BÄR & KARRER BRIEFING APRIL 2026

CLOUD-NUTZUNG UND DIGITALE SOUVERÄNITÄT: HANDLUNGSOPTIONEN FÜR SCHWEIZER BEHÖRDEN

Cloud-Dienste sind ein fester Bestandteil moderner Verwaltungsarbeit. Gleichzeitig sind bei der Auslagerung von Datenbearbeitungen durch Bundes-, Kantons- und Gemeindebehörden die Vorgaben des Datenschutzes, Geheimhaltungsverpflichtungen wie das Amtsgeheimnis sowie die Vorschriften der Informationssicherheit einzuhalten und die langfristige Handlungsfähigkeit zu sicherzustellen. In der öffentlichen Diskussion, die durch aktuelle politische Entwicklungen in den USA zusätzlichen Auftrieb erhalten hat, steht derzeit die Nutzung von US-Cloud-Diensten durch Schweizer Behörden im Kontext digitaler Souveränität[1] im Fokus.[2] Diese Debatte wurde durch die im November 2025 veröffentlichte Resolution von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten, akzentuiert, die sich als *De-facto*-Verbot der Nutzung von Hyperscalern in der öffentlichen Verwaltung lesen lässt. Auch im Beschaffungswesen wird diese Stossrichtung punktuell bereits konkret: So verlangt etwa die Ausschreibung des BAG zur SwissHDS-Infrastruktur (Februar 2026), dass sämtliche Infrastrukturkomponenten keine technische oder rechtliche Abhängigkeit von äusseren Jurisdiktionen (z.B. US CLOUD Act) aufweisen dürfen.

Digitale Souveränität von Schweizer Behörden bedeutet weder Autarkie noch Abschottung, sondern die Fähigkeit, den Einsatz externer digitaler Leistungen eigenverantwortlich zu steuern und zu kontrollieren. Dieses Briefing ordnet die vorgebrachten Argumente ein, macht Spannungsfelder sichtbar und bietet Orientierung für die Cloud-Nutzung in der Verwaltung. Die Analyse zeigt, dass es keine vollumfänglich risikofreien Lösungen gibt: Jede Variante – sei es ein US-Cloud-Dienst, ein schweizerischer oder ein europäischer Anbieter, eine On-Premises- oder eine Open-Source-Lösung – erfordert einzelfallbezogene Abwägungen zwischen Funktionalität, Sicherheit, Souveränität und Betriebsaufwand.

[1] Der Bundesrat versteht unter digitaler Souveränität die für die Erfüllung staatlicher Aufgaben im digitalen Raum erforderliche Kontroll- und Handlungsfähigkeit (Bericht «Digitale Souveränität der Schweiz» vom 26.11.2025, S. 6).

[2] Die Vereinbarkeit der Cloud-Nutzung mit dem Amtsgeheimnis (Art. 320 StGB) und datenschutzrechtlichen Pflichten ist weitgehend geklärt: Cloud-Anbieter können als Hilfspersonen der Behörde in die staatliche Aufgabenerfüllung eingebunden werden, sofern sie sorgfältig ausgewählt, instruiert und überwacht werden. Damit unterstehen sie selbst dem Amtsgeheimnis. Datenschutzrechtlich ist die Auslagerung an einen Cloud-Anbieter als Auftragsbearbeitung unter den Voraussetzungen von Art. 9 DSG zulässig. Auf diese beiden Aspekte wird im vorliegenden Briefing nicht weiter eingegangen.

A. KERNAUSSAGEN

- **Digitale Souveränität** bedeutet weder Autarkie noch Abschottung, sondern die Fähigkeit von Behörden, den Einsatz externer digitaler Leistungen eigenverantwortlich zu steuern und zu kontrollieren.
- Der **US CLOUD Act** begründet **kein direktes Zugriffsrecht** von US-Behörden auf im Ausland gespeicherte Daten. Herausgabeanordnungen erfordern einen richterlichen Beschluss, hinreichenden Tatverdacht und einen konkreten Strafverfolgungszweck. Zusätzlich begrenzen rechtsstaatliche Schranken ihre Reichweite.
- **Herausgabeanordnungen** unter dem US CLOUD Act dienen primär der Ermittlung bei **schwerer Kriminalität** (wie Terrorismus, Cyberkriminalität). Gewöhnliche Verwaltungsdaten wie Projektunterlagen, Statistiken oder Personalakten stehen typischerweise nicht im Fokus von US-Ermittlungen.
- Die **Transparenzberichte** der US-Hyperscaler bestätigen dies: **Offenlegungen von Inhaltsdaten ausländischer** Enterprise-Kunden gegenüber US-Strafverfolgungsbehörden sind **äusserst selten** (bei Microsoft 0,008 % aller Anfragen). Für Kunden aus dem öffentlichen Sektor sind bislang keine Fälle bekannt (Stand: April 2026).
- Auch **EU-/CH-Cloud-Anbieter** garantieren **keine vollständige Risikofreiheit**. Subprozessoren, globale Lieferketten oder Notfall-Failover in Drittstaaten können mittelbar extraterritoriale Zugriffsrechte auslösen. Zudem bestehen häufig operative Einschränkungen bei Portfolio, Skalierbarkeit, Support und Zertifizierungstiefe, was zusätzlichen Integrations- und Prüfaufwand verursachen kann.
- **Open-Source- und On-Premises-Lösungen** verlagern die gesamte Sicherheits- und Betriebsverantwortung auf die Behörde und sind mit erheblichen Kosten sowie spezifischen Cyberrisiken verbunden. Open-Source-Projekte unterliegen zudem sanktionsbezogenen Risiken und Supply-Chain-Risiken. On-Premises-Lösungen bieten zwar physische Kontrolle, sind aber in Skalierbarkeit und Ausfallsicherheit eingeschränkt.
- **Im Ergebnis** erfordert daher jedes (Cloud-)Vorhaben eine **Risikoanalyse**, unabhängig davon, ob ein US-, EU- oder CH-Anbieter, eine Open-Source- oder On-Premises-Lösung gewählt wird. Auf dieser Grundlage hat die Behörde einen **risikobasierten Entscheid** darüber zu treffen, ob die verbleibenden Restrisiken tragbar sind und das Vorhaben freigegeben werden kann.

