

Kleine Anfrage

Datensicherheit

Frage von Landtagsabgeordneter Daniel Seger

Antwort von Regierungschefin Brigitte Haas

Frage vom 05. November 2025

Sicherheit inklusive Datensicherheit stehen wieder mehr im Fokus. In der Schweiz wird dazu intensiv über den Einsatz von Microsoft 365 und anderen US-Cloud-Lösungen in der öffentlichen Verwaltung diskutiert. Armeechef Thomas Süssli forderte jüngst eine Exit-Strategie aus Microsoft 365 und warnte vor einer Schwächung der digitalen Souveränität. Datenschutzbeauftragte mehrerer Kantone sehen erhebliche Risiken für den Datenschutz, die staatliche Unabhängigkeit und IT-Sicherheit. Grund dafür ist unter anderem der Cloud Act der USA, der US-Behörden Zugriff auf Daten amerikanischer Firmen auch ausserhalb der USA erlaubt.

Auch in Liechtenstein nutzen verschiedene Behörden, Bildungseinrichtungen und staatsnahe Betriebe grosse Techunternehmen. Vor dem Hintergrund internationaler Entwicklungen stellt sich die Frage, wie Liechtenstein seine digitale Souveränität, insbesondere bei sensiblen Daten, sicherstellt. Gleichzeitig bieten sich europäische und Open-Source-Alternativen an, die Datensouveränität und regionale Wertschöpfung stärken könnten. Angesichts der sicherheitspolitischen und wirtschaftlichen Bedeutung der Thematik ist eine strategische Positionierung Liechtensteins erforderlich.

- * Wie bewertet die Regierung die Abhängigkeit öffentlicher Stellen von US-Softwareanbietern, insbesondere Microsoft?
- * Welche Risiken sieht die Regierung hinsichtlich des Cloud Act der USA für sensible oder personenbezogene Daten liechtensteinischer Behörden?
- * Gibt es eine Strategie oder Vorgabe, um staatliche Daten ausschliesslich in europäischen oder national kontrollierten Rechenzentren zu speichern?
- * Welche Stellen der Landesverwaltung oder staatsnahe Betriebe nutzen aktuell Microsoft 365 oder andere Cloud-Dienste US-amerikanischer Anbieter?

- * Gibt es eine interstaatliche Kooperation beispielsweise mit der Schweiz oder Österreich, um gemeinsame Open-Source-Lösungen für den öffentlichen Sektor zu entwickeln oder einzusetzen?

Antwort vom 07. November 2025

zu Frage 1:

Die Regierung erkennt die strategische Abhängigkeit von US-Softwareanbietern, hält sie jedoch in der Gesamtbetrachtung für vertretbar. Um einem Vendor-Lock-in entgegenzuwirken, verbleiben geschäftskritische Daten in On-Premise-Fachanwendungen der Landesverwaltung (LLV). Ein mehrstufiges Backup-Konzept sichert zudem die Wiederherstellung cloudverarbeiteter Daten. Schulungen der Mitarbeitenden, ein Nutzungsreglement und Anwendungseinschränkungen je nach Datenklassifikation verhindern die Verlagerung sensibler Prozesse in Microsoft 365 (M365).

Open-Source-Alternativen wurden geprüft. Die Wahl fiel jedoch aufgrund von Funktionsvielfalt, Integration und Synergien mit bestehenden Lösungen auf M365. Zur Wahrung der Datensouveränität setzt die LLV auf technische und organisatorische Schutzmechanismen wie die Microsoft EU Data Boundary, Customer Lockbox, Bring Your Own Key und verbindliche vertragliche Regelungen. Ein vollständiger Ausstieg bleibt durch die gewählte Architektur grundsätzlich möglich.

zu Frage 2:

Die vor der Einführung von M365 durchgeführte Risikoanalyse zu Informationssicherheit und Datenschutz erfolgte differenziert nach technischen, organisatorischen und rechtlichen Gesichtspunkten, wobei besonderes Augenmerk auf den Schutz vor Zugriffen ausländischer Behörden gelegt wurde. Der US CLOUD Act wurde dabei als spezifisches Restrisiko identifiziert, dessen Auswirkungen in Kombination mit der Umsetzung von technischen und organisatorischen Massnahmen – wie Verschlüsselung mit eigenen Schlüsseln, Datenklassifikation und Speicherung in EU-Rechenzentren – insgesamt als tragbar eingestuft wurden.

Um die Risiken weiter zu minimieren, sind Mitarbeiterschulungen verpflichtend und die Nutzung von M365 unterliegt strengen Vorgaben. Die LLV stellt damit sicher, dass moderne Arbeitsmittel genutzt werden können, ohne Kompromisse bei der Informationssicherheit einzugehen.

zu Frage 3:

Die LLV arbeitet bei der Umsetzung von IT-Projekten nach einer strukturierten Projektmanagement-Methodik, in der auch rechtliche und datenschutzrechtliche Fragen von Anfang an integraler Bestandteil sind. Bereits in der Planungsphase wird für jedes Projekt eine Cloud-Risikoanalyse durchgeführt. Dabei gilt die Grundregel, dass Standorte innerhalb des EWR bevorzugt werden. Nur wenn die datenschutzrechtlichen Anforderungen umfassend erfüllt werden können, kann ein Cloud-Dienst auch mit globalem Anbieteranteil zum Einsatz kommen.

Die Cloud Daten (M365) der LLV werden in Rechenzentren von Microsoft innerhalb des EWR gespeichert. Dies ist auch vertraglich vereinbart.

zu Frage 4:

Verschiedene Behörden, Bildungseinrichtungen und Staatsbetriebe in Liechtenstein nutzen M365 oder andere Cloud-Dienste US-amerikanischer Anbieter. Die Einführung erfolgt im Einklang mit den datenschutzrechtlichen Vorgaben und in enger Abstimmung mit der Datenschutzstelle Liechtenstein.

zu Frage 5:

Derzeit gibt es keine spezifischen Kooperationen mit anderen Staaten zur Entwicklung und Nutzung von Open-Source-Lösungen für den öffentlichen Sektor. Die Regierung prüft jedoch regelmässig Alternativen und Notfallpläne, um die digitale Souveränität zu gewährleisten.