LAUX LAWYERS AG
ZURICH | BASEL

BÜRO ZÜRICH
A Seegartenstrasse 2
P. O. Box · CH 8024 Zürich
T +41 44 880 2424
F +41 44 880 2425
W www.lauxlawyers.ch

BÜRO BASEL
A Steinenring 40 · CH 4051 Basel
T +41 61 283 0606
W www.lauxlawyers.ch

Alle Anwälte in den zuständigen Anwaltsregistern eingetragen

Rechtsgutachten

Erstattet am: 16. September 2021

An: Organisation und Informatik der Stadt Zürich (OIZ)

Von: Christian Laux; Alexander Hofmann

Betrifft: **Rechtmässigkeit von Public Cloud Services**

«Cloud-Gutachten» (unter Berücksichtigung des CLOUD Act)

(zwecks Publikation redaktionell leicht überarbeitete Version vom 13. Juli 2022; ohne inhaltlich-rechtliche Anpassungen oder Aktualisierungen)

I. Einleitung 2
A. Ausgangslage 2
B. Fragestellungen 2
C. Gang der Analyse und Abgrenzungen 3

II. Teil 1: Konzeptionelle und rechtliche Grundlagen 4
A. Grundlegende Konzepte 4
B. Informationsschutz in der Stadt Zürich 9
C. Verstärkung des Informationsschutzes durch Straf- und Prozessrecht 21

III. Teil 2: Anwendung der Grundlagen auf ausgewählte Zugriffsszenarien 29
A. Unbefugte Klartextzugriffe durch die Cloud-Anbieterin oder deren Mitarbeitende 29
B. Klartextzugriffe durch Behörden in der Schweiz 30
C. Klartextzugriffe durch Behörden im Ausland (namentlich in den USA) 33

IV. Teil 3: Beantwortung der Gutachterfragen und Empfehlungen 53
A. Antworten auf die Gutachterfragen auf Basis der Ausführungen 53
B. Handlungsempfehlungen 56
C. Schlussfazit 57

Anhang 1: Begriffsdefinitionen 58

Anhang 2: Abstrakte Beschreibung von Public Cloud Services (IaaS, PaaS, SaaS) 63

Anhang 3: Zum Cloud-Merkblatt der Kantonalen Datenschutzbeauftragten 67

I. Einleitung

A. Ausgangslage

1 Die Dienstabteilung «Organisation und Informatik der Stadt Zürich» (**OIZ**) ist IT-Provider für die stadtzürcherischen Organisationseinheiten (Departemente bzw. Dienstabteilungen). Es ist langjährige Praxis der OIZ, sich für IT-Infrastrukturen[1] auf verschiedenen Ebenen – Betriebsumgebungen, Plattformsoftwares und Applikationen – in vielfältiger Weise auf Dritte zu verlassen und diese IT-Infrastrukturen zu verwalten. Künftig sollen auch Angebote von externen Cloud-Anbieterinnen, namentlich sog. Public Cloud Services, in diese IT-Infrastrukturen einbezogen werden.

2 Die zum Teil kontroverse Wahrnehmung von Public Cloud Services in der Öffentlichkeit[2] rechtfertigt einen konzentrierten Blick darauf, ob die derzeit geplanten Erweiterungen der IT-Infrastrukturen der OIZ um Public Cloud Services zu besonderen Massnahmen Anlass geben bzw. ob der Einsatz von Public Cloud-Angeboten durch die Stadt Zürich überhaupt zulässig ist.

3 Die OIZ erwägt, beim Stadtrat der Stadt Zürich einen Beschluss zu erwirken, der klärt, dass bei gegebenem Basisschutz[3] das Leistungsangebot der OIZ auch dann zu nutzen ist, wenn die OIZ Cloud-Angebote in ihr Serviceportfolio einbindet.

4 OIZ ist die Auftraggeberin für dieses Rechtsgutachten. Das Gutachten richtet sich jedoch an alle Organisationseinheiten der Stadt Zürich.

B. Fragestellungen

5 Die OIZ will geklärt sehen, ob die verantwortlichen Organisationseinheiten die von der OIZ bereitgestellten Leistungen auch dann noch nutzen können, wenn die OIZ Public Cloud Services einsetzt. Ergänzend ist zu klären, ob und wenn ja nach welchen Kriterien allenfalls zu differenzieren ist.

6 Das vorliegende Rechtsgutachten beantwortet dabei insbesondere die folgenden Fragen:

1. *Darf eine Organisationseinheit der Stadt Zürich Public Cloud Services nutzen?*
2. *Gilt dies auch für Informationen mit besonderem Schutzbedarf (vertrauliche oder streng vertrauliche Informationen)?*
3. *Verändert sich die Analyse, je nachdem, welcher Rechtsordnung die Cloud-Anbieterin oder eine ihrer Gruppengesellschaften unterstehen (Sitz im Ausland, namentlich in den USA)?*
4. *Verändert sich die Analyse, je nachdem, wo die in den Public Cloud Services gespeicherten Daten gehalten werden (Data at Rest) (Datenstandort in der Schweiz bzw. im Ausland, namentlich in den USA)?*

---

[1] Bestimmte Begrifflichkeiten wie IT-Infrastrukturen werden im Anhang 1: Begriffsverwendung beschrieben. Wir verwenden jeweils gleichlautende Begrifflichkeiten, die wir für die Zwecke des Gutachtens spezifisch definieren.

[2] Zum Beispiel Workplace Conference der Schweizerischen Informatikkonferenz vom 15. September 2021, abrufbar unter: https://www.youtube.com/watch?v=TKlLhJsYKxk.

[3] Der Basisschutz kann verkürzt als städtische Informationssicherheitsminimum verstanden werden, siehe Beschluss des Stadtrats der Stadt Zürich vom 9. Juli 2014, Nr. 634: Organisation und Informatik (OIZ), Informationssicherheit der Stadt Zürich und Handbuch Informationssicherheit der Stadt Zürich, Inkraftsetzung. Zum Begriff «Basisschutz» führt das Handbuch Informationssicherheit («HISi») in Ziff. 3.1 Folgendes aus: «Der Basisschutz definiert die verbindlichen organisatorischen und technischen Sicherheitsmassnahmen und –vorgaben für alle Informationen, die in und von der Stadtverwaltung Zürich bearbeitet werden, resp. für die dafür verwendeten Systeme. Der Basisschutz ist ausreichend für die Bearbeitung von Informationen mit normalem Schutzbedarf (Klassifizierungsschema, Kap. 4.1.4). Das Handbuch Informationssicherheit definiert den verbindlichen Basisschutz für die Stadt. Wenn Informationen einen erhöhten Schutzbedarf aufweisen, ist zu prüfen, ob der in der Stadtverwaltung festgelegte Basisschutz ausreicht, um diese Informationen angemessen zu schützen. Wenn nicht, sind die zusätzlichen Anforderungen durch geeignete Massnahmen abzudecken.»

5. *Verändert sich die Analyse, je nachdem, ob Personen aus dem Ausland (namentlich aus den USA) auf die in den Public Cloud Services gespeicherten Daten zugreifen können?*

Die Fragen sind jeweils unter den Aspekten Amtsgeheimnis sowie Personendaten zu beurteilen; die Analyse erfolgt auf Basis des Strafgesetzbuches,[4] allgemeiner Überlegungen des städtischen bzw. kantonalen Verwaltungsrechts sowie auf Basis des anwendbaren Datenschutzgesetzes.

C. Gang der Analyse und Abgrenzungen

7 Die Aufgabenstellung ist komplex und bedarf einer umfassenden Schilderung der Grundlagen, was einen Aufbau des Gutachtens nach gestellter Frage als unzweckmässig erscheinen lässt. Das Rechtsgutachten wird zur Verbesserung der Nachvollziehbarkeit der Grundlagen somit im systematischen Stil aufbereitet. Die Erkenntnisse der Darstellung werden in den Zusammenfassungen beschrieben. Am Ende ergeben sich aus diesen Schilderungen die Antworten auf die vorstehenden Fragen.

8 Im Rahmen von besonderen Fact Sheets können Einzelfragen vertieft werden.[5] Allenfalls kann in solchen eine besondere Frage vertieft oder zusammenfassend dargestellt werden, wenn sie für die gesamte Stadtverwaltung von Bedeutung sein könnte. Das vorliegende Rechtsgutachten bildet demgegenüber einen allgemeinen Rahmen. Es bildet damit nur die allgemeinen Regeln ab. Es ist nicht Gegenstand dieses Rechtsgutachtens, z.B. für den Bereich des Steuerrechts zu beurteilen, ob eine explizite steuerrechtliche Sonderregelung die Nutzung von Cloud-Lösungen verbietet.[6] Dies kann in Nachtragsgutachten vertieft werden.

9 Die Aussage darüber, ob die Stadt Zürich Cloud-Angebote einsetzen darf, hängt ab von einer Risikobeurteilung. Wie diese vorzunehmen sein wird, ergibt sich einerseits aus der *Rechtslage* (davon handelt das vorliegende Rechtsgutachten) sowie andererseits aus der *Faktenlage* (und diesbezüglich – um es vorwegzunehmen – ob genügende Massnahmen technischer, organisatorischer oder vertraglicher Natur umgesetzt sind).

10 Nicht Gegenstand dieser Analyse ist die Prüfung der *Faktenlage* von einzelnen Cloud-Angeboten der verschiedenen kommerziellen Cloud-Anbieterinnen, d.h. eine Prüfung der konkreten Ausgestaltung und Angemessenheit vertraglicher, organisatorischer und technischer Schutzmassnahmen im Lichte der Anforderungen an die Datensicherheit und den Informationsschutz. Diese Prüfung ist Gegenstand von Umsetzungsprojekten.

11 Was jedoch beschrieben wird ist, ob sich aus der *Rechtslage* ein besonderes Risiko ergibt, das die Stadt Zürich zu berücksichtigen hat. Aus der Analyse des vorliegenden Rechtsgutachtens ergibt sich, dass die häufig diskutierten Risiken des Zugriffs von Strafverfolgungsbehörden aus dem US-amerikanischen Ausland überbewertet werden (dazu Fragen #3, #4 und #5).

[4] Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB; SR 311.0).

[5] Anmerkung Laux Lawyers AG vom 13. Juli 2022: Es wurden im Rahmen der anknüpfenden Diskussionen insgesamt vier Fact Sheets erstellt (**FS01 – Anwendbares Recht**; **FS02 – Gerichtsstand**; **FS03 – Verschlüsselung**; **FS04 – Berufsgeheimnis**. Diese sind zum Schluss (ab Seite 72) in der jeweils aktuellsten Form angehängt.

[6] Das Beispiel Steuern ist *pars pro toto* gemeint. Der Vorbehalt erstreckt sich auch für andere Fälle, wo ein Sondergesetz eine spezifische Vorgabe macht (Beispiel: Eine Regelung in einem Sondergesetz könnte eine Speicherung von Daten im Ausland verbieten; eine solche Regel wird im vorliegenden Rechtsgutachten nicht reflektiert).

II. Teil 1: Konzeptionelle und rechtliche Grundlagen

A. Grundlegende Konzepte

1. Es geht um den Begriff «Offenbarung»

12 Wer für eine andere ein Geheimnis wahrt (die Geheimnisträgerin), hat zu kontrollieren, dass das Geheimnis keinen Unbefugten offenbart wird. *Geheimnisschutz* ist das Ziel und die *Verschwiegenheitspflicht* das zentrale Mittel zur Umsetzung. Offenbarung ist die Testfrage zur Prüfung, ob der Kernaspekt der Verschwiegenheitspflicht eingehalten ist.

13 Der Begriff der Offenbarung steht im Zentrum dieses Rechtsgutachtens. Damit ist gesagt, dass es um weitere Teilaspekte des Geheimnisrechts, welche auch zu einem wirksamen Geheimnisschutz gehören, wie z.B. Verwertungsverbote und Löschpflichten, nicht geht bzw. diese Aspekte hier im Wesentlichen ausgeklammert bleiben (es sei denn, dass diese Aspekte für eine realistische Risikobewertung massgeblich wären). Im Rahmen von Umsetzungsanleitungen oder anknüpfenden Ausführungen kann aber zu abgeleiteten Themen ergänzend Stellung genommen werden.

2. Man darf die Technizität nicht ausblenden

14 Die Gerichtspraxis weiss seit jeher, dass es auf die *Wirkung* einer Handlung oder Unterlassung ankommt.[7] Somit lautet die Formel im Wesentlichen wie folgt: Wer die Möglichkeit zur Kenntnisnahme setzt, ist gleich zu behandeln wie jene, die das Geheimnis der Nachbarin direkt ins Ohr flüstert. Das ist auch vernünftig. Aber die mit diesem Rechtsgutachten anzugehende Aufgabenstellung stösst auf eine weitere Komplexität: *Die Technizität*.

15 Glaubt man der Statistik der Rechtsprechung, schien die Aufgabenstellung früher etwas weniger vielschichtig gewesen zu sein. Es gab Fälle der *aktiven Offenbarung* zuhauf[8]; Fälle der *Offenbarung durch Unterlassung* scheinen dagegen äusserst selten vorgefallen zu sein.[9] Man hätte sich indes auch früher schon Fälle der Offenbarung durch Unterlassung vorstellen können.[10,11]

[7] Z.B. BGE 141 IV 249 E. 1.1; BGE 140 IV 11 E. 2.4.2.

[8] Fälle, die wie die nachfolgenden gelagert waren, hat es in der Rechtsprechung des Bundesgerichts und der kantonalen Gerichte zuhauf gegeben. Die handelnde Person hat die Offenbarung aktiv begangen, etwa wie folgt: ein Geheimnis explizit ausgeplaudert (und durch eine aktive Handlung mündlich offenbart); das Geheimnis auf einen Zettel geschrieben und der Gesprächspartnerin vis-à-vis hinübergeschoben (und durch eine aktive Handlung schriftlich offenbart); das Geheimnis auf das Tischtuch im Restaurant gekritzelt, um dann aufzustehen, damit die Neugierigen am Nachbartisch, die zuvor vom Gespräch nichts mitnehmen konnten, weil man diskret gesprochen hat, nur noch aufzustehen brauchten, um nachzulesen (durch eine aktive Handlung schriftlich offenbart); oder das Geheimnis auf Papier ausgedruckt und die Ausdrucke dann absichtlich, eventualvorsätzlich oder bewusst fahrlässig ins Altpapier geworfen hat, so dass es jede andere später im Vorbeigehen wahrnehmen könne (durch eine aktive Handlung, welche im Resultat die Offenbarung ermöglicht).

[9] Und wenn doch, so scheinen sie es nicht bis ans Bundesgericht «geschafft» zu haben.

[10] **Fall 1** – *Sachverhalt*: Die Einzelanwältin führt eine Kanzlei mit drei Zimmern und einem Toilettenraum. Im Besprechungszimmer hat sie gerade ihre Klientin empfangen. Nachdem die Besprechung bereits begonnen hat, verlässt die Anwältin für ca. fünf Minuten das Besprechungszimmer, damit die Klientin in Ruhe Akten studieren kann. Die Anwältin nutzt die Zeit dazu, die Toilette aufzusuchen. Derweil arbeitet das Sekretariat im Nebenraum eifrig an einer Eingabe und bemerkt nicht, dass die Klientin während der Abwesenheit der Anwältin in deren unverschlossenes Arbeitszimmer (Türe hat offen gestanden) eindringt und dort in Akten eines anderen Mandats wühlt. Die Klientin kann unbemerkt Geheimes wahrnehmen. *Würdigung*: Es liegt keine aktive Offenbarung vor. Es ist auch nicht so, dass die Anwältin vorsätzlich oder eventualvorsätzlich eine Situation geschaffen hat, die einer anderen die Möglichkeit der Kenntnisnahme eröffnet (gilt auch als aktive Offenbarung). Die Anwältin wollte diese Offenbarung gerade nicht. Und doch hat sie, obwohl sie hätte schützen müssen, keine oder zu wenig Schutzmassnahmen getroffen. Es liegt eine passive Offenbarung bzw. eine durch Unterlassen vor.

[11] **Fall 2** – *Sachverhalt*: Die Anwaltskanzlei führt einen Empfangsraum im Erdgeschoss. Von der Strasse ist der Bildschirm sichtbar, aber mit normalem Auge sieht man nichts von der Strasse aus. Die Gegenpartei benutzt ein neuartiges hochvergrösserndes Fernrohr und kann Geheimes vom Bildschirm ablesen. *Würdigung*: Die Anwaltskanzlei wollte die Offenbarung nicht, und doch ist sie geschehen. Die Anwaltskanzlei hat – mit Blick auf den bislang anerkannten Stand der Technik – Massnahmen getroffen (Distanz zum Fenster), damit man nichts auf dem Bildschirm erkennen kann. Nur hat sie nicht mit dem technischen Fortschritt gerechnet, weswegen es zur Offenbarung kam. Offenbarung durch Unterlassen.

16 Die Komplexität der *Technizität* ergibt sich aus dem aus vielen Einzelteilen zusammengesetzten Wirkzusammenhang, als der *Cloud Computing* begriffen werden muss.[12] Die Frage ist nun, ob sich aus einem solchen komplexen Wirkungszusammenhang, auf den man im öffentlichen Diskurs und in der Fachsprache als *Cloud Computing* referenziert, eine Offenbarung ergibt. Man muss nämlich von der Prämisse ausgehen, dass jede, die eine IT-Infrastruktur organisiert und sie beherrscht (sprich: eine Cloud-Anbieterin), in letzter Instanz Massnahmen treffen kann, um geheime Informationen der Kundin im Klartext einzusehen[13] (was, wenn es gemacht würde, eine Offenbarung sein könnte: Die *Büchse der Pandora* wäre ja geöffnet). Man könnte sagen: Da «die Cloud» die *Möglichkeit* der Kenntnisnahme eröffnet, wäre jede Nutzung der Cloud im Sinne der althergebrachten Rechtsprechung eine Offenbarung.

17 Dieses Rechtsgutachten legt nahe, dass dies eine fehlerhafte Rechtsanwendung wäre. Wer Recht anwendet, das nicht zum Sachverhalt passt, begeht einen Subsumptionsfehler. Die gefundene Rechtsfolge wäre rechtlich nicht haltbar. Die Formel «oder die Möglichkeit schafft» kann nicht unbesehen bzw. ohne Würdigung der technischen Realitäten auf die Cloud angewendet werden. Die Ausführungen in Anhang 2 zu diesem Rechtsgutachten sollten auch im Licht dieser Aussage gelesen werden.

18 Die Herausforderungen setzen sich fort: Die geltenden Gesetze unterscheiden nicht zwischen den verschiedenen Informationsebenen, die Herbert Zech[14] und vor ihm bereits Lawrence Lessig und Yochai Benkler[15] beschrieben haben. Marc Amstutz hat bislang am deutlichsten zum Ausdruck gebracht, dass es «nicht gut kommt», wenn man für das Informationsrecht statisches altes Denken bemüht.[16]

3. Informationsschutz heisst Perimeterschutz

19 Wie schützt man ein Geheimnis? Beziehungsweise, genereller: Wie schützt man Information vor unbefugten Zugriffen? Wenn man es nicht aufgeschrieben hat: Indem man niemandem davon erzählt. Wenn man es aufgeschrieben hat: Indem man es in ein verschlossenes Couvert legt. Und das Couvert in eine Box. Und die Box in einen abgeschlossenen Raum. Und wenn mehr als jemand Zutritt zu diesem Raum

[12] «Cloud ist Cloud» gilt zwar nicht, d.h.: Hinter dem Begriff «Cloud» verstecken sich technisch bzw. sachverhaltsmässig eine grosse Vielzahl von Angeboten. Und doch gilt für die meisten von ihnen, dass der Wirkzusammenhang in sachverhaltsmässiger Hinsicht vielschichtig und komplex ist, weil sich die technische Lösung aus verschiedenen Komponenten zusammenfügt, die sich nicht auf fünf Zeilen verständlich darlegen lassen: *Backsteine* (Rechenzentrumsbauten), *Blech und Kabel etc.* (Computing-Geräte mit Vernetzung, kurz: Hardware), *Software* auf einer Vielzahl von Ebenen (Virtualisierungsschicht, Betriebssysteme, Datenbanken, Anwendungsprogramme), *Menschen* (jene, welche Maschinen bedienen oder Geräte in die Rechenzentren hinein- oder hinaustragen), Abläufe (organisatorische Aspekte) sowie Regeln und Kontrollen (Gesetzesrecht sowie Verträge mit Anspruchsrechten, etc.). In Anhang 2 unterbreiten wir eine abstrakt gehaltene Schilderung dessen, wie eine hochskalierende IT-Infrastruktur, die den Namen «Cloud» verdient, verwaltet wird. Die Wirklichkeit ist indes noch komplexer.

[13] Siehe z.B. den Fall ProtonMail: Der Dienst https://protonmail.com/ wirbt mit Ende-zu-Ende-Verschlüsselung, was – wenn es korrekt umgesetzt wird – eine Offenlegung des Inhalts der ausgetauschten Nachrichten mit einer sehr hohen (aber nicht 100%igen) Wahrscheinlichkeit ausschliesst. Nachrichten-Metadaten und Randdaten können aber auch von Protonmail eingesehen werden. Diesbezüglich ist Protonmail zwar nicht viel besser gestellt, als was auch beliebige Dritte mit Zugang zu gewissen Knotenpunkten im Internet erkennen können. Protonmail sitzt aber dennoch gleichsam «an der Quelle» und es ist für eine Strafverfolgungsbehörde einfacher, direkt auf Protonmail zuzugehen. Das Beispiel hat RA Martin Steiger aufgearbeitet: http://web.archive.org/web/20190524134759if_/https://twitter.com/martinsteiger/status/1126818939105886208 und https://steigerlegal.ch/2021/08/02/protonmail-daten-usa/; siehe auch: https://steigerlegal.ch/2019/07/27/protonmail-transparenzbericht-buepf (alles angesehen am 5. August 2021).

[14] HERBERT ZECH, Information als Schutzgegenstand, Basel 2012; nach Herbert Zech kann und muss man Information auf drei Ebenen beschreiben: *Semantische Information* wird durch ihren Aussagegehalt abgegrenzt (bei Lessig: «Content Layer», im IDG und damit auch in diesem Rechtsgutachten: «Informationen», ausser wenn es um Angaben über Personen geht, dann «Personendaten»), *syntaktische Information* durch ihre Darstellung als eine Menge von Zeichen (bei Lessig: «Code Layer», im IDG gibt es dafür keine Kategorie; in diesem Rechtsgutachten «Daten», ausser wenn der Begriff «Personendaten» verwendet wird – diesen Begriff verwenden wir in diesem Rechtsgutachten gleich wie das IDG, auf der Ebene des Content Layer) und *strukturelle Information* durch ihre Verkörperung (die Beschaffenheit der Oberfläche einer Schiefertafel spricht ebenfalls zum Menschen; diese Kategorie benötigen wir für dieses Rechtsgutachten nicht, da sonst die Komplexität unnötig gesteigert würde – man könnte aber selbstverständlich alle Aussagen in diesem Rechtsgutachten auch über diese dritte Ebene «laufen lassen» – das Rechtsgutachten würde immer noch Richtigkeit beanspruchen).

[15] LAWRENCE LESSIG, The Future of Ideas. The Fate of the Commons in a Connected World, New York 2002, S. 23; YOCHAI BENKLER, Federal Communications Law Journal, 2000, S. 562 ff.

[16] MARC AMSTUTZ: «Die meisten JuristInnen begreifen Daten von ihrem Inhalt (content) her, d.h. als Information. Sie denken semiotisch. Nur: die Digitalität kennt keine Semiotik. Sinnieren sie über Digitalität, tun sie das in den Kategorien der Hermeneutik. So wurden sie ausgebildet. Nur: die Digitalität kennt keine Hermeneutik.» Marc Amstutz schrieb dies als Einleitung zu einer Präsentation, die im Kontext zu seiner Forschung zum Eigentum an Informationen steht, das Zitat ist heute aber online nicht mehr verfügbar (MARC AMSTUTZ, Dateneigentum – Funktion und Form, AcP 218 [2018], 438ff.). Dieselbe Diskrepanz diskutiert Amstutz auch in einem Artikel mit dem Titel «Dateneigentum – Eckstein der kommenden Digitalordnung», in Neue Zürcher Zeitung, September 2018, S. 10.

haben muss: Durch Verfahren, die einer Person allein nicht die Möglichkeit der Einsichtnahme geben. Diese Methode erinnert erneut an Pandoras Büchse: Die Geheimnisträgerin erreicht das Ziel, Offenbarungen zu verhindern, indem sie ihre Einfluss- und Risikosphäre gegen «Löcher» absichert, durch welche das Geheimnis ansonsten (bei unterlassener Sicherung) Dritten bekannt werden könnte. Diese Absicherungsmassnahmen bezeichnen wir in diesem Rechtsgutachten als die Summe aller Massnahmen, die es benötigt, den eigenen Perimeter[17] zu sichern.

20 Im Cloud Computing geht es genauso um Perimeterschutz. Dieses Rechtsgutachten postuliert Folgendes: Massnahmen, die *rein faktisch* dazu führen, dass die Cloud-Anbieterin keinen Zugriff auf das Geheimnis nehmen, sichern den Perimeter der Organisationseinheit der Stadt Zürich ab. Das heisst konkret: Die Tatsache allein, dass die Stadt Zürich Geheimes auf fremden Infrastrukturen speichert, heisst nicht, dass sie diese Daten ausserhalb ihres Perimeters speichert. Wenn sie Massnahmen trifft, die *rein faktisch betrachtet* wirksam vor Zugriff schützen (obwohl die Daten auf fremden IT-Infrastrukturen gespeichert sind), hat sie ihren Perimeter ausgedehnt, gleichsam in die IT-Infrastrukturen der Cloud-Anbieterin «hinein». Umgangssprachlich: «Hauptsache ausreichend geschützt, wie – und auch wo – ist geheimnisrechtlich egal».

21 Warum ist dies die richtige Betrachtungsweise? Weil die Verschwiegenheitspflicht einen Erfolg sicherzustellen hat (keine Offenbarung). Juristisch gesprochen geht es um Folgendes: Art. 320 StGB ist ein Erfolgsdelikt. Das bedeutet – wiederum in der Alltagssprache – Folgendes: Ohne Offenbarung keine Strafbarkeit.

22 Dass das Recht der Stadt Zürich dieses so umrissene Modell des Perimeterschutzes geradezu idealtypisch abgebildet hat, ergibt eine Analyse des stadtzürcherischen Rechts (siehe hinten, Rz. 37).

23 Es geht u.a. um Zutritts- und Zugriffskontrolle. Perimeterschutz im so verstandenen Sinne verlangt mindestens die drei folgenden Arten von Perimeterschutzmassnahmen:

- Physischer Perimeter: Gebäude etc. sind vor Zutritt durch Unbefugte zu schützen. Dies geschieht massgeblich mit baulichen Massnahmen.
- Logischer Perimeter: Netzwerk und andere IT-Infrastrukturen sind vor dem logischen Zugriff durch unbefugte Dritte (Hacker, etc.) zu schützen.
- Personeller Perimeter: In der arbeitsteiligen Wirtschaft arbeitet niemand mehr allein. Eine Organisationseinheit z.B. muss aber gleichwohl jederzeit in der Lage sein zu beantworten, «wo die Behörde anfängt und wo sie aufhört». Dies geschieht durch angemessene Verträge mit jenen Personen und Unternehmen, welche die Organisationseinheit in ihrer Aufgabe unterstützen.

24 Dieser Betrachtungsansatz wurde bereits in einem öffentlich verfügbaren Rechtsgutachten von LAUX/HOFMANN/SCHIEWECK/HESS betreffend Cloud-Nutzung durch Banken dargestellt und soweit ersichtlich bis heute nicht ernsthaft in Frage gestellt.[18]

4. Reine Dienstgeheimnisse, reine Privatgeheimnisse und gemischte Geheimnisse

25 Ein Gemeinwesen kann selbstbestimmt darüber entscheiden, ob es in seinem Hoheitsbereich ein grundsätzliches Geheimhaltungsinteresse an Informationen hat (bzw. an welchen Informationen) oder

[17] Der Begriff «Perimeter» war ursprünglich ein Begriff aus der Mathematik und meinte die äussere Umrandung einer zweidimensionalen Figur. Dann wurde der Begriff auch in anderen Bereichen verwendet, z.B. im Gebäudebau (Gebäudeperimeter), in der Vermessung (die umgrenzende Linie einer Verwaltungseinheit, v.a. einer politischen), im Militär (räumliche Bezeichnung von Zonen, die es zu verteidigen gilt), und von dort her auch in der IT (ebenfalls zur Bezeichnung der zu verteidigenden Bereiche). Der Perimeter ist die Stelle, wo ein Raum endet und ein neuer anfängt. Der Begriff eignet sich gut, um auch für die Cloud zu definieren, wie ein Bereich, den die Stadt Zürich exklusiv für sich kontrollieren will, abzugrenzen ist von solchen, die für aussenstehende Dritte zugänglich sind. Rz. 23 nennt Perspektiven, die dabei eingenommen werden können.

[18] CHRISTIAN LAUX/ALEXANDER HOFMANN/MARK SCHIEWECK/JÜRG HESS, Rechtsgutachten zur Nutzung von Cloud-Angeboten durch Banken: Zur Zulässigkeit nach Art. 47 BankG (zit. SBVg-Gutachten), abrufbar unter: https://www.swissbanking.ch/de/downloads (angesehen am 31. Juli 2021).

nicht (Selbstorganisation).[19] Die Stadt Zürich hat sich z.B. auf den Öffentlichkeitsgrundsatz verpflichtet (Open Government Data) und macht ihr Staatshandeln weitgehend transparent bzw. öffentlich. Ungeachtet dessen werden gewisse Informationen nicht nach aussen getragen, was unter bestimmten Voraussetzungen zulässig ist (§ 23 IDG). Soweit die Stadt Zürich an einer Information ein Geheimhaltungsinteresse aufrecht erhält, ohne dass Private ihrerseits ein Interesse an der Geheimhaltung der betreffenden Information haben, spricht man von **reinen Dienstgeheimnissen**.[20]

26 Die Stadt Zürich kommt in Kontakt mit Informationen über Privatpersonen (Bevölkerung und sonstige Dritte wie z.B. Unternehmen). Gemäss IDG wird das Geheimhaltungsinteresse für solche Informationen vermutet (§ 23 Abs. 3 IDG). Man kann sie zunächst als **reine Privatgeheimnisse** denken. Wenn sowohl Private wie auch die Stadt Zürich selbst ein Interesse an der Geheimhaltung von Informationen im Hoheitsbereich der Stadt Zürich haben, spricht man von **gemischten Geheimnissen**. Da die Stadt Zürich immer auch am Schutz solcher Informationen interessiert ist (weil sie nach § 23 Abs. 3 IDG verpflichtet ist), werden Informationen mit Personenbezügen meistens gemischte Geheimnisse sein.

5. Informationsschutz bei der Behörde dient dem Vertrauensschutz

27 Die Verschwiegenheitspflicht dient dem Schutz der Willensbildung innerhalb der Behörde[21] und, soweit es um Privatgeheimnisse geht, nicht zuletzt dem Gesetzmässigkeitsprinzip (keine Drittrechte verletzen). Der Schutz in Bezug auf Privatgeheimnisse dient sodann auch dem Schutz des Vertrauens in die Institution des Staats: Der Staat ist kein Selbstzweck.[22] Er steht im Dienst der Bevölkerung. Er soll nicht willkürlich handeln und *sich nicht gegen seine Bevölkerung wenden* (Art. 13 Abs. 2 Bundesverfassung, BV: Persönliche Daten dürfen vom Staat nicht missbraucht werden). Insgesamt geht es bei allen genannten Schutzzielen darum, das Verwaltungshandeln voraussehbar zu machen, damit die staatliche Tätigkeit in geordneten Bahnen («*nachvollziehbar*», siehe FN 22) verläuft. Es geht letztlich um den Schutz der Verfassung und der Grundrechte. Das übergeordnete Schutzziel ist der *Vertrauensschutz*.

28 Diesem Schutzinteresse dient auch der Datenschutz.[23] Insofern verfolgt das verwaltungsrechtliche Datenschutzrecht (Rz. 76 ff.) dieselbe Stossrichtung wie das Amtsgeheimnis (Rz. 36 ff.). Man kann sogar eine gewisse Konvergenz dieser Regeln feststellen, worauf im Kontext der Entbindung vom Amtsgeheimnis genauer einzugehen sein wird (Rz. 44 ff.).

29 Folgendes bildet die verfassungs- und verwaltungsrechtlichen Grundlagen[24] des Vorstehenden: Datenschutz ist als Pflicht in der Bundesverfassung verankert (siehe oben, Art. 13 Abs. 2 BV). Wenn der Staat über eine Angelegenheit mit Bedeutung für die betroffene Person entscheidet, hat diese Anspruch auf Beurteilung durch eine richterliche Behörde (Art. 29a BV, Rechtsweggarantie). Dies sind inhaltliche Mindestgarantien in der Bundesverfassung, auf die später zurückzukommen sein wird. Jedenfalls kann man

[19] HANS SCHULTZ, Der Beamte als Zeuge im Strafverfahren, ZBl 86 (1985) 199. Zur Abgrenzung der Fragestellung im Verhältnis zu kantonalen Behörden und ihren Beamten siehe zudem BGE 87 IV 138, 142; BGE 94 IV 68, 69 f. Siehe auch BezGer ZH vom 10. Juni 1987, das in diesem Zusammenhang lapidar festhält: „Ein Amtsgeheimnis gemäss Art. 320 StGB liegt vor, wenn sich formell die Geheimhaltepflicht eines Beamten für Tatsachen, die er in seiner amtlichen Eigenschaft erfahren hat, aus dem kantonalen oder eidgenössischen Recht ergibt und materiell tatsächlich ein Geheimnis vorliegt" (ZR 1988 [87] Nr. 2 S. 3). Die Verschwiegenheitspflicht muss mindestens dem Erfordernis des Rechtssatzes genügen. URS SAXER, Möglichkeiten und Grenzen der Informationspolitik des Polizeidepartements und der Stadtpolizei Zürich vor dem Hintergrund gesetzlicher Geheimhaltungsverpflichtungen, namentlich von Art. 320 StGB, 38 (Rz. 88); offener BERNHARD ISENRING, in: Andreas Donatsch (Hrsg.), StGB/JStG Kommentar, 20. Aufl., Zürich 2018, Art. 320 N 7a ff.

[20] Zur Unterscheidung Dienst- und Privatgeheimnis THALMANN, Kommentar zum Zürcher Gemeindegesetz, 3. Auflage, Zürich 2000, § 71 N 7, 224; mit Ergänzungsband, Zürich 2011, § 71 N 1, 75.

[21] BGE 136 II 399 E. 2.3.2, wobei die Verschwiegenheit nicht das Vertrauen bzw. die Privatsphäre schützt, sondern das Kollegialitätsprinzip und die freie Meinungs- und Willensbildung innerhalb der Bundesregierung; SYLVAIN MÉTILLE, L'utilisation de l'informatique en nuage par l'administration publique, AJP 2019 609 ff., S. 612.

[22] In den Worten des IDG meint dies «Rechenschaftsfähigkeit», siehe § 5 Abs. 1 IDG: «Das öffentliche Organ verwaltet seine Informationen so, dass das Verwaltungshandeln nachvollziehbar und die Rechenschaftsfähigkeit gewährleistet ist.»

[23] JOHANNES EICHENHOFER, Privatheit im Internet als Vertrauensschutz, in: Der Staat 2016, 55(1), 41 ff., S. 50 f.

[24] Zu diesen allgemein: RENÉ WIEDERKEHR/PAUL RICHLI, Praxis des Allgemeinen Verwaltungsrechts, Band I, Bern 2012; PETER SAILE/MARC BURGHERR/THEO LORETAN, Verfassungs- und Organisationsrecht der Stadt Zürich, Zürich/St. Gallen 2009; sowie THALMANN (FN 20).

feststellen, dass eine Bearbeitung von Personendaten durch eine Behörde potenziell geeignet ist, die Bundesverfassung zu verletzen (Bundesverfassung tangiert). Eine solche Situation liegt auch vor, wenn eine schweizerische Behörde sich zum Einsatz einer Cloud-Lösung entscheidet.[25]

30 Ob eine Verletzung vorliegt oder nicht, richtet sich nach den folgenden etablierten Grundsätzen des Verfassungsrechts:

> ***Art. 5 Grundsätze rechtsstaatlichen Handelns***
>
> *[1] Grundlage und Schranke staatlichen Handelns ist das Recht.*
> *[2] Staatliches Handeln muss im öffentlichen Interesse liegen und verhältnismässig sein.*

31 Dies bedeutet Folgendes: Behörden haben nur dort eine Aufgabe, wo das Gesetz ihnen eine zuweist (Art. 5 Abs. 1 BV). Weitere Grundprinzipien des Verwaltungsrechts – Art. 5 Abs. 2 BV: Tätigwerden nur im öffentlichen Interesse und der Verhältnismässigkeitsgrundsatz – binden Behörden zusätzlich zurück: Dies ist im Kern der gesetzliche Rahmen, der auch für das vorliegende Rechtsgutachten relevant ist. Und die Erfahrung zeigt, dass gesetzliche Grundlagen zur Gestaltung der Bedarfsverwaltung regelmässig vorhanden sind (dazu gehört auch der Entscheid, eigene IT-Bedürfnisse mit einer Cloud-Lösung zu befriedigen), und dass der Wunsch, Effizienz und Sicherheit mit Hilfe einer Cloud-Anbieterin zu lösen, einem öffentlichen Interesse entspricht.

