CLOUD UND DATENSCHUTZ – WAS IST ZU BEACHTEN?

Dr. iur., Dominika Blonski

Dr. iur., Dominika Blonski, Executive MPA Unibe, ist Datenschutzbeauftragte des Kantons Zürich, Herausgeberin und Autorin verschiedener Kommentare und Fachpublikationen sowie Dozentin zum Datenschutzrecht.

Abstract: Beschaffen Behörden eine Cloud-Lösung, liegt datenschutzrechtlich eine Auftragsdatenbearbeitung vor. Behörden als öffentliche Organe haben diese Datenbearbeitung – wie jede Datenbearbeitung – rechtmässig auszugestalten. Es stellen sich somit primär rechtliche Fragen: zunächst ist die Rechtsfrage zu beantworten, ob überhaupt ausgelagert werden darf, weil keine rechtliche Bestimmung der Auslagerung entgegensteht und der Auftraggeber seine Verantwortung wahrnehmen kann. Wird diese erste Frage bejaht, stellt sich in einem zweiten Schritt die Frage der angemessenen organisatorisch-technischen Massnahmen für die Datenbearbeitung. Diese Massnahmen werden anhand einer Risikoanalyse – je nach Art der Daten – festgelegt und damit die Frage gestellt, wie ausgelagert werden darf.

INHALTSVERZEICHNIS

1. Einleitung 136
2. Cloud Computing ist eine Auftragsdatenbearbeitung 137
   2.1 Was ist Cloud Computing? 137
   2.2 Was ist eine Auftragsdatenbearbeitung? 137
   2.3 Besondere Risiken 138
3. Wann ist eine Auftragsdatenbearbeitung in der Cloud rechtmässig? 139
4. Was sind die Voraussetzungen einer Auftragsdatenbearbeitung in der Cloud? 141
   4.1 Rechtsfrage: Darf in die Cloud ausgelagert werden? 142
      4.1.1 Stehen rechtliche Bestimmungen entgegen? 142

4.1.1.1 Geheimhaltungspflichten 143
4.1.1.2 Weitere Bestimmungen, die der Auslagerung entgegenstehen können 146
4.1.2 Ist die Wahrnehmung der Verantwortung möglich? 146
4.2 Risikofrage: Wie darf in die Cloud ausgelagert werden? 148
5. Vorgehensweise zur Prüfung der Voraussetzungen 149
6. Übersicht Vorgaben 151
6.1 Rechtsfrage – Geheimnisse 151
6.2 Risikofrage – Art der Personendaten 151
7. Fazit 151
Literaturverzeichnis 152

1. EINLEITUNG

Cloud-Lösungen werden in immer mehr Bereichen eingesetzt, sowohl in privaten Unternehmen als auch bei öffentlichen Organen. Dafür gibt das Datenschutzrecht sowohl rechtliche als auch organisatorisch-technische Rahmenbedingungen vor. Dieser Beitrag beleuchtet die juristischen Vorgaben für öffentliche Organe (gem. Art. 5 lit. i DSG und auf kantonaler Ebene z.B. § 3 Gesetz über die Information und den Datenschutz des Kantons Zürich, LS 170.4 [IDG/ZH]), also Bundesorgane und öffentliche Organe in den Kantonen, die gleichzeitig auch als öffentliche Auftraggeber bzw. Beschaffungsbehörden auftreten, wenn die Cloud-Lösung auf dem privaten Markt im öffentlichen Beschaffungsprozess eingekauft wird.[1]

Die juristischen Vorgaben für öffentliche Organe bei der Auslagerung von Daten in die Cloud bleiben bei der Diskussion über den Einsatz von Cloud-Lösungen häufig im Hintergrund, was angesichts ihrer Relevanz für den Datenschutz als Grundrecht der Bürgerinnen und Bürger unhaltbar ist. Denn für die öffentlichen Organe ergeben sich spezifische Anforderungen aus dem öffentlichen Recht, die sich von jenen für private

[1] Im Folgenden wird deshalb entweder die datenschutzrechtliche Terminologie des «öffentlichen Organs» oder die beschaffungsrechtliche Terminologie der «Auftraggeber» oder «Beschaffungsbehörde» bedient.

Datenbearbeitende unterscheiden. Anhand der gesetzlichen Vorgaben führt dieser Beitrag Schritt für Schritt durch die Fragen, die sich für öffentliche Organe stellen, wenn sie Cloud-Lösungen öffentlich beschaffen, bzw. Daten in die Cloud an Dritte auslagern.[2]

2. CLOUD COMPUTING IST EINE AUFTRAGSDATENBEARBEITUNG

2.1 WAS IST CLOUD COMPUTING?

Aus technischer Perspektive ist Cloud Computing ein Netzwerk, auf das jederzeit und ortsungebunden zugegriffen werden kann. Es handelt sich um einen geteilten Pool von konfigurierbaren Rechnerressourcen (z.B. Netze, Server, Speichersysteme, Anwendungen und Dienste), die mit minimalem Verwaltungsaufwand und minimaler Serviceprovider-Interaktion rasch bereitgestellt und freigegeben werden können. Cloud Computing ermöglicht damit insbesondere Flexibilität und Skalierbarkeit. Es gibt unterschiedliche Servicemodelle: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) und verschiedene Organisationsmodelle wie Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud (NIST, 2011; Blonski, 2022).

2.2 WAS IST EINE AUFTRAGSDATENBEARBEITUNG?

Im datenschutzrechtlichen Sinne liegt beim Beizug von Cloud-Dienstleistungen eine Auftragsdatenbearbeitung vor (gem. Art. 9 DSG und auch § 6 IDG/ZH), weil die Datenbearbeitung einem Dritten übergeben wird. Entsprechend sind die Vorgaben für die Auftragsdatenbearbeitung einzuhalten (Blattmann, 2021, Rz 1).

