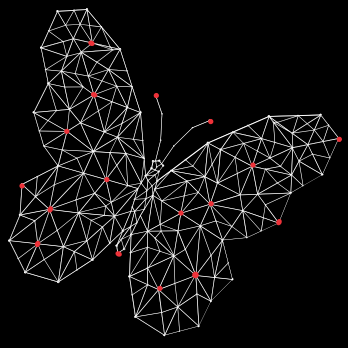
PROJEKTAS
COMPLIANCE ◆ RECHT ◆ PROJEKTE

GRAF FORM

DIGITALE SOUVERÄNITÄT IM IMMOBILIENWESEN

WAS DER US CLOUD ACT ÜBER KONTROLLE, ABHÄNGIGKEITEN UND INFORMATIONSMANAGEMENT OFFENLEGT



Autoren: Nicolas Graf, GRAF FORM GmbH | Anja Schmitz, Projektas GmbH | Version 1.0 | 08.26

Was der US CLOUD Act über die digitale Souveränität der Schweizer Bau- und Immobilienbranche offenlegt

Pläne, Verträge, Gebäudedokumentationen, technische Informationen, Kosten, Modelle und Bewirtschaftungsdaten werden zunehmend auf internationalen Cloud Plattformen gespeichert und verarbeitet. Gleichzeitig erschliessen künstliche Intelligenz und Automatisierung diese Informationen für neue Anwendungen. In dieser Entwicklung taucht ein Begriff immer häufiger auf, der in der Bau- und Immobilienbranche bisher kaum eine Rolle gespielt hat: **Der US CLOUD Act**[1].

Das Gesetz ist allerdings nicht neu. Es wurde bereits 2018 verabschiedet. Neu ist vielmehr die Bedeutung der Systeme, auf die es sich auswirken kann.

Cloud Plattformen sind heute keine ergänzenden Ablagen mehr. Sie bilden zunehmend die Grundlage für Kommunikation, Zusammenarbeit, Dokumentation, Datenmanagement, Automatisierung und künstliche Intelligenz. Damit wächst nicht nur die Menge der dort gespeicherten Informationen, sondern auch die Abhängigkeit von den Anbietern, die diese Plattformen bereitstellen.

Der CLOUD Act ist deshalb weniger ein neues Risiko als ein Anlass, eine längst notwendige Frage zu stellen:

Wie souverän verfügen wir über das digitale Wissen unserer Gebäude und Immobilienportfolios?

Warum ein Gesetz von 2018 gerade jetzt zum Thema wird

Der CLOUD Act, ausgeschrieben «*Clarifying Lawful Overseas Use of Data Act*», ist nicht neu. Neu ist die Rolle der Systeme, auf die er sich auswirken kann.

Im Jahr 2018 wurden Cloud Dienste vielerorts noch als ergänzende Werkzeuge genutzt. Heute bilden sie die Grundlage für Kommunikation, Fachanwendungen, Datenmanagement, Automatisierung und ganze Informationsbestände. Künstliche Intelligenz verstärkt diese Entwicklung zusätzlich, weil Informationen nicht mehr nur gespeichert, sondern analysiert, klassifiziert und miteinander verknüpft werden.

Gleichzeitig werden technologische Abhängigkeiten zunehmend als strategisches und geopolitisches Thema verstanden. Der Bundesrat hat die digitale Souveränität deshalb zu einem Fokusthema der Strategie Digitale Schweiz 2026 erklärt[2]. Auch die Anbieter reagieren mit zusätzlichen Modellen für lokale Betriebsführung, Kontrolle und Geschäftskontinuität[3].

Der CLOUD Act wird heute somit nicht intensiver diskutiert, weil er neu wäre, sondern weil Cloud und künstliche Intelligenz wesentlich tiefer in die Kernprozesse von Staat und Wirtschaft eingreifen als bisher.