32 Die folgenden Ausführungen finden in der aktuellen Diskussion allerdings nicht immer in ihrer vollen Ausprägung Gehör:

1. *Erstens* leitet sich aus dem Verhältnismässigkeitsgrundsatz die Pflicht der Behörde zur Auswahl reifer und sicherer Cloud-Lösungen ab.[26] Die Behörde bleibt in der Verantwortung, für ein angemessenes Lösungsdesign zu sorgen (in der Praxis wird dies nach einem Shared Responsibility-Modell ausgestaltet sein) und sie muss der Cloud-Anbieterin verbindliche Vorgaben machen, z.B. in Bezug auf die Nutzung von Daten, so dass die Cloud-Anbieterin in ihrem Alltag dafür sorgen kann, dass sie der Sondersituation der Behörde gerecht wird.

   Man kann es nicht genug betonen: Wer Cloud-Lösungen einsetzt, muss die damit einhergehenden Risiken im Griff haben. Das heisst, die Behörde hat die Kontrolle zu behalten. Kontrollieren kann nur wer auch versteht. Wer die Risiken versteht, kann sie sichern, bis sie unter Kontrolle sind, damit das Risiko vertretbar wird. Die Behörde muss die eingesetzten Lösungen so sichern, dass sie mit Blick auf die Aufgabenstellung als angemessen erscheinen.[27]

2. *Zweitens* leitet sich aus einer technisch reifen Lösung direkt die *verwaltungsrechtliche Rechtmässigkeit* der Cloud-Nutzung ab. Hält die Behörde die Verhältnismässigkeit ein, dann ist die Behördentätigkeit erlaubt – dies ist die direkte Ableitung aus Art. 5 Abs. 2 BV.

33 Dies scheint auf den ersten Blick ein Widerspruch zu sein zu jenen Stellungnahmen, die dafürhalten, dass der Staat nur Lösungen wählen kann, die allerhöchsten Ansprüchen genügen – was ein strengerer Massstab zu sein scheint. Ein solcher Widerspruch besteht jedoch nur für jene, die behaupten, das «allerhöchste Sicherheitsniveau» habe durchs Band hindurch immer dann zum Einsatz zu kommen, wenn eine Behörde Personendaten oder Daten unter dem Amtsgeheimnis in die Cloud speichern will.[28] Das wäre in der Tat ein Widerspruch zum Verhältnismässigkeitsgrundsatz; denn dieser verlangt nicht statisch-abstrakte Antworten, sondern eine spezifische Risikoabwägung unter Würdigung der konkreten Umstände.

[25] Vgl. SÖNKE E. SCHULZ, Cloud Computing in der öffentlichen Verwaltung, in: Verwaltung & Management 2010, 16(1), 36 ff., S. 38.

[26] WOLFGANG STRAUB, Cloud Verträge – Regelungsbedarf und Vorgehensweise, in: AJP 7/2014, S. 912.

[27] Vgl. STRAUB (FN 26), S. 912.

[28] Siehe etwa die strengen Empfehlungen dieses Merkblatts: ÖDSB, Merkblatt über die Auslagerung der Datenbearbeitung des Staates Freiburg in eine Cloud, 28. August 2017, abrufbar unter: https://www.fr.ch/sites/default/files/2019-11/ATPrD_externalisation%20dans%20un%20Cloud%20-%20D.pdf (angesehen am 14. September 2021).

34 Insofern bedeutet Angemessenheit letztlich «situativ angemessen». Und aus diesem Fazit leitet sich Verschiedenes ab, z.B. auch, dass die Behörde – selbst bei Einsatz einer Cloud-Lösung – keine 100%ige Sicherheit abzusichern hat, sondern nur jene, die nach der allgemeinen Lebenserfahrung und dem gewöhnlichen Lauf der Dinge sichert, dass das Vertrauen der Bevölkerung in das ordnungsgemässe Funktionieren der Behördentätigkeit nicht beeinträchtigt wird.[29] Diese Erkenntnis deckt sich mit der Würdigung, die sich im Kontext der strafrechtlichen Prüfung ergibt (dazu hinten, Rz. 84 ff.).

35 Die verwaltungsrechtliche Ableitung lautet: Cloud Computing ist für Behörden zulässig, sofern die Sicherung und Einbindung in die eigenen Abläufe die Anforderungen erfüllt. Auf das Datenschutzrecht (Rz. 76 ff.) und auf das Amtsgeheimnis (Rz. 84 ff.) wird separat noch einzugehen sein (die Resultate sind aber deckungsgleich, soviel sei vorweggenommen; siehe auch vorn, Rz. 28: «Konvergenz»).

B. Informationsschutz in der Stadt Zürich

1. Die Stadt Zürich muss Geheimnisse kraft kantonalen Rechts schützen

36 Die Kompetenz zur Selbstorganisation (vorn Rz. 25) ist für Gemeinden wie die Stadt Zürich beschränkt. Den Rahmen bilden das kantonale Recht bzw. das Gemeindegesetz (GG; LS 131.1) sowie das Gesetz über die Information und den Datenschutz (IDG; LS 170.4): Im Gemeindegesetz ist die Schweigepflicht von Behördenmitgliedern und Gemeindeangestellten geregelt (§ 8 GG), während das IDG festhält, unter welchen Voraussetzungen es zulässig oder notwendig ist, Informationen anderen nicht mitzuteilen (§ 23 IDG).

2. Die Stadt Zürich hat Reglemente zum Perimeterschutz erlassen

37 Daneben finden sich auch auf städtischer Ebene Regeln zum Geheimhaltungsinteresse der Stadt Zürich an Informationen.[30] Es ist hier nicht der Raum, diese zu vertiefen. Festzuhalten ist aber Folgendes: Das Verwaltungsrecht fordert Verschwiegenheit, soweit nicht Grundsätze von Open Government Data gelten.[31] Die städtischen Reglemente über mobiles Arbeiten, über Fernwartung und über die Nutzung elektronischer Infrastrukturen oder Dienste der Stadt Zürich zielen allesamt darauf ab, den Perimeter (zu dem hier verwendeten Begriffsverständnis siehe vorn, Rz. 19 ff.) zu schützen. Beispielhaft kann auf Art. 9 des Reglements über mobiles Arbeiten (Gewährleistung der Vertraulichkeit) sowie auf Art. 13 des Reglements über Fernwartung (REFE, Bewilligungspflicht für Fernwartungen) und auf Art. 8 des Reglements über die Nutzung elektronischer Infrastrukturen oder Dienste der Stadt Zürich (Verbot der automatischen Um- oder Weiterleitung von E-Mails an E-Mail-Adressen ausserhalb des Stadtnetzes) verwiesen werden.

3. Die Stadt Zürich hat sich eine Informationsklassifizierung gegeben

38 Die Stadt Zürich hat sich eine Informationsklassifizierung gegeben, um dieses Regelsystem abzubilden:[32]

[29] Vgl. PETER KARLEN, in: Peter Karlen/Susan Hodel (Hrsg.), Schweizerisches Verwaltungsrecht: Gesamtdarstellung unter Einbezug des europäischen Kontextes, 7. Aufl., Zürich 2018, S. 125.

[30] Zunächst ist auf die allgemeine Grundlagenordnung der Geheimhaltung gemäss Art. 80 des städtischen Personalrechts (PR; 177.100) hinzuweisen: «***(1)** Die Angestellten sind zur Verschwiegenheit über dienstliche Angelegenheiten verpflichtet, die ihrer Natur nach oder gemäss besonderer Vorschrift geheim zu halten sind.* ***(2)** Diese Verpflichtung bleibt nach Beendigung des Arbeitsverhältnisses bestehen.*» Ergänzend kann angemerkt werden, dass die «Grundsätze über die Schweigepflicht» (177.130) vom 20. Mai 1949 mit Wirkung auf den 1. September 2010 ausser Kraft gesetzt worden sind. Sodann kennt das stadtzürcherische Recht für besondere Rollen spezialgesetzlich statuierte Geheimhaltungspflichten.

[31] Siehe etwa die «Strategie für offene Verwaltungsdaten in der Schweiz 2019-2023», die vom Bundesrat am 30. November 2018 gutgeheissen wurde, abrufbar unter: https://fedlex.data.admin.ch/eli/fga/2019/125 (angesehen am 14. September 2021).

[32] Formular «ISDS-Grundlageninformationen» (Informationssicherheit und Datenschutz) der Stadt Zürich (Stand 30. Juni 2021).

- **Nicht klassifiziert** – Die niedrigste Vertraulichkeitsstufe gilt für Informationen, die uneingeschränkt öffentlich zugänglich gemacht werden können.
- **Intern (Grundwert)** – Der Grundwert von Informationen in der Stadt Zürich ist «intern». Erfasst sind Informationen, die verwaltungsintern zu behalten sind. Verwaltungsintern besteht jedoch unter dem Aspekt der Vertraulichkeit keine besondere Beschränkung von Zugriffsrechten. Innerhalb der Stadt Zürich spricht man hier auch von Informationen mit normalem Schutzbedarf.
- **Vertraulich / Streng Vertraulich** – Als vertraulich oder als Informationen mit besonderem Schutzbedarf werden in der Stadt Zürich Informationen bezeichnet, die nur Berechtigten zugänglich gemacht werden dürfen. Dies verlangt nach einer auch verwaltungsintern wirkenden Beschränkung von Zugriffsrechten. Personendaten werden dieser Kategorie zugeordnet.

39 Diese Zuordnungskriterien ziehen nach sich, dass der Kreis jener, die Einsicht in Daten erhalten dürfen, immer enger wird. Insofern hat die Differenzierung eine Bedeutung. Man kann aber im Gesetzesrecht der Stadt Zürich oder des Kantons Zürich kaum eine Regel erkennen, die eine Sonderbehandlung der Informationen innerhalb der Informationen mit besonderem Schutzbedarf (vertraulich / streng vertraulich) nach sich ziehen würde. Als seltenes Beispiel einer Regel mit Differenzierung kann § 25 Abs. 3 IDV (Genehmigungspflicht bei der Auslagerung von besonderen Personendaten[33]) herhalten. Zu nennen sind auch die gesteigerten Anforderungen an die Informationssicherheit, wenn besondere Personendaten verarbeitet bzw. extern gespeichert werden gemäss dem Handbuch Informationssicherheit.[34]

4. Die verwaltungsrechtliche Verschwiegenheitspflicht gilt nicht absolut

a. Allgemeine Ausnahmen

40 Die der Organisationseinheit auferlegte Schweigepflicht gilt nicht absolut. Die Vertraulichkeit ist nur (aber immerhin) im Rahmen einer *Interessenabwägung* zu schützen, was sich aus den nachstehend besprochenen Regeln ergibt. Dass zusätzlich Ausnahmen von der Schweigepflicht bestehen (Mitteilungsrechte[35] oder -pflichten[36], Anzeigepflichten[37]), ist für die Zwecke des vorliegenden Rechtsgutachtens ohne Belang. Relevant und zu diskutieren ist, dass das Recht weitere Regeln bereithält, welche den Geltungsanspruch des behördlichen oder privaten Geheimhaltungsinteresses durchbrechen.

41 Dabei ist hier noch nicht einmal die strafrechtliche Rechtfertigungsregelung nach Art. 14 StGB[38] gemeint (diese gilt es erst zu diskutieren, wenn eine verbotene Offenbarung stattgefunden hat). Vielmehr geht es um Regeln, welche letztlich nur verwaltungsrechtlich erklärt werden können, wie zum Beispiel die *reaktive Entbindung* vom Berufsgeheimnis im Rahmen des Zivil- oder Strafprozesses (dazu Rz. 115) oder die *proaktive Entbindung* vom Berufsgeheimnis für Projekte, in denen unklar ist, ob die für die Organisationseinheit geltenden Vorschriften vollständig umgesetzt werden können. Auf die *proaktive Entbindung* wird anschliessend vertieft eingegangen. Sie ist für das Thema des vorliegenden Gutachtens von Interesse.

b. Einschränkung durch erstinstanzliches Verwaltungshandeln

42 Die Nutzung von Cloud-Infrastrukturen zur Erledigung von Behördenaufgaben kann z.B. als faktisches

[33] Dazu mehr hinten, Rz.55 ff., 60.

[34] Siehe z.B. das Handbuch Informationssicherheit der Stadt Zürich, aktualisiert mit Beschluss des Stadtrats vom 9. Juli 2014 (FN 3).

[35] Beispiel: § 15 Abs. 4 des kantonalzürcherischen Gesundheitsgesetzes (GesG; LS 810.1).

[36] Zum Beispiel nach dem IDG.

[37] Beispiel: § 15 Abs. 3 GesG.

[38] Art. 14 StGB lautet wie folgt: *«Wer handelt, wie es das Gesetz gebietet oder erlaubt, verhält sich rechtmässig, auch wenn die Tat nach diesem oder einem andern Gesetz mit Strafe bedroht ist.»*

Verwaltungshandeln verstanden werden.[39] Es ist hier in Erinnerung zu rufen, dass ein Tätigwerden unter Wahrung der Verhältnismässigkeit mit gesetzlicher Grundlage und im öffentlichen Interesse faktisch auf eine Einschränkung auch privater Geheimhaltungsinteressen hinausläuft. Zwar haben private Geheimhaltungsinteressen verfassungsrechtlichen Gehalt (vorn, Rz. 29). Zugleich ist rechtmässiges Verwaltungshandeln im Rahmen von Art. 5 BV möglich, auch wenn private Geheimhaltungsinteressen tangiert sind (vorn, Rz. 31). Wenn sich nach der Prüfung der bekannten Anforderungen (gesetzliche Grundlage, öffentliches Interesse und Verhältnismässigkeit) zeigt, dass die verfassungsrechtlichen Voraussetzungen auch zu Einschränkungen gegeben sind, bedeutet dies, dass das Staatshandeln rechtmässig ist. Mit anderen Worten ist auch die Einschränkung des entsprechenden Rechts rechtmässig. Nukleus der Rechtmässigkeitsprüfung ist dabei, dass die Stadt Zürich durch die Cloud-Nutzung eine Offenbarung gerade nicht will (hinten, Rz. 86 f.). Damit ist auch das Amtsgeheimnis nicht verletzt, was auf Ebene der Prüfung der Gesetzmässigkeit von Bedeutung ist.

43 Verkürzt bedeutet dies, dass – soweit sich aus der Nutzung einer Cloud-Infrastruktur überhaupt eine erhöhte Gefährdung der geheim zu haltenden Information ergeben sollte – die Behörde eine allenfalls privat bestehende Anspruchsposition wegen der durch die erhöhte Gefährdung begründbaren Verletzung im Rahmen des erstinstanzlichen Verwaltungsverfahrens rechtmässig einschränkt. Wer dies anders sieht, müsste sich mittels verwaltungsrechtlicher Beschwerde gegen das faktische Verwaltungshandeln wehren.[40] Dabei dürften auch Fragen der formellen und materiellen Rechtskraft massgeblich werden, worauf an dieser Stelle nicht weiter einzugehen ist.[41]

c. Entbindung vom Geheimnis als Instrument zur Planung interner Abläufe

(i) Vorbemerkungen

44 Üblicherweise denkt man an die Entbindung als Reaktion auf eine entsprechende Anfrage im Zivil- oder Strafprozess. Die Entbindung kann aber auch antizipierend von der vorgesetzten Behörde «abgeholt» werden, worauf zum Beispiel im Bundesumfeld das Informatiksteuerungsorgan des Bundes ausdrücklich hingewiesen hat (dazu sogleich, Rz. 45).

45 Das ehemalige Informatiksteuerungsorgan Bund (heute: Bundeskanzlei, hernach gleichwohl als «ISB» bezeichnet) hat präzisierende Richtlinien zum Umgang mit dem Dienstgeheimnis in IT-Infrastrukturen erlassen (hernach: Richtlinien ISB)[42]. Darin sind Massnahmen für den Fall vorgesehen, dass die Behörde, die IT-Infrastrukturen eines Dritten nutzen will, im Kontext jenes Vorhabens eine Offenbarung von Geheimnissen nicht zweifelsfrei ausschliessen kann. Das ISB differenziert dabei nach Dienstgeheimnissen (d.h. Geheimnissen, welche die Sphäre der Behörde betreffen bzw. Informationen, welche diese Sphäre beschreiben) und Privatgeheimnissen (d.h. Geheimnissen, welche die Sphäre von ausserhalb der Bundesverwaltung stehenden Dritten beschreiben; zu dieser Unterscheidung bereits vorn, Rz. 25 f.).[43] Das ISB empfiehlt und «instruiert» Bundesstellen, dass die Leistungsbezügerin (d.h. die Dienststelle, entsprechend im Kontext der Stadt Zürich: die Organisationseinheit) im Voraus die schriftliche Einwilligung der vorgesetzten Behörde – im Sinne einer vorangehenden *Genehmigung der Nutzung* – einholen solle. Andernfalls könnten sich die (allenfalls) offenbarenden Mitarbeitenden strafbar

[39] Vgl. KARLEN, in: Karlen/Hodel (FN 29), S. 260.

[40] KARLEN, in: Karlen/Hodel (FN 29), S. 260 f.

[41] Siehe m.w.H. zum Rechtsschutz gegen Realakte: JULIAN-IVAN BERGIER/ANDREAS GLASER, Rechtsschutz gegen Realakte: Bundesgericht schafft Klarheit, in: SJZ 111/2015, S. 169 ff.

[42] Informatiksteuerorgan des Bundes ISB, Anforderungen angesichts des Risikos von Amtsgeheimnisverletzungen in der Bundesverwaltung, Version 1.0 vom 1. März 2017. Die aktuellste verfügbare Version ist vom Nationalen Zentrum für Cybersicherheit NCSC, Si001-Hi03 – Anforderungen angesichts des Risikos von Amtsgeheimnisverletzungen in der Bundesverwaltung, Version 1.4 vom 1. April 2021.

[43] Der Passus mit dieser Unterscheidung fehlt in der aktuellsten verfügbaren Version 1.4 des NCSC (siehe FN 42).

machen.[44] Die strafbefreiende Wirkung einer solchen proaktiven Genehmigung könnte angezweifelt werden, da die Entbindung eine auf den Einzelfall bezogene Interessenabwägung voraussetzt.[45]

46 Die folgenden Beispiele im stadtzürcherischen Recht (Rz. 47 – Rz. 56) sollen zeigen, dass das Institut der proaktiven Genehmigung innerhalb der Stadt Zürich bereits etabliert ist. Auf dieser Grundlage soll beurteilt werden, wie in der Stadt Zürich mit dem Instrument der proaktiven Genehmigung umgegangen werden könnte. Nachdem gezeigt wird, dass das Institut der proaktiven Genehmigung im stadtzürcherischen Recht nicht nur im Kontext von Art. 320 Ziff. 2 StGB existiert, wird aufgezeigt, wie im Zusammenwirken mehrerer Stellen die Anforderungen von Gesetz und herrschender Lehre umgesetzt werden können (die *vorgesetzte Stelle* erteilt die Genehmigung *konkret* und nach Vornahme einer *umfassenden Interessenabwägung* sowie *schriftlich*).

(ii) Beispiele

47 Im stadtzürcherischen Recht findet man Beispiele für Genehmigungsszenarien bei unvollkommener Faktenlage (hernach [a] und [b]), ebenso wie Genehmigungsszenarien, die eher Compliance absichern (hernach [c]) oder das Vertrauen in die ordnungsgemässe Abwicklung von Projekten stärken wollen (hernach [d]).

(a) *Technisch* unvollkommener Auslagerungssetup (Genehmigungspflicht)

48 Mit Beschluss vom 9. Juli 2014 hat der Stadtrat der Stadt Zürich das «Handbuch Informationssicherheit der Stadt Zürich» in Kraft gesetzt («HISi», STRB Nr. 634). Es hat stadtweite Sicherheitsanforderungen definiert und ist z.B. auch an die Stelle der in Art. 10 des Reglements Fernwartung (236.200, hernach als REFE bezeichnet) genannten Anforderungen getreten. Wenn die Stadtverwaltung mit Dritten zusammenarbeitet und/oder Leistungen für Dritte erbringt, müssen entsprechende Verbindlichkeiten bezüglich der Informationssicherheit in den Verträgen geregelt werden. Der Stadtrat hat eine klare Weisung dahingehend erlassen, dass das HISi bei neuen Projekten stets zur Anwendung kommen muss.

49 Im Einzelfall kann die verantwortliche Organisationseinheit der Stadt Zürich vom Basisschutz im Sinne einer Unterschreitung über den Umsetzungszeitplan hinaus abweichen (was nur mit zeitlicher Befristung geschehen soll[46]). Dies löst jedoch ein *Genehmigungsverfahren* aus (STRB Nr. 634, Ziffer 7): Die Organisationseinheit hat die durch die Unterschreitung entstehenden Risiken zu identifizieren, zu quantifizieren und in einem Antrag der Fachstelle Informationssicherheit zur Beurteilung und Stellungnahme zu unterbreiten. Diese informiert die IT-Delegation über die zwischen ihr und den Organisationseinheiten vereinbarten Ausnahmen. Wenn keine Vereinbarung getroffen werden kann, entscheidet die IT-Delegation über das weitere Vorgehen[47] (siehe zum Vergleich auch Art. 13 Abs. 4 lit. a REFE).

50 Das im HISi bzw. im Stadtratsbeschluss vom 9. Juli 2014 beschriebene Genehmigungsverfahren bettet sich lückenlos in das Entbindungskonzept gemäss Art. 320 Ziff. 2 StGB ein (wie es auch das ISB für den Bund etabliert hat, Rz. 45): Ist die Faktenlage in technischer Hinsicht ungenügend bzw. ist absehbar, dass der Basisschutz im Umsetzungsprojekt nicht erreicht werden kann, entsteht eine Gefährdungssituation, die potenziell zu einer Verletzung des Amtsgeheimnisses führen könnte. Mit der Entbindung (im Sinne einer proaktiven Entbindung) durch das Fachgremium werden sowohl disziplinar- als auch strafrechtliche Sanktionen abgewendet, wobei an die Stelle der hierarchisch übergeordneten Stelle mit dem

[44] Dieser Passus ist in der aktuellsten Version 1.4 auch enthalten (siehe FN 42).

[45] Z.B. für den Strafprozess: Art. 170 Abs. 3 StPO; dazu BGE 147 IV 27 ff. Siehe auch WOLFGANG WOHLERS, Kommentar zum Strafgesetzbuch, Bern 2020, StGB 320 N 9; siehe auch Entscheid des Bundesgerichts 1P.156/2004 vom 28.6.2004, E. 2.2.1.

[46] Nach dem Stadtratsbeschluss vom 9. Juli 2014 kann eine solche Ausnahme aus organisatorischen, technischen, wirtschaftlichen oder rechtlichen Gründen naheliegen.

[47] Inwiefern sich im Anwendungsbereich von Art. 10 REFE (Zuständigkeit des Vorstehers bzw. der Vorsteherin des städtischen Finanzdepartements) allenfalls ein Kompetenzkonflikt ergeben könnte, braucht nicht im Rahmen des vorliegenden Gutachtens analysiert zu werden.

Willen des Gesamtstadtrats ein Fachgremium tritt. Dieses ist am besten geeignet, die Angemessenheit der Einschätzung der auslagernden Organisationseinheit zu beurteilen.

(b) *Rechtlich* unvollkommene Ziel-Rechtsordnung (Genehmigungspflicht)

51 Nach STRB Nr. 634, Ziffer 7 (ebenso Art. 13 Abs. 4 lit. c REFE) ist die proaktive Genehmigung eines IT-Vorhabens auch dann vorgesehen, wenn im Rahmen einer Fernwartung, die von einem sog. «unsicheren» Ausland ausgeht, Klartextzugriff auf Daten genommen werden soll, die dem Amtsgeheimnis unterstehen (Klassierung vertraulich oder streng vertraulich, zur Klassierung siehe vorn, Rz. 38). Die Nähe zur Entbindung vom Amtsgeheimnis bzw. zu Art. 320 Ziff. 2 StGB ist unverkennbar, handelt es sich bei Informationen mit der Klassierung vertraulich bzw. streng vertraulich doch regelmässig um solche, die dem Amtsgeheimnis unterstehen werden.

52 Auch wenn das Zielland gleichsam «rechtlich unvollkommen» ist, sollen Auslagerungen möglich bleiben. Um in einer solchen Konstellation aber die Risiken einer Rechtsverletzung zu mildern, bedarf es abermals einer Genehmigung. Ablauf und Wirkungen der Genehmigung ergeben sich per Analogie aus den Ausführungen in Rz. 48 – Rz. 66. Es bedarf in einem solchen Fall – jedenfalls bei Fernwartung bzw. Anwendbarkeit des Art. 13 REFE – zudem einer Vorprüfung und Stellungnahme der/des städtischen Datenschutzbeauftragten (Art. 13 Abs. 4 REFE; fast deckungsgleich wohl die Regelung in § 19 lit. c IDG und § 22 Abs. 2 IDV).

(c) *Compliancemässig* unvollkommene Vertragsdokumentation (Genehmigungspflicht)

53 Kann die Organisationseinheit die in Art. 11 REFE formulierten Anforderungen nicht umsetzen, bleibt eine Auslagerung möglich; nur muss die Vorsteherin bzw. der Vorsteher des städtischen Finanzdepartements seine Genehmigung erteilen (Art. 13 Abs. 4 lit. b REFE).

54 Die Genehmigung nach Art. 11 REFE zielt hier darauf ab, die Einhaltung formeller (der Effizienz geschuldeter) Vorgaben routinemässig sicherzustellen bzw. Ausnahmen zu dokumentieren. Ziel ist Compliance – d.h. sicherstellen, dass Vorgaben gelebt werden.

(d) Besondere Personendaten (§ 25 Abs. 3 IDV: Genehmigungspflicht)

55 Auch die Genehmigungspflicht nach § 25 Abs. 3 IDV kann besser verstanden werden, wenn man sie mit der proaktiven Entbindung vom Amtsgeheimnis (Rz. 41) vergleicht. Die Genehmigung nach § 25 Abs. 3 IDV hat die Wirkung eines «Sicherungsankers» bzw. sie dient der Wahrung des behördeninternen Vier-Augen-Prinzips. Es soll sichergestellt sein, dass das Projekt auf soliden Grundlagen steht. Im Rahmen der Genehmigung nach § 25 Abs. 3 IDV prüft die vorgesetzte Stelle namentlich, ob die folgenden Massnahmen der Datensicherheit umgesetzt worden sind: (1) Vorliegen angemessener Schutzmassnahmen (§ 7 Abs. 1 IDG, § 25 Abs. 2 IDV); (2) Organisationsvorschriften (§ 13 Abs. 1 IDG, mit Konkretisierung in § 26 IDV); (3) Massnahmen gemäss Rz. 80.

56 Das Ziel von § 25 Abs. 3 IDV ist es nicht (anders als im Kontext von Art. 11 und Art. 13 REFE), die Folge von Unvollkommenheiten im Setup aufzufangen bzw. würdigend einordnen zu können, sondern schlicht, der besonderen Rolle von besonderen Personendaten gerade im Behördenumfeld gerecht zu werden.[48] Mit anderen Worten: Einer Genehmigung bedarf es auch dann, wenn der Setup nicht unvollkommen ist.

[48] Besondere Personendaten sind nicht zuletzt deswegen besonders, weil man sie als besondere Kategorie definiert hat. Diese gesetzgeberische Massnahme ist berechtigt, was uns die Geschichte lehrt (zu erinnern ist an die Verfolgung von Personen durch Unrechtsregimes aufgrund von Aspekten, die «an der Haut kleben» – rassische Merkmale – oder untrennbar mit der Identität der Person verbunden sind, wie z.B. Religion oder Weltanschauungen). Es gibt diese Kategorie gerade deswegen, weil das Vertrauen in die Behördentätigkeit abzusichern ist (vorn, Rz. 27 f.).

d. Würdigung

(i) Verwaltungs- und strafrechtliche Wirkung des Genehmigungsprozesses

57 Die beiden zuerst genannten Beispiele (Rz. 48 ff.: technisch unvollkommen, und Rz. 51: rechtlich unvollkommen) wirken als Entbindung vom Amtsgeheimnis, wobei die formellen Voraussetzungen nach Art. 320 Ziff. 2 StGB zusätzlich einzuhalten sein werden. Dies gilt ungeachtet dessen, dass Art. 13 Abs. 4 lit. a/c REFE und der Stadtratsbeschluss vom 9. Juli 2014 (Rz. 48) dies nicht ausdrücklich festhalten. Die verwaltungsrechtliche Motivation der Regel (dazu Rz. 58) zieht die strafrechtliche Genehmigungswirkung (Rz. 60) notwendigerweise nach sich und lässt somit keinen anderen Schluss zu.

58 Die *verwaltungsrechtliche Motivation* der Regelung ist schnell ersichtlich: Die Genehmigungsregel bezweckt, das Vorhaben nach Abwägung der involvierten Interessen und nach Verhältnismässigkeitsprüfung kontrolliert würdigen zu können, damit sich auch für nicht ganz eindeutige Konstellationen eine Lösung finden lässt. Der Vorgang hat verwaltungsrechtliche Bedeutung, weil eine bestimmte Stelle eingesetzt wird, den Willen der Organisationseinheit auf Umsetzung eines bestimmten Vorhabens zu stützen. Die eingesetzte Stelle ist bei technischen Unzulänglichkeiten nur indirekt vorgesetzte Stelle: Sie handelt aber gestützt auf eine Delegation des Stadtrats und damit anstelle des Stadtrats, der hierarchisch und politisch betrachtet in jedem Fall als vorgesetzte Stelle im Sinne von Art. 320 Ziff. 2 StGB gilt. [49] Der Entscheid der Stelle hat den Charakter einer Weisung in die Organisation hinein (dass das beantragte Vorhaben von der Stadt Zürich gewollt ist) und stellt insofern eine verbindliche Klärung des Willens der Stadt Zürich dar. Damit sind verbundene disziplinarrechtliche Sanktionen für weisungsgemässes Verhalten nicht mehr vorstellbar.

59 Aus *strafrechtlicher Sicht* bedeutet dies Folgendes: Mit Vorliegen einer derart verbindlichen verwaltungsrechtlichen Klärung des Willens der Stadt Zürich ist es nicht mehr denkbar, von Strafbarkeit der konkret handelnden Personen zu reden, wenn sie sich weisungsgemäss verhalten (die zur Klärung eingesetzte Stelle setzt in Vertretung des Stadtrats ihren Willen an die Stelle des Willens der handelnden Personen). Dies ist nichts anderes als eine strafrechtlich wirksame Genehmigung. Für die mit dem unvollkommenen Setup verbundenen Risiken haben die handelnden Personen nicht mehr einzustehen. Damit verbundene strafrechtlichen Sanktionen sind somit ebenfalls abgewendet.[50]

(ii) Zu § 25 Abs. 3 IDV insbesondere

60 Die Genehmigung nach § 25 Abs. 3 IDV kann gleichermassen eine strafrechtlich relevante proaktive Genehmigung im Sinne von Art. 320 Ziff. 2 StGB mit einschliessen, wie sie nur datenschutzrechtlich verstanden werden kann. Hintergrund ist, dass die Genehmigung sowohl nach § 25 Abs. 3 IDV ebenso wie nach Art. 320 Ziff. 2 StGB von der vorgesetzten Stelle ausgeht.

61 Wie gezeigt (Rz. 56) zielt § 25 Abs. 3 IDV – im Ursprung wohl – eher nicht auf eine strafrechtliche Genehmigungswirkung im Sinne von Art. 320 Ziff. 2 StGB ab.[51] Die genehmigende Behörde sollte deswegen stets klären, ob sie nur *datenschutzrechtlich* genehmigt (dazu Rz. 56: Schutz des Vertrauensprinzips; Sicherung erhöhter Sorgfalt) oder ob sie zusätzlich auch eine *verwaltungsrechtlich* und damit auch *strafrechtlich* wirkende Weisung «nach unten» in die Organisation hinein erteilt (was auch die

[49] Vgl. NIKLAUS OBERHOLZER, Basler Kommentar zum StGB, Art. 320 N 15.

[50] NIKLAUS OBERHOLZER, Basler Kommentar zum StGB, Art. 320 N 14 ff.

[51] *Erstens* ist zu beachten, ob die jeweiligen Gegenstände der Genehmigung wirklich identisch sind. Während im ersten Fall (§ 25 Abs. 3 IDV) die Bearbeitung von Personendaten im Auftrag genehmigt wird, wird im zweiten Fall in den Klartextzugriff (Offenbarung) auf geheimnisgebundene Informationen eingewilligt. *Zweitens* ist Folgendes relevant: Der Begriff «Bearbeiten von Personendaten» meint nicht dasselbe wie der Begriff «Klartextzugriff». Man sollte sorgfältig darauf achten, diese beiden Begriffe zu unterscheiden. Mit einer Datenbearbeitung geht nicht notwendigerweise auch ein Klartextzugriff einher bzw. werden nicht alle Daten und ihr Bedeutungsgehalt auch von einem Menschen zur Kenntnis genommen.

Wirkung einer Entbindung im Sinne von Art. 320 Ziff. 2 StGB, siehe Rz. 59, nach sich zieht).[52] Dies ist sinnvoll, wenn die handelnden Personen im Vorfeld des Cloud-Sourcing-, Outsourcing- bzw. sonstigen Sourcingprojekts nicht mit absoluter Gewissheit ausschliessen können, dass es im Projekt nicht doch im Einzelfall zu rechtlich relevanten Offenbarungen kommen könnte.

e. Wie dies für die Cloud-Projekte in der Stadt Zürich nutzbar gemacht werden kann

62 Die Beispiele in den Rz. 47 – Rz. 56 zeigen auf, dass die stadtzürcherischen Normen Abläufe kennen, wie sie auch bei der vom ISB angeregten proaktiven Entbindung vom Amtsgeheimnis (Rz. 45) vorgesehen sind. Verwaltungsrechtlich gesprochen, und mit Blick auf die Konvergenz der Schutzziele von Verwaltungsrecht, Datenschutzrecht und Strafrecht (Rz. 28), ist dies relevant: Das angedachte Vorgehen, eine stadträtliche Weisung an alle Organisationseinheiten in Bezug auf die Cloud-Nutzung zu erlassen, fügt sich harmonisch in das Gesetzesrecht der Stadt Zürich ein.

63 Die von der OIZ angestrebte stadträtliche Weisung (Rz. 3) wird von den Gutachtern unterstützt. Zu präzisieren ist, dass sie nur einen Rahmen geben kann; sie allein kann ohne weitere Draufsicht einer anderen Stelle keine strafbefreiende Wirkung haben (sie kann aber in Kombination mit anderen Bestätigungen diese Wirkung haben). Der konkrete Entscheid über die Nutzung eines bestimmten Service-Angebots der OIZ wird weiterhin bei der jeweils betreffenden Organisationseinheit verbleiben (konkreter Positionsbezug im Einzelfall). Die Weisung kann aber die Ausgangslage dahingehend klären, dass der Stadtrat allen Organisationseinheiten[53] der Stadt Zürich verbindlich Folgendes vorgibt:

1. **Nutzungspflicht**: Service-Angebote, welche die OIZ den Organisationseinheiten bereitstellt, sind von allen Organisationseinheiten auch dann zu nutzen, wenn die OIZ diese unter Einbindung von Cloud-Angeboten bereitstellt und für diese Cloud-Angebote bestätigt, dass diese das Schutzniveau Basisschutz+ gemäss Ziffer 2 nachstehend aufweisen. Die Organisationseinheit hat jedoch keine Nutzungspflicht, wenn sie bei sich Daten verwaltet, die von der OIZ mit dem Schutzansatz Basisschutz+ nicht antizipiert worden sind.

2. **Prüfpflicht**: Die OIZ wird angewiesen und ist verantwortlich, im SSA (standardisierten Angebot) für eingebundene Cloud-Angebote sicherzustellen, dass diese den «Basisschutz+» gemäss Ziffer 3 erfüllen.

3. **Basisschutz+**: «Basisschutz+» umfasst Folgendes:

3.1. den Basisschutz gemäss Beschluss des Stadtrats STRB 634 vom 9. Juli 2014[54]

3.2. Massnahmen, die im Normalbetrieb sicherstellen, dass vertrauliche Informationen und besondere Personendaten gemäss § 3 Abs. 4 IDG im Sinne des Handbuchs Informationssicherheit HISi ausreichend geschützt sind. Die nach dem HISi zu treffenden zusätzlichen Prüfschritte[55] sind von der OIZ vor der in Ziffer 2 vorausgesetzten Bestätigung umzusetzen und langfristig sicherzustellen.

4. **Konkreter Entscheid**: Organisationseinheiten müssen ergänzend plausibilisieren, ob mit Blick auf ihre Datenlage eine Sondersituation (Sonderfall) vorliegt, für die über den Basisschutz+ hinausgehend ergänzende Massnahmen erforderlich sind.[56] Die Organisationseinheit überprüft in

[52] Ein solches Vorgehen würde befreien von der Diskussion, ob die Genehmigung im Sinne von § 25 Abs. 3 IDV notwendigerweise und stets auch eine Entbindung im Sinne von Art. 320 Ziff. 2 StGB nach sich zieht. Diese Diskussion ist gerade mit Blick auf die hier postulierte Konvergenz zwischen Verwaltungs-, Straf- und Datenschutzrecht im Behördenumfeld naheliegend.

[53] Erinnert wird an die Begriffsdefinition in Anhang 1, wonach der Begriff «Organisationseinheit» für die Zwecke dieses Rechtsgutachtens so zu verstehen ist, dass er die OIZ nicht mit umfasst. Die OIZ definiert Massnahmen und setzt sie um. Die Organisationseinheit nutzt das SSA.

[54] Beschluss des Stadtrats der Stadt Zürich vom 9. Juli 2014, Nr. 634 (FN 3).

