Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich

KR-Nr. 271/2021

Sitzung vom 27. Oktober 2021

1176. Anfrage (Alibaba – Wo werden Daten aus dem Kanton Zürich gespeichert und verarbeitet?)

Kantonsrat Erich Vontobel, Bubikon, Kantonsrätin Erika Zahler, Boppelsen, und Kantonsrat Martin Huber, Neftenbach, haben am 5. Juli 2021 folgende Anfrage eingereicht:

Wie kürzlich bekannt wurde, wird die Schweiz in Zukunft voraussichtlich einen Teil ihrer Daten in China beim Anbieter Alibaba speichern und verarbeiten lassen. Alibaba hat sich den prestigeträchtigen Auftrag mit einem Billigangebot ergattert und damit mit der Schweiz einen sehr wichtigen Referenzkunden gewonnen. Obschon der haushälterische Umgang mit Steuergeldern löblich ist, ist dieser Schritt politisch brisant und löst berechtigte Bedenken aus. Es ist kaum bestritten, dass zum Beispiel die USA über den Geheimdienst ihre Unternehmen als Einfallstor zu sensiblen Daten anderer Länder benutzt. Wenn dies aber in Zukunft auch China mit unseren Daten machen kann, ist das nicht dasselbe. Vergleicht man Demokratie und Rechtsstaatlichkeit der beiden Länder, ist klar, warum.

Vor diesem Hintergrund bitten wir den Regierungsrat um die Beantwortung folgender Fragen:

1. Wo werden Daten aus dem Kanton Zürich aktuell gespeichert und verarbeitet? Bitte um tabellarische Übersicht mit Angabe von Anbieter und Art der betroffenen Daten.
2. Was sind mittel- und langfristige Pläne des Regierungsrates betreffend Datenspeicherung und -verarbeitung?
3. Wie sieht die Ausschreibepraxis des Kantons Zürich in Sachen Cloud-Diensten bezüglich Datenschutz aus?
4. Welches Gewicht haben Vorschläge und Empfehlungen der Zürcher Datenschutzbeauftragten, wenn es um die mögliche Speicherung und Verarbeitung von Daten im Ausland geht?
5. Werden inländische Anbieter von Cloud-Diensten verpflichtet, die Bürgerdaten in der Schweiz derart zu speichern, dass sie 100% vor ausländischem Zugriff gesichert sind?
6. Gibt es Daten, welche der Kanton Zürich mit dem Bund austauscht und deren Ort der Verarbeitung und Speicherung nicht durch den Kanton Zürich beeinflusst werden kann? Wenn ja, was für Daten konkret?

7. Falls der Kanton Zürich Daten im Ausland speichert bzw. verarbeitet: Was sind die Szenarien im Fall, dass solche Cloud-Dienste unterbrochen oder für längere Zeit nicht mehr verfügbar sind? Wie wurden diese Szenarien getestet?
8. Noch nie war es in der Geschichte der Informatik so günstig wie heute, selber Daten zu speichern. Das ruft geradezu danach, solches in der Schweiz zu tun. Was für Bemühungen unternimmt der Kanton diesbezüglich im eigenen Kanton oder beim Bund?
9. Nimmt der Kanton Zürich an der «Cyber Polygon 2021» teil, mit der das WEF eine globale Cyberattacke simulieren und damit die Welt auf solche Ereignisse vorbereiten will? Gibt es zur allfälligen Teilnahme Informationen?

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Die Anfrage Erich Vontobel, Bubikon, Erika Zahler, Boppelsen, und Martin Huber, Neftenbach, wird wie folgt beantwortet:

Zu Frage 1:

Der Kanton Zürich speichert und verarbeitet seine Daten gemäss der gesetzlichen Grundlage, dem Gesetz über die Information und den Datenschutz vom 12. Februar 2007 (LS 170.4), sowie gemäss den Vorgaben der Datenschutzbeauftragten des Kantons Zürich und den Vorgaben im Bereich Informationssicherheit.

Die Daten des Kantons Zürich liegen mehrheitlich in eigenen Rechenzentren (on premise) oder in privaten Rechenzentren von Lieferanten (private cloud) mit Datenstandort Schweiz. Vereinzelt kommen im Kanton Zürich auch öffentliche Cloud-Lösungen (public cloud) zum Einsatz mit Datenstandort Europa, konkret Deutschland und Niederlande. Auf eine tabellarische Übersicht wird aus Schutzgründen im Bereich Informationssicherheit bewusst verzichtet.

Zu Frage 2:

Mittel- und langfristig verfolgt der Regierungsrat eine duale Strategie. Mit dem Betrieb von zwei redundanten Rechenzentren werden Mittel für die Datenspeicherung und -verarbeitung bereitgestellt, die insbesondere gemäss den gesetzlichen Vorgaben eine Datenhaltung in den kantonseigenen Rechenzentren verlangen.

Parallel dazu kommen Cloud-Anbieter bzw. Cloud-Lösungen zur Anwendung. Bereits heute werden viele Lösungen nur noch aus der Cloud angeboten und dies wird sich in der Zukunft verstärken. Beim Einsatz solcher Public- oder Private-Cloud-Lösungen werden die gesetzlichen Anforderungen eingehalten.

Zu Frage 3:

Öffentliche Ausschreibungen sind grundsätzlich lösungsoffen auszugestalten. Cloud-Dienste müssen wie jede andere Lösung auch die Vorgaben des Datenschutzes und der Informationssicherheit erfüllen. Zusätzlich müssen anbietende Unternehmen darlegen, wie die Vorgaben eingehalten werden und welche Datenbearbeitungsorte möglich sind. Ferner sind bei Vertragsabschlüssen die datenschutzrechtlichen Allgemeinen Geschäftsbedingungen des Kantons (AGB Auslagerung Informatikleistungen, AGB Datenbearbeitung durch Dritte) verbindlich (vgl. RRB Nrn. 670/2015).

