Stadt Zürich
Stadtrat

Beschluss des Stadtrats

vom 13. Juli 2022

Nr. 670/2022
Organisation und Informatik, Nutzung von Cloud-Services im Rahmen der standardisierten städtischen Service-Angebote, Neuerlass einer Richtlinie

IDG-Status: öffentlich

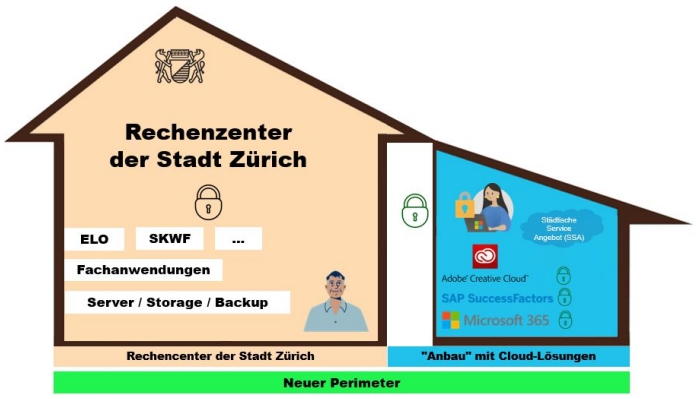
1. Zweck der Vorlage

In Umsetzung der IT-Strategie der Stadt 2016 (Stadtratsbeschluss [STRB] Nr. 401/2016) werden die Nutzung von Cloud-Services im Rahmen der standardisierten stadtweiten Service-Angebote der Organisation und Informatik (OIZ) verbindlich für alle Organisationseinheiten beschlossen und die diesbezüglichen Verantwortlichkeiten festgelegt.

2. Ausgangslage

Bereits heute bieten namhafte Anbieterinnen ihre IT-Leistungen nur noch in einer Cloud oder in Kombination von Vorort- mit Cloud-Services (hybride Lösungen) an. Damit die OIZ den städtischen Organisationseinheiten weiterhin zentrale IT-Services gemäss Anhang 2 (Anhang DGA) zum Reglement über Organisation, Aufgaben und Befugnisse der Stadtverwaltung (ROAB, AS 172.101) zur Verfügung stellen kann, ist es unumgänglich, dass sie sich dabei nebst den wie bis anhin aus den Rechenzentren der Stadt erbrachten Services auch auf Services aus einer Cloud abstützen kann.

Mit der Genehmigung der IT-Strategie der Stadt 2016 (STRB Nr. 401/2016) hat der Stadtrat der OIZ den Auftrag erteilt, die Grundlagen für den Bezug externer Cloud-Services zu erarbeiten. Gemäss dem darin formulierten Ziel soll die Stadt dabei externe Cloud-Services auf rechtskonforme, sichere und risikoarme Weise nutzen können, um insbesondere auch von Innovationen und/oder Kostenvorteilen zu profitieren. Mit der Nutzung von Cloud-Angeboten erweitert die Stadt somit ihren «Rechenzenter-Perimeter»:



Bei einem Bezug von Cloud-Services handelt es sich grundsätzlich um eine faktische Informations- und Datenauslagerung. Mitarbeitende bearbeiten nebst unkritischen Informationen und Daten auch besonders schützenswerte Informationen und Daten. Zu berücksichtigen sind deshalb insbesondere die gesetzlichen Vorgaben zu Schweige- bzw. Geheimnispflichten, wie z. B. Art. 320 Strafgesetzbuch (StGB, SR 311.0), § 8 Gemeindegesetz (LS 131.1), das Gesetz über die Information und den Datenschutz (IDG, LS 140.4) oder auch die Verordnung über das Arbeitsverhältnis des städtischen Personals (AS 177.100). In Bezug auf einige Organisationseinheiten, vor allem solche mit Aufgaben in den Bereichen Sozial-, Gesundheits- und Steuerwesen, gilt es, allfällige zusätzlich gesetzlich geregelte Geheimhaltungspflichten und im Zusammenhang mit den Berufsgeheimnissen insbesondere auch Art. 321 StGB (Verletzung des Berufsgeheimnisses) zu berücksichtigen.