[1] US CLOUD Act
[2] Strategie digitale Schweiz
[3] Microsoft Schweiz: How Microsoft is addressing digital sovereignty in Switzerland 25.02.2026

GRAF FORM GMBH | Technoparkstrasse 2 | 8406 Winterthur
grafform.ch | info@grafform.ch | +41 79 526 00 40

PROJEKTAS
COMPLIANCE ◆ RECHT ◆ PROJEKTE

GRAF FORM

Was der US CLOUD Act tatsächlich bedeutet

Für Fachpersonen aus der Bau- und Immobilienbranche ist keine vertiefte juristische Kenntnis des CLOUD Act erforderlich. Einige Grundzüge müssen jedoch verstanden werden, damit die Diskussion weder verharmlost noch unnötig dramatisiert wird.

Kein beliebiger Zugriff auf Cloud Daten

Der CLOUD Act betrifft den Zugang zu elektronischen Beweismitteln im Rahmen strafrechtlicher Ermittlungen und Verfahren. Er gibt US-Strafverfolgungsbehörden keinen pauschalen oder direkten Zugang zu internationalen Cloud-Plattformen. Betroffen sind insbesondere Anbieter elektronischer Kommunikations- und Cloud-Dienste, die der US-Gerichtsbarkeit unterstehen. Eine Herausgabe setzt ein gültiges rechtliches Verfahren voraus. Welche Voraussetzungen gelten, hängt insbesondere von der Art der verlangten Informationen ab.

Die Vorstellung, amerikanische Behörden könnten jederzeit sämtliche in der Schweiz gespeicherten Daten einsehen, ist deshalb falsch. Ebenso falsch wäre jedoch die Annahme, ein Schweizer Speicherort schliesse eine Herausgabe auf der Grundlage ausländischen Rechts grundsätzlich aus.

Der Speicherort ist nicht allein entscheidend

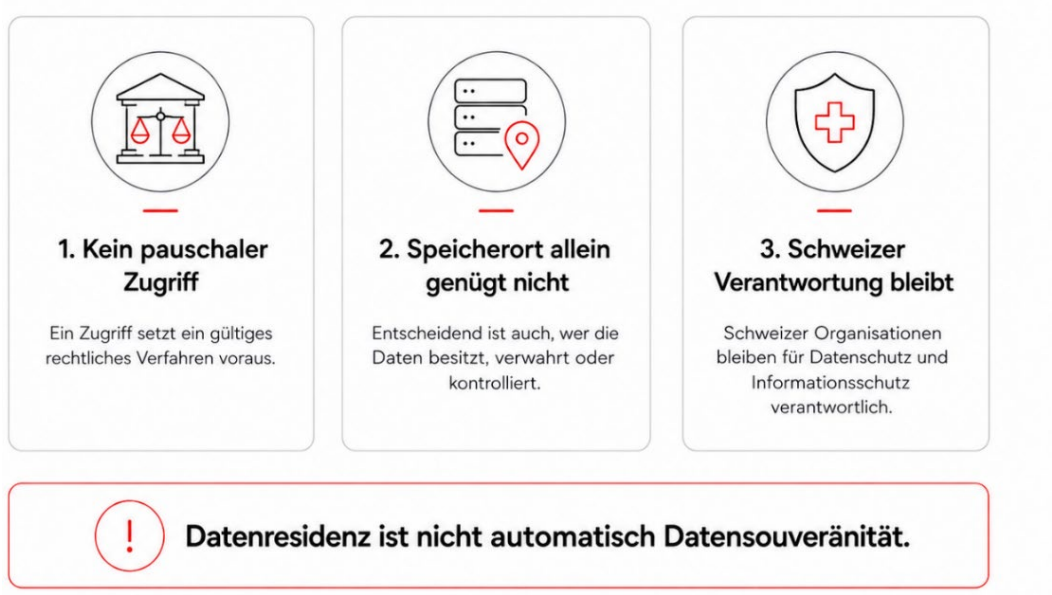
Für den CLOUD Act ist nicht ausschliesslich relevant, in welchem Land ein Server steht. Entscheidend ist auch, ob sich die verlangten Informationen im Besitz, in der Verwahrung oder unter der Kontrolle eines Anbieters befinden, der der amerikanischen Gerichtsbarkeit untersteht.

