Auszug aus dem Protokoll
des Regierungsrates des Kantons Zürich

Sitzung vom 30. März 2022

542. Einsatz von Cloud-Lösungen in der kantonalen Verwaltung (Microsoft 365), Zulassung

1. Ausgangslage

In den letzten Jahren hat sich die Informationstechnologie stark weiterentwickelt. Mit dem Angebot von Cloud-Lösungen entstand ein grundlegend neues, globales Verständnis für den Bezug von Informatikleistungen. Cloud-Lösungen ermöglichen, jederzeit bedarfsgerecht, schnell und flexibel auf standardisierte IT-Angebote zuzugreifen.

Namhafte Softwarehersteller wie Microsoft, Google, Amazon und Apple haben ihre Geschäftsstrategie in Richtung Cloud ausgerichtet. Zukünftige Dienstleistungen werden nur noch in der Cloud angeboten. Gemäss Gartner, einem der weltweit führenden Unternehmen für Analysen über die Entwicklungen in der IT, werden bis 2023 70% aller IT-Ressourcen von Unternehmen in Cloud-Infrastrukturen und -Plattformdiensten bereitgestellt, da Unternehmen durch die Einführung von Cloud Computing bedeutende Fortschritte in den Bereichen IT-Modernisierung, Effizienz, Sicherheit und Produktivität erzielen (vgl. «Cloud End-User Buying Behavior Survey 2020»). Die Investitionen der grossen Softwarehersteller erfolgen denn auch vorzugsweise im Bereich von Cloud-Lösungen. Der Support für lokal betriebene Anwendungen (Fachsprache «on premises») wird Schritt für Schritt zurückgefahren oder ganz eingestellt.

2. Cloud-Lösungen in der IKT-Grundversorgung

In der kantonalen Verwaltung wird im Rahmen der Umsetzung der kantonalen IKT-Strategie (RRB Nr. 383/2018) eine standardisierte IKT-Grundversorgung bereitgestellt. Die IKT-Grundversorgung schafft bestmögliche Voraussetzungen für die digitale Transformation der kantonalen Verwaltung (Ziff. 5 IKT-Strategie). Die Erweiterung der bestehenden On-Premises-Anwendungen durch Cloud-Lösungen ermöglicht eine flexible, skalierbare, performante und sicherere Infrastruktur, die den Kanton Zürich in die Lage versetzt, zeitnah auf sich ändernde Geschäftsanforderungen zu reagieren. Microsoft bietet mit Microsoft 365 (M365) eine Cloud-Lösung mit einem breiten Angebot an Diensten an. Die wichtigsten Dienste sind «Exchange Online» als Cloud-Alternative zur On-Premises-Variante «Microsoft Exchange» und «Microsoft Teams», das ausschliesslich als Cloud-Dienst angeboten wird.

Die IKT-Strategie wird in einem Programm mit zwölf Projekten nach der Projektmethodik HERMES umgesetzt (RRB Nr. 625/2019). Das methodische Vorgehen stellt sicher, dass die erforderlichen Ergebnisse entlang des Projektverlaufs zur Einführung neuer Lösungen erarbeitet werden. Dazu gehören auch die Rechtsgrundlagenanalyse und die für die Informationssicherheit und den Datenschutz erforderlichen Abklärungen. Die Rechtsgrundlagenanalyse beschreibt die für das Projektergebnis einzuhaltenden Rechtsgrundlagen und den allfälligen Bedarf für deren Änderung. Im Zusammenhang mit der Beschaffung von Lösungen für die neue standardisierte IKT-Grundversorgung sind insbesondere folgende Rechtsgrundlagen von Bedeutung:

- Gesetz über die Information und den Datenschutz (IDG; LS 170.4), insbesondere §§ 6 (Bearbeiten im Auftrag), 7 (Informationssicherheit) und 10 (Datenschutz-Folgenabschätzung und Vorabkontrolle), sowie
  - Verordnung über die Information und den Datenschutz (IDV; LS 170.41)
  - Verordnung über die Informationsverwaltung und -sicherheit (IVSV; LS 170.8)
- Gesetz über die Auslagerung von Informatikleistungen (LS 172.71), insbesondere §§ 2 (Sicherung der Verwaltungstätigkeit) und 3 (Amtsgeheimnis und Datenschutz)

