An den Grossen Rat **25.5488.02**

FD/P255488

Basel, 3. Dezember 2025

Regierungsratsbeschluss vom 2. Dezember 2025

Interpellation Nr. 120 Franziska Stier betreffend aktuelle Entwicklungen zu Microsoft 365

(Eingereicht vor der Grossratssitzung vom 12. November 2025)

«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 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 microsoftinterne 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?

Franziska Stier»

Wir beantworten diese Interpellation wie folgt:

1. Einleitung

Die Digitalisierung der Verwaltung ist ein zentrales strategisches Ziel des Kantons Basel-Stadt. Mit dem «Leitbild Digitale Verwaltung» und der darauf aufbauenden Digitalstrategie hat der Regierungsrat festgelegt, dass neue Technologien und Betriebsmodelle genutzt werden sollen, um durchgängig digitale Verwaltungsprozesse zu erreichen und einen starken Service public sowie eine moderne, effiziente Verwaltung zu gewährleisten. Cloud-Lösungen internationaler Anbieter spielen dabei eine wichtige Rolle.

Der neue Legislaturplan 2025–2029 führt diesen Weg fort und hebt unter dem Schwerpunkt «Innovation und Wettbewerbsfähigkeit» ausdrücklich hervor, dass die Verwaltung digital gut für die Zukunft aufgestellt sein soll. Die Einführung einer standardisierten Kollaborations- und Kommunikationsplattform wie Microsoft 365 ist vor diesem Hintergrund ein zentraler Umsetzungsschritt, der diese strategischen Vorgaben konkretisiert.

Die Geschäftsprüfungskommission des Grossen Rates hat im Zusammenhang mit dieser kantonalen Strategie nicht nur Fragen zu CLOUD Act, Datensouveränität und Anbieterabhängigkeit aufgeworfen, sondern auch spezifische Forderungen zur Datensicherheit und IT-Security formuliert. Der Regierungsrat nimmt diese Anliegen ernst. In seiner Einordnung der Risiken muss er entsprechend eine Gesamtbeurteilung vornehmen, die in Bezug auf Datensicherheit auch das deutlich höhere Risiko von unrechtmässigen Datenzugriffen auf Verwaltungsdaten – etwa durch Hackerangriffe, Ransomware oder Fehlkonfigurationen – mitberücksichtigt. Gerade hier bieten moderne Cloud-Dienste wie Microsoft 365 mit ihrer professionell betriebenen, laufend aktualisierten Sicherheitsinfrastruktur die Möglichkeit, dieses Risiko im Vergleich zu einer fragmentierten Eigeninfrastruktur deutlich zu senken. Die vorliegende Stellungnahme ordnet die genannten Bedenken in diesen strategischen und sicherheitstechnischen Kontext ein.

2. Zu den einzelnen 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?

Für die Beurteilung der Gesamtrisikosituation hat der Regierungsrat basierend auf der Rosenthal Methode 62 Risiken bewertet. Das Risiko des «Lawful Access» wurde dabei vertieft analysiert. Die Auswertung hat gezeigt, dass ein Behördenzugriff nach US-Recht möglich, aber die Eintretenswahrscheinlichkeit sehr gering ist, da hohe rechtliche Hürden bestehen. Ein Zugriff bedeutet die Lieferung von Daten durch Microsoft an die Strafverfolgungsbehörden zu einem spezifischen Verbrechen, das Gegenstand der Strafverfolgung ist. Ein Antrag für einen «Zugriff» bezieht sich nicht auf alle Daten des Kantons, sondern auf jene eines beschuldigten Mitarbeitenden. Der Regierungsrat hält basierend auf den vorhandenen empirischen Daten an seiner Risikoeinschätzung fest. So zeigen die aktuellen Zahlen von Microsoft im Bericht über die Anfragen von Justizbehörden (Law enforcement requests report RERR) für das erste Halbjahr 2025, dass die Anzahl an Strafverfolgungsanfragen für alle Enterprise-Kunden global mit 168 Fällen (H1/2024: 166) stabil geblieben sind, entgegen der Sorge, dass unter Präsident Trump diese Zahl stark zunehmen würde. 57% der Begehren wurden ohne Datenlieferung erledigt. In 46 Fällen wurde «non content Data» eines Kunden geliefert also Metadaten wie IP- oder Standortlogs. Nur in 27 Fällen, kam es schlussendlich zur Auslieferung von Kundendaten. Nur 5 Anfragen bezogen sich auf Enterprise Kunden ausserhalb der USA. In einem Fall fand ein Zugriff auf ein Handelsunternehmen mit Sitz in Europa statt, das Auftragnehmer der US-Regierung war. Es wurde weiterhin kein Fall eines Datenzugriff auf einen staatlichen Kunden registriert.