Ein solcher Anbieter kann deshalb unter bestimmten Voraussetzungen mit einer Herausgabeanordnung für Daten konfrontiert werden, die ausserhalb der USA gespeichert sind. Damit entsteht die für Schweizer Organisationen entscheidende Unterscheidung:

Datenresidenz ist nicht automatisch Datensouveränität

Ein Rechenzentrum in der Schweiz beantwortet die Frage, wo Daten gespeichert werden. Es beantwortet noch nicht vollständig, wer rechtlich und technisch auf sie einwirken kann.

GRAF FORM GMBH | Technoparkstrasse 2 | 8406 Winterthur
grafform.ch | info@grafform.ch | +41 79 526 00 40



Ausländisches Recht wird nicht bedeutungslos

Der CLOUD Act setzt andere Rechtsordnungen nicht einfach ausser Kraft. Anbieter können bestimmte Anordnungen bei Konflikten mit ausländischem Recht anfechten. Ob dies im konkreten Fall möglich und erfolgreich ist, hängt von den jeweiligen Umständen ab.

Für Schweizer Organisationen bleibt gleichzeitig das Schweizer Recht massgebend. Sie bleiben für die rechtmässige Bearbeitung und den Schutz ihrer Daten verantwortlich und müssen insbesondere Auftragsbearbeitung, Datensicherheit, Unterauftragnehmer und mögliche Bekanntgaben ins Ausland beurteilen[4]. Der CLOUD Act ist deshalb kein isoliertes amerikanisches Thema. Er ist Teil einer umfassenderen Betrachtung von Recht, Technik, Organisation und Informationsschutz.

Was hat das mit Gebäuden und Immobilien zu tun?

Ein Gebäude besteht aus Beton, Holz, Stahl, Glas und technischen Anlagen. Für seinen Betrieb ist jedoch zunehmend ein zweites Bauwerk entscheidend:

Sein digitaler Informationsbestand.

Dieser umfasst unter anderem Pläne, Modelle, Verträge, Bewilligungen, Kosteninformationen, technische Dokumentationen, Prüfberichte, Wartungsunterlagen, Flächendaten, Fotos, Zustandsinformationen und Projektdokumentationen. Über Jahrzehnte entsteht daraus ein digitales Gedächtnis des Gebäudes.

Wer dieses Wissen kontrolliert, kann ein Gebäude planen, verändern, betreiben, prüfen, veräussern und langfristig dokumentieren. Fehlen die Informationen oder sind sie in einem nicht mehr verfügbaren

[4] Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB: Outsourcing Auftragsdatenbearbeitung

System eingeschlossen, verliert eine Organisation einen Teil ihrer Handlungsfähigkeit. Dabei besitzt nicht jede Information dasselbe Schutzbedürfnis.

Eine öffentlich verfügbare Produktdokumentation ist anders zu beurteilen als ein Mieterverzeichnis. Ein Wartungshandbuch für ein Bauteil oder eine technische Anlage ist anders zu beurteilen als ein detaillierter Plan der Zutrittskontrolle. Allgemeine Flächeninformationen haben eine andere Sensitivität als Sicherheitskonzepte, Personendaten oder Informationen über kritische technische Anlagen.

Deshalb sollte die erste Frage nicht lauten:

Dürfen wir einen bestimmten Cloud Anbieter verwenden?

Die erste Frage sollte lauten:

Welche Informationen besitzen wir, wie kritisch sind sie und welches Mass an Kontrolle benötigen wir dafür?

Erst danach kann entschieden werden, welche Plattform, welche Betriebsform und welche Schutzmassnahmen angemessen sind.