Cloud-Services, die die OIZ als zentrale IT-Services gesamtstädtisch zur Verfügung stellt, haben aufgrund dieser Ausgangslage hohe datenschutzrechtliche und sicherheitstechnische Anforderungen zu erfüllen. Der vorliegende Beschluss soll daher die Nutzung der durch die OIZ zur Verfügung gestellten zentralen IT-Services auch für besonders schützenswerte Informationen und Daten ermöglichen, wenn die OIZ diese unter Einbindung von Cloud-Services gemäss den in diesem Beschluss formulierten Bedingungen bereitstellt.

3. Standardisiertes stadtweites Service-Angebot

Die OIZ stellt den Organisationseinheiten unter Anderem zentrale Services (z. B. SAP-Anwendungen, Microsoft Office Palette wie Word oder Outlook) im Rahmen eines standardisierten stadtweiten Service-Angebots (nachfolgend SSA) zur Verfügung. Will eine Organisationseinheit eine Funktionalität nutzen, die die OIZ mittels eines solchen SSA anbietet, ist sie verpflichtet, diese bei der OIZ zu beziehen. Das SSA ist entsprechend den Anforderungen der Stadt konfiguriert und durch die OIZ, bei Bedarf auch unter Beizug von spezialisierten Drittfirmen, zur Verfügung gestellt. In Zukunft wird das SSA jedoch nicht mehr nur auf Infrastrukturen vor Ort in den Rechenzentren der Stadt bereitgestellt, sondern durch die Nutzung von Cloud-Services und/oder hybriden Lösungen («Cloud-SSA») ergänzt (z. B. SAP SuccessFactors mit eRecruiting oder SLS oder M365 mit Microsoft Teams, Exchange Online, Sharepoint Online).

Cloud-SSA können je nach Bedarf bei sogenannten «Hyperscaler» (z. B. Microsoft, Amazon, Google) oder spezialisierten Cloud-Anbieterinnen bezogen werden. Hyperscaler stellen grosse, weltweit verteilte IT-Infrastrukturen zur Verfügung. Der Kundschaft wird dabei innerhalb dieser IT-Infrastrukturen ein logisch abgetrennter Bereich («Tenant») zugewiesen, der alleine ihr oder ihm zur Verfügung steht.

4. Auslagerung von Informationen und Daten

Das kantonale Datenschutz- und Informationsrecht erlaubt es, externe Dienstleisterinnen mit der Bearbeitung von Informationen (einschliesslich Personendaten) zu betrauen (§ 6 IDG i. V. m. § 25 Verordnung über die Information und den Datenschutz [IDV, LS 170.41]). Unbestritten ist, dass diese Erlaubnis auch die Nutzung von Services externer IT-Anbieterinnen umfasst, sofern die gesetzlich vorgegebenen Voraussetzungen und Rahmenbedingungen für die Nutzung von Cloud-Services eingehalten werden. Auch der Beizug von Dienstleistungen mit Auslandsbezug (Haltung der Informationen und Daten im Ausland und/oder ausländische

Anbietende) ist gesetzlich nicht ausgeschlossen (vgl. dazu auch Rechtsgutachten «Rechtmässigkeit von Public Cloud Services, Cloud-Gutachten unter Berücksichtigung des CLOUD Act», Laux Lawyers AG, vom 16. September 2021). Dasselbe Rechtsgutachten kommt ferner explizit zum Schluss, dass die Nutzung von Cloud-Services, die im Normalbetrieb – also zum Beispiel ohne Vorliegen eines Störfalls – zu keinen Zugriffen auf Inhaltsdaten (sogenannte «Klartextzugriffe») führen, kein gemäss den relevanten Normen des StGB strafrechtlich verbotenes Verhalten der Behörden darstellt. Somit besteht insbesondere kein Anwendungsfall der Art. 320 StGB (Verletzung des Amtsgeheimnisses), Art. 271 StGB (Verbotene Handlungen für einen fremden Staat), Art. 273 StGB (Wirtschaftlicher Nachrichtendienst) oder Art. 293 StGB (Veröffentlichung amtlicher geheimer Verhandlungen). Die Normen des kantonalen Verwaltungsrechts stehen einer Nutzung von Cloud-Services gemäss Analyse des erwähnten Rechtsgutachtens ebenfalls nicht entgegen.

