Policy Brief – Kurzfassung

Digitale Souveränität in Europa

Befunde und Handlungsoptionen · Policy Brief Nr. 2026-001 (DE), Version 3, November 2026

Die grundlegende digitale Infrastruktur Europas — Cloud, Identität, Kommunikation, KI — wird überwiegend von Plattformen bereitgestellt, die fremden Rechtsordnungen unterliegen und monopolartige Marktstrukturen aufweisen. Sie unterliegt damit konkurrierenden Rechtsansprüchen, deren Folgen europäische Kunden weder vollständig kontrollieren noch zuverlässig ausschließen können. Eine rechtlich zulässige Nutzung beseitigt diese Abhängigkeit nicht.

In zentralen digitalen Funktionen fehlt Europa derzeit die wirksame Kontrolle über wesentliche Abhängigkeiten — rechtlich, technologisch und ökonomisch.

Vier Ebenen: Warum Zulässigkeit nicht reicht

Das Papier unterscheidet vier Ebenen; die Erfüllung der einen belegt nicht die der anderen:

Rechtliche Zulässigkeit: Darf die Verarbeitung stattfinden?

Wirksamkeit von Schutzmaßnahmen: Welches Risiko wird tatsächlich verringert?

Praktische Kontrollfähigkeit: Kann der betroffene Kunde die Maßnahmen nutzen, überprüfen, durchsetzen — und finanzieren?

Digitale Souveränität: Kann er seine wesentlichen digitalen Funktionen auch bei Konflikten, Ausfällen oder einem notwendigen Anbieterwechsel aufrechterhalten?

Das Datenschutz-Trilemma: Rechenschaft ohne Kontrolle

Der Verantwortliche bleibt nach Art. 5 Abs. 2 und Art. 28 DSGVO rechenschaftspflichtig. Einen großen Cloud-Anbieter kann er in der Praxis aber nur anhand von Prüfberichten kontrollieren, die der Anbieter selbst beauftragt. Eine eigene Prüfung sieht etwa das Datenschutz-Addendum von Microsoft nur nachrangig und auf Kosten des Kunden vor; eine von einem Microsoft-Partner veröffentlichte Vertragsfassung für den Finanzsektor setzt dafür beispielhaft 4.000 US-Dollar pro Tag und Fachkraft an (Vertragsstand September 2021). Kleinen Auftraggebern — Gemeinden, Schulen, Vereinen, KMU — gewährleistet das Vertragswerk damit keine wirtschaftlich zugängliche eigene Prüfung.

Selbst eine eigene Prüfung könnte nicht belegen, dass keine Herausgabe nach US-Recht (CLOUD Act, FISA Section 702) erfolgt ist: Solche Anordnungen können mit Verschwiegenheitspflichten verbunden sein.

> Der Verantwortliche trägt damit ein Restrisiko, **das er weder vollständig prüfen noch vertraglich ausschließen kann.**

Wie weit Rechtskonformität und nachweisbarer Schutz auseinanderfallen, zeigt der Bericht des Hessischen Datenschutzbeauftragten zu Microsoft 365 (November 2025): Er hält die vertraglichen Anforderungen für erfüllbar, obwohl Microsoft eine Offenlegung auf Anordnung der US-Regierung nicht vollständig ausschließen kann. Die positive Vertragsbewertung beantwortet die entscheidende Frage des Kunden nicht: Sind meine Daten gegen einen solchen Zugriff tatsächlich geschützt?

Die Verfügbarkeit von Verschlüsselung schließt diese Lücke bei Microsoft 365 nicht automatisch: Schließt sie Microsoft wirksam vom Inhalt aus (Double Key Encryption), fehlen zentrale Funktionen wie Office im Web, gemeinsames Bearbeiten und Copilot; zudem sind höherwertige Lizenzen und ein eigener

Schlüsseldienst nötig. Andere Architekturen zeigen, dass Schutz vor dem Anbieter und Zusammenarbeit vereinbar sein können — souveräne Alternativen sind an genau dieser Frage zu messen.

Der Cloud and AI Development Act: die richtige Frage, offene Lücken

Mit dem Vorschlag für den CADA (COM(2026) 502) schlägt die Kommission erstmals einen unionsrechtlichen Rahmen dafür vor, was als souveräne Cloud gilt. Gemessen an Kriterien, die dieses Papier vor dem Vorschlag formuliert hat, bleiben Lücken, die in den ausgewerteten CADA-Analysen nicht behandelt werden:

Stufe 1 ohne Schutz vor Drittstaatenzugriff: Die Basisstufe beruht auf Selbstbewertung und enthält keine Pflicht, Zugriffe von Drittstaaten auf Kundendaten zu verhindern.

Sektor statt durchgängiger Datenorientierung: Außerhalb der erfassten Tätigkeiten verlangt CADA keine höhere Stufe allein deshalb, weil sensible Daten verarbeitet werden. Dadurch drohen Schutzlücken gerade bei horizontal eingesetzten Büro-, Kollaborations- und Identitätsplattformen.

Undefinierte Kostenausnahme: Art. 30 Abs. 4 erlaubt Abweichungen bei „unverhältnismäßigen Kosten", ohne diese zu definieren — das begünstigt gerade tiefe Abhängigkeiten.

Keine nachgewiesene Ersetzbarkeit: CADA berücksichtigt Anbieterwechsel, verlangt aber keine allgemeine praktische Erprobung, ob öffentliche Auftraggeber ihre Dienste tatsächlich ersetzen können.

