KANTON AARGAU

GROSSER RAT

GR.25.345

VORSTOSS

Motion Lukas Huber, GLP, Berikon (Sprecher), René Bodmer, SVP, Unterlunkhofen, Martin Bossert, EDU, Rothrist, Carol Demarmels, SP, Obersiggenthal, Lutz Fischer, EVP, Wettingen, Dr. Mirjam Kosch, Grüne, Aarau, Sabine Sutter-Suter, Mitte, Lenzburg und Bruno Tüscher, FDP, Münchwilen, vom 18. November 2025 betreffend Schaffung einer rechtlichen Grundlage für Datenauslagerungen, Schlüsselhoheit und Exit-Strategien

---

Text:

Der Regierungsrat wird beauftragt, dem Grossen Rat eine Vorlage zu unterbreiten, welche:

1. eine spezifische rechtliche Grundlage für die Auslagerung von Datenbearbeitungen des Kantons schafft;
2. die Schlüsselhoheit des Kantons für ausgelagerte Daten verbindlich festschreibt;
3. verpflichtende Exit- und Migrationsstrategien für alle geschäftskritischen Informationssysteme vorsieht, unabhängig davon, ob sie intern oder extern betrieben werden;
4. und dabei insbesondere die Risiken von Cloud-Diensten unter ausländischem Recht ausserhalb von CH und EU (US CLOUD Act, FISA) und die diesbezügliche Beurteilungen der Beauftragte für Öffentlichkeit und Datenschutz (ÖDB) in der Antwort zur Interpellation „Gefährden M365 und Co. unsere Datensouveränität?“ (25.192) berücksichtigt.

Begründung:

Aus der Antwort auf die Interpellation „Gefährden M365 und Co. unsere Datensouveränität?“ (25.192) ergibt sich, dass für die Auslagerung von Daten an externe Rechenzentren (Outsourcing) im Kanton Aargau keine spezifische rechtliche Grundlage existiert. Der Regierungsrat stellt sich auf den Standpunkt, die allgemeinen Datenschutzvorgaben würden für die Auslagerung selbst sensibler Daten genügen. Diese rechtliche Einschätzung ist angesichts des erheblichen drohenden Grundrechtseingriffs der betroffenen Bürgerinnen und Bürger nicht haltbar. Entsprechend haben mehrere andere Kantone auf Gesetzes- oder Verordnungsstufe entsprechende Regelungen geschaffen (wie ZH, SO oder FR) oder spezifische Bestimmungen in bestehenden Informatikerlassen verankert (wie LU, SZ, GL, NW).

Eine systematische Auslagerung von Datenbearbeitungen – insbesondere in Cloud-Infrastrukturen – muss auf einer hinreichend konkreten rechtlichen Grundlage erfolgen. Nur so kann der Kanton definieren, welche Daten ausgelagert werden dürfen, welche Schutzstufen gelten und welche Anforderungen an Transparenz, Auditierbarkeit und Kontrolle einzuhalten sind. Ohne solche Normen besteht ein nicht hinnehmbares Risiko für Datenschutz, Rechtssicherheit und staatliche Handlungsfähigkeit.

Die Interpellationsantwort bestätigt zudem, dass der Kanton in massgeblichen Fällen (wie M365) nicht über die Schlüsselhoheit für die Daten verfügt und dass ausländische Erlasse (namentlich US

CLOUD Act und FISA) potentielle Zugriffe durch ausländische Staaten auf in der Schweiz an internationale Firmen ausgelagerte Daten ermöglichen. Solche Risiken betreffen auch besonders schützenswerte Daten aus Sicherheit, Gesundheit, Justiz und Sozialwesen sowie zahlreichen weiteren Bereichen. Ohne Schlüsselhoheit kann der Kanton weder Zugriffe verhindern noch den Zugriff im Notfall selbstständig wiederherstellen. Ein Staat darf die Kontrolle über seine Schlüssel nicht aus der Hand geben. Die Schlüsselhoheit muss deshalb rechtlich verankert werden.

Auch sicherheitspolitisch ist eine rechtliche Grundlage für die Datenauslagerung notwendig: Digitale Infrastrukturen gehören heute zur kritischen Grundversorgung und Datenhoheit ist ein sicherheitspolitisches Element der staatlichen Resilienz. Wer im Krisenfall keinen Zugriff auf seine Daten hat – oder nicht weiss, wer sonst darauf zugreifen kann –, verliert faktisch seine Handlungsfähigkeit.

Ökonomisch stärken klare rechtliche Regeln die Verhandlungsmacht des Kantons. Sie verhindern Lock-in-Effekte, schaffen Planungssicherheit und ermöglichen es, Alternativen wie Swiss-Cloud-Lösungen oder Open-Source-Systeme gleichwertig zu prüfen. Ohne Exit- und Migrationsstrategien ist der Kanton strukturell abhängig. Eine Pflicht zu solchen Strategien ist daher unverzichtbar.