5. Richtlinie

5.1 Allgemein

1. Im Zusammenhang mit der Nutzung von Cloud-Services SSA sind die Pflichten bzw. Aufgaben der OIZ sowie der übrigen städtischen Organisationseinheiten klar zu regeln. Der Stadtrat erlässt hierzu eine neue Richtlinie mit nachfolgendem Inhalt.

5.2 Gegenstand, Pflichten und Inkrafttreten

2. Im Gegenstand wird der Regelungsinhalt der Richtlinie festgelegt. Anschliessend folgen die Pflichten bzw. die unterschiedlichen Aufgaben bei der Nutzung von Cloud-Services SSA.

3. Pflichten OIZ:

   Die OIZ sorgt beim Cloud-SSA dafür, dass die zur Leistungserbringung beigezogenen Cloud-Anbieterinnen sorgfältig ausgewählt werden und führt eine Überprüfung der Cloud-SSA aus rechtlicher, technischer und organisatorischer Sicht durch. Die OIZ legt die sich daraus ergebenden technischen und organisatorischen Massnahmen («TOM») fest und setzt sie um. Die OIZ ist zuständig und verantwortlich, dass während der gesamten Nutzungszeit der Cloud-SSA ein hoher Sicherheitsstandard (Basisschutz oder Basisschutz+) gewährleistet ist (vgl. zu den einzelnen Massnahmen unten).

   Sollte bei einem Cloud-SSA nur der Basisschutz, nicht aber der Basisschutz+ erreicht werden, erlaubt die OIZ die Nutzung einzelner Services oder Funktionalitäten eines Cloud-SSA nur für Informationen und Daten mit normalem Schutzbedarf (einschliesslich nicht besonderer Personendaten und Informationen, die nicht der Schweigepflicht des Amtsgeheimnisses unterliegen).

   Werden im evaluierten Cloud-SSA Ausnahmen zum Basisschutz (Unterschreitung) identifiziert, sieht die OIZ grundsätzlich von der Zurverfügungstellung eines solchen Angebots ab.

   Während der gesamten Nutzungsdauer des Cloud-SSA verifiziert die OIZ die Einhaltung der «TOM» durch die Cloud-Anbieterinnen fortlaufend unter Leitung der hierfür geschaf-

fenen OIZ-Stelle Cloud-Compliance Management. Diese Überprüfung erfolgt insbesondere auch mittels systemgenerierter Auswertungen. Die OIZ berichtet jährlich in geeigneter Weise über die Resultate dieser Überprüfungen an die IT-Delegation bzw. den Stadtrat.

4. Pflichten Organisationseinheiten:

   Die Organisationseinheiten müssen sich weder um die technischen Konfigurationen des von der OIZ zur Verfügung gestellten Cloud-SSA, noch um die durch die OIZ beurteilten organisatorischen und vertraglichen Massnahmen oder die Resultate der kontinuierlichen Kontrolle der Cloud-SSA durch die OIZ kümmern. Organisationseinheiten, bei denen zusätzlich gesetzlich geregelte Geheimhaltungspflichten und/oder Berufsgeheimnisse zu berücksichtigen sind, überprüfen gemeinsam mit der OIZ, ob die sich daraus allfällig ergebenden Zusatzanforderungen durch den Basisschutz+ abgedeckt sind. Falls nicht, werden die notwendigen Massnahmen gemeinsam mit der OIZ festgelegt.

   Organisationseinheiten, die Cloud-SSA auch für die Bearbeitung besonders schützenswerter Informationen und Daten einsetzen wollen, obwohl die OIZ dieses Angebot hierfür nicht freigegeben hat (Basisschutz+ ist [noch] nicht erreicht), reichen ihr Vorhaben vorgängig der IT-Delegation zur Prüfung und anschliessend dem Stadtrat zur Bewilligung ein.

6. Massnahmen

6.1 Vertragliche Massnahmen

Die vertraglichen Vorgaben der möglichen Cloud-SSA-Anbieterinnen werden von der OIZ einer sorgfältigen Prüfung unterzogen. Wenn nötig und möglich werden Zusatzvereinbarungen verhandelt, die zu einer weiteren Risikominimierung für die Stadt führen und somit den Basisschutz+ sicherstellen. Als Beispiel kommt hierfür eine vertraglich wirksame Einbindung der Cloud-Anbieterinnen als Hilfspersonen in Frage, wodurch diese denselben Vorgaben und Pflichten unterstellt werden, wie sie für die Stadt gelten.