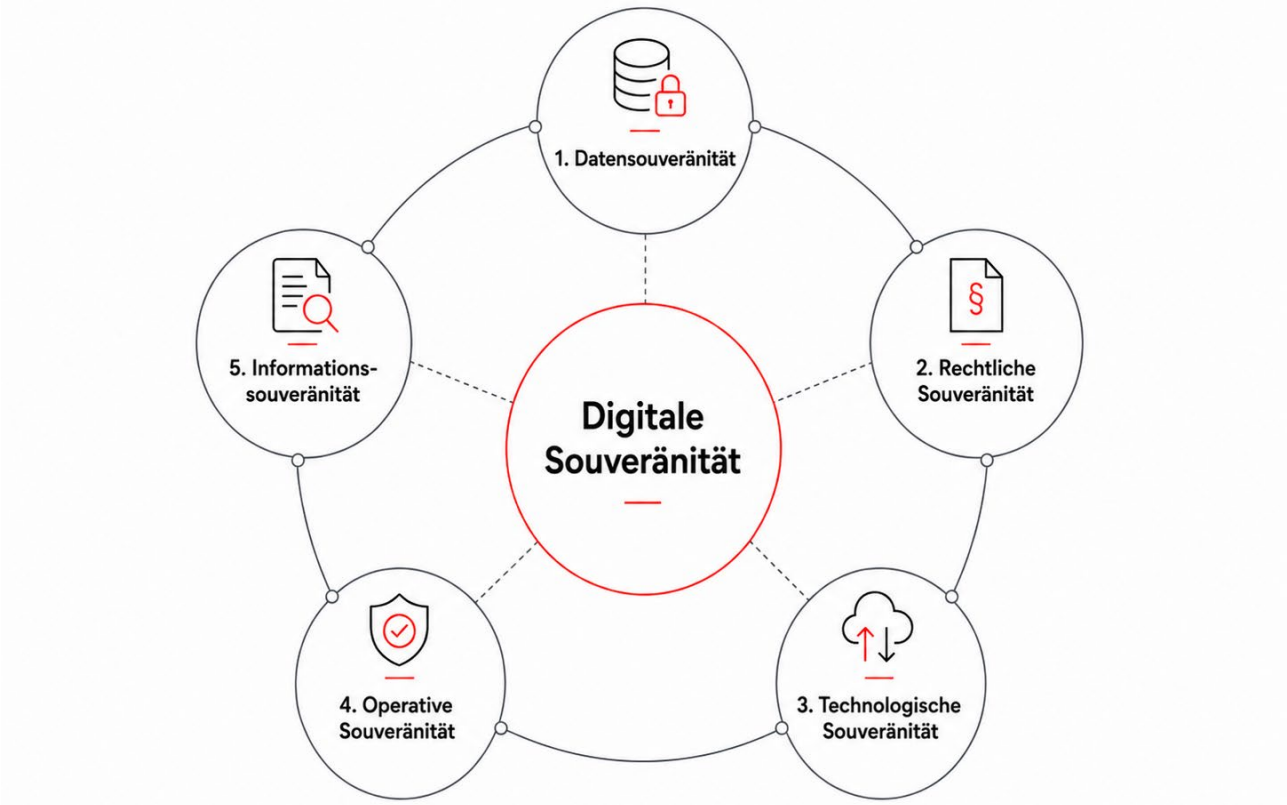
Digitale Souveränität wird häufig mit vollständiger Unabhängigkeit gleichgesetzt. Eine solche Unabhängigkeit ist in der Praxis jedoch kaum erreichbar. Organisationen bleiben von Technologien, Anbietern, Infrastrukturen, Fachwissen und regulatorischen Rahmenbedingungen abhängig.

Souveränität bedeutet deshalb nicht Unabhängigkeit, sondern die bewusste Steuerung von Abhängigkeiten. Entscheidend ist, Risiken, Verantwortlichkeiten und Handlungsoptionen so zu gestalten, dass eine Organisation auch bei veränderten Rahmenbedingungen handlungsfähig bleibt.

Für die Bau- und Immobilienbranche lässt sich diese Handlungsfähigkeit anhand von fünf miteinander verbundenen Ebenen betrachten. Keine einzelne Ebene reicht für sich allein aus.

GRAF FORM GMBH | Technoparkstrasse 2 | 8406 Winterthur
grafform.ch | info@grafform.ch | +41 79 526 00 40

Fünf Ebenen digitaler Souveränität



1. Datensouveränität

Datensouveränität betrifft den Schutz und die zulässige Verwendung der vorhandenen Daten.