Wenn die öffentliche Hand sich also entscheidet, Cloud-Leistungen von externen Anbieterinnen einzukaufen, muss sie auch in der öffentlichen Ausschreibung beachten, dass die Vorgaben für die Auftragsdatenbearbeitung eingehalten werden. Wie bei jeder Auftragsdatenbearbeitung verbleibt auch bei der Auslagerung in eine Cloud das öffentliche Organ datenschutzrechtlich vollständig für die Datenbearbeitung verantwortlich. Eine

[2] Eine Abhandlung der verfassungs- und grundrechtskonformen Nutzung von Cloud-Diensten eines US-amerikanischen Anbieters durch öffentliche Organe findet sich in einem Gutachten, das für den Cloud-Einsatz in Gemeinden des Kantons Zürich erstellt wurde, siehe Schefer & Glass, 2023.

Auftragsdatenbearbeitung ist keine Datenbekanntgabe,[3] da die Auftragnehmerin eine Drittperson ist, die keine datenschutzrechtliche Verantwortung gegenüber denjenigen Personen hat, die von der Datenbearbeitungen des öffentlichen Organs betroffenen sind.[4]

Die Auftragnehmerin (bzw. die «Anbieterin» in der beschaffungsrechtlichen Terminologie) darf die Daten entsprechend nur so wie der öffentliche Auftraggeber/die Beschaffungsstelle bearbeiten und sie nicht für eigene Zwecke nutzen. Sie führt die Datenbearbeitung im Auftrag und nur auf Weisung des Auftraggebers durch. Dies gilt auch, wenn das Bearbeiten im Ausland stattfindet, wie dies bei der Inanspruchnahme von Cloud-Lösungen häufig der Fall ist (Privatim, 2022; Datenschutzbeauftragte des Kantons Zürich, 2022; Baeriswyl, 2019, S. 120). Geht eine Datenbearbeitung durch die Auftragnehmerin über das im Rahmen der Auslagerung Zulässige hinaus, z.B. wenn die Cloud-Anbieterin die Daten zu eigenen Zwecken nutzt, müsste dies von der Rechtsgrundlage des öffentlichen Organs gedeckt sein (Botschaft DSG, 7053; Epiney & Fasnacht, 2020, Rz 51 sowie Baeriswyl, 2019).

2.3 BESONDERE RISIKEN

Die Ausschreibung und Nutzung von Cloud-Lösungen bringt aus datenschutzrechtlicher Sicht besondere Risiken mit sich. Dazu gehört beispielsweise ungenügende Transparenz über die Bearbeitung von Personendaten durch die Cloud-Anbieterin, womit u.a. die Einhaltung der Zweckbindung nicht gewährleistet ist. Weitere Risiken sind erschwerte Kontrollmöglichkeiten, der Einfluss ausländischer Rechtsordnungen (wie beispielsweise der CLOUD-Act, siehe auch sogleich 3) und die Gewährleistung eines gleichwertigen Datenschutzes, die Portabilität der Daten und die Interoperabilität mit anderen Systemen sowie Datenverlust und Datenmissbrauch.

In der Praxis wird oft moniert, dass der Auftraggeber bei der Beschaffung von Cloud-Lösungen kaum Einflussmöglichkeiten auf das Angebot sowie die Ausgestaltung der

---

[3] Bei einer Datenbekanntgabe geht die datenschutzrechtliche Verantwortung für die Daten auf die Auftragnehmerin über. Zum Schutz der Grundrechte der betroffenen Personen, sind andere datenschutzrechtliche Rahmenbedingungen vorgesehen, die bei der Auftragsdatenbearbeitung nicht zur Anwendung kommen (vgl. Art. 36 DSG; z.B. §§ 16 und 17 IDG/ZH).

[4] Art. 9 DSG; z.B. § 6 IDG/ZH; Die Botschaft spricht davon, dass die Auftragnehmerin mit dem Beginn der vertraglichen Tätigkeit keine Drittperson mehr ist (Botschaft DSG, 7023).

Cloud-Lösung hat und sich entscheiden muss, das Angebot anzunehmen oder ganz darauf zu verzichten. In einer solchen Situation besteht die Gefahr, dass Rahmenbedingungen der Auslagerung insgesamt und im Besonderen bei der Bearbeitung von Personendaten Grundrechte und Persönlichkeitsrechte verletzt werden. Umso wichtiger ist es bei öffentlichen Beschaffungen, die oben genannten Risiken durch ein vollständiges Pflichtenheft, das alle datenschutzrechtlichen Anforderungen abdeckt und in die Ausschreibung aufnimmt, zu minimieren und somit auf die Ausgestaltung der Cloud-Lösung Einfluss zu nehmen.

3. WANN IST EINE AUFTRAGSDATENBEARBEITUNG IN DER CLOUD RECHTMÄSSIG?

Jede Datenbearbeitung muss rechtmässig – also unter Einhaltung aller rechtlicher Vorgaben – erfolgen, damit sie zulässig ist.[5] Für öffentliche Organe bedeutet dies insbesondere, dass das Legalitätsprinzip eingehalten sein muss, indem sich die Datenbearbeitung auf eine Rechtsgrundlage stützt. Neben dem Legalitätsprinzip sind durch die öffentlichen Organe des Weiteren die verfassungsmässigen Prinzipien und somit auch die Grundrechte einzuhalten und dürfen diese nicht unrechtmässig einschränken (Art. 36 der Bundesverfassung [BV, SR 101]). Diese verfassungsmässigen Vorgaben werden in den Datenschutzgesetzen sowie für einzelne Datenbearbeitungen in bereichsspezifische Gesetze konkretisiert und sind Teil der Rechtmässigkeit der Datenbearbeitung.