6.2 Technische Massnahmen

Cloud-SSA müssen sicherheitsmässig den gleichen Anforderungen entsprechen, wie sie in den städtischen Rechenzentren gelten.

Insbesondere Hyperscaler-Cloud-Anbieterinnen verfügen über ein umfassendes Regelwerk in Bezug auf die von ihnen zur Verfügung gestellten IT-Infrastrukturen, das insbesondere auch eine Beschreibung der technischen Schutzmassnahmen und Zertifizierungen enthält. Modular aufgebaute Serviceangebote ermöglichen den Kundinnen, das für sie geeignetste und wirtschaftlichste Angebot auszuwählen.

Die OIZ überprüft diese Serviceangebote gestützt auf das Handbuch Informationssicherheit der Stadt Zürich (HISi, vgl. STRB Nr. 634/2014) sowie auf weltweit verwendete Standards (zum Beispiel BSI-C5, ein auf ISO Standards – ISO27018, Cloud-Computing und ISO27001, Informationssicherheit – basierender anerkannter Kriterienkatalog mit Beschreibung der Mindestanforderungen an die Informationssicherheit für Cloud-Services). Sie legt die Konfigura-

tion der einzelnen Services so fest, dass die Sicherheits-Anforderungen gemäss HISi und internationalen Standards grundsätzlich so sichergestellt sind, dass sie dem Basisschutz+ entsprechen.

Basisschutz+:

Die OIZ stellt sicher, dass Cloud-SSA in der Regel das Sicherheitsniveau Basisschutz+ aufweisen. Mit dem Sicherheitsniveau Basisschutz+ werden die Basisschutzanforderungen gemäss HISi und der weiteren verwendeten Standards durch die Umsetzung zusätzlicher rechtlicher, technischer und organisatorischer Massnahmen überschritten. Dadurch wird sichergestellt, dass die Cloud-SSA-Anbieter*innen sämtliche rechtlichen und infrastrukturseitigen Anforderungen erfüllen, die sich aus den datenschutzrechtlichen Vorgaben, auch in Bezug auf besondere Personendaten, und dem Amtsgeheimnis ergeben können. Beispiele, die zur Erreichung eines Basisschutz+-Sicherheitsniveaus führen, sind:

– Verpflichtung der Cloud-Anbieterin, sich in jedem Fall gerichtlich gegen Herausgabebegehren staatlicher Stellen zu wehren
– Verpflichtung der Cloud-Anbieterin, dass die Server nur in der Schweiz oder in der EU stationiert sein dürfen
– Datenzugriffe von Mitarbeitenden der Cloud-Anbieterin nur aus der Schweiz und/oder der EU erlaubt
– Zugriffe nur via zwei Faktoren oder gleichwertige Authentisierung für Mitarbeitende der Cloud-Anbieterinnen mit privilegierten Rechten möglich.

Bestätigt die OIZ den Basisschutz+, kann das Cloud-SSA auch für die Bearbeitung besonders schützenswerter Daten, insbesondere auch für besondere Personendaten, und Informationen, die der Schweigepflicht gemäss Amtsgeheimnis unterliegen, verwendet werden.

Basisschutz:

Die für die Erreichung des Schutzniveaus Basisschutz umzusetzenden Massnahmen umfassen die Umsetzung und Einhaltung der im HISi und weiteren verwendeten Standards entsprechend beschriebenen rechtlichen, technischen und organisatorischen Vorgaben. Der Basisschutz geht aber im Gegensatz zum Sicherheitsniveau Basisschutz+ nicht darüber hinaus. In gewissen Fällen stellt die OIZ ein Cloud-SSA auch dann zur Verfügung, wenn es «nur» dem Sicherheitsniveau Basisschutz entspricht. Dies kann zum Beispiel temporär der Fall sein, solange die OIZ noch nicht alle Abklärungen für Erreichung des Sicherheitsniveaus Basisschutz+ durchgeführt hat, aber das Cloud-SSA schon zur Bearbeitung von nicht besonders schützenswerten Daten zur Verfügung stellen will. Es kann aber auch Fälle geben, in denen der Basisschutz auf Dauer ausreicht, so beispielsweise, wenn es in der Natur der Services liegt, dass keine besonders schützenswerten Daten und Informationen bearbeitet werden können (z. B. technische Messungen) oder wenn es sich um reine IT-technische Services handelt. Cloud-SSA mit dem Schutzniveau Basisschutz eignen sich dann aber nicht für die Bearbeitung von besonderen Personendaten oder Informationen, die dem gemäss Amtsgeheimnis unterliegen.