Zu Frage 4:

Die Direktionen und die Staatskanzlei halten sich an die Vorgaben der Datenschutzbeauftragten.

Zu Frage 5:

Massgebend sind die Vorgaben des Datenschutzes und der Informationssicherheit. Ist der Zugriff auf Informationen und damit die Datenbearbeitung ausserhalb der Schweiz möglich, ist zu klären, ob es sich ausschliesslich um Staaten mit angemessenem Datenschutzniveau handelt. Ist dies nicht der Fall, müssen zusätzliche Massnahmen getroffen werden (z. B. Verschlüsselung der Daten) oder es muss auf die entsprechende Auslagerung verzichtet werden.

Zu Frage 6:

In Geschäftsbereichen, bei denen die Kantone im Auftrag des Bundes Vollzugsaufgaben wahrnehmen, z. B. Einwohnerkontrolle, Regionale Arbeitsvermittlung, Arbeitslosenversicherung, Migration usw., ist der Kanton Zürich verpflichtet, mit dem Bund Daten auszutauschen und auf den Systemen des Bundes die Verarbeitung und Speicherung der Daten vorzunehmen. Dabei kann es sich auch um besonders schützenswerte Personendaten handeln.

Zu Frage 7:

Bei Daten, die in einer ausländischen Cloud gespeichert oder verarbeitet werden, sind die Massnahmen grundsätzlich die gleichen wie bei einer Speicherung oder Verarbeitung im Inland. Die Anforderungen an die Verfügbarkeit eines Services und damit die Vorgaben an das IT-Service Continuity Management (IT-SCM) werden im Business Continuity Management definiert. Auch müssen die Nutzerorganisationen Notfallszenarien entwickeln, wie mit einem Ausfall oder Verlust von Daten umgegangen werden muss. Zudem ist auf RRB Nr. 172/2021 zu verweisen, wonach Grundlagen für ein integrales Risikomanagement geschaffen werden sollen (Empfehlung 8), das die Anforderungen an ein IT-SCM beschreibt.

Aufgrund der Anforderungen der Nutzerorganisation und in Abstimmung mit den Vorgaben der Zürcher Datenschutzbeauftragten lässt sich entscheiden, wo ein Service überhaupt betrieben werden kann (eigene Datenhaltung, Cloud Schweiz, Cloud Ausland). Mittels eines IT-SCM-Systems, das sich derzeit im Aufbau befindet, werden alle Services der IKT-Grundversorgung überprüft, und wo nötig werden Massnahmen getroffen, um die geforderte Servicequalität sicherstellen zu können. Wenn ein Cloud-Dienst unterbrochen oder für längere Zeit nicht mehr verfügbar ist, werden Datensicherungsstrategien angewendet, bei denen die Cloud-Datenbestände auf den Systemen in den eigenen Rechenzentren gesichert werden.

Ein weiterer Ansatz ist, dass ein Notsystem in den eigenen Rechenzentren aufgebaut wird, mit dem der Notfallbetrieb beim Ausfall eines Cloud-Dienstes gewährleistet werden kann. Ein wesentlicher Bestandteil eines IT-SCM-Systems besteht darin, die Szenarien laufend zu überprüfen und mittels Testszenarien zu verifizieren.

Zu Frage 8:

Es trifft zu, dass die Medien für die Datenspeicherung immer günstiger werden. Allerdings steigen die zu speichernden Datenvolumen massiv an. Deshalb wird die Datenhaltung insgesamt nicht günstiger. In der Schweiz gibt es weitere Faktoren, welche die Kosten der Datenhaltung beeinflussen, wie insbesondere Infrastrukturkosten und Lohnkosten. Entsprechend wird es auch zukünftig Angebote von ausländischen Anbietern geben, die in der preislichen Gestaltung interessant und mit den entsprechenden Auflagen und Vorkehrungen nutzbar sind.

Der Kanton Zürich baut zurzeit zwei Rechenzentren auf, in denen die kantonseigenen IT-Infrastrukturen konsolidiert werden und in denen ein sicherer Betrieb für sensitive Applikationen und Daten zur Verfügung stehen wird.

Zu Frage 9:

Nein, der Kanton Zürich nimmt an der erwähnte Veranstaltung nicht Teil.

Der Fokus der Veranstaltung «Cyber Polygon 2021» liegt bei international tätigen Unternehmen aus der Privatwirtschaft. Es gibt vergleichbare internationale Übungen im Behörden- bzw. staatlichen Umfeld.

Gemäss der Empfehlung des Sicherheitsverbundes Schweiz erarbeitet das Amt für Informatik zusammen mit der Kantonspolizei Zürich, der Staatsanwaltschaft sowie dem Bevölkerungsschutz einen Vorschlag für die kantonale Cyberorganisation. Es gilt festzulegen, wie die Verwaltung und der Kanton Zürich langfristig mit dem Thema Cyberrisiken umgehen. Eine Aufgabe der kantonalen Cyberorganisation wird die Vernetzung im Bereich Cybersicherheit mit dem Bund (NCSC), an-

deren Kantonen sowie den Städten und Gemeinden, der Wirtschaft und Hochschulen im Kanton Zürich sein. Mit «mehr Sicherheit» im Kanton Zürich soll ein Wettbewerbsvorteil geschaffen werden, um die Attraktivität des Wirtschaftsstandortes Zürich zu steigern.

Ein Vorschlag für die zukünftige Cyberorganisation im Kanton Zürich soll dem Regierungsrat 2022 vorgelegt werden.

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

Vor dem Regierungsrat
Die Staatsschreiberin:
Kathrin Arioli