Eine Organisation muss wissen, welche Daten sie bearbeitet, wo diese gespeichert und verarbeitet werden, wer darauf zugreifen darf und ob beziehungsweise wo sie ausserhalb der Schweiz bearbeitet oder bekanntgegeben werden. Die Grundlage bildet eine nachvollziehbare Klassifikation der Informationen nach Schutzbedarf.

Als einfache Orientierung kann eine Organisation ihre Informationen beispielsweise in vier Schutzstufen einteilen:

- **Öffentlich**, zur Veröffentlichung oder freien Weitergabe bestimmt
- **Intern**, für Mitarbeitende und definierte Partner zugänglich
- **Vertraulich**, nur für klar berechtigte Personen bestimmt
- **Kritisch**, mit erhöhten Anforderungen an Zugriff, Speicherung, Weitergabe und Wiederherstellung

Die konkreten Bezeichnungen und Kriterien müssen an die Organisation, ihre Aufgaben und die gesetzlichen Anforderungen angepasst werden.

Ohne diese Differenzierung werden entweder sämtliche Daten mit unverhältnismässigem Aufwand geschützt oder besonders kritische Informationen unzureichend behandelt.

2. Rechtliche Souveränität

Rechtliche Souveränität betrifft die Rechtsordnungen und Verpflichtungen, denen eine Organisation, ihre Anbieter und deren Unterauftragnehmer unterstehen.

Dazu gehören das Schweizer Datenschutzrecht, vertragliche Regelungen, Geheimhaltungspflichten, gesetzliche Aufbewahrungsvorgaben, beispielsweise nach dem Obligationenrecht und der Geschäftsbücherverordnung[5] für geschäftsrelevante Unterlagen, sowie mögliche Herausgabepflichten ausländischer Staaten.

Je nach Dokumentart können davon etwa Verträge, Rechnungen, Protokolle oder kaufmännische Projektunterlagen betroffen sein. Nicht jede Gebäudedokumentation untersteht diesen Vorgaben automatisch.

Entscheidend ist, dass die Organisation ihre Verantwortung nicht vollständig an den Plattformanbieter überträgt. Sie muss selbst beurteilen, welche Informationen ausgelagert werden dürfen, welche vertraglichen Garantien erforderlich sind und welches verbleibende Risiko sie akzeptiert.

3. Technologische Souveränität

Technologische Souveränität zeigt sich bei der Frage, ob Informationen aus einem System herausgelöst und in einem anderen System weiterverwendet werden können. Dabei genügt es nicht, lediglich die Dateien herunterladen zu können.

Zu einem nutzbaren Informationsbestand gehören auch Metadaten, Klassifikationen, Versionen, Beziehungen, Berechtigungsinformationen und dokumentierte Strukturen. Sie geben den Dateien ihren fachlichen Kontext.

Ein Ordner mit zehntausend exportierten Dokumenten ist noch kein souverän beherrschter Datenbestand, wenn nicht mehr nachvollziehbar ist, zu welchem Gebäude, Projekt, Fachbereich oder Lebenszyklusabschnitt die einzelnen Informationen gehören.

[5] Art. 958f OR sowie Verordnung über die Führung und Aufbewahrung der Geschäftsbücher, Geschäftsbücherverordnung, GeBüV, SR 221.431

Offene Formate, dokumentierte Schnittstellen, strukturierte Exportmöglichkeiten und ein geprüftes Migrationskonzept sind deshalb wesentliche Bestandteile technologischer Souveränität.

Praxisbeispiel, Verkauf eines Immobilienportfolios

Ein Eigentümer verkauft ein Portfolio mit mehreren Liegenschaften. Die Dokumente lassen sich aus der verwendeten Cloud Plattform exportieren, wesentliche Metadaten, Verknüpfungen und Historien jedoch nur eingeschränkt.

Die Unterlagen sind damit zwar vorhanden, verlieren aber einen Teil ihres fachlichen Zusammenhangs. Die Übergabe an den neuen Eigentümer wird aufwendig, teuer und fehleranfällig. Das Risiko liegt in diesem Fall nicht primär im CLOUD Act, sondern in Defiziten bei der technologischen Souveränität und der Informationssouveränität.