6.3 Organisatorische Massnahmen

Begleitende organisatorische Massahmen beziehen sich sowohl auf Massnahmen, die die überprüften Cloud-Anbieterinnen betreffen, als auch auf solche der OIZ und der nutzenden Organisationseinheiten.

Die organisatorischen Massnahmen der Cloud-Anbieterinnen werden in der Regel anlässlich der vertraglichen Überprüfung verifiziert (z. B. «Wie sind die Zutrittsrechte in die Rechenzentren der Anbietenden geregelt?»). Die durch die OIZ einzuhaltenden organisatorischen Massnahmen und solche, die für die alle Nutzenden Organisationseinheiten gleichermassen gelten, werden im Rahmen der einzelnen Services festgelegt (z. B. «Wie sind die Zugriffe von OIZ-Mitarbeitenden auf Informationen und Daten geregelt?, Wie werden Tickets abgesetzt?»).

Besteht in einzelnen Organisationseinheiten der Bedarf für zusätzliche, nur auf die jeweilige Organisationseinheit ausgerichtete, organisatorische Regelungen (z. B. organisationsspezifische Anleitungen) kann die OIZ hierfür beratend beigezogen werden.

7. Auswirkungen

Bestätigt die OIZ für ein Cloud-SSA das Vorliegen des Sicherheitsniveaus Basisschutz+, müssen die nutzenden Organisationseinheiten für die Bearbeitung von Daten und Informationen, die Schweigepflichten gemäss Amtsgeheimnis unterliegen, (einschliesslich besonderer Personendaten i. S. v. § 3 Abs. 4 IDG, allfälliger zusätzlich gesetzlich geregelter Geheimhaltungspflichten und/oder Berufsgeheimnissen, sofern deren Überprüfung keine zusätzlichen Anforderungen ergeben hat), keine weitere Genehmigung nach § 25 Abs. 3 IDV für die einzelnen Bearbeitungsfälle einholen.

Aufgrund der Bestätigung des Basisschutzes+ eines Cloud-Angebots durch die OIZ, erteilt der Stadtrat den nutzenden Organisationseinheiten als vorgesetzte Behörde die schriftliche Einwilligung zur straffreien Offenbarung eines Geheimnisses gemäss Art. 320 Ziff. 2 StGB.

8. Zuständigkeit

Durch die Vorlage werden der Einsatz von Cloud-SSA verbindlich für alle Organisationseinheiten beschlossen und mittels Richtlinie die diesbezüglichen Verantwortlichkeiten zwischen OIZ und den Organisationseinheiten festgelegt. Für solche Geschäfte ist gemäss Art. 4 sowie Art. 5 e contrario ROAB der Stadtrat zuständig.

Der Stadtrat beschliesst:

1. Die standardisierten stadtweiten Service-Angebote (SSA) der OIZ können ganz oder teilweise durch Nutzung von Cloud-Services (Cloud-SSA) erbracht werden. Vorbehalten bleiben übergeordnete anderslautende rechtliche Bestimmungen, die einer solchen Nutzung entgegenstehen.
2. Es wird eine Richtlinie zur Nutzung von Cloud Services für standardisierte stadtweite Service-Angebote erlassen (Beilage).
3. Der Stadtrat erteilt den Organisationseinheiten für die Nutzung von Cloud-SSA die schriftliche Einwilligung zur straffreien Offenbarung eines Geheimnisses gemäss Art. 320 Ziff. 2 StGB und die Genehmigung für das Bearbeiten besonderer Personendaten gemäss § 25 Abs. 3 IDV.

4. Mitteilung je unter Beilage an die Departemente und Dienstabteilungen und den Datenschutzbeauftragten.

Im Namen des Stadtrats
Die Stadtschreiberin

Dr. Claudia Cuche-Curti