Policy Brief:

Digital Sovereignty in Europe

Definition, Status, Policy Options

Version 3
November 2026

4future.institute Policy Brief Series
Policy Brief No. 2026-001 (EN)
ISSN 3061-1881 (Online)
DOI: 10.5281/zenodo.24042486

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

Imprint

4future.institute · Graben 17/10 · 1010 Vienna · Austria · Phone: +43 1 31440-0 · hello@4future.institute

4future.institute is part of the 4future.group and is organised as an independent unit within 4future business GmbH.

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

About the 4future.institute: On almost every issue that matters today, there are more opinions than orientation. The 4future.institute asks: What is actually true here, what are the structural conditions — and does this make sense, not just economically but for us as a society? Its frame of reference is the 4future House: the goal is a good life for all, today and for future generations. It rests on three pillars, the "three Vs" — the transformation of work and the economy, distributive fairness and security of supply — linked by the rule of law, citizen-oriented administration and coordination, and founded on European fundamental values, ethics and sustainability (guiding paper "Strategie für eine lebenswerte Zukunft", 4future.institute Papers No. 2026-001, in German). Digital sovereignty is part of security of supply: being able to use digital services reliably, switch providers and decide over one's own data. The 4future.foundation enables the institute's independent work; financial support confers no influence over content or conclusions.

Series: 4future.institute Policy Brief Series, No. 2026-001 (EN), ISSN 3061-1881 (Online), DOI: https://doi.org/10.5281/zenodo.24042486

Language versions: German version: Policy Brief Nr. 2026-001 (DE). In case of discrepancies, the German version prevails.

Disclosure: Werner Illsinger is Executive Director of the 4future.institute, managing director of 4future business GmbH and chair of the board of the 4future.foundation. He also built 4future.digital, where he serves as CTO; 4future.digital provides cloud and collaboration services as a European alternative to Microsoft 365 and Google Workspace. 4future.digital is currently an independent company; the aim is for it to become, like 4future business GmbH, a subsidiary of the 4future.foundation. 4future business GmbH does not itself provide cloud services. The institute's recommendations are formulated in a provider-neutral way; 4future.digital and its services are neither mentioned nor assessed in this paper.

Executive Summary

Since 1990, the EU-27's share of global nominal GDP has fallen from around 27% to around 18%. The US share has remained broadly stable at around 26%, while China's has risen from under 2% to almost 17% (IMF, World Economic Outlook). A declining share is not an absolute decline: the European economy has grown, but more slowly than others. This trajectory has many causes. This paper examines one of them that is amenable to policy: a considerable part of what Europe generates in data, users and markets becomes value added in the balance sheets of non-European platform companies. 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 and operating in monopolistic market structures. They are thus subject to competing legal claims whose consequences European customers can neither fully control nor reliably exclude; lawful use does not remove this dependency.

This creates a structural deficit across three dimensions: Legally, European customers can neither control nor exclude access under US law such as the CLOUD Act and FISA Section 702. Technologically, the dominance of proprietary multi-tenant architectures limits verifiability and portability. Economically, a considerable part of digital value creation flows out of Europe.

Developments since the first publication of this paper have sharpened the situation: the PCLOB — a central oversight body on which the EU-US Data Privacy Framework relies — has lacked a quorum since its Democratic members were dismissed in January 2025.

FISA Section 702 lapsed on 12 June 2026 — for the first time since its enactment in 2008 — after two short-term extensions in April. Existing authorisations remain in force until they expire, expected around March 2027, under the continuing oversight of the FISA Court. Thereafter, absent new legislation, surveillance previously conducted under Section 702 would generally require individual orders under Title I of FISA. At the time of writing, a lasting arrangement remains outstanding. The legal basis on which the assessment of US protection in the Data Privacy Framework rests is therefore in flux.

The DPF is under legal challenge before the Court of Justice of the European Union (Case C-703/25 P). Industry responses such as Microsoft's EU Data Boundary and the AWS European Sovereign Cloud improve data residency and operational control in Europe, but do not remove the problem of conflicting legal claims from third countries (Section 2.2).

How far legal compliance and demonstrable protection diverge is shown by the November 2025 report of the Hessian Commissioner for Data Protection and Freedom of Information on Microsoft 365: it considers the contractual requirements on the processor being bound by instructions capable of being met, although it records that Microsoft cannot fully exclude disclosure on the order of the US government. The positive contractual assessment thus does not answer the customer's decisive question: are my data actually protected against such access? (Section 2.1)

On 3 June 2026, the European Commission proposed the Cloud and AI Development Act (CADA) — the first attempt to define in Union law what a sovereign cloud is. This is a step in the right direction; whether it achieves its objective will depend on the legislative process (Section 2.4).

What this paper adds. This paper adds to existing analyses in four respects:

- **The Data Protection Trilemma:** The conflict between European data protection law and US cloud services is structural rather than political. The controller remains accountable under Articles 5(2) and 28 GDPR, can in practice check processing only against audit reports commissioned by the provider itself, and can exclude a decisive risk neither through audits nor through contracts: access by authorities under the law of a third country, which may be subject to non-disclosure obligations. With Microsoft 365, encryption that effectively excludes the provider at the same time significantly restricts core functions of the service. This conflict persists irrespective of the political situation in the United States (Section 2.1).
- **An independent benchmark:** CADA is assessed against certification criteria set out in this paper before the proposal was published (Section 3.1.2; Version 2 of 1 June 2026) — rather than in terms of compliance obligations for providers or the interests of particular market participants.

- **Findings from the legislative text:** On the basis of the proposal, its annexes and the impact assessment, this paper shows that the baseline assurance level confers a sovereignty designation without any requirement to prevent third-country access to customer data; that the obligation to use higher levels is triggered by sector and activity rather than by the data processed, which systematically underestimates horizontal office, collaboration, email and identity platforms; that the impact assessment and the legislative text diverge on whether providers controlled from outside the Union can reach Level 3; and that the Commission's estimate of the distribution of use cases rests on a narrow empirical basis — points not addressed in the analyses reviewed in Section 2.4.
- **Digital and energy sovereignty:** Large data centres operated by non-European providers create few permanent jobs locally, while the value-adding functions remain at the operator's headquarters; at the same time, their electricity demand can deepen dependence on imported fossil fuels unless it is matched by additional renewable generation. Using the Kronstorf data centre as a case study, this paper argues that digital sovereignty must not be pursued at the expense of energy sovereignty, and proposes an additionality requirement modelled on Ireland's 2025 connection policy (Sections 2.3 and 3.3.5).

In addition, the companion paper "Digitale Souveränität braucht überprüfbare Interoperabilität" (June 2026, in German) examines whether services can be replaced in practice. This paper takes up its proposal for a European interoperability certification and links it to the CADA assurance levels (Sections 2.4 and 3.2.2).

In central digital functions, Europe currently lacks effective control over essential dependencies — legally, technologically and economically.

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 entail costs. They are offset by avoided dependency and disruption risks and by expected benefits for resilience, competition and European value creation; in this sense they are an investment in Europe's future viability.

Table of Contents

Executive Summary 3
1 Defining Digital Sovereignty 8
1.1 Legal Sovereignty 9
1.2 Technological Sovereignty 9
1.3 Economic and Societal Sovereignty 9
2 Status of Digital Sovereignty in Europe 10
2.1 Legal Status: Conflicting Legal Frameworks and Structural Tensions 10
2.2 Technological Status: Dependence on Non-European Platforms 18
2.3 Economic Status: Loss of Value Creation and Strategic Vulnerability 21
2.4 Policy Developments: The Cloud and AI Development Act (CADA) 25
2.4.1 Assessment Against the Requirements of This Paper 28
3 Policy Options for Strengthening Digital Sovereignty 32
3.1 Legal Framework 32
3.1.1 Define Applicable Law Clearly 32
3.1.2 EU-Wide Certification of Cloud and AI Services 32
3.1.3 Renegotiation of Transatlantic Agreements 34
3.1.4 Legal Framework for Critical Digital Infrastructure 34
3.1.5 Establish Global Regulation of Multinational Corporations 35
3.2 Technological Framework: Building European Control Capability 35
3.2.1 Building a European Cloud and AI Infrastructure 35
3.2.2 Interoperability as a Binding Standard 36
3.2.3 European Identity and Trust Services 37
3.2.4 European Security Architecture 37
3.3 Economic Framework: Reshaping Market Mechanisms 38
3.3.1 Strategic European Digital Investment and Innovation 38
3.3.2 Reducing Economic Dependencies 39
3.3.3 Market 39
3.3.4 European Procurement Reform 40

3.3.5 Energy Obligations for Large Data Centres 41
3.4 Societal Framework: Competence, Transparency and Participation 43
3.4.1 Education as the Foundation 43
3.4.2 Transparency as a Prerequisite for Trust 44
3.4.3 Building European Talent, Research and Innovation Capacity 45
3.4.4 Civil Society Participation in Major Digital Projects 45
3.4.5 Strengthening Global Cooperation 46
4 Conclusion 47
5 Call to Action 48
I. About the Author 49
II. Annex: Glossary 50
III. Annex: Sources & References 51
Legal Foundations 51
Market Data & Economic Facts 51
Technical Foundations 51
Policy Debates & Think Tank Analysis 51
Education, Skills & Society 51
Developments 2025–2026 52

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.

Digital sovereignty cannot be achieved in isolation from energy sovereignty and ecological sustainability. Digital infrastructure that deepens dependence on imported fossil fuels, or that consumes land, water and renewable capacity without contributing to them, merely replaces one strategic dependency with another.

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 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 limit European customers' direct technical control; customers generally receive only reports by auditors commissioned by the provider itself.

In Schrems II (C-311/18), the Court of Justice of the European Union invalidated the Privacy Shield because US law — in particular FISA Section 702 — did not ensure a level of protection essentially equivalent to that guaranteed in the Union and did not provide data subjects with an effective remedy. Standard contractual clauses remained valid, but require a case-by-case assessment and, where necessary, supplementary measures. The judgment does not establish a general prohibition on the use of US cloud services; since July 2023, transfers to companies certified under the Data Privacy Framework have been permitted on the basis of an adequacy decision. The following analysis therefore distinguishes four levels, none of which establishes the others: legal permissibility (may the processing take place?), the effectiveness of safeguards (which risk is actually reduced?), practical control capability (can the customer concerned use, verify and enforce the safeguards?) and digital sovereignty (can it maintain its essential digital functions in the event of conflict, disruption or a necessary change of provider?). The yardstick is practical usability: a safeguard establishes control capability only if the customer concerned can actually deploy it, verify its effectiveness and afford its use.

How easily these levels become blurred in practice is illustrated by the November 2025 report of the Hessian Commissioner for Data Protection and Freedom of Information (HBDI) on Microsoft 365. It examines the contractual framework against the criticisms raised by the German Data Protection Conference in 2022 and concludes that compliant operation is possible, provided that customers also fulfil their obligations as controllers. The report is not based on technical audits, and it expressly does not address questions of digital sovereignty (p. 9). Notably, the report itself records that Microsoft has acknowledged that disclosure on the order of the US government without the controller's express consent cannot be fully excluded in future; the HBDI refers to the hearing before the French Senate (pp. 67 f.). Immediately afterwards, it finds that the requirement of being bound by instructions under Article 28(3)(a) GDPR "can be met" (p. 68). The report thus records both at once: access on the order of the US government cannot be excluded — and the requirement is nonetheless deemed capable of being met. Its conclusion rests on contractual commitments: Microsoft will take legal action against such orders and, towards Hessian public bodies, will comply with the GDPR even where foreign authorities compel different conduct. Whether these commitments are honoured when it matters is something the customer cannot verify. The report also considers it "debatable" whether an IT service provider with significant market power can appropriately be classified as a processor bound by instructions, and sees this as a matter for the legislator (p. 46, fn. 66). Consistently, it recommends that controllers carry out their own audits and technical checks in appropriate cases (p. 87) and always evaluate, document and test alternative, preferably European solutions in order to reduce dependence on individual providers and the ability of third-country actors to exert political pressure (p. 93). The report thus answers the question of permissibility at the contractual level while naming — without resolving — the questions of control capability and sovereignty with which this paper is concerned. This is the core of the Data Protection Trilemma: a positive assessment at the contractual level does not answer whether the data are actually protected against third-country access. The report does not establish that any access has occurred — it makes the control gap visible.

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 must be able to verify the processor's compliance: Article 28(3)(h) GDPR requires the processor to allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. The audit right lies with the customer. In practice, large cloud providers replace this right with reports by auditors whom they commission themselves and whose scope they define themselves. Microsoft, for example, has its online services audited regularly and makes the reports available in its Service Trust Portal, in part only after acceptance of a non-disclosure agreement. Microsoft's general Data Protection Addendum provides for an audit by the customer only to the extent that the customer's audit requirements cannot reasonably be satisfied through these reports; scope and timing must be agreed with Microsoft, and the customer bears all costs, including Microsoft's time at its service rates. The order of magnitude involved is illustrated by a version of the Financial Services Amendment for financial-sector customers published by a Microsoft partner: it sets 4,000 US dollars per day for each Microsoft employee involved, plus travel expenses — an example of a documented contractual arrangement, not a general current tariff. The contractual framework thus does not guarantee small contracting authorities an economically accessible audit of their own; it shifts the organisation and funding of additional control onto customers — municipalities, schools, associations, SMEs — whose resources for this are regularly limited. For the great majority of controllers, control is thus in practice limited to what the provider chooses to show. And even an audit of their own could not establish one thing: the absence of disclosure orders issued under the law of a third country. Such orders may be subject to non-disclosure obligations and are then invisible to both customer and auditor.

In addition, the provider undertakes in the Data Processing Agreement (DPA) to comply with the GDPR and bears obligations of its own under Articles 28 and 32 GDPR. A provider subject to US law, however, cannot give a legally binding assurance that disclosure orders under US law (such as the CLOUD Act or FISA Section 702) will not occur; it can only commit to challenging such orders and to informing the customer where this is legally permitted.

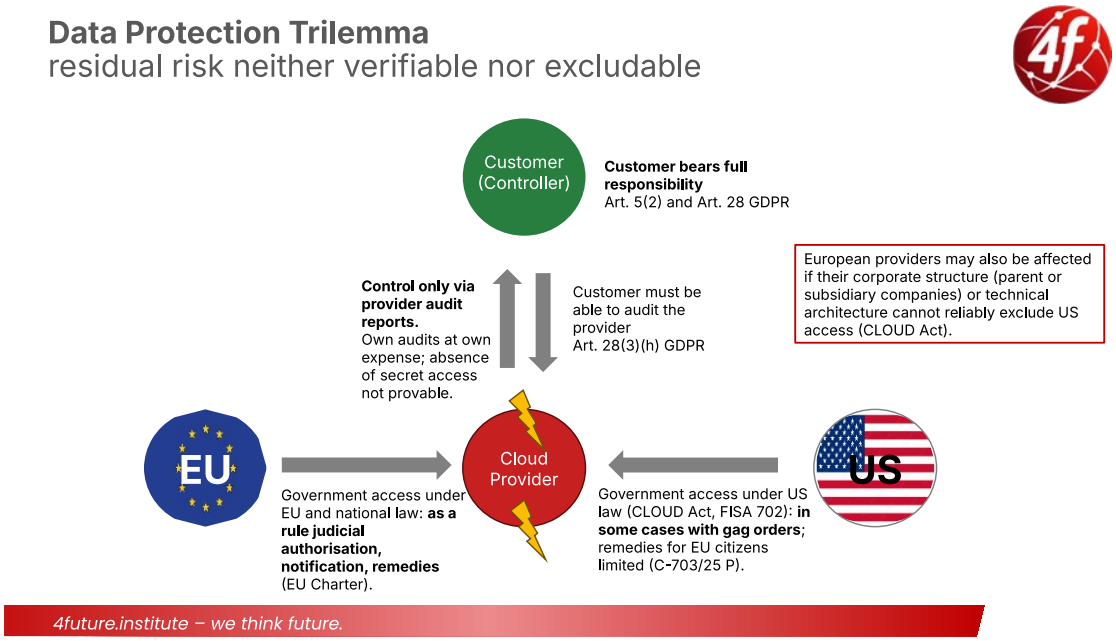
Reference is often made to technical and organisational measures, above all encryption. What matters is who holds the keys and who processes the data in clear text. Where the customer manages the keys but the service itself uses them — as with Microsoft Customer Key — the provider continues to decrypt the data for processing; this offers no protection against a disclosure order addressed to the provider. Where encryption effectively excludes the provider, as with Microsoft's Double Key Encryption, the service loses precisely the functions for which it is used: such documents cannot be viewed in the Office web apps, co-authoring and AutoSave are not supported, and AI features such as Copilot cannot process the content. With Microsoft 365, encryption that effectively excludes Microsoft from access to content thus significantly restricts core functions of the collaboration platform; the mere availability of such encryption does not show that customers can secure the service against third-country access without losing functionality. Then there is the effort involved: Double Key Encryption requires additional or higher-tier licence rights (such as Microsoft 365 E5 or corresponding add-on products), is supported only in the Office desktop applications on Windows, and requires the customer to operate its own key service — itself or through a service provider. For a small business, a municipality or an association, this is neither financially nor organisationally straightforward; the most effective safeguard is thus hardest to reach for precisely those with the least bargaining power.

The European Data Protection Board reaches the same conclusion for cloud services that require access to data in clear text to perform their task: given the state of the art, it is incapable of envisioning an effective technical measure to prevent access by third-country authorities with disproportionate powers (Recommendations 01/2020, Use Case 6). Services designed, like Microsoft 365, for the provider to process clear text therefore face a trade-off: the more effectively encryption excludes the provider, the less usable the service becomes; the safeguard that actually addresses the risk described removes core functions of the service. This is not a law of nature of digital collaboration: there are architectures that enable end-to-end encrypted collaboration with real-time editing in the browser, such as CryptPad. They are not equivalent in every respect and raise trust questions of their own, for instance regarding the program code delivered, but they show that protection against the provider and collaboration can be compatible. Sovereign alternatives should be measured against precisely this question. A general reference to "appropriate technical and organisational measures" is therefore not a sustainable justification. Each measure must be assessed against the risk it is meant to address:

- **Storage in Europe:** Which avenues of access and control remain outside Europe?
- **Encryption:** Who holds the keys and clear-text access — including during processing?
- **Audit and certification:** Which systems, periods and risks were actually audited, and who commissioned the audit?
- **Contractual assurances:** Which obligations remain enforceable in the event of conflict?
- **Data export:** Can data, permissions and workflows actually be reused after a switch (see Section 3.2.2)?
- **Exit plan:** Has the switch been tested under realistic conditions and costed?

Anyone claiming that a measure provides protection must disclose its preconditions, its reach and its limits.

This creates what this paper terms the Data Protection Trilemma: a tension between the controller's full accountability, its control over processing, which in practice is limited to the provider's own reports, and the competing legal claims of a third country. The trilemma does not render the use of such services unlawful per se. It describes a residual risk that the controller can neither fully verify nor exclude by contract. For personal data requiring a high level of protection and for public-order activities, this paper considers that residual risk unacceptable. This is a policy judgement, not a legal conclusion. Equally important is the distinction: that access cannot be excluded is not evidence that it has occurred — it is a finding about the limits of control.



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. Since then, the PCLOB has lacked a quorum. The agency continues to exist but cannot take formal decisions; the independent oversight presupposed in the adequacy decision is therefore significantly weakened.

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 (Case C-703/25 P, filed on 31 October 2025) 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: after two short-term extensions in April 2026, FISA Section 702 — together with the whole of Title VII of FISA — lapsed on 12 June 2026, for the first time since 2008. Under the transition provisions, existing orders, authorisations and directives remain in effect until they expire; Title VII continues to apply to them, the FISA Court retains its oversight authority, and providers remain obliged to comply (Congressional Research Service, 2026). The certifications approved in March 2026 are reported to remain valid until around March 2027. Thereafter, surveillance previously conducted under Section 702 is governed by Title I of FISA, which generally requires individual orders. At the time of writing, Congress has not passed a lasting arrangement. The assessment of US protection in the Data Privacy Framework rests in part on the Section 702 framework; how the Commission will respond to its lapse or to new legislation remains open.

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 around 70% of the European cloud market; European providers together account for around 15%, down from 29% in 2017 (Synergy Research Group, 2025).

Collaboration & communications: Strong dependence on Microsoft and Google. An analysis by Compass Lexecon commissioned by the Open Cloud Coalition, on which a study for the European Parliament draws, estimates the two providers' combined share of the EU market for collaboration software at up to 93% (2023 data). The figures are modelled: they are based on commercial market data adjusted using assumptions about partner networks, are considerably lower in other calculation scenarios, and do not provide a separately measured public-sector share

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

Identity management: Strong dependence on Azure AD / Entra ID (Microsoft)

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 made the AWS European Sovereign Cloud generally available: a cloud located in the EU and physically and logically separate from other AWS Regions. It is operated by a new parent company and three subsidiaries incorporated under German law, led by EU citizens resident in the EU, with operations and support provided by EU-resident staff. The companies nevertheless remain part of the Amazon group. The approach thus goes beyond contractual assurances and addresses operational dependencies more seriously than previous market solutions. Whether it excludes disclosure orders under the CLOUD Act depends on whether the US parent is legally regarded as having "possession, custody, or control" of the data (18 U.S.C. § 2713) — a question that has not yet been settled by the courts.

In February 2025, Microsoft completed its EU Data Boundary: customer data and pseudonymised personal data for its core cloud services — including Microsoft 365 and most Azure services — as well as data from support cases are now stored and processed in the EU and EFTA. This is an implemented data-residency measure; it does not change the legal structure, since the services continue to be provided by companies under the full control of the US parent. Microsoft France's director of public and legal affairs acknowledged under oath 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]

For comparison, all offerings should be assessed against the same criteria: ownership and control, operational dependencies on the parent company, avenues for data access, management of cryptographic keys, dependence on software supply, and the ability to continue operating if the relationship with the group is interrupted. Measured against these criteria, both approaches improve data residency and operational control to differing degrees; neither removes membership of a group subject to US law.

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

The practical relevance of this exposure has since become visible. Following US sanctions against the International Criminal Court (ICC) in February 2025, it was reported in May 2025 that the Court's Chief Prosecutor had lost access to his Microsoft-hosted email account; Microsoft has disputed these reports. In October 2025, the ICC confirmed that it would replace Microsoft Office with openDesk, an open-source suite developed by Germany's Centre for Digital Sovereignty in Public Administration (ZenDiS).

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.

Public institutions have begun to act. In Schleswig-Holstein, around 80% of state-government workstations had moved from Microsoft Office to LibreOffice by autumn 2025. Denmark's Ministry of Digital Affairs announced in June 2025 that it would replace Microsoft 365 with LibreOffice. The Austrian Armed Forces have replaced Microsoft Office with LibreOffice on around 16,000 workstations. In April 2026, France selected Scaleway to replace Microsoft Azure as host of its national Health Data Hub, with migration planned for late 2026 to early 2027. In the same month, the European Commission awarded a sovereign cloud framework contract worth up to €180 million over six years to four European provider groups, one of which includes S3NS, a joint venture of Thales and Google Cloud. These developments indicate both that alternatives exist and that the meaning of "sovereign" remains contested in practice.

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

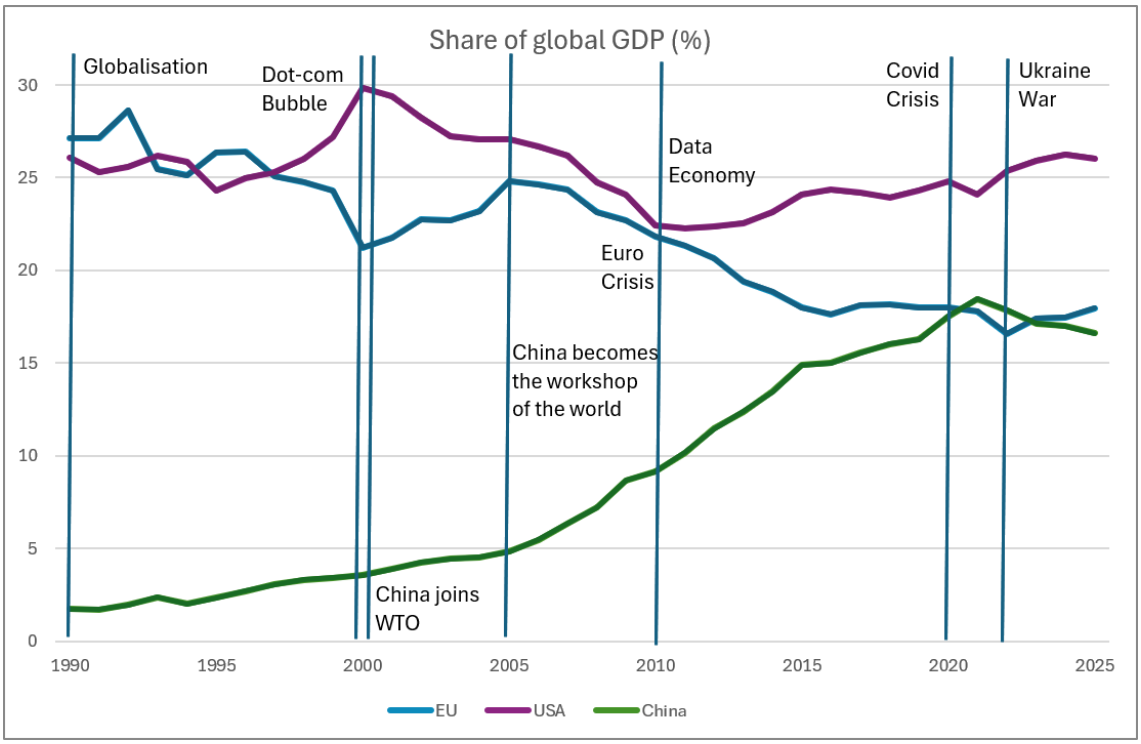
These dependencies result in:

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.

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.



Share of the EU-27, the US and China in global nominal gross domestic product (GDP), 1990–2025. 2025: IMF projection. Source: International Monetary Fund (IMF), World Economic Outlook Database (indicator NGDPD), 4future.institute.

These developments have consequences for our economy. The EU-27's share of global nominal GDP has fallen from around 27% in 1990 to around 18% in 2025; the EU thus remains narrowly ahead of China, whose share rose from under 2% to almost 17% over the same period (IMF, World Economic Outlook Database, indicator NGDPD). The chart shows the context, not the causes: demographics, exchange rates, the financial and euro crises, and China's rise as the workshop of the world all contribute to the declining share. How much digital dependency contributes cannot be derived from the chart. This paper instead grounds its economic significance in concrete mechanisms: value creation accruing at providers' headquarters, lock-in and limited bargaining power (see below and Section 3.3).

Whatever the causes of this trajectory, over the past three decades Europe has largely 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 central digital functions cannot in practice be replaced, European businesses and public bodies remain exposed to the pricing, product and operational decisions of a few platform providers. A growing European digital market does not automatically remove this dependency.

Case in point: Kronstorf. In April 2026, construction began on Google's first Austrian data centre in Kronstorf, Upper Austria, on a site of around 50 hectares. Google cites around 100 direct jobs; the regional government described the project as the largest single investment in the region's history. Public debate has centred on electricity, water and land use. The case illustrates three distinct dimensions of the problem described in this paper.

Jurisdiction: The physical location of a data centre does not change the law to which its operator is subject. A facility in Austria operated by a US company remains within the reach of the CLOUD Act. It can satisfy the location criteria of the baseline assurance level proposed under CADA without addressing extraterritorial access (Section 2.4).

Value creation: Data centres are highly automated. Construction generates substantial but temporary employment; operation requires comparatively few permanent staff. A 2024 study by Virginia's Joint Legislative Audit and Review Commission found that data-centre jobs are predominantly temporary construction jobs, and recent UK research estimates as few as 1.6 permanent jobs per megawatt for new large campuses. The functions that generate most of the value — software and platform engineering, systems architecture, product development, intellectual property, margins and the associated tax base — are located where the operator has its headquarters and development organisation. For a US hyperscaler, that is predominantly outside Europe; for a European operator, it is within Europe, though not necessarily in the host Member State. Proponents point to indirect employment, supply-chain effects and regional attractiveness; these effects are real but do not alter the location of the core value-adding functions.

Energy: According to Netz Oberösterreich, the planned expansion could consume up to 4.4 TWh of electricity per year — nearly one third of Upper Austria's total consumption of 14 TWh in 2024. This demand arises at a time when Austria and the European Union are committed to climate neutrality. Even in Austria, with its high share of hydropower, gas-fired generation is reported to set the wholesale electricity price around two thirds of the time, and Austria's gas is now imported predominantly via Germany, as Norwegian pipeline gas and liquefied natural gas. Large additional demand that is not matched by additional renewable generation therefore risks deepening dependence on imported fossil fuels — replacing one strategic dependency with another. Guarantees of origin purchased on paper do not change this, as they reallocate existing renewable generation rather than adding to it (see Section 3.3.5).

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.

2.4 Policy Developments: The Cloud and AI Development Act (CADA)

On 3 June 2026, the European Commission presented its Technological Sovereignty Package. Its centrepiece is the proposal for a Regulation on a Cloud and AI Development Act (CADA, COM(2026) 502 final, procedure 2026/0138(COD)). Title IV of the proposal (Articles 16–31, Annexes II and III) establishes, for the first time in Union law, a framework defining graduated levels of sovereignty for cloud computing services provided to public-sector bodies and Union entities. CADA is a proposal under the ordinary legislative procedure and remains subject to negotiation between the European Parliament and the Council.

The framework comprises four cumulative "Union assurance levels", the criteria for which are set out in Annex II (Article 16). Within one year of entry into force and every two years thereafter, Member States and Union entities must carry out risk assessments that identify public-sector activities contributing to the preservation of public order — in the sectors covered by Annexes I and II of the NIS2 Directive and in the areas of national security, internal security, external border management, defence, justice and law enforcement — and determine whether Level 2, 3 or 4 is appropriate for them (Article 29(1)). These assessments must consider, inter alia, the sensitivity of the data processed, the risk of unlawful third-country access and the risk of service disruption (Article 29(2)); the Commission may specify different levels by implementing act where it considers an assignment inappropriate (Article 29(5)). Activities so identified may only use services recognised at Level 2, 3 or 4 (Article 30(3)); all other activities must use services recognised at least at Level 1 (Article 30(2)). In summary:

Level 1: The provider is established in the Union; infrastructure, assets and customer data — including metadata and telemetry — remain in the Union, unless the public-sector body explicitly requires otherwise; the service complies with state-of-the-art cybersecurity standards; and the use of subcontractors is transparent (Annex II, Section 1.1(a)–(f)). Control by a third country is permitted. A provider subject to such control must guarantee that no third-country law or practice requires it to report software vulnerabilities to third-country authorities before they are known to have been exploited (Annex II, Section 1.1(g)). Conformity is established by self-assessment and a published EU statement of conformity, by which the provider assumes responsibility for compliance (Article 19); statements issued by SMEs are recognised automatically in all Member States (Article 17(3)).

Level 2: Independent third-party audit (Article 20). Provider and subcontractors are established in the Union, and infrastructure, assets and personnel are located there; a European cybersecurity certificate at assurance level "substantial" is required (or, pending such a scheme, national schemes); data generated by the service may not be used to train AI systems operated by third-country entities; support is performed exclusively within the Union; and software supply-chain measures apply, including an SBOM, source-code audits of security-relevant third-country components and documented migration plans (Annex II, Section 2.1). Third-country control remains permitted, provided that measures ensure that it does not restrict service delivery, that third-country access to customer data and disruption of service continuity are prevented, and that the provider cannot be obliged to give effect to third-country sanctions or embargoes (Annex II, Section 2.1(g)).

Level 3: In addition, personnel must be Union citizens (with national security clearance where classified information is handled), and support must be provided by Union residents and by parties not subject to third-country control (Annex II, Section 3.1(d) and (h)). Third-country control is excluded in principle, but may be permitted where the Commission has recognised the third country by implementing act (Annex II, Section 3.1(g)). Article 18 sets six cumulative conditions for such recognition, including an adequacy decision under Article 45 GDPR, the absence of measures enabling control that conflicts with the lawful-access rules of Article 32 of the Data Act, and the absence of measures compelling service disruption or compliance with third-country sanctions. (Annex II, Section 3.1(g), refers to an implementing act "under Article 19"; the reference is evidently intended to be to Article 18.)

Level 4: No third-country control, without derogation; a European cybersecurity certificate at assurance level "high"; and further requirements concerning control over software components (Annex II, Section 4).

The Commission's impact assessment (SWD(2026) 502) assumes that around 70% of public-sector use cases would require Level 1, 20% Level 2, 9% Level 3 and 1% Level 4. These figures are based on discussions with three public authorities representing about 200 contracting authorities, out of an estimated 6,400 NIS2 entities; the impact assessment itself presents them as an assumption. Article 30(4) permits contracting authorities, on an exceptional and duly justified basis, not to procure recognised services where no adequate recognised service is available, where a comparable procurement in the previous year produced no suitable tenders, or where applying the requirements would entail disproportionate cost; the proposal does not define disproportionality. Article 32 requires non-price award criteria assessing the tenderer's contribution to a European cloud and AI ecosystem in procurements of innovative cloud services and AI systems; these criteria must be ancillary and not decisive, and Recital 67 suggests a maximum weighting of 15 out of 120 points.

The graduated approach is defensible in principle: not every public-sector workload requires the highest level of protection, and Recital 52 frames the levels as a proportionate framework. Level 2 is also more demanding than its permissive treatment of third-country control suggests, since it requires demonstrable protection against data access, service disruption and the enforcement of third-country sanctions. The impact assessment states that its preferred option would not allow providers whose parent company is headquartered outside the Union to qualify as Level 3; the legislative text, however, provides for exactly such a possibility via recognition under Article 18.

2.4.1 Assessment Against the Requirements of This Paper

Positioning in the existing debate. The analyses of CADA published so far come predominantly from legal advisory practice and are addressed to providers and businesses. Covington & Burling and Hogan Lovells describe the structure and levels of the framework and identify uncertainties for providers; Bird & Bird analyses the levels as a condition of market access and asks which types of provider can reach which level; Lawfare places the proposal in a transatlantic perspective and notes that the conditions of Article 18 could exclude US providers despite the adequacy decision. Eurosmart, an association of the European digital security industry, calls for Level 3 not to be opened to providers under third-country control. The present analysis differs from these in perspective and yardstick: it assesses the proposal from the standpoint of public contracting authorities as controllers under the GDPR — in particular smaller bodies without their own audit capacity — and measures it against criteria formulated before its publication. Several of the following findings are not addressed in any of the analyses mentioned: the absence of an obligation to prevent third-country access at Level 1; the linking of the obligation to use higher levels to sector and activity rather than to the data processed, and the resulting underestimation of horizontal platforms; the undefined cost exception in Article 30(4); the contradiction between the impact assessment and the legal text on Level 3; the narrow empirical basis of the Commission's distribution estimate; the erroneous cross-reference in Annex II; and the absence of an additionality requirement for data centres in acceleration zones. This positioning is based on the analyses mentioned and does not claim to be exhaustive.

Measured against the certification requirements set out in Section 3.1.2, CADA addresses the right question. Five aspects, however, merit critical attention in the legislative process:

The baseline level contains no protection against third-country access: Level 1 — expected to cover the large majority of use cases — rests on self-assessment and permits third-country control. Unlike Level 2 (Annex II, Section 2.1(g)(ii)), its criteria contain no requirement that third-country access to customer data be prevented; the location requirements may, moreover, be waived at the request of the public-sector body. For providers subject to the CLOUD Act, Level 1 therefore does not address the extraterritorial access risk described in Section 2.1 — a limitation acknowledged by Microsoft before the French Senate (see Section 2.2). Recognised Level 1 services will nonetheless carry an official designation within a framework explicitly described as a sovereignty framework.

The obligation to use higher levels is triggered by sector and activity: Although Article 29(2)(a) requires the sensitivity of the data, including personal data, to be considered, Levels 2 to 4 are mandatory only for activities identified as contributing to public order in the sectors and areas listed in Article 29(1)(a). For all other activities, Level 1 suffices as the minimum requirement, irrespective of the personal data they process; public bodies may choose higher levels but are not required to do so. In organisational practice, moreover, personal and sensitive data does not remain confined to the specialised systems for which it was collected: it is exported into spreadsheets, shared on collaboration platforms and transmitted as email attachments. Horizontal office, collaboration, email and identity platforms therefore typically process personal and frequently sensitive data, irrespective of how the specialised applications from which that data originates are classified.

An undefined cost derogation: Article 30(4)(c) allows departures where the requirements would entail disproportionate cost, without defining proportionality. Since switching costs increase with the depth of existing dependencies, an undefined cost criterion risks favouring precisely those arrangements whose lock-in the framework seeks to reduce.

Third-country recognition by implementing act: The conditions in Article 18 are demanding; in particular, the requirement that a third country have no measures compelling service disruption or compliance with its sanctions regimes would be difficult to reconcile with current US law. However, recognition is decided by implementing act and presupposes an adequacy decision under Article 45 GDPR — a mechanism whose current application to the United States is under review before the Court of Justice (Case C-703/25 P; see Section 2.1).

No additionality requirement for accelerated data centres: CADA aims to accelerate data-centre deployment through acceleration zones and shortened permitting procedures (Articles 10–13). When designating such zones, Member States must consider grid capacity, on-site clean energy generation and the reuse of waste heat (Article 10(1)); sustainability requirements within the zones are, however, limited to the key performance indicators of Delegated Regulation (EU) 2024/1364 (Article 11(1)). The proposal does not require operators to contribute to additional renewable generation. Accelerated permitting thus risks accelerating demand without accelerating the corresponding supply of renewable electricity (see Section 3.3.5).

With regard to exit capability, the proposal relies on the switching provisions of the Data Act (Regulation (EU) 2023/2854). Where a risk assessment requires a change of service, migration must take place within a transition period of no more than twelve months (Article 29(6)), and risk assessments must consider whether a multi-vendor or multi-cloud strategy is appropriate (Article 29(9)). Levels 2 and 3 also require documented migration plans for third-country software components. The proposal does not, however, make a public body's own tested exit capability a general procurement requirement. CADA thus measures how far a service is exposed to third-country influence, but not whether it can be replaced. Sovereignty requires both: control over the provider and the ability to switch away from it. That the Data Act's switching provisions are insufficient for complex collaboration platforms — because a data export does not carry over workflows, permissions and organisational context — is shown in the companion paper on interoperability (see Section 3.2.2).

Small contracting authorities: Cutting across these points is a question the proposal barely addresses: whether smaller public bodies — municipalities, schools, smaller agencies — can make practical use of the framework. The risk assessments under Article 29 are carried out by the Member States; but the selection, procurement and control of services lie with the individual body. It must judge the differences between the levels and evaluate declarations of conformity or audit reports whose significance it can hardly assess itself; at Level 1, it has only the provider's self-assessment. Whether a documented exit plan will hold in an emergency, it cannot determine without testing it. And the cost exception in Article 30(4) is likely to be invoked precisely where funds and expertise are lacking. A framework whose application presupposes a control capability that small contracting authorities lack shifts the burden of managing structural dependency onto those least able to bear it.

An official sovereignty designation is therefore informative only in conjunction with two further pieces of information: the assurance level concerned, and whether conformity rests on self-assessment or on independent audit. Procurement decisions, public communication and market offerings should state both.

Conclusion: CADA is the first serious attempt to translate digital sovereignty from political rhetoric into verifiable legal criteria. Its effectiveness will depend on the outcome of the legislative process — in particular on the criteria for Level 1, the scope of the risk assessments under Article 29, the cost derogation in Article 30(4), the conditions for third-country recognition under Article 18 and the energy conditions attached to accelerated data-centre deployment.

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.

CADA provides a concrete legislative vehicle for these requirements (see Section 2.4). For the negotiations in the European Parliament and the Council, the following amendments would be consistent with the analysis of this paper:

- **Protection and verification at Level 1:** Level 1 should include a requirement to prevent third-country access to customer data and be subject to independent verification — or should not be presented as part of a sovereignty framework.
- **Classification by data:** Article 29 should allow higher levels to be assigned on the basis of the personal and sensitive data processed, not only for activities related to public order; office, collaboration, email and identity platforms used in public administration should require at least Level 2.
- **A defined cost derogation:** The cost derogation in Article 30(4)(c) should be defined, time-limited, publicly justified and tied to a binding migration plan.
- **Third-country recognition:** Recognition under Article 18 should rest on statutory safeguards in the third country that are subject to independent oversight, rather than on adequacy decisions based on executive commitments; the cross-reference in Annex II, Section 3.1(g), should be corrected.
- **Exit capability as a criterion:** Documented data portability, open formats and a tested exit plan should be required at every assurance level; in the medium term, the levels should be coupled with a European interoperability certification (see Section 3.2.2).
- **Transparency:** Public bodies should disclose the assurance level at which each cloud service has been procured and the basis of its recognition (self-assessment or audit).

So that the burden does not fall on the small contracting authorities whose lack of control this paper describes, the following are also needed:

- **Jointly funded audits:** Member States or Union entities should commission audits of recognised services jointly and on behalf of all contracting authorities, rather than each body having to negotiate and pay for audit rights individually.
- **Expert support:** Competence centres should evaluate declarations of conformity and audit reports for smaller contracting authorities and provide model assessments.
- **Joint procurement:** Framework agreements at national or European level should include audit and exit rights that benefit all bodies entitled to call off from them.

- **Understandable evidence:** Publicly accessible summaries of audit results per level should be available for each recognised service.
- **Tested switching options:** For the most widely used services, regular publicly funded switching tests should be carried out and their results published.

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 lapsed on 12 June 2026 after two short-term extensions, without a lasting reauthorisation. Existing authorisations remain in force under FISA Court oversight until they expire; the future legal basis is open. At the same time, the PCLOB, on which the EU-US Data Privacy Framework relies as an oversight body, has lacked a quorum since January 2025.

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.

The companion paper “Digitale Souveränität braucht überprüfbare Interoperabilität” (Digital sovereignty requires verifiable interoperability; 4future.institute, June 2026, in German) develops this section further. It shows that formally open standards are not enough: dominant platforms set de facto references through their implementations, and dependencies are shifting from file formats to workflows, identities, interfaces and AI-based knowledge systems. It therefore proposes a European interoperability certification with open test procedures and reference implementations at three levels — from documented support for open standards, through full interoperability of core functions, to lossless migration of data, metadata, workflows and organisational context — which should gradually become a precondition for public procurement. It also recommends examining whether Microsoft Office, in all its forms of distribution, should be designated as a gatekeeper under the Digital Markets Act.

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. These providers' revenue in Europe should not, however, be equated with value creation lost to Europe: part of it remains in Europe through local employment, partner companies and taxes, and European providers also source hardware, components and services from outside Europe. The most value-intensive functions — development, intellectual property and margins — are, however, located predominantly at the providers' headquarters (cf. Section 2.3).

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 can shift value creation back to Europe: data centres, software development, research, maintenance and operations can be delivered locally, creating skilled jobs, tax revenues and technological know-how. A larger share of value creation thus remains in Europe — though not all of it, since European providers also source hardware, components and services from outside Europe.

Support programmes for migration, investment incentives for interoperable systems and tax incentives for open technologies are subsidies. They are justified where they absorb transition and transformation costs, lower market barriers and can be expected to generate long-term economic returns; their benefits must be weighed against their costs. The public expenditure is time-limited; the expected structural benefit is lasting: reduced dependencies, greater digital resilience, a broader competitive base and a stable European technology market.

Investment in digital sovereignty can therefore be expected to yield not only social and security benefits but economic ones; whether it pays off must be demonstrated for specific programmes on the basis of their costs and effects. 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.

(4) Contractual exit safeguards make freedom of choice enforceable: full data export in open formats at no additional charge, customer-controlled encryption keys, a documented and tested exit plan, audit rights and maximum contract terms. An exit that exists only on paper is not an exit.

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.

3.3.5 Energy Obligations for Large Data Centres

Digital sovereignty must not be pursued at the expense of energy sovereignty. This applies irrespective of the operator's origin: European operators, too, must justify their resource requirements and their contribution to security of supply. Large data centres should therefore be required to contribute to the renewable generation capacity they consume, rather than drawing on existing capacity. Two Member States provide reference models:

Ireland: Under the connection policy adopted by the Commission for Regulation of Utilities in December 2025, new data centres must, within six years of energisation, meet at least 80% of their annual electricity demand with additional renewable electricity projects generating in Ireland; during this transition period, demand may also be met from fossil generation; generation already supported through existing support schemes does not count towards this requirement. The policy also requires on-site or proximate dispatchable generation or storage — a requirement that may in practice be met with gas-fired generation and should therefore be designed with care.

Germany: The Energy Efficiency Act (EnEfG, § 11) requires data-centre operators to cover their electricity consumption on a balance-sheet basis with renewable electricity — 50% from 2024 and 100% from 2027 — and imposes minimum shares of reused energy for new facilities. A draft amendment would postpone the 100% requirement to 2030.

Austria: Austria is in a structurally different position from Ireland. With around 4.8 GW of pumped-storage capacity — including the Kaprun group, which reaches 1,335 MW following the opening of Limberg III (480 MW) in September 2025 — it has substantial capacity to store renewable electricity and to provide flexibility without new gas-fired generation. Pumped storage, however, shifts electricity in time rather than generating it, and existing capacity already serves the entire interconnected system. An Austrian implementation of the Irish model should therefore combine an additionality requirement for renewable generation with a contribution to additional storage capacity — for instance through long-term contracts that help finance new pumped-storage projects such as the planned Schaufelberg plant at Kaprun — in place of on-site dispatchable fossil generation.

On this basis, the following measures are recommended:

Such obligations are not only a burden on operators. Electricity is one of the largest operating costs of a data centre; in Germany, energy is estimated to account for around half of operating expenditure. Renewables have become the lowest-cost source of new generation: according to the International Renewable Energy Agency, more than 90% of utility-scale renewable capacity added worldwide in 2025 was cheaper than the lowest-cost fossil alternative. Under merit-order pricing, however, the wholesale price is set by the most expensive plant required to meet demand — frequently a gas-fired plant — so that the low cost of renewable generation reaches consumers only in part. Long-term power purchase agreements with new renewable and storage projects give operators direct access to these lower generation costs and long-term price stability. Storage, in turn, shifts surplus renewable output into periods of scarcity and reduces the number of hours in which gas-fired plants set the price, to the benefit of all consumers. Operators would thus be among the first to benefit from the additional capacity they help to finance. Additionality aligns the interests of operators, host regions and the energy transition.

- **Additionality:** A substantial share of the annual electricity demand of large data centres should be met by newly built, unsubsidised renewable generation in the same country or bidding zone, rather than by guarantees of origin alone.