Für die Auftragsdatenbearbeitung, bei der ein Dritter im Auftrag des öffentlichen Organs die Daten bearbeitet (Art. 9 i.V.m. Art. 5 lit. k DSG; z.B. § 6 IDG/ZH.), bedeutet dies, dass aufgrund der spezifischen Risiken zusätzliche rechtliche Anforderungen gelten. Diese sind gesondert in den Datenschutzgesetzen festgehalten.[6]

Bei der Frage, ob eine Datenbearbeitung rechtmässig erfolgt, ist zudem die gesamte Rechtsordnung einzubeziehen, die im Rahmen einer Auftragsdatenbearbeitung involviert sein könnte. So beispielsweise auch ein Bezug zu ausländischem Recht: Sieht

---

5 Siehe dazu auch Dominika Blonski, Cloud – alles Risiko? Rechtliche Vorgaben für die Auslagerung von Datenbearbeitungen in die Cloud, in: SJZ 2023/20, S. 991 ff.

6 Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 4.

es z.B. vor, dass Behörden auf Daten zugreifen können, stellt sich die Frage, ob dieser Zugriff nach allgemein anerkannten rechtsstaatlichen Kriterien erfolgt (z.B. im Rahmen der internationalen Rechtshilfe). Ist dies nicht erfüllt und widerspricht eine ausländische Regelung beispielsweise dem ordre public der Schweiz – wie dies beim CLOUD Act[7] der USA der Fall ist[8] –, kann keine rechtmässige Auftragsdatenbearbeitung stattfinden, da ein rechtlicher Kontrollverlust stattfindet, der je nach Konstellation nicht kompensiert werden kann.[9] Dies ist bei der Auslagerung von Datenbearbeitungen an Cloud-Anbieterinnen, die dem US-amerikanischen Recht unterliegen, besonders zu beachten, denn diese können die Einhaltung des anerkannten internationalen Rechts nicht vorbehaltslos garantieren.

Bei öffentlichen Ausschreibungen von Cloud-Dienstleistungen hat die Beschaffungsstelle als Auftraggeberin diesen Umstand bei der Ausschreibung und somit bei der Wahl der Auftragnehmerin zu beachten. Nur so kann sie ihre rechtlichen Vorgaben einhalten.[10]

---

7 Clarifying Lawful Overseas Use of Data Act, abrufbar unter: <https://www.congress.gov/bill/115th-congress/ senate-bill/2383> (zuletzt besucht am 25.11.2023).

8 Der CLOUD Act ist ein Gesetz der USA, das es bestimmten US-Behörden ermöglicht, amerikanische Unternehmen zu verpflichten, Daten ihrer Kundinnen und Kunden herauszugeben, selbst wenn diese Daten nicht in Datenzentren in den USA gespeichert sind. Es handelt sich dabei somit um ein Gesetz mit extraterritorialer Wirkung. Dieses Verfahren und dieser Zugriff auf Daten ist mit dem Datenschutzrecht und dem übergeordneten schweizerischen Recht nicht vereinbar. Es verstösst gegen den ordre public der Schweiz, weil es eine Umgehung des internationalen Rechtshilfewegs darstellt (Bundesamt für Justiz, Bericht zum US CLOUD Act, 17. September 2021, S. 35).

9 Markus Schefer/Philip Glass, Der grundrechtskonforme Einsatz von M365 durch öffentliche Organe in der Schweiz. Eine Analyse am Beispiel des Kantons Zürich, S. 55 ff.

10 Im Zusammenhang mit dem CLOUD Act führt es nicht weiter, anhand einer Risikoanalyse mit Wahrscheinlichkeitsberechnung aufzuzeigen, dass der behördliche Zugriff unwahrscheinlich sei. Die Rechtsfrage kann damit nicht umgangen werden, denn ein öffentliches Organ hat das Recht immer zu beachten und sich rechtmässig zu verhalten («Legalitätsprinzip»). Zudem kann das Verhalten einer amerikanischen Strafbehörde mit einer Methode mit Wahrscheinlichkeitsberechnungen nicht vorausgesagt werden (Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 76.).

Im Ergebnis liegt eine rechtmässige – und damit zulässige – Datenbearbeitung vor, wenn alle rechtlichen Vorgaben eingehalten sind. Das heisst folglich, dass sich auch bei der Auftragsdatenbearbeitung primär rechtliche Fragen stellen.

4. WAS SIND DIE VORAUSSETZUNGEN EINER AUFTRAGSDATENBEARBEITUNG IN DER CLOUD?

Die Auslagerung von Datenbearbeitungen ist unter Einhaltung der spezifischen rechtlichen Vorgaben gemäss den Datenschutzgesetzen grundsätzlich zulässig. Dabei ist insbesondere zu beachten, dass die von der Datenauslagerung in die Cloud bzw. Auftragsdatenbearbeitung durch die Cloud-Anbieterin betroffenen Personen dadurch insgesamt nicht schlechter gestellt werden. Aufgrund der spezifischen Risiken, die bei der Auftragsdatenbearbeitung für die Grundrechte der betroffenen Personen bestehen, präzisieren die Datenschutzgesetze die Rahmenbedingungen für den Beizug einer Auftragsdatenbearbeiterin und geben kumulativ zwei Voraussetzungen für die Auslagerung vor (vgl. Art. 9 DSG, § 6 IDG/ZH).[11] Eine Auftragsdatenbearbeitung ist demnach zulässig und rechtmässig, wenn:

1. keine gesetzliche oder vertragliche Bestimmung der Auslagerung entgegensteht und
2. die datenschutzrechtliche Verantwortung durch den Auftraggeber wahrgenommen werden kann.