B. US CLOUD ACT: REICHWEITE, SCHRANKEN UND PRAKTISCHE RELEVANZ FÜR SCHWEIZER BEHÖRDEN

I. RECHTLICHE EINORDNUNG: BEDEUTUNG DES CLOUD ACT

Der im März 2018 in Kraft getretene CLOUD Act konkretisiert den *Stored Communications Act* (SCA) und stellt klar, dass US-Behörden bei Ermittlungen im Zusammenhang mit schwerwiegenden Straftaten, wie Terrorismus, Gewaltkriminalität, sexueller Ausbeutung von Kindern und Cyberkriminalität auf der Grundlage eines Gerichtsbeschlusses (*Warrant*), einer Vorladung (*Subpoena*) oder eines Gerichtsbefehls (*Court Order*) die Herausgabe von Kommunikationsdaten verlangen können, die von einem dem CLOUD Act unterliegenden Anbieter gespeichert oder bearbeitet werden, auch wenn diese Daten auf Servern ausserhalb der USA gespeichert sind. Der Zweck des CLOUD Act besteht also insbesondere darin, Ermittlungen zu schweren Straftaten zu unterstützen.

Der persönliche Anwendungsbereich des CLOUD Act ist weit gefasst: Er erfasst sämtliche Anbieter von elektronischen Kommunikationsdiensten (*electronic communication services*) oder Remote-Computing-Diensten (*remote computing services*), die in den USA ansässig sind, dort eine Niederlassung haben oder in den USA einer Geschäftstätigkeit nachgehen.

Entscheidend für die Anwendbarkeit ist das US-Rechtsverständnis von "*possession, custody, or control*". Danach genügt bereits die faktische oder rechtliche Kontrolle über Daten durch einen Provider, selbst wenn diese auf Rechenzentren in der Schweiz oder Europa gespeichert sind. Der CLOUD Act begründet damit extraterritoriale Herausgabepflichten, die potenziell im Widerspruch zu schweizerischen Rechtsgarantien (wie Amts- und Rechtshilfe) stehen können.

Da der CLOUD Act im Vordergrund der aktuellen Diskussion steht, fokussiert sich dieses Briefing auf den CLOUD Act. Davon zu unterscheiden ist Section 702 des *Foreign Intelligence Surveillance Act* (FISA), der US-Geheimdienstbehörden die programmgesteuerte Erhebung von Auslandsnachrichtendaten ermöglicht. Anders als beim CLOUD Act ist keine individuelle richterliche Anordnung erforderlich. Die Zugriffsbefugnis basiert auf einem vom *Foreign Intelligence Surveillance Court* genehmigten Programmrahmen, der US-Provider zur Mitwirkung verpflichtet.

II. KEIN FREIFAHRTSCHEIN: DIE RECHTSSTAATLICHEN GRENZEN DES CLOUD ACT

Trotz der Risiken einer Herausgabeanordnung ist ein pauschales Infragestellen oder ein generelles Verbot der Nutzung von US-Cloud-Diensten durch schweizerische Behörden nicht sachgerecht. Entscheidend ist bei der Bewertung der Risiken nicht allein die theoretische Reichweite der US-Gesetze, sondern insbesondere die bestehenden rechtlichen Hürden, die Herausgabebegehren auf Daten begrenzen und kontrollieren, die Schweizer Behörden speichern, sowie die praktische Wahrscheinlichkeit, dass US-Behörden tatsächlich auf diese Daten zugreifen.