Kleine Auftraggeber: Der Rahmen setzt eine Prüffähigkeit voraus, die ihnen fehlt.

Keine Zusätzlichkeitspflicht: Beschleunigte Genehmigungen für Rechenzentren verlangen keinen Beitrag zu zusätzlicher erneuerbarer Erzeugung.

Digitale und energetische Souveränität

Die geplante Erweiterung des Google-Rechenzentrums in Kronstorf könnte laut Netz Oberösterreich im Vollausbau bis zu 4,4 TWh Strom pro Jahr verbrauchen — fast ein Drittel des oberösterreichischen Stromverbrauchs. Zusätzlicher Strombedarf ohne entsprechende zusätzliche erneuerbare Erzeugung kann fossile Importabhängigkeiten vertiefen. Digitale Souveränität darf nicht auf Kosten energetischer Souveränität gehen — unabhängig von der Herkunft des Betreibers.

Warum jetzt

Die Rechtsgrundlage transatlantischer Datentransfers ist in Bewegung: FISA Section 702 ist am 12. Juni 2026 ausgelaufen; bestehende Genehmigungen gelten bis etwa März 2027 fort, eine dauerhafte Neuregelung steht aus. Das Data Privacy Framework ist vor dem Europäischen Gerichtshof angefochten (Rs. C-703/25 P). Und mit dem CADA wird gerade festgelegt, was in Europa als souverän gilt.

Was jetzt zu tun ist

Die Maßnahmen bilden ein System und richten sich an die Europäische Union, die Mitgliedstaaten und die öffentlichen Auftraggeber. Die ersten vier sind die politischen Kernentscheidungen; Transparenz und Urteilsfähigkeit sind die Voraussetzungen, damit sie wirken.

1. Den CADA nachschärfen

Pflicht zur Verhinderung von Drittstaatenzugriffen und unabhängige Prüfung schon auf Stufe 1; Einstufung auch nach den verarbeiteten Daten — mindestens Stufe 2 für Büro-, Kollaborations-, E-Mail- und

Identitätsplattformen der Verwaltung; eine definierte, befristete Kostenausnahme; Anerkennung von Drittstaaten nur bei gesetzlichen, unabhängig beaufsichtigten Schutzvorkehrungen.

2. Kontrolle für kleine Auftraggeber organisieren

Gemeinsam finanzierte Prüfungen im Namen aller öffentlichen Auftraggeber, Kompetenzstellen zur Auswertung von Nachweisen, gemeinsame Beschaffung mit Prüf- und Ausstiegsrechten sowie öffentlich verständliche Prüfergebnisse.

3. Ersetzbarkeit messbar machen

Erprobte Ausstiegspläne auf jeder Stufe, öffentlich finanzierte Wechseltests für die meistgenutzten Dienste und mittelfristig eine europäische Interoperabilitätszertifizierung als Vergabevoraussetzung.

→ Wahlfreiheit gibt es nur, wo sich ein Dienst tatsächlich ersetzen lässt.

4. Rechenzentren an zusätzliche Erneuerbare binden

Zusätzlichkeitspflicht nach irischem Vorbild, stündlicher und regionaler Abgleich, Speicher statt Gasturbinen, Nutzung der Abwärme; beschleunigte Genehmigungen nur gegen einen überprüfbaren Beitrag zu Erzeugung, Speicherung und Netzverträglichkeit.

5. Transparenz herstellen

Öffentliche Stellen legen offen, auf welcher Stufe und auf welcher Nachweisbasis — Selbstbewertung oder Audit — sie Cloud-Dienste nutzen; Betreiber großer Rechenzentren legen Strom- und Wasserverbrauch und die Herkunft ihres Stroms offen.

6. Digitale Urteilsfähigkeit stärken

Bildung, die kritisches Denken fördert, ist die demokratische Grundlage aller anderen Maßnahmen. Wer nur auswendig lernt, kann die Ergebnisse von KI nicht beurteilen.

Kernbotschaft

Digitale Souveränität bedeutet nicht Autarkie. Sie bedeutet die Freiheit zu wählen, wem wir vertrauen, auf welchen Technologien wir aufbauen und unter welchem Rechtsrahmen unsere digitale Zukunft steht.

Eine Schutzmaßnahme, ein Prüfrecht oder eine Ausstiegsmöglichkeit, die der betroffene Kunde weder nutzen noch überprüfen kann, belegt keine Souveränität. Und digitale Souveränität, die auf Kosten energetischer Souveränität und der Umwelt geht, ist keine Souveränität — sie ist eine verlagerte Abhängigkeit.

Ausführliche Fassung mit allen Belegen: Policy Brief Nr. 2026-001, Version 3 (November 2026), 4future.institute Policy Brief Series, ISSN 3061-1881 (Online): https://4future.institute/wp-content/uploads/sites/31/2026/11/PB-Digitale_Souveraenitaet_in_Europa-v3.pdf

Kontakt:

Werner Illsinger (Executive Director) | werneri@4future.institute | +43 664 7996221
4future.institute | Graben 17/10 | 1010 Wien | Österreich | Europa
Teil der 4future.group · unabhängige Einheit in der 4future business GmbH · Mehrheitseigentümerin: 4future.foundation · Offenlegung: Der Autor ist zudem CTO von 4future.digital (europäische Cloud- und Kollaborationsdienste); diese werden im Papier weder genannt noch bewertet.