Die Rechtsgrundlagenanalyse wurde als projektübergreifende Aufgabe innerhalb des IKT-Programms erstellt (RRB Nr. 625/2019, Ziff. 2). Im Zusammenhang mit der neuen IKT-Organisation und deren Aufgaben zeigt sich Änderungsbedarf. Dieser wird in einem nächsten Schritt in einem Normkonzept vertieft. In Bezug auf die Einführung von Cloud-Lösungen müssen keine Rechtsgrundlagen geändert oder geschaffen werden. Es besteht kein Regelungsbedarf, sondern die geltenden Bestimmungen sind bei der Einführung einzuhalten.

Die für ein konkretes Vorhaben bestehenden Anforderungen an die Informationssicherheit und den Datenschutz werden mit der Schutzbedarfsanalyse bereits vor der Projektfreigabe erhoben. Ergibt sich ein erhöhter Schutzbedarf, müssen ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) erstellt, die Massnahmen festgelegt sowie die Restrisiken aufgezeigt werden. Mit der Allgemeinen Informationssicherheitsrichtlinie (AISR, RRB Nr. 795/2019) und den auf deren Grundlage für verschiedene Regelungsbereiche erarbeiteten Besonderen Informationssicherheitsrichtlinien (BISR), besteht ein Regelwerk, das die technischen und organisatorischen Massnahmen zum Schutz von Informationen definiert, um die Schutzziele gemäss § 7 IDG sicherzustellen.

Das Schutzziel der Vertraulichkeit (§ 7 Abs. 2 lit. a IDG; Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen) stellt insbesondere auch sicher, dass personenbezogene Daten nur von Personen bearbeitet werden, die dazu berechtigt sind. Da mit den Lösungen der IKT-Grundversorgung Personendaten bearbeitet werden können, werden die für die Informatiklösungen erarbeiteten ISDS-Konzepte nach Massgabe von § 10 IDG im Rahmen der Vorabkontrolle der Datenschutzbeauftragten des Kantons Zürich zur Prüfung unterbreitet.

Bei Cloud-Lösungen bestehen grundsätzlich nicht höhere Risiken für die Informationssicherheit und den Datenschutz als bei On-Premises-Lösungen. Das Risikoprofil kann sich aber unterscheiden. Während Schutzziele wie Verfügbarkeit in der Cloud grundsätzlich besser erreicht werden können, gibt es in Bezug auf Cloud-Lösungen von ausländischen Unternehmen ein Risiko im Bereich «Lawful Access». Gemeint ist der behördliche Zugriff, der sich auf einen Rechtserlass stützt und ein Unternehmen unter bestimmten Voraussetzungen zur Herausgabe von Kundendaten zwingt. Ein solcher Zugriff stellt im Eintretensfall – genau wie ein illegaler Zugriff durch Dritte wie Hacker oder kriminelle Organisationen – eine unrechtmässige Datenbearbeitung im Sinne des IDG dar.

Bei Cloud-Anbietern mit Sitz oder Muttergesellschaften in den USA bildet der CLOUD Act (Clarifying Lawful Overseas Use of Data Act) die rechtliche Grundlage für einen möglichen Zugriff auf Kundendaten.

3. Lawful Access in Bezug auf M365 (CLOUD Act)

Der CLOUD Act erlaubt US-Strafverfolgungsbehörden, zur Aufklärung oder Verfolgung schwerer Straftaten («serious crimes») wie beispielsweise Cyberkriminalität, Diebstahl von Geschäftsgeheimnissen oder Terrorismus von US-Unternehmen die Herausgabe von Daten zu verlangen, die diese in ihrem Besitz oder unter ihrer Kontrolle haben. Dies gilt auch dann, wenn sich die entsprechenden Daten im Ausland befinden, was dem Gesetz einen extraterritorialen Anwendungsbereich verleiht.