Diese beiden Voraussetzungen lassen sich in zwei Schritten abbilden, die einerseits rechtliche und andererseits organisatorisch-technische Anforderungen vorgeben:

In einem ersten Schritt ist zunächst die Rechtsfrage, das heisst die Rechtmässigkeit der Datenbearbeitung an sich, zu beantworten: **Darf ausgelagert werden?** Es ist somit zu prüfen, ob rechtliche Bestimmungen einer Auftragsdatenbearbeitung entgegenstehen. Entgegenstehende rechtliche Bestimmungen können beispielsweise Geheimhaltungspflichten, aber auch vertragliche Vereinbarungen, Klassifizierungen von Informationen oder weitere Regelungen sein (vgl. 4.1). Zur Rechtsfrage gehört aber auch die Prüfung, ob

[11] Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 4 f.

die Beschaffungsstelle/Auftraggeberin ihre Sorgfaltspflicht bei der Auswahl, Instruktion und Überwachung der Auftragnehmerin (analog Art. 55 Obligationenrecht [OR], SR 220) wahrnimmt. Zudem hat sie sicherzustellen, dass die Anbieterin/Auftragnehmerin die Daten nur so bearbeitet, wie es die Beschaffungsstelle selber auch tun dürfte. Um diese Verantwortungen wahrzunehmen, muss dies bereits in der Ausschreibung kommuniziert werden und die Einhaltung als Eignungskriterium eingefordert und nach dem Zuschlag vertraglich festgehalten werden.

Der zweite Schritt stellt die Beantwortung folgender Frage dar: **Wie darf ausgelagert werden?** Bei diesem Schritt – und nur hier – werden anhand einer klassischen Risikoanalyse angemessene organisatorisch-technische Massnahmen festgelegt (vgl. sogleich 4.2).

4.1 RECHTSFRAGE: DARF IN DIE CLOUD AUSGELAGERT WERDEN?

Damit eine Auftragsdatenbearbeitung rechtmässig erfolgt, ist zunächst die Rechtsfrage zu beantworten, ob rechtliche oder andere Bestimmungen der Auftragsdatenbearbeitung in einer Cloud-Lösung entgegenstehen.

Steht eine rechtliche oder andere Bestimmung entgegen, kann geprüft werden, ob technische Massnahmen eine rechtswidrige Kenntnisnahme der Personendaten durch die Cloud-Anbieterin verhindern können (Verschlüsselung mit Schlüsselmanagement beim öffentlichen Organ, Anonymisierung oder Pseudonymisierung mit Schlüssel zur Re-Identifizierung beim Auftraggeber) und, falls ja, dennoch ausgelagert werden kann.[12]

4.1.1 Stehen rechtliche Bestimmungen entgegen?

Im Rahmen einer Rechtsgrundlagenanalyse ist zunächst zu prüfen, ob rechtliche Bestimmungen einer Auslagerung entgegenstehen.[13]

---

[12] Wolfgang Wohlers, Auslagerung einer Datenverarbeitung und Berufsgeheimnis (Art. 321 StGB), Rechtsgutachten, 2015, S. 20; Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 3.

[13] Astrid Epiney/Tobias Fasnacht, § 10 Besondere Grundsätze, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann, Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011,

4.1.1.1 Geheimhaltungspflichten

Ob eine Geheimhaltungspflicht einer Auftragsdatenbearbeitung entgegensteht, ist im Einzelfall zu eruieren. Bei dieser Prüfung spielt die Art der Personendaten keine Rolle, es geht einzig um die Frage des Geheimnisschutzes. Ob Geheimhaltungspflichten einer Auslagerung entgegenstehen, kann anhand folgenden zwei Fragen eruiert werden:

1. Was schützt das Geheimnis und wer ist somit «Geheimnisherr» oder «Geheimnisherrin»? Diese/r kann über das Geheimnis verfügen und entsprechend über die Durchbrechung der Geheimnispflicht entscheiden. Davon ist der/die GeheimnisträgerIn zu unterscheiden, der/die das Geheimnis zwar trägt, aber nicht darüber verfügen kann.
2. Findet mit der Auftragsdatenbearbeitung eine Offenbarung[14] des Geheimnisses statt? Eine Offenbarung findet nicht statt, wenn die Auftragnehmerin als Hilfsperson (im strafrechtlichen Sinne)[15] qualifiziert werden kann. Findet hingegen eine Offenbarung statt, ist die Auftragsdatenbearbeitung nicht zulässig, wenn die Geheimhaltungspflicht der Auslagerung entgegensteht.

So steht das im öffentlichen Arbeitsverhältnis geltende und strafbewehrte Amtsgeheimnis[16] einer Auslagerung grundsätzlich nicht entgegen. Denn beim Amtsgeheimnis ist die

---

N 46; Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 34 ff.; Datenschutzbeauftragte des Kantons Zürich, Leitfaden Bearbeiten im Auftrag, V 1.12 / August 2022, S. 5, abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf> (zuletzt besucht am 25.11.2023).

14 D.h. das Geheimnis wurde einer dazu nicht ermächtigten Drittperson zur Kenntnis gebracht (z.B. BGE 147 II 227, E. 7.3).

15 Da es bei der Auftragsdatenbearbeitung nicht auf die Haftung ankommt, ist der haftungsrechtliche Hilfspersonenbegriff (gemäss Art. 101 OR oder Art. 55 OR) nicht anwendbar. Es stellt sich vielmehr die Frage, ob ein Geheimnis aus strafrechtlicher Perspektive offenbart wird, wenn keine entsprechende Hilfspersonenqualität vorliegt.

16 Z.B. § 51 Personalgesetz des Kantons Zürich vom 27. September 1998 (PG/ZH), LS 177.10; Art. 320 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB), SR 311.0 (wobei der Versuch strafbar ist (Art. 22 StGB) und damit bereits die Möglichkeit der Kenntnisnahme für die Bejahung der Strafbarkeit ausreicht (Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 43)).

