Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich

KR-Nr. 336/2022

Sitzung vom 14. Dezember 2022

1644. Anfrage (Microsoft-365-Cloud-Lösungen, ist der Kanton Zürich ein verantwortungsvoller Datenbearbeiter und Dateneigentümer?)

Die Kantonsräte Lorenz Habicher und Valentin Landmann, Zürich, haben am 19. September 2022 folgende Anfrage eingereicht:

Der Kanton Zürich, vertreten durch das Amt für Informatik, hat im Sommer 2021 Verträge betreffend den Bezug von MS365-Services-Cloud-Lösungen mit Microsoft abgeschlossen. Die Grundlage dafür bildet ein Rahmenwerk, das die Schweizerische Informatikkonferenz (SIK) mit Microsoft für die öffentlichen Verwaltungen vereinbart haben. Im Rahmen der IKT-Grundversorgung bezieht der Kanton Zürich Leistungen aus den Rechenzentren von Microsoft und speichert dort auch Daten.

Das wirft in Bezug auf die Datensicherheit und den Zugriff ausländischer Behörden, dem Lawful Access und der geltenden Gesetzgebung über die Verletzung des Amtsgeheimnisses (Art.320 StGB), verbotene Handlungen für einen fremden Staat (Art.271 StGB) etc. doch einige Fragen auf, für deren Beantwortung wir dem Regierungsrat bereits danken:

1. Wie werden mit Blick auf Datenschutz und Informationssicherheit die heutigen und neu entstehenden Risiken von MS365 Cloud-Lösungen überwacht?
2. Welche Ressourcen werden zurzeit zur Datensicherheit und IT-Risikoreduktion in den Direktionen eingesetzt und wird ein Ausbau, spezifisch aufgrund von Cloud-Lösungen, neu ins Auge gefasst? Mit der Bitte um tabellarische Aufstellung nach Budget-Leistungsgruppen für die Jahre 2019, 2020 und 2021.
3. Die US-Behörden haben mehrfach Softwareanbieter und Betreiber von Rechenzentren zur Herausgabe von Kundendaten, dem Lawful Access / US Cloud Act, gezwungen. Stellen ausländische Gesetzgebung, die Existenz des Cloud Act und anderen Datenzugriffe ausländischer Strafverfolgungsbehörden keinen Hinderungsgrund für den Einbezug sämtlicher Daten, der IKT-Strategie unterstehenden Verwaltungseinheiten, im Zusammenhang mit dem geltenden IDG / StGB dar?

4. Welche Wahrscheinlichkeit, der Herausgabe von spezifischen Daten von Microsoft an die US-Behörden zieht der Regierungsrat in Betracht und wie gedenkt sich der Kanton Zürich oder die betroffene Behörde dagegen zur Wehr zu setzen? Mit der Bitte, die Beurteilungsmethode oder Berechnungsgrundlage zu erläutern und mögliche Massnahmen zu benennen.
5. Beschaffungs- und Vertragswesen des Kantons Zürich unterstehen grundsätzlich dem Öffentlichkeitsprinzip. Anscheinend wurde ein Zusatz der Datenschutzbeauftragten des Kantons Zürich zu diesen Verträgen mit Microsoft verfasst. Wie lautet dieser und warum sind die Verträge mit Microsoft vertraulich und nicht öffentlich zugänglich?

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Die Anfrage Lorenz Habicher und Valentin Landmann, Zürich, wird wie folgt beantwortet:

Zu Frage 1:

Um den Risiken betreffend die Anwendung von M365 entgegenzuwirken, wurde mit RRB Nr. 542/2022 die Stelle einer oder eines Cloud-Sicherheitsbeauftragten geschaffen. Die oder der Cloud-Sicherheitsbeauftragte wird in die Organisation des IKT-Sicherheitsbeauftragten eingebunden. Sie oder er ist auf Stufe Kanton tätig und Mitglied der Fachgruppe Informationssicherheit. Die oder der Cloud-Sicherheitsbeauftragte verantwortet insbesondere die Prozesse zur Sicherstellung der Cloud Compliance, auditiert bestehende Cloud-Lösungen und orientiert in regelmässigen Abständen über Veränderungen der Risikosituation im Bereich Informationssicherheit und Datenschutz. Sie oder er erarbeitet Massnahmen zur Minimierung von Risiken der Datenhaltung in der Cloud und beantragt deren Umsetzung. Im Weiteren berät die oder der Cloud-Sicherheitsbeauftragte die Direktionen und die Staatskanzlei bei Fragen zu Cloud-Vorhaben und führt in deren Auftrag die Berechnung zur Bestimmung der Restrisiken aus einem ausländischen Lawful Access durch.

