Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich

KR-Nr. 354/2022

Sitzung vom 14. Dezember 2022

1645. Anfrage (Sicherheit von durch kantonale Stellen auf Cloud-Diensten gespeicherten Daten)

Kantonsrätin Nicola Yuste, Zürich, sowie die Kantonsräte Hans-Peter Amrein, Küsnacht, und Florian Heer, Winterthur, haben am 26. September 2022 folgende Anfrage eingereicht:

Der Regierungsrat beschloss an seiner Sitzung vom 30. März 2022 die Zulassung der Cloud-Lösung Microsoft 365 für sämtliche der IKT-Strategie unterstehenden Einheiten der kantonalen Verwaltung sowie die Kantonspolizei. Mit Microsoft 365 stehe eine Cloud-Lösung mit einer Breite an Diensten zur Verfügung, darunter die Cloud-Services Exchange Online sowie Microsoft Teams.

Der Regierungsrat geht in der Publikation auch auf Fragen zur IT-Sicherheit und zum Datenschutz im Zusammenhang mit Cloud-Lösungen ein. Im Vergleich zu On-Premises-Lösungen würden bei Cloud-Lösungen grundsätzlich keine höheren Risiken bestehen, aber das Risikoprofil unterscheide sich.

Der Kanton, vertreten durch das Amt für Informatik, habe im Juni 2021 Verträge mit Microsoft abgeschlossen. Die Verhandlungen seien von der Datenschutzbeauftragen des Kantons begleitet worden und das Vertragswerk sei mit einer von der Datenschutzbeauftragten gestützten Ergänzung abgeschlossen worden. Diese Ergänzung ist allerdings nicht öffentlich einsehbar.[1] Ein Gesuch um Informationszugang betreffend Einsatz von Microsoft 365 in der kantonalen Verwaltung wurde im Juli 2022 vom Amt für Informatik mit Berufung auf eine Vertraulichkeitsvereinbarung mit Microsoft abgelehnt.[2]

Die Regierung weist im RRB 542/2022 über die Zulassung von Microsoft 365 auf das spezifische Risiko im Bereich «Lawful Access» hin. Amerikanische Softwareanbieter können gestützt auf den CLOUD Act (Clarifying Lawful Overseas Use of Data Act) unter bestimmten Voraussetzungen von Behörden zur Herausgabe von Kundendaten gezwungen werden. Die Regierung stellt im genannten RRB jedoch fest, dass ein solches Szenario in der Praxis höchst unwahrscheinlich sei.

[1] https://steigerlegal.ch/2022/06/11/kanton-zuerich-microsoft-365-geheimhaltung/
[2] https://steigerlegal.ch/2022/08/05/kanton-zuerich-microsoft-cloud-geheimhaltung/

Datenschützer anderer Kantone (Thurgau, Luzern) sehen die Vertraulichkeit von persönlichen Daten mit Microsoft als nicht durchsetzbar und weisen auf eine potenzielle Verletzung des Amtsgeheimnisses hin.

Vor diesem Hintergrund bitten wir (in Ergänzung der Anfrage von Lorenz Habicher und Valentin Landmann vom 19. September 2022) die Regierung um die Beantwortung folgender Fragen:

1. Wie begründet das Amt für Informatik den Entscheid, das Vertragswerk mit Microsoft und die Ergänzung der Datenschützerin geheim zu halten?
2. Wie wird das Interesse der Öffentlichkeit, auch vor dem Hintergrund der Vertrauensbildung der Bevölkerung in den Datenschutz der öffentlichen Verwaltung, in diesem Fall gewichtet?
3. Hat der Kanton Zürich abgesehen vom CLOUD Act auch die potenziellen Risiken durch extraterritoriale Zugriffsrechte von US-Behörden nach dem USA Patriot Act, USA Freedom Act und FISA (Foreign Intelligence Surveillance Act) analysiert? Zu welchem Schluss kommt diese Analyse?
4. Wie geht die Verwaltung im Kanton Zürich mit Personendaten und besonderen Personendaten (z. B. Daten des Justizvollzugs, Gesundheits-, Steuer- oder Sozialhilfedaten) um, werden diese ebenfalls über den Cloud-Dienst gespeichert oder geteilt?
5. Hat der Regierungsrat Massnahmen für die Speicherung solcher sensitiver Daten (auf geschlossenen Netzwerken) kantonaler Stellen verfügt oder ist er daran, dies zu tun, und wenn nicht, warum?
6. Welche gesetzlichen Grundlagen gelten für die Sicherheit von auf Cloud-Diensten gespeicherten Daten kantonaler Stellen und Institutionen (u. a. Polizei, Gerichte, Spitäler, Schulen, Universitäten etc.)? Bitte um Auflistung der betreffenden eidgenössischen und kantonalen Gesetze resp. Gesetzesparagraphen.
7. Gibt es eidgenössische respektive kantonale Verordnung(en) betreffend die Speicherung und Sicherheit von Daten staatlicher Institutionen und/oder die Speicherung und Sicherheit von auf Cloud-Diensten gespeicherter Daten? Falls nicht, hat sich oder nimmt sich der Regierungsrat diesen Fragen an respektive was und bis wann plant er in dieser Sache?
8. Was sind die Gründe der Regierung, dass sie sich bisher im Gegensatz zu anderen Kantonen gegen eine Erstellung einer eigenen Cloud oder eines Dienstes mit Server in der Schweiz entschieden hat?