Ein IT-Dienstleister hat das Recht, gerichtlich gegen einen Durchsuchungsbefehl der US-Strafverfolgungsbehörden vorzugehen, wenn dessen Befolgung einschlägiges Recht verletzt. Der IT-Dienstleister ist somit nicht automatisch verpflichtet, Kundendaten an US-Ermittlungsbehörden herauszugeben. Ebenso müssen Strafverfolgungsbehörden in den USA vorgängig eine unabhängige richterliche Anordnung einholen, die das Vorliegen eines verbrecherischen Sachverhalts bestätigt. Erst dann kann ein Durchsuchungsbefehl ausgestellt werden.

Im Rahmen der IKT-Grundversorgung wird der Kanton Zürich Leistungen aus schweizerischen Rechenzentren von Microsoft beziehen und dort Daten speichern. Der Kanton schliesst seinen Vertrag mit der irischen Gesellschaft von Microsoft. Microsoft untersteht als US-amerikanisches Unternehmen dem CLOUD Act und ist beim Vorliegen einer entsprechenden Verfügung zum Handeln verpflichtet. Dies bedeutet, dass die US-amerikanische Strafverfolgung Microsoft zur Offenbarung von spezifischen Daten auffordern kann.

In der Praxis ist ein derartiges Szenario 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.

Microsoft unterhält 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 Kundin oder den 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 (microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report?culture=de-de&country=DE).

Der Kanton Zürich, vertreten durch das Amt für Informatik, hat im Juni 2021 Verträge mit Microsoft abgeschlossen. Diese bilden den Rahmen für den Bezug von M365-Online-Diensten. Grundlage des Vertrags bildet ein Rahmenwerk, das die Schweizerische Informatikkonferenz mit Microsoft für die öffentlichen Verwaltungen vereinbart hat. Die Ver-

tragsverhandlungen wurden von der Datenschutzbeauftragten des Kantons Zürich begleitet. Der Kanton Zürich hat das Vertragswerk mit einer von der Datenschutzbeauftragten gestützten Ergänzung abgeschlossen, nachdem die Datenschutzbeauftragte am 23. Juni 2021 schriftlich erklärt hatte, dass die datenschutzrechtlichen Anforderungen mit Microsoft auf vertraglicher Ebene erfüllt sind.

4. Risikobeurteilung Lawful Access für M365

Für die Risikobeurteilung eines ausländischen Lawful Access im Falle von M365 wurde 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 Berechnungsmethode zur strukturierten Ermittlung der Eintrittswahrscheinlichkeit eines erfolgreichen Lawful Access durch eine ausländische Behörde bei einem Cloud-Vorhaben ist seit 2020 unter einer freien Lizenz publiziert und wurde durch die International Association of Privacy Professionals (IAPP) übernommen. Die Berechnungsmethode hat sich als Instrument im Schweizer Finanzsektor etabliert und wird unter anderem auch von der Zürcher Kantonalbank im Zusammenhang mit der Einführung von M365 angewendet.

Die Risikoberechnung für M365 für die kantonale Verwaltung wurde in einem Workshop mit juristischen und technischen Fachexpertinnen und Fachexperten aus dem Amt für Informatik, der Staatsanwaltschaft, dem kantonalen Steueramt, der Staatskanzlei und der Kantonspolizei durchgeführt. Für die statistischen Berechnungen wurden ferner vom Bundesamt für Justiz Zahlen aus der US-Rechtshilfe erhoben, ergänzt mit Erfahrungswerten der dortigen Spezialistinnen und Spezialisten im Zusammenhang mit abgelehnten und nicht gestellten Gesuchen von US-Behörden.

