic European Digital Investment and Innovation

A European "Digital Sovereignty Fund" to finance:

- AI models
- Cloud infrastructure
- Hardware production
- Open-source and auditable core components

Innovation does not arise from isolation — it arises from competition and freedom of choice. A functioning European digital market therefore needs more providers, more diversity and lower barriers to entry — not a "Europe builds everything itself" scenario.

Monopolistic structures — even European ones — slow innovation, limit technological alternatives and prevent the emergence of new business models. Open standards, interoperable platforms and transparent legal frameworks, by contrast, create a market in which start-ups, mid-sized companies and European developers can build new, innovative services on existing infrastructures.

Digital sovereignty thus becomes a driver of innovation: it creates a fair, open and competitive single market in which technological creativity is rewarded — rather than constrained by lock-in effects or structural dependencies.

3.3.2 Reducing Economic Dependencies

Companies should be empowered to systematically identify and assess digital dependencies — analogous to established practices in risk management and supply chain due diligence. This creates transparency without generating additional bureaucratic burden.

3.3.3 Market

European companies and public institutions currently source a substantial share of their digital infrastructure from non-European platform providers. Microsoft and Google together generate annual revenues of over 60 billion US dollars in Europe — the majority of which leaves the European economic area without meaningful local value creation or sustainable tax contribution.

The market could resolve much of this — if a functioning market actually existed. In many key digital sectors, however, there is no longer a market in any meaningful sense: what exists is extreme concentration among a handful of global platforms.

Digital sovereignty therefore does not mean restricting the market — it means restoring it: through open standards, competition, freedom of choice and fair conditions that enable innovation rather than suppress it.

Measures promoting interoperability, open standards and European alternatives lead to a lasting shift of value creation back to Europe: data centres, software development, research, maintenance and operations are delivered locally, generating skilled jobs, tax revenues and technological know-how. Every euro invested in European digital infrastructure largely remains within the European economic and innovation cycle.

Support programmes for migration, investment incentives for interoperable systems and tax incentives for open technologies are therefore not "subsidies" — they are instruments that absorb transition and transformation costs, lower market barriers and generate long-term economic returns. The public expenditure is time-limited; the structural benefit is permanent: reduced dependencies, greater digital resilience, a broader competitive base and a stable European technology market.

This makes one thing clear: investment in digital sovereignty pays off — not only socially and in terms of security policy, but economically. It creates the conditions for Europe to develop, operate and advance key digital technologies — rather than simply consume them.

3.3.4 European Procurement Reform

Public procurement is one of the most powerful instruments available for strengthening digital sovereignty and establishing fair market conditions. European public administrations are among the largest purchasers of digital services. When they systematically prioritise open standards, transparent legal frameworks and limited vendor dependencies, they automatically create a market environment that enables competition and fosters innovation.

In concrete terms, this means:

(1) **Prioritisation of open standards** ensures that systems remain interoperable, data remains portable and switching providers remains technically feasible. This prevents structural lock-in effects and reduces long-term operating costs.

(2) **Exclusion of extraterritorial legal risks** ensures that public data is subject exclusively to legal frameworks that are democratically legitimised and controllable under European law. This is indispensable in critical areas — public administration, law enforcement, justice, health and education.

(3) **Limiting vendor dependency** through clear exit strategies, maximum contract durations and technical portability requirements ensures that public bodies do not become trapped in one-sided dependencies that are costly, risky and difficult to unwind.

The result is a digital procurement market that enables freedom of choice rather than entrenching oligopolies. Rather than inadvertently reinforcing monopolistic structures, public authorities instead promote competition, innovation and European alternatives. This reduces costs over time, strengthens the negotiating position of public bodies and enhances the structural resilience of Europe's digital infrastructure.

3.4 Societal Framework: Competence, Transparency and Participation

Digital sovereignty can only take lasting hold if it is embraced by society as a whole.

Without broad digital competence, transparent information and meaningful opportunities for participation, digital sovereignty remains a project for experts — with no practical impact on the daily lives of citizens, businesses and institutions. A societal framework is therefore indispensable for anchoring digital independence over the long term.

3.4.1 Education as the Foundation

Europe's education systems are still heavily oriented towards reproduction and memorisation. Sovereign engagement with digital technologies, however, requires above all critical thinking, problem-solving capability and the ability to question systems. Only those who genuinely understand can work with AI and digital tools in a safe, self-determined and responsible way.