[55] Namentlich Ziff. 3.3 HISi: *«Für Informationen mit erhöhtem Schutzbedarf muss anhand einer Risikoanalyse im Rahmen eines Informationssicherheits- und Datenschutzkonzepts (ISDS-Konzept) (Kap. 7.1.2) festgestellt werden, ob die im Basisschutz definierten Sicherheitsmassnahmen ausreichend sind. Wenn nicht, sind die zusätzlichen Anforderungen durch geeignete Massnahmen abzudecken.»*

[56] Zum Begriff der Sondersituation siehe die Ausführungen in Rz. 66 und Rz. 67.

keinem Fall den technischen Setup, den die OIZ bereitstellt, sondern plausibilisiert einzig ihren eigenen Datenbestand: «Haben wir Daten, die von der OIZ nicht antizipiert werden konnten?» Die Organisationseinheit protokolliert ihren Entscheid schriftlich.

4.1. Sondersituation nein: Wenn keine Sondersituation vorliegt, sind keine ergänzenden Massnahmen zu treffen. Es tritt dann bereits ohne Weiteres Genehmigungswirkung im Sinne von Ziffer 5 ein.

4.2. Sondersituation ja: Wenn wirklich eine Sondersituation vorliegt, sind ergänzende Massnahmen umzusetzen (Verantwortung der Organisationseinheit, nach Abstimmung auch mit Unterstützung durch die OIZ). Eine Sondersituation wird erwartungsgemäss sehr selten zu bejahen sein.

5. **Genehmigungswirkung**: Soweit keine Sondersituation gemäss Ziffer 4.2 vorliegt (sondern ein Fall von Ziffer 4.1), sind Nutzungen gestützt auf den konkreten Positionsbezug im Einzelfall (Ziffer 4, Einleitung) hiermit im Sinne von Art. 320 Ziff. 2 StGB genehmigt. Soweit keine Sondersituation gemäss Ziffer 4.2 vorliegt, gilt diese Genehmigungswirkung auch für besondere Personendaten. Die Genehmigung im Sinne von § 25 Abs. 3 IDV gilt hiermit als erteilt.

6. **Ausnahmeprüfung**: Im Einzelfall können Projekte mit bestehenden technischen, organisatorischen oder rechtlichen Unzulänglichkeiten genehmigt werden. Die Zuständigkeit hierzu ergibt sich primär aus STRB 634 vom 9. Juli 2014, Ziff. 6 und Ziff. 7. Unzulänglichkeiten in der Vertragsdokumentation genehmigen im Anwendungsbereich der REFE die Vorsteherin bzw. der Vorsteher des Finanzdepartements (Art. 13 Abs. 4 lit. b REFE).

Ein solcher Beschluss des Stadtrats hat den Charakter einer städtischen Weisung an die gesamte Stadtverwaltung und im Resultat eine genehmigende Wirkung im Sinne von Art. 320 Ziff. 2 StGB, in Analogie zu den Vorgaben auf Ebene der Bundesverwaltung (siehe Rz. 45).

64 Mit anderen Worten würde Folgendes gelten, wenn die Empfehlung in Rz. 63 umgesetzt wird:

- Ist die faktische Ausgangslage ausreichend und ist in ihr der Basisschutz+ sichergestellt, genügt der nutzungswilligen Organisationseinheit die Bestätigung der OIZ, dass der Basisschutz+ eingehalten ist.
- Eine zusätzliche Genehmigung gestützt auf die REFE oder im Sinne von Ziff. 7 des Stadtratsbeschlusses vom 9. Juli 2014 ist nicht erforderlich.
- Die nutzende Organisationseinheit muss dann nur noch (aber immerhin) plausibilisieren[57], ob sie in ihren Daten oder Abläufen Anhaltspunkte dafür sieht, dass sie mit Basisschutz+ nicht auskommt. Normalerweise (ausgenommen besondere Umstände, dazu Rz. 66 f.) wird dies nicht der Fall sein.
- Basisschutz+ (auf Ebene der Faktenlage, vorn Rz. 10) ist von der OIZ so aufzusetzen, dass er für das Gros der Stadt Zürich voraussichtlich gut genug sein wird (also auch wenn eine Organisationseinheit das Cloud-Angebot für vertrauliche Informationen und/oder besondere Personendaten nutzen will).
- Auf dieser Basis darf die Organisationseinheit das Service-Angebot der OIZ (auch mit Cloud) dann ohne weitere Genehmigung der vorgesetzten Stelle nutzen.[58]

65 Der Stadtratsbeschluss wirkt bei dieser Ausgestaltung gleichsam a*ls institutionelle Sicherung* des ordnungsgemässen Geschäftsgangs der Stadt Zürich. Er dient auch der Effizienz: Hinterfragen kann man immer und es ist auch richtig, regelmässige Reviews anzulegen. Wenn die Organisationseinheit und ihre Mitarbeitenden sich aber täglich vor einer strafrechtlich relevanten Untersuchung fürchten müssten, würde die Verwaltung gelähmt. Der von der OIZ angedachte Stadtratsbeschluss (Rz. 3) schützt damit nicht zuletzt auch vor potentiell querulatorisch wirkenden Anfechtungen eines Cloud-Vorhabens. Er stellt

[57] Gefordert ist eine konkrete Auseinandersetzung mit (i) dem *Stadtratsbeschluss*, (ii) mit der *Bestätigung der OIZ* und (iii) der *eigenen Datenlage*.

[58] Die Begründung dafür ergibt sich aus dem Folgenden: (1) Nutzt die Organisationseinheit eine reife Cloud-Lösung, bei der es im Normalbetrieb zu keinen Offenbarungen kommt oder ist die Cloud-Anbieterin als Hilfsperson eingebunden, ist das Amtsgeheimnis nicht verletzt; (2) Das Datenschutzrecht lässt sich einhalten, wenn der notwendige Basisschutz erfüllt ist, was die OIZ vorab prüft.

– bildlich gesprochen – gleichsam eine um das Cloud-Konzept der Stadtverwaltung gelegte Schutzhülle dar. Die Schutzhülle schützt den *Normalfall*.

66 Die Leiterin der Organisationseinheit mit einem *Sonderfall* (Sondersituation) muss Zusätzliches prüfen. Der Stadtratsbeschluss (wie in Rz. 3 antizipiert und in Rz. 63 präzisiert) ist kein Freipass dafür, allenfalls notwendige Ergänzungen schlicht nicht mehr anzudenken. Bestehen besondere Umstände, sind diese aufzugreifen und zu würdigen. In Übereinstimmung mit der Informationsklassifizierung der Stadt Zürich würden besondere Umstände (und damit ein Sonderfall bzw. eine Sondersituation) vorliegen, wenn:

1. Eine für das von der Organisationseinheit betreute Fachgebiet massgebliche rechtliche Bestimmung die Massnahmen des Basisschutz+ als ungenügend bezeichnet (oder sich dieser Schluss sonst wie aus den für das Fachgebiet anwendbaren Regeln ergibt).
2. Sich dieser Schluss aus einer Risikoanalyse ergibt oder ergeben würde, mit Blick auf die aussergewöhnliche Bedeutung der von der Cloud-Nutzung betroffenen Informationen (namentlich, wenn sich ergibt, dass die OIZ im Rahmen ihrer allgemeinen Prüfung diese aussergewöhnliche Bedeutung der betreffenden Informationen nicht antizipiert hat).
3. Sich dieser Schluss aus vertraglichen Bestimmungen ergibt, denen sich die Organisationseinheit unterworfen hat.

67 Erreicht die Faktenlage den Basisschutz+ nicht, hat der ins Auge gefasste Stadtratsbeschluss nicht die Wirkung gemäss Art. 320 Ziff. 2 StGB (ergänzend hierzu Rz. 70 und Rz. 74: Use Cases #2 und #3).

68 Die Nutzung von Cloud-Angeboten wird sich bei Umsetzung des geplanten Stadtratsbeschlusses somit auf eine Basis stellen, die sich aus verschiedenen Bausteinen zusammensetzt:

1. *Stadtratsbeschluss* (Rz. 3 und Rz. 63), unter Verweis auf das vorliegende Rechtsgutachten.
2. *Bestätigung der OIZ*, dass Basisschutz+ gegeben ist (Rz. 63 Ziff. 2).
3. *Entscheid der Organisationseinheit*, welche das Service-Angebot der OIZ (mit Cloud) nutzen will, nach Erörterung bzw. Plausibilisierung der Frage, ob ein Sonderfall vorliegt, der nach besonderen bzw. zusätzlichen Massnahmen ruft (Rz. 63 Ziff. 4.2) oder nicht (Rz. 63 Ziff. 4.1).

69 In vielen Fällen[59] wird sich die Rechtmässigkeit einer Cloud-Nutzung somit aus einem Zusammenwirken mehrerer Stellen ergeben:

- Die *OIZ* stellt in Bezug auf die Faktenlage eine zentrale Grundlage für den Entscheid zur Verfügung.
- Der *Stadtrat* schützt den Normalfall vor Angriffen «im Kleinen».
- Die *Organisationseinheit* hat das letzte Wort.

70 Ergänzend zu Punkt 2 in Rz. 68 ist Folgendes anzumerken:

- Die OIZ prüft das Vorliegen von genügendem Basisschutz+ generell nur für Services, welche eine Organisationseinheit der Stadt Zürich über die OIZ bezieht (Ausnahmen sind im Einklang mit dem Stadtratsbeschluss vom 9. Juli 2014 betreffend das Handbuch Informationssicherheit möglich).
- Soweit zwar Basisschutz, aber nicht Basisschutz+ erreicht wird, kommt der angedachte neue Stadtratsbeschluss nicht zum Tragen; es gilt dann allein der Stadtratsbeschlusses Nr. 634 vom 9. Juli 2014 (FN 3). Für eine Entbindung bräuchte es eine zusätzliche Einzelfallprüfung.
- Soweit die OIZ im Sinne von Ziff. 7 des Stadtratsbeschlusses Nr. 634 vom 9. Juli 2014 (FN 3) in ihrem Service-Angebot Ausnahmen sogar zum Basisschutz identifiziert, macht sie dies gegenüber der nutzungswilligen Organisationseinheit bekannt und koordiniert die Abstimmung mit der IT-Delegation der Stadt Zürich sowie gegebenenfalls mit der Fachstelle Informationssicherheit. Da der Basisschutz nicht

[59] Zum Standardfall siehe Rz. 74, Use Case #1. Zu den Ausnahmen siehe Rz. 74, Use Cases #2 - #4.

eingehalten ist, kann auch der Basisschutz+ nicht bestätigt werden. Für eine Entbindung bräuchte es eine zusätzliche Einzelfallprüfung.

71 Die OIZ kann zur Umsetzung von Basisschutz+ auf Strategien mit einem Schwerpunkt auf technisch-organisatorische Massnahmen oder auf solche mit rechtlich-konzeptionellem Schwerpunkt setzen.

72 Technisch-organisatorische Strategien fokussieren darauf, dass aus technischen Gründen oder aufgrund von organisatorischen Massnahmen Klartextzugriffe nach dem gewöhnlichen Lauf der Dinge, der Erfahrung einer technisch geschulten Fachperson und mit Blick auf den Stand der Technik ausgeschlossen werden können.[60] Verschlüsselungstechniken *können* eingesetzt werden und sind oft sinnvoll. **Technisch-organisatorische Strategien können das notwendige Schutzziel auch ohne durchgehende Verschlüsselung erreichen**. Anhang 2 zeigt auf, dass sich aus einer hochskalierenden IT-Architektur oft ein sehr weit gehender Schutz ergibt. Im Umsetzungsprojekt lässt sich erfahrungsgemäss für etablierte Cloud-Anbieter bestätigen, dass bereits die von der Cloud-Anbieterin bereitgestellten IT-Infrastrukturen die Anforderungen des Basisschutz+ erreichen werden.

73 Rechtlich-konzeptionelle Strategien fokussieren darauf, dass die Stadt Zürich (bzw. die OIZ) die Cloud-Anbieterin als Hilfsperson aufstellen wird. Dies erlaubt Klartextzugriffe durch Mitarbeitende der Cloud-Anbieterin, ohne dass es zu einer Strafbarkeit der Stadt Zürich kommt.

74 Auf Basis des Vorstehenden lassen sich somit die folgenden Use Cases für die Cloud-Nutzung in der Stadt Zürich abbilden:

1. **Service-Angebot von OIZ; OIZ bestätigt Basisschutz+** (siehe Rz. 68 Punkt 2)

   Rolle der Organisationseinheit: Plausibiliert, dass kein Sonderfall vorliegt.
   Wirkung des Stadtratsbeschluss: Gilt als Genehmigung i.S.v. Art. 320 Ziff. 2 StGB.
   Rechtmässigkeit der Cloud-Nutzung: Ja (direkt gestützt auf Rechtsgutachten).
   Weitere Genehmigung einholen: Nein.
   OIZ stellt das Service-Angebot als Standard bereit: Ja.

2. **Service-Angebot von OIZ; OIZ bestätigt nur Basisschutz** (Rz. 70, zweites Lemma)

   Rolle der Organisationseinheit: Prüft den eigenen Datenbestand, eruiert den Schutzbedarf und sorgt für weitere Massnahmen, soweit nötig[61] (Koordination mit der IT-Delegation gem. HISi bzw., soweit anwendbar, mit weiteren Stellen gemäss Rz. 47 – Rz. 56).
   Wirkung des Stadtratsbeschluss: Gilt nicht als Genehmigung i.S.v. Art. 320 Ziff. 2 StGB.
   Rechtmässigkeit der Cloud-Nutzung: Ja (gestützt auf Rechtsgutachten), wenn Faktenlage OK.
   Weitere Genehmigung einholen: Nicht erforderlich für Rechtmässigkeit. Eine Organisationseinheit würde eine Genehmigung mit Wirkung nach Art. 320 Ziff. 2 StGB allenfalls in Betracht ziehen, wenn sich eine «institutionelle Sicherung» des Geschäftsgangs (dazu Rz. 65) aufdrängt.[62]
   OIZ stellt das Service-Angebot als Standard bereit: Nein (oder gem. sep. Entscheid OIZ).

3. **Service-Angebot von OIZ; OIZ bestätigt auch Basisschutz nicht** (Rz. 70, drittes Lemma; dies dürfte ein kaum je auftretender Ausnahmefall sein)

   Rolle der Organisationseinheit: Sorgt für Einhaltung der Voraussetzungen gem. HISi[63].
   Wirkung des Stadtratsbeschluss: Gilt nicht als Genehmigung i.S.v. Art. 320 Ziff. 2 StGB.

[60] Mit den Präzisierungen, wie sie in Rz. 95 dargestellt werden.

[61] Siehe Auszug aus dem Stadtratsbeschluss Nr. 634 vom 9. Juli 2014 (FN 3): *«Jede Organisationseinheit ist für die Umsetzung in ihrem Verantwortungsbereich verantwortlich»*.

[62] Das Einholen einer Entbindung vom Amtsgeheimnis ist angezeigt, wenn die Wahrnehmung des Projekts nach aussen heikel sein könnte. Beispiel: Es sind Klartextzugriffe der Cloud-Anbieterin auf vertrauliche oder streng vertrauliche Information wahrscheinlich, die sich zwar mittels vertraglicher Einbindung der Cloud-Anbieterin rechtmässig ausgestalten lassen, deren Wahrnehmung aber gleichwohl heikel bleiben kann.

[63] Siehe Auszug aus dem Stadtratsbeschluss Nr. 634 vom 9. Juli 2014 (FN 3): *«Jede Organisationseinheit ist für die Umsetzung in ihrem Verantwortungsbereich verantwortlich»*.

Rechtmässigkeit der Cloud-Nutzung: Ja (gestützt auf Rechtsgutachten, wenn Faktenlage OK, und sofern erforderliche gesetzliche Genehmigungen, z.B. nach HISi, evtl. weitere[64], vorliegen).
Weitere Genehmigung einholen: Nicht erforderlich für Rechtmässigkeit. Ansonsten grundsätzlich wie Use Case #2, die Wirkung allenfalls bereits eingeholter Genehmigungen ist im Einzelfall zu würdigen.
OIZ stellt das Service-Angebot als Standard bereit: Nein.

4. Anderes Cloud-Angebot (Organisationseinheit bezieht nicht über OIZ)

Rolle der Organisationseinheit: Wie Use Case #3.
Wirkung des Stadtratsbeschluss: Gilt nicht als Genehmigung i.S.v. Art. 320 Ziff. 2 StGB
Rechtmässigkeit der Cloud-Nutzung: Ja (gestützt auf Rechtsgutachten), wenn Faktenlage OK.
Weitere Genehmigung einholen: Wie Use Case #3.
OIZ stellt das Service-Angebot als Standard bereit: n.a. (kein Service-Angebot von OIZ).

75 Die Use Cases in Rz. 74 zeigen, dass die Stadt Zürich ihre Cloud-Projekte auch in Situationen mit verbleibendem Ermessensspielraum zum Abschluss bringen kann, d.h. also auch dann, wenn keine abschliessenden Antworten möglich sein sollten. Der Staat muss seine Cloud-Projekte im Normalfall *nicht mit einer Vollkasko-Mentalität* umsetzen (dazu vorn, Rz. 34). Eine sachlich nicht begründete Zurückhaltung kann auch zu einer ungerechtfertigten Verteuerung von Projekten führen oder Projekte ganz verunmöglichen – beides liesse sich verwaltungsrechtlich nicht rechtfertigen.[65]

5. Die datenschutzrechtliche Regelung deckt sich mit dem Verwaltungsrecht

76 Das anwendbare Datenschutzrecht (Gesetz über die Information und den Datenschutz [IDG], die Verordnung über die Information und den Datenschutz [IDV] und, soweit ergänzend, das städtische Datenschutzrecht) sekundiert das Geheimnisrecht bzw. geht mit diesem, wie bereits geschildert, gleichsam Hand in Hand.

77 Für die hier zur Diskussion stehende Cloud-Nutzung lautet die Analyse wie folgt: Die Cloud-Nutzung ist datenschutzrechtlich nicht verboten, wenn sie nicht aufgrund der sonstigen Regeln des Geheimnisschutzrechts verboten ist. Im Gegenteil: Der Beizug von Dritten zum Zweck des Betriebs von IT-Infrastrukturen wird beispielsweise in § 6 Abs. 1 IDG, wonach das öffentliche Organ das Bearbeiten von Informationen Dritten übertragen kann, ausdrücklich ermöglicht. Die Auftragsbearbeitung wird sodann in § 25 IDV weiter konkretisiert,[66] was man nicht getan hätte, wenn sie per se als ein (*de lege lata*) datenschutzrechtlich problematischer Vorgang angesehen worden wäre. So regelt § 25 Abs. 2 IDV den Mindestinhalt eines Vertrags über die Auftragsbearbeitung für Fälle, in denen die Auftragsbearbeitung nicht gesetzlich geregelt ist. Folglich ist die vertragliche Überbindung an einen externen Dienstleister ausdrücklich zulässig.[67]

78 Erfolgt die Auslagerung in Einklang mit der Rechtsordnung, stehen also beispielsweise keine rechtlichen Bestimmungen oder vertraglichen Vereinbarungen der Auslagerung entgegen (§ 6 Abs. 1 IDG), ist die Auslagerung *nicht* als eine Bekanntgabe an Dritte zu qualifizieren. Folglich sind die Bestimmungen über die Bekanntgabe an Dritte nicht einschlägig (z.B. § 14 ff. IDG). Das öffentliche Organ kann neben der Auslagerung aber auch Daten an Dritte bekanntgeben oder von Amtes wegen *über* die Auslagerung

[64] Im Einklang mit dem Stadtratsbeschluss Nr. 634 vom 9. Juli 2014 (IT-Delegation) oder im Sinne der Ausführungen gemäss Rz. 47 – Rz. 56.

[65] WIEDERKEHR/RICHLI (FN 24), Rz. 328 ff.

[66] Der Vollständigkeit halber ist anzumerken, dass das kantonale Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1999 (LS 172.71, GAVI) für Auslagerungen, welche die Stadt Zürich vornimmt, nicht zur Anwendung kommt. Es gilt nur für Organe bzw. Organisationseinheiten des Kantons, nicht aber für solche der Stadt Zürich.

[67] Zu den Anforderungen an einen inhaltlich vollständigen Vertrag über die Auftragsbearbeitung nach Datenschutzrecht des Bundes und der Kantone, vgl. THOMAS STEINER, Digitalisierter Arztbesuch und Cloud-Nutzung im Lichte des Datenschutzrechts des Bundes und der Kantone, in: sic! 12/2020, 677 ff., S. 685–687.

informieren, wenn daran ein allgemeines Interesse besteht (§ 14 IDG). Darüber hinaus setzt der Beizug eines Dritten zur Auftragsdatenbearbeitung keinen Rechtfertigungsgrund voraus.

79 Das kantonale Recht enthält eine Vielzahl von Regeln, die im Kontext von Cloud-Projekten erörtert werden könnten. Vollkommen im Einklang mit dem System des Geheimnisrechts steht, dass die Organisationseinheit auch datenschutzrechtlich vorab nur für Massnahmen zum Schutz der Vertraulichkeit sorgen muss (Rz. 80), und dort, wo dies nicht uneingeschränkt möglich sein sollte, um Genehmigung («proaktive Entbindung» vom Amtsgeheimnis, Rz. 81) ersuchen muss. Das wird im Cloud-Merkblatt des kantonalzürcherischen Datenschutzbeauftragten wohl anders gesehen, worauf in Anhang 3 zu diesem Gutachten einzugehen ist (siehe aber bereits Rz. 82).

80 Erstens: Umsetzungsmassnahmen zum Schutz gegen Offenbarung bei Cloud-Nutzungen ohne qualifizierende Elemente: Der Verfasser geht davon aus, dass die Bestimmungen der REFE zu verallgemeinern sind, bei Cloud-Auslagerungen sollten somit die **(1) IT-Sicherheitsbestimmungen** der Stadt Zürich stets eingehalten sein. Die Organisationseinheit muss somit die verbindlichen technischen Sicherheitsbestimmungen des städtischen Finanzdepartements zur IT-Sicherheit beachten (Art. 10 REFE). – Die folgenden im Cloud-Merkblatt (S. 3) des kantonalen Datenschutzbeauftragten genannten zusätzlichen Aspekte scheinen sodann mit der Verhältnismässigkeit vereinbar und sollten demnach zusätzlich umgesetzt werden: **(2) Orientierungspflicht**: Der Cloud-Anbieter muss das öffentliche Organ regelmässig über die Erfüllung der wichtigsten Massnahmen im IT-Sicherheitsbereich sowie sicherheitsrelevante Vorfälle orientieren. **(3) Informationssicherheitskonzept**: Der Cloud-Anbieter muss in einem Informationssicherheitskonzept die organisatorischen und technischen Sicherheitsmassnahmen (z.B. kryptografische Verfahren, Identity- und Accessmanagement, Notfallmanagement) festhalten. **(4) Massnahmen zur Sicherung der Mandantentrennung**: Massnahmen zur Sicherung der Mandantentrennung erscheinen heute State of the Art zu sein. Zutreffend ist aber das Gegenteil: Eine Cloud-Lösung, die Mandantentrennung nicht realisiert, kann von einer öffentlichen Stelle wohl nicht eingesetzt werden.[68] Diese Ergänzungen sind gemäss Auffassung des kantonalen Datenschutzbeauftragten dem Cloud-Anbieter vertraglich aufzuerlegen, was als nachvollziehbar erscheint und im Übrigen auch notwendig ist; denn kantonales Recht wirkt nicht ohne Weiteres verbindlich für Cloud-Anbieter.[69]

81 Zweitens: Genehmigungspflichten bestehen bei technischer (Rz. 48), rechtlicher (Rz. 51) oder vertraglicher (Rz. 53) Unvollkommenheit des Cloud-Projekts.

82 Im Anhang 3 («Zum Cloud-Merkblatt der Kantonalen Datenschutzbeauftragten») sind jene Vorgaben im Cloud-Merkblatt des Kantonalen Datenschutzbeauftragten genannt, die über das legiferierte Datenschutzrecht im Kanton Zürich hinausgehen und insofern «überschiessend» sind.

6. Zwischenfazit zum Geheimnisrecht in der Stadt Zürich

83 Die vorstehenden Ausführungen zeigen, dass die Verschwiegenheitspflicht von Organisationseinheiten der Stadt Zürich als ein Gesamtsystem von Bestimmungen unterschiedlicher Art zu erfassen ist, wobei die verwaltungsrechtlichen, datenschutzrechtlichen und weiteren Bestimmungen (namentlich die «Verstärkungen» durch Straf- und Prozessrecht, worauf hinten noch vertieft eingegangen wird) über die Entbindungsmechanismen als Ausfluss des hierarchisch aufgebauten Verwaltungshandelns miteinander eng verwoben sind: Die in Rz. 27 erfassten Schutzziele des Geheimnisrechts werden durch alle Rechtsquellen gesamthaft geschützt (dies ist gemeint, wenn vorn, in Rz. 28, von «Konvergenz» gesprochen wird).

[68] Dies ist dahingehend zu präzisieren, dass diese Aussage einschränkend dann nicht gilt, wenn die Mandantentrennung keinen Mehrwert für die Vertraulichkeit oder dergleichen bietet (Beispiel: Es gibt Anbieterinnen, die Datenhaltungslösungen mit Ende-zu-Ende-Verschlüsselung anbieten; das im Rahmen der Ende-zu-Ende-Verschlüsselung erfolgende Tagging von Dateien läuft auf eine Massnahme hinaus, die eine ähnliche Wirkung wie eine Mandantentrennung aufweist – ohne aber eine eigentliche Mandantentrennung darzustellen. Solche Lösungen dürften wohl von einer Behörde ebenfalls eingesetzt werden, wenn alle weiteren Voraussetzungen erfüllt sind.

[69] Zusätzlich sind auch noch Bestimmungen betreffend Datenportabilität aufzunehmen. Diese hängen jedoch nicht mit dem Untersuchungsgegenstand für dieses Rechtsgutachten zusammen, weswegen darauf nicht besonders einzugehen ist.

C. Verstärkung des Informationsschutzes durch Straf- und Prozessrecht

1. Strafbare Handlungen gegen die Amtspflicht (Art. 320 StGB und Art. 293 StGB)

a. Art. 320 StGB

84 Art. 320 StGB stellt die Offenbarung des Amtsgeheimnisses unter Strafe. Das vorliegende Rechtsgutachten beschränkt sich wie erwähnt auf die Betrachtung des zentralen Begriffs der «Offenbarung». Da die weiteren Tatbestandsmerkmale – insb. wer Beamter ist und was ein Geheimnis ist – bereits in der Standardliteratur ausreichend beschrieben worden sind, wird an dieser Stelle darauf verwiesen.[70]

(i) Zur Offenbarung

85 Es existiert in der Schweiz soweit ersichtlich keine publizierte Rechtsprechung, die den Begriff der Offenbarung im Zusammenhang mit Cloud Computing im Allgemeinen bzw. mit Cloud-Angeboten im Speziellen klarstellen oder auch nur behandeln würde. Es ist demnach zu untersuchen, ob das Übertragen von Daten in die IT-Infrastrukturen eines Cloud-Anbieters eine Offenbarungshandlung im Sinne von Art. 320 StGB darstellt.

86 In einem das Amtsgeheimnis betreffenden Entscheid hat das Bundesgericht das strafbare Verhalten einer «Offenbarung» umschrieben. Demnach offenbart ein Geheimnis diejenige, die das Geheimnis «einer **dazu nicht ermächtigten Drittperson zur Kenntnis bringt** oder dieser die **Kenntnisnahme zumindest ermöglicht**.»[71] In einem die Verletzung des Fabrikations- und Geschäftsgeheimnisses (Art. 162 StGB) betreffenden Fall hat das Bundesgericht präzisiert, dass die Kenntnisnahme durch die unbefugte Dritte (im vorliegenden Rechtsgutachten als «**Klartextzugriff**» bezeichnet) zur Vollendung der Tat erforderlich sei. Die Erfahrung zeigt, dass technisch-organisatorische Strategien zum Schutz vor Klartextzugriffen bei Einsatz von reifen Cloud-Angeboten möglich sind (zu diesen Rz. 72). Bei solchen kommt es im Normalbetrieb zu keinen Klartextzugriffen. Also liegt keine Offenbarung vor. Dann fehlt es an einem Element im objektiven Straftatbestand. Strafbarkeit nach Art. 320 Ziff. 1 StGB ist damit ausgeschlossen.

Personensicht v. Maschinensicht (Exkurs): Im Sinne eines Exkurses sei die folgende Differenzierung angemerkt: Wenn im vorliegenden Rechtsgutachten von «Klartextzugriff» gesprochen wird, ist die sog. «Personensicht»[72] gemeint, in Abgrenzung zur sog. «Maschinensicht», die im Lichte der Offenbarungstatbestände (Art. 320 StGB, Art. 273 StGB, Art. 293 StGB, etc.) nicht relevant ist. Zum heutigen Zeitpunkt ist diese Differenzierung ausreichend. Mit fortschreitender Digitalisierung ist durchaus möglich, dass sich aus blosser Maschinensicht eine Erkenntnis bei einer Person über die schützende Information ergibt, die auf eine Offenbarung hinausläuft. Man müsste dann den Begriff des Klartextzugriffs differenzierend betrachten und stattdessen auf Bearbeitungen auf dem sog. «Content Layer» abstellen. Anlass dazu könnten neue Technologien geben, die zwar nicht die in der Cloud-Infrastruktur gespeicherte Information «lesen», sondern nur deren Hash-Werte und diese Hash-Werte mit einer Referenzdatenbank abgleichen – woraus sich dann Erkenntnisse über den Inhalt der gespeicherten Information ergeben würden. Selbstverständlich sind mit den Begriffen «Offenbarung» bzw. «Klartextzugriff» bzw. «Personensicht» im hier verwendeten Sinn auch solche Zugriffe auf die Inhaltsebene der gespeicherten Informationen gemeint – denn daraus resultiert tatsächlich eine Offenbarung bzw. ein Resultat, das einer Offenbarung bei würdigender Betrachtung gleichkommt. – Die Differenzierung zwischen

[70] WOLFGANG WOHLERS, Kommentar zum Strafgesetzbuch, Bern 2020, StGB 320 N 1 ff.; MATTHIAS MICHLIG/EVA WYLER, Kommentar zum Strafgesetzbuch, Bern 2020, StGB 320 N 1 ff.

[71] BGE 142 IV 65 E. 5.1 (Hervorhebungen hinzugefügt).

[72] Zum Begriff siehe Anhang 1: Es geht um das, was ein Mensch erkennt. Demgegenüber ist die blosse Datenhaltung in einer Maschine, ohne dass ein Mensch die Daten einsieht, strafrechtlich im Lichte von Art. 320 Ziff. 1 StGB (oder ähnlicher Normen, die auf Offenbarung abstellen: Art. 273 StGB, 293 StGB) nicht relevant.

Personensicht und Maschinensicht ist auf datenschutzrechtlicher Ebene auf jeden Fall von Bedeutung. Solche Erkenntnisse in der Maschine (z.B. der Cloud-Anbieterin) sind datenschutzrechtlich sowie im Licht des Handbuchs Informationssicherheit (HISi) relevant und die OIZ muss im Rahmen der Beschaffung von Cloud-Angeboten prüfen, inwiefern sich diesbezüglich Risiken für die zu schützenden Informationen ergeben und inwiefern diesbezüglich Massnahmen zu treffen sind.

(ii) Versuch ist ausgeschlossen, da Adäquanz (Normalbetrieb) zu berücksichtigen ist

87 Das Gericht räumte in der zitierten Rechtsprechung ein, dass bereits wegen Versuchs bestraft werden könne, wer die Möglichkeit zur Kenntnisnahme schaffe.[73]

88 Der Umstand, dass die Cloud-Anbieterin das Gesamtsystem kontrolliert und theoretisch die technische Macht zum Datenzugriff hat (siehe bereits vorn, Rz. 16), könnte zum vorschnellen Schluss verleiten, der Cloud-Anbieterin sei eine strafbare «Möglichkeit der Kenntnisnahme» im Sinne dieser Rechtsprechung bereits dann eröffnet, wenn die Organisationseinheit der Stadt Zürich einen Datensatz auf die IT-Infrastrukturen der Cloud-Anbieterin lädt. Im öffentlichen Diskurs entsteht so der Eindruck, eine Cloud-Nutzung führe damit *immer* zur Strafbarkeit der Geheimnisträgerin wegen Versuchs (im Sinne des Bundesgerichts-Urteils 6B_1403/2017[74]). Dem ist nicht so:

- Die im Rechtsgutachten von LAUX/HOFMANN/SCHIEWECK/HESS zur Zulässigkeit der Verwendung von Cloud-Anwendungen nach Art. 47 BankG dargelegte Begründung zeigt auf, dass nur die aktive Offenbarung oder die schuldhaft und pflichtwidrig unterlassene Sicherung der von der Geheimhaltungspflicht erfassten Informationen gegen Klartextzugriffe sanktionswürdig ist.[75] Dies deckt sich namentlich mit den Regeln im stadtzürcherischen Recht zur Sicherung des Perimeters (Rz. 37) sowie mit der datenschutzrechtlichen Hauptflicht nach dem IDG, angemessene Sicherungsmassnahmen zu treffen (dazu Rz. 80; bzw. ersatzweise um eine proaktive Entbindung, d.h. Genehmigung bei der zuständigen übergeordneten Stelle zu ersuchen, Rz. 81).
- Die Organisationseinheit der Stadt Zürich setzt mit der Speicherung von geheimen Tatsachen auf IT-Infrastrukturen der Cloud-Anbieterin zwar durchaus den Grund, warum ein (verbotener) Klartextzugriff z.B. durch eine Mitarbeitende der Cloud-Anbieterin überhaupt erst möglich wird (wenn die Mitarbeitende die aufgesetzten Sicherheitsmassnahmen überwinden kann). Die Speicherung kann deshalb als kausal im Sinne des natürlichen Kausalzusammenhangs bezeichnet werden. *Mit der Speicherung als solcher findet aber rein tatsächlich noch kein Klartextzugriff statt.* Ein solcher wäre aber erforderlich, um ein Offenbaren im Sinne des Art. 320 StGB annehmen zu können (Rz. 86).
- Wenn die Speicherung von geheimen Tatsachen somit zwar als *Ursache im Sinne des natürlichen Kausalzusammenhangs* verstanden werden kann, aber noch kein Klartextzugriff stattfindet und nur die pflichtwidrig unterlassene Sicherung sanktionswürdig ist, dann ist das Kriterium der Adäquanz auch für die Geheimnispflicht der Beamtin massgeblich: Im genannten Rechtsgutachten von LAUX/HOFMANN/SCHIEWECK/HESS wurde nachgewiesen, dass die Geheimnisträgerin nicht eine zu 100% wirksame Sicherung einrichten muss, sondern nur eine solche, die *nach dem gewöhnlichen Lauf der Dinge und der allgemeinen Lebenserfahrung* normalerweise gegen unbefugte Klartextzugriffe schützt. Diese Sicht wurde für die Schweizerische Lehre anschliessend z.B. auch von ROSENTHAL aufgenommen.[76]

[73] Urteil des Bundesgerichts 6B_1403/2017 vom 8. August 2018, E. 1.2.2.

[74] Urteil des Bundesgerichts 6B_1403/2017 vom 8. August 2018, E. 1.2.2.

[75] LAUX/HOFMANN/SCHIEWECK/HESS, SBVg-Gutachten, Rz. 17 ff.; siehe zu einer Reflexion dazu in der Einleitung, Rz. 15.

[76] DAVID ROSENTHAL, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter 10. August 2020, S. 14, Rz. 39a: *«Es verbleibt immer ein Restrisiko eines Zugriffs unerwünschter Dritter (oder eines Missbrauchs der Daten durch befugterweise eingeweihte Personen). Das ist allgemein akzeptiert.»* Und Rz. 40, S. 15: *«[...] Realität, dass es für [Kunden] in aller Regel einzig darauf ankommt, dass der Berufsgeheimnisträger die Bearbeitung seiner Daten mit entsprechenden technischen und organisatorischen Massnahmen insgesamt so ausgestaltet, dass die Wahrscheinlichkeit, dass es zu einer unerwünschten Preisgabe oder Verwendung seiner Daten kommt, hinreichend gering ist. Ist also dem Risiko einer Verletzung der Datensicherheit angemessen vorgebeugt, wird es für den Kunden normalerweise keine Rolle mehr*

Im Ergebnis wird die Strafbarkeit nicht bereits durch die Datenspeicherung in der Cloud begründet (natürlicher Kausalzusammenhang), sondern erst wegen ungenügender Datensicherung, infolge derer ein unbefugter Klartextzugriff erfolgt (*adäquater* Kausalzusammenhang).

89 Zwar will die konstante Rechtsprechung des Bundesgerichts,[77] dass auch das Schaffen einer Möglichkeit des Zugriffs zur Strafbarkeit führt. Damit sollen Konstellationen des ungehinderten Klartextzugriffs erfasst werden (z.B. «Liegenlassen von Dokumenten im Altpapier»), die im Resultat auf eine aktive Mitteilung von geheimen Tatsachen hinauslaufen. In hochskalierenden Cloud-Umgebungen sind erfahrungsgemäss aber eine Vielzahl von Massnahmen eingerichtet, die bewirken, dass kein ungehinderter Klartextzugriff resultiert (Rz. 72). Solange die Organisationseinheit der Stadt Zürich **angemessene Massnahmen getroffen hat, um einen solchen Klartextzugriff zu verhindern**,[78] kann man somit auch im Sinne der bundesgerichtlichen Rechtsprechung nicht sagen, dass die Organisationseinheit der Stadt Zürich den eigentlichen Tatbeitrag dafür geleistet hat, dass es zum unerlaubten Klartextzugriff kommt.[79]

90 **Somit scheidet die Strafbarkeit von Mitarbeitenden einer Organisationseinheit der Stadt Zürich *wegen aktiver Tatbegehung* nach Art. 320 StGB aus, wenn sie ein von der OIZ für gut befundenes Cloud-Angebot nutzen**.