Die Beurteilung des Restrisikos erfolgte in Bezug auf die für den neuen digitalen Arbeitsplatz relevanten Anwendungen Office (Word, Excel, PowerPoint und OneNote), Kommunikation und Kollaboration (Teams und SharePoint Online), E-Mail und Kalender (Exchange Online und Outlook), Aufgaben und Projektmanagement (Planner und Whiteboard) sowie Cloud-Speicher (OneDrive). Im Weiteren berücksichtigt die Berechnung die technischen und organisatorischen Massnahmen zur Absicherung der Daten in der Microsoft-Cloud M365. So sieht beispielsweise die Implementation von Exchange Online eine zusätzliche Verschlüsselungsmöglichkeit vor, bei der die Schlüsselhoheit ausschliesslich beim Kanton Zürich liegt und durch eine On-Premises-Infrastruktur sichergestellt wird. Ferner sind auch Faktoren wie das Interesse der ausländischen Behörden an den Daten und die rechtlichen Vo-

raussetzungen für einen Lawful Access berücksichtigt. Das nachfolgend beschriebene Restrisiko des Lawful Access ist der Massstab dafür, wie gut das gewählte Massnahmenbündel vor einem solchen Zugriff schützt.

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 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 Sender 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 in der 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 Einwilligung des Kantons zugreifen können und werden. Die Ergebnisse der Risikobeurteilung sind in einem Memorandum dokumentiert (Memorandum David Rosenthal, Sarah Bischof vom 24. März 2022 betreffend Berechnung des ausländischen Lawful Access / US CLOUD Act).

5. Risikobeurteilung eines Lawful Access bei weiteren Cloud-Lösungen

Wie erwähnt ist davon auszugehen, dass die meisten Softwareanbieter zunehmend nur noch für die Cloud weiterentwickeln und ihre Leistungen teilweise oder ausschliesslich in der Cloud anbieten. Dies gilt nicht nur für Lösungen der IKT-Grundversorgung, sondern auch für Dienste und Funktionalitäten im Bereich der Kantons- und Fachapplikationen.

Die Frage, wie das Restrisiko eines Lawful Access zu bewerten ist, stellt sich durch die wachsende Verbreitung von Cloud-Lösungen folglich immer häufiger und ist für die kantonale Verwaltung mit Blick auf die Digitalisierungsbestrebungen von grundlegender Bedeutung. Aus diesem Grund wird mit dem vorliegenden Beschluss ein standardisiertes Vorgehen für die Risikobeurteilung definiert.

Das Modell von David Rosenthal zur Ermittlung der Restrisiken eines Lawful Access ist breit abgestützt und anerkannt. Es wird deshalb für die Risikobeurteilung beim Einsatz von Cloud-Lösungen in der kantonalen Verwaltung als Standard festgelegt. Das Restrisiko und die durchgeführten Berechnungen zum Lawful Access sind in den ISDS-Konzepten der entsprechenden Cloud-Lösungen auszuweisen.

In Bezug auf das Risiko des Lawful Access gilt dabei das Folgende: Liegt die 90%-Eintrittswahrscheinlichkeit eines erfolgreichen Lawful Access bei über 100 Jahren, wird der Einsatz der Cloud-Lösung zugelassen. Wenn diese unter 100 Jahren liegt, sind die Direktionen und die Staatskanzlei verpflichtet, dem Regierungsrat die Zulassung der risikobewerteten Cloud-Lösung zu beantragen.

Diese Regelung bietet den Direktionen und der Staatskanzlei eine einfache und effiziente Möglichkeit im Umgang mit dem Restrisiko eines ausländischen Lawful Access. Sie entbindet die zuständige Stelle aber nicht, die übrigen Risiken im Zusammenhang mit der Cloud-Lösung im Rahmen des ISDS-Konzepts zu bewerten und ebenfalls auszuweisen.

6. Weitere Risiken bei Cloud-Lösungen im Allgemeinen und M365 im Besonderen (ISDS-Konzepte)

Die ISDS-Konzepte weisen sämtliche Restrisiken aus, die mit dem Betrieb der IT-Lösung und der Organisation einhergehen. Weitaus grössere Risiken als der Lawful Access bei Cloud-Lösungen birgt die Offenlegung vertraulicher Informationen durch unerlaubte und illegale Zugriffe durch Dritte wie Hacker oder kriminelle Organisationen. Die grossen Anbieter von Cloud-Lösungen schützen die Daten mit der neuesten Technologie und den höchsten Sicherheitsvorkehrungen und passen diese stets an die neueste Bedrohungslage an. Daher sind die Risiken der Of-

