

LEARNING NUGGET DIGITALE SOUVERÄNITÄT 8. SEPTEMBER 2026

Gespeichert in der Schweiz ist nur die halbe Antwort

Warum bei Cloud-Diensten nicht nur der Speicherort zählt, was der US CLOUD Act und die privatim-Resolution vom November 2025 dazu sagen und welche drei Fragen du vor dem nächsten Tool stellen kannst.

Von Rico Eberle, E-Learning-Experte für Weiterbildung und Gemeinderat in Dübendorf

RICO EBERLE · DIGITALE SOUVERÄNITÄT

Gespeichert in der Schweiz.

Sagt der Anbieter.



Video zum Beitrag

Dieses Learning Nugget gibt es als Video mit Transkript (1:28 Min.). QR-Code scannen oder Link öffnen:

ricoeberle.ch/blog/wo-liegen-deine-daten/

«Gespeichert in der Schweiz» ist ein Satz, den Schulen und Verwaltungen oft hören, wenn sie einen Cloud-Dienst prüfen. Er beantwortet eine wichtige Frage. Aber nicht die einzige.

Speicherort und Rechtsraum

Bei Daten in der Cloud lohnt es sich, zwei Fragen auseinanderzuhalten. Der **Speicherort** sagt, wo die Server physisch stehen. Der **Rechtsraum** sagt, welchem Recht das Unternehmen untersteht, das den Dienst betreibt.

Die beiden Antworten können auseinanderfallen. Ein Rechenzentrum kann in Zürich stehen und trotzdem von einem Konzern mit Sitz in den USA betrieben werden. Solche Angebote gibt es: Microsoft hat im Dezember 2019 Office 365 mit Datenhaltung in Schweizer Rechenzentren lanciert. Die Ankündigung spricht von ruhenden Kundendaten und nennt Exchange Online, SharePoint Online, OneDrive for Business und Teams, nicht alle Dienste.

Was der CLOUD Act regelt

Der CLOUD Act wurde im März 2018 in den USA unterzeichnet. Er hat einen neuen Paragraphen ins US-Recht eingefügt, 18 U.S.C. § 2713. Danach müssen Anbieter Daten herausgeben, die sie besitzen, verwahren oder kontrollieren, unabhängig davon, ob diese Daten in den USA oder im Ausland liegen. Das gilt für Ermittlungen der Strafverfolgung.

BEISPIEL

CLOUD Act

US-Gesetz seit 2018 · Herausgabe bei Ermittlungen, auch für Daten im Ausland

Konzernsitz USA

Rechenzentrum Zürich

Zugriff

Der CLOUD Act kann auch Daten in einem Schweizer Rechenzentrum erfassen, wenn der Anbieter US-Recht untersteht.

Die Schweizer Datenschutzbeauftragten weisen in ihrer Resolution darauf hin, dass eine solche Herausgabe ohne die Regeln der internationalen Rechtshilfe erfolgen kann. Für die Frage, wer auf Daten zugreifen kann, zählt also auch der Sitz des Anbieters.

Was privatim im November 2025 festgehalten hat

privatim ist die Konferenz der schweizerischen Datenschutzbeauftragten. Dazu gehören die kantonalen Beauftragten, der EDÖB und mehrere Städte. Am 18. November 2025 hat die Konferenz eine Resolution verabschiedet, publiziert am 24. November.

PRIVATIM · NOVEMBER 2025

Besonders schützenswerte Personendaten von Behörden und öffentlichen Schulen gehören in der Regel nicht in Cloud-Software grosser internationaler Anbieter.

🔑 **Ausnahme: Die Behörde verschlüsselt selbst und hält den Schlüssel.**



Die Kernaussage der privatim-Resolution vom November 2025, sinngemäss und kein wörtliches Zitat. Die Resolution spricht von öffentlichen Organen; die öffentlichen Schulen habe ich ergänzt, weil sie dazu gehören.

Der Kern in den Worten der Resolution: Wenn öffentliche Organe besonders schützenswerte oder geheimhaltungspflichtige Personendaten in Cloud-Software grosser internationaler Anbieter auslagern, ist das in den meisten Fällen unzulässig. Als Beispiel nennt die Resolution Microsoft 365. Möglich bleibt es, wenn die Behörde die Daten selbst verschlüsselt und der Anbieter keinen Zugang zum Schlüssel hat.

Zur Einordnung:

- Die Resolution ist eine Einschätzung der Aufsichtsbehörden, kein Gesetz. Der Kanton Thurgau liest sie vorsichtiger: nicht zwingend in jedem Fall.
- Schulen werden in der Resolution nicht ausdrücklich genannt. Im Video und auf der Folie ist das meine Übertragung: Öffentliche Schulen sind öffentliche Organe und damit erfasst, private Schulen nicht. Die Aussage im Video ist deshalb eine sinngemässe Zusammenfassung, kein wörtliches Zitat.
- Es geht um Cloud-Software grosser Anbieter, nicht um jeden internationalen Cloud-Dienst.
- Der Kanton Glarus hat sich der Resolution nicht angeschlossen.