(iii) Prüfung aus der Perspektive des Unterlassungsdelikts

91 Zu prüfen bleibt einzig, ob die Organisationseinheit der Stadt Zürich im Sinne des adäquaten Kausalzusammenhangs für ungenügende Sicherungsmassnahmen einstehen muss. Es geht um die Frage, ob die von der Organisationseinheit der Stadt Zürich getroffenen vertraglichen, technischen und organisatorischen Sicherungsmassnahmen ausreichend sind. Sind sie es nicht, hat die Organisationseinheit der Stadt Zürich für den Klartextzugriff einzustehen. Bildlich gesprochen: Wer das Scheunentor geöffnet hält, muss für Klartextzugriffe durch jene, die in den eigentlich zu schützenden Bereich hineinspaziert, einstehen. Wer jedoch genügend sichert, ist nicht verantwortlich dafür, dass z.B. eine bösartige Dritte die Sicherungshürde übersteigt. Strafbar ist vielmehr diejenige, welche die Sicherungsmassnahmen mit krimineller Energie überwindet (Art. 143 StGB, Art. 143bis StGB und Art. 179^{novies} StGB).

92 **Es geht im Kontext der Cloud-Nutzung durch Behörden somit nur um die Tatbegehung von Art. 320 StGB durch Unterlassung**, d.h. durch pflichtwidriges Untätigbleiben.[80] Pflichtwidrig untätig bleibt, wer eine Gefährdung oder Verletzung eines strafrechtlich geschützten Rechtsgutes nicht verhindert, obwohl er aufgrund seiner Rechtstellung dazu verpflichtet ist, namentlich weil er die Gefahr geschaffen hat (Art. 11 Abs. 2 lit. d StGB).

93 Problematisch wäre, wenn Mitarbeitende der Cloud-Anbieterin auf Daten im Tenant der Organisationseinheit der Stadt Zürich ungehindert Klartextzugriff nehmen könnten.[81] Dann würde – ausser, wenn die Cloud-Anbieterin als Hilfsperson bestellt wird – im Zeitpunkt von solchen ungehinderten Klartextzugrif-

spielen, ob und welche Dritten beigezogen wurden.» Das ist die ausformulierte Version der folgenden Position bei LAUX/HOFMANN/SCHIEWECK/HESS, Rz. 13*: «Die Bank darf auch darauf vertrauen, dass der Bankkunde ihrer internen Organisation nicht widersprechen wird, solange die Bank angemessene Massnahmen zur Sicherung ihres Perimeters aufrechterhält. Insofern greift das Vertrauensprinzip. Solange die Bank angemessene Schutzmassnahmen ergreift, darf sie somit auch die implizite Einwilligung des Bankkunden voraussetzen.»*

[77] Vgl. oben Rz. 86.

[78] Gleichbedeutend: Nur IT-Infrastrukturen (eigene oder von Dritten, wie z.B. von Cloud-Anbieterinnen) einsetzt, welche die geforderte Sicherung aufweisen.

[79] Insofern unterscheidet sich die Cloud-Nutzung von den in der Rechtsprechung diskutierten Szenarien, wie z.B. im Urteil des Bundesgerichts 6B_1403/2017 vom 8. August 2018, wo es darum ging, dass der Täter geschützte Informationen ins Altpapier gelegt hat, wo sie für Dritte ungeschützt zugänglich waren.

[80] Art. 11 StGB.

[81] Ob Massnahmen geeignet sind, vor Klartextzugriffen zu schützen, beurteilt sich danach, ob alle der getroffenen Massnahmen in ihrer Kombination zu einem angemessenen Schutz führen. Es muss sich nicht durchwegs allein um technische Massnahmen handeln. Insbesondere lässt sich ein angemessener Schutz auch ohne Verschlüsselungsmassnahmen erzielen.

fen auch eine der Organisationseinheit der Stadt Zürich anzulastende Offenbarung (durch unterlassene Sicherung) stattfinden. **Um solche Szenarien zu vermeiden**, muss die Stadt Zürich sich für die technische Lösung der Cloud-Anbieterin interessieren und **im Rahmen eines Umsetzungsprojekts beurteilen, ob gemäss den der Organisationseinheit der Stadt Zürich vorliegenden Informationen auf Seiten der Cloud-Anbieterin ein genügender Schutz durch technische und organisatorische Massnahmen gegen Klartextzugriffe eingerichtet ist und ob diese durch vertragliche Massnahmen genügend abgesichert sind**. In der Stadt Zürich gilt Folgendes: OIZ ist für die Prüfung der technischen und organisatorischen Massnahmen bei der Cloud-Anbieterin zuständig, soweit das Cloud Angebot einen Teil des Standards bildet, den die OIZ den Organisationseinheiten anbietet. Die Organisationseinheit kann auf diese Prüfung abstellen. Soweit die Organisationseinheit selbst einkauft, prüft sie auch selbst (andere Absprache vorbehalten) und bleibt diesbezüglich in der Verantwortung.

94 Diese Pflicht zur Sicherung des städtischen Perimeters auch bei Beizug von Dritten (im Sinne wie vorn beschrieben, siehe Rz. 20) ist deckungsgleich mit den *verwaltungsrechtlichen Pflichten* zum Schutz des Perimeters (vorn, Rz. 19) sowie den datenschutzrechtlichen Pflichten zur Vornahme technischer und organisatorischer Massnahmen (wie hier beschrieben, Rz. 80).

95 Die Organisationseinheit der Stadt Zürich hat somit keine abstrakte Erfolgshaftung dafür, dass es nicht zu Klartextzugriffen durch unbefugte Dritte kommt. Umgangssprachlich: **Die Organisationseinheit muss nicht für 100%ige Sicherheit einstehen**. Zwar gilt, dass die Organisationseinheit der Stadt Zürich vollumfänglich für die Einhaltung aller Vorgaben und Regularien einstehen muss, wenn sie Dritte beizieht. Die Organisationseinheit der Stadt Zürich muss aber nur für ein Verhalten einstehen, das ihr im strafrechtlichen Sinne zuzurechnen ist. Kriminelle Energie von Mitarbeitenden der Cloud-Anbieterin ist der Organisationseinheit der Stadt Zürich im strafrechtlichen Sinne nicht zuzurechnen.

96 Die vorstehenden Regeln lassen sich mit dem Begriff des **Normalbetriebs** umschreiben. Wenn nach dem gewöhnlichen Lauf der Dinge und der allgemeinen Lebenserfahrung mit Klartextzugriffen *nicht zu rechnen* ist, dann kann man von Normalbetrieb sprechen. **Aussergewöhnliche Ereignisse gehören nicht zum Normalbetrieb, auch wenn die Organisationseinheit der Stadt Zürich weiss, dass sie vorkommen könnten**.[82]

97 Ein solches Ereignis ausserhalb des Normalbetriebs wäre namentlich ein **Behördenzugriff** auf geheime Tatsachen. Dies ist hier in allgemeiner Weise bereits festzuhalten und in Teil 2 dieses Rechtsgutachtens im Detail zu begründen (hinten Rz. 118 ff.). Behördenzugriffe auf geheimnisgeschützte Daten sind nicht an der Tagesordnung. Nach allem was bekannt ist, kommen sie selten vor (deswegen kein Normalbetrieb, siehe zum Beispiel hinten, Rz. 208 ff.). Zusätzlich ist von Bedeutung, dass es in Ländern mit gefestigtem Rechtssystem bei einer reinen Beschlagnahmung noch zu keinen strafrechtlich relevanten Klartextzugriffen kommt. Näheres zum Behördenzugriff auf geheime Tatsachen und besonders zur Beschlagnahmung siehe unten Rz. 124.

(iv) Bei Bestellung der Cloud-Anbieterin als Hilfsperson

98 Es fällt bei systematischer Betrachtung von Art. 320 StGB (im Vergleich zu Art 321 StGB) auf, dass der Gesetzgeber davon abgesehen hat, auch **Hilfspersonen** der Strafbarkeit nach Art. 320 StGB zu unterstellen. Dennoch entspricht es ständiger Behördenpraxis, Hilfspersonal (z.B. IT-Dienstleistende oder Reinigungspersonal) als Hilfspersonen in Analogie zu Art. 321 StGB einzusetzen.[83] Dies ist mit Blick auf die Pflichten zum Perimeterschutz auch durchaus sachgerecht.

[82] LAUX/HOFMANN/SCHIEWECK/HESS, SBVg-Gutachten, Rz. 23: *«Dies bedeutet, dass die Bank ausreichende Schutzmassnahmen vorkehren muss, die nach dem gewöhnlichen Lauf der Dinge (d.h. im Normalbetrieb) normalerweise verhindern, dass Unbefugte den Inhalt des Geheimnisses wahrnehmen, d.h. Klartext-Zugriff erhalten.»*; ROSENTHAL, Rz. 99, S. 32: *«Der Täter handelt folglich nicht fahrlässig, wenn der Eintritt des Taterfolgs dermassen unwahrscheinlich erscheint und deshalb nach dem gewöhnlichen Lauf der Dinge und den Erfahrungen des Lebens nicht vorhersehbar ist.»*

[83] DSB des Kantons Zürich, Auslagerung, abrufbar unter: https://www.datenschutz.ch/datenschutz-in-oeffentlichen-organen/auslagerung (angesehen am 11. August 2021).

99 Der Gesetzgeber hat Art. 320 StGB im Rahmen des Erlasses des Informationssicherheitsgesetzes des Bundes (ISG; die Referendumsfrist ist am 10. April 2021 abgelaufen)[84] an diese gelebte Praxis angepasst.[85] Künftig unterstehen auch als Hilfsperson eingebundene IT-Dienstleister bzw. deren Mitarbeiter der Strafbarkeit nach Art. 320 StGB.[86] Für die Organisationseinheiten der Stadt Zürich bedeutet dies, dass sich ihre Mitarbeiter selbst dann **nicht** nach Art. 320 StGB strafbar machen, wenn sie einem Cloud-Anbieter bzw. dessen Mitarbeitern Klartextzugriff gewähren (z.B. im Rahmen von Wartungs- oder Supportarbeiten oder für Unterstützung bei der Datenmigration), sofern sie jedenfalls die Cloud-Anbieterin als Hilfsperson einbinden.

100 Wie wird diese Einbindung als Hilfsperson umgesetzt? Die an das Amtsgeheimnis gebundene Kundin (Behörde) muss die Cloud-Anbieterin mit vertraglichen und organisatorischen Massnahmen in ihren Perimeter[87] (den Kreis derjenigen, der zur Verantwortungssphäre der Behörde gehört) einbinden und somit ein Subordinationsverhältnis begründen. Die formelle Benennung als Hilfsperson ist nicht erforderlich. Es empfiehlt sich aber, von der Cloud-Anbieterin im Vertrag **bestätigen** zu lassen, dass die Cloud-Anbieterin den Umstand kennt, dass Kundendaten Informationen enthalten, die durch das Amts- oder Berufsgeheimnis geschützt sind. Benötigt die Cloud-Anbieterin Klartextzugriff und hat sie bestätigt, dass sie **Kenntnis hat davon, dass die Kundin (hier die Stadt Zürich) einer strafrechtlich geschützten Geheimhaltungspflicht untersteht**, gehört sie funktional verstanden zum Perimeter der Behörde.[88] Cloud-Anbieter (und, durch entsprechende Überbindung der Geheimhaltungspflichten, ihre Mitarbeitenden) sind somit **Hilfspersonen** der an das Amts- oder Berufsgeheimnis gebundenen Cloud-Kunden.[89]

101 Das Ermöglichen von Klartextzugriff an eine Hilfsperson ist keine strafbare Offenbarung. Verletzt die Hilfsperson ihrerseits die Geheimnispflicht, macht sie sich nach Art. 320 Abs. 1 (neu) StGB strafbar – nicht aber die Organisationseinheit der Stadt Zürich, die die Hilfsperson beigezogen hat.

102 Davon geht auch das Bundesgericht aus. Das viel diskutierte Urteil BGE 145 II 229 hat daran nichts geändert. Dieses betrifft die Frage, wie weit Anwältinnen den Kreis der Hilfspersonen ziehen dürfen – konkret: Dürfen Anwältinnen auch Hilfspersonen beiziehen, die ihrerseits Dritte beiziehen? Das Bundesgericht verneinte dies für den Fall, dass (1) die Anbieterin völlig frei ist, wen sie ihrerseits als Hilfsperson (Unter-Hilfsperson) beiziehen möchte und, dass (2) sie in Bezug auf die Unter-Hilfsperson (bzw. ganz generell) die Gewährleistung und Haftung gegenüber der Anwältin weitgehend einschränkt.[90]

103 BGE 145 II 229 ff. betraf einen Fall, in dem die beigezogene Hilfsperson im Alltag regelmässig uneingeschränkt und ohne besondere Kontrolle durch die Anwältin Klartextzugriff auf Mandatsakten nehmen konnte. Bei vielen modernen Cloud-Anbieterinnen kann mit technischen und organisatorischen Massnahmen nach dem allgemeinen Lauf der Dinge und der Lebenserfahrung (sprich «im Normalbetrieb») ausgeschlossen werden, dass seitens der Cloud-Anbieterin oder ihrer Mitarbeitenden Klartextzugriffe auf Vertrauliches genommen wird. Sofern die Stadt Zürich im Rahmen der von ihren Organisationseinheiten geplanten Umsetzungsprojekten darauf achtet, dass nur solche Lösungen verwendet werden, bei denen im Normalbetrieb kein Klartextzugriff stattfindet, hat somit BGE 145 II 229 von vornherein

[84] BBl 2020 9975.

[85] Mit den Umsetzungsarbeiten des ISG wurde im Juni 2021 begonnen. Die Vernehmlassung ist für anfangs 2022 geplant (erstes oder zweites Quartal 2022); die Inkraftsetzung des ISG samt entsprechenden Verordnungen auf den 1. Januar 2023. Gleichwohl ist es sinnvoll, bereits die Situation mitzubetrachten, die ab Inkrafttreten des ISG (und somit mit Anpassung von Art. 320 StGB) gelten wird.

[86] Art. 320 Abs. 1 StGB (neu), BBl 2020 9975, S. 10010.

[87] Zur Verwendung des Begriffs «Perimeter» im Zusammenhang mit der Wahrung von Berufsgeheimnissen (Bankkundengeheimnis), vgl. LAUX/HOFMANN/SCHIEWECK/HESS, SBVg-Gutachten, Rz. 5.

[88] Zur Auslegung des Begriffs vgl. CHRISTIAN SCHWARZENEGGER/FLORENT THOUVENIN/BURKHARD STILLER/DAMIAN GEORGE, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, in: Awaltsrevue 2019, 25, S. 28. Vgl. auch LAUX/HOFMANN/SCHIEWECK/HESS, SBVg-Gutachten, Rz. 35, 37. Die Nähe zur Formulierung in Art. 110 Abs. 3 StGB: *«Als Beamter gelten [...] Personen, die [...] vorübergehend amtliche Funktionen ausüben.»*

[89] SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, S. 29; STEINER (FN 67), S. 683.

[90] BGE 145 II 229 E. 7.4.

keine Bedeutung. Es werden somit technische und organisatorische Kontrollen dahingehend vorzusehen sein.

104 Umgekehrt betraf BGE 145 II 229 nicht ein Szenario, in dem sich z.B. eine Cloud-Anbieterin den Beizug z.B. einer Hosting-Anbieterin als Unter-Beauftragte von der Kundin genehmigen lässt und für deren Leistungen einsteht (Gewähr leistet). Die Stadt Zürich sollte aber mit vertraglichen Massnahmen sicherstellen, dass der von ihr gewählte Setup sich vom Sachverhalt gemäss BGE 145 II 229 (keine Kontrolle über den Beizug von Unter-Beauftragten) unterscheidet. Die Stadt Zürich kann somit auch Cloud-Anbieter beiziehen, die ihrerseits Unter-Beauftragte beiziehen.

(v) Zur Hilfsperson bei Auslandsbezügen

105 Teilweise wird in der öffentlichen Diskussion die Auffassung vertreten, dass die Cloud-Anbieterin im Ausland nicht als Hilfsperson der Geheimnisträgerin (Cloud-Kundin) anerkannt werden kann. Im Ausland entfalle der Schutz durch Strafrecht, wie er in der Schweiz greift. Dies wiederum laufe auf eine derart relevante Schutzreduktion hinaus, dass man von Strafbarkeit der Cloud-Nutzung durch Geheimnisträgerinnen sprechen müsse («over the border, out of control»).

106 Dieser Auffassung kann nicht gefolgt werden. Sofern die dem Amtsgeheimnis unterliegende Cloud-Kundin die geheimnisgebundenen Daten gemäss aktuellem Stand der Technik vor Klartextzugriffen durch Mitarbeiter des Cloud-Anbieters auch im Ausland schützt (Massnahmen gemäss Rz. 103), entsteht von vornherein keine Situation, die aus Sicht des Strafrechts sanktionswürdig wäre. Die Frage, ob die beigezogene Dritte (Cloud-Anbieterin) sich auch im Ausland im Sinne des (revidierten[91]) Art. 320 Ziff. 1 StGB als Hilfsperson strafbar machen könnte, wird dann gar nicht relevant; denn es kommt gar nicht erst zu Klartextzugriffen. Folglich steht auch die fehlende Unterstellung der Cloud-Anbieterin der Bearbeitung von amtsgeheimnisgebundenen Daten auf einer IT-Infrastruktur im Ausland nicht entgegen.

107 Sodann steht die in Rz. 105 erwähnte Auffassung dem Gesetzestext entgegen und damit Art. 1 StGB, wonach eine Strafrichterin ohne ausdrückliche gesetzliche Anordnung nicht auf Strafbarkeit erkennen darf. Die genannte Interpretation von Art. 320 StGB stellt eine Verschärfung dar, die im Gesetz keine Stütze findet. Namentlich die Regel, dass Informationen bei Beizug von Dritten nur geschützt wären, wenn diese Dritten der Strafbarkeit in der Schweiz unterstehen, ergibt sich nicht aus dem Gesetzestext.

108 Sodann gilt: Selbst wenn die Tathandlung der «Offenbarung» (Gewähren von Klartextzugriff) im Ausland ausgeführt wird, ist sie in der Schweiz strafbar, wenn der Erfolg (Offenbarung) in der Schweiz eintritt (Art. 8 Abs. 1 StGB). Nur wenn sich die Tat in keiner Weise in der Schweiz auswirkt (was jedoch schwer vorstellbar ist), würde eine Strafbarkeit in der Schweiz entfallen. In Bezug auf Mitarbeitende von Cloud-Anbietern im Ausland können sich zwar Durchsetzungsprobleme ergeben. Dies ist aber für die Zwecke des vorliegenden Rechtsgutachtens für so lange nicht relevant, als man noch von genügendem Schutz der Informationen sprechen kann.[92] Auch § 6 Abs. 1 IDG hält fest, dass Dritte beigezogen werden dürfen. § 6 Abs. 2 IDG verlangt sinngemäss nach Wahrung des Geheimnisses im Interesse der Stadt Zürich und § 7 IDG verlangt dann nach gehörigem Schutz der Informationen – alles unabhängig von einer strafrechtlichen Absicherung.[93]

[91] Ab Inkrafttreten der mit dem ISG begründeten Revision, d.h. (erwartungsgemäss) ab 1. Januar 2023. Vor diesem Zeitpunkt besteht von vornherein kein Anknüpfungspunkt dafür, den Beizug von Hilfspersonen im Ausland gestützt auf Überlegungen des Strafrechts zu limitieren, da Art. 320 StGB derzeit noch gar nicht mit dem Konzept der Hilfsperson operiert.

[92] Strafbarkeitsdrohung mit vernünftiger Erwartung, dass die Strafbarkeit auch durchgesetzt wird, vermittelt durchaus einen womöglich faktisch wirkenden «synthetischen» oder «rechtlich-konzeptionellen» Schutz (zu diesem Rz. 73). Es handelt sich aber nur um eines von vielen möglichen Elementen im Gesamtkonzept zum Schutz der Informationen. Dass es angemessenen Schutz ohne Sanktionswirkung nicht geben kann, dafür bleibt die in Rz. 105 genannte Auffassung den Nachweis schuldig.

[93] Vgl. ROSENTHAL, Rz. 70.

(vi) Subjektiver Tatbestand

109 In subjektiver Hinsicht verlangt Art. 320 StGB Vorsatz. Inkaufnahme, im Sinne des Eventualvorsatzes, genügt (Art. 12 Abs. 2 StGB). Wer im Sinne der vorstehenden Ausführungen für Sicherungsmassnahmen sorgt, die nach dem üblichen Lauf der Dinge und der allgemeinen Lebenserfahrung zu einem akzeptierten Schutzniveau beitragen («genügender Schutz»), hat keinen strafrechtlich sanktionierten Eventualvorsatz auf eine Verletzung[94] – dies gilt selbst dann, wenn ein verbotener Klartextzugriff am Ende doch stattfinden sollte.

110 Anders wäre der Fall zu beurteilen, in dem keine oder nur deutlich ungenügende Sicherungsmassnahmen getroffen werden; daraus könnte eine eventualvorsätzlich versuchte oder vollendete Geheimnisverletzung resultieren.

(vii) Zwischenfazit: Keine Verletzung von Art. 320 StGB

111 Dies bedeutet für die Stadt Zürich Folgendes: Die Organisationseinheiten der Stadt Zürich sollten soweit möglich reife Cloud-Lösungen wählen und einsetzen, bei denen es im Normalbetrieb nicht zu Klartextzugriffen kommt (Rz. 103). Lässt es sich aufgrund der Art der Lösung nicht vermeiden, dass Mitarbeitende der Cloud-Anbieterin in Einzelfällen Klartextzugriff auf geheimnisgebundene Informationen nehmen könnten, so hat die Stadt Zürich die Cloud-Anbieterin als Hilfsperson in ihren Perimeter (zum Perimeterbegriff vorn, Rz. 19) einzubinden. Dies kann dadurch erfolgen, dass die Cloud-Anbieterin im Vertrag bestätigt, von der Sondersituation der Stadt Zürich (Behördentätigkeit, Amtsgeheimnis) Kenntnis zu haben (vertragliche Massnahmen, siehe zum Vorgehen Rz. 100).[95]

112 Durch die Nutzung von Public Cloud Services durch eine Organisationseinheit der Stadt Zürich zur Speicherung und Verarbeitung von Amtsgeheimnissen kommt es somit nicht per se zu einer Verletzung von Art. 320 StGB, was freilich voraussetzt, dass die Organisationseinheit der Stadt Zürich (bzw. die OIZ[96]) im Rahmen eines Umsetzungsprojekts Massnahmen zum Schutz der geheimen Tatsachen getroffen hat, die nach dem gewöhnlichen Lauf der Dinge und der allgemeinen Lebenserfahrung dazu führen, dass Mitarbeitende der Cloud-Anbieterin oder sonstige unbefugte Dritte keinen Klartextzugriff auf die geheimen Tatsachen nehmen. Diese Massnahmen müssen im Lichte einer von der Organisationseinheit der Stadt Zürich (bzw. der OIZ) durchgeführten Risikoanalyse als angemessen erscheinen, so dass ein allenfalls bestehendes Restrisiko, dass gleichwohl ein Klartextzugriff vorkommen könnte, als wenig wahrscheinlich erscheint. Dass die Organisationseinheit der Stadt Zürich (bzw. die OIZ) im Rahmen ihrer Risikoüberlegungen zu diesem Resultat kommen wird («Angemessenheit der Massnahmen liegt vor»), ist aufgrund der bisherigen Erfahrungen und wegen allgemeiner technischer Gründe, wie sie sich z.B. aus Anhang 2 ergeben und wie sie im erwähnten SBVg-Gutachten bereits dargelegt wurden,[97] mit genügender Sicherheit zu erwarten.

---

[94] LAUX/HOFMANN/SCHIEWECK/HESS, SBVg-Gutachten, Rz. 28: *«Weder vorsätzliche noch fahrlässige Tatbegehung liegen vor, wenn die Organe der Bank zum Schluss kommen, dass die von ihnen gewählte technische IT-Infrastruktur wirksam gegen Offenbarungen an unbefugte Dritte schützt.»* ROSENTHAL, Rz. 86, S. 29: *«Prüfte [der Berufsgeheimnisträger] das Risiko einer Offenbarung sorgfältig, versucht[e] er alle möglichen Massnahmen treffen, um eine solche zu verhindern, und kam er zum Schluss, dass zwar rechnerisch eine nicht nur theoretische Wahrscheinlichkeit einer Offenbarung besteht, diese aber nicht allzu hoch war und er somit darauf vertrauen konnte, dass nichts passiert, so handelte er nicht mehr eventualvorsätzlich.»*

[95] Diese Gestaltungsform kann gleichsam als Sicherungsanker benutzt werden für den Fall, dass die gewählten technischen und organisatorischen Massnahmen im Einzelfall doch nicht ausreichen sollten. Rechtlich-konzeptionelle Strategien (Rz. 73) haben dann die Wirkung eines Sicherungsankers.

[96] Hier wird stets aus der Perspektive der nutzenden Organisationseinheit formuliert. Es ist aber mitverstanden, dass innerhalb der Stadt Zürich Aufgaben zur Kontrolle der Cloud-Anbieterin und zur Umsetzung von Schutzmassnahmen an die OIZ delegiert sind und von dieser wahrgenommen werden. Die Massnahmen der OIZ sind der nutzenden Organisationseinheit zuzurechnen, siehe Rz. 90; nach Bestätigung der OIZ (Rz. 68, Punkt 2) muss die Organisationseinheit noch plausibilieren (Rz. 68 Punkt 3), kann sich aber im Übrigen auf die Prüfung der OIZ verlassen; siehe auch Ziff. 2 der angedachten stadträtlichen Weisung, der Fokus auf den sog. «Basisschutz+» dient gerade dem Zweck, eine gesamtstädtische Perspektive einzunehmen (Rz. 64), für weiteren Kontext siehe auch Rz. 120).

[97] LAUX/HOFMANN/SCHIEWECK/HESS, SBVg-Gutachten, Rz. 75.

113 Will die Stadt Zürich hingegen Cloud-Lösungen einsetzen, für deren Betrieb auch im Normalbetrieb in der Regel ein Klartextzugriff durch Mitarbeitende der Cloud-Anbieterin notwendig ist, dann muss die Stadt Zürich die Cloud-Anbieterin und (durch Überbindung der Geheimhaltungspflichten der Cloud-Anbieterin und Hinweis auf die Strafbarkeit) ihre Mitarbeitenden als Hilfspersonen in ihren Perimeter einbinden.

b. Art. 293 StGB

114 Der Vollständigkeit halber ist auf den Sondertatbestand (eine Übertretung) der Veröffentlichung amtlicher geheimer Verhandlungen hinzuweisen. Tathandlung ist dort im deutschen Gesetzestext «etwas an die Öffentlichkeit bring[en]».[98] Auf die Ausführungen zu Art. 320 StGB (vorstehend) kann gesamthaft verwiesen werden.

2. Verstärkung der Schweigepflichten durch Prozessrecht

115 Der Schutz des Amtsgeheimnisses wird nicht nur durch Art. 320 StGB verstärkt, sondern zusätzlich auch durch das Recht bzw. die Pflicht zur Aussageverweigerung. Dies ist hier zur Vervollständigung kurz anzumerken. Vorn wurde dies bereits in aller Kürze angesprochen (im Kontext der reaktiven Entbindung vom Amtsgeheimnis, Rz. 41). Es geht dabei jeweils um Folgendes:

- Verweigerungspflicht: Die Beamtin muss die Aussage zunächst verweigern, wenn sie von einer Straf- oder Zivilbehörde zur Aussage aufgefordert wird (Art. 320 Ziff. 1 Satz 1 StGB). Wer der Strafnorm untersteht, kann auch im Prozess nicht zur Aussage zum Geheimnis gezwungen werden (Art. 171 StPO, Art. 166 Abs. 1 lit. c ZPO, Art. 16 Abs. 1 VwVG, Art. 42 Abs. 3 BZP).
- Aussagerecht: Wird die Beamtin von der vorgesetzten Behörde schriftlich von der Schweigepflicht entbunden, hat sie ein Aussagerecht (Art. 320 Ziff. 2 StGB).
- Kein Verweigerungsrecht: Wird eine Art. 320 StGB unterstehende Geheimnisträgerin wie die Organisationseinheit von der Geheimhaltungspflicht entbunden, muss sie an der Beweiserhebung mitwirken (Art. 166 Abs. 1 lit. c ZPO; Art. 170 Abs. 2 StPO).[99]

116 Zusätzlich ist auf die Regeln zur Beschlagnahme hinzuweisen (dazu ausführlich hinten, Rz. 120 ff.). Diesbezüglich gelten andere Abläufe, wobei die Stellung der Geheimnisträgerin zu Besonderheiten führen kann. Ausserdem ist ergänzend anzumerken, dass Vorstehendes die Situation beschreibt, wo die Organisationseinheit als Drittperson im Verfahren befragt würde. Für den Bereich des Zivilprozesses ist zusätzlich die Fallkonstellation zu erwähnen, in der die Organisationseinheit selbst Verfahrenspartei ist (siehe Rz. 121). In einem solchen Szenario geht der Schutz des Amtsgeheimnisses nicht so weit: Das Amtsgeheimnis nach Art. 320 StGB wird dann nur als ein weiteres gesetzlich geschütztes Geheimnis behandelt.[100] Die Organisationseinheit wäre als Partei grundsätzlich zur Aussage verpflichtet, es sei denn, sie kann glaubhaft machen, dass das Geheimhaltungsinteresse das Interesse an der Wahrheitsfindung überwiegt (Art. 163 Abs. 2 ZPO).

[98] Art. 293 StGB lautet wie folgt: «*(1) Wer aus Akten, Verhandlungen oder Untersuchungen einer Behörde, die durch Gesetz oder durch einen gesetzmässigen Beschluss der Behörde als geheim erklärt worden sind, etwas an die Öffentlichkeit bringt, wird mit Busse bestraft. (2) Die Gehilfenschaft ist strafbar. (3) Die Handlung ist nicht strafbar, wenn der Veröffentlichung kein überwiegendes öffentliches oder privates Interesse entgegengestanden hat.*»

[99] Siehe BGE 97 II 369, 370; siehe etwa SVEN RÜETSCHI, in: Christoph Hurni et al. (Hrsg.), Berner Kommentar, Schweizerische Zivilprozessordnung, Band II, Bern 2012, Art. 166 N 24.

[100] ERNST F. SCHMID, in: Karl Spühler/Luca Tenchio/Dominik Infanger (Hrsg.), Basler Kommentar, Schweizerische Zivilprozessordnung, 2. Aufl., Basel 2013, Art. 163 N 8c.

3. Zwischenfazit zum Amtsgeheimnis: Sowohl bei Cloud-Angeboten ohne Klartextzugriff sowie bei Cloud-Angeboten mit Klartextzugriff kann das Amtsgeheimnis eingehalten werden

117 Im Resultat ergibt sich, dass die Umsetzung einer Cloud-Migration unter Wahrung der Geheimhaltungspflichten gemäss Art. 320 StGB machbar ist (vorn Rz. 111 ff.).

III. Teil 2: Anwendung der Grundlagen auf ausgewählte Zugriffsszenarien

A. Unbefugte Klartextzugriffe durch die Cloud-Anbieterin oder deren Mitarbeitende

118 Kommt es auf den IT-Infrastrukturen der Cloud-Anbieterin zu unbefugten Klartextzugriffen im Normalbetrieb, sei es durch Mitarbeitende der Cloud-Anbieterin oder durch Mitarbeitende von Subakkordantinnen der Cloud-Anbieterin, kann dies zu einer Strafbarkeit der jeweils zugreifenden Personen (und nicht etwa der Mitarbeiterinnen einer Organisationseinheit der Stadt Zürich) führen. Dies ist direkte Folge der Ausführungen zu Art. 320 StGB und Art. 293 StGB (dazu vorn, Rz. 84 ff.).

119 Es ist namentlich auf die Strafbestimmungen von Art. 179^{novies} StGB hinzuweisen, welche Bestimmung vor «Hausfriedensbruch»[101] und «Veruntreuung» im Informationsrecht schützt. Ausserdem kann im Einzelfall auch eine Strafbarkeit von Art. 143 StGB oder Art. 143bis StGB begründet werden. Es ist für eine Strafbarkeit nach Art. 179^{novies} StGB nicht erforderlich, dass die Daten – wie bei Art. 143 StGB (Unbefugte Datenbeschaffung) und Art. 143bis StGB (Unbefugtes Eindringen in ein Datenverarbeitungssystem) – gegen den Zugriff der Täterin besonders gesichert sind.[102] Für die Strafbarkeit nach Art. 179^{novies} StGB genügt bereits eine fehlende Zugriffsberechtigung.[103] Wenn die Cloud-Anbieterin der Dienststelle vertraglich zusichert, während des Normalbetriebs keinen Klartextzugriff auf Inhalte zu nehmen, dann anerkennt die Cloud-Anbieterin damit, dass sie in Bezug auf diese Daten keine Zugriffsberechtigung hat. Mit anderen Worten: Aufgrund solcher Vertragsbestimmungen sind Serverinhalte (Daten auf virtuellen Maschinen oder auf Tenants) für die Cloud-Anbieterin «fremd» und gelten als Daten, zu denen sie keine Zugangsberechtigung hat. Wenn z.B. Personal der Cloud-Anbieterin sich doch unbefugt Zugriff auf Daten der Organisationseinheit der Stadt Zürich verschafft, führt dies nach dem Vertrauensprinzip *nicht* zur Strafbarkeit der Organisationseinheit, da sich diese darauf verlassen durfte, dass das Personal der Cloud-Anbieterin sich an die Zugriffsverbote halten würde.[104]

[101] Zum Vergleich: Der Vermieter von Büroräumlichkeiten, der sich gegen den Willen des Mieters in die Räumlichkeiten begibt und die Ordner mit Geheimnissen durchsucht, macht sich des Hausfriedensbruchs i.S.v. Art. 186 StGB strafbar, selbst wenn er einen Ersatzschlüssel für Notfälle hat oder sich einen solchen hat nachmachen lassen. Die Berechtigung des Mieters ergibt sich einzig aus dem Vertrag. Niemand würde auf die Idee kommen, vom Vermieter zu verlangen, sich als Hilfsperson i.S.v. Art. 321 StGB ins Geheimnis einbinden zu lassen. Der vertragliche Schutz (allenfalls mit Verstärkung durch Art. 186 StGB) genügt. Dasselbe muss für den Mitarbeiter der Cloud-Anbieterin gelten, der gegen den Willen des Kunden Einsicht in die geschützten Informationen nimmt. Bei der Miete von Büroräumlichkeiten wie bei der Nutzung von Cloud-Angeboten geht es nicht um den absoluten Schutz, sondern um die Verhinderung von Offenbarungen im Normalbetrieb. Mit den soeben genannten Mechanismen wird dieser Schutz sichergestellt, und zwar alternativ mit oder ohne Einbindung des Cloud-Anbieters als Hilfsperson i.S.v. Art. 321 StGB.

[102] Unzutreffend deswegen der Entscheid VD.2019.93 des Appellationsgerichts Basel-Stadt vom 11. September 2019: *«Wie jedoch der Tatbestand des unbefugten Beschaffens von Personendaten gemäss Art. 179^{novies} StGB erfüllt worden sein sollte, ist bei provisorischer und summarischer Prüfung entgegen der Auffassung des Rekurrenten (vgl. Rekursbegründung vom 16. Mai 2019 S. 4) nicht ersichtlich. Unter Beschaffen im Sinne dieser Bestimmung wird das Überwinden oder Umgehen einer Zugangssperre verstanden (RAMEL/VOGELSANG, in: Basler Kommentar, 4. Auflage, 2019, Art. 179^{novies} N 23).»* Dieser Entscheid will Art. 179^{novies} StGB als Instrument zum logisch-technischen Perimeterschutz verstehen. Schutzgegenstand ist aber «bloss» das Vertrauen dessen, der auf vertragliche Zusicherungen vertraut.

[103] ANDREAS DONATSCH, in: Andreas Donatsch (Hrsg.), StGB/JStG Kommentar, 20. Aufl., Zürich 2018, Art. 179^{novies} N 5 (zit. StGB/JStG-DONATSCH).

[104] DAVID ROSENTHAL, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter, 10. August 2020, Rz. 99, S. 32 (zit. Cloud und CLOUD Act): «[D]er Täter [bleibt] straffrei, wenn der Taterfolg durch das pflichtwidrige Verhalten einer Drittperson herbeigeführt wurde, sich der Täter aber gemäss dem Vertrauensprinzip darauf verlassen durfte, dass die mitwirkende Person sich pflichtgemäss verhalten würde.»

B. Klartextzugriffe durch Behörden in der Schweiz

1. Vorbemerkungen zu Behördenzugriffen im Allgemeinen

120 Es kann nicht von vornherein ausgeschlossen werden, dass Strafverfolgungsbehörden an Informationen interessiert sind, die sich in einem Tenant einer Organisationseinheit der Stadt Zürich befinden. Für die Zwecke des vorliegenden Rechtsgutachtens muss man sich jedoch vor Augen halten, dass die Stadt Zürich von der Strafuntersuchung zumeist *relativ weit entfernt* sein wird:

- Fall 1: Geht es um eine Abfrage von Meldedaten einer Person, wird die Strafuntersuchungsbehörde eine Direktanfrage an die relevante Organisationseinheit richten.
- Fall 2: Ähnlich ist es wohl, wenn die Strafuntersuchungsbehörde wissen will, ob eine beschuldigte Person zu einem bestimmten Zeitpunkt Kontakt hatte mit der Stadt Zürich; auch dann gelangt sie wohl direkt an die Stadt Zürich. Ein Zugriff auf Daten bei der Cloud-Anbieterin ist auch hier nicht besonders wahrscheinlich.
- Fall 3: Eine theoretische Relevanz von Daten im Cloud-Tenant der Stadt Zürich ist denkbar, wenn die beschuldigte Person eine Mitarbeiterin der Stadt Zürich ist und die Tat mutmasslich vom Arbeitsplatz bei der Stadt Zürich aus vorgenommen wurde. Auch dann ist aber damit zu rechnen, dass die Strafverfolgungsbehörde sich direkt an eine ihr vertrauenswürdig erscheinende Stelle der Stadt Zürich wenden wird, um das Vorgehen abzustimmen (Datenherausgabe direkt durch die Stadt Zürich). Es wird der Strafverfolgungsbehörde darum gehen abzusichern, dass die angefragte Stelle nicht mit der verdächtigten Person kolludieren wird.