Dabei stehen den formalen Herausgabeanordnungen des CLOUD Act verschiedene rechtsstaatliche Schranken und Verfahrensgarantien gegenüber, die Herausgabebegehren begrenzen und strukturieren. So sind Daten nur auf Grundlage eines gerichtlichen US-Beschlusses herauszugeben, wenn sie für eine laufende strafrechtliche Untersuchung in den USA relevant sind. Für den Erlass eines solchen Beschlusses muss ein hinreichender Verdacht ("*probable cause*") auf eine konkrete Straftat bestehen, und die angeforderten Daten müssen konkret zur Aufklärung oder Verfolgung dieser Straftat beitragen. Eine allgemeine, pauschale oder lediglich interessengeleitete Datenanforderung genügt den Anforderungen des CLOUD Act nicht.

Der CLOUD Act sieht zudem nicht vor, dass Daten automatisch herausgegeben werden müssen. Vielmehr eröffnet der Gesetzestext ausdrücklich die Möglichkeit, eine gerichtliche Anordnung anzufechten oder modifizieren zu lassen, wenn ein Anbieter, der in den Anwendungsbereich des CLOUD Act fällt, begründete Bedenken hat, dass die Herausgabe gegen das Recht eines anderen Staates verstösst. Diese sogenannte *comity analysis* erfordert, dass ein US-Gericht bei entsprechenden Einwänden prüft, ob eine Herausgabepflicht den Gesetzen des betroffenen ausländischen Rechts widerspricht, und bei Vorliegen bestimmter Voraussetzungen den Prozess anpasst oder sogar aufhebt. In der Praxis bedeutet dies, dass Anordnungen, die nicht den gesetzlichen Anforderungen genügen, nicht automatisch umgesetzt werden, sondern einem Prüfprozess unterliegen, wodurch die theoretische Reichweite des CLOUD Act durch rechtsstaatliche Hürden erheblich relativiert wird.

Schliesslich verhindert der CLOUD Act nicht generell, dass Cloud-Anbieter betroffene Kunden über die Herausgabe ihrer Daten informieren. In bestimmten Fällen kann jedoch eine behördliche oder gerichtliche Anordnung eine Benachrichtigung einschränken oder vorübergehend untersagen (*gag orders*), wobei solche Massnahmen zu begründen und umfangmässig sowie zeitlich einzuschränken sind.

III. TRANSPARENZBERICHTE DER US-CLOUD-ANBIETER: HERAUSGABEN ALS SELTENE AUSNAHME

Entscheidend ist auch die seit 2018 gesammelte praktische Erfahrung mit entsprechenden Anfragen. Die Transparenzberichte grosser US-Cloud-Anbieter zeigen, dass tatsächliche Herausgaben von Daten im Zusammenhang mit Enterprise-Kunden selten sind.

Bei Microsoft[3] betrafen im ersten Halbjahr 2025 (wie bereits in den Vorjahren[4]) weniger als 0.7 % der weltweiten Anfragen von Strafverfolgungsbehörden überhaupt Enterprise-Kunden. In der Mehrzahl der Fälle wurden diese Anfragen abgelehnt, zurückgezogen oder so umgeleitet, dass die Behörden direkt beim Kunden anfragen mussten. Soweit Unternehmenskundendaten übermittelt wurden, entfiel der Grossteil auf Nicht-Inhaltsdaten (z.B. Basis-Teilnehmerinformationen oder IP-Logs), während Inhaltsdaten nur in einer Minderheit der Fälle offengelegt wurden. Grenzüberschreitende Offenlegungen von Inhaltsdaten blieben weiterhin selten: Microsoft übermittelte in fünf Fällen Inhaltsdaten an US-Behörden zu Nicht-US-Enterprise-Kunden, deren Daten ausserhalb der USA gespeichert waren. Nur in einem dieser Fälle war ein Kunde mit Sitz in der EU betroffen, wobei es sich um einen Auftragnehmer der US-Regierung handelte.

Setzt man dies in Relation zur Gesamtzahl der seit Inkrafttreten des CLOUD Act bei Microsoft eingegangenen Anfragen, wird das Ausmass der Seltenheit der auf dem CLOUD Act basierenden Anfragen noch greifbarer: Offenlegungen von Inhaltsdaten ausländischer Enterprise-Kunden gegenüber US-Strafverfolgungsbehörden machten lediglich 0.008 % aller weltweiten Anfragen aus.[5] Laut Angaben von Microsoft waren in keinem dieser seltenen Fälle Behörden oder staatliche Institutionen betroffen.[6]

Amazon Web Services (AWS) gibt an, seit Beginn der Erfassung keine Daten von Unternehmenskunden oder Behörden, die sich ausserhalb der USA befinden, aufgrund von CLOUD Act Anordnungen offengelegt zu haben,[7] und verfolgt eine Praxis, bei der Anfragen – soweit möglich – zunächst an den Kunden selbst adressiert werden. Diese Praxis reflektiert, dass eine

