Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich

KR-Nr. 71/2025

Sitzung vom 21. Mai 2025

560. Anfrage (Risiken von Microsoft-365-Cloud)

Kantonsrätin Selma L'Orange Seigo, Zürich, und Mitunterzeichnende haben am 3. März 2025 folgende Anfrage eingereicht:

Mit RRB 542/2022 hat der Regierungsrat dem Einsatz von Microsoft 365 als Cloud-Lösung für die IKT-Grundvesorgung in der kantonalen Verwaltung zugestimmt. Er beurteilt darin die Wahrscheinlichkeit für einen Datenzugriff US-amerikanischer Behörden im Rahmen des «CLOUD Act» (Claryfing Lawful Oveseas Use of Data Act) als «höchst unwahrscheinlich».

Die Datenschützerin hingegen äusserte sich sehr kritisch gegenüber der Verwendung von Microsoft 365, wie auch im Jahresbericht 2023 festgehalten ist (S. 19 f.) Zusammenfassend hält sie fest: «Die Daten sämtlicher Personen im Zuständigkeitsbereich des öffentlichen Organs werden durch den Einsatz dieser Cloud-Lösung auf Vorrat zugänglich für US-Behörden.»

Das «Transatlantic Data Privacy Framework», TADPF, soll sicherstellen, dass die Daten europäischer Nutzerinnen und Nutzer bei amerikanischen Tech-Unternehmen geschützt sind. Die Aufsicht erfolgt hauptsächlich durch das «Privacy and Civil Liberties Oversight Board», PCLOB. Dieses besteht jedoch seit Ende Januar nur noch aus einer einzelnen Person und kann seine Aufgabe nicht mehr warhnehmen.

Nebst der Datensicherheit ist auch die Abhängigkeit von amerikanischen Tech-Firmen kritisch zu sehen. Sie könnte als Druckmittel eingesetzt werden, um amerikanische Interessen durchzusetzen.

Vor dem Hintergrund dieser Entwicklungen bitten wir den Regierungsrat um die Beantwortung der folgenden Fragen:

1. Ist der Regierungsrat der Ansicht, dass die Risikoanalyse bezüglich Microsoft 365 aus dem Jahr 2021 immer noch angemessen ist und die tatsächlichen Risiken widerspiegelt?
2. Findet eine regelmässige und systematische Überprüfung der Risikoanalyse statt, die auch sich wandelnde politische Entwicklungen miteinbezieht?
3. Im RRB 542/2022 wird lediglich die geschätzte Wahrscheinlichkeit für einen «lawful access» angegeben, aber nicht, welche Konsequenzen dieser hätte. Was wären die Folgen, wenn amerikanische Behörden auf die von der Zürcher Verwaltung in der Cloud gespeicherten Daten Zugriff nehmen würden? Welche Personenkreise wären wie betroffen?

4. Könnte die kantonale Verwaltung noch ordnungsgemäss funktionieren, wenn Microsoft 365 seine Dienstleistungen einschränken oder sogar sistieren würde? Welche Bereiche der kantonalen Verwaltung wären inwiefern betroffen?
5. Plant der Regierungsrat verstärkt Wert zu legen auf Datenhoheit und Unabhängigkeit von amerikanischen bzw. ausländischen Tech-Firmen?

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Die Anfrage Selma L'Orange Seigo, Zürich, und Mitunterzeichnende wird wie folgt beantwortet:

Zu Frage 1:

Vor der Inbetriebnahme von Microsoft 365 wurde eine umfassende Bewertung der Risiken in Bezug auf die Informationssicherheit und den Datenschutz durchgeführt. Bestandteil dieser Analyse war unter anderem die Bewertung des Risikos eines behördlichen Zugriffs, der sich auf einen Rechtserlass stützt und ein Unternehmen unter bestimmten Voraussetzungen zur Herausgabe von Kundendaten zwingt («Lawful Access»).

Der Regierungsrat ist der Ansicht, dass sich der gewählte Ansatz zur Risikoanalyse bewährt hat und dass die Fragestellung, die dem gewählten Modell in Bezug auf die Bewertung des Risikos eines «Lawful Access» zugrunde liegt, nach wie vor treffend ist und die gegenwärtigen Risiken widerspiegelt.

Zu Frage 2:

Das Modell zur Bewertung des Risikos eines «Lawful Access» wurde zuletzt Anfang 2024 überarbeitet. Auf der Grundlage des angepassten Modells erfolgte eine Überprüfung des Einsatzes von Microsoft 365, welche die bisherige Nutzung bestätigte.

Neben den politischen werden auch technologische Entwicklungen laufend hinsichtlich ihres Potenzials zur Minimierung bestehender Risiken beobachtet. Auch dies fliesst in die Risikobewertung ein.