öffentliche Hand Geheimnisherrin, da das Geheimnis primär die Funktionstüchtigkeit des Amtes schützt. Damit kann und muss das Amt selber darüber befinden, ob eine Information dem Amtsgeheimnis unterliegt oder nicht. Betroffene Personen werden nur geschützt, wenn ihre privaten Interessen einer Veröffentlichung überwiegen. Untersteht eine Information dem Amtsgeheimnis, ist durch den Auftraggeber zu prüfen, ob er mit der Auslagerung seine Verantwortung wahrnehmen kann. Ist dies der Fall, kann (und muss) das Amt der Auftragnehmerin bzw. deren Mitarbeitenden das Amtsgeheimnis vertraglich überbinden.[17]

Besondere (auch unter Art. 320 StGB oder direkt aus der spezialgesetzlichen Regelung strafbewehrte Amtsgeheimnisse, wie beispielsweise das Steuergeheimnis (z.B. § 120 Steuergesetz des Kantons Zürich, LS 631.1) oder das Sozialhilfegeheimnis (z.B. § 47 Sozialhilfegesetz des Kantons Zürich, LS 851.1), wurden geschaffen, weil in bestimmten Bereichen des Amtsgeheimnisses nicht nur die Funktionstüchtigkeit des Amtes an sich geschützt werden soll, sondern auch das Vertrauensverhältnis zwischen dem Amt und den betroffenen Personen. Entsprechend hat das Amt als Geheimnisherr bei der Entscheidung, ob eine Information dem besonderen Amtsgeheimnis unterliegt, die Interessen der betroffenen Personen einzubeziehen. Die besonderen Amtsgeheimnisse stehen daher einer Auslagerung grundsätzlich entgegen, wenn keine technische Lösung die Kenntnisnahme durch die Auftragnehmerin bzw. ihre Mitarbeitenden unterbindet, da mit der Auftragsdatenbearbeitung ein Offenbaren stattfindet.[18]

---

17 Entsprechend sieht die Strafbestimmung mit der Einwilligung der vorgesetzten Behörde nur einen Rechtfertigungsgrund vor und nicht auch die Einwilligung der betroffenen Person: Matthias Michlig, Öffentlichkeitskommunikation der Strafbehörden unter dem Aspekt der Amtsgeheimnisverletzung (Art. 320 StGB), in: ZStStr - Zürcher Studien zum Strafrecht Band/Nr. 68, 2013, S. 204; Matthias Michlig/Eva Wyler, Art. 320 Verletzung des Amtsgeheimnisses, in: Damian K. Graf (Hrsg.), StGB Annotierter Kommentar, 2020, Rn. 6; Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 42 und 45.

18 Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 46 f. und 49.

Das ebenso strafbewehrte Berufsgeheimnis (z.B. § 15 Abs. 1 und 2 Gesundheitsgesetz des Kantons Zürich (GesG/ZH), LS 810.1; Art. 321 StGB). schützt die betroffene Person selber und damit auch das Vertrauensverhältnis zwischen dieser und der einer bestimmten Berufsgruppe zugehörigen Person. Geheimnisherr oder -herrin ist beim Berufsgeheimnis allein die betroffene Person. Entsprechend kann – anders als beim Amtsgeheimnis – nicht der Geheimnisträger oder die Geheimnisträgerin darüber befinden, ob dem Geheimnis unterliegende Informationen offenbart werden dürfen. Die Geheimhaltungspflicht kann nur im Einzelfall durchbrochen werden, wenn eine gesetzliche Bestimmung dies vorsieht, die betroffenen Person eingewilligt hat oder die vorgesetzte Behörde die Geheimhaltungspflicht aufgehoben hat. Anders als beim Amtsgeheimnis, ist beim Berufsgeheimnis die vertragliche Erweiterung des Kreises der Geheimnisträger durch den Geheimnisträger nicht möglich ist.[19] Bei einer Cloud-Lösung steht das Berufsgeheimnis somit einer Auslagerung grundsätzlich entgegen, es sei denn, eine technische Lösung verhindert die Kenntnisnahme durch die Auftragnehmerin bzw. ihre Mitarbeitenden.[20]

Geheimnis	**Schutz / Geheimnisherr**	**Offenbarung Geheimnis**
Amtsgeheimnis	Funktionstüchtigkeit Amt / Öffentliches Organ	Geheimnis vertraglich überbinden
Besondere Amtsgeheimnisse	Funktionstüchtigkeit Amt und Vertrauensverhältnis / Öffentliches Organ	Ja, stehen grundsätzlich entgegen, wenn keine technische Lösung
Berufsgeheimnis	Vertrauensverhältnis / Betroffene Person	Ja, steht grundsätzlich entgegen, wenn keine technische Lösung

[19] Dies, weil der strafrechtliche Hilfspersonenbegriff des Berufsgeheimnisses sehr eng gefasst ist.

[20] Wolfgang Wohlers, Auslagerung einer Datenverarbeitung und Berufsgeheimnis (Art. 321 StGB), Rechtsgutachten, 2015, S. 18 und 21 ff.; Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 50 f. und 52 f.

4.1.1.2 Weitere Bestimmungen, die der Auslagerung entgegenstehen können

Auch vertragliche Vereinbarungen können der Auslagerung entgegenstehen. So kann der Auftraggeber beispielsweise mit der Auftragnehmerin vereinbaren, dass keine weiteren Unterauftragnehmenden beigezogen werden dürfen.[21]

Des Weiteren können Klassifizierungen der Auftragsdatenbearbeitung entgegenstehen. Das neue Informationssicherheitsgesetz des Bundes (ISG, SR 128) hält verschiedene Klassifikationen beispielsweise zum Schutz der Interessen der inneren und äusseren Sicherheit der Schweiz fest.