[3] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MSFT-GRR-Enterprise-One-Pager-H1-2025.pdf
[4] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MSFT-GRR-Enterprise-One-Pager-H2-2024.pdf
[5] https://news.microsoft.com/source/emea/2026/02/how-microsoft-is-addressing-digital-sovereignty-in-switzerland/
[6] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/CLOUD-Act-What-it-is-and-is-not.pdf
[7] https://d1.awsstatic.com/onedam/marketing-channels/website/aws/en_US/whitepapers/compliance/Amazon_AWS_Information_Request_Report_H2_2025.pdf

Herausgabepflicht nur besteht, wenn eine rechtlich gültige, bindende Anordnung vorliegt, und nicht automatisch bei jedem Herausgabebegehren. Zudem stellt AWS ausdrücklich klar, dass weder der US-Regierung noch einer anderen Regierung ein uneingeschränkter oder automatischer Zugang zu Kundendaten gewährt wird – einschliesslich auf die in der Cloud gespeicherten Daten.[8]

IV. GERINGE BETROFFENHEIT TYPISCHER VERWALTUNGSDATEN VON CLOUD ACT-ANORDNUNGEN

Der CLOUD Act beschränkt die Kategorien herausverlangbarer Daten grundsätzlich nicht – erfasst sind potenziell alle bei einem dem CLOUD Act unterliegenden Anbieter gespeicherten Daten, unabhängig vom Speicherort. Der erklärte Zweck des Gesetzes besteht dabei aber wie erwähnt darin, den Zugang zu elektronischen Kommunikationen im Rahmen von Ermittlungen bei schwerer Kriminalität zu ermöglichen, namentlich bei Terrorismus, Gewaltkriminalität, sexueller Ausbeutung von Kindern und Cyberkriminalität. Praktisch konzentrieren sich richterlich genehmigte Herausgabeanordnungen im Rahmen von US-Strafverfahren typischerweise auf Kommunikationsinhalte (E-Mails, Chats, Nachrichten), Metadaten zu Kommunikationen sowie Identitätsdaten, da diese für strafrechtliche Ermittlungen den grössten Beweiswert haben. Kommunikationsdaten sind typischerweise relevant bei der Aufklärung von Absprachen oder Tatplanung und Identitätsdaten zur Zuordnung von Accounts zu realen Personen. Technische Systemdaten, interne Dokumente oder Personalakten dürften demgegenüber nur in spezifischen Ermittlungskontexten von Interesse sein und deutlich seltener betroffen sein.

Schweizer Behörden speichern demgegenüber primär Verwaltungsdaten: Interne Dokumente, Korrespondenz, Projektunterlagen, Statistiken oder Personalakten. Diese Datentypen sind für Ermittlungen bei Terrorismus, Gewaltkriminalität oder Cyberkriminalität typischerweise nicht von Interesse und damit deutlich weniger exponiert als beispielsweise Kommunikationsdaten privater Nutzer.

V. DIFFERENZIERTE RISIKOBEURTEILUNG STATT PAUSCHALER AUSSCHLUSS

Vor diesem Hintergrund liegt das Risiko einer tatsächlichen Herausgabe von Inhaltsdaten an US-Strafverfolgungsbehörden deutlich unter dem, was eine rein theoretische Analyse des CLOUD Act nahelegen würde. Zwar sind Anfragen von US-Behörden nicht ausgeschlossen, wobei diese Möglichkeit bei der Risikobewertung berücksichtigt werden muss. Doch zeigen die konkreten Zahlen und etablierten Prozesse, dass US-Behördenanfragen auf ausserhalb der USA gespeicherte Inhalte von Cloud-Diensten in realen Szenarien selten und stark reglementiert sind. Dies relativiert die praktische Relevanz der theoretischen Herausgabepflichten gerade für den Einsatz von Cloud-Diensten bei Behörden.

Damit ist nicht gesagt, dass ein geringes statistisches Risiko per se ein tragbares Risiko darstellt. Gerade im öffentlich-rechtlichen Kontext kann bereits ein einzelner Vorfall – etwa die Offenlegung nachrichtendienstlich relevanter Informationen oder aussenpolitisch heikler Dokumente – erhebliche rechtsstaatliche und politische Konsequenzen nach sich ziehen. Entscheidend ist daher nicht allein die Eintrittswahrscheinlichkeit, sondern das Zusammenspiel von Eintrittswahrscheinlichkeit und potenziellem Schadensausmass. Die von der Behörde durchzuführende Schutzbedarfsanalyse dient genau diesem Zweck: Sie legt das erforderliche Schutzniveau der betreffenden Informationen fest. Für Daten, die dem Amtsgeheimnis unterliegen, gelten erhöhte Vertraulichkeitsanforderungen. Die Ergebnisse sind in einem Informationssicherheits- und Datenschutz-Konzept (ISDS-Konzept) nachvollziehbar zu dokumentieren. Die Schutzbedarfsanalyse stellt somit sicher, dass Daten mit erhöhtem Schutzbedarf – unabhängig von der statistischen Seltenheit eines Zugriffs – einem angemessenen Schutzniveau zugeführt werden. Dies kann im Einzelfall auch den Einsatz zusätzlicher technischer Schutzmassnahmen oder den Verzicht auf eine Cloud-Auslagerung umfassen. Regelmässig ist zudem eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen. Sie beurteilt die Risiken der Datenbearbeitung aus Sicht der betroffenen Personen, ergänzt das ISDS-Konzept und kann eine Vorabkontrolle durch die Datenschutzaufsichtsbehörde auslösen.