Zu Frage 2:

Mit RRB Nr. 676/2022 hat der Regierungsrat die Cybersicherheitsstrategie für den Kanton Zürich festgesetzt, die u. a. den Aufbau eines kantonalen Zentrums für Cybersicherheit vorsieht. Ein Vergleich der heutigen Situation mit der Anzahl Stellen, die sich künftig, nach Um-

setzung der Cybersicherheitsstrategie in der Sicherheitsdirektion und der Finanzdirektion sowie den anderen Direktionen und der Staatskanzlei, mit den Fragen der Cybersicherheit auseinandersetzen werden, ergibt folgendes Bild (vgl. RRB Nr. 676/2022, S. 20):

	Heutige Anzahl Stellen	Anzahl Stellen nach der Umsetzung der Cybersicherheitsstrategie
Sicherheitsdirektion (einschliesslich SOC KAPO)	**5**	**6**
Finanzdirektion	**8**	**25**
– davon Stellen der Cyber-Koordinatorin oder dem Cyber-Koordinator (Leistungsgruppe Nr. 4620) unterstellt	1	11
– davon Stellen der Leiterin oder dem Leiter Cyber Defence Center des AFI (Leistungsgruppe Nr. 4610) unterstellt	7	14
Fünf weitere Direktionen und Staatskanzlei	**6**	**6**
Total	**19**	**37**

Die vorstehende Tabelle gibt Aufschluss über die Situation in den Direktionen und der Staatskanzlei. Auf eine zusätzliche Detailierung wird aus Gründen der Komplexität verzichtet.

Die Grösse der zukünftigen Cyberorganisation des Kantons Zürich ist vergleichbar mit der Grösse der Cyberorganisationen des Kantons Waadt sowie des Bundes (vgl. RRB Nr. 676/2022, S. 21):

Verwaltung/Organisation	Anzahl Mitarbeitende mit Cybersicherheitsaufgaben in zentraler Sicherheitsorganisation	Anzahl Mitarbeitende mit Cybersicherheitsaufgaben dezentral in den Departementen, Direktionen und Ämtern	Grösse der Organisation (Anzahl Mitarbeitende)	Anzahl betreute Arbeitsplätze	Anzahl betreute Applikationen	Anzahl Einwohner/innen
Kanton Zürich (Soll gemäss RRB)	24	13	30 000	20 000	1 500	1 550 000
Kanton Waadt (Stand Februar 2022)	30		15 000	15 000	3 000	800 000
Bund (Stand Februar 2022)	40	25 Vollzeitstellen; 76 Teilzeitstellen	35 000	43 000	1 200	8 600 000

Zu Frage 3:

In der Praxis ist ein Szenario, wonach eine US-Behörde einen Zugriff auf Daten der kantonalen Verwaltung erwirken will, höchst unwahrscheinlich. So ist es im Bereich der öffentlichen Hand gemäss Auskunft von Microsoft vom 7. Dezember 2021 noch nie zur Offenlegung von Daten europäischer Kunden durch Microsoft gekommen.

Es werden auch nicht sämtliche Daten einbezogen. Die der IKT-Strategie unterstehenden Verwaltungseinheiten haben unter Berücksichtigung der sie betreffenden gesetzlichen 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.

Die getroffenen Schutzmassnahmen, einschliesslich der Allgemeinen Nutzungsrichtlinien M365 werden in ihrer Gesamtheit und mit Blick auf die Risiken und Schutzziele regelmässig evaluiert und bei Bedarf angepasst.

Zu Frage 4:

Wie in RRB Nr. 542/2022, Erwägung 4, dargelegt, wurde für die Risikobeurteilung eines ausländischen Lawful Access im Falle von M365 die Berechnungsmethode von David Rosenthal verwendet (vgl. dazu David Rosenthal, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter vom 10. August 2020).

Die Beurteilung erfolgte für zwei verschiedene Kategorien von Daten, da für sie ein unterschiedliches Risikoprofil besteht.