This model looks increasingly out of place today: digital technologies — and AI in particular — do not reward the repetition of pre-formed answers. They demand critical thinking, problem-solving, contextual understanding and the ability to ask good questions.

Those who only memorise cannot use AI. Full stop.

Digital sovereignty therefore begins in the classroom. We need an education system that fosters curiosity, allows for dissent, rewards independent thinking and encourages children to take unconventional paths.

Or to put it more simply: we need more Pippi Longstocking — people who do not simply accept the world as it is, but have the confidence to imagine it differently.

Digital literacy education is additionally necessary. The following competency areas should be embedded in curricula:

Data literacy: Understanding data flows, data protection, consent and data processing.

AI literacy: How algorithmic systems work, their limitations, opportunities and risks.

Cybersecurity: Password hygiene, phishing awareness and safe behaviour in everyday digital life.

How digital systems work: Core principles of networks, protocols, hardware and software.

The goal is not technical specialisation — it is the emergence of a digitally literate population capable of making informed decisions and not remaining passively dependent on opaque systems.

Pedagogical reform alone is not enough. Schools and teachers also need the necessary resources, time and support. Critical thinking, digital literacy and AI competence can only develop if the education system is strengthened both structurally and in terms of staffing.

3.4.2 Transparency as a Prerequisite for Trust

Every digital service — whether commercial or public — should be required to disclose in clear and accessible terms:

- where data is processed,
- which legal framework governs it,
- what technical and organisational dependencies exist.

This transparency builds trust, enables comparison and supports informed decision-making. It allows citizens, businesses and public authorities to make conscious choices about the digital services they use — and in doing so, strengthens the market for sovereign systems.

3.4.3 Building European Talent, Research and Innovation Capacity

Digital sovereignty requires European competence in key technologies. This includes:

- Targeted support for independent public research in AI, cryptography, cybersecurity, cloud and hardware development (e.g. chips, servers, robotics).
- Establishment of European centres of excellence connecting universities, industry and start-ups.
- Incentives for technology talent currently working abroad.
- Improved conditions for European tech founders to reduce brain drain.

Europe must not only use digital technologies — it must develop and control them itself in order to remain globally competitive.

3.4.4 Civil Society Participation in Major Digital Projects

Digital infrastructure is today as socially significant as transport, energy or the environment. Major digital initiatives should therefore — analogous to environmental impact assessment procedures —:

- undergo transparent public participation processes,
- incorporate civil society and scientific expertise,
- openly disclose risks, alternatives and impacts.

This strengthens democratic legitimacy, avoids poor decision-making and builds public trust in state-led digitalisation processes.

3.4.5 Strengthening Global Cooperation

Europe should actively build partnerships with states that:

- share the principles of the rule of law,
- respect data protection and fundamental rights,
- have transparent and accountable governance structures.

Together, interoperable technical standards, secure data spaces and responsible AI development can be advanced. Cooperation creates scalability, innovation capacity and stable global conditions.

Outcome

Digital sovereignty becomes a whole-of-society project — not merely a government programme. Through education, transparency, talent development and civil society participation, a broad base of support emerges that stabilises digital independence over the long term and anchors it democratically.

4 Conclusion

Digital sovereignty is not a technological option — it is a strategic prerequisite for Europe's economic stability, political capacity to act and societal resilience.

The analysis shows that Europe is currently unable to act independently — legally, technologically or economically. The root causes are structural dependencies on platforms and infrastructures that operate outside the European legal and regulatory space.

Strengthening digital sovereignty can only be achieved through a systemic approach: a clearly defined legal framework, technological alternatives, economic investment in European value creation, and a society that understands digital systems and actively helps to shape them. These measures are not a cost — they are an investment in Europe's future viability. They create local value, reduce geopolitical risk and enable Europe to safeguard its fundamental values — data protection, democracy and competition — in the digital age as well.

5 Call to Action

Europe stands at a strategic turning point. Digital sovereignty is not an abstract vision of the future — it is an immediate prerequisite for economic stability, democratic control and societal resilience. The next five years will determine whether Europe acts with self-determination — or is steered by external dependencies.

- What is needed now is a resolute European agenda for digital sovereignty:
- with a clear and enforceable legal framework,
- with verifiable technological infrastructure,
- with a competitive digital single market,
- and with an informed society that understands digital systems and uses them with confidence.

Digital sovereignty is not a cost — it is an investment in Europe's future viability and capacity for innovation.

Europe must seize this opportunity — decisively.

Now.