fenlegung vertraulicher Informationen durch unerlaubte und illegale Zugriffe tendenziell eher geringer, als wenn die Daten on premises gehalten werden. Nach eigenen Angaben hat Microsoft 2021 mehr als 9,6 Mrd. Malware-Bedrohungen und mehr als 35,7 Mrd. Phishing- oder andere bösartige E-Mails blockiert, die Endkundinnen und -kunden oder Unternehmen zum Ziel hatten, sowie 25,6 Mrd. Angriffe auf Unternehmenskonten erkannt und blockiert. Gemäss Gartners «Cloud End-User Buying Behavior Survey 2020» haben 30% der Organisationen, die in die Cloud gewechselt haben, diesen Schritt aus Sorge um die Sicherheit ihrer Daten getan.

Die Verantwortung für die ISDS-Konzepte im Bereich der IKT-Grundversorgung liegen beim Amt für Informatik, das die standardisierte IKT-Grundversorgung bereitstellt (Ziff. 21 IKT-Strategie). Die meisten Risiken im Zusammenhang mit M365 werden durch die Umsetzung der AISR und BISR sowie die weiteren rechtlichen, organisatorischen und technischen Sicherheitsmassnahmen wirksam vermindert. Mit dem neuen digitalen Arbeitsplatz der IKT-Grundversorgung werden insbesondere folgende Massnahmen umgesetzt:

– Zur Authentifizierung von Benutzerinnen und Benutzern kommt eine starke Zweifaktoren-Authentisierung zum Einsatz.
– Das Generieren und das Übermitteln von Diagnosedaten an Microsoft werden auf ein Minimum reduziert.
– Bei der Speicherung oder der Übertragung von Daten zwischen dem digitalen Arbeitsplatz und Exchange Online sowie internen und externen Kommunikationspartnerinnen und -partnern kommen kryptografische Verfahren und Werkzeuge zum Einsatz.
– Mit «Azure Information Protection» wird ein Werkzeug zur Verfügung gestellt, um die technische Umsetzung der BISR 3 bezüglich Klassifizierung von Informationen sicherzustellen. Alle Dokumente und E-Mails können entsprechend der Richtlinie klassifiziert und der Zugriff entsprechend reguliert werden.
– Der Zugriff auf die Informationen vom Kanton Zürich durch Microsoft wird durch den Einsatz der «Customer Lockbox» geregelt. Der Zugriff durch eine Support-Mitarbeiterin oder einen Support-Mitarbeiter ist dadurch zeitlich und thematisch eingeschränkt und kann erst nach Genehmigung durch den Kanton Zürich erfolgen.

Im Weiteren erstellt das Amt für Informatik eine allgemeine Nutzungsrichtlinie M365 für den sicheren Einsatz des digitalen Arbeitsplatzes und der M365-Dienste.

Die Verantwortung für den Schutz von Personendaten und anderen Informationen durch angemessene Massnahmen liegt bei den einzelnen Verwaltungseinheiten gemäss § 59 und Anhang 2 der Verordnung über

die Organisation des Regierungsrates und der kantonalen Verwaltung (VOG RR; LS 172.11). Die Direktionen treffen die zur Umsetzung des IDG erforderlichen Regelungen (§ 60 Abs. 1 lit. e VOG RR). Daher obliegt es den Direktionen und der Staatskanzlei, zu beurteilen, ob die allgemeine Nutzungsrichtlinie M365 für die konkreten Bedürfnisse ausreicht oder ob diese für die jeweilige Organisationseinheit durch weitergehende organisatorische Regelungen ergänzt werden müssen.

Mit der Umsetzung der verschiedenen Massnahmen wird ein hoher Grundschutz der M365-Cloud-Lösung sichergestellt. Gleichzeitig werden den Direktionen und der Staatskanzlei Werkzeuge angeboten, um bei Bedarf den Schutz ihrer Daten individuell zu erhöhen.