Demgegenüber schätzt der Regierungsrat das Risiko eines unrechtmässigen Datenzugriffs aufgrund von Cybercrime als deutlich höher ein. Gemäss ENISA, der EU-Agentur für Cybersicherheit ist der international am stärksten von Cybercrime betroffene Sektor die öffentliche Verwaltung. Auch die Schweiz ist davon nicht ausgenommen, wie 2023 der Angriff auf den Bundesdienstleister Xplain zeigte, bei denen grosse Datenmengen gestohlen und im Darknet veröffentlicht wurden. Das Nationale Zentrum für Cybersicherheit verzeichnete 2024 einen neuen Höchststand mit 62'000 gemeldeten Cybervorfällen über alle Sektoren. Sowohl Eintretenswahrscheinlichkeit als auch Auswirkung werden als hoch eingeschätzt. Die grössten Schäden entstehen durch veraltete, lokal betriebene Systeme (Mail, Fileserver, Fachanwendungen), unsauberes Patchen und fehlende Sicherheitsfunktionen.

Kollaborationsdienste wie E-Mail sind das wichtigste Einfallstor für Hacker. Microsoft 365 setzt hier an und bietet eine integrierte Sicherheitsplattform: E-Mails, Geräte, Benutzerkonten und Cloud-Apps werden gemeinsam überwacht, Angriffe wie Phishing und Ransomware früh erkannt und oft gestoppt, bevor Schaden entsteht. KI-gestützte Analysen und automatisierte Reaktionen sorgen dafür, dass neue Bedrohungen schnell abgewehrt werden. Systeme und Einstellungen werden laufend auf Schwachstellen geprüft und automatisch mit internationalen Sicherheitsstandards abgeglichen. Im Unterschied zu vielen einzelnen «On-Premises-Lösungen» profitiert der Kanton bei M365 direkt von der weltweiten Sicherheitsforschung von Microsoft – eine vergleichbare Eigenlösung wäre teurer, schwerer zu betreiben und damit anfälliger für unberechtigte Datenzugriffe.

Der Regierungsrat ist bei seiner Gesamtbeurteilung zum Schluss gekommen, dass aus Sicht der Informationssicherheit das eigentliche Hauptrisiko für Staat und Bevölkerung heute nicht der seltene, rechtlich kontrollierte Zugriff einer ausländischen Behörde, sondern der alltägliche, oft erfolgreiche Angriff von Cyberkriminellen oder staatlichen Akteuren auf schlecht geschützte Systeme ist. Der «Lawful Access» wird vom Regierungsrat nicht als «ungefährlich» eingestuft. Er erachtet es als verantwortbar, ein seltenes Risiko in Kauf zu nehmen, wenn damit sehr häufige und bereits eingetretene Risiken substanziell reduziert werden können.

2. *Ist der Regierungsrat trotz der Interventionen des Schweizer Armeechefs der Meinung, dass die microsoftinterne qualifizierte Verschlüsselungsmöglichkeit, bei der die Schlüssel ausschliesslich innerhalb des Microsoft-Netzwerks verbleiben, ausreichend sicher ist?*

An der Bewertung der Sicherheit der Verschlüsselung ändert sich mit heutigem Kenntnisstand nichts. Die beschlossene Handhabung des Regierungsrats würde eine Nutzung von M365-Services für die geheimen Daten der Armee ebenfalls nicht zulassen. Im Kanton Basel-Stadt ist die Nutzung der Cloud für Informationen des Landesschutzes bzw. für geheim eingestufte Daten nicht zulässig.

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.*

Die Verantwortung für die Daten und deren Bearbeitung liegt, wie im kantonalen Informations- und Datenschutzgesetz (IDG) festgehalten, bei der Dateneignerschaft, d.h. den Dienststellen und Departementen. Eine Übersicht darüber, welche konkreten Daten wo gespeichert sind, wie es die Interpellation skizziert, besteht heute nicht. Der Regierungsrat investiert jedoch aktiv in den Ausbau des Datenmanagements, um einen zentralen Datenkatalog aufzubauen. Damit können ähnliche Fragen in Zukunft potenziell einfacher beantwortet werden.

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?*

Die Bearbeitung von als geheim klassifizierten Daten in der Cloud ist nicht zulässig. Alle Daten werden nach Schutzstufen kategorisiert. Die Risikoabwägung zeigt dabei auf, welche Schutzmassnahmen erforderlich sind, um die Daten bestmöglich zu schützen und ein effizientes Arbeiten zu ermöglichen.

Es gilt ebenfalls festzuhalten, dass mit der Einführung von M365 die Daten aus Cybersecurity-Sicht besser geschützt sind. Auch unter Berücksichtigung bestehender Risiken, hat die Einführung von M365 zu einer deutlichen Verbesserung der Informationssicherheit geführt (siehe Antwort zur 1. Frage).