Solche Defizite führen in der Praxis weniger zu einem vollständigen Datenverlust als zu aufwendigen Migrationen, Bereinigungen und Wiederherstellungen. Bei grossen Immobilienportfolios können dadurch hohe Projektkosten entstehen, der laufende Betrieb beeinträchtigt und der fachliche Zusammenhang von Informationen beschädigt werden.

4. Operative Souveränität

Operative Souveränität betrifft die Fähigkeit, auch bei Störungen und Veränderungen handlungsfähig zu bleiben. Was geschieht bei einem längeren Ausfall? Wie wird gearbeitet, wenn ein Dienst vorübergehend nicht verfügbar ist? Was passiert bei einer Vertragsbeendigung, einem Eigentümerwechsel oder einer strategischen Neuausrichtung des Anbieters?

Datensicherungen allein beantworten diese Fragen nicht.

Eine Organisation benötigt auch ein Verständnis dafür, wie zentrale Prozesse weitergeführt, Informationen wiederhergestellt und Systeme ersetzt werden können. Dazu gehören Verantwortlichkeiten, Notfallverfahren, Ausstiegsszenarien und die regelmässige Prüfung der Wiederherstellbarkeit.

Operative Souveränität setzt deshalb dokumentierte Notfallszenarien, Wiederherstellungsverfahren und Ausstiegskonzepte voraus.

5. Informationssouveränität

Informationssouveränität betrifft die fachliche Beherrschung des eigenen Wissens.
Weiss die Organisation, welche Dokumente und Daten vorhanden sind? Sind Begriffe, Dokumenttypen und Metadaten einheitlich definiert? Sind Verantwortlichkeiten, Lebenszyklen, Aufbewahrungsfristen und Archivierungsanforderungen geklärt?

Daten werden erst durch Kontext zu nutzbaren Informationen.

Ein Plan ist nicht allein deshalb verständlich, weil er als PDF oder Modell vorliegt. Seine Bedeutung entsteht durch den Bezug zu einem Gebäude, einer Anlage, einem Projekt, einer Phase, einem Fachbereich und einem Dokumenttyp. Informationssouveränität unterscheidet sich damit von der Datensouveränität. Die Datensouveränität betrifft Schutz, Zugriff und zulässige Verwendung des Bestands. Die Informationssouveränität stellt sicher, dass dieser Bestand verstanden und langfristig genutzt werden kann.

Gerade für die Bau- und Immobilienbranche ist diese Ebene zentral. Bauwerksinformationen müssen häufig über Jahrzehnte verfügbar bleiben. Die heute eingesetzte Plattform wird jedoch kaum über denselben Zeitraum unverändert bestehen. Ein Informationsmodell muss deshalb länger leben können als das System, in dem es aktuell umgesetzt ist.

PROJEKTAS
COMPLIANCE ◆ RECHT ◆ PROJEKTE

GRAF FORM

Ein Gedankenexperiment

Nehmen wir zwei Immobilienorganisationen.

Organisation A betreibt ihre Ablage auf eigener Infrastruktur in der Schweiz. Die Dokumente liegen jedoch in unstrukturierten Ordnern, Metadaten fehlen und ein strukturierter Export ist kaum möglich.
Organisation B nutzt eine internationale Cloud Plattform. Ihre Informationen werden nach einem dokumentierten Datenmodell verwaltet und können strukturiert exportiert werden.
Welche Organisation ist souveräner?

Keine der beiden Organisationen ist automatisch souverän. Organisation A kontrolliert ihre Infrastruktur, Organisation B beherrscht ihre Informationen besser. Digitale Souveränität entsteht erst, wenn Abhängigkeiten auf allen fünf Ebenen gemeinsam gesteuert werden.

Welche Risiken prägen die Praxis?

Die folgende Gegenüberstellung ist eine qualitative Einordnung und keine statistische Risikobewertung.

Im Alltag häufiger sichtbar	**Seltener, aber potenziell weitreichend**
Unstrukturierte Dokumentation	Herausgabeanordnungen nach dem CLOUD Act
Wissensverlust	Geopolitische Eingriffe
Plattformabhängigkeit	Regulatorische Sonderfälle

Die öffentliche Diskussion konzentriert sich häufig auf geopolitische und rechtliche Szenarien. Operative und wirtschaftliche Schäden entstehen im Alltag jedoch oft durch unzureichend strukturierte Informationen, fehlende Dokumentationsstandards oder starke Plattformabhängigkeiten.
Eine Souveränitätsstrategie muss deshalb beide Risikogruppen berücksichtigen.