Demgegenüber wird ein pauschaler Verzicht auf die Nutzung von US-Cloud-Diensten diesem Befund nicht gerecht: Risiken variieren je nach Datenkategorie, Schutzbedarf und eingesetzten Sicherheitsvorkehrungen erheblich, und technische, vertragliche und rechtliche Hürden reduzieren die Wahrscheinlichkeit, dass Daten aufgrund von US-Behördenanfragen tatsächlich herausgegeben werden müssen, weiter. Dass diese Hürden nicht alle Risiken vollständig eliminieren können, spricht nicht gegen die Nutzung von US-Cloud-Diensten als solche, sondern für eine differenzierte, risikobasierte Entscheidung durch die Behörde im Einzelfall.

C. Alternativen zu US-Cloud-Diensten: Chancen, Grenzen und spezifische Risiken

Die Diskussion richtet den Blick zunehmend auf weitere Beschaffungsoptionen, von Cloud-Angeboten europäischer und schweizerischer Anbieter, bis zu Open-Source-Lösungen und On-Premises-Infrastrukturen. Da jede dieser Optionen mit eigenen rechtlichen, technischen und operativen Risiken verbunden ist, ist

[8] https://aws.amazon.com/compliance/cloud-act/

es verfehlt, sie pauschal als risikoärmere Alternativen zur Nutzung von US-Cloud-Diensten zu behandeln. Auch hier sind Einsatzfähigkeit und Risikoprofil sorgfältig zu bewerten.

I. CLOUD-ANGEBOTE VON EU-/CH-ANBIETERN

1. Verbleibende extraterritoriale Herausgabepflichten

Die Nutzung von Cloud-Angeboten von EU-/CH-Anbietern reduziert das Risiko einer Herausgabeanordnung unter dem CLOUD Act, sofern der Anbieter nicht dem CLOUD Act unterliegt. Gleichwohl sind auch solche Modelle nicht frei von Risiken im Hinblick auf den Zugriff aus Drittländern. So können etwa ausländische Konzerngesellschaften, der Einsatz von Subprozessoren mit Sitz in Drittstaaten oder die Einbindung globaler Lieferanten, beispielsweise durch globale Content Delivery Network (CDN)/Domain Name System (DNS)-Ketten, 24/7-Support oder Notfall-Failover in Nicht-EU/CH-Regionen, mittelbar extraterritoriale Zugriffsrechte bzw. Herausgabeverpflichtungen auslösen.

Aktuelles Beispiel ist hierbei der Fall OVHcloud: Ende September 2025 bestätigte der Ontario Superior Court of Justice eine Herausgabeanordnung gegenüber der französischen Muttergesellschaft von OVHcloud zur Übermittlung von in Europa gespeicherten Kundendaten an die Royal Canadian Mounted Police. Grundlage war insbesondere die angenommene "virtuelle Präsenz" des Unternehmens in Kanada über seine dortige Tochtergesellschaft. Der Fall zeigt, dass bereits eine solche Unternehmenspräsenz in einem Drittstaat extraterritoriale Herausgabeanordnungen auslösen kann, selbst bei entgegenstehendem lokalem Recht.

Darüber hinaus sieht die EU-Verordnung über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel (*E-Evidence-Verordnung*) vor, dass Behörden der EU-Mitgliedstaaten künftig unter bestimmten Voraussetzungen grenzüberschreitende Herausgabeanordnungen unmittelbar an Diensteanbieter in anderen Mitgliedstaaten richten können.

Unabhängig davon bleiben Behördenzugriffe über die internationale Amts- und Rechtshilfe (bspw. auf Grundlage des Zweiten Zusatzprotokolls zum Budapester Übereinkommen) möglich. Diese erfolgen nicht unmittelbar über den Cloud-Anbieter, sondern richten sich an die zuständige inländische Behörde und unterliegen den verfahrensrechtlichen Vorgaben der Amts- bzw. Rechtshilfe (einschliesslich des Bundesgesetzes über internationale Rechtshilfe in Strafsachen).