7. Folgen bei Verzicht auf Einführung der Cloud-Lösung M365

Insgesamt sind in Bezug auf M365 keine erheblichen Restrisiken, weder durch Lawful Access noch andere Faktoren, ermittelt worden, die einen Verzicht auf die Einführung der Cloud-Lösung aufdrängen. Wie für alle Lösungen bestehen auch für M365 Risiken, die nicht vermindert werden können:

– *Lieferantenabhängigkeit:* Durch die Wahl von Microsoft als Anbieter begibt man sich grundsätzlich in eine Lieferantenabhängigkeit.
– *Kontrollverlust:* Durch die Nutzung einer Cloud-Lösung gehen betriebliche Aspekte und Verantwortlichkeiten, auch hinsichtlich Sicherheit, an den Anbieter über, womit sie nicht mehr unmittelbar im Einflussbereich des Kunden liegen. Müssten solche Risiken gänzlich ausgeschlossen werden, würde jegliche Art der Datenbearbeitung verunmöglicht.

Wird die Cloud-Lösung M365 im Kanton Zürich nicht eingeführt, hat dies weitreichende Auswirkungen auf die Betriebsprozesse und die Digitalisierungsvorhaben der kantonalen Verwaltung.

Zwar kann beispielsweise Microsoft Office (in der Version Microsoft Office Professional 2021 anstelle von M365) weiterhin in den eigenen Rechenzentren installiert und betrieben werden. Dabei muss aber in Kauf genommen werden, dass Leistungen und Werkzeuge, die Microsoft heute bereits ausschliesslich in der Cloud zur Verfügung stellt, wie beispielsweise Microsoft Teams, nicht zur Verfügung stehen.

Mit dem Verzicht auf M365 ergeben sich unter anderem folgende Auswirkungen:

– *Geringe Zukunftsfähigkeit:* Microsoft hat eine klare Cloud-Strategie mit dem erklärten Ziel, je länger, desto mehr nur noch für die Cloud weiterzuentwickeln und zunehmend Lösungen und Funktionalitäten nur noch aus der Cloud anzubieten.

- *Eingeschränkte Kollaborationsmöglichkeiten:* Das übergreifende Arbeiten in Teams innerhalb der eigenen Organisation und auch in der Zusammenarbeit mit Lieferantinnen und Lieferanten sowie Kundinnen und Kunden wird in der Microsoft-Welt bereits heute vor allem durch Cloud-Lösungen ermöglicht (insbesondere mit Microsoft Teams, SharePoint-Online und OneDrive). Bei einem Vor-Ort-Betrieb von M365 müssen für die gleichen Funktionalitäten alternative Drittanwendungen genutzt werden, die standardmässig nicht gleich stark in die Microsoft-Produktepalette bzw. das Microsoft-Ökosystem integriert sind. Dadurch werden die Möglichkeiten zur effizienten Zusammenarbeit stark eingeschränkt und die Komplexität in der IKT-Grundversorgung erhöht.
- *Geringere Arbeitgeberattraktivität:* Im privatwirtschaftlichen Umfeld haben sich die Cloud-Lösungen sowohl von Microsoft als auch von anderen Anbietenden etabliert. Viele Mitarbeitende wollen mit diesen Tools arbeiten und an deren rasch voranschreitender Entwicklung teilhaben. Würde der Kanton Zürich seinen Mitarbeitenden diese Möglichkeit verwehren, würde seine Arbeitgeberattraktivität leiden.
- *Einschränkungen für die Digitalisierung:* Können M365-Cloud-Dienste nicht genutzt werden, fallen Optionen für die Optimierung der Büroautomation und der Prozessoptimierung weg. So bietet die M365-Cloud eine Vielzahl von Schnittstellen und Applikationen für die Digitalisierung von Prozessen (beispielsweise das Tool PowerAutomate zur Digitalisierung administrativer Prozesse).
- *Einbussen im Bereich der Cybersecurity:* Neben den funktionalen Möglichkeiten werden zunehmend Tools und technische Lösungen im Bereich Cybersecurity in erster Linie oder ausschliesslich als Cloud-Lösung im M365-Ökosystem angeboten (z. B. «Microsoft Information Protection» oder «Microsoft Advanced Threat Protection»). Das Sicherheitsniveau einer Cloud-Lösung kann daher mittelfristig in einem On-Premises-Ansatz nicht mehr erreicht werden.