Schliesslich können weitere Bestimmungen einer Auslagerung entgegenstehen bzw. diese einschränken. So sieht beispielsweise die Verordnung über das elektronische Patientendossier (Art. 12 Abs. 5 Verordnung über das elektronische Patientendossier [EPDV, SR 816.11]) vor, dass sich die Datenspeicher, auf denen die Informationen des Patientendossiers abgelegt werden, in der Schweiz befinden müssen und dem Schweizer Recht zu unterstehen haben.

4.1.2 Ist die Wahrnehmung der Verantwortung möglich?

Da die öffentliche Auftraggeberin für die Datenbearbeitung verantwortlich bleibt, muss sie bei Auslagerungen – auch in die Cloud – ihre Verantwortung wahrnehmen können. Dies ist die zweite Voraussetzung für die Zulässigkeit der Auftragsdatenbearbeitung.

Dies erfordert zunächst die Wahrnehmung der Sorgfaltspflicht analog Art. 55 OR bei der Auswahl, Instruktion und Kontrolle der Auftragsnehmerin (Botschaft a-DSG, 463 f.).[22] Handelt es sich bei der Cloud-Auslagerung um eine öffentliche Beschaffung, darf bei der Ausschreibung nur eine Auftragnehmerin den Zuschlag erhalten, die die

---

21 Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 35 f.

22 Gemäss Botschaft zum alten DSG muss «Bei der Übertragung der Bearbeitung an einen Dritten [...] der Auftraggeber in Analogie zu Artikel 55 des Obligationenrechts alle gebotene Sorgfalt aufwenden, um Verstösse gegen das Datenschutzgesetz zu verhindern. Er muss den Auftragnehmer entsprechend auswählen, ihm die richtigen Instruktionen erteilen und ihn soweit als möglich auch überwachen.»

Anforderungen einhalten kann und die somit für die Auftragserfüllung geeignet ist.[23] Das öffentliche Organ hat dabei zu prüfen, wie die Auftraggeberin organisiert ist und wie sie arbeitet sowie in welchen (Rechts-)Umfeld sie sich befindet. Weiter muss das öffentliche Organ die Auftragnehmerin instruieren und sie bei der Aufgabenerfüllung überwachen. Das bedeutet, dass die Auftragnehmerin einem durchsetzbaren Weisungsrecht des Auftraggebers unterstehen muss. Zudem muss das öffentliche Organ jederzeit die Kontrollmöglichkeit haben, indem es überprüfen können muss, ob der Auftrag nach seinen Vorgaben und damit rechtskonform erfolgt.

Die Vorgaben, an die sich das öffentliche Organ zu halten hat, sind vertraglich auf die Auftragnehmerin zu übertragen.[24] Besonders hinzuweisen ist auf die Regelung der Vorgabe, dass die Auftragnehmerin die Daten nicht zu ihren eigenen Zwecken bearbeiten darf. Liegt keine Rechtsgrundlage für die Datenbekanntgabe durch das öffentliche

---

[23] Astrid Epiney/Tobias Fasnacht, § 10 Besondere Grundsätze, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann, Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011, N 43; Veronica Blattmann, § 6 Bearbeiten im Auftrag, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Schulthess 2012, Rn. 16; Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 2.

[24] Im Kanton Zürich sind die Grundzüge des Vertragsinhalts in der Verordnung über die Information und den Datenschutz festgehalten (§ 25 Verordnung über die Information und den Datenschutz des Kantons Zürich vom 28. Mai 2008 (IDV/ZH), LS 170.41; Datenschutzbeauftragte des Kantons Zürich, Leitfaden Bearbeiten im Auftrag, V 1.12 / August 2022, S. 8 f., abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf> (zuletzt besucht am 25.11.2023).). Der Regierungsrat des Kantons Zürich hat die AGB Auslagerung Informatikleistungen (Allgemeine Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen des Kantons Zürich (AGB Auslagerung Informatikleistungen) vom 24. Juni 2015, abrufbar unter: <https://www.zh.ch/content/dam/zhweb/bilder-dokumente/organisation/finanzdirektion/afi/agb_auslagerung_informatikleistungen.pdf> (zuletzt besucht am 25.11.2023).) und die AGB Datenbearbeitung durch Dritte (Allgemeine datenschutzrechtliche Geschäftsbedingungen bei der Datenbearbeitung durch Dritte des Kantons Zürich (AGB Datenbearbeitung durch Dritte) vom 24. Juni 2015, abrufbar unter: <https:// www.zh.ch/content/dam/zhweb/bilder-dokumente/organisation/finanzdirektion/afi/agb_datenbearbeitung_ durch_dritte.pdf> (zuletzt besucht am 25.11.2023).) erlassen (RRB 2015/670 vom 24. Juni 2015.). Diese AGB sind durch die öffentlichen Organe der kantonalen Verwaltung in ihre Verträge einzubeziehen.

Organ an die Auftragnehmerin vor, ist eine Verwendung zu eigenen Zwecken durch die Auftragnehmerin strafbar..[25]

Schliesslich hat sich eine öffentliche Auftraggeberin zu vergewissern, dass die Auftragnehmerin in der Lage ist, die Datensicherheit zu gewährleisten. Sie hat dafür mittels einer Risikoanalyse festzuhalten, welche organisatorisch-technischen Massnahmen zu ergreifen sind und diese Verpflichtung der Auftragnehmerin vertraglich zu überbinden (siehe sogleich 4.2).

4.2 RISIKOFRAGE: WIE DARF IN DIE CLOUD AUSGELAGERT WERDEN?

Ergibt die Rechtsfrage, dass eine Auftragsdatenbearbeitung zulässig ist, stellt sich in einem letzten Schritt die organisatorisch-technische Frage der Umsetzung von angemessenen Massnahmen zum Schutz der Daten, also die Frage, wie ausgelagert werden darf.

