privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Resolution zur Auslagerung von Datenbearbeitungen in die Cloud

Cloudbasierte Software erscheint heute als so attraktiv wie nie. Infrastrukturen, die potenziell allen Internet-Usern zur Verfügung stehen (sog. «Public Clouds»), erlauben eine dynamische Zuweisung von Rechen- und Speicherleistungen nach dem jeweiligen Bedarf der Kunden. Dieser Skaleneffekt ist umso grösser, je weitreichender – und in der Regel auch internationaler – die Infrastruktur des Cloud-Anbieters ist (man denke an sogenannte «Hyperscaler» wie Microsoft, Google oder Amazon). Nebst Einzelpersonen und Privatunternehmen greifen auch immer mehr öffentliche Organe auf zur direkten Nutzung bereitgestellte Anwendungen («Software-as-a-Service», kurz: SaaS) solcher Anbieter zurück. Auch lässt sich beobachten, dass Anbieter ihre Kunden vermehrt in die Cloud zu drängen versuchen.

Allerdings tragen öffentliche Organe eine besondere Verantwortung gegenüber den Daten ihrer Bürgerinnen und Bürger. Zwar dürfen sie deren Bearbeitung an Dritte auslagern, müssen dabei aber sicherstellen, dass der Datenschutz und die Informationssicherheit gewahrt bleiben. Vor einer Auslagerung von Personendaten in Cloud-Dienste müssen die Behörden deshalb unabhängig von der Sensitivität der Daten die besonderen Risiken im Einzelfall analysieren und mit geeigneten Massnahmen auf ein tragbares Mass reduzieren (vgl. Cloud-Merkblatt von privatim).

Aus folgenden Gründen hält privatim die Auslagerung von besonders schützenswerten oder einer gesetzlichen Geheimhaltungspflicht unterstehenden Personendaten in SaaS-Lösungen von grossen internationalen Anbietern durch öffentliche Organe in den meisten Fällen (wie namentlich M365) für unzulässig:

1. Die meisten SaaS-Lösungen bieten noch keine echte Ende-zu-Ende-Verschlüsselung, die einen Zugriff des Anbieters auf Klartextdaten ausschliessen würde.
2. Global operierende Firmen bieten zu wenig Transparenz, als dass Schweizer Behörden die Einhaltung der vertraglichen Pflichten betreffend Datenschutz und -sicherheit überprüfen könnten. Dies gilt für die Implementierung technischer Massnahmen und das Change-/ Release-Management gleichermassen wie für den Einsatz und die Kontrolle von Mitarbeitenden und Subunternehmen, die teils lange Ketten externer Leistungserbringer bilden. Erschwerend kommt hinzu, dass Softwareanbieter die Vertragsbedingungen periodisch einseitig anpassen können.
3. Mit der Nutzung von SaaS-Anwendungen geht deshalb ein erheblicher Kontrollverlust einher. Das öffentliche Organ kann die Wahrscheinlichkeit einer Verletzung von Grundrechten nicht beeinflussen. Es kann nur die Schwere potenzieller Rechtsverletzungen mindern, indem es besonders schützenswerte Daten nicht aus dem von ihm kontrollierbaren Herrschaftsbereich herausgibt.
4. Bei Daten, die unter einer gesetzlichen Geheimhaltungspflicht stehen, besteht teilweise eine erhebliche Rechtsunsicherheit, inwieweit diese überhaupt in Cloud-Dienste ausgelagert werden dürfen. Nicht jeder Dritte kann als Hilfsperson beigezogen werden, nur weil die Vorschriften des Strafrechts über das Amts- und das Berufsgeheimnis auch die Hilfspersonen von Geheimnisträgern zur Verschwiegenheit verpflichten.
5. US-Anbieter können aufgrund des 2018 erlassenen CLOUD Act dazu verpflichtet werden, Daten ihrer Kunden an US-Behörden herauszugeben, ohne die Regeln der internationalen Rechtshilfe einzuhalten – selbst, wenn diese Daten in Schweizer Rechenzentren gespeichert sind.

Fazit: Die Nutzung internationaler SaaS-Lösungen für besonders schützenswerte oder einer gesetzlichen Geheimhaltungspflicht unterstehende Personendaten durch öffentliche Organe ist nur dann möglich, wenn die Daten vom verantwortlichen Organ selbst verschlüsselt werden und der Cloud-Anbieter keinen Zugang zum Schlüssel hat.

Bern, 18. November 2025

Der Kanton Glarus hat von der Möglichkeit zum «opting out» nach Art. 18.2 der Statuten Gebrauch gemacht.