Interpellation Nr. 120 (November 2025)
betreffend aktuelle Entwicklungen zu Microsoft 365

25.5488.01

Microsoft untersteht dem US CLOUD Act, der US-Behörden weitreichende Kompetenzen einräumt, auf Daten zuzugreifen – unabhängig von deren physischem Speicherort oder den lokal geltenden Datenschutzgesetzen.

Eine Studie von Markus Schefer und Philip Glass (Universität Basel, 2023) für den Kanton Zürich ergibt, dass die Speicherung von Personendaten in der Microsoft-Cloud einen schwerwiegenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt.[1]

Der Jahresbericht der GPK verweist darauf, dass der Kanton vorsieht, auch besonders schützenswerte Daten in der Cloud zu bearbeiten.[2] Dies soll zwar unter qualifizierter Verschlüsselung stattfinden, doch den Ausführungen des Chefjuristen von Microsoft France, Anton Carniaux (2025), vor dem französischen Senat, ist jedoch zu entnehmen, dass Microsoft Zugriffe durch US-Behörden nicht verhindern kann.[3]

Auch die Verfügbarkeit der Dienste hängt letztlich vom Wohlwollen der Betreiber ab.

Exemplarisch dafür ist der Fall vom Februar 2025, als US-Präsident Trump Microsoft anwies, dem Chefankläger des Internationalen Strafgerichtshofs, Karim Khan, den Zugang zu seinem Mailkonto zu entziehen. Zwar hat Microsoft seither zugesichert, keine Konten europäischer Organisationen mehr zu sperren, doch ändert dies nichts an der rechtlichen und machtpolitischen Abhängigkeit.

Sollte die US-Regierung ihre Interessen gegenüber der Schweiz durchsetzen wollen, könnte sie US-Technologiekonzerne anweisen, den Zugang für bestimmte Kunden einzuschränken.

Ein solcher Fall würde die kantonale Verwaltung unmittelbar in ihrer Handlungsfähigkeit treffen, weshalb GPK und kantonale Datenschutzbeauftragte eine Exitstrategie und ein Business Continuity Management (BSM) für dieses Szenario fordern.

Der Internationale Strafgerichtshof hat sich mittlerweile von Microsoft gelöst und setzt auf eine open-source Lösung des Zentrums für Digitale Souveränität (ZenDis).[4] Auch der Chef der Schweizer Armee, Thomas Süssli, fordert eine eigenständige IT-Infrastruktur für die Armee. Grund ist nicht nur, dass sicherheitsrelevante Daten nicht in die Cloud dürfen, auch die Abhängigkeit von US-Techkonzernen wird sicherheitspolitisch zunehmend kritisch gesehen. Nicht zuletzt begibt man sich mit Microsoft 365 auch in eine finanzpolitische Pfadabhängigkeit.[5]

Vor diesem Hintergrund und den aktuelleren Entwicklungen rund um die Nutzung von Microsoft Cloudsystemen bittet die Interpellantin um die Beantwortung folgender Fragen:

1. Hat sich die bisherige Risikoeinschätzung des Regierungsrats, wonach ein erfolgreicher Zugriff des US-Staats auf in M365 gespeicherte Daten ausserhalb bestehender Rechtshilfeverfahren als «gering»[6] eingestuft wurde, aufgrund der jüngsten Entwicklungen (z. B. Zugriffsbefugnisse nach dem CLOUD Act, Fall ICC/Microsoft) geändert?
2. Ist der Regierungsrat trotz der Interventionen des Schweizer Armeechefs der Meinung, dass die Microsoft-interne qualifizierte Verschlüsselungsmöglichkeit, bei der die Schlüssel ausschliesslich innerhalb des Microsoft-Netzwerks verbleiben, ausreichend sicher ist?
3. Welche konkreten besonders schützenswerten Daten (bspw. religiöse oder politische Zugehörigkeit, Asylstatus, Gesundheits-, Vermögensdaten etc.) werden in der Cloud gespeichert und bearbeitet und welche nicht? Bitte um tabellarische Auflistung nach Datenkategorie und verantwortlichem Departement.
4. Die Interpellantin teilt die Einschätzung, dass geheime Daten wie sicherheitsrelevante Strategiepapiere nicht in einer Cloud abgelegt werden dürfen. Doch wie begründet die Regierung eine Digitalisierungsstrategie, die allfällig sicherheitsrelevante Informationen über seine Bevölkerung gegenüber Microsoft und schliesslich auch gegenüber der US-Regierung zugänglich macht?
5. Im Mai 2025 gab der Regierungsrat im Rahmen einer Interpellationsbeantwortung bekannt, dass ein Grobkonzept einer Exit-Strategie vorhanden ist, mit dem Ziel die rudimentäre Aufrechterhaltung der Geschäftsfähigkeit zu garantieren.[7] Mit Blick auf das Ziel handelt es sich hierbei eher um das (ebenso wichtige) «Business Continuity Management». Wurde daneben auch eine Exitstrategie erarbeitet, die technische, organisatorische und rechtliche Massnahmen zur Datenextraktion, Systemablösung, Datenimport und Wiederaufnahme der Geschäftsprozesse in einer alternativen Umgebung umfasst? Falls nein, warum nicht?
   a. Ist das damals beschriebene «Grobkonzept» innerhalb der letzten 7 Monate ausgereift?
   b. Welche Massnahmen und welche Software kommen hier zum Einsatz?
   c. Unter welchen Umständen werden Exitstrategie und «Business Continuity» Strategie angewendet?
   d. Fanden bereits Schulungen der Mitarbeitenden für Notfälle statt?

[1] Tätigkeitsbericht 2023, Besondere Risiken für die Grundrechte: M365, Datenschutzbeauftragte des Kantons Zürich und Link Jusletter IT

[2] Rechenschaftsbericht der Geschäftsprüfungskommission und Bericht zum Jahresbericht 2024 des Regierungsrats, S.53

[3] Emma Woollacott, Microsoft Can 't Keep EU Data Safe From US Authorities. Forbes, 22. Juli 2025

[4] Christof Kerkmann, «Strafgerichtshof ersetzt Microsoft durch deutsche Lösung» Handelsblatt (30.10.2025)

[5] Adrienne Fichter, «Der Armeechef stemmt sich gegen Microsoft» (31.10.2025) siehe auch
Edith Hollenstein, Konrad Staehelin «Wegen Trump und hoher Kosten Schweizer Armee will weg von Microsoft» 1.11.2025

[6] Interpellationsbeantwortung Nr. 46 Anina Ineichen betreffend Regierungsratsbeschluss zum Einsatz von M365 für die ICT-Grundversorgung (S.9ff)

[7] vgl. Interpellationsbeantwortung Nr. 46 Anina Ineichen betreffend Regierungsratsbeschluss zum Einsatz von M365 für die ICT-Grundversorgung (S.9ff)

Franziska Stier