Zu Frage 3:

Trotz der getroffenen technologischen, vertraglichen und organisatorischen Massnahmen zum Schutz der Daten kann ein «Lawful Access» nicht vollständig ausgeschlossen werden. Daher hat die Finanzdirektion eine Allgemeine Nutzungsrichtlinie für Microsoft 365 erlassen, die auch von der Datenschutzbeauftragten des Kantons Zürich begrüsst wurde.

Diese Nutzungsrichtlinie gibt in Abhängigkeit von der Klassifikation der zu bearbeitenden Daten vor, welche Anwendungen bzw. Funktionen von Microsoft 365 genutzt werden dürfen. Die Daten sind sowohl aus geschäftlicher als auch aus datenschutzrechtlicher Sicht zu klassifizieren. Damit wird sichergestellt, dass der Datenschutz und die Informationssicherheit in der verwaltungsinternen Kommunikation und Zusammenarbeit angemessen gewahrt werden. Ausserdem sollen Geschäftsfalldaten in Fachapplikationen gespeichert werden, und nicht in Microsoft 365. Demzufolge wäre von einem «Lawful Access» insbesondere die E-Mail-Kommunikation der kantonalen Verwaltung betroffen, wobei E-Mails verschlüsselt und dadurch vor einem unerwünschten Zugriff geschützt werden können.

Zu Frage 4:

Die digitale Transformation gehört zu den erklärten Zielen des Regierungsrates. Im Zusammenhang mit der Strategie Digitale Verwaltung und deren Umsetzung werden die Voraussetzungen dafür geschaffen, dass der Austausch zwischen der Bevölkerung, den Unternehmen und den kantonalen Behörden künftig beispielsweise über das «Zürikonto» als sicheren und massgeblichen Kanal für elektronische Verfahrenshandlungen (vgl. § 4e Verwaltungsrechtspflegegesetz [LS 175.2], gemäss Änderung vom 30. Oktober 2023 und Verordnung über elektronische Verfahrenshandlungen im Verwaltungsverfahren [ABl 2024-07-12]) erfolgen kann.

Gleichwohl handelt es sich bei Microsoft 365 um einen wesentlichen Bestandteil des Digitalen Arbeitsplatzes im Bereich der Büroautomation. Eine eingeschränkte Verfügbarkeit von Microsoft 365 hätte somit unmittelbare Auswirkungen auf die Arbeitsfähigkeit der Mitarbeitenden sowie auf Dienstleistungen und Angebote, die damit im Zusammenhang stehen. Insbesondere mit Bezug auf den Austausch innerhalb der Verwaltung wäre im Falle einer eingeschränkten Verfügbarkeit mit Behinderungen zu rechnen.

Bei der gegenwärtigen Überarbeitung der Risikobewertung von Microsoft 365 wird auch der Weiterführung des Geschäftsbetriebs besondere Aufmerksamkeit geschenkt. Das Ziel ist eine erhöhte Widerstandsfähigkeit im Umgang mit den Folgen einer möglichen kurz- oder langfristigen Störung im Bereich von Microsoft 365. Auch heute schon ist es möglich, den Mitarbeitenden alternative, von Microsoft 365 unabhängige Anwendungen verfügbar zu machen, um möglichen Einschränkungen in der Verfügbarkeit entgegenzuwirken.

Zu Frage 5:

Die Rahmenbedingungen für den Einsatz von Cloud-Diensten in der kantonalen Verwaltung werden laufend weiterentwickelt. Im Mittelpunkt steht dabei die Klärung, welches Cloud-Bereitstellungsmodell – etwa Public, Private oder Hybrid Cloud – für welche Anwendungsfälle geeignet und zulässig ist, unter Berücksichtigung von Kriterien wie Datenstandort und Anbieterherkunft (Schweiz oder Europa).

Zudem hat der Regierungsrat dem Kantonsrat am 18. September 2024 den Erlass des Gesetzes über elektronische Basisdienste (Vorlage 5985) beantragt. Diese Gesetzesvorlage sieht in § 17 Abs. 1 eine Regelung vor, in der festgelegt werden soll, unter welchen Voraussetzungen das Bearbeiten von Personendaten und besonderen Personendaten in Applikationen digitaler Arbeitsplätze der Behörden an Dritte übertragen werden kann: Zum einen sollen sich deren Rechenzentren in der Schweiz oder in einem Staat mit einem angemessenen Datenschutz befinden müssen (lit. a), und zum anderen soll aufgrund der getroffenen technischen, organisatorischen und vertraglichen Massnahmen kein Grund zur Annahme bestehen dürfen, dass ein ausländischer Staat auf die Daten zugreifen wird (lit. b).

II. Mitteilung an die Mitglieder des Kantonsrates und des Regierungsrates sowie an die Finanzdirektion.

Vor dem Regierungsrat
Die Staatsschreiberin:
Kathrin Arioli