Die Datenschutzgesetze sehen vor, dass Daten angemessen geschützt werden müssen.[26] Um die Angemessenheit von organisatorisch-technischen Massnahmen zu eruieren, wird eine Risikoanalyse durchgeführt. Welche Massnahmen angemessen sind, hängt von der Art der Daten ab. Die Risikoabwägung zeigt die zu ergreifenden angemessenen organisatorisch-technischen Massnahmen passend zur Art der Personendaten auf. Der Auftraggeber hat sich im Rahmen der Wahrnehmung seiner Verantwortung zu vergewissern, dass die Auftragnehmerin die notwendigen organisatorischen und technischen Massnahmen einhalten kann und damit die Datensicherheit gewährleisten kann – so wie wenn die Daten durch ihn selber bearbeitet würden.[27]

Im Rahmen der Risikoanalyse ist einzubeziehen, ob die Auslagerung in der Schweiz, in einem EU-Land oder in einem Land ohne angemessenes Datenschutzniveau stattfindet oder ob andere Rechtsordnungen Bestimmungen vorsehen, die sich auf die Auslagerung

---

[25] § 40 IDG/ZH; Bruno Baeriswyl, Wenn die Rechtsauslegung «nebulös» wird. Cloud-Computing in der Verwaltung verändert die Art und Weise der Datenbearbeitung – aber nicht das Recht, in: digma 2019, S. 119.

[26] Art. 8 DSG, z.B. § 7 IDG/ZH.

[27] Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 55.

auswirken können. Mit der Übermittlung von Personendaten ins Ausland im Rahmen der Auslagerung, steigen die Risiken für die Grundrechte der betroffenen Personen. Gleichzeitig steigen auch die Risiken für den Auftraggeber. Denn die sich im Ausland befindenden Daten sind einer dem Auftraggeber fremden Rechtsordnung ausgesetzt, deren Auswirkungen er nicht einschätzen kann. Damit werden Kontrollen durch den Auftraggeber erschwert, wobei er allenfalls weitere Massnahmen ergreifen muss. Keine zusätzlichen Massnahmen müssen hingegen ergriffen werden, wenn das Datenschutzniveau im konkreten Land dem schweizerischen Datenschutz angemessen ist – dies ist bei Anwendbarkeit der Konvention 108[28] der Fall.[29]

5. VORGEHENSWEISE ZUR PRÜFUNG DER VORAUSSETZUNGEN

Um die umschriebenen Schritte abzudecken, kann eine übliche Projektmethodik beigezogen werden (beispielsweise die beim Bund und beim Kanton Zürich verwendete Methode HERMES). Die im Rahmen dieser Vorgehensweise vorgesehenen Dokumente adressieren die sich stellenden Fragen.

So wird mit einer Rechtsgrundlagenanalyse die rechtliche Lage eruiert und bewertet. Sie beantwortet rechtliche Fragen, wie beispielsweise: Welche rechtlichen Grundlagen sind anwendbar? Welche Vorgaben halten diese fest? Welche Bestimmungen könnten einer Auftragsdatenbearbeitung entgegenstehen? Liegen Geheimnispflichten vor und was schützen diese? Welche ausländischen Regelungen haben auf die Auftragsdatenbearbeitung Einfluss?

Mit der Risikoanalyse werden die Risiken, deren Eintretenswahrscheinlichkeit sowie die Auswirkungen bzw. das Schadensausmass im Falle des Eintretens der Risiken eruiert und bewertet.

---

[28] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (Konvention 108), SR 0.235.1.

[29] § 19 IDG/ZH i.V.m. § 22 IDV/ZH; Veronica Blattmann, § 6 Bearbeiten im Auftrag, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Schulthess 2012, Rn. 27 f.; Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 65 ff.

Die Datenschutzgesetze geben für entsprechende Projekte zwei spezifische Schritte vor, die durch die öffentlichen Organe bei einer beabsichtigten Datenbearbeitung durchzuführen sind – auch bei der Absicht, eine Cloud-Lösung zu beschaffen. Damit ist zunächst eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen. Diese zeigt auf, ob im Anschluss das Projekt bei der Datenschutzbeauftragten zur Vorabkontrolle einzureichen ist (Art. 22 und Art 23 DSG; z.B. § 10 IDG/ZH). Beschaffungsstellen als öffentliche Organe sind verpflichtet, bei der Datenbearbeitung bestehende Risiken für die Grundrechte von Betroffenen zu identifizieren und mit geeigneten Massnahmen zu reduzieren. Diese können sie mit der Durchführung einer DSFA erkennen und bewerten.[30] In diesem Dokument definiert das öffentliche Organ zudem Massnahmen, um die Risiken zu reduzieren.

Weist die beabsichtigte Bearbeitung von Personendaten eines öffentlichen Organs besondere Risiken für die Grundrechte der betroffenen Personen auf, ist eine Vorabkontrolle durch die Datenschutzbeauftragten erforderlich.[31] In diesem Fall legt die Beschaffungsstelle das Projekt der oder dem jeweiligen Datenschutzbeauftragten vor. Diese prüft die rechtlichen, organisatorischen und technischen Rahmenbedingungen der beabsichtigten Datenbearbeitung und nimmt dazu Stellung. Sie hält insbesondere fest, welche weiteren Massnahmen zu ergreifen sind bzw. wie das Projekt datenschutzkonform umgesetzt werden kann.

Schliesslich sind immer auch alternative weitere Möglichkeiten der Datenbearbeitung zu evaluieren. So ist zu prüfen, ob eine On-premises-Lösung möglich wäre, ob eine hybride Cloud oder eine treuhänderische Cloud eingesetzt werden könnte, ob andere Produkte genutzt werden könnten oder ob eine eingeschränkte Nutzung des Produkts (beispielsweise Nutzung von nur einzelnen Diensten oder nur für einzelne Datenkategorien) möglich ist.