2. Erhöhter Integrationsaufwand durch eingeschränkte Portfolio- und Plattformreife

Daneben bestehen bei EU-/CH-Anbietern im Vergleich zu US-Hyperscalern auch faktische und operative Risiken. Das Dienste- und Anwendungsportfolio ist häufig weniger breit oder ausgereift, insbesondere im Bereich von KI-, Analytics-Funktionen sowie bei Plattform- und Managed-Services, was zu zusätzlichem und erhöhtem Integrationsaufwand oder funktionalen Einschränkungen führen kann. Schnittstellen und Integrationen sind oftmals weniger standardisiert, wodurch Migrationen, Automatisierungen und der Betrieb komplexer Architekturen, die im Bereich der modernen Verwaltungsarbeit erforderlich sind, zeitaufwändiger, kostspieliger und fehleranfälliger werden.

3. Begrenzte Skalierbarkeit, Supporttiefe und Zertifizierungsabdeckung

Zudem ist die Innovations- und Release-Kadenz niedriger. Auch Skalierung und Resilienz sind tendenziell eingeschränkt: EU-/CH-Anbieter verfügen über weniger Regionen und Verfügbarkeitszonen sowie eine geringere globale Netzabdeckung, was sich in höheren Latenzen, engeren Kapazitätsgrenzen und einer stärkeren Abhängigkeit von einzelnen Rechenzentren niederschlägt.

Im operativen Betrieb sind Einschränkungen beim Incident Response-Management und beim 24/7-Support zu beobachten, etwa hinsichtlich der Reaktionszeiten, der Eskalationspfade oder der Sprachabdeckung. Zertifizierungen und Compliance-Nachweise decken zudem seltener branchenspezifische Rahmenwerke ab. Während grössere, etablierte Cloud-Anbieter regelmässig über anerkannte Zertifizierungen wie ISO 27001 oder SOC 2 Type II verfügen und diese proaktiv auf sektorale Zusatzanforderungen erweitern, fehlen bei kleineren Anbietern häufig nicht nur die entsprechenden formellen Nachweise, sondern auch die internen Governance-Strukturen, die eine belastbare Aussage über die tatsächliche Einhaltung solcher Rahmenwerke ermöglichen würden.

4. Erhöhter Prüfungs- und Validierungsaufwand durch Verlagerungseffekt

Diese Lücke hat zur Folge, dass sich der Prüf- und Validierungsaufwand faktisch auf die beschaffende Behörde verlagert, die dann selbst im Rahmen von Due-Diligence-Prüfungen, vertraglichen Auditrechten und individuellen Freigabeverfahren sicherstellen muss, dass die regulatorischen und sicherheitstechnischen Anforderungen eingehalten werden. Für Behörden, die ohnehin mit begrenzten personellen und fachlichen Ressourcen im Bereich der IT-Sicherheit, des Datenschutzrechts und des Beschaffungswesens operieren, bedeutet dies eine zusätzliche Belastung. Diese verschärft sich insbesondere dann, wenn mehrere kleinere Anbieter parallel geprüft und überwacht werden müssen, da jeder Anbieter individuelle Risikoanalysen, massgeschneiderte Vertragsklauseln und laufende Kontrollmechanismen erfordert, ohne dass sich

Synergieeffekte erzielen lassen, wie sie bei der Zusammenarbeit mit einem zertifizierten Grossanbieter typischerweise entstehen.

In der Praxis führt dies häufig dazu, dass entweder die Prüftiefe reduziert wird, was das Risiko unerkannter Compliance-Defizite erhöht, oder dass Beschaffungsverfahren erhebliche Verzögerungen erfahren, weil die notwendigen internen Freigabeprozesse die vorhandenen Kapazitäten übersteigen. Schliesslich sind kleinere Anbieter stärker von Preisschwankungen, Marktkonsolidierung und Insolvenzrisiken betroffen, was bei der langfristigen Planung zu berücksichtigen ist.

II. OPEN-SOURCE-LÖSUNGEN

1. Operative und rechtliche Risiken durch eigenverantwortlichen Betrieb

Eigene Open-Source-Lösungen der Verwaltung ermöglichen ein hohes Mass an Kontrolle über Betrieb, Architektur und Schlüsselverwaltung. Sie können damit zu einer grösseren Unabhängigkeit im Betrieb und Schutz vor Herausgabeersuchen unter dem CLOUD Act führen. Vollständig ausschliessen lassen sich solche Ersuchen jedoch auch bei Open-Source-Lösungen nicht, etwa wenn der Betrieb über Infrastruktur eines dem CLOUD Act unterliegenden Anbieters erfolgt. Unabhängig davon setzt der eigenverantwortliche Betrieb dauerhaft ausreichend qualifizierte Fachkräfte, klar definierte Sicherheits- und Betriebsprozesse sowie einen verlässlichen 24/7-Betrieb voraus.