Drei Fragen vor dem nächsten Tool

- 1. Wo liegen die Daten?** Gilt die Zusage für alle Funktionen oder nur für einen Teil der Daten?
- 2. Welchem Recht untersteht der Anbieter?** Wo haben der Betreiber und sein Mutterkonzern ihren Sitz?
- 3. Wer hält den Schlüssel?** Verschlüsselt deine Organisation selbst, oder verwaltet der Anbieter die Schlüssel?

Hilfreich ist eine vierte Frage vorab: Um welche Daten geht es überhaupt? Für eine Linkliste gelten andere Massstäbe als für Förderberichte oder Gesundheitsangaben.

Meine Sicht

Speicherort ist Geografie. Rechtsraum ist Politik. Darum gehören vor jedes neue Tool die drei Fragen von oben: Wo liegen die Daten? Welchem Recht untersteht der Anbieter? Und wer hält den Schlüssel?

Speicherort ist Geografie.
Rechtsraum ist Politik.



Wo die Server stehen, sagt noch nicht, welches Recht gilt.

Und bei dir?

Wer hält bei deiner Organisation den Schlüssel?

Häufige Fragen

Schützt ein Speicherort in der Schweiz vor dem US CLOUD Act?

Nicht allein. Der CLOUD Act verpflichtet Anbieter bei Ermittlungen der US-Strafverfolgung, Daten herauszugeben, die sie besitzen, verwahren oder kontrollieren, unabhängig davon, ob die Daten in den USA oder im Ausland liegen. Für den Zugriff zählt also auch, welchem Recht der Anbieter untersteht.

Was ist der Unterschied zwischen Speicherort und Rechtsraum?

Der Speicherort sagt, wo die Server physisch stehen, der Rechtsraum, welchem Recht das Unternehmen untersteht, das den Dienst betreibt. Beides kann auseinanderfallen, etwa bei einem Rechenzentrum in Zürich, das ein Konzern mit Sitz in den USA betreibt.

Was hat privatim im November 2025 zu Cloud-Diensten festgehalten?

Laut der Resolution der Konferenz der schweizerischen Datenschutzbeauftragten ist es in den meisten Fällen unzulässig, wenn öffentliche Organe besonders schützenswerte oder geheimhaltungspflichtige Personendaten in Cloud-Software grosser internationaler Anbieter auslagern. Möglich bleibt es, wenn die Behörde selbst verschlüsselt und der Anbieter keinen Zugang zum Schlüssel hat. Die Resolution ist eine Einschätzung der Aufsichtsbehörden, kein Gesetz. Schulen nennt sie nicht ausdrücklich; öffentliche Schulen gehören als öffentliche Organe dazu.

Quellen

1. privatim: Resolution zur Auslagerung von Datenbearbeitungen in die Cloud (18.11.2025, PDF)
https://www.privatim.ch/wp-content/uploads/2025/11/20251124_privatim_Resolution-Hyperscaler_DE.pdf
2. privatim: Medienmitteilung zur Resolution zu internationalen Cloud-Lösungen (24.11.2025)
<https://www.privatim.ch/de/privatim-verabschiedet-resolution-zu-internationalen-cloud-losungen/>
3. Congressional Research Service: CLOUD Act, R45173
<https://www.congress.gov/crs-product/R45173>
4. Datenschutzbeauftragte Kanton Thurgau: Einordnung der privatim-Resolution
<https://www.datenschutz-tg.ch/ds/resolution-privatim-auslagerung-datenbearbeitung.html>
5. Microsoft Schweiz: Office 365 hat jetzt den Schweizer Pass (10.12.2019)
<https://news.microsoft.com/de-ch/2019/12/10/office-365-hat-jetzt-den-schweizer-pass/>



ÜBER DEN AUTOR

Rico Eberle

Rico Eberle ist E-Learning-Experte, Betriebsökonom FH und Gemeinderat in Dübendorf. Er präsidiert den Stiftungsrat der Stiftung Weiterbildungskurse Dübendorf (WBK). In den Learning Nuggets erklärt er Forschung zu Lernen, KI und digitaler Souveränität kurz und mit Quellen.

Kontakt: ricoeberle.ch · LinkedIn: linkedin.com/in/rico-eberle

LIZENZ

Text, Transkript und Video von Rico Eberle stehen unter der Lizenz CC BY 4.0 (ausgenommen Musik und Soundeffekte des Videos). Du darfst die Inhalte teilen und bearbeiten, auch im Unterricht, wenn du die Quelle nennst.
creativecommons.org/licenses/by/4.0/deed.de

ZITIERVORSCHLAG

«Gespeichert in der Schweiz ist nur die halbe Antwort», Rico Eberle, ricoeberle.ch, 2026, <https://ricoeberle.ch/blog/wo-liegen-deine-daten/>, CC BY 4.0