Allgemein kann festgehalten werden, dass der Verzicht auf die M365-Cloud-Lösung dazu führt, dass der Kanton Zürich sich technologisch ins Abseits manövriert, da er sich im Unterschied zur Privatwirtschaft und zu fortschrittlichen Gemeinwesen dem technologischen Fortschritt verschliesst. Zudem muss davon ausgegangen werden, dass der Support von Microsoft für on premises installierte Lösungen bereits mittelfristig nur noch reduziert und längerfristig gar nicht mehr angeboten wird.

Der Einsatz von M365 wird unter Berücksichtigung der voranstehenden Ausführungen und der Beurteilung der Risiken in der kantonalen Verwaltung zugelassen.

8. Cloud-Sicherheitsbeauftragte/r

Die hohe Veränderungsgeschwindigkeit im Bereich des Angebots von Cloud-Lösungen und deren Funktionalitäten erfordert aus Sicht des Datenschutzes und der Informationssicherheit ein entschlossenes und fortdauerndes Überwachen sowie ein stetiges Beurteilen der Risiken. Gleichzeitig muss die Compliance sichergestellt werden.

Um diesem Umstand Rechnung zu tragen, ist als weitere Massnahme die Stelle einer oder eines Cloud-Sicherheitsbeauftragten des Kantons Zürich zu schaffen. Die oder der Cloud-Sicherheitsbeauftragte wird in die Organisation des IKT-Sicherheitsbeauftragten des Kantons Zürich 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 Fragestellungen zu Cloud-Vorhaben und führt in deren Auftrag die Berechnung zur Bestimmung der Restrisiken aus einem ausländischem Lawful Access durch.

Die Stelle der oder des Cloud-Sicherheitsbeauftragten mit einem Beschäftigungsgrad von 100% wird auf den 1. April 2022 geschaffen und in Lohnklasse 22 VVO eingereiht. Die Kosten sind für 2022 zu kompensieren und ab 2023 in den Konsolidierten Entwicklungs- und Finanzplan 2023–2026 einzustellen.

9. Stellungnahme SDI

Das Gremium Steuerung Digitale Verwaltung und IKT hat den Antrag an seiner Sitzung vom 28. Januar 2022 zuhanden des Regierungsrates vorberaten und diesem zugestimmt. Er wurde danach noch in einigen Punkten angepasst.

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Der Einsatz der Cloud-Lösung M365 in der kantonalen Verwaltung wird für alle der IKT-Strategie unterstehenden Organisationseinheiten sowie für die Kantonspolizei zugelassen.

II. Die Direktionen und die Staatskanzlei werden beauftragt, für Cloud-Lösungen in ihrem Zuständigkeitsbereich die Restrisiken eines erfolgreichen ausländischen Lawful Access analog zum Modell gemäss Erwägung 4 zu ermitteln und im ISDS-Konzept auszuweisen.

Liegt die 90%-Eintrittswahrscheinlichkeit eines erfolgreichen Lawful Access bei unter 100 Jahren, beantragen die Direktion und die Staatskanzlei die Zulassung der risikobewerteten Cloud-Lösung dem Regierungsrat.

III. Die Direktionen und die Staatskanzlei werden beauftragt, zu beurteilen, ob über die durch die Finanzdirektion zu erlassende «Allgemeine Nutzungsrichtlinie M365» hinaus eine weitergehende, organisationsspezifische Regelung notwendig ist, und im Bedarfsfall eine solche zu erlassen.

IV. Mit Wirkung auf den 1. April 2022 wird im Stellenplan des Amtes für Informatik folgende unbefristete Stelle geschaffen:

Stellen	Richtposition	Klasse VVO
1,0	Informatikspezialist/in mbA (Cloud-Sicherheitsbeauftragte/r)	LK 22

V. Mitteilung an die Direktionen des Regierungsrates und die Staatskanzlei, die Datenschutzbeauftragte und die Finanzkontrolle.

Vor dem Regierungsrat
Die Staatsschreiberin:

Kathrin Arioli