121 Dass die Stadt Zürich nicht als Dritte, sondern als direkt von der Strafuntersuchung betroffene Entität im Fokus einer Strafuntersuchung steht, ist nicht vorstellbar.

122 Wenn man sich dies vor Augen hält, geht es bei der Problemstellung Behördenzugriff um eine sehr wenig relevante Aufgabenstellung. Nur im Fall 3 wird sich eine Strafverfolgungsbehörde für Daten «der Stadt Zürich» und (womöglich) im Tenant der Stadt Zürich interessieren. Dass nicht die übergeordnete Stelle direkt angegangen wird und dass die Strafverfolgungsbehörde stattdessen den Weg über die Cloud-Anbieterin nimmt, ist zwar nicht ausgeschlossen und also möglich, aber doch sehr unwahrscheinlich.

123 Für ein derart entferntes Risiko würde allerdings niemand ein Rechtsgutachten in Auftrag geben, jedenfalls wenn es nur um Strafverfolgungsbehörden in der Schweiz ginge (gerade mit Blick auf die zu erwartenden Abläufe, wie in Rz. 122 geschildert). Auslöser für dieses Rechtsgutachten sind befürchtete Zugriffe von Strafverfolgungsbehörden in den USA; mit deren Praktiken ist man hierzulande weniger vertraut (siehe dazu auch hinten, Rz. 139). Um den Vergleich zur Rechtslage in der Schweiz zu ziehen, sind Ausführungen zur Rechtslage in der Schweiz voranzustellen.

2. Prüfung

124 Cloud-Anbieterinnen behalten sich üblicherweise vor, Kundendaten an Strafverfolgungsbehörden herausgeben zu dürfen. Es kann dabei um eine grosse Bandbreite von unterschiedlichen Angaben von der oder über die Kundin – d.h. die Organisationseinheit der Stadt Zürich – gehen:

- «Bestandsdaten» sind Daten, welche die Cloud-Anbieterin benötigt, um die Geschäftsbeziehung mit der Kundin (der Organisationseinheit der Stadt Zürich, welche die Vertragsbeziehung unterhält) zu verwalten. Dazu können gehören: Vorname, Name, Adresse, Telefonnummer, alternative E-Mail-Adresse und andere Registrierungsdetails, die zeigen, wie die Kontoinhaberin zu identifizieren ist. Diese Angaben erlauben z.B. Strafverfolgungsbehörden festzustellen, wer einen Dienst bei der Cloud-Anbieterin bezieht. Je nach Kundenbeziehung kann die Strafverfolgungsbehörde auch erkennen, wer den Dienst verwendet. Da z.B. E-Mail-Adressen eines Cloud-Dienstes andernorts eingesetzt werden,

z.B. um sich beim anderen Service zu registrieren, können solche Angaben für Strafverfolgungsbehörden bereits interessant sein, z.B. um die Täterin einer Straftat zu ermitteln.

- «Randdaten» oder «Verkehrsdaten» sind solche, die bei der Nutzung eines Cloud-Angebots anfallen. Solche Informationen geben zum Beispiel Auskunft darüber, wer mit wem, wann, wie lange und von wo aus einen bestimmten Cloud-Dienst genutzt hat, z.B., um mit anderen zu kommunizieren.
- «Inhaltsdaten» schliesslich bezeichnen die konkreten Informationsinhalte, die im Rahmen eines Cloud-Dienstes erstellt und ausgetauscht werden (z.B. Sprachaufzeichnungen, Textaufzeichnungen vom gesprochenen Wort- (oder Video-)Anrufen oder der Inhalt von versandten oder empfangenen E-Mails).

125 Die Strafverfolgungsbehörde müsste sich, wenn sie solche Angaben in das Strafverfahren ziehen wollte, auf eine der verfügbaren gesetzlichen Grundlagen (Art. 265 StPO: Beschlagnahme, Art. 22 BÜPF: Auskünfte, Art. 269 f. StPO: Überwachung von Anschlüssen; oder gar noch weiter gehende Aufforderungen zur Datenherausgabe nach Art. 273 StPO) beziehen.

126 Die Organisationseinheit der Stadt Zürich wird aber jeweils ihr Amtsgeheimnis geltend machen. Dieses verhindert auf den ersten Blick die Verwertung der Information im Strafverfahren. Es handelt sich jedoch nur um ein grundsätzliches Verwertungsverbot im Strafverfahren. Das Amtsgeheimnis resultiert nicht in jedem Fall in einem Verwertungsverbot. Es gibt verschiedene Situationen, in denen die geschützte Information dennoch Eingang in das Strafverfahren finden kann (je nach Ausgang der Interessenabwägung könnte es z.B. zu einer Entbindung des Amtsgeheimnisses kommen, siehe vorn, Rz. 41).

127 Wenn man nun hypothetisch davon ausgeht, dass es im Einzelfall doch nicht zu einer solchen Entbindung kommt, würde eine ungewollte Offenbarung von geheimen Informationen drohen. Ein genauerer Blick zeigt aber, dass es auf die Geheimnisverweigerungsrechte gar nicht ankommen wird, sondern vielmehr darauf, *wie eine Strafverfolgungsbehörde beschlagnahmt, wie sie anschliessend das Beschlagnahmte siegelt und wie bzw. wann die Strafverfolgungsbehörde auf die geschützte Information Klartextzugriff* nimmt.[105] Denn es gilt auch hier. **Erst die Offenbarung ist im Lichte der Aufgabenstellung relevant** (Rz. 13).

128 Oder anders ausgedrückt: Es ist nicht der Vorgang der Beschlagnahmung als solcher entscheidend, sondern die Frage, ob es der Organisationseinheit der Stadt Zürich im Rahmen des anknüpfenden strafprozessualen Verfahrens gelingt, erfolgreich die Freigabe von geschützter Information (geschützten Tatsachen) bzw. den Klartextzugriff im Strafprozess zu verhindern. Im Zentrum steht jeweils das Institut der Siegelung, das auch den Trägern des Amtsgeheimnisses (Art. 170 i.V.m. Art. 248 StPO) zur Verfügung steht.[106] Erst nach einer *Ent*siegelung kommt es zum eigentlichen Klartextzugriff.

129 **In dieser Konstellation beschränkt sich deshalb die Schutzpflicht der Geheimnisträgerin – der Organisationseinheit der Stadt Zürich – auf die Geltendmachung von Siegelungsmassnahmen. Für eine Erfolgsgarantie, dass es bei der beantragten Versiegelung bleibt bzw. dass ein Gericht die Entsiegelung nicht anordnen wird, muss die Stadt Zürich nicht einstehen. Die Organisationseinheit der Stadt Zürich hat somit auch in einem solchen Szenario keine Erfolgshaftung dafür, dass es zu keinen Klartextzugriffen kommt.**

130 Strafverfolgungsbehörden können jederzeit jegliche in ihrem Zugriffsbereich liegenden Daten beschlagnahmen. Es ist denkbar, dass die Beschlagnahmung aus rechtlichen Gründen später vom zuständigen Gericht aufgehoben wird. Das ändert jedoch nichts daran, dass niemand davor geschützt ist, dass eine Strafverfolgungsbehörde einen bei ihr gespeicherten Datensatz beschlagnahmt. Dies gilt sogar für Anwältinnen oder Ärztinnen. Und auch für die Organisationseinheiten der Stadt Zürich gilt Entsprechendes.

[105] Der Begriff «Behördenzugriff» suggeriert sofortigen Klartextzugriff durch die Strafverfolgungsbehörde. Dies ist allerdings nicht zutreffend, siehe dazu die Ausführungen in Rz. 133 f.

[106] THOMAS MÜLLER/STEFAN GÄUMANN, Siegelung nach Schweizerischer StPO, in: Anwaltsrevue, 2012, 290 ff., S. 291.

131 Für Daten, die auf IT-Infrastrukturen einer Cloud-Anbieterin gespeichert sind, gilt nun nichts anderes. Strafverfolgungsbehörden können auch solche Daten jederzeit beschlagnahmen. Einschränkend ist höchstens anzumerken, dass es einer Strafverfolgungsbehörde wohl rein faktisch deutlich schwerer fallen wird, Daten auf den komplexen IT-Infrastrukturen einer Cloud-Anbieterin mit einem hochskalierenden Cloud-Angebot zu lokalisieren, als wenn sie Geräte direkt bei der Organisationseinheit der Stadt Zürich durchsuchen würde.[107]

132 Die Ausgangslage bei der Nutzung eines Cloud-Angebots verändert sich somit für die Organisationseinheit der Stadt Zürich nicht (namentlich nicht im Vergleich zur Situation, wie sie bestehen würde, wenn die Dienststelle eigene IT-Infrastrukturen verwenden würde). Die Dienststelle könnte sich der Beschlagnahme von Akten oder Daten aus ihrem Perimeter nicht erfolgreich widersetzen – obwohl sie dem Amtsgeheimnis untersteht. Die Strafverfolgungsbehörden könnten den Gewahrsam notfalls mit Gewalt erzwingen – obwohl die Dienststelle der Geheimnispflicht nach Art. 320 StGB untersteht und ein Zeugnisverweigerungsrecht gemäss Art. 171 StPO geltend machen könnte.

133 Der Rechtsschutz zu Gunsten der Geheimnisherrin erfolgt erst im Anschluss an das In-Gewahrsam-Nehmen durch die Strafverfolgungsbehörde in der Weise, dass die Strafverfolgungsbehörden in Bezug auf edierte oder sichergestellte Daten eine Siegelung vorzunehmen hat (Art. 248 Abs. 1 StPO). Das Bundesgericht hat in seinem Urteil 1B_274/2019 vom 12. August 2019, E. 3.3 in aller Klarheit festgehalten, dass die Beschlagnahme der Datenträger (Massnahme «auf dem Code Layer») keinen Klartextzugriff (Einsichtnahme «in den Content Layer») zur Folge hat:

> *«Der Wortlaut von Art. 248 StPO ist in dem Sinne doppelt eindeutig, als er festhält, dass auszusondernde Aufzeichnungen von den Strafbehörden nicht nur nicht verwendet, sondern auch nicht eingesehen werden dürfen (Abs. 1) und dass über ein Entsiegelungsgesuch im Vorverfahren das Zwangsmassnahmengericht bzw. ansonsten das Gericht, bei dem der Fall hängig ist, zu entscheiden hat (Abs. 3); das Gericht kann dafür überdies eine sachverständige Person beiziehen (Abs. 4), wird also gesetzlich ermächtigt, sich Unterstützung zu organisieren.»*

134 Im Rahmen von Art. 248 Abs. 4 StPO kann es freilich zu Klartextzugriffen kommen. Dies durch das über die Entsiegelung befindende Gericht oder seine Sachverständige. Es handelt sich dabei aber um eine Art. 320 StGB vorgehende Sonderregel (*lex specialis*), was sich aus Art. 14 StGB ergibt:

> *«Wer handelt, wie es das Gesetz gebietet oder erlaubt, verhält sich rechtmässig, auch wenn die Tat nach diesem oder einem andern Gesetz mit Strafe bedroht ist.»*

135 Klartextzugriffe durch das Zwangsmassnahmengericht sind infolge der Sonderregel des Art. 248 Abs. 4 StPO somit nicht rechtswidrig im Sinne von Art. 320 StGB. Mit anderen Worten hat die Dienststelle nicht die Pflicht, bereits die Beschlagnahme von Amtsgeheimnissen zu verhindern. Die Dienststelle müsste im Beschlagnahmefall nur die Siegelung verlangen und sich – soweit dies in ihren Möglichkeiten steht – auf ihr Zeugnisverweigerungsrecht berufen. Damit hätte sie getan, was die Schweigepflicht von ihr verlangt.[108] Für mehr besteht keine Pflicht.

136 Nach dem Wortlaut der Bestimmung hat die Siegelung von Amtes wegen oder auf Antrag der betroffenen Person zu erfolgen. Als betroffene Person kommen namentlich die Inverkehrbringerin der beschlagnahmten Information oder eben die Organisationseinheit selbst in Frage. Jedenfalls wenn möglich sollte sie im Fall der Beschlagnahme bei den Strafverfolgungsbehörden intervenieren, auf das Bestehen von Amtsgeheimnissen hinweisen und die Siegelung in einem solchen Fall formell beantragen (**Pflicht zur Vornahme von Siegelungsbegehren**). Die Dienststelle sollte Methoden und interne Abläufe festlegen, die sicherstellen, dass bei ihr eingehende Anfragen von Strafverfolgungsbehörden auf Mitwirkung bei

[107] Die Ausführungen in Anhang 2 zeigen, dass bei Verwendung einer grossen, unpersönlich verwalteten IT-Infrastruktur eines sog. Hyperscalers unter verschiedenen Blickwinkeln womöglich faktisch eine Besserstellung der Organisationseinheit der Stadt Zürich resultiert, im Vergleich dazu, wenn sie Daten auf eigenen IT-Infrastrukturen bei sich selbst gespeichert hält. Dies wird freilich differenzierend zu beantworten sein, je nachdem, ob man eine Kurz- oder eine Langzeitbetrachtung anlegt, sodann kann die Antwort abhängig davon sein, um welche Art von Informationen es geht.

[108] Man könnte auch argumentieren, dass die Strafverfolgungsbehörde die Siegelung auch von sich aus vorzunehmen hat, selbst wenn die Siegelung von der Organisationseinheit der Stadt Zürich nicht beantragt worden ist.

der Datenbeschlagnahme routinemässig so beantwortet werden, dass die Behörde sofort und umgehend zur Siegelung der beschlagnahmten Daten aufgefordert wird. Die Dienststelle sollte auch die Cloud-Anbieterin vertraglich verpflichten, einen solchen Antrag jeweils routinemässig und in jedem Fall der anfragenden Behörde zu stellen. Alle involvierten Parteien, insbesondere die Cloud-Anbieterin, müssen jedoch dafür sorgen, dass es bei der Behörde umgehend zu einer Siegelung kommt (**Schutzpflichten**). Die Cloud-Anbieterin muss die Dienststelle im Fall, dass eine fremde Behörde auf solche Daten zugreift, informieren (**Informationspflicht**). Die Organisationseinheit der Stadt Zürich hat diese Information dann unverzüglich ihrer direkt übergeordneten Behörde weiterzuleiten, damit vor dieser das Verfahren nach Art. 320 Ziff. 2 StGB abgewickelt werden kann (dazu Rz. 41). Die Dienststelle sollte die Cloud-Anbieterin zudem verpflichten, technische Massnahmen zu implementieren, die einen Zugriff auf bestimmte Informationen automatisch dokumentieren (**Event Logging**) und an die Organisationseinheit übermitteln (**Informationspflicht**).

137 Mit anderen Worten ist im Kontext von Datenbeschlagnahmungen in der Schweiz sowohl die Stellung der Cloud-Anbieterin als auch die Frage, ob sich Daten der Dienststelle auf eigenen IT-Infrastrukturen oder solchen der Cloud-Anbieterin befinden, nicht von Bedeutung. Denn in jedem Fall muss die Dienststelle dafür besorgt sein, dass an Strafverfolgungsbehörden übermittelte Informationen tatsächlich nach den Vorschriften über die Siegelung der Verwertung im Prozess entzogen werden.

138 Soweit es dann im Rahmen eines richterlichen Entscheids zu einer Entsiegelung kommen sollte, würde dies für die Organisationseinheit der Stadt Zürich noch immer nicht zu einer Strafbarkeit wegen Offenbarung führen. Die Offenbarung wäre Folge behördlichen Zwangs und die Repräsentanten der betreffenden Organisationseinheit könnten sich auf jeden Fall auf den Rechtfertigungsgrund von Art. 14 StGB berufen.

C. Klartextzugriffe durch Behörden im Ausland (namentlich in den USA)

1. Problematik

a. Im Allgemeinen

139 Die Problematik des Behördenzugriffs durch Behörden im Ausland ist zunächst gleich gelagert wie jene nach schweizerischem Recht. Die Stadt Zürich und ihre Daten sind relativ weit entfernt von einer potenziellen Strafuntersuchung (siehe dazu bereits vorn, Rz. 120).

140 Und doch sorgt die Thematik in der öffentlichen Diskussion für Wirbel. Wenn es nicht um befürchtete Zugriffe «einer fremden Macht» ginge, würde es dieses Rechtsgutachten nicht geben (vorn, Rz. 123). Auslöser für das Rechtsgutachten ist die sehr grosse Bedeutung, die dem Thema beigemessen wird. Ursächlich hierfür sind wohl verschiedene Wahrnehmungen, die teilweise berechtigt sind, die aber mit der Fragestellung gleichwohl nicht zusammenhängen.[109] Sodann spielt auch für die hier zu beantwortende Frage der «gefühlte Datenschutz» eine nicht zu unterschätzende Rolle: Das Unbekannte kann für die mit der Materie zu wenig vertraute Person bedrohlich wirken. Die Diskussion kann sodann auch rasch auf eine Spur geraten, auf der es statt um die Rechtsfrage um andere Themen geht bzw. wo kommerzielles bzw. heimatschützendes Wunschdenken verschiedene Aussagen in der Öffentlichkeit nähren. Solche Aspekte sind in einem Rechtsgutachten auszublenden.

141 Im Vergleich zur womöglich geringen praktischen Bedeutung weist das Thema in rechtlicher Hinsicht eine sehr grosse Komplexität auf. Nur schon die Verortung fällt schwer. Die nachfolgenden Vorbemerkungen sind notwendig zur Verortung des Themas.

[109] Die Thematik rund um «Schrems II» hängt mit der Fragestellung der Stadt Zürich nicht zusammen. Dazu mehr in Rz. 170.

142 Vorab ist präzisierend festzuhalten, dass es stets – und auch für diese Frage – um eine Risikobewertung geht, d.h. um die Frage, wie wahrscheinlich es ist, dass eine Drittperson von Informationen der Stadt Zürich Kenntnis erhält. Im vorliegenden Rechtsgutachten geht es nicht um eine Risikoeinschätzung, ob die Faktenlage (dazu vorn, Rz. 10) vor solchen Kenntnisnahmen schützt. Es geht um die Prüfung, ob Auslandsbezüge ein Risiko darstellen. Man geht in der öffentlichen Diskussion a priori davon aus, dass z.B. der Zugriff wegen des sog. «langen Arms», den das ausländische Recht unter Umständen postuliert (Beispiel CLOUD Act), offensichtlich ein grösseres Risiko dafür darstellt, dass die ausländische Strafverfolgungsbehörde auf Informationen der Stadt Zürich zugreifen kann, als wenn der ausländische Staat z.B. das Rechtshilfeverfahren bemüht (siehe Rz. 146). Rechtstatsächliche Forschungen stehen zwar nicht zur Verfügung und wären interessant (Beispiel: «*Wie wahrscheinlich ist es, dass das Bundesamt für Justiz (BJ) im Rechtshilfeverfahren Informationen zurückhalten wird, wenn eine US-amerikanische Behörde beim BJ vorstellig wird?*»). Man muss einstweilen ohne sie auskommen. Indem man solche Fragen stellt, kann man aber immerhin schon aufzeigen, dass der intuitive Schluss («Risiko beim BJ ist kleiner» bzw. «Risiko im Ausland ist grösser») womöglich vorschnell ist (Bias: «Jumping to Conclusions»).

b. Der ausländische Behördenzugriff wird anders behandelt als der inländische

143 Wenn man anknüpft an die Ausführungen im voranstehenden Abschnitt (Zugriff von Strafverfolgungsbehörden in der Schweiz, Rz. 120 ff.) kann Folgendes als gesichert gelten:

- dass eine strafverfolgende Behörde Zugriff auf Daten haben muss, ist anerkannt.
- dass ein solches Strafverfolgungsinteresse dazu führen kann, dass die Geheimnisträgerin (die Stadt Zürich bzw. eine ihrer Organisationseinheiten) das Geheimnis nicht durchsetzen kann, ist ebenfalls anerkannt.
- die Stadt Zürich als Geheimnisträgerin muss nicht zu 100% vor solchen Durchbrechungen ihres Geheimnisbereichs schützen (Rz. 133 und Rz. 34).

144 Die Problemstellung für Zugriffe von Behörden im Ausland nach ausländischem Recht könnte somit gleich betrachtet werden, wie wenn der Zugriff von einer inländischen Behörde ausginge (dazu vorn, Rz. 124 ff.). Diese Art der Betrachtung ist jedoch in der Lehre und der öffentlichen Diskussion nicht mehrheitsfähig; denn es besteht ein formaler und womöglich fundamentaler Unterschied zum inländischen Behördenzugriff: Der Unterschied – der im Folgenden noch genauer auszuleuchten sein wird – besteht darin, dass der aus Sicht des Rechts im Ausland rechtmässige Zugriff einer ausländischen Behörde für Strafverfolgungszwecke (hernach im Einklang mit anderen Lehrmeinungen als ***lawful access***[110] bezeichnet) keinen Rechtfertigungsgrund nach Art. 14 StGB darstellen kann[111] (für die Schweiz: Rz. 138). Dies gilt ungeachtet dessen, dass eine zuständige Behörde wirksamen Zwang gegen die Geheimnisträgerin anwendet.

[110] Hier wird als *lawful access* nur das Szenario bezeichnet, dass eine nach ausländischem Recht kompetente Strafverfolgungsbehörde die in einem abgegrenzten Deliktskatalog bezeichneten Strafverfolgungsinteressen hat und zu deren Durchsetzung auf Informationen angewiesen ist, die in Daten der Stadt Zürich gespeichert sind. Mit «Daten der Stadt Zürich» sind jene gemeint, welche die Stadt Zürich in die IT-Infrastrukturen der Cloud-Anbieterin lädt; es kann sein, dass es sich aus Sicht der Stadt Zürich dabei um Daten unter Dritteinfluss handelt, z.B. weil die Stadt Zürich wegen bestehender Personenbezüge das IDG einzuhalten hat. Ergänzend ist anzumerken, dass hier nur das folgende Szenario zu betrachten ist: Die «Daten der Stadt Zürich» sind in einer IT-Infrastruktur einer Cloud-Anbieterin gespeichert und die Strafverfolgungsbehörde gelangt an die Cloud-Anbieterin mit der Aufforderung auf «Herausgabe» der Daten. Was «Herausgabe» bedeutet, ist ebenfalls zu schärfen. Somit ist insgesamt der Begriff *lawful access* zu schärfen. Massgeblich hierfür ist, dass eine Offenbarungshandlung erst vorliegt, wenn ein Mensch Klartextzugriff erhält. Es können – wie noch zu zeigen sein wird – in den Abläufen des *lawful access* mannigfache Zwischenstufen vorkommen, bei denen man bereits von *lawful access* sprechen kann, bei denen aber noch keine unbefugte Dritte Klartextzugriff auf geschützte Informationen erhalten hat. Beispiel: Eine US-Behörde gelangt an die Cloud-Anbieterin «der Stadt Zürich» und verlangt von ihr im Sinne einer Sofortmassnahme, den aktuellen Datenbestand zu sichern («Snapshot»). Anschliessend veranlasst die Behörde das eigentliche Herausgabeverfahren. Es hat in diesem Zeitpunkt noch keine unbefugte Dritte Klartextzugriff erhalten. Siehe zur entsprechenden Diskussion für das schweizerische Recht Rz. 133 ff und FN 105.

[111] KURT SEELMANN, Basler Kommentar zum StGB, Art. 14 N 4, wonach nur eidgenössische oder kantonale Rechtssätze in Frage kommen.

145 Wenn und soweit nun im Rahmen von *lawful access* ein *Klartextzugriff tatsächlich stattfindet* (erst die Offenbarung ist relevant, Rz. 127), stellt sich abermals die Frage, ob die inländische Cloud-Kundin (die Stadt Zürich) mit einem solchen realistischerweise rechnen musste. Wenn ja (so wird gesagt[112]) könnte die Behörde mehr als nur bewusst fahrlässig sein – sie könnte den Klartextzugriff wissentlich in Kauf genommen haben, wie sie die Migration ihrer Daten in die ausländische Cloud veranlasst hat. Bildlich und verkürzt: Die Stadt Zürich stünde nach dieser Sicht somit stets «mit einem Bein im Gefängnis».

146 Bereits hier sei hingewiesen auf die folgende Unstimmigkeit: Sobald die ausländische Behörde jedoch über den bestehenden Rechtshilfeweg denselben Zugriffsanspruch in der Schweiz durchsetzt, steht der Rechtfertigungsgrund nach Art. 14 StGB der Stadt Zürich wieder offen. Faktisch ist dasselbe «passiert» wie im Szenario ohne den Rechtshilfeweg (*lawful access*), und doch soll nach Auffassung Vieler die Rechtslage anders beurteilt werden – was zeigt, wie zufällig die Resultate nach jener Auffassung sein sollen.

2. Verortung der Aufgabenstellung: Strafverfolgung im internationalen Kontext

a. Der CLOUD Act löst eine Diskussion aus, die EU-Kommission greift sie auf

(i) CLOUD Act

147 Die Problematik hat sich seit Erlass des US Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in der öffentlichen Wahrnehmung verschärft. Nach dem CLOUD Act kann eine US-Behörde mit einem richterlichen Beschluss direkt beim US Service Provider die Daten herausverlangen – auch wenn diese aus Sicht der USA im Ausland (also z.B. in der Schweiz) gespeichert werden.[113] *Die US-amerikanische Strafverfolgungsbehörde geht dabei einseitig vor*. Eines Rechtshilfegesuchs bedarf es nicht bzw. die Behörde beschränkt sich darauf, die Cloud-Anbieterin (resp. deren Konzerngesellschaft in den USA) anzugehen.

148 Die Behörden des «ausliefernden Staats» (hier: jene der Schweiz), welche ansonsten in ein Rechtshilfeverfahren zu involvieren wären, werden übergangen. Entsprechend sehen Viele im CLOUD Act einen Grund, dass US-amerikanische Cloud-Anbieter nicht von Organisationen in der Schweiz eingesetzt werden dürften – und schon gar nicht von einer schweizerischen Behörde. Wenn diese Auffassung zuträfe, wäre die Stadt Zürich deutlich eingeschränkt, Cloud-Anbieterinnen aus den USA (oder aus anderen Rechtsordnungen mit entsprechender Gesetzgebung oder Rechtsordnungen), für welche sich ein Zugriff auf Daten durch Strafverfolgungsbehörden nicht vollkommen abwenden lässt, einzusetzen.

(ii) Auslöser des CLOUD Act

149 Auslöser des CLOUD Act war das Verfahren United States v. Microsoft Corporation[114] In diesem wurde die Zulässigkeit von unilateral erlassenen und mit Sanktionsdrohungen erzwingbaren Beibringungsanordnungen[115] verhandelt. Konkret ging es im betreffenden Verfahren um einen im Jahr 2013 gegen Microsoft in den USA ausgestellten *warrant* nach 18 U.S. Code § 2703(a) des Stored Communications Act (SCA).[116]

[112] Vgl. SwissBanking, Cloud-Leitfaden: Wegweiser für sicheres Cloud Banking, Juni 2020, 2. Aufl., S. 37 f., abrufbar unter: https://www.swissbanking.ch/_Resources/Persistent/7/3/0/c/730c70284521c90f1fddad9ffb3e67b4164bef0e/SBVg_Cloud-Leitfaden_2020_DE.pdf (angesehen am 4. September 2021); vgl. auch CHRISTIAN SCHWARZENEGGER/FLORENT THOUVENIN/BURKHARD STILLER, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Zürich 2019, S. 56.

[113] Es lohnt sich, auf die massgeblichen Regeln des US-Rechts vertiefend einzugehen, um Verständnis zu schaffen und die Ausführungen dieses Rechtsgutachtens in einen Kontext zu setzen, für einen weiteren Kontext siehe auch Rz. 174 ff.

[114] Supreme Court: United States, Petitioner v. Microsoft Corporation, S. Ct. 17-2 (Entscheid vom 21. Mai 2018); Vorinstanz: Microsoft v. United States, No. 14-2985 (2d Cir.; 14. Juli 2016); Vorinstanz United States District Court for the Southern District of New York.

[115] Beibringungsanordnungen nach dem Stored Communications Act sind seit jeher: *warrant*, *court order*, *subpoena*.

[116] § 2703(a) ist eine Bestimmung, die durch den CLOUD Act *nicht* angepasst wurde.

Zum Stored Communications Act: Der US Kongress hat den Stored Communications Act (SCA) im Jahr 1986 als Teil des Electronic Communications Privacy Act verabschiedet.[117] Um diese potenziellen Datenschutzverletzungen anzugehen, hält der SCA eine Reihe von Datenschutzbestimmungen bereit, die dem Vierten Zusatzartikel der US Bundesverfassung ähnlich sind und die Beziehung zwischen staatlichen Ermittlern und Dienstanbietern im Besitz von privaten Informationen von Nutzerinnen regeln.[118] Insbesondere schützt der SCA die Vertraulichkeit elektronischer Kommunikation, die Nutzerinnen ihren Diensteanbieterinnen (z.B. Cloud-Anbieterinnen) anvertrauen. So werden mit dem SCA beispielsweise die Möglichkeiten der US-Regierung beschränkt, Netzdienstanbieter zur Offenlegung von Informationen über ihre Kundinnen zu zwingen (so namentlich 18 U.S.C. § 2703). Der SCA verbietet es Netzwerkdienstanbieterinnen auch, freiwillig Informationen über ihre Kunden und Abonnenten an die US-Regierung weiterzugeben (18 U.S.C. § 2702). Ein Verstoss gegen diese Bestimmungen kann zu einer straf- oder zivilrechtlichen Haftung führen (18 U.S.C. §§ 2703(e), 2707(e)).

150 Microsoft wehrte sich gegen diesen *warrant*, weil die nachgesuchten Inhaltsdaten auf irischen Servern lagen und zunächst in die USA transferiert werden mussten. Festzuhalten ist, dass es sich um einen kostenlosen Einzel-Account eines Privatnutzers handelte[119], und nicht um einen Organisations-Account, wie er für die Stadt Zürich zur Anwendung käme. Unbestritten war, dass Microsoft zu der Beibringung dieser E-Mail-Daten faktisch in der Lage war. Microsoft bestritt aber, dass ein *warrant* ein dafür mögliches bzw. zulässiges Vehikel war. Die Frage musste nicht entschieden werden, da noch vor dem Entscheid der CLOUD Act in Kraft gesetzt wurde. Am 21. Mai 2018 schrieb der Supreme Court das Verfahren als durch Gesetz erledigt ab.

(iii) E-Evidence Verordnung

151 Der CLOUD Act mag zunächst der Auslöser der Aufregung gewesen sein (Rz. 147). Es geht dabei oft vergessen, dass auch die EU Regelungen einführen will, welche den Zugriff ihrer Strafverfolgungsbehörden auf Daten in Cloud-Infrastrukturen in der EU verändern werden. Und es zeigt sich: Auch die Europäische Kommission will, dass *europäische Strafverfolgungsbehörden einseitig vorgehen können* (siehe Texte im Kasten, Rz. 151 und Rz. 152).

E-Evidence Verordnung (Kommissionsentwurf): Im April 2018 (d.h. einen Monat nach Unterzeichnung des CLOUD Act) hat die Europäische Kommission einen Vorschlag für eine Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen[120] [im Folgenden E-Evidence-Verordnung] publiziert[121]. Kernpunkte des Vorschlags sind (1.) die Schaffung einer europäischen Vorlageanordnung, die es ermöglichen soll, elektronische

[117] *«The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address.»* Quon v. Arch Wireless Operating Co., 529 F. 3d 892, 900 (9th Cir. 2008), mit Folgeentscheid des US Supreme Courts in 130 S. Ct. 2619 (2010).

[118] *«[The SCA] creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information.»* Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1212 (2004).

[119] Im konkreten Fall ging es um [einen des Drogenhandels verdächtigten Mann], der E-Mails zum Austausch bzw. zur Abstimmung über Drogentransaktionen über ein [Webmail-Dienst mit Speicherung in Irland] versendet und empfangen hat. Die Behörden wollten den Inhalt der E-Mails sehen (konkret ging es um «sämtliche E-Mails» der beschuldigten Person).

[120] Gegenstand der E-Evidence Verordnung (Kommissionsentwurf) sollen sein: **Teilnehmerdaten** (zur Identifizierung der Nutzerin; gelten als «Nichtinhaltsdaten»), **Zugangsdaten** (Informationen, die gleichsam einen Steigbügel darstellen, auf deren Basis dann Teilnehmerdaten abgefragt werden können – z.B. die Aufzeichnung von Ereignissen in einem Server-Protokoll; zeitliche Angaben wie Beginn und Beendigung der Zugangssitzung der Nutzerin; die Bekanntgabe der IP-Adresse zur Identifizierung der Netzschnittstelle; gelten als «Nichtinhaltsdaten»), **Transaktionsdaten** (Kontakte, Aufenthaltsort der Nutzerin; gelten als «Nichtinhaltsdaten») sowie **Inhaltsdaten** (die eigentlichen von der Nutzerin veranlassten oder erhaltenen Informationen).

[121] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen; COM(2018) 225 final, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52018PC0225 (angesehen am 14. September 2021).

Beweismittel unmittelbar bei Diensteanbietern, die in der EU Dienstleistungen anbieten, anzufordern[122]; (2.) die Verhinderung von Datenlöschungen durch eine Europäische Datenspeicherungsanordnung, (3.) die Pflicht zur Benennung eines gesetzlichen Vertreters in der EU und (4.) die Erhöhung der Rechtssicherheit für Unternehmen und Diensteanbieter.[123]

152 Der Verordnungsentwurf wurde u.a. von der Bundesrechtsanwaltskammer in Deutschland stark kritisiert.[124] Im Dezember 2020 hat der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments einen Bericht über den Vorschlag der Kommission verabschiedet und dabei Änderungen am Entwurf vorgeschlagen.[125] Diese zeigen, dass in Europa noch nicht geklärt ist, ob echte Extraterritorialität begründet werden soll (wie nach dem CLOUD Act) oder ob sich diese nur zu Lasten anderer Mitgliedstaaten auswirken soll. Es wird damit gerechnet, dass sich erste Klärungen bis Ende 2021 ergeben.

E-Evidence Verordnung (nach Anpassungen im Europäischen Parlament): Die Anpassungen im Europäischen Parlament waren substanziell. So wurde der Anwendungsbereich der E-Evidence Verordnung auf das Territorium der EU beschränkt und somit die von der EU-Kommission noch vorgesehene extraterritoriale Wirkung aufgehoben. Zudem wurden andere Datenkategorien vorgeschlagen.

(Nachweise zum Text im Kasten (Seite 35): Eliminierung der Extra-Territorialität[126] und andere Datenkategorien[127])

b. Zur Bedeutung des Territorialitätsprinzips in der internationalen Strafverfolgung

153 Wenn in Rz. 136 davon die Rede ist, dass der ausliefernde Staat übergegangen wird, impliziert dies zugleich, dass der ausliefernde Staat die Erwartungshaltung hätte, «mitreden» zu können. Diese Erwartungshaltung kommt mit dem Grundsatz des Territorialitätsprinzips zum Ausdruck.

154 Das Territorialitätsprinzip ist traditionell vorherrschende Meinung. Als Alternativen zum Territorialitätsprinzip sind das Marktortprinzip (bei dem die Regeln des Ziellandes, auf welches ein Angebot gerichtet ist, Anwendung finden) das Ursprungslandprinzip (bei dem die Regeln des Landes, in welchem das zur Datenherausgabe aufgeforderte Unternehmen seinen Sitz hat, Anwendung finden), das Bestimmungslandprinzip (bei dem die Regeln des Landes, in dem der Beschuldigte seinen Wohnsitz oder Sitz hat,

[122] Art. 1 des Kommissionsentwurfs lautet wie folgt: «Mit dieser Verordnung werden die Regeln festgelegt, nach denen eine Behörde eines Mitgliedstaats von einem **Diensteanbieter, der in der Union Dienstleistungen anbietet**, verlangen kann, elektronische Beweismittel herauszugeben oder zu sichern, unabhängig davon, wo sich die Daten befinden. Diese Verordnung berührt nicht die Befugnisse der nationalen Behörden, Diensteanbieter, die in dem betreffenden Hoheitsgebiet niedergelassen oder vertreten sind, zur Einhaltung ähnlicher nationaler Maßnahmen zu verpflichten.» (Hervorhebungen nicht im Original).

[123] Pressemitteilung der Europäischen Kommission vom 17. April 2018, abrufbar unter https://ec.europa.eu/commission/presscorner/detail/de/IP_18_3343.

[124] Stellungnahme Nr. 28/2018 der Bundesrechtsanwaltskammer zum Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, abrufbar unter: https://www.brak.de/zur-rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2018/september/stellungnahme-der-brak-2018-28.pdf (angesehen am 11. August 2021).

[125] Bericht vom 11. Dezember 2020 über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM(2018)0225 – C8-0155/2018 – 2018/0108(COD)), abrufbar unter: https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_DE.html (angesehen am 11. August 2021).