Neben den operativen Risiken bestehen auch spezifische rechtliche und faktische Risiken: Dazu zählen Sicherheitslücken infolge verzögerter Updates, Fehlkonfigurationen in komplexen Software-Stacks, unzureichende Überwachung (z.B. fehlendes Vulnerability Monitoring, mangelhaftes Dependency Tracking) sowie Compliance-Risiken bei fehlendem Lizenzmanagement, insbesondere im Zusammenhang mit Copyleft-Lizenzen. Hinzu kommen Haftungs- und Gewährleistungsfragen, da Open-Source-Software regelmässig "as is" bereitgestellt wird, was den Behörden entsprechende Verantwortung zuweist. Die Behörde trägt dabei die volle Betreiberverantwortung: Systemausfälle, Compliance-Verstösse oder Sicherheitsvorfälle infolge unzureichender Dokumentation von Architektur und Abhängigkeiten, Know-how-Konzentration auf Einzelpersonen oder verzögerter Patch-Einspielung gehen vollständig zu ihren Lasten.

Der eigenverantwortliche Betrieb ist zudem mit erheblichen Kosten verbunden: Neben den laufenden Personalkosten für spezialisierte Fachkräfte fallen Aufwände für Infrastruktur, Sicherheitsaudits, Lizenz-Compliance und die kontinuierliche Weiterentwicklung an. Die Gesamtbetriebskosten von Open-Source-Lösungen werden dabei häufig unterschätzt, da sie nicht durch Lizenzgebühren, sondern durch Betriebs- und Wartungsaufwände entstehen.

2. Sanktions-, Lieferketten- und Cyberrisiken

Zudem bestehen sanktionsbezogene Risiken im Zusammenhang mit der (Weiter-)Entwicklung und damit indirekt auch beim Einsatz von Open-Source-Software. Die derzeit bedeutendsten Betreiber von Hosting-Plattformen von Open-Source-Software sind in den USA domiziliert oder börsennotiert. Als solche unterliegen sie dem US-Sanktionsregime, was dazu führen kann, dass sie den Zugang für sanktionierte Entwickler einschränken müssen, um Verstösse gegen das US-Sanktionsregime zu vermeiden. Bezieht eine Schweizer Behörde Open-Source-Software von solchen Hosting-Plattformen, können Änderungen des Sanktionsregimes – etwa durch Erweiterungen von Sanktionslisten oder die Einbeziehung neuer Länder und Organisationen – erhebliche Risiken für Betrieb, Wartung und Weiterentwicklung begründen. Dass solche Risiken nicht nur theoretischer Natur sind, zeigt das Beispiel des Linux-Kernels: Im Oktober 2024 wurden elf russische Kernel-Entwickler aus Compliance-Gründen von ihren Rollen entbunden, was die operative Abhängigkeit grosser Open-Source-Projekte von der Sanktionslage einzelner Entwickler verdeutlicht.

Darüber hinaus bestehen spezifische Cyberrisiken: Open-Source-Software kann aufgrund ihrer öffentlich einsehbaren Codebasis gezielt auf Schwachstellen untersucht werden. Zudem besteht das Risiko von Supply-Chain-Angriffen, bei denen Schadcode über kompromittierte Abhängigkeiten oder manipulierte Beiträge eingeschleust wird – wie die im März 2024 aufgedeckte Backdoor in der xz-Utils-Bibliothek verdeutlicht, die vom bis heute unbekannten Akteur "Jia Tan" erfolgreich in den Code eingebettet worden war, jedoch rechtzeitig entdeckt wurde, bevor sie sich breit verteilen konnte.

Vergleichbare Überlegungen gelten für Open-Source-Hardware, deren Einsatz ebenfalls mit Verfügbarkeits- und Lieferkettenrisiken verbunden ist.

III. ON-PREMISES-LÖSUNGEN

1. Einschränkungen bei Skalierung, Resilienz und Hardware-Abhängigkeiten

On-Premises-Lösungen, bei denen die Systeme vollständig unter behördlicher Kontrolle stehen (im eigenen Serverraum, im behördeneigenen Rechenzentrum oder bei einem Colocation-Anbieter mit ausschliesslichem Behördenzugriff), stärken die physische Kontrolle über Infrastruktur und Daten. Dem stehen jedoch spezifische operative, rechtliche und wirtschaftliche Risiken gegenüber. So ist die Skalierung bei kurzfristigem Mehrbedarf oft eingeschränkt, das Ausfallrisiko ist im Vergleich

zu grossen Cloud-Infrastrukturen höher, und es bestehen Abhängigkeiten von Hardware-Lieferketten.

2. Alleinige Sicherheits- und Betriebsverantwortung ohne Aufgabenteilung

Zudem besteht ein erhöhter Bedarf an qualifizierten Fachkräften, um on-premises eine Lösung zu betreiben. Die Behörde muss sämtliche Betriebs- und Sicherheitsanforderungen – einschliesslich des Schutzes vor Cyberrisiken – selbst erfüllen und nachweisen. Anders als beim *Shared Responsibility Model*, bei dem Cloud-Anbieter und Kunde die Verantwortlichkeiten aufteilen und der Anbieter wesentliche Sicherheits- und Betriebsaufgaben übernimmt, trägt die Behörde bei On-Premises-Lösungen die alleinige Verantwortung für Verfügbarkeit und Wiederherstellung, Datenintegrität und Nachvollziehbarkeit, Archivierungs- und Aufbewahrungspflichten sowie den Datenschutz und die Informationssicherheit insgesamt. Dazu gehören insbesondere technische und organisatorische Sicherheitsmassnahmen, Zugriffskontrollen, Rollen- und Trennungskonzepte sowie Notfall- und Wiederherstellungsprozesse.