Die Konsequenz für Bauherren und Immobilieneigentümer

Die Diskussion über den CLOUD Act sollte nicht mit der Auswahl eines Produktes beginnen.
Sie sollte mit dem eigenen Informationsbestand beginnen.

Bauherren und Immobilieneigentümer müssen zuerst verstehen, welche Informationen sie über ihre Gebäude und Portfolios besitzen, wie diese genutzt werden, wie lange sie erhalten bleiben müssen und welche Schutzbedürfnisse bestehen.

Darauf aufbauend lässt sich festlegen, welche rechtlichen, technischen und organisatorischen Anforderungen eine Plattform erfüllen muss.

Für allgemeine Projektdokumentationen kann eine etablierte Public Cloud eine angemessene Lösung sein. Besonders sensible Informationen können zusätzliche Zugriffsbeschränkungen, getrennte Ablagen, kundenseitig kontrollierte Verschlüsselungsschlüssel oder lokal betriebene Umgebungen erfordern. Bei hochkritischen Informationen kann eine vollständige Auslagerung ungeeignet sein.

- Es braucht deshalb keine pauschale Entscheidung zwischen Cloud und eigener Infrastruktur.
- Es braucht eine bewusste Architektur, die unterschiedliche Informationsklassen angemessen behandelt.

Auch neue Angebote unter dem Begriff «Sovereign Cloud» lösen diese Aufgabe nicht automatisch. Sie können zusätzliche Kontrolle über Betrieb, Datenresidenz, Schlüssel und administrative Zugriffe ermöglichen. Welche dieser Funktionen tatsächlich erforderlich sind, lässt sich jedoch erst beurteilen, wenn der Schutzbedarf und die Abhängigkeiten der eigenen Organisation bekannt sind.

Digitale Souveränität beginnt vor der Plattformentscheidung

Der US CLOUD Act schafft berechtigte Fragen. Er rechtfertigt jedoch weder eine pauschale Ablehnung amerikanischer Cloud Anbieter noch die Annahme, ein Schweizer Rechenzentrum löse sämtliche Probleme.

Seine eigentliche Bedeutung für die Bau- und Immobilienbranche liegt an einem anderen Ort.

Er macht sichtbar, dass das Wissen über Gebäude und Immobilienportfolios zunehmend auf Plattformen liegt, deren rechtliche, technische und operative Rahmenbedingungen von den verantwortlichen Organisationen nicht vollständig bestimmt werden können.

Darauf sollte die Branche nicht mit Angst, sondern mit besserem Informationsmanagement reagieren. Organisationen müssen ihre Informationen kennen, klassifizieren, schützen, strukturieren, exportieren und unabhängig von einer einzelnen Benutzeroberfläche weiterverwenden können.

GRAF FORM GMBH | Technoparkstrasse 2 | 8406 Winterthur
grafform.ch | info@grafform.ch | +41 79 526 00 40

Die entscheidende Frage lautet deshalb nicht nur:

Wo liegen unsere Gebäudedaten?

Sondern:

Können wir auch dann noch über unser Immobilienwissen verfügen, wenn sich Anbieter, Technologien oder rechtliche Rahmenbedingungen verändern?

Digitale Souveränität beginnt nicht im Rechenzentrum. Sie beginnt mit der Beherrschung der eigenen Informationen.

GRAF FORM GMBH | Technoparkstrasse 2 | 8406 Winterthur
grafform.ch | info@grafform.ch | +41 79 526 00 40

GRAF FORM

Gemeinsame Publikation von

GRAF FORM GmbH

Technoparkstrasse 2
8406 Winterthur

www.grafform.ch

und

Projektas GmbH

Baarerstrasse 75
6300 Zug

www.projektas.ch

GREIFBARE DIGITALE TRANSFORMATION

Datum 08.2026