[126] Art. 1 Abs. 1 der E-Evidence Verordnung soll nach den Anpassungen im Europäischen Parlament soll wie folgt lauten: «Mit dieser Verordnung werden die Regeln festgelegt, nach denen eine Behörde eines Mitgliedstaats im Rahmen eines Strafverfahrens von einem **Diensteanbieter, der in der Union Dienstleistungen anbietet und der in einem anderen Mitgliedstaat niedergelassen ist oder – falls er dort nicht niedergelassen ist – rechtlich vertreten ist**, verlangen kann, elektronische Informationen, die als Beweismittel dienen können, herauszugeben oder zu sichern, unabhängig davon, wo sich die Daten befinden.» (Hervorhebungen nicht im Original).

[127] Gegenstand der E-Evidence Verordnung (Anpassungen im Europäischen Parlament) sollen sein: **Teilnehmerdaten** (zur Identifizierung der Nutzerin); **Verkehrsdaten** (Kontakte, Aufenthaltsort der Nutzerin); **IP-Adressen** (gemäss den im Europäischen Parlament eingeführten Erwägungsgrund 22a soll Folgendes gelten: «[IP-Adressen] können […] unter bestimmten Umständen als Verkehrsdaten gelten. … [Wenn eine IP-Adresse gleichsam der Steigbügel ist, um Teilnehmerdaten abzufragen] sollte die gleiche Regelung wie für Teilnehmerdaten im Sinne dieser Verordnung angewandt werden»), **Metadaten** (gemäss dem im Europäischen Parlament eingeführten Erwägungsgrund 22b: «Es ist daher unerlässlich, dass Metadaten anderer elektronischer Kommunikationsdienste oder -protokolle, die durch die Nutzung der betreffenden Dienste oder von den Diensteanbietern gespeichert, übermittelt, verbreitet oder ausgetauscht werden, als Inhaltsdaten zu betrachten sind.») sowie **Inhaltsdaten**.

Anwendung finden) und das Personalitätsprinzip (bei dem die Regeln des Landes, dessen Staatsbürger der Beschuldigte ist, Anwendung finden) zu nennen.[128]

155 Es gibt verschiedene internationale Vereinbarungen mit Vorgaben dazu, wie einzelne Staaten untereinander einen Ausgleich zu finden versuchen zwischen den verschiedenen möglichen Positionierungen, die einzelne Staaten in der Frage der internationalen Strafverfolgung einnehmen.

(i) Der Zusammenhang zum Strafrechtsmonopol des Staats

156 Der Staat hält das Strafrechtsmonopol. Es handelt sich um eine der bedeutendsten Errungenschaften unserer zivilisierten Gesellschaft. Das Strafrechtsmonopol hat zum Inhalt, dass nicht nur das Bestrafen, sondern auch das Untersuchen von Straftaten als Aufgaben des Staats gelten. Die Strafuntersuchung dient der Sammlung jener Informationen, die zur Meinungsbildung im Strafverfahren massgeblich sind. Dass die Bestrafung die Persönlichkeitsrechte jeder Einzelnen tangiert, liegt auf der Hand. Und ebenso verhält es sich mit den Informationen, die während einer Strafuntersuchung erhoben werden. Vom Recht, sich selbst nicht belasten zu müssen bis hin zum Aussageverweigerungsrecht: Die Strafrechtsdoktrin hat eine lange Tradition an Grundsätzen aufgebaut, um die Macht des Staats nicht überborden zu lassen. Und es gibt sehr gute Gründe dafür, den Staat an dieser Stelle zurückzubinden.[129]

157 Diese Anmerkung ist wichtig, um zu verstehen, dass der CLOUD Act ein sehr wichtiges Thema betrifft. Sie erklärt auch die Intensität der Diskussion. Und sie erklärt, warum das Thema rechtspolitisch wichtig ist. Die folgenden Ausführungen zeigen aber, dass das Thema für den Entscheid der Stadt Zürich nicht relevant ist.

(ii) Zum Territorialitätsprinzip als Garantieverantwortung

158 Das Territorialitätsprinzip kann funktional durchaus so betrachtet werden, dass der Staat, auf dessen Gebiet Daten «belegen» sind (ausliefernder Staat), eine Form von Garantieverantwortung ausübt (und zwar als demokratische, rechtsstaatliche und grund- bzw. datenschutzrechtliche Garantieverantwortung[130]). Dahinter steht die folgende Idee: Der Staat ist kein Selbstzweck (vorn Rz. 27). Im Rahmen der Verfassung wurden die Bedingungen ausgehandelt, unter denen der Staat für die Gesellschaft tätig werden darf und Zuständigkeiten zwischen mehreren Staaten werden *faute de mieux* traditionell über das Territorium abgegrenzt. Daraus kann sich eine gewisse Erwartungshaltung ergeben (wiederum spielt das Vertrauensprinzip), dass der Staat die ausgehandelten Prinzipien zur Anwendung bringt. Hier geht es um den Zugang zum Recht bzw. die sog. Rechtsweggarantie (z.B. Art. 29a Bundesverfassung). Die so verstandene Garantieverantwortung hat im hier interessierenden Kontext die Funktion, Datentransfers aus dem Inland heraus für die Zwecke der Strafverfolgung andernorts nicht blindlings geschehen zu lassen. Diese Garantieverantwortung führt dazu, dass beschuldigte Personen eher von den ihnen zuerkannten Rechten (gemäss innerstaatlichem Recht) profitieren können sollen.[131]

159 Für die Zwecke des vorliegenden Rechtsgutachtens ist dieser Kontext von Bedeutung. Dies gilt allerdings *nur unter Vorbehalten*, die freilich in der Diskussion bislang stets ausgeblendet wurden. Es geht um die Vorbehalte, dass die so definierte Garantieverantwortung, *erstens*, überhaupt **Anwendung** findet (es geht um die Bedeutung des Territorialitätsprinzips im Sinne der berechtigten Erwartungen), *zweitens*, dass die Garantieverantwortung **tangiert** ist (es geht um die Frage, ob die Garantieverantwortung das, was diskutiert wird – Behördenzugriffe im Ausland – überhaupt regeln will) und sodann, *drittens*, ob die Garantieverantwortung **verletzt** ist, wenn man die Abläufe im Ausland betrachtet (führen die

[128] CHRISTOPH BURCHARD, Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 2, in: Zeitschrift für Internationale Strafrechtsdogmatik 2018, S. 249 ff., S. 254; siehe auch VINEETH NARAYANAN, Harnessing the Cloud: International Law Implications of Cloud-Computing, in: Chicago Journal of International Law, 12(2) (2012), S. 783 ff., S. 790 ff.

[129] So bereits ERNST HAFTER, Lehrbuch des Schweizerischen Strafrechts: Allgemeiner Teil, Berlin 1926, S. 4 ff.

[130] BURCHARD, FN 128, S. 263.

[131] BURCHARD, FN 128, S. 251.

Behördenzugriffe im Ausland bei materieller Betrachtung zu einer Beeinträchtigung der Rechtsstellung der betroffenen Person, die sich mit der Rechtsweggarantie nach Art. 29a Bundesverfassung nicht vereinbaren liessen). Bejaht man diese Vorstufen, geht es, *viertens*, um die Frage, in wessen **Zuständigkeit** das Handeln gemäss der Garantieverantwortung fällt und, *fünftens*, im Sinne eines Exkurses, ob Wege möglich sind, die Garantieverantwortung gleichwohl **umzusetzen** (und welche Massnahmen dazu in Frage kämen).

160 Die in Rz. 159 angedeuteten Vorbehalte sind an dieser Stelle nicht zu vertiefen, könnten aber in anschliessenden Rechtsgutachten aufgegriffen werden, wenn andere Rechtsordnungen als die USA im Fokus stehen sollten. Hier ist nur zum dritten Punkt (zur Verletzung, Rz. 161) und zum vierten Punkt (zur Zuständigkeit, Rz. 162) kurz Ergänzendes zu äussern.

161 Zur Frage, ob die Garantieverantwortung verletzt ist, wenn die Stadt Zürich ein Cloud-Angebot mit US-Bezügen nutzt:

- Auch wenn die betroffene Person berechtigten Anlass zur Erwartung hat, dass ihre Angaben von der schweizerischen Rechtsordnung erfasst sind, muss erst die Frage geprüft werden, ob die Rechtsweggarantie verletzt wäre, wenn die Daten im ausländischen Verfahren offenbart würden.
- Die Rechtsweggarantie ist nicht verletzt, wenn im Fall eines allfälligen Klartextzugriffs auf Informationen im Ausland im dortigen Verfahren ein Schutzniveau gilt, das im Resultat jenem in der Schweiz entspricht. Dies kann vollkommen abstrahiert – d.h. losgelöst von der betreffenden Rechtsordnung – nicht beantwortet werden. Wie in einem Exkurs aufgezeigt werden kann, wird die Stadt Zürich jedenfalls in den USA nicht mit einer Situation konfrontiert werden, in der die US-amerikanische Strafverfolgungsbehörde ohne Mitwirkung der Stadt Zürich auf Daten im Tenant der Stadt Zürich zugreifen wird (wie sich aus den Ausführungen in Rz. 174 ff. ergibt). Soweit es um die Bedeutung des CLOUD Act geht, kann die Frage, ob die USA über ein zu wenig ausgereiftes Justizsystem verfügen, somit offengelassen werden. Es kann aber angemerkt werden, dass die Gutachter es für überaus unwahrscheinlich halten, dass dem Justizwesen in den USA für die vorliegende Diskussion relevante Mängel nachgewiesen werden könnten. Immerhin verfügen die USA über ein Justizwesen von jahrhundertealter Tradition, das historisch auch für die Schweiz durchaus eine Vorbildwirkung entfaltet hat.
- Die Garantieverantwortung nimmt auch in keiner Weise vorweg, dass man die Lösung des CLOUD Act rundweg abzulehnen hätte. Die Garantieverantwortung hatte ihren «Auftritt» bislang jeweils dann, wenn der ausländische Staat den Weg der Rechtshilfe beschritten hat (dass dieses Verfahren aus einer Risikobetrachtung zu besseren Resultaten führt, als das US-amerikanische Rechtssystem einen Schutz bereitstellt, kann nicht a priori gesagt werden).[132] Die Garantieverantwortung kann jedenfalls auch dann ordnungsgemäss umgesetzt sein, wenn die Herausgabe von Beweismitteln mit Belegenheitsort im Ausland an Private – nämlich die Cloud-Anbieterinnen mit Sitz oder Hauptsitz in den USA – delegiert wird.[133] Die Praxis der Cloud-Anbieterinnen, wie sie mit Strafbehörden ausserhalb der Schweiz kooperieren, kann z.B. einer Form von demokratisch legitimierter Kontrolle unterworfen werden. Wo eine solche fehlt, kann die tatsächliche Praxis der gewählten Cloud-Anbieterin gewürdigt werden. Somit kann aufgezeigt werden, dass die Existenz eines CLOUD Act per se nicht bedeutet, dass schweizerisches Recht verletzt ist.

162 Gewichtiger wirkt am Ende die formale Überlegung, dass es nicht Sache der Stadt Zürich ist, die Garantieverantwortung auszuüben:

[132] Es wäre eine gesonderte Untersuchung wert, um zu beschreiben, wie die Eidgenossenschaft ihre Garantieverantwortung im Rahmen von Rechtshilfeersuchen in Strafsachen wahrnimmt. Dies könnte in einer separaten Untersuchung mit Gewinn vertieft werden, um in rechtstatsächlicher Hinsicht aufzuzeigen, inwiefern sich materiell ein Unterschied auftut, wenn künftig Rechtshilfetätigkeiten an Private (d.h. Cloud-Anbieterinnen) delegiert werden. Im Übrigen ist aber darauf hinzuweisen, dass im Rahmen einer Risikoanalyse a priori keine Aussagen gemacht werden können, dass das Rechtshilfeverfahren zu besseren Resultaten führt als das US-amerikanische Verfahrensrecht, wie es tatsächlich von jenem US-amerikanischen Gericht angewendet wird, wenn die Stadt Zürich sich direkt mit einem US-amerikanischen Gericht konfrontiert sieht.

[133] Man kann hier durchaus von einer Form der Privatisierung sprechen, wie es Burchard tut (BURCHARD, FN 128, S. 259 ff.).

- Wenn zu beantworten ist, ob die Stadt Zürich (oder eine andere Cloud-Kundin) ein Cloud-Angebot nutzen darf, das unilateralen *lawful access* im Ausland erst ermöglicht, ist dies im Lichte dieser Garantieverantwortung der Eidgenossenschaft (Art. 29a Bundesverfassung) zu beantworten.
- Es geht mit der so geschärften Fragestellung also darum, ob die Stadt Zürich die Garantieverantwortung der Eidgenossenschaft (zu Lasten der beschuldigten Person) vereitelt, wenn sie ein Cloud-Angebot mit einem derartigen Auslandsbezug einsetzt. Der Hinweis darauf, dass es sich um eine Problematik handelt, mit der sich die Eidgenossenschaft konfrontiert sieht, legt wiederum die folgende Frage nahe: Ist es Aufgabe der Stadt Zürich, das Problem der Eidgenossenschaft zu lösen? Die Frage stellen heisst, sie zu beantworten: Nein. Es geht nur um die Frage, ob die Stadt Zürich in rechtsverletzender Weise die Garantieverantwortung der Eidgenossenschaft vereitelt. Dies kann verneint werden, was sich aus der Analyse ab Rz. 174 ff. ergibt; denn es wird im Resultat jeweils zu einem direkten Einbezug der stadtzürcherischen Stellen kommen, wenn sich ein Anwendungsfall unter dem CLOUD Act ergeben sollte. In einem solchen Fall kann die Stadt Zürich sicherstellen, dass die Eidgenossenschaft ihre Garantieverantwortung wahrnehmen kann. Jedenfalls wird die Stadt Zürich durch geeignetes Vorgehen sicherstellen, dass sie Strafbarkeit nach Art. 271 StGB im Fall einer an sie gerichteten Anfrage abwenden kann. Eine Rechtsverletzung kann somit systematisch ausgeschlossen werden.

163 Zusammenfassend ist nicht ersichtlich, wie die Stadt Zürich das auf sie anwendbare Recht verletzen würde, wenn eine Auswirkung des CLOUD Act auf Daten im Tenant der Stadt Zürich nicht ausgeschlossen werden kann.

c. Zum rechtspolitischen Schutzinteresse

164 Nachdem die Fragestellung, die der Erlass des CLOUD Act effektiv losgetreten hat, wie in Rz. 159 ff. beschrieben geschärft wurde, wird Folgendes klar: Der CLOUD Act hat mit dem Amtsgeheimnis weniger zu tun als mit der Garantieverantwortung der Schweizerischen Eidgenossenschaft.

165 Die beiden rechtspolitischen Ziele verfolgen auch unterschiedliche Schutzinteressen und haben unterschiedliche Schutzsubjekte:

- Das Amtsgeheimnis will das Vertrauen in die Stadt Zürich als voraussehbar handelnde Akteurin schützen (dazu vorn, Rz. 27).
- Die Garantieverantwortung will das vom Staat verfolgte Individuum (die beschuldigte Person[134]) schützen, wie es sich die Eidgenossenschaft mit Art. 29a BV aufgegeben hat.

d. Die Analyse hat sich auf die Prüfung von Verbotstatbeständen zu beschränken

166 Damit kann und sollte der Blick für dieses Rechtsgutachten zurückgelenkt werden auf das Wesentliche: Es muss nicht der Frage nachgehen, wie Beschuldigtenrechte am besten zu wahren sind. Obwohl dies eine gesellschaftlich und rechtsstaatlich eminent wichtige Fragestellung ist (Rz. 157), ist doch festzu-

[134] Es fällt auf, dass die USA sich ihrerseits stärker aus dieser Garantieverantwortung zurückgezogen haben und die Frage, ob eine Cloud-Anbieterin einer Strafverfolgungsbehörde im Ausland (z.B. eine schweizerische Strafverfolgungsbehörde) Angaben machen darf, bereits vor Erlass des CLOUD Act an die Cloud-Anbieterin (Anbieterin eines Communication Services) delegiert hatten. Dies ergibt sich aus § 2702(a)(3), mit der Überschrift „voluntary disclosure of customer communications or records". Es geht um Nicht-Inhaltsdaten, und somit um **Bestandsdaten** (Rz. 124) bzw. **Teilnehmerdaten** (FN 120 und FN 127) zur Identifizierung der Nutzerin, **Zugangsdaten** (Server-Protokoll; zeitliche Angaben; siehe FN 120 und FN 127, bzw. **Randdaten** wie in Rz. 124 genannt) unter Einschluss von **IP-Adresse** (FN 127) und **Metadaten** (FN 127), **Verkehrsdaten** bzw. **Transaktionsdaten** (Kontakte, Aufenthaltsort der Nutzerin; siehe FN 120 und FN 127; zu Verkehrsdaten siehe auch Rz. 124). Diese Rechtslage ergibt sich daraus, dass das US-Recht die Offenlegung solcher Informationen nur an eine *government entity* verbietet. Dieser Begriff ist in 18 U.S.C. § 2711(4) wie folgt definiert, und meint demnach nur US-amerikanische Behörden: A «governmental entity' means a department or agency of the United States or any State or political subdivision thereof.» (siehe dazu das Whitepaper des US Department of Justice «Sharing Cyberthreat Information Under 18 USC § 2702(a)(3)», abrufbar unter: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/03/26/guidance-for-ecpa-issue-5-9-2014.pdf, angesehen am 11. August 2021). Diese Regel erklärt sich daraus, dass der Supreme Court im Jahr 1976 seinen Entscheid i.S. United States v. Miller gefällt hat (United States v. Miller, 425 U.S. 435 1976) – es geht da um Schutz in den USA unter dem Vierten Verfassungszusatz, der vor übermässigen Zugriffen der US Behörden schützt. Ergänzend hat der CLOUD Act geklärt, dass die Offenlegung an eine ausländische Behörde, dessen Staat ein sog. Executive Agreement mit den USA geschlossen hat, rechtmässig ist (§ 2702(c)(9) für «records or other information pertaining to a subscriber or customer» und § 2702(b)(9)) für «contents of communication»).

halten: **Diese Thematik ist für die Frage, ob die Stadt Zürich ein Cloud-Angebot nutzen darf, nicht massgeblich.**

167 Es geht hier einzig darum, ob die Stadt Zürich wegen allfälliger Behördenzugriffe aus dem Ausland das Amtsgeheimnis verletzt (Nein[135]), und ob die Stadt Zürich[136] geltendes Recht (wie z.B. Art. 271 oder Art. 273 StGB) verletzt, wenn sie Daten in IT-Infrastrukturen einer Cloud-Anbieterin auslagert (Nein[137]). Da generell auch keine anderen Rechtsverletzungen ersichtlich sind, gibt es auch keinen anderen Grund, auf Widerrechtlichkeit zu schliessen, insbesondere: (i) Die Stadt Zürich kann auch nach Auslagerung von Daten in ein Cloud-Angebot bzw. mit Nutzung eines Cloud-Angebots ihre Funktion als nicht bevormundender bzw. immer noch vertrauenswürdiger und willkürfrei handelnder Staat ausüben; (ii) die Stadt Zürich stellt aufgrund des Umstands, dass sie Cloud-Angebote nutzt, auch keine Gefahr für jene dar, die mit der Stadt Zürich interagieren (die Stadt Zürich muss aber Schutzmassnahmen treffen, Rz. 94); dies gilt «sogar» bei US-Bezug (Rz. 183 ff.); (iii) und es ist auch nicht so, dass die Stadt Zürich die Garantieverantwortung der Eidgenossenschaft vereitelt, wenn sie eine Lösung benutzt, die auf dem Territorium der Schweiz rechtmässig angeboten wird[138], die womöglich aber trotzdem in der Rechtsfolge resultiert, dass die Garantieverantwortung der Schweiz nicht wie bisher durchgesetzt werden kann (vorn, Rz. 162).

e. Everybody gets Everybody's Data

168 Im Rahmen des über mehrere Instanzen hinweg ausgetragenen Gerichtsverfahrens zwischen dem US-amerikanischen Staat und Microsoft, das dann zuletzt Anlass gegeben hat zum Erlass des CLOUD Act, hat der oberste Leiter des Rechtsdiensts als Argument gegen den CLOUD Act und v.a. die von den US-Behörden vertretene Auffassung, ob ein sog. *warrant* auch mit Wirkung ins Ausland ausgesprochen werden könne, die folgende Aussage gemacht:

> *«If every country asserts extraterritorial jurisdiction […] then everybody gets everybody's data.»*

169 Der Satz klingt wie ein Horrorszenario. Und es gibt Gründe, warum man dieses Horrorszenario für die Zukunft als Gesellschaft nicht will. Und doch ist die Aussage problematisch; denn sie verschweigt einen wichtigen Aspekt: Diesen Zustand gibt es im Wesentlichen bereits heute. Ein Rechtshilfeverfahren resultiert oft in einer Auslieferung von Daten (so die berufliche Erfahrung des Verfassers). Mit anderen Worten: Die angeblich kontrollierende Rolle des ausliefernden Staats führt in einer der überwiegend grossen Mehrheit aller im Rechtshilfeverfahren beantragten Fälle nicht zu einer Zurückhaltung von Daten, sondern in deren Preisgabe (Auslieferung, dazu vorn, Rz. 146).

f. Zur Abgrenzung: Worum es nicht geht

170 Die USA sind bekannt für Strafverfolgungsmassnahmen und Verfahren, die wenig transparent sind. Die Praktiken unter dem US-amerikanischen Foreign Intelligence Surveillance Act (FISA) genügen den Anforderungen der europäischen Staaten bzw. ihrem Verfassungsrecht nicht, was der Europäische

[135] Dazu unten, Rz. 215.

[136] Es ist nicht ausgeschlossen, dass die gewählte Cloud-Anbieterin – wenn sie das Cloud-Angebot mit Datenstandort Schweiz betreibt – im Fall eines Direktbegehrens an sie (ausgehend von einer Behörde, betreffend Auslagerung von Daten ins Ausland) Recht verletzt. Das muss aber nicht die Sorge der Stadt Zürich sein (kann aber umgekehrt ein Kriterium sein, das den Schutz der Daten der Stadt Zürich faktisch verbessert).

[137] In Bezug auf Ar. 273 StGB steht das Tatbestandsmerkmal des «Zugänglichmachen» zur Diskussion, das deckungsgleich ist zum Begriff der Offenbarung. Die Analyse verläuft somit gleich wie nach Art. 320 bzw. Art. 293 StGB. In Bezug auf Art. 271 StGB geht es um das "Betreiben von politischem Nachrichtendienst" oder um das Vorschubleisten davon. Eine Strafbarkeit vor Aufforderung durch eine ausländische Behörde ist nicht denkbar, weswegen das blosse Auslagern von Daten in eine Cloud-Umgebung nicht nach Art. 271 StGB strafbar sein kann.

[138] Organisationseinheiten müssen sich jeweils auch gewahr werden, dass sie mit Art. 2 der Kantonsverfassung («Grundlage und Schranke staatlichen Handelns ist das Recht.») das Recht von Privaten (z.B. Cloud-Anbieterinnen mit rechtmässigen Angeboten) verletzen, wenn sie einem Angebot die Rechtmässigkeit absprechen, ohne dass hierzu eine gesetzliche Grundlage bestehen würde. Das Zurückbinden der Rechte einer Marktteilnehmerin unter Hinweis auf eine zu weit verstandene Garantieverantwortung ist gleichermassen rechtswidrig wie das vollständige Nichtausüben der Garantieverantwortung (zur Garantieverantwortung vorn, Rz. 158).

Gerichtshof in der Rechtssache Schrems II[139] festgehalten hat. Das zur Kontrolle eingesetzte Privacy and Civil Liberties Oversight Board (PCLOB) hat die mit dem Executive Order 12333[140] ermöglichten geheimdienstlichen Aktivitäten in den USA geprüft und diese zwar als bedenkenlos eingestuft. Aber der Bericht aus dem Jahr 2021 wurde erstmals nicht mehr von allen Mitgliedern des PCLOB mitgetragen, was diese in zwei ergänzenden «Statements»[141] dargelegt haben.[142]

171 Die Kritik an der Geheimdiensttätigkeit in den USA könnte ausgebaut und vertieft werden. Dafür besteht hier aber kein Raum und auch kein Bedarf. Die Frage der Zugriffe durch Strafverfolgungsbehörden im Ausland auf Daten in der Schweiz ist deutlich zu trennen von der Frage, wie ausländische Staaten geheimdienstlich agieren. Darum geht es nicht. Namentlich hat der CLOUD Act mit geheimdienstlicher Tätigkeit in den USA nichts zu tun (sondern mit Anliegen von Strafverfolgungsbehörden).

172 Damit ist auch das Urteil Schrems II[143] nur insoweit relevant für die mit diesem Gutachten zu beantwortenden Fragestellungen, als es im Rahmen der Cloud-Nutzung zu Datenübermittlungen in die USA kommt. Soweit es zu solchen kommt, ist im Umsetzungsprojekt zu entscheiden, welche besonderen Schutzmassnahmen die Stadt Zürich "nach Schrems II" zu treffen hat.[144]

g. Zwischenfazit zum CLOUD Act: Kein Grund von der Cloud-Nutzung abzusehen

173 Daran anknüpfend bleibt die Feststellung, dass die Existenz des CLOUD Act und anderer Datenzugriffe ausländischer Strafverfolgungsbehörden bereits aus konzeptionellen Überlegungen keinen Hinderungsgrund für den Gang der Stadt Zürich «in die Cloud» darstellen. Gleichwohl sind ergänzende Ausführungen angebracht. Aber es kann an dieser Stelle nur noch um eine Darstellung des CLOUD Act im Sinne eines Exkurses gehen.

3. Der Blick auf die Abläufe in den USA (Exkurs)

174 An dieser Stelle kann ein kurzer Überblick darüber gegeben werden, wie ein sog. *lawful access* in den USA überhaupt umgesetzt würde. Dies ist zwar nur ein Exkurs und beschlägt nicht die nach schweizerischem Recht zu beurteilende Rechtsfrage. Aber die Erläuterungen mögen dem Verständnis dienen.

[139] EuGH, Urteil v. 16. Juli 2020, Rs. C-311/18 – Schrems II.

[140] PCLOB, Executive Order 12333, abrufbar unter: https://documents.pclob.gov/prod/Documents/OversightReport/b11b78e0-019f-44b9-ae4f-60e7eebe8173/12333%20Public%20Capstone.pdf (angesehen am: 12. August 2021).

[141] [PCLOB] Board Members Ed Felten and Travis LeBlanc's Statement on Executive Order 12333 Public Report vom 2. April 2021, abrufbar unter: https://documents.pclob.gov/prod/Documents/Projects/dab7d585-475b-446e-aad6-7cc18f9edeed/Felten%20and%20LeBlanc%20Statement%20on%20EO%2012333%20Public%20Report.pdf (angesehen am: 12. August 2021); siehe auch Additional Unclassified Statement by [PCLOB] Board Member Travis LeBlanc vom 12. März 2021, abrufbar unter: https://documents.pclob.gov/prod/Documents/Projects/4b4f65ff-0dba-444b-9c10-7e6b3fce407c/2021.06.28.Member%20LeBlanc%2012333%20Unclass%20Statement.pdf (angesehen am: 12. August 2021).

[142] Hierzu siehe namentlich Electronic Frontier Foundation (EFF), PCLOB «Book Report» Fails to Investigate or Tell the Public the Truth About Domestic Mass Surveillance vom 30. Juni 2021, abrufbar unter: https://www.eff.org/deeplinks/2021/06/pclob-book-report-fails-investigate-or-tell-public-truth-about-domestic-mass (angesehen am 11.August 2021). Der EFF-Blog ist generell lesenswert, um die Bedeutung der «FISA-Problematik» aus gesellschaftlicher und staatspolitischer bzw. rechtsstaatlicher Sicht einzuordnen, siehe z.B. EFF, The Problems With FISA, Secrecy, and Automatically Classified Information vom 26. Februar 2018, abrufbar unter: https://www.eff.org/deeplinks/2018/02/problems-fisa-secrecy-and-automatically-classified-information (angesehen am 11.August 2021).

[143] Hier ist auch nicht der Ort, das Schrems II-Urteil allgemein zu hinterfragen. Dass es den Privacy Shield aufgehoben hat, ist Tatsache. Darüber hinaus sollte es aber kritisch reflektiert werden (z.B. Anwendbarkeit für die Schweiz, Prozessgeschichte). Siehe hierzu CHRISTIAN LAUX, Überwachung als Superproblem unserer Zeit, 12. Oktober 2018, in: inside-it.ch, abrufbar unter: https://www.inside-channels.ch/de/post/lex-laux-ueberwachung-im-internet-das-superproblem-unserer-zeit-update-20181012 (angesehen am 11.August 2021). Diese kritische Reflektion kommt nach Auffassung der Verfasser in der öffentlichen Diskussion allerdings zu kurz.

[144] Die zu treffenden Massnahmen müssen in diesem Rechtsgutachten nicht vertieft werden. Darauf kann anknüpfend eingegangen werden, soweit dafür in einem Umsetzungsprojekt ein entsprechender Bedarf entsteht. In genereller Weise kann gesagt werden, dass erhöhte Schutzmassnahmen dann zu prüfen sind, wenn relevante Daten in die USA übermittelt werden. Sorgt die Stadt Zürich für Datenhaltung Schweiz und weiter dafür, dass die Cloud-Anbieterin keinen «incidental storage» in den USA erstellt, kann eine Relevanz der Schrems II-Rechtsprechung des EuGH von vornherein ausgeschlossen werden; denn Schrems II soll vor den Folgen von Bulk Review auf Kernfreiheiten schützen (Bulk Review in den USA setzt aber Daten in den USA voraus, die in einen solchen Bulk Review einbezogen werden könnten).

a. Grundlage

175 Grundlage bzw. Anknüpfungspunkt für die Betrachtung ist der Stored Communications Act (SCA) und die vorn, Rz. 149 dazu zusammengefasste Ausgangslage. Das US-amerikanische Justizdepartement hat dazu ein Manual verfasst, das ihren Beamten erklärt, wie sie vorzugehen haben. Es handelt sich um eine lesenswerte Ressource für alle, welche dem Thema näherkommen möchten, wobei man berücksichtigen muss, dass es sich um eine Schilderung aus Sicht der US-amerikanischen Strafverfolgungsbehörde von 2009 handelt.[145] Dabei ist jeweils der Fokus darauf zu legen, welche Rechtsposition die Stadt Zürich als sog. «Disinterested Third Party» einnehmen würde.[146] Das Manual stellt eine Zusammenfassung der Rechtslage in den USA dar. Obwohl das Manual von den Strafverfolgungsbehörden ausgeht, kann man für die Zwecke des vorliegenden Rechtsgutachtens darauf abstellen:

- wenn «sogar» die Strafverfolgungsbehörden (zu ihren Lasten) Beschränkungen anerkennen, ist dies ein Hinweis darauf, dass diese Beschränkungen von den Gerichten verbindlich durchgesetzt werden (was für das US-Recht bestätigt werden kann)
- es ist für die Zwecke des vorliegenden Rechtsgutachtens (mit Adressatenkreis in der Schweiz) nützlich, die Praktiken der Beweiserhebung im digitalen Umfeld in einem Dokument zusammengefasst zu sehen.

176 In den USA können die folgenden Informationen bei Cloud-Anbieterinnen erhoben werden[147]:

- Basic subscriber information, sessions, billing information
- Other transactional records and account records
- Retrieved Communications and Content of other stored files
- Unretrieved Communications (including email and voice mail)[148]

b. Schutz von Geheimnissen

177 Es ist Pflicht der Strafverfolgungsbehörden, Berufsgeheimnisse zu schützen (von Rechtsanwälten, von Ärzten etc.). Das US Justizministerium instruiert ihre Beamten, diese Geheimnisse zu schützen. Das US Justizministerium hat sodann die langstehende Praxis, mit solchen Dritten zusammenarbeiten, die Zugriff auf die nachgesuchten Informationen haben:

> *«When agents seize a computer that contains legally privileged files, a trustworthy third party must examine the computer to determine which files contain privileged material. After reviewing the files, the third party will offer those files that are not privileged to the prosecution team. Preferred practices for determining who will comb through the files vary widely among different courts. In general, however, there are three options. First, the court itself may review the files in camera. Second, the presiding judge may appoint a neutral third party known as a "special master" to the task of reviewing the files. Third, a team of prosecutors or agents who are not working on the case may form a "filter team" or "taint team" to help execute the search and review the files afterwards. The filter team sets up a so-called "ethical wall" between the evidence and the prosecution team, permitting only unprivileged files to pass over the wall.»*

178 Es zeigt sich damit, dass die US Gerichte einer "trustworthy third party" eine grosse Bedeutung zumessen und sie als Partnerin akzeptieren werden, um die Triage zu machen, welche Informationen bzw. Daten vor dem Zugriff der Strafverfolgungsbehörden zu schützen sind, weil sie nicht relevant sind oder dem Amtsgeheimnis unterstehen. Dass die Stadt Zürich eine solche "trustworthy thid party" sein kann,

[145] Computer Crime and Intellectual Property Section, U.S. Department of Justice, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (200), abrufbar unter: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf (angesehen am 12. August 2021). Siehe auch 42 U.S. Code § 2000aa-11(a) zu «Procedures to obtain documentary evidence; protection of certain privacy interests» sowie 28 C.F.R. § 59.4(b) zu «Provisions governing the use of search warrants which may intrude upon professional, confidential relationships».

[146] Dass die Stadt Zürich nicht als *Disinterested Third Party*, sondern als direkt betroffene Straftäterin im Fokus der US-amerikanischen Verfahren stünde, darf hier wohl ausgeklammert werden; siehe bereits vorn, Rz. 121.

[147] Zu den Angaben in der Schweiz siehe Rz. 124, zu den Revisionsbemühungen in der EU siehe Rz. 151 f. (mit Fussnoten).

[148] Es muss noch unterschieden werden, ob die Information bereits 180 Tage beim Provider gespeichert ist.

ergibt sich zum Beispiel auch aus der Weisung des US Justizdepartements aus dem Jahr 2017 zum Umgang mit Daten bei einer Cloud-Anbieterin.[149]

179 Dass dies nicht nur Theorie ist, sondern von Gerichten auch so gelebt wird, lässt sich durch die Gerichtspraxis in den USA aufzeigen.[150] Das Department of Justice übersetzt diese gerichtlichen Vorgaben im Search and Seizure Manual (ab Seite 112) in die folgenden Weisungen an die Strafverfolgungsbehörden des Bundes:

> *«When a search may result in the incidental seizure of network accounts belonging to innocent third parties, agents should take every step to protect the integrity of the third party accounts.»*

Wenn eine Beamtin beim Gericht um einen warrant ersucht, hat sie diesen Antrag mit einer Schilderung zu versehen, wie sie mit allfälligen Geheimnissen der Disinterested Third Party (hier: der Stadt Zürich) umgehen würde (Das Search and Seizure Manual anerkennt dies und das US Justizdepartement weist seine Beamtinnen wie folgt an):

> *«Because each of the provider's computers might contain records relating to users who are wholly unrelated to the criminal investigation, special procedures designed to uphold those users' privacy interests may be appropriate. For example, agents might inform the magistrate judge in the search warrant affidavit that they will take steps to ensure the confidentiality of the accounts and not expose their contents to human inspection.»*

c. Vor einem Klartextzugriff kommt es zu blossen Sicherungen

180 Das Search and Seizure Manual geht davon aus, dass in der Regel eine blosse Datensicherung ausreichen sollte und das Mittel der Wahl ist, um Daten für die Zwecke der Strafuntersuchung verfügbar zu machen:

> *«Safeguarding the accounts of innocent persons absent specific reasons to believe that evidence may be stored in the persons' accounts should satisfy the concerns expressed in Steve Jackson Games. »*

181 Dass eine blosse Sicherung noch nicht zu einem Klartextzugriff führt und damit das Amtsgeheimnis dadurch noch nicht gebrochen wird, ist dabei aus Sicht des vorliegenden Rechtsgutachtens besonders relevant. Dass eine Sicherung nötig sein aber fürs Erste auch genügen kann, unterstreicht das Department of Justice in der bereits erwähnten Weisung an ihre Beamtinnen von Dezember 2017.[151] Wie mit sichergestelltem Material umzugehen ist, ergibt sich aus der Strafprozessordnung (Federal Rules of Criminal Procedure, namentlich Rule 41). Man kann erkennen, dass die Abläufe in den USA gar nicht so unterschiedlich sind zu jenen in der Schweiz (siehe zu diesen Rz. 133 f.). Man kann durchaus davon ausgehen, dass es auch in den USA nicht sofort zu Klartextzugriffen auf das sichergestellte Datenmaterial kommt. Und die Stadt Zürich hat das Recht, Daten, die ihrer Auffassung nach dem Amtsgeheimnis unterstehen, aus dem Prozess entfernen zu lassen (Rule 41(g) Motion to Return).

182 Der Stadt Zürich stehen aber nicht nur die allgemeinrechtlichen Rechtsbehelfe unter dieser Rule 41(g) zu. Die USA haben ergänzende Regeln, die dem Zweck dienen, fremde Staaten (und damit auch die Stadt Zürich zu schützen). Diese Regeln können als Regeln der International Comity bezeichnet werden, worauf übersichtsartig im Folgenden eingegangen werden soll.

4. Das Vertrauensprinzip zwischen den USA und der Schweiz (Comity)

183 Die USA haben erkannt, dass nicht nur sie ein Bedürfnis an Strafverfolgung haben. Es ist auch klar etabliert, dass sich die USA einem grenzüberschreitenden Vertrauensprinzip unterwerfen, damit die

[149] US Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division: Seeking Enterprise Customer Data Held by Cloud Service Providers, abrufbar unter: https://www.justice.gov/criminal-ccips/file/1017511/download (angesehen am 11. August 2021).