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. 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?*

Das Exit-Konzept ist ein übergeordneter Plan für eine kurzfristige Ersatzlösung für M365-Services, wenn der Zugriff auf die Cloud durch den Anbieter eingeschränkt wird, oder ein Ereignis (siehe Antwort zu c.) eintrifft, das den Kanton zu einem raschen Ausstieg veranlasst. Das Konzept stellt die Geschäftsfähigkeit des Kantons im Szenario eines erzwungenen kurzfristigen Exits aus der

Cloud sicher. Es geht nicht um einen gleichwertigen Ersatz, sondern darum wie die Basisfunktionalitäten aufrechterhalten werden können. Für das IT-Continuity Management sind technische Massnahmen vorgesehen, wie das microsoftexterne Backup sämtlicher E-Mails und Dokumente oder «on-premise» Reserve-Kapazitäten für rund 1'000 geschäftskritische E-Mail-Konten. So kann eine rasche Wiederherstellung essenzieller Mailboxen sichergestellt werden.

Der Regierungsrat hat das Finanzdepartement beauftragt, der Konferenz für Informatik und Informationssicherheit (KIS) sowie der Regierungsrätlichen Delegation Informatik jährlich darüber zu berichten, wie es die Notwendigkeit und Möglichkeit einschätzt, von Microsoft zu einem alternativen Anbieter zu wechseln. Dafür müssen die geopolitischen und technischen Entwicklungen laufend beobachtet werden.

In einer Gesamtbeurteilung, ob anstelle von Microsoft ein Alternativanbieter gewählt werden soll, müssen neben Datenschutz, Souveränität und Informationssicherheit auch Dimensionen wie Funktionalität, Benutzerfreundlichkeit und Wirtschaftlichkeit berücksichtigt werden.

a. Ist das damals beschriebene «Grobkonzept» innerhalb der letzten 7 Monate ausgereift?

Ein Detailkonzept muss auf eine konkrete Alternativlösung ausgerichtet werden. Dieses definiert dann, welche Planungsschritte für eine Ablösung nötig sind, wie zum Beispiel Infrastrukturmassnahmen, Dienstleistungseinschränkungen, Schulungen und so weiter. Da die Entwicklungen in diesem Feld rasant sind, macht es keinen Sinn, frühzeitig ein Detailkonzept für ein Alternativangebot festzulegen, das dann im Ereignisfall nicht mehr die beste Lösung darstellt.

b. Welche Massnahmen und welche Software kommen hier zum Einsatz?

Heute werden im Exit-Konzept mögliche Alternativprodukte aufgeführt, deren Gemeinsamkeit es ist, dass sie lokal installierbar sind, und lokal betrieben werden können. Dabei handelt es sich sowohl um «on-premise» Lösungen von Microsoft als auch von alternativen Anbietern. Der Markt wird aktiv beobachtet mit dem Ziel, aufkommende Alternativlösungen zu identifizieren, die beim Eintreffen eines Krisenszenarios ermöglichen, sich vom Hersteller Microsoft unabhängig zu machen.

c. Unter welchen Umständen werden Exitstrategie und «Business Continuity» Strategie angewendet?

Das Exit-Konzept kommt zur Anwendung, wenn bestimmte Auslösekriterien eintreten. Dazu gehört erstens die Kündigung des Vertragsverhältnisses, sei es durch den Kanton oder durch Microsoft, sei dies ordentlich oder aus wichtigem Grund. Zweitens greifen die Strategien, wenn der Anbieter unzumutbare Änderungen im Service vornimmt, etwa durch eine erhebliche Reduktion des Leistungsumfangs, der Servicequalität oder der zugesicherten Sicherheits- und Datenschutzstandards. Drittens werden sie aktiviert, wenn es zu untragbaren Preiserhöhungen kommt.

Weitere Auslöser sind politische Veränderungen, welche das Risiko für den Kanton deutlich erhöhen, beispielsweise neue gesetzliche Zugriffsrechte ausländischer Behörden, Sanktionen oder geopolitische Spannungen, die die Verfügbarkeit der Dienste in Frage stellen. Auch Fehlverhalten des Anbieters, insbesondere bei Datenmissbrauch sowie schwerwiegenden oder wiederholten Verstössen gegen Datenschutz- oder Sicherheitsbestimmungen zählt dazu.

d. Fanden bereits Schulungen der Mitarbeitenden für Notfälle statt?

Der Ausfall der Services wie Mail und Kollaboration hat für die unterschiedlichen Fachstellen des Kantons sehr unterschiedliche Auswirkungen. Der Ausfall dieser Services ist ein Szenario das Dienststellen unabhängig von der IT-Technologie M365 je nach Relevanz in Ihrem BCM planen. Mit M365 konnte die Wahrscheinlichkeit eines Ausfalls gesenkt werden.

Mitarbeiter werden mit der Einführung von M365 umfassend geschult, was die Benutzung und die Einhaltung der Verwendungszwecke angehen. Schulungen der Gesamtem Belegschaft für das aktuell sehr unwahrscheinliche Szenario eines Microsoft Exits sind aktuell nicht vorgesehen.

Im Namen des Regierungsrates des Kantons Basel-Stadt

Dr. Conradin Cramer
Regierungspräsident

Barbara Schüpbach-Guggenbühl
Staatsschreiberin