Bei Geschäftsfalldaten handelt es sich um Daten, die grundsätzlich in Geschäftsverwaltungssystemen lokal abgelegt oder in Fachanwendungen bearbeitet werden. Diese Daten sind möglicherweise von grösserem Interesse für einen ausländischen Zugriff. Werden Dokumente in diesen Anwendungen erstellt oder von dort geöffnet, geschieht auch dies lokal, d. h. Word, Excel und PowerPoint laufen auch in diesen Fällen lokal und nicht in der Cloud. Allerdings ist ein Versand über E-Mail oder ein Austausch über die M365-Cloud-Lösung möglich. Die Mitarbeitenden werden durch entsprechende Weisungen und Reglemente verpflichtet, in diesen Fällen die zusätzliche Verschlüsselung zu nutzen. Für Microsoft erkennbar sind der Betreff des E-Mails sowie Senderinnen und Sender und Empfängerinnen und Empfänger, nicht jedoch der Inhalt des E-Mails.

Die zweite Datenkategorie wurde in der Beurteilung mit «normale Daten» bezeichnet. Bei diesen Daten kommen die Dienste der M365-Cloud-Lösung breiter zum Einsatz, beispielsweise im Austausch über E-Mail oder die Zusammenarbeit in Projekten über Teams und Ablage von Daten in Speicherlaufwerken der Cloud.

Die Risikobeurteilung kommt zum Ergebnis, dass die prognostizierte Wahrscheinlichkeit eines erfolgreichen ausländischen Lawful Access in Bezug auf Daten in Geschäftsverwaltungssystemen in der Betrachtungsperiode von fünf Jahren bei 0,74% liegt. Bei diesem Wert braucht es 1552 Jahre, damit es – statistisch gesehen – mit einer Wahrscheinlichkeit von 90% mindestens einmal zu einem erfolgreichen Lawful Access kommt. Bei normalen Daten liegt diese Eintrittswahrscheinlichkeit bei 0,95%. Bis mit einer Wahrscheinlichkeit von 90% einmal ein Lawful Access erfolgt, müssten folglich 1206 Jahre vergehen. Die Wirksamkeit der getroffenen Schutzmassnahmen ist somit in beiden Fällen ausserordentlich hoch.

Demnach ist es höchst unwahrscheinlich, dass US-Behörden über Microsoft auf vom Kanton Zürich im Rahmen von M365 in der Cloud gespeicherte Daten ohne dessen Einwilligung zugreifen können und werden.

Microsoft unterhält zudem eine Auswahl an wirksamen rechtlichen, technischen und organisatorischen Kontrollmechanismen, um das Risiko eines Lawful Access zu minimieren:

- Microsoft verpflichtet sich vertraglich, eine Strafverfolgungsbehörde immer direkt an die Kundinnen und Kunden zu verweisen. Wenn Microsoft gezwungen wird, verarbeitete Daten an Strafverfolgungsbehörden weiterzugeben, benachrichtigt Microsoft die Kundin oder den Kunden unverzüglich.
- Microsoft unterzieht alle Behördenanfragen einer juristischen Vorprüfung und lehnt diejenigen Anfragen ab, die ungültig sind oder formale Fehler aufweisen. Im Falle eines Verbots zur Kundeninformation garantiert Microsoft vertraglich, alle rechtmässigen Anstrengungen zu unternehmen, um die Offenbarungsanordnung abzuwehren. Dies kann aufgrund von Rechtsmängeln oder Konflikten mit dem schweizerischen Recht geschehen.
- Microsoft bietet keiner Strafverfolgungsbehörde einen direkten, indirekten, pauschalen oder uneingeschränkten Zugriff auf gespeicherte Daten sowie auf die für die Sicherung der verarbeiteten Daten verwendeten Verschlüsselungsschlüssel. Auch wird die Möglichkeit, eine solche Verschlüsselung zu umgehen, verwehrt.
- Microsoft veröffentlicht alle sechs Monate einen sogenannten Law Enforcement Request Report, um Transparenz über die Art und den Umfang solcher Vorfälle zu gewährleisten (https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report?culture=de-de&country=DE).

Zu Frage 5:

Nach § 23 Abs. 1 des Gesetzes über die Information und den Datenschutz (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 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 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.

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

Vor dem Regierungsrat
Die Staatsschreiberin:
Kathrin Arioli