---

30 Datenschutzbeauftragte des Kantons Zürich, Merkblatt Datenschutz-Folgenabschätzung (DSFA), V 2.0 / Oktober 2023, S. 1 f., abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_dsfa.pdf> (zuletzt besucht am 25.11.2023).

31 Datenschutzbeauftragte des Kantons Zürich, Merkblatt Vorabkontrolle, V 3.0 / Oktober 2023, S. 1 f., abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_vorabkontrolle.pdf> (zuletzt besucht am 25.11.2023).

6. ÜBERSICHT VORGABEN

6.1 RECHTSFRAGE – GEHEIMNISSE

Amtsgeheimnis	Besondere Amtsgeheimnisse	Berufsgeheimnis
Steht grundsätzlich nicht entgegen	Stehen entgegen	Steht entgegen
Risikoanalyse und Festlegung organisatorisch-technischer Massnahmen	Technische Massnahmen, die Kenntnisnahme verhindern	Technische Massnahmen, die Kenntnisnahme verhindern

6.2 RISIKOFRAGE – ART DER PERSONENDATEN

Personendaten	Besondere Personendaten
Risikoanalyse und Festlegung organisatorisch-technischer Massnahmen	Technische Massnahmen, die Kenntnisnahme verhindern

7. FAZIT

Cloud Computing bringt als Auftragsdatenbearbeitung spezifische Risiken mit sich. Während sich das öffentliche Beschaffungsrecht dazu nicht äussert, sehen die Datenschutzgesetze aus diesem Grund klare Voraussetzungen für die grundsätzlich zulässige Auftragsdatenbearbeitung vor, denn die Verantwortung verbleibtauch bei der Auslagerung in die Cloud beim öffentlichen Auftraggeber.

Damit rechtmässig in die Cloud ausgelagert werden kann, müssen zwei rechtliche Voraussetzungen erfüllt sein: Es dürfen der Auslagerung keine rechtlichen Bestimmungen entgegenstehen und die datenschutzrechtliche Verantwortung des Auftraggebers muss wahrgenommen werden können.

Zur Einhaltung der ersten Bedingung hat das öffentliche Organ zu prüfen, ob das Amtsgeheimnis, ein besonderes Amtsgeheimnis oder das Berufsgeheimnis oder ob vertragliche Vereinbarungen, eine Klassifizierung von Informationen oder weitere Regelungen der Auslagerung entgegenstehen. Ist dies der Fall, kann geprüft werden,

ob eine technische Massnahme die Kenntnisnahme verhindern kann (beispielsweise, wenn die Informationen verschlüsselt werden und das Schlüsselmanagement beim öffentlichen Organ verbleibt, wenn die Personendaten anonymisiert oder pseudonymisiert werden) und dennoch ausgelagert werden kann. Andernfalls ist auf die Auslagerung in die Cloud bzw. auf die Beschaffung der Cloud-Lösung zu verzichten, weil diese nicht rechtmässig erfolgt.

Die zweite Voraussetzung sieht vor, dass das öffentliche Organ bei der Auswahl, Instruktion und Kontrolle der Auftragsnehmerin seine Sorgfaltspflicht wahrnimmt, die Vorgaben vertraglich auf die Auftragnehmerin weitergibt und sich vergewissert, dass die Auftragnehmerin die notwendigen organisatorischen und technischen Massnahmen einhalten kann. Sind diese beiden Voraussetzungen erfüllt und kann damit die Rechtsfrage, ob ausgelagert werden darf, bejaht werden, stellt sich die zweite Frage, wie ausgelagert werden darf. Um diese Frage zu beantworten, muss die Projektleitung bei öffentlichen Beschaffungen von Cloud-Dienstleistungen eine Risikoanalyse anhand der Art der Daten durchführen und angemessene organisatorisch-technische Massnahmen festlegen. Wenn dies umgesetzt wird, erfolgt die Auftragsdatenbearbeitung in der Cloud rechtmässig und die Cloud-Dienstleistungen dürfen öffentlich ausgeschrieben werden.

LITERATURVERZEICHNIS

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 7023.

Baeriswyl, B. (2019). Wenn die Rechtsauslegung «nebulös» wird. Cloud-Computing in der Verwaltung verändert die Art und Weise der Datenbearbeitung – aber nicht das Recht (S. 118 – 122). digma.

Blattmann, V. (2012). § 6 Bearbeiten im Auftrag. In Baeriswyl, B. & Rudin, B. (Hrsg.*). Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich.* Schulthess.

Blonski, D. (2021). Cloud Computing. Datenschutzrechtliche Rahmenbedingungen am Beispiel des Kantons Zürich. In A Epiney & S Rovelli (Hrsg.), *Künstliche Intelligenz und Datenschutz. L'intelligence artificielle et protection des données* (S. 65 – S. 80), Tagungsband zum Dreizehnten Schweizerischen Datenschutzrechtstag, 2. Oktober 2020. Schulthess.

Datenschutzbeauftragte des Kantons Zürich. (2022). Merkblatt Cloud Computing (V 1.6). https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf>

NIST (National Institute of Standards and Technology). (2011). *The NIST Definition of Cloud Computing* (Special Publication 800-145). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Privatim. (2022). Merkblatt Cloud-spezifische Risiken und Massnahmen. https://www.privatim.ch/wp-content/uploads/2022/02/privatim_Cloud-Merkblatt_v3_0_20220203_def._DE-1.pdf> (zuletzt besucht am 25.11.2023)

Schefer, M. & Glass, Ph. (2023). Gutachten zum grundrechtskonformen Einsatz von M365 durch die Gemeinden im Kanton Zürich. Edition Weblaw.