I. About the Author

Ing. Werner Illsinger, MBA, is the founder and Executive Director of the 4future.institute. He spent 18 years at Microsoft — from the era of the personal computer through to the age of cloud dominance. He witnessed at first hand how a company that once democratised the PC became a global platform infrastructure that today controls core societal functions — and has drawn his own conclusions for Europe.

Trained as a communications engineer and organisational psychologist, he combines technical systems understanding with a systemic and societal perspective. This paper is not a commissioned work — it is the result of a growing conviction that Europe must shape the structural conditions of its digital future now, while the window remains open.

II. Annex: Glossary

Multi-Tenant Cloud An architecture in which many customers share the same technical infrastructure (servers, platforms, management services). This is efficient, but prevents individual customers from fully auditing or operating the underlying systems in isolation. The result is structural dependency and limited technical control.

Interoperability The ability of different systems to freely exchange data, documents and processes and work together — without proprietary barriers or vendor dependencies. It is a prerequisite for portability, competition and the capacity for innovation.

Portability The ability to transfer data, documents or entire systems from one provider to another without technical or legal barriers. Portability prevents lock-in and strengthens competition.

Extraterritorial Legal Effect When the laws of one country apply even when the data or persons concerned are located in another state. Example: the US CLOUD Act compels US companies to disclose data — even when that data is stored in the EU and subject to EU law.

Vendor Lock-in A situation in which companies or public authorities are effectively unable to switch to another provider, because proprietary interfaces, formats or contractual structures make an exit prohibitively expensive or technically unfeasible.

Digital Identity The technical and organisational mechanisms by which users, public authorities or businesses verify their identity and securely access digital services. Examples: EU Digital Identity Wallet, OpenID Connect.

Auditability The ability to independently verify technical systems — including software, architecture, security mechanisms and data processing. In multi-tenant cloud environments, this is only possible to a limited extent.

SBOM (Software Bill of Materials) A complete inventory of all components, libraries and dependencies that make up a piece of software. SBOMs increase transparency, security and traceability across supply chains.

III. Annex: Sources & References

Legal Foundations

- Datenschutz-Grundverordnung (DSGVO) – Regulation (EU) 2016/679
- CLOUD Act – Clarifying Lawful Overseas Use of Data Act, Public Law 115-141 (USA, 2018)
- FISA Section 702 – Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881a
- EuGH – Schrems II (C-311/18) – Urteil des Europäischen Gerichtshofs vom 16. Juli 2020
- EU Charter of Fundamental Rights, Art. 7, 8 – Datenschutz, Privatsphäre

Market Data & Economic Facts

- Synergy Research Group (2024) – Global Cloud Market Share (AWS, Azure, Google > 65 %)
- IDC & Gartner Reports 2023/2024 – Collaboration & Office Software Market (> 90 % US-Anbieter)
- Microsoft Annual Report (Form 10-K, FY2024) – Regionale Umsätze inkl. Europa
- Alphabet Annual Report (Form 10-K, FY2024) – Regionale Umsätze inkl. Europa
- EU Industrial R&D Investment Scoreboard (2023/2024) – Investitionsschwerpunkte außerhalb Europas

Technical Foundations

- NIST SP 800-145 – The NIST Definition of Cloud Computing
- ENISA (2022, 2023) – Reports zu Cloud Security, Sovereignty & Multi-Tenant Architectures
- GAIA-X Architecture Documents (2023) – Federated Cloud Principles
- EU Cyber Resilience Act (2023/2024) – Anforderungen an sichere Software-Lieferketten
- SBOM Standards – NTIA / OASIS

Policy Debates & Think Tank Analysis

- European Parliament Research Service (EPRS) – „Digital Sovereignty for Europe“
- Bertelsmann Stiftung – „Europas digitale Abhängigkeiten“
- Bruegel – „Open Strategic Autonomy and the Digital Transition“
- CERRE – „Cloud Competition & Regulation in Europe“

Education, Skills & Society

- OECD – Future of Education & Skills 2030
- UNESCO – Digital Literacy Framework
- European Skills Agenda (2020–2025)
- World Economic Forum – Future of Jobs Reports (2020–2023)

Society. Economy. Technology. Sustainability.

The future emerges from balance and deliberate design.

The 4future.institute is a clearly defined and independent unit within 4future.business GmbH. The majority shareholder is the 4future.foundation.

Independence is the prerequisite for our work — not its outcome.

4future.institute | Graben 17/10 | 1010 Vienna | +43 1 31440-0 | hello@4future.institute