[150] Beispielhaft In Re: Grand Jury Subpoenas, 454 F.3d 511 (6th Cir. 2006), abrufbar unter: https://law.justia.com/cases/federal/appellate-courts/F3/454/511/489658/ (angesehen am 11. August 2021).

[151] US Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division: Seeking Enterprise Customer Data Held by Cloud Service Providers, abrufbar unter: https://www.justice.gov/criminal-ccips/file/1017511/download (angesehen am 11. August 2021).

USA ein ausländisches Land nicht in einer Weise vor den Kopf stossen, dass künftig die eigenen Gerichte von diesem keine Rechtshilfe mehr erhalten.

184 Die USA haben deswegen mit dem Foreign Sovereign Immunities Act (FSIA) schon vor bald 50 Jahren eine Gesetzgebung erlassen, die in Worte fasst, dass und wie die Immunität von ausländischen Staaten respektvoll behandelt werden soll.

185 Sodann ergeben sich Regeln dieses grenzüberschreitenden Vertrauensprinzips (in den USA als «international comity» bezeichnet) in verschiedener Hinsicht aus der Gerichtspraxis:

- Die USA haben dazu materialisierte Regeln, die in mehreren Gerichtsentscheidungen Gestalt angenommen haben und sich zu mittlerweile ziemlich klar umrissenen Tests gemausert haben.
- Die USA hören auf echte Bedürfnisse eines anderen Staats, würden aber rein formale bzw. inhaltsleere Blocking Statutes eher übersteuern. Beispielsweise sind die USA französischen Blocking Statutes eher zögernd begegnet (sie wurden von den US-Richtern mehrfach übersteuert), während schweizerische Normen (wie z.B. das Bankgeheimnis) von US-Richtern als Blocking Statute anerkannt wurden (nicht aber Art. 271 StGB).

Exkurs – Zu Art. 271 StGB als Blocking Statute[152]: Art. 271 StGB[153] will den Anspruch der Schweiz auf das Gewaltmonopol in ihrem Hoheitsgebiet schützen. Hoheitliche Handlungen sollen nur die in der Schweiz rechtmässig aufgestellten Behörden bzw. Amtsstellen vornehmen können. Die Strafnorm richtet sich somit gegen alle, ungeachtet ihrer Nationalität oder Stellung. Die Tathandlung des Haupt-Tatbestands ist sehr breit umschrieben: «Handlungen vornehmen, die einer Behörde oder einem Beamten zukommen». Das Bundesstrafgericht hatte im Jahr 2000 z.B. die Strafbarkeit eines Mossad-Agenten nach Art. 271 StGB zu beurteilen, der eine Telefonleitung in der Schweiz «anzapfte».[154] Von der Norm erfasst wird generell «jede Handlung, die [sich] für sich betrachtet, d.h. nach ihrem Wesen und Zweck, […] als Amtstätigkeit charakterisiert». Das Gericht sah den Straftatbestand unter Hinweis darauf, dass eine Telefonüberwachung als Zwangsmassnahme der Strafuntersuchungsbehörden vorgesehen sei, als gegeben an.

In gleicher Weise würde ein schweizerisches Gericht die Möglichkeit, die Herausgabe digitaler Daten zu erzwingen (Art. 263 StPO), als Amtstätigkeit betrachten. Denn bei der Beschlagnahme handelt es sich um eine Zwangsmassnahme im Sinne von Art. 196 StPO. Solche Zwangsmassnahmen sind bundesrechtlich geregelt und den zuständigen (nationalen) Behörden vorbehalten. Wer nun für einen fremden Staat und unter Umgehung Schweizer Rechts gleichartige Handlungen auf schweizerischem Gebiet vornimmt, macht sich also gemäss Art. 271 StGB strafbar. Wenn die Tathandlung (Zugriff gewähren oder einem solchen Zugriff Vorschub leisten) von einer Person (Standort Inland) auf Daten im Inland (Standort Inland) ausgeführt wird, kann eine Strafbarkeit nach Art. 271 Ziff. 1 StGB resultieren.

In *Motorola v. Uzan*[155] hatte sich ein US District Court u.a. mit dem Schweizerischen Bankgeheimnis und der Herausgabe von Dokumenten gestützt auf Art. 271 StGB zu befassen. Richter Rakoff führte aus: «*Although the Court finds Article 47 of the Swiss Banking Act worthy of substantial deference, the Court rejects the banks' argument that similar deference is due to Article 271 of the Swiss Penal Code,*

[152] Dies wird allenfalls zu berücksichtigen sein, wenn es in einem Umsetzungsprojekt um die Frage geht, ob die Organisationseinheit der Stadt Zürich Lösungen mit Datenstandort Schweiz wählen muss. Wenn im Rahmen dieses Rechtsgutachtens somit der Schluss begründbar ist, dass die Strafbarkeit nach Art. 271 StGB oder Art. 273 StGB eine Bedeutung haben könnte, um den Schutz für die Organisationseinheiten der Stadt Zürich zu verbessern, sollte die OIZ im Rahmen der Cloud-Beschaffung bei den zur Auswahl stehenden Cloud-Anbieterinnen nachfragen, welche Teilkomponenten der Aufgabenstellung «Cloud» aus der Schweiz heraus erbracht wird: Gebäudehülle Rechenzentrum; sonstige IT-Infrastrukturen (Betriebsumgebungen wie Servers, Netzwerk, etc.); Maintenance für die IT-Infrastrukturen; Plattformsoftware (Installation, Maintenance); sonstige zentral verwaltete Software (Installation, Maintenance); Helpdesk-Services; Anwendersupport.

[153] Art. 271 Ziff. 1 StGB (Verbotene Handlungen für einen fremden Staat) lautet wie folgt: «*(1) Wer auf schweizerischem Gebiet ohne Bewilligung für einen fremden Staat Handlungen vornimmt, die einer Behörde oder einem Beamten zukommen, (2) wer solche Handlungen für eine ausländische Partei oder eine andere Organisation des Auslandes vornimmt, (3) wer solchen Handlungen Vorschub leistet, | wird […] bestraft.*»

[154] Urteil des Bundesstrafgerichts 9X.1/1999 vom 7. Juli 2000, E. 6b.

[155] *Motorola Corporation*, et al v. Uzan, et al, No. 1:2002cv00666 - Document 1048 (S.D.N.Y. 2014).

which speaks only tangentially to the production of documents and, according to the Swiss Federal Department of Justice and Police, does not create criminal liability for a bank that adheres to a U.S. court's order to search for bank account documents located in Swiss bank branches.»[156]

Insofern wurde das Bankgeheimnis als Blocking Statute anerkannt, Art. 271 StGB infolge mangelnder Vertrauenswürdigkeit (keine «substantial deference») hingegen nicht. Dabei stützte sich Richter Rakoff auf die Meinung des Eidgenössischen Justiz- und Polizeidepartements, wonach Art. 271 StGB keine strafrechtliche Verantwortlichkeit für eine Bank begründet, die sich an die Anordnung eines US-Gerichts hält, in Schweizer Bankfilialen befindliche Kontounterlagen zu suchen.[157]

Diese Vorbemerkungen sind wichtig, da sie den Boden bilden, auf den der CLOUD Act trifft. Dabei ist hervorzuheben, dass die Comity-Analyse bereits vor Erlass des CLOUD Act – also nach dem sog. Common Law – vorzunehmen ist, nicht erst wegen des CLOUD Act (§ 2703 (h)(3)[158]).

a. Die sog. «Sovereign-Deference Doctrines»

186 Die im Kontext des CLOUD Act relevanten Zugriffs-Instrumente *warrant* (z.B. Durchsuchungsbefehle) und *subpoena* (z.B. Herausgabeverfügungen) sind seit jeher geltendes Recht der USA. Es ist die Praxis der USA, diese Instrumente nicht gegenüber dem Unternehmen (ausserhalb der USA) durchzusetzen, das die Daten direkt hostet (also z.B. die lokalen Tochterfirmen des Cloud-Anbieters in der Schweiz oder Europa). Stattdessen werden die Instrumente gegenüber den entsprechenden Muttergesellschaften der Cloud-Anbieter durchgesetzt, wenn diese über ein ausreichendes Standbein in den USA verfügen.

187 Die angegangenen US-Cloud-Anbieter haben die Möglichkeit zur Anfechtung einer solchen richterlichen Anordnung, insbesondere wenn die Datenherausgabe eine Verletzung des am Ort der Datenhaltung geltenden nationalen Rechts hervorruft. In der Schweiz (Datenhaltung in der Schweiz) kann dies beispielsweise eine Verletzung von Art. 271 StGB (Verbotene Handlungen für einen fremden Staat) oder Art. 273 StGB (Wirtschaftlicher Nachrichtendienst) betreffen oder auch Bestimmungen des Amts- oder Berufsgeheimnisses.

188 Das angerufene US-Gericht wird dabei nach der in den USA üblichen Vorgehensweise die Interessen der Beteiligten gegeneinander abwägen (sog. «**common-law comity analysis**»[159]). Allein die Tatsache, dass eine ausländische Rechtsordnung Gesetze erlässt, die einen Normenkonflikt provozieren, würde ein US-Gericht noch nicht abhalten davon, einem eigenen, mit dem ausländischen Recht in Konflikt stehenden Rechtssatz den Vorrang zu geben.

189 Sogenannte «blocking statutes» sind Spezialgesetze, die die Einhaltung von Gesetzen eines anderen Landes verbieten. Sie könnten deshalb auch als «Anti-Comity» Gesetze verstanden werden. Aus diesem Grund wird ihnen (nicht nur) in der US-amerikanischen Rechtspflege zum Teil nicht dieselbe Beachtung geschenkt wie anderen ausländischen Gesetzen, und die Gerichte haben Rechtssprechungsregeln gegen blocking statutes entwickelt. So könnten gewisse Gerichte, die im Regelfall die Interessen eines fremden Staates im Rahmen der Comity-Analyse Beachtung schenken würden, dies ablehnen,

[156] *Motorola Corporation*, et al v. Uzan, et al, No. 1:2002cv00666 - Document 1048 (S.D.N.Y. 2014), FN 3.

[157] *Motorola v. Uzan* hat in der Schweiz sodann zu BGE 129 III 626 geführt, worin u.a. die sog. «Mareva Injunction» beurteilt wurde.

[158] Mit dem CLOUD Act wurde § 2703 (h)(3) mit der Überschrift «Comity Analysis and Disclosure of Information Regarding Legal Process Seeking Contents of Wire or Electronic Communication.» in den Stored Communication Act eingefügt: «(3) COMITY ANALYSIS.—For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into account, as appropriate— (A) the interests of the United States […], (B) the interests of the qualifying foreign government in preventing any prohibited disclosure; (C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider; (D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States […]; (E) the nature and extent of the provider's ties to and presence in the United States; (F) the importance to the investigation of the information required to be disclosed; (G) the likelihood of timely and effective access to the information […]; and (H) [Rechtshilfefall].»

[159] Begriff in Abgrenzung zur Comity-Analyse, die ergänzend durch den CLOUD Act eingeführt wurde, dazu FN 158.

wenn besagter Staat absichtlich blocking statutes erlassen hat, um extraterritoriale Anordnungen zu vereiteln.[160]

190 Der US Supreme Court hat dazu in *Société Nationale Industrielle Aérospatiale v United States District Court* folgendes festgehalten:

> *«The lesson of comity is that neither the discovery order nor the blocking statute can have the same omnipresent effect that it would have in a world of only one sovereign. The blocking statute thus is relevant to the court's particularized comity analysis only to the extent that its terms and its enforcement identify the nature of the sovereign interests in nondisclosure of specific kinds of material.»*[161]

b. Comity-Analyse

191 Globale Internet-Aktivitäten schaffen in vielerlei Hinsicht jurisdiktionsübergreifende Probleme und den sich überschneidenden und manchmal konkurrierenden Interessen verschiedener Staaten bei der Regulierung von Strafverfolgung im digitalen Raum muss Rechnung getragen werden. Diese Herausforderung ist allerdings nicht neu. Amerikanische Gerichte haben sich schon immer sehr sorgfältig um die aussenpolitischen Auswirkungen ihrer Entscheidungen gekümmert.

192 Diesen Gedanken ganz besonders zum Ausdruck bringen die sog. «Comity»-Doktrinen. «Comity» ist ein – wenn auch nicht genau definiertes, aber grundlegendes – Instrument der amerikanischen Rechtspflege mit langer Tradition. Im weitesten Sinne ist es ein rechtswissenschaftlicher Grundsatz zu den zwischenstaatlichen Beziehungen, welcher besagt, *dass Gerichte die legitimen Souveränitätsinteressen anderer Staaten anerkennen und ggf. dahinter zurückstehen sollen*. Man kann «Comity» somit als eine Art *zwischengerichtliche Diplomatie* verstehen, welche in der Kompetenz der Gerichte selbst liegt, also gewissermassen eine *Rücksichtnahme auf ausländische staatliche Akteure, die nicht durch internationales Recht vorgeschrieben ist, sondern im nationalen Recht verankert ist*.[162] Comity ist damit ein Rechtsgrundsatz zur Förderung der Zusammenarbeit zwischen Staaten.

193 Gerade in Bezug auf Informationsbegehren in der Strafverfolgung kann Comity eine Doktrin der Zurückhaltung sein, welche eine Abwägung der staatlichen Interessen verlangt. Ein Gericht eines Landes sollte sich bemühen, mögliche Konflikte zwischen seinen Anordnungen und dem Recht eines ausländischen Staates, der von seiner Entscheidung betroffen ist, so gering wie möglich zu halten.[163]

194 So wurde bspw. in *Linde v. Arab Bank*[164] anerkannt, dass Informationsbegehren aus Rücksicht auf internationale hoheitliche Interessen eingeschränkt werden können:

> *«We observe that when weighing the conflicting legal obligations of U.S. discovery orders and foreign laws, [m]echanical or overbroad rules of thumb are of little value; what is required is a careful balancing of the interests involved and a precise understanding of the facts and circumstances of the particular case.»*[165]

Bei dieser Interessenabwägung geht es nicht einfach um die Frage, ob die betreffende gerichtliche Massnahme zu einem Gesetzeskonflikt führt oder eine Partei dem Risiko ausländischer strafrechtlicher Sanktionen aussetzt. *Vielmehr erfordert die Untersuchung eine Abwägung (einerseits) der Interessen ausländischer Regierungen an der Durchsetzung ihrer Gesetze und der potenziellen Nachteile für die*

[160] Siehe bspw. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 442 Reporters' Note 4 (AM. LAW INST. 1987): «*Blocking statutes are designed to take advantage of the foreign government compulsion defense by prohibiting the disclosure, copying, inspection, or removal of documents located in the territory of the enacting state in compliance with orders of foreign authorities.*»

[161] *Société Nationale Industrielle Aérospatiale v. United States District Court, 482 U.S. 522 (1987), 545.*

[162] «*International comity is deference to foreign government actors that is not required by international law but is incorporated in domestic law.*»; WILLIAM S. DODGE, International Comity in American Law, in: 115 Columbia Law Review. 2071, 2078 (2015), abrufbar unter https://columbialawreview.org/wp-content/uploads/2016/03/Dodge-William-S..pdf (angesehen am 31. Juli 2021).

[163] *United States v. First Nat'l City Bank*, 396 F.2d 897, 902 (2d Cir. 1968): «*[A] court of one country should make an effort to minimize possible conflict between its orders and the law of a foreign state affected by its decision.*»

[164] *Linde v. Arab Bank,* 706 F.3d 92 (2d Cir. 2013).

[165] *Linde v. Arab Bank,* FN 164, 108 (zitiert aus *United States v. First Nat'l City Bank*, 396 F.2d 897, 901 (2d Cir. 1968).

belastete Partei gegen (andererseits) die Interessen der Vereinigten Staaten an der Durchsetzung ihrer Gesetze und den Bedarf der Kläger am Material für die Verfolgung ihrer Ansprüche.[166]

195 Ein weiterer Rechtspflegegrundsatz im Rahmen der Comity-Doktrin besagt, dass Gerichte vage Gesetze so auslegen sollen, dass sie nicht gegen die Autorität eines anderen Staates verstossen.[167] Ein Beispiel für eine solche Auslegungsregel ist der sog. «*Charming-Betsy*-Kanon», nach dem Gerichte mehrdeutige Gesetze so auslegen sollen, dass sie nicht gegen internationales Recht verstossen.[168]

196 Damit kann ein Cloud-Provider, der auf der Grundlage eines Gesetzes wie dem Stored Communications Act (resp. dem CLOUD Act) zur Herausgabe von im Ausland gespeicherten Daten aufgefordert wird, welche unter speziellen amtlichen Geheimnispflichten einer Behörde dieses Staates fallen, in das Verfahren einbringen, dass dies die territoriale Souveränität eines anderen Staates verletzen würde. Dieses Verteidigungsargument würde grundsätzlich angehört, da eine Verletzung der traditionellen Vorstellungen von territorialer Souveränität nach dem US-Recht grundsätzlich zu vermeiden ist.

197 Anstatt für eine bestimmte Auslegung der gesetzlichen Vermutung zugunsten oder gegen eine extraterritoriale Anwendung zu argumentieren, fordert der «*Charming-Betsy*-Kanon» die Gerichte auf, Wege zu finden, vage Gesetze so auszulegen, dass sie nicht gegen internationales Recht verstossen.

198 Obwohl der CLOUD Act festhält, dass Cloud-Anbieterinnen die Verpflichtungen des Stored Communications Act einhalten müssen, um Informationen über einen *Kunden* («customer») oder *Teilnehmer* («subscriber») im Rahmen eines gültigen Informationsersuchen von US-Strafverfolgungsbehörden offenzulegen (vorbehaltlich des oben beschriebenen Verfahrensschutzes), kann argumentiert werden, dass diese Begriffe («customer» und «subscriber») ausländische Regierungen und deren Behörden nicht einschliessen. US-Gerichte anerkennen seit langem, dass der *allgemeine Wortlaut eines Gesetzes Regierungen nicht einschliesst und die Rechte von Regierungen nicht beeinträchtigt*, es sei denn, eine solche Auslegung ergibt sich eindeutig und unbestreitbar aus dem Wortlaut des Gesetzes.[169] Dies muss insbesondere dann gelten, wenn die dergestalte Anwendung des Gesetzes eine souveräne ausländische Regierung oder deren Behörden ihrer anerkannten und berechtigten Interessen berauben würde, was mit Bezug auf dem Amtsgeheimnis unterstehende Informationen der Fall wäre.

199 Eine Auslegung des CLOUD Acts dahingehend, dass die US-Strafverfolgungsbehörden auf die Cloud-Inhalte ausländischer Regierungen zugreifen können, würde dem US Foreign Sovereign Immunities Act (FSIA) widersprechen, der die souveräne Immunität eines anderen Staats schützt. Die US-Behörde würde sonst in die Lage versetzt, Informationen einer ausländischen Regierung zu erhalten. Es gibt keinerlei Hinweise darauf, dass der CLOUD Act diesbezüglich die Möglichkeiten der US-Strafverfolgungsbehörden erweitern sollte.

200 Der FSIA ist vielmehr der ausschliessliche gesetzliche Rahmen, unter welchem die Gerichtsbarkeit über eine ausländische Regierung vor US-Gerichten zu erlangen[170] oder zu verneinen ist. Dies wurde vom

[166] *Linde v. Arab Bank,* FN 164, 98.

[167] EDWARD T. SWAINE, Cooperation, Comity, and Competition Policy: United States, in COOPERATION, COMITY, AND COMPETITION POLICY 3, 13 (Andrew T. Guzman ed., 2011) («*[T]he Supreme Court is receptive to comity when presented as a tool for statutory construction.*»).

[168] *Murray v. Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804) («*[A]n act of Congress ought never to be construed to violate the law of nations if any other possible construction remains…*»).

[169] *F. Hoffmann-La Roche Ltd v. Empagran* S. A., 542 U. S. 155, 164 (2004): «*[T]his Court ordinarily construes ambiguous statutes to avoid unreasonable interference with other nations' sovereign authority. This rule of construction reflects customary international law principles and cautions courts to assume that legislators take account of other nations' legitimate sovereign interests when writing American laws. It thereby helps the potentially conflicting laws of different nations work together in harmony.»;* siehe auch *RJR Nabisco, Inc. v. European Community.*

[170] Die Ausnahmen sind in 28 U.S.C. §§ 1605, 1605A und 1607 aufgeführt. Die häufigsten Ausnahmen sind, wenn der ausländische Staat auf die Immunität verzichtet (§ 1605(a)(1)) oder sich bereit erklärt, eine Streitigkeit einem Schiedsverfahren zu unterwerfen (§ 1605(a)(6)), eine gewerbliche (also mithin nicht hoheitliche Tätigkeit) ausübt (§ 1605(a)(2)), eine unerlaubte Handlung in den Vereinigten Staaten begeht (§ 1605(a)(5)) oder Eigentum unter Verletzung des Völkerrechts enteignet (§ 1605(a)(3)).

Obersten Gerichtshof der USA wiederholt so bestätigt.[171] Der Oberste Gerichtshof hat zudem wiederholt erklärt, dass er «*Gesetze so auslegen wird, dass eine unangemessene Einmischung in die souveräne Autorität anderer Nationen nach Möglichkeit vermieden wird*».[172] Dies schränkt die Zuständigkeit eines Gerichts ein, denn sobald die souveräne Immunität einer Regierung oder Behörde festgestellt ist, fehlt dem Gericht sowohl die persönliche als auch die sachliche Zuständigkeit. Die Zuständigkeit ist von wesentlicher Bedeutung, da die Gerichte ohne Zuständigkeit ein Auskunftsersuchen nach dem CLOUD Act nicht bewilligen können, und die Befugnis eines Gerichts, Anordnungen zur Auskunftserteilung zu erlassen, kann nicht umfassender sein als seine Zuständigkeit.

201 Obwohl die angegangenen Cloud-Anbieter selbst keinen eigenen Anspruch auf souveräne Immunität geniessen, ist davon auszugehen, dass Cloud-Anbieter als Reaktion auf Informationsanfragen der US-Strafverfolgungsbehörden im Rahmen des CLOUD Acts tatsächlich eine (von ihrem Cloud-Kunden, welcher eine Behörde eines ausländischen souveränen Staats ist) *abgeleitete souveräne Immunität* geltend machen können. In der Vergangenheit haben US-Gerichte den Schutz einer solchen *abgeleiteten souveränen Immunität* für private US-Unternehmen anerkannt, die auf Anweisung ausländischer Regierungen handelten.[173] Eine solch *abgeleitete souveräne Immunität* ist aus Sicht des Cloud-Anbieters dort anzunehmen, wo die Nutzung der Cloud-Dienste durch die ausländische Regierung resp. deren Behörde im Rahmen der Ausführung von hoheitlichen resp. Verwaltungs-Aufgaben geschieht, also mithin auch überall dort, wo vom Amtsgeheimnis erfasste Informationen in den Cloud-Diensten bearbeitet oder gespeichert werden.[174]

202 Die Berücksichtigung der Souveränität fremder Staaten beruht weitgehend auf der Erkenntnis, dass Staaten Teil eines internationalen Systems sind, das zum Teil auf Nichteinmischung und gegenseitigem Respekt beruht. Comity ist damit nicht nur eine Folge dieser Tatsache, sondern auch eine Ursache. Entsprechend ergreifen US-Gerichte oft Massnahmen, um Comity aktiv zu fördern:

203 In *Aérospatiale* stellte Richter Blackmun bspw. fest, dass Comity nicht nur ein vages politisches Anliegen ist, das die internationale Zusammenarbeit fördert, wenn dies in unserem (d.h. dem amerikanischen) Interesse liegt. Vielmehr handelt es sich um einen Grundsatz, nach dem gerichtliche Entscheidungen den systemischen Wert der gegenseitigen Toleranz und des Wohlwollens widerspiegeln.[175] US-Amerikanische Gerichte sind sich also der Tatsache durchaus bewusst, dass ihre Anordnungen nicht im luftleeren Raum ergehen.

c. Zwischenfazit: Die Stadt Zürich ist als Behörde in den USA respektiert und gut geschützt

204 Man kann somit sagen, dass somit gerade die Stadt Zürich berechtigten Anlass zur Annahme hat, dass ihre Daten in einem Strafverfahren gegen einen Dritten besonders gut geschützt würden – und zwar gerade, weil die Stadt Zürich eine offizielle Stelle ist.

205 Dies ergibt sich aufgrund der Analyse von Rechtstexten und Gerichtsentscheidungen. Man könnte einwerfen, dass die Rechtswirklichkeit anders aussehen würde. Gerade dass aber Gerichtsentscheidungen vorliegen, welche das Vorstehende erhärten, zeigt, dass sich die Rechtswirklichkeit tatsächlich in die Richtung bewegt, wie sie hier geschildert wird. Entsprechend darf bis zu Moment, wo Nachweise für

[171] *Permanent Mission of India to the United Nations v. City of New York* (zitiert aus *Argentine Republic v. Amerada Hess Shipping Corp.)*: «*[T]he FSIA provides the sole basis for obtaining jurisdiction over a foreign state in federal court.*»

[172] *RJR Nabisco, Inc. v. European Community 579 U.S. (2016)*: *«[W]e construe statutes to avoid unreasonable interference with other nations' sovereign authority where possible.*»; Anwendung durch ein Appellationsgericht: Trader Joe's Co. v. Hallatt, No. 14-35035 (9th Cir. 2016).

[173] *Butters v. Vance Int'l, Inc. and Alicog v. Kingdom of Saudi Arabia*: «*[A]gents enjoy derivative immunity when following the commands of a foreign sovereign employer.*»

[174] *Permanent Mission of India to the United Nations v. City of New York*; «*[T]he immunity of the sovereign is recognized with regard to sovereign or public acts (jure imperii) of a state, but not with respect to private acts (jure gestionis).*»

[175] *Aérospatiale*, 482 U.S., 555 (Blackmun, J., concurring in part and dissenting in part: «*[c]omity is not just a vague political concern favoring international cooperation when it is in our interest to do so. Rather it is a principle under which judicial decisions reflect the systemic value of reciprocal tolerance and goodwill.*»).

einen Bruch der internationalen Comity durch die USA angeführt werden, vom Vorstehenden ausgegangen werden.

5. Rückführung des Blicks auf die Frage, ob eine sanktionswürdige Offenbarung resultiert

a. Würdigung unter dem Aspekt des Amtsgeheimnis

206 Für die Organisationseinheit der Stadt Zürich gilt nach wie vor (und auch gegenüber ausländischem *lawful access*), dass die Organisationseinheit der Stadt Zürich, welche die Cloud nutzen will, nicht für einen 100%igen Schutz vor ausländischen Behördenzugriffen sorgen muss, dass sie die Beschlagnahmung genauso wenig aktiv verhindern muss, wie sie dies in der Schweiz tun muss und dass der *lawful access* nicht von ihr, sondern eben einem Dritten verursacht wird. Dass ein Dritter aber auf geheimnisgeschützte Daten zugreifen kann im Sinne des Klartextzugriffs, ist auch bei ausländischen Zugriffen nur selten der Fall (**aussergewöhnliches Ereignis**). Es ist also auch in der Konstellation der ausländischen Behördenzugriffe nicht von einem üblichen Normalbetrieb zu sprechen.

207 Zusammenfassend kann also gesagt werden, dass die Problemstellung für ausländische Behördenzugriffe zunächst einmal gleich gelagert ist wie bei schweizerischen Behördenzugriffen. Zudem ist die Anzahl der Zugriffe in den letzten Jahren zwar leicht angestiegen. Trotzdem sind ausländische Behördenzugriffe – entgegen der öffentlichen Wahrnehmung – immer noch aussergewöhnliche Ereignisse, welche auf der internationalen Bereitschaft gründet, das System der internationalen Rechtshilfe durch alternative Modelle zu modernisieren.

b. Wahrscheinlichkeitsprognosen

208 Vor diesem Hintergrund können nun quantitative Überlegungen einfliessen.

209 Zum Beispiel veröffentlicht Microsoft seit 2013 jeweils pro Halbjahr Zahlen zu den bei ihr eingegangenen Anfragen von Strafverfolgungsbehörden.[176] Diese Zahlen zeigen Folgendes:

- Im zweiten Halbjahr 2020 ist es bei weltweiter Betrachtung (Herausgabeaufforderungen aller Staaten) bei 24'798 eingegangenen Anfragen[177] lediglich in 5.34% der Fälle zu einer Herausgabe von «Content Data» gekommen.
- Im zweiten Halbjahr 2020 haben schweizerische Behörden 263 Anfragen gestellt. Microsoft hat bislang noch in keinem einzigen Fall den Strafverfolgungsbehörden in der Schweiz Klartext-Zugriff auf Kundendaten gewährt (Herausgabe von «Content Data»), sondern einzig Einsicht in Non-Content Daten gewährt (Nutzungsdaten). Keine der Anfragen führte zu einer Herausgabe von «Content Data».

210 Dass ein schweizerisches Unternehmen von einer Strafverfolgungsmassnahme in den USA betroffen gewesen wäre und Microsoft diesbezüglich eine relevante Rolle gespielt hätte, ist nicht bekannt.

211 Diese Zahlen beziehen sich allerdings auf alle Kundenkategorien, insbesondere auch auf die zahlreichen Kunden von Gratis-Diensten wie Hotmail oder Skype. Dies ist in Bezug auf ihre Aussagekraft zu würdigen.

212 Gleichzeitig betont Microsoft ihren gewissenhaften Umgang mit Anfragen von Strafverfolgungsbehörden: Behörden werden – wann immer möglich – direkt an die Cloud-Kunden verwiesen,[178] subsidiär werden die Anordnungen eingehend auf ihre formelle Zulässigkeit geprüft und auch regelmässig mit

[176] Abrufbar unter: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report (angesehen am 5. August 2021).

[177] Es ist davon auszugehen, dass die Anzahl der Anfragen steigen wird.

[178] Abrufbar unter: https://blogs.microsoft.com/datalaw/our-practices/#is-rejecting-request-the-only-way-microsoft-resists-government (angesehen am 8. August 2021).

rechtlichen Mitteln bekämpft.[179] Diese von Microsoft selbst stammenden Angaben lassen sich für Aussenstehende zwar nur schwer überprüfen, diverse von Microsoft initiierte rechtliche Verfahren[180] sind jedoch belegt und entsprechen dem von Microsoft gezeichneten Bild. Ausserdem sind Weisungen von staatlichen Stellen z.B. in den USA verfügbar, welche die Aussagen von Microsoft bestätigen.[181] Für Anfragen von US-amerikanischen Behörden kann also mit einer hohen Wahrscheinlichkeit davon ausgegangen werden, dass die Dienststelle von der strafverfolgenden Behörde kontaktiert würde, bevor es zu Klartextzugriffen kommen würde. Die Dienststelle kann in solchen Fällen dann das Verfahren gemäss Art. 320 Ziff. 2 StGB initiieren (siehe Rz. 115).

213 Seit Einführung des CLOUD Acts im Jahr 2018 sind bei Microsoft 785 Anfragen von US-Behörden für Daten, welche auf einem Server im Ausland liegen, eingegangen. Lediglich in *sehr seltenen* Fällen wurden in der Folge «Content Data» herausgegeben.[182] Man darf zwar nicht dem Irrtum verfallen, dass andere Datenkategorien «nichts wert» seien oder vollkommen unproblematisch wären, weil auf Basis z.B. von Traffic Data und Event Logs sehr viel über eine Person in Erfahrung gebracht werden kann. Man kann aber feststellen, dass im Bereich des Amtsgeheimnisses doch wohl eher der Inhalt eines Dokuments als der Zeitpunkt seines Versands eine Bedeutung haben wird.

214 Aus heutiger Sicht kann man feststellen, dass die Wahrscheinlichkeit eines Klartextzugriffs durch inländische und ausländische Behörden für die Dienststelle sehr klein ist. Weitere Gewichtungen sind im Rahmen eines Umsetzungsprojekts anzulegen, das von der Dienststelle im Anschluss an dieses Gutachten zu planen sein wird (Relevanz für Strafverfahren; Prüfung, inwiefern Relevanz für Zivilverfahren, etc.).

6. Zwischenfazit zur Nutzung von Cloud-Angeboten mit Bezug zu den USA

215 Das Gesagte bedeutet damit Folgendes:

- Es gibt weder unter dem Amtsgeheimnis noch unter dem Datenschutzrecht eine Pflicht der Stadt Zürich, Behördenzugriffe aus dem Ausland in jedem Fall zu verhindern. Es braucht Schutzmassnahmen, und diese müssen gut sein. Aber das theoretisch bzw. in kleinem Umfang verbleibende Restrisiko, dass Behördenzugriffe vorkommen, stellt keine Verletzung des Amtsgeheimnisses oder des Datenschutzrechts dar.
- Tatsächlich ist es so, dass das effektive Risiko der Offenlegung im Rahmen von ausländischen Strafverfahren gering ist. Die Diskussion über Behördenzugriffe wird somit in der öffentlichen Diskussion eher aufgebauscht.
- Darüber hinaus zeigen die gesamten Ausführungen, namentlich auch jene zum CLOUD Act, beziehungsweise zum Verfahren im Kontext von Behördenzugriffen, dass die Stadt Zürich im Fall eines Behördenzugriffs im Strafverfahren aufgrund der Gegebenheiten unter dem US-Recht eine Vielzahl von Sicherungsankern zur Verfügung stehen, um ihren Rechten bzw. ihrem Anspruch auf Einhaltung der Amtsgeheimnispflicht Gehör zu verschaffen.
- Der CLOUD Act löst zwar bedeutende Fragen aus (Stichwort "Garantieverantwortung der Eidgenossenschaft"), diese hat die Stadt Zürich aber nicht zu lösen. Mit anderen Worten: Wenn Zugriffe unter

[179] Abrufbar unter: https://blogs.microsoft.com/datalaw/our-practices/#what-is-process-disclosing-customer-information-legal (angesehen am 8. August 2021).

[180] Microsoft Corporation v. United States Department of Justice et al, Case No. 2:16-cv-00538 (filed 2014-04-14, W.D. Wash.); United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018), abrufbar unter: https://www.forbes.com/sites/emmawoollacott/2014/05/23/microsoft-stands-up-to-fbi-over-customer-data/ (angesehen am 8. August 2021).

[181] Weisung des US Department of Justice: Seeking Enterprise Customer Data Held by Cloud Service Providers (Dezember 2017), abrufbar unter: https://www.justice.gov/criminal-ccips/file/1017511/download (angesehen am 8. August 2021); US Department of Justice, Office of the Deputy Attorney General, MEMORANDUM FOR HEADS OF DEPARTMENT LAW ENFORCEMENT COMPONENTS, DEPARTMENT LITIGATING COMPONENTS, THE DIRECTOR, EXECUTIVE OFFICE FOR U.S. ATTORNEYS, ALL UNITED STATES ATTORNEYS (19. Oktober 2017).

[182] Abrufbar unter: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report?rtc=2 (angesehen am 8. August 2021). Die Berichte nennen eine Häufigkeit von ca. 3 Fällen pro Halbjahr.

dem CLOUD Act auf Daten der Stadt Zürich vorkämen, wäre dies zwar ein Problem, aber – sofern die Stadt Zürich mit aller geschuldeten Sorgfalt die notwendigen Massnahmen zum Schutz getroffen hat – nicht jenes der Stadt Zürich.

- Gerade für die Stadt Zürich ist die Problematik der unilateralen Datenzugriffe bzw. der Umgehung der Rechtshilfeinstrumente deutlich weniger relevant als zum Beispiel für ein privates Unternehmen – und zwar eben gerade, weil die Stadt Zürich eine öffentlich-rechtliche Körperschaft ist. Im Zusammenhang mit den Ausführungen zur Comity Analyse muss man zum Schluss kommen, dass in den USA für die Stadt Zürich positive institutionelle Rahmenbedingungen bestehen. Diese schützen die Stadt Zürich eher als dass sie sie mit Blick auf das Amtsgeheimnis eminent gefährden.

216 Daraus ergibt sich, dass das Risiko eines ausländischen Behördenzugriffs jedenfalls aus den USA keinen Hinderungsgrund darstellt, eine Cloud-Anbieterin auszuwählen. Es könnten für Cloud-Lösungen mit besonderen Bezügen zu anderen Rechtsordnungen vertiefende Überlegungen angestellt werden. Aus heutiger Sicht besteht für den Verfasser kein Anlass dafür, solche vorzubehalten. Je nach Bedeutung der ausgelagerten Datensätze (z.B. Stadtrichteramt der Stadt Zürich) könnte es aber sinnvoll sein, bei Nutzung von Cloud-Angeboten mit Datenhaltungsstandort in anderen Rechtsordnungen als den USA (z.B. Frankreich, Grossbritannien, Deutschland, Australien, Neuseeland, Kanada oder Israel) ergänzende Betrachtungen anzustellen.

IV. Teil 3: Beantwortung der Gutachterfragen und Empfehlungen

A. Antworten auf die Gutachterfragen auf Basis der Ausführungen

217 Generell sind die verwaltungsrechtlichen, datenschutzrechtlichen und strafrechtlichen Rahmenbedingungen für die Stadt Zürich günstig und ermöglichen ihr, ohne Verletzung von Geheimnisrecht und anderen Rechtsregeln, generell Cloud-Angebote grösserer Hyperscaler (wie natürlich grundsätzlich auch kleinerer Cloud-Anbieterinnen) zu prüfen und abzuschliessen. Rechtliche Hürden sind nicht ersichtlich, jedenfalls keine, die man nicht mit der normalen Sorgfalt einer ordnungsgemässen Projektführung überwinden könnte.