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Die Anfrage Nicola Yuste, Zürich, Hans-Peter Amrein, Küsnacht, und Florian Heer, Winterthur, wird wie folgt beantwortet:

Zu Frage 1:

Nach § 23 Abs. 1 des Gesetzes über die Information und den Datenschutz (IDG, LS 170.4) verweigert das öffentliche Organ die Bekanntgabe von Informationen ganz oder teilweise oder schiebt sie auf, wenn eine rechtliche Bestimmung oder ein überwiegendes öffentliches oder privates Interesse entgegensteht.

Das Vertragswerk zwischen dem Kanton Zürich und Microsoft sieht vor, dass die vereinbarten Bestimmungen vertraulich sind und dass beide Parteien sich dadurch verpflichten, Informationen Dritten gegenüber nicht offenzulegen. Der Bekanntgabe der vertraglichen Informationen steht somit das überwiegende private Interesse von Microsoft an der Wahrung der im Vertrag enthaltenen Geschäftsgeheimnisse und sowie der Vertraulichkeit der getroffenen Abmachungen entgegen. Zudem hat auch der Kanton Zürich ein Interesse daran, seine vertraglichen Pflichten einzuhalten und hierdurch als zuverlässiger Vertragspartner anerkannt zu bleiben.

Zu Frage 2:

Das Interesse der Öffentlichkeit wird hoch gewichtet. Die Gründe, weshalb die Verträge nicht herausgegeben werden, sind in der Beantwortung der Frage 1 beschrieben. Um das Interesse der Öffentlichkeit einzubinden, wurde die kantonale Datenschutzbeauftragte in die Vertragserstellung mit Microsoft einbezogen.

Zu Frage 3:

Das Risiko solcher Zugriffe wurde vom Kanton ebenfalls analysiert. In der betreffenden Excel-Datei, mit der die Risikobeurteilung dokumentiert worden ist, ist diese Prüfung vorgenommen und dokumentiert worden, während die Prüfung nach dem US CLOUD Act in Schritt 2 und 3 erfolgt. Im Zentrum der Analyse zum US Foreign Intelligence Surveillance Act (FISA) steht Section 702 und die damit verbundene Executive Order (EO) 12333. Section 702 erlaubt US-Nachrichtendiensten, von in den USA ansässigen Internet-, Telefon- und Cloud-Providern die Herausgabe von Kommunikation und dazugehörigen Metadaten zu verlangen, wenn diese an eine oder von einer von ihnen nachrichtendienstlich aus Gründen der nationalen Sicherheit überwachten

Person übermittelt werden. Da Section 702 eine Massenüberwachung darstellt, die nicht gezielt gegen den Kanton Zürich durchgeführt wird, ist das Prüfschema in diesem Fall etwas anders als im Zusammenhang mit dem US CLOUD Act.

Die Ergebnisse dieser Analyse sind in das Gesamtergebnis der Prüfung eingeflossen. Im Falle der Geschäftsfalldaten in M365 (Beispiel: E-Mail mit Fallakten) entfallen von den 0,74 Prozentpunkten 0,60 Prozentpunkte auf die Analyse nach Section 702 FISA. Der gegenüber dem US CLOUD Act erhöhte Anteil lässt sich aus der Natur dieser Zugriffe erklären, die nicht gezielt gegen den Kanton erfolgen. Es handelt sich dabei um ein bloss theoretisches Risiko, weil verschiedene rechtliche, technische und faktische Gründe dem Zugriff nach Section 702 FISA entgegenstehen, da für einen solchen Zugriff bestimmte Voraussetzungen erfüllt sein müssen.

Zu Fragen 4 und 5:

RRB Nr. 542/2022 bezieht sich auf die Zulassung des Einsatzes der Cloud-Lösung M365 in der kantonalen Verwaltung. Für weitere Cloud-Lösungen besteht die Pflicht, die Restrisiken eines ausländischen Lawful Access analog zum Modell gemäss RRB Nr. 542/2022 zu ermitteln und in einem Informationssicherheits- und Datenschutzkonzept auszuweisen.

In die Anwendung von M365 werden nicht sämtliche Daten einbezogen. Die der IKT-Strategie unterstehenden Verwaltungseinheiten haben unter Berücksichtigung der sie betreffenden gesetzliche Grundlagen festzulegen, wie ihre Daten zu klassifizieren und wo diese abzulegen sind. Die Allgemeinen Nutzungsrichtlinien M365 (vgl. RRB Nr. 542/2022) legen fest, für welche Datenkategorien die einzelnen M365-Lösungen genutzt werden können.