Zudem ergeben sich erhebliche Investitions- und Betriebskosten sowie zusätzliche Herausforderungen bei Beschaffung und Betrieb, etwa im Zusammenhang mit Erneuerungszyklen, Herstellerabhängigkeiten sowie Wartungs- und Supportverträgen.

D. Fazit: Risikobasierte Einzelfallentscheidung als Schlüssel zur rechtskonformen Cloud-Nutzung

Die vorstehende Analyse zeigt, dass der CLOUD Act kein generelles Hindernis für die Nutzung von US-Cloud-Diensten durch Schweizer Behörden darstellt: Die effektiven Zahlen und etablierten Verfahren belegen, dass US-Behördenanfragen auf ausserhalb der USA gespeicherte Inhaltsdaten in der Praxis selten und rechtlich stark eingeschränkt sind. Gleichwohl verlangt gerade der öffentlich-rechtliche Kontext eine differenzierte Beurteilung: Da bereits ein einzelner Vorfall erhebliche rechtsstaatliche und politische Konsequenzen nach sich ziehen kann, kommt es nicht allein auf die Eintrittswahrscheinlichkeit an, sondern auf ihr Zusammenspiel mit dem potenziellen Schadensausmass – was für eine risikobasierte Einzelfallentscheidung der Behörde spricht, nicht für einen pauschalen Ausschluss von US-Cloud-Diensten.

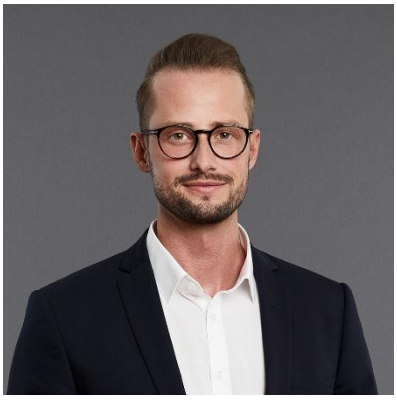
Jedes (Cloud-)Vorhaben hängt somit von einer Risikoentscheidung der handelnden Behörde ab, die auf einer eigenen, fundierten Risikoanalyse gründen muss. Jede Cloud-Lösung – ob von einem US-amerikanischen, schweizerischen oder europäischen Anbieter – ist, ebenso wie eigene Open-Source- und On-Premises-Lösungen, mit spezifischen rechtlichen, faktischen und operativen Herausforderungen behaftet. Die Behörde muss die konkreten Risiken unter Berücksichtigung des Schutzbedarfs der betroffenen Informationen systematisch erfassen, ihre Mitigierbarkeit prüfen und im Rahmen einer informierten Entscheidung beurteilen, ob die verbleibenden Restrisiken tragbar sind und das Vorhaben freigegeben werden kann.

Die Risikoanalyse kann ergeben, dass für bestimmte Vorhaben – etwa bei nachrichtendienstlich sensiblen Informationen oder aussenpolitisch heiklen Dokumenten – ein hybrider Ansatz die geeignetere Lösung ist. Dabei wird beispielsweise ein Public-Cloud-Dienst gezielt mit einer On-Premises- oder Open-Source-Lösung kombiniert, um unterschiedliche Schutzanforderungen zu erfüllen.

Diesem Befund liegt zugleich ein zeitgemässes Verständnis digitaler Souveränität zugrunde: Digitale Souveränität von Schweizer Behörden bedeutet weder Autarkie noch Abschottung, sondern die bewusste Fähigkeit, den Einsatz externer digitaler Leistungen eigenverantwortlich zu steuern und zu kontrollieren. Beziehungen zu externen Dienstleistern sind gelebte Praxis moderner Verwaltung und begründen keinen Souveränitätsverlust, solange sie transparent gestaltet, klar begrenzt und wirksam steuerbar bleiben. Eine zukunftsfähige Cloud-Strategie der öffentlichen Hand wird daher nicht an der Frage scheitern, ob Cloud-Dienste genutzt werden dürfen, sondern daran, ob die Behörden die institutionellen, technischen und rechtlichen Voraussetzungen schaffen, um diese Nutzung eigenverantwortlich, risikobasiert und im Einklang mit den rechtsstaatlichen Anforderungen zu gestalten.

AUTHORS

Dr. Christian Kunz
Partner
christian.kunz@baerkarrer.ch
T: +41 58 261 52 66



Ferdinand Rombach
Associate
ferdinand.rombach@baerkarrer.ch
T: +41 58 261 54 12

Dr. Katharina Cardon
Associate
katharina.cardon@baerkarrer.ch
T: +41 58 261 52 82