218 Für die OIZ dürfte es zum ganz normalen Alltag werden, Cloud-Angebote für die städtischen Organisationseinheiten zu beschaffen und diese in das städtische Service-Angebot zu integrieren. Der aktuelle gesetzliche Rahmen gibt der Stadt Zürich und der OIZ hierzu einen ausgereiften Rahmen und gute Werkzeuge in die Hand.

219 Basierend auf der vorstehenden Analyse ergeben sich folgende Antworten auf die Gutachterfragen:

1. Darf eine Organisationseinheit der Stadt Zürich Public Cloud Services nutzen?

220 Ja. Die Analyse zeigt, dass Organisationseinheiten der Stadt Zürich Public Cloud Services für die Speicherung und Verarbeitung aller Informationen und Daten nutzen dürfen, die sie in Erfüllung ihrer Aufgaben erstellen oder bearbeiten:

- Cloud-Angebote, die im Normalbetrieb zu keinen Klartextzugriffen führen, führen aus Sicht der im Raum stehenden Strafnormen (Art. 320 StGB, Art. 271 StGB, Art. 273 StGB, Art. 293 StGB) nicht zum Schluss, dass die Behörde ein strafrechtlich verbotenes Verhalten begehen würde oder sich sonstwie strafbar machen würde.
- Cloud-Angebote, bei denen es zu Klartextzugriffen kommt, können genutzt werden, wenn die Cloud-Anbieterin wirksam als Hilfsperson eingebunden wird.

221 Hinzu kommt Folgendes: Das kantonale Datenschutz- und Informationsrecht (§ 6 IDG i.V.m. § 25 IDG) erlaubt es den Organisationseinheiten ausdrücklich, externe Dienstleister (was auch die Nutzung externer IT-Infrastrukturanbieter beinhaltet) mit der Bearbeitung von Informationen (einschliesslich Personendaten) zu betrauen (Rz. 77).

222 Das Verwaltungsrecht liegt dieser Analyse zu Grunde und man kommt gemäss verwaltungsrechtlicher Analyse zu keinem anderen Schluss, wenn die Cloud-Lösungen in technischer und organisatorischer Hinsicht reif sind. Die Stadt Zürich muss die Cloud-Anbieterin zudem sorgfältig auswählen und mit ihr Verträge eingehen, die der Situation ihrer Organisationseinheiten gerecht werden. In diesem Rechtsgutachten wird ein Modell vorgeschlagen, wie die OIZ Cloud-Angebote in ihre Service-Angebote einbinden kann, so dass die Organisationseinheiten der Stadt Zürich effizient davon Gebrauch machen können (Rz. 62 ff.). Auch die Verträge zu Cloud-Anbieterinnen können zentral über die OIZ vereinbart werden.

223 Es ist denkbar, dass eine Organisationseinheit in ihrem Informationsinventar einzelne Informationsbestände findet, die sie aus strategischen Gründen anders behandeln und keiner Cloud-Nutzung zuführen will, obwohl dies mit Blick auf die Massnahmen im Basisschutz+ durchaus möglich und rechtlich zulässig wäre. Eine solche Sonderbehandlung ist im Rahmen der vom antizipierten Stadtratsbeschluss vorgesehenen Einzelfallprüfung (Rz. 63, Punkt 4) möglich. Die Organisationseinheit sollte die Gründe für eine solche ausnahmsweise Sonderbehandlung in der Regel kurz und zumindest abstrakt umreissen.

224 Soweit die OIZ als zentrale Beschaffungsstelle für Cloud-Angebote in der Stadt Zürich fungiert, sorgt sie zu Gunsten der Stadt Zürich dafür, dass die folgenden, an sich den nutzenden Organisationseinheiten obliegenden Verantwortlichkeiten, durch die OIZ erledigt werden:

- Sorgfältige Auswahl der Cloud-Anbieterinnen
- Kontrolle der Cloud-Anbieterin durch vertragliche Massnahmen sicherstellen (insbes. Einhaltung der Weisungen der Organisationseinheit, keine Bearbeitung zu eigenen Zwecken der Cloud-Anbieterin und Kontrolle der Datensicherheitsmassnahmen; Rz. 77)
- für die Einhaltung der Anforderungen der Stadt Zürich an die IT-Sicherheit sorgen (kundenseitig ebenso wie auf Seiten der Cloud-Anbieterin; die OIZ erfüllt die kundenseitigen Anforderungen, soweit diese nach Koordination nicht von der nutzenden Organisationseinheit zu erledigen sind)

Die Organisationseinheit muss diese Massnahmen nicht selbst vornehmen, wenn sie den Service von der OIZ bezieht, sondern darf sich darauf verlassen, dass die OIZ die diesfalls ihr obliegenden Massnahmen umgesetzt hat. Dies ergibt sich nicht zuletzt aus dem von der OIZ angeregten Stadtratsbeschluss, der im Sinne einer verbindlichen Weisung an die städtische Verwaltung regeln soll, wie die Beschaffung sowie die Nutzung von Cloud-Lösungen in der Stadt Zürich zu organisieren ist.

225 Bei Vorliegen eines ausreichenden Basisschutzes+ ist das Einholen ergänzender Genehmigungen nicht erforderlich. Genehmigungen sind nur dann in Betracht zu ziehen, soweit der Basisschutz+ nicht erreicht werden kann, auf die Cloud-Nutzung aber dennoch nicht verzichtet werden soll. Es sei hier auf vier Use Cases verwiesen, die in der Stadt Zürich regelmässig vorkommen könnten (Rz. 74).

2. Gilt dies auch für Informationen mit besonderem Schutzbedarf (vertrauliche oder streng vertrauliche Informationen)?

226 Ja. Die Nutzung von Public Cloud-Angeboten ist auch möglich, wenn Daten mit besonderem Schutzbedarf in die Cloud ausgelagert werden sollen. Hintergrund hierfür ist der Umstand, dass die Gesetzgebung diesbezüglich keine Einschränkungen macht.

227 Die OIZ sorgt dadurch, dass sie generell für einen erweiterten Basisschutz sorgt (Basisschutz+), dafür, dass die Cloud-Nutzung auch für Informationen mit besonderem Schutzbedarf auf Basis des in Rz. 63 – Rz. 69 beschriebenen Konzepts möglich ist. Da der Basisschutz+ Schutzmassnahmen vorsieht, die für besondere Personendaten für gewöhnlich geeignet sind (Rz. 63, Ziff. 3.2), bedarf es auch keiner weiteren Genehmigung nach § 25 Abs. 3 IDV.

228 In Sonderfällen (dazu Rz. 63 Ziff. 6 und Rz. 66; für die einzelnen Use Cases siehe zusammenfassend Rz. 74) braucht es je nach den Besonderheiten des städtischen Rechts unter Umständen eine weitere Genehmigung. Diese ist aber nicht cloud-spezifisch, sondern ergibt sich aus anderen Überlegungen im städtischen Recht. Eine ergänzende Genehmigung kann in wohl eher seltenen Fällen deshalb angezeigt sein, weil ein Cloud-Vorhaben unter Umständen mit Blick auf besondere Daten, die Gegenstand des Projekts bilden, eine erhöhte Aufmerksamkeit erfahren könnten. Diesfalls könnte es in der Praxis nützlich sein, das Projekt zu entlasten, indem über eine weitere Genehmigung nachgedacht wird. Im Normalfall bedarf es einer solchen aber nicht.

3. Verändert sich die Analyse, je nachdem, welcher Rechtsordnung der Provider oder eine seiner Gruppengesellschaften unterstehen (Sitz im Ausland, namentlich in den USA)?

229 Die Stadt Zürich darf auch Cloud-Angebote von Cloud-Anbieterinnen mit Auslandsbezug nutzen. Die Ausführungen zur Rechtslage in den USA ist diesbezüglich genügend klar. Namentlich stehen weder die Existenz noch die Durchführung des CLOUD Act oder generell die Möglichkeit von Datenzugriffen ausländischer Behörden dem Gang der Stadt Zürich «in die Cloud» entgegen. Dies gilt in Bezug auf den CLOUD Act der USA bereits aus konzeptionellen Überlegungen (Rz. 147–173). Umso mehr gilt es aufgrund der in den USA geltenden Abläufen (Rz. 174 ff.) und Vertrauensprinzipien (Rz. 183–203).

230 Es fällt auf, dass die gängigen Vorbehalte gegen die Rechtsordnung der USA sich auf Ebene CLOUD Act nicht auswirken. Es stellen sich in diesem Zusammenhang zwar durchaus viele rechtspolitische Fragen, aber es ist nicht die Aufgabe der Stadt Zürich, diese zu beantworten.

231 Es ist denkbar, dass die Auslagerung von Daten in Cloud-Angebote mit Bezügen aus anderen Rechtsordnungen als aus den USA nochmals separat plausibilisiert werden muss. Das vorliegende Rechtsgutachten zeigt aber auf, welche Fragen diesbezüglich zu stellen bzw. zu beantworten sein werden.

232 Das Kantonale Datenschutzrecht enthält auf jeden Fall keine Anforderung, wonach die gewählte Cloud-Anbieterin in der Schweiz domestiziert oder dem Datenschutzrecht des Bundes oder des Kantons unterstehen muss. An der Analyse ändert sich daher nichts, wenn die Cloud-Anbieterin Sitz im Ausland, einschliesslich der USA hat.

4. Verändert sich die Analyse, je nachdem, wo die in den Public Cloud Services gespeicherten Daten gehalten werden (Data at Rest) (Datenstandort in der Schweiz bzw. im Ausland, namentlich in den USA)?

233 Wenn die Stadt Zürich Cloud-Angebote mit Datenhaltungsstandort Schweiz bezieht, kann dies einen faktischen Schutz zu Gunsten der Stadt Zürich ergeben. Das stadtzürcherische Recht schreibt die Datenhaltung Schweiz jedoch nicht vor.

234 Eine Aussage dazu, ob bei einer Datenspeicherung im Ausland zusätzliche Risiken entstünden, kann im Rahmen des vorliegenden Gutachtens nicht abschliessend gemacht werden. Es wäre eine offene Suche. Konkret: Es ist möglich, dass eine Datenspeicherung im Ausland Risiken begründet, die der Verfasser beim heutigen Kenntnisstand allenfalls nicht erkennen kann (*unknown unknowns*). Solche Risiken müssten bei Kenntnis des konkreten Cloud-Angebots, das eine Organisationseinheit der Stadt Zürich nutzen will, konkret evaluiert werden. Heute wird aufgrund von Wahrscheinlichkeitsüberlegungen oft dafürgehalten, dass auch Datenhaltungen z.B. im US-amerikanischen Ausland möglich wären. Da man aber in verschiedener Hinsicht organisatorische und betriebliche Vereinfachungen erwirken kann, wenn man als Behörde eine Datenhaltung in der Schweiz wählt, sprechen aus Gründen der Verargumentierbarkeit und zum Schutz der Wahrnehmung der städtischen Cloud-Projekte in der Öffentlichkeit auf jeden Fall im verwaltungsrechtlichen Kontext oft gute Gründe für Lösungen mit Datenhaltungsstandort Schweiz. Es wäre jedoch nicht korrekt, den Datenhaltungsstandort Schweiz als *conditio sine qua non* darzustellen.

5. Verändert sich die Analyse, je nachdem, ob Personen aus dem Ausland (namentlich aus den USA) auf die in den Public Cloud Services gespeicherten Daten zugreifen können?

235 Generell ist davon auszugehen, dass Strafverfolgungsbehörden weltweit alle in ihrem Zugriffsbereich liegenden Daten herausverlangen bzw. beschlagnahmen können. Grundsätzlich ist keine Behörde, kein Unternehmen und keine Privatperson davor geschützt, dass eine Strafverfolgungsbehörde nach einen bei ihr gespeicherten Datensatz gemäss strafprozessualen Regeln herausverlangt (zu Zugriffen durch Schweizer Behörden: Rz. 124 –138).

236 Selbst der Zugriff staatlicher Institutionen ausserhalb der Schweiz (z.B. in den USA) auf Informationen, die Cloud-Kunden auf Cloud-Infrastrukturen in der Schweiz oder im Ausland bereitstellen lassen, ist somit nicht per se problematisch. Es kann einzig darum gehen, ob im Ausland die aus Sicht der Schweiz geforderten Verfahrensgarantien eingehalten werden (Rz. 158 – 163). Zugriffe einer ausländischen Strafverfolgungsbehörde sind somit so lange nicht von Belang für die hier behandelte Fragestellung, als der Zugriff im Rahmen eines geordneten Untersuchungs- oder Gerichtsverfahrens in einem Rechtsstaat erfolgt (Rz. 161). Dies wäre für den Zugriff von Strafverfolgungsbehörden der USA heute wohl zu bejahen (Rz. 161). Die Frage kann offen gelassen werden, weil die Stadt Zürich jeweils wird mitreden können in solchen Verfahren, da sie vom befassten US-Gericht direkt kontaktiert würde, bevor es dort zu Klartextzugriffen auf Daten in ihrem Tenant kommen wird (Rz. 174 ff.).

237 Auch allfällige Klartextzugriffe von Mitarbeitenden der Cloud-Anbieterin aus dem Ausland stehen der Cloud-Nutzung durch die Organisationseinheiten nicht entgegen. Die Einbindung als Hilfsperson gilt auch für sie (Rz. 105 – 108). Allfällige Hindernisse bei der Strafverfolgung gegenüber Mitarbeitenden der Cloud-Anbieterin (Hilfspersonen) im Ausland sind für die Frage der Zulässigkeit des Beizugs solcher Hilfspersonen unerheblich (Rz. 107 – Rz. 108).

B. Handlungsempfehlungen

238 Aus den vorstehenden Ausführungen ergeben sich die folgenden Handlungsempfehlungen für ein Umsetzungsprojekt:

1. Die OIZ sollte in einem Umsetzungsprojekt – bereits bei der Beschaffung der Leistung einer Cloud-Anbieterin – sicherstellen, dass gemäss den ihr vorliegenden Informationen auf Seiten der Cloud-Anbieterin ein genügender **Schutz durch technische und organisatorische Massnahmen gegen Klartextzugriffe** eingerichtet ist. Zudem muss sich die OIZ eine Organisationsstruktur geben, welche es ihr erlaubt, auch im Betrieb regelmässig zu prüfen, ob die Massnahmen noch greifen. Dafür ist ein internes Kontrollmodell aufzustellen. Beim Einrichten eines solchen Kontrollmodells (Rollen, Zuständigkeiten, Abläufe und evtl. Systeme), kann man sich durch darauf spezialisierte Firmen unterstützen lassen.

2. Die OIZ sollte geeignete vertragliche Massnahmen treffen, um die ausgewählte **Cloud-Anbieterin als Hilfsperson** zu bestellen (Einbindung der Cloud-Anbieterin als Hilfsperson, wie in Rz. 111 beschrieben; es handelt sich dabei um einen Sicherungsanker für den Fall, dass Klartextzugriffe trotz geeigneter Massnahmen stattfinden könnten; die Einbindung der Cloud-Anbieterin als Hilfsperson kann auch die Diskussion über die Strafbarkeit eindämmen).

3. Die OIZ sollte wie geplant beim Stadtrat den in Rz. 3 angedachten **Stadtratsbeschluss** erwirken. Auch ein solcher Stadtratsbeschluss ist eher ein Sicherungsanker. Er hat den Zweck, die handelnden Personen nicht der womöglich abschreckenden Wirkung von Mutmassungen auszusetzen. Solche Mutmassungen betreffen ein befürchtetes Restrisiko der Rechtswidrigkeit von Cloud-Nutzungen durch die öffentliche Hand. Dieses Restrisiko wurde zwar mit dem vorliegenden Rechtsgutachten widerlegt. Die Befürchtungen könnten aber in der öffentlichen Diskussion gleichwohl noch auftauchen. Hintergrund ist, dass mit Cloud Computing ein Paradigmenwechsel im Raum steht, der in der Öffentlichkeit noch nicht von allen Kreisen in derselben Weise akzeptiert wird. Erfahrungsgemäss können auch kritische Stimmen einer «Teil-Öffentlichkeit» eine durchaus einschüchternde Wirkung haben, was zu Projektverzögerungen führen kann. Der Stadtratsbeschluss dient dem Zweck, solche rein faktischen (nicht rechtlichen) Hürden zu überwinden.

C. Schlussfazit

239 Organisationseinheiten der Stadt Zürich dürfen Public Cloud-Angebote nutzen. Für Informationen mit besonderem Schutzbedarf müssen sie reife Anbieterinnen mit technisch ausgereiften Lösungen aussuchen. Für Informationen mit minderem Schutzbedürfnis können reduzierte Anforderungen genügen.

240 Wenn Informationen ausgelagert werden sollen, die dem Amtsgeheimnis unterstehen, sollten Lösungen ausgewählt werden, bei denen es nach der allgemeinen Lebenserfahrung und dem gewöhnlichen Lauf der Dinge zu keinen Klartextzugriffen kommt (d.h. Informationen werden z.B. von Mitarbeitenden der Cloud-Anbieterin nicht eingesehen werden). Ob die Organisationseinheit davon ausgehen darf, hängt davon ab, ob solcher Zugriffsschutz durch technische und organisatorische Massnahmen genügend abgesichert ist. Wenn die OIZ der Organisationseinheit ein Leistungsangebot mit Einbindung einer Cloud-Lösung anbietet, darf die Organisationseinheit sich auf die Bestätigung der OIZ verlassen, dass diese an Stelle der Organisationseinheit das Vorliegen eines genügenden Schutzes überprüft hat. Im Allgemeinen ist die Nutzung der Public Cloud für Informationen, die dem Amtsgeheimnis unterstehen sowie für besondere Personendaten zulässig, da die OIZ für den vorgegeben Basisschutz+ sorgen wird.

241 Eine beim Stadtrat zu beantragende Weisung wird in solchen Szenarien (Nutzung von Cloud-Lösungen über die OIZ mit Vorliegen von Basisschutz+) für die handelnde Personen strafbefreiende Wirkung haben. Wichtig und vorausgesetzt ist dafür, dass die Leiterin der auslagernde Organisationseinheit vor dem Entscheid plausibilisiert, ob die bei ihr vorliegenden Daten und Bedürfnisse eine Sonderbehandlung erfordern, die im Basisschutz+, den die OIZ bereitstellt, noch nicht abgebildet ist. Ist dies der Fall, ist der Sondersituation mit ergänzenden Massnahmen Rechnung zu tragen. Wenn die in Rz. 240 bezeichneten Schutzmassnahmen nicht umgesetzt werden, bedarf es über den Stadtratsbeschluss und den Entscheid der Leiterin der Organisationseinheit hinaus einer weiteren Genehmigung (sonst nicht). Diese wird bei der sog. *IT-Delegation* (Stelle der Stadt Zürich) einzuholen sein.

242 Es stellt keine Durchbrechung des Amtsgeheimnisses dar, wenn eine schweizerische Strafverfolgungsbehörde auf Daten der Stadt Zürich in der Schweiz zugreift. Die Stadt Zürich wird aber zunächst versuchen, auf ihr Amtsgeheimnis hinzuweisen und die Beschlagnahme solcher Daten bzw. einen späteren Zugriff abzuwenden. Dasselbe gilt in Bezug auf drohenden Zugriff auf Daten der Stadt Zürich durch Strafverfolgungsbehörden in den USA. Ein US-amerikanisches Gericht würde einen ausländischen Staat (und die Stadt Zürich wird als ein solcher verstanden) schützen. Bevor es zu einem Klartextzugriff kommt, würde die Stadt Zürich direkt angegangen. Dies ergibt sich nicht nur aufgrund von bedeutender Rechtsprechung, sondern auch aus einem US-amerikanischen Gesetz, dem sog. Foreign Sovereign Immunities Act (FSIA[183]). Gerade eine Behörde wie die Stadt Zürich ist in den USA sehr gut gegen Behördenzugriffe geschützt – auch wenn sie Daten in IT-Infrastrukturen einer US-amerikanischen Cloud-Anbieterin speichert. Hinzu kommen rein quantitative Erfahrungswerte, die zeigen, dass sich die Problematik sehr selten stellt. Noch wichtiger als dies ist aber die Analyse nach schweizerischem Recht: Die Stadt Zürich hat nach schweizerischem Recht keine Garantieverantwortung, Zugriffe von ausländischen Strafverfolgungsbehörden abzuwenden. Zusammenfassend kann die Gefahr der Strafbarkeit der Stadt Zürich bzw. ihrer Mitarbeitenden bzw. Organe (Behördenmitglieder) wegen ausländischer Behördenzugriffe als nicht existent bezeichnet werden.

243 Damit kann als Resultat festgehalten werden: Erreicht man in der Public Cloud ein Schutzniveau, das den zu schützenden Informationen und Bedürfnissen gerecht wird, ist die Nutzung des betreffenden Cloud-Angebots durch die Stadt Zürich zulässig.

* * *

[183] Nicht zu verwechseln mit dem Foreign Intelligence Surveillance Act (FISA).

Anhang 1: Begriffsdefinitionen

Daten und Information sind Begriffe, die heute in der Schweiz nicht einheitlich verwendet werden und «kaleidoskopartig» geregelt sind, d.h. viele Gesetze behandeln verschiedene Erscheinungsformen von Daten: *Unterlagen* (BGA), *Dokumente* (BGÖ), *Daten* (StGB, MetG, StatG, DSG), *Informationen* (GeoIG, ISG), *Geheimnisse* (StGB, UWG), *Arbeitsergebnisse* (UWG), Urkunden (StGB), (urheberrechtlich geschützte) *Werke* oder *Halbleitererzeugnisse* (URG, ToG), *technische Lehren* (PatG), *kennzeichnungskräftige Information* (MSchG und DesG). Für den Kanton Zürich (und somit auch für die Stadt Zürich) ist das IDG der relevante Rahmen und Begriffe im Rechtsgutachten sollten so gewählt werden, dass sie mit dem IDG in Einklang stehen.

Darüber hinaus sollen in diesem Anhang auch die zentralen Begriffe der IT-Infrastrukturen und der Cloud definiert werden. Dabei beziehen sich erstere besonders auf die IT-Infrastrukturen der Stadt Zürich.

Im Rahmen des Rechtsgutachtens werden somit die folgenden Begriffe hinsichtlich Daten[184] sowie IT-Infrastrukturen und Cloud verwendet:

Anonymisierung bezeichnet die Befreiung von Information von ihren personenbezogenen Identifikationsmerkmalen. Weil der Personenbezug durch die Anonymisierung vollständig entfernt wird, kommt das IDG nicht zur Anwendung. Anonymisierung erfordert unter Umständen Massnahmen zur Umgestaltung der Datenarchitektur oder der Datenformate.

Applikation ist ein Computerprogramm, das in Verbindung mit einer Maschine (Endgeräte wie Mobiltelefone, Server, etc.) spezifische Funktionen ausführt. Computerprogramme reagieren auf Anforderungen eines Anwenders oder einer anderen Applikation.

Auslandsbezug bezeichnet Bezüge entweder der Cloud-Anbieterin (rechtlicher Sitz, etc.) oder des Cloud-Angebots (Rechenzentrumsstandort, Standort von Mitarbeitenden oder beigezogenen Dritten, etc.) ins Ausland. Ein Auslandsbezug liegt bspw. vor, wenn (i) die Cloud-Anbieterin ihren rechtlichen Sitz im Ausland hat; (ii) die Cloud-Anbieterin IT-Infrastrukturen im Ausland betreibt oder betreiben lässt oder (iii) sie Personal im Ausland oder Subakkordanten im Ausland beschäftigt.[185]

Basiskomponenten ist ein Begriff, der zum Ausdruck bringt, dass die IT-Infrastrukturen der Anbieterin über den Tenant hinaus auch Gegenstand von Betriebsleistungen der Anbieterin sind und von der Anbieterin im Hintergrund über Steuerungssysteme administriert werden.

Bekanntgeben von Daten ist das Zugänglichmachen von Daten (zu den «Daten», *siehe dort*). Regelmässig führt dies auch zu einer Bekanntgabe von Informationen.

Bekanntgeben von Informationen ist das Zugänglichmachen von Informationen (zu den «Informationen», *siehe dort*) wie das Einsichtgewähren, Weitergeben oder Veröffentlichen.

Cloud-Anbieterin steht stellvertretend für Anbieterinnen von IT-Dienstleistungen, welche auf der Basis des Cloud Computing aufbauen. Dies umfasst sämtliche Integrationstiefen der Cloud-Lösung, von IaaS über PaaS bis SaaS (zu diesen Begriffen *siehe* sogleich «Cloud-Angebot oder Cloud-Lösung»).

[184] Diese Begriffswelt stellt ab auf ROLF H. WEBER/CHRISTIAN LAUX/DOMINIC OERTLY: Datenpolitik als Rechtsthema, Zürich 2016, S. 12 ff.

[185] Für diese Kategorie (Personal oder Subakkordanten) besteht der Auslandsbezug dann, wenn aus dem Ausland Zugriff auf das Cloud-Angebot genommen werden kann.

Cloud-Angebot oder Cloud-Lösung ist die Gesamtheit der Leistungen, mit denen eine Anbieterin einer Organisationseinheit der Stadt Zürich die Nutzung gewisser IT-Infrastrukturen standardisiert, automatisiert, skalierbar und in nicht dedizierter Form über Datennetze gewährt. Cloud-Angebote können die Organisationseinheit der Stadt Zürich davon entbinden, eigene Rechenzentren, eigene Hardware und eigene Serversoftware zu betreiben (man spricht dann von Infrastructure as a Service, **IaaS**) oder weitergehend auch dazu dienen, dass die Organisationseinheit der Stadt Zürich gewisse Software (Betriebssoftware oder Anwenderapplikationen) nicht selber betreiben und warten muss (man spricht dann von Platform as a Service, **PaaS**, oder Software as a Service, **SaaS**). Cloud-Angebot steht hier stellvertretend für den umgangssprachlich geprägten Begriff «**Public Cloud**», was zum Ausdruck bringen soll, dass die Basiskomponenten der Anbieterin für keinen Kunden individuell-exklusiv («dediziert») nutzbar sind; demgegenüber ist die bereitgestellte Nutzungsmöglichkeit innerhalb eines Tenant kundenindividuell und abgegrenzt gegenüber anderen Kunden («Isolation»), was z.B. mittels Netzwerktechnologie ermöglicht wird.

Daten sind die konkreten Speicherobjekte in einem bestimmten Speicherformat (PDF-Dateien; png-Dateien; SQL-Datenbanken-Speicherformate etc.). Der Datenbegriff bildet ein technisches Verständnis ab. In Abgrenzung zum Informationsbegriff lässt sich bildhaft sagen, dass Daten gewissermassen der «Behälter» für Informationen sind (*siehe* dazu mehr unter «Information»). Zur Reduktion des Risikos eines unbefugten Datenzugriffs lassen sich Daten auf verschiedene Arten technisch verändern (z.B. mittels Verschlüsselung, *siehe dort*). Der Begriff der Daten ist Anknüpfungspunkt für die zentralen Begriffe «Daten unter Dritteinfluss» (*siehe dort*) und «Kontrolle über Daten» (*siehe dort*).

Daten – **Personendaten** sind Informationen, welche sich auf eine bestimmte oder bestimmbare Person beziehen. Beispiele für Information, aus der ein Rückschluss auf Personen möglich ist («Personenbezug»): Geburtsdaten, Angaben zu Ausgabenbewegungen, Angaben zu besuchten Websites.[186]

Daten – **Besondere Personendaten** sind erstens Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht (z.B. Daten über religiöse und politische Ansichten, biometrische Daten, Daten über strafrechtliche Verfolgung). Zweitens fallen unter den Begriff der «besonderen Personendaten» auch Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit natürlicher Personen erlauben sowie drittens Daten im Rahmen des Profiling.

Daten – **Sachdaten** sind Informationen, welche keine Personendaten sind. Beispiele für Information ohne Personenbezug: Angabe zur Höhe eines Berges, Angaben zur Temperaturentwicklung.

Daten unter Dritteinfluss bestehen dann, wenn ein anderer als die Organisationseinheit (der Stadt Zürich), die den Zugriff auf bestimmte Daten kontrolliert, das Schicksal dieser Daten mitbestimmen kann – sei es aufgrund eines Gesetzes oder einer privaten Beschränkung (z.B. Vertrag, einseitige Zusicherung oder interne Weisung) –, liegen Daten unter Dritteinfluss vor. Der Dritteinfluss kann von Seiten eines Privaten oder einer öffentlichen Institution ausgehen.

Datenbearbeitung ist ein Vorgang, der dazu führt, dass der Mensch die in den Daten gespeicherten Informationen erkennt, sie wahrnehmen (siehe Klartext-Zugriff, siehe Personensicht) und allenfalls auch bearbeiten kann.

[186] Nach der in diesem Gutachten verwendeten Terminologie müsste man hier streng genommen von «Personeninformationen» sprechen. Da die Begriffe in diesem Gutachten allerdings die Terminologie des IDG widerspiegeln sollen, wird hier der Begriff «Personendaten» (gemäss der hier beschriebenen Definition bzw. § 3 Abs. 3 IDG) verwendet.

Information meint im vorliegenden Rechtsgutachten den Bedeutungsgehalt von Daten («das ‚it' vom ‚bit'»). Gemeint ist also, was man «mit der Personensicht wahrnehmen kann» (zur «Personensicht», *siehe dort*). Als Information werden hier also Aufzeichnungen bezeichnet, die etwas oder jemanden beschreiben und welche die Erfüllung einer öffentlichen Aufgabe betreffen.[187] Dies gilt unabhängig von ihrer Darstellungsform und ihrem Informationsträger. Zur Reduktion des Risikos eines unbefugten Informationszugriffs lassen sich Informationen auf verschiedene Arten verändern (siehe «Pseudonymisierung» oder «Anonymisierung»). Anmerkung: Der Begriff der «Information» wird im IDG nicht ganz einheitlich verwendet, da Informationen mit Personenbezug im Einklang mit der Tradition auf Bundesebene (DSG) und der europäischen Rechtstradition (DSGVO) als «Personendaten» (*siehe dort*) bezeichnet werden, obwohl es sich um Angaben handelt, die in der menschlichen Wahrnehmung als beschreibend verstanden werden. Mit anderen Worten: Der Begriff «Personendaten» ist für die Personensicht (*siehe dort*) massgeblich, und nicht für die Maschinensicht (*siehe dort*).

Informationsbearbeitung ist jeder Umgang mit Informationen wie das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben oder Vernichten. Beispiel: Wer in einer Tabellenkalkulationssoftware eine Tabelle öffnet (Zugriff auf Information) und eine Reihe von Angaben in die Tabelle einfügt, hat Information bearbeitet. Gleichzeitig wird ein Datenbearbeitungsvorgang ausgelöst.

IT-Infrastrukturen ist ein Oberbegriff für die städtischen ICT-Infrastrukturen der Stadt Zürich einerseits und IT-Infrastrukturen privater Provider andererseits, d.h. je nach Kontext die Gesamtheit von Gebäuden, Hardware, Software, Netzwerktechnologie etc., die das jeweils relevante Rechtssubjekt einsetzt, um eine Nutzungsmöglichkeit bereitzustellen. Siehe auch städtische IT-Infrastruktur. Anmerkung: Wenn die IT-Infrastrukturen der Stadt Zürich allein referenziert werden sollen, wird stattdessen der Begriff «städtische ICT-Infrastrukturen» (*siehe dort*) oder ein weiterer Begriff verwendet.

Klartext-Zugriff meint den Vorgang, mit dem ein Mensch ohne weiteres Hilfsmittel den Bedeutungsgehalt von ihm präsentierten Zeichen erkennen, lesen und sich merken oder weitergeben kann. *Blosser Zutritt* zum Ort der Datenhaltung begründet demgegenüber keinen Klartext-Zugriff. Wer einen Serverraum besuchen darf und im Gang zwischen den Servern an den Datenträgern vorbeischlendert, hat offenbar Zutritt zu Daten (genauer: zum Ort der Datenhaltung). Selbst wenn er dies ohne Aufsicht tut, hat er von den Inhalten, die auf den Datenträgern gespeichert sind, noch keine Kenntnis erhalten. Wenn der Besucher den Serverraum anschliessend wieder verlässt, ohne auf die Datenträger zuzugreifen, ist in Bezug auf das zu wahrende Geheimnis nichts passiert. Gleichermassen sprechen wir nicht von Klartext-Zugriff, wenn jemand erst ein technisches Hilfsmittel benötigt, bevor er den Bedeutungsgehalt erkennen kann etc. Ein solches Hilfsmittel könnte etwa ein Bildschirm sein, der an einem Datenverarbeitungsgerät angeschlossen ist; oder eine Applikation, die auf eine Datenbank zugreift und dank der die in der Datenbank gespeicherte Information erst für den Anwender transparent erkennbar wird. Der Begriff ist von Bedeutung für das Verständnis von Geheimnispflichten. Das schweizerische Recht hält aber keine geeigneten Begrifflichkeiten bereit, um für Menschen erkennbare Angaben von technisch geprägten Formatierungen zu unterscheiden, die nur von Maschinen interpretiert werden können, aber ohne Hilfsmittel nicht für Menschen erkennbar sind. Entsprechend verwenden wir hier diese umgangssprachliche Begrifflichkeit. Man könnte auch (synonym) von «Zugriff auf Information» sprechen.

Kontrolle über Daten hat, wer mittels technischer, organisatorischer oder vertraglicher Massnahmen gewährleisten kann, dass nur befugte Dritte (i) auf die Daten zugreifen, (ii) die Daten verwerten und (iii) die Daten verändern bzw. löschen können. Vollständige Kontrolle hat nur, wer unter den vorgenannten

[187] Keine Informationen sind nach dem Willen des IDG allerdings Aufzeichnungen, die nicht fertig gestellt oder die ausschliesslich zum persönlichen Gebrauch bestimmt sind. Im umgangssprachlichen Sinn (und auch nach der Begriffsdefinition, die wir hier verwenden), wären auch solche «halbfertigen» Notizen und dergleichen «Informationen» (wie hier definiert). Die Negativabgrenzung ist zu verstehen im Lichte des verwaltungsrechtlichen Anliegens, den Anwendungsbereich des IDG eingrenzend zu klären.

Punkten (Zugang, Verwertung, Löschung) gegenüber anderen einen Exklusivitätsanspruch durchsetzen kann und von Dritten zudem die Veränderung oder Löschung der betreffenden Daten verlangen kann.

Maschinensicht (im Gegensatz zu Personensicht[188]) meint in sachverhaltsmässiger Hinsicht, dass innerhalb einer IT-Infrastruktur zwar Daten verschoben oder verarbeitet werden können, dass dies jedoch nicht in jedem Fall dazu führt, dass ein Mensch deswegen Klartext-Zugriff auf Informationen bzw. auf einen bestimmten Bedeutungsgehalt erhalten würde. Im Informationsrecht muss man jeweils kritisch hinterfragen, ob aufgrund eines bestimmten Vorgangs tatsächlich ein Mensch erkennt, welcher Bedeutungsgehalt in einer Speicherung enthalten ist, oder ob diese Wirkung nicht eintritt.

Normalbetrieb[189] meint, dass das Cloud-Angebot wie geplant von der Anbieterin betrieben wird. Dies steht im Gegensatz zu den ausserordentlichen Situationen, die dem Normalbetrieb gerade nicht zuzurechnen sind (z.B. Konkurs[190] der Anbieterin, Behördenzugriff[191] auf das Cloud-Angebot, Zugriffe von Kriminellen auf das Cloud-Angebot).

OIZ ist die Dienstabteilung «Organisation und Informatik der Stadt Zürich».

Organisationseinheiten sind Departement oder Dienstabteilungen. Für die Zwecke des vorliegenden Rechtsgutachtens schliesst der Begriff der Organisationseinheit die OIZ nicht mit ein (obwohl die OIZ nach städtischem Recht ebenfalls eine Dienstabteilung ist).

Papierakten sind Akten, welche nicht elektronisch gespeichert sind und sich an Standorten der Stadt Zürich befinden. Ihre Mitnahme ist auf das Notwendigste zu beschränken.

Personensicht (im Gegensatz zur Maschinensicht) meint in sachverhaltsmässiger Hinsicht das, was ein Mensch erkennt, wenn er – je nachdem – auf IT-Infrastrukturen oder Teile davon bzw. auf Daten oder Informationen blickt.

Pseudonymisierung ist der Ersatz von personenbezogenen Merkmalen in Information durch eine alternative Bezeichnung (ein «Pseudonym», z.B. einen Zahlencode). Ob die Datenschutzgesetze auf solche Information noch zur Anwendung kommen, wird international nicht einheitlich beantwortet. Je nachdem kommt es darauf an, auf welche Optik man abstellt. Pseudonymisierung erfordert unter Umständen Massnahmen zur Umgestaltung der Datenarchitektur oder der Datenformate.

[188] Als Beispiel siehe https://e-idblog.ch/2021/02/17/was-bedeutet-kenntnis/ (abgerufen am 15. August 2021).

[189] Die Berechtigung zu dieser Unterscheidung ergibt sich aus der Überlegung, dass eine Organisationseinheit der Stadt Zürich rechtliche Risiken der Offenbarung nur in dem Ausmass berücksichtigen muss, wie sie sie beherrschen kann.

[190] Die Organisationseinheit der Stadt Zürich muss dieses Szenario sorgfältig planen und muss ausserdem die Anbieterin hinsichtlich des Insolvenzrisikos überwachen. Dies umfasst die Verpflichtung der Organisationseinheit der Stadt Zürich, eine enge Interaktion mit dem Key Account Manager der Anbieterin aufrechtzuerhalten und die Finanzabschlüsse der Anbieterin regelmässig zu überprüfen. Die Organisationseinheit der Stadt Zürich muss auch ihre Planung zur Aufrechterhaltung ihrer Geschäftstätigkeit (Business Continuity) an solchen Szenarien messen lassen können (um ein schnelles Back-Sourcing und das sofortige Löschen von Daten zu