Zu Frage 6:

In allen Kantonen und beim Bund gilt der Grundsatz, dass das öffentliche Organ in Bezug auf das Risiko einer Verletzung der Datensicherheit angemessene technische und organisatorische Massnahmen der Sicherheit treffen muss. Unter «Sicherheit» wird der Schutz der Vertraulichkeit, der Integrität und der Verfügbarkeit der Daten und mitunter auch die Nachvollziehbarkeit von deren Bearbeitung verstanden.

Konkret unterliegen die Verwaltungseinheiten des Kantons Zürich grundsätzlich dem IDG und der Verordnung über die Information und den Datenschutz (LS 170.41).

Nach § 7 Abs. 1 IDG muss das öffentliche Organ Informationen durch angemessene organisatorische und technische Massnahmen schützen. § 7 Abs. 2 IDG zählt die dabei zu beachtenden Schutzziele auf. § 7 Abs. 3 IDG hält fest, dass die zu treffenden Massnahmen sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik richten.

Ferner stellt das öffentliche Organ gemäss § 13 Abs. 1 und 2 IDG die Einhaltung der Datenschutzbestimmungen insbesondere durch Organisationsvorschriften sicher. Dies bezieht sich auf den Datenschutz insgesamt. Es kann zur Sicherstellung der Qualität und Informationsbearbeitung seine Verfahren, seine Organisation und seine technischen Einrichtungen durch eine unabhängige und anerkannte Stelle prüfen und bewerten lassen.

Im Zusammenhang mit der Beauftragung von Cloud-Providern ist ferner auf § 6 IDG zu verweisen, der es dem öffentlichen Organ erlaubt, die Bearbeitung von Informationen einem Dritten wie z. B. einem Cloud-Provider zu übertragen, sofern keine rechtliche Bestimmung oder vertragliche Vereinbarung dem entgegensteht.

Weitere Vorgaben zur Informatiksicherheit enthält die Verordnung über die Informationsverwaltung und -sicherheit (IVSV, LS 170.8). Sie regelt in Ausführung des IDG die Verwaltung und den Schutz von Informationen der öffentlichen Organe des Kantons. Sie bezieht sich nicht spezifisch auf Cloud-Angebote, ist aber beim Beizug entsprechender Provider ebenfalls zu beachten, so namentlich § 15 IVSV, der festhält, dass beim Beizug von Dritten das öffentliche Organ dafür zu sorgen hat, dass die Vorgaben der Verordnung eingehalten werden. Somit werden die Massnahmen zur Wahrung der Schutzziele in der IVSV etwas näher umschrieben: Details enthält sie aber ebenfalls keine. So wird lediglich verlangt, dass zum Schutz der Vertraulichkeit Verschlüsselung zum Einsatz kommt. In welcher Weise genau, wird nicht vorgeschrieben.

Für kantonale öffentliche Organe besteht ferner eine Allgemeine Informationssicherheitsrichtlinie (AISR), die mit RRB Nr. 795/2019 erlassen wurde und die der Umsetzung der genannten rechtlichen Vorgaben zur Informationssicherheit dient. Aus der AISR sind wiederum die Besonderen Informationssicherheitsrichtlinien (BISR) abgeleitet worden, welche die Ziele und Grundsätze der AISR konkretisieren (vgl. dazu auch RRB Nr. 1193/2020). Es handelt sich bei der AISR und den BISR allerdings nicht um gesetzliche Grundlagen im eigentlichen Sinne. Sie gelten für die kantonale Verwaltung, jedoch nicht für den Kantonsrat, die Gerichte, die ihnen angegliederten Einheiten und die selbstständigen Anstalten sowie auch nicht für die Gemeinden.

Zu Frage 7:

Gesetzliche Regelungen spezifisch für die Speicherung und Sicherheit von Cloud-Diensten gibt es keine und solche sind auch nicht geplant. Eine solche Regelung entspricht nicht der in der Rechtsetzung beim Bund und den Kantonen üblichen und bewährten Vorgehensweise. Diese beruht darauf, Grundsätzen zu regeln, die so weit wie möglich technologieneutral ausgestaltet sind, um mit den technischen Entwicklungen Schritt halten zu können.

Der Begriff «Cloud» ist ohnehin weder rechtlich noch technisch klar definiert. Letztlich geht es um die Nutzung von Anbietenden, die an definierten Standorten Rechenzentren betreiben, auf denen sie ihre Rechnerleistungen und Software in unterschiedlichen Ausprägungen anbieten.

Die eidgenössischen Räte haben im Dezember 2020 ein neues Informationssicherheitsgesetz (SR 128) erlassen. Die entsprechenden bundesrechtlichen Vorgaben werden im Kanton Zürich umzusetzen sein (vgl. ferner die Beantwortung der Frage 6).

Zu Frage 8:

RRB Nr. 542/2022 bezieht sich auf die Zulassung des Einsatzes der Cloud-Lösung M365 von Microsoft. Die Nutzung einzelner M365-Services (z. B. MS Teams) bedingt die Nutzung der Microsoft-Cloud. Die Erstellung einer eigenen Cloud oder eines Dienstes mit Server in der Schweiz fällt daher offensichtlich ausser Betracht.

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

Vor dem Regierungsrat
Die Staatsschreiberin:
Kathrin Arioli