- **Temporal and regional matching:** Renewable supply should be matched to consumption on a regional basis and, as far as feasible, on an hourly rather than an annual basis. An annual renewable balance does not demonstrate continuous supply; generation, storage, grid capacity and availability over time must be considered together.
- **Storage instead of gas turbines:** Dispatchable capacity should be provided through additional storage and demand flexibility rather than new fossil generation.
- **Waste heat reuse:** Minimum shares of reused waste heat should be a condition of permits wherever suitable heat networks exist or are planned.
- **Conditional acceleration:** Accelerated permitting in CADA acceleration zones should be conditional on additionality and waste-heat reuse.
- **Transparency:** Operators should disclose electricity and water consumption, the origin of their electricity and the share of additional renewable generation, as a basis for informed public participation (see Section 3.4.4).

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 judge what AI produces.

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 entail costs, but they are above all 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.

Digital sovereignty that comes at the expense of energy sovereignty and the natural environment is not sovereignty — it is a shifted dependency.

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 a Cloud and AI Development Act whose sovereignty label is independently verified,
- 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 comes at a price — 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
- 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)

Developments 2025–2026

- European Commission (2026) – Proposal for a Regulation on the Cloud and AI Development Act, COM(2026) 502 final, 3 June 2026
- European Commission (2026) – Annexes to the CADA Proposal, COM(2026) 502 final
- European Commission (2026) – Impact Assessment accompanying CADA, SWD(2026) 502
- Agence Europe (2026) – Commission wants European cloud providers to double market share to 30% (Bulletin 13883)
- Covington & Burling (2026) – The EU Cloud and AI Development Act in Depth
- Bird & Bird (2026) – Sovereignty as Market Access: What CADA's Assurance Levels Mean for Public-Sector IT Providers
- Hogan Lovells (2026) – The EU's Cloud and AI Development Act: Towards a Sovereignty-Focused Framework
- Eubelius (2026) – The Cloud and AI Development Act: Public Procurement as a Strategic Tool
- Lawfare (2026) – The EU Cloud and AI Development Act
- Congressional Research Service (2026) – The Impact of FISA Section 702's Repeal, LSB11444
- Official Journal of the EU (2025) – Appeal in Case C-703/25 P, Latombe v Commission, C/2025/6610
- Synergy Research Group (2025) – European Cloud Providers' Local Market Share Holds Steady at 15%
- EJIL:Talk! (2025) – Why It Matters that the International Criminal Court Embraced Open-Source Software
- Heise (2025) – Schleswig-Holstein Relies on Open Source and Saves Millions
- The Record (2025) – Denmark's Digital Ministry to Replace Microsoft with Open-Source Software
- Militär Aktuell (2026) – Why the Austrian Armed Forces Replaced Microsoft Office with LibreOffice
- Plateforme des données de santé (2026) – Press release on migration to Scaleway, 23 April 2026
- Der Standard (2026) – Die neue Schwerindustrie: Was hat Kronstorf vom KI-Boom?

- ORF (2026) – Großbaustelle von Google in Kronstorf
- MeinBezirk (2026) – Protest in Kronstorf gegen Großprojekt (Netz Oberösterreich consumption estimate)
- Computing (2026) – UK Datacentre Jobs Claim Overstated by Three-Quarters, Says Research
- Nature Forward (2025) – Data Centers Are Said to Create Jobs (summary of Virginia JLARC 2024 study)
- Der Standard (2025) – Merit order and gas as price-setting technology in Austria
- ORF (2025) – Gasversorgung laut E-Control gesichert
- Commission for Regulation of Utilities (2025) – Decision on New Electricity Connection Policy for Data Centres
- Energieeffizienzgesetz (EnEfG), § 11 – Klimaneutrale Rechenzentren
- Gleiss Lutz (2026) – Gesetzentwurf zur Änderung des Energieeffizienzgesetzes
- Salzburg24 (2025) – Neues Verbund-Kraftwerk Limberg III in Kaprun fällt für Monate aus (pumped-storage capacity in Austria)
- Leadersnet (2025) – Pumpspeicherkraftwerk Limberg III in Kaprun eröffnet
- Salzburg24 – Pläne für das Pumpspeicherkraftwerk Schaufelberg in Kaprun
- SolarQuarter (2026) – IRENA: Over 90% of New Renewable Power Added in 2025 Was Cheaper than Fossil Fuels
- KPMG – Drei Erfolgsfaktoren für die Zukunft deutscher Rechenzentren
- DatacenterDynamics (2026) – EU Commission Selects Four Cloud Providers under €180m Sovereign Cloud Tender
- Gineikyte-Kanclere, V. et al. (2025) – European Software and Cyber Dependencies, study for the ITRE Committee of the European Parliament, PE 778.576 (p. 49, Figure 10)
- Microsoft – Microsoft Customer Agreement, Financial Services Amendment (Germany), Sections 2–4 (audits by Microsoft; audit rights of customers and regulators)
- European Data Protection Board (2021) – Recommendations 01/2020 on measures that supplement transfer tools, Version 2.0 (Use Case 6)
- Microsoft – Double Key Encryption (licensing and system requirements)
- Entrust (2024) – Microsoft Double Key Encryption and Entrust KeyControl, Integration Guide (supported applications)
- CryptPad – end-to-end encrypted collaboration in the browser

- Microsoft – Double Key Encryption FAQ
- Microsoft – Enable co-authoring for files encrypted with sensitivity labels (limitations)
- Practical365 – Securing Copilot for Microsoft 365 (DKE-protected content)
- Illsinger, W. (2026) – Digitale Souveränität braucht überprüfbare Interoperabilität [Digital sovereignty requires verifiable interoperability], 4future.institute, Version 1.1, 1 June 2026 (in German)
- 4future.institute (2026) – Digital Sovereignty in Europe, Policy Brief, Version 2 of 1 June 2026
- Eurosmart (2026) – Position Paper on the Cloud and AI Development Act (CADA)
- Hessian Commissioner for Data Protection and Freedom of Information (2025) – Report on Microsoft 365 (in German), Version 1.0, 15 November 2025
- Microsoft – Products and Services Data Protection Addendum (DPA), section on auditing compliance
- Microsoft – Microsoft Customer Agreement, Financial Services Amendment, Section 4 (cost of customer audits: US$4,000 per day per employee)
- Microsoft – Get started with Microsoft Service Trust Portal (audit reports, non-disclosure agreement)
- Microsoft (2025) – Microsoft completes landmark EU Data Boundary, 26 February 2025
- Amazon Web Services (2026) – AWS launches AWS European Sovereign Cloud, 15 January 2026
- 18 U.S.C. § 2713 – Required preservation and disclosure of communications and records (CLOUD Act)
- European Data Protection Board (2021) – Guidelines 07/2020 on the concepts of controller and processor in the GDPR
- International Monetary Fund – World Economic Outlook Database (indicator NGDPD)



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