Policy Brief Summary

Digital Sovereignty in Europe

Findings and Policy Options · Policy Brief No. 2026-001 (EN), Version 3, November 2026

Europe's core digital infrastructure — cloud, identity, communications, AI — is provided predominantly by platforms subject to foreign legal systems and operating in monopolistic market structures. It is thus subject to competing legal claims whose consequences European customers can neither fully control nor reliably exclude. Lawful use does not remove this dependency.

In central digital functions, Europe currently lacks effective control over essential dependencies — legally, technologically and economically. This summary presents the findings and recommendations of Policy Brief No. 2026-001; evidence and sources are contained in the full version.

Four Levels: Why Permissibility Is Not Enough

The paper distinguishes four levels. Meeting one does not establish the others:

Legal permissibility: May the processing take place?

Effectiveness of safeguards: Which risk is actually reduced?

Practical control capability: Can the customer concerned use, verify and enforce the safeguards — and afford them?

Digital sovereignty: Can it maintain its essential digital functions in the event of conflict, disruption or a necessary change of provider?

The Data Protection Trilemma: Accountability without Control

The controller remains accountable under Articles 5(2) and 28 GDPR. In practice, however, it can check a large cloud provider only against audit reports commissioned by the provider itself. Microsoft's Data Protection Addendum, for example, provides for an audit by the customer only as a fallback and at the customer's expense; a contract version for the financial sector published by a Microsoft partner sets, by way of example, 4,000 US dollars per day per expert (contract version of September 2021). The contractual framework thus does not guarantee small contracting authorities — municipalities, schools, associations, SMEs — an economically accessible audit of their own.

Moreover, even an audit of their own could not establish that no disclosure under US law (CLOUD Act, FISA Section 702) has taken place: such orders may be subject to non-disclosure obligations.

> The controller thus bears a residual risk **that it can neither fully verify nor exclude by contract.**

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

With Microsoft 365, the availability of encryption does not automatically close this gap: where it effectively excludes Microsoft from content (Double Key Encryption), core functions such as Office for the web, co-authoring and Copilot are unavailable, and higher-tier licences and a self-operated key service are

required. Other architectures show that protection against the provider and collaboration can be compatible — sovereign alternatives must be measured against precisely this question.

The Cloud and AI Development Act: The Right Question, Open Gaps

With its proposal for CADA (COM(2026) 502), the Commission proposes for the first time a Union-law framework for what counts as a sovereign cloud. Measured against criteria this paper formulated before the proposal, gaps remain that are not addressed in the CADA analyses reviewed:

Level 1 without protection against third-country access: The baseline level rests on self-assessment and contains no obligation to prevent third-country access to customer data.

Sector rather than consistent data orientation: Outside the activities covered, CADA requires no higher level merely because sensitive data are processed. This risks protection gaps precisely for horizontally deployed office, collaboration and identity platforms.

Undefined cost exception: Article 30(4) allows derogations for "disproportionate costs" without defining them — favouring precisely the deepest dependencies.

No demonstrated replaceability: CADA takes provider switching into account, but does not require general practical testing of whether public contracting authorities can actually replace their services.

Small contracting authorities: The framework presupposes an audit capacity they lack.

No additionality requirement: Accelerated permits for data centres require no contribution to additional renewable generation.

Digital and Energy Sovereignty

According to the Upper Austrian grid operator, the planned expansion of Google's data centre in Kronstorf could, at full build-out, consume up to 4.4 TWh of electricity a year — almost a third of Upper Austria's total consumption. Additional electricity demand without corresponding additional renewable generation can deepen fossil import dependencies. Digital sovereignty must not come at the expense of energy sovereignty — irrespective of the operator's origin.

Why Now

The legal basis of transatlantic data transfers is in flux: FISA Section 702 lapsed on 12 June 2026; existing authorisations remain in force until around March 2027, and a lasting arrangement is outstanding. The Data Privacy Framework is under challenge before the Court of Justice (Case C-703/25 P). And CADA is now defining what counts as sovereign in Europe.

What Needs to Be Done

The measures form a system and are addressed to the European Union, the Member States and public contracting authorities. The first four are the core policy decisions; transparency and judgement are the preconditions for them to work.

1. Strengthen CADA

An obligation to prevent third-country access and independent audit from Level 1 onwards; classification also by the data processed — at least Level 2 for office, collaboration, e-mail and identity platforms in public administration; a defined, time-limited cost exception; recognition of third countries only where statutory, independently supervised safeguards exist.

2. Organise Control for Small Contracting Authorities

Jointly funded audits on behalf of all contracting authorities, competence centres to evaluate evidence, joint procurement with audit and exit rights, and publicly understandable audit results.

3. Make Replaceability Measurable

Tested exit plans at every level, publicly funded switching tests for the most widely used services and, in the medium term, a European interoperability certification as a procurement requirement.

→ Freedom of choice exists only where a service can actually be replaced.

4. Tie Data Centres to Additional Renewables

An additionality requirement on the Irish model, hourly and regional matching, storage instead of gas turbines, waste-heat use; accelerated permits only in return for a verifiable contribution to generation, storage and grid compatibility.

5. Create Transparency

Public bodies disclose at which level and on which basis of evidence — self-assessment or audit — they use cloud services; operators of large data centres disclose their electricity and water consumption and the origin of their electricity.

6. Strengthen Digital Judgement

Education that fosters critical thinking is the democratic foundation of all other measures. Those who only memorise cannot judge what AI produces.

Core Message

Digital sovereignty does not mean autarky. It means the freedom to choose whom we trust, on which technologies we build, and under which legal framework our digital future stands.

A safeguard, an audit right or an exit option that the customer concerned can neither use nor verify does not establish sovereignty. And digital sovereignty that comes at the expense of energy sovereignty and the environment is not sovereignty — it is displaced dependency.

Full version with all evidence: Policy Brief No. 2026-001, Version 3 (November 2026), 4future.institute Policy Brief Series, ISSN 3061-1881 (Online). German version prevails:
https://4future.institute/wp-content/uploads/sites/31/2026/11/PB-Digital_Sovereignty_in_Europe-v3.pdf

Contact:

Werner Illsinger (Executive Director) | werneri@4future.institute | +43 664 7996221
4future.institute | Graben 17/10 | 1010 Vienna | Austria | Europe
Part of the 4future.group · independent unit within 4future business GmbH ·
Majority shareholder: 4future.foundation · Disclosure: the author is also CTO of 4future.digital (European cloud and collaboration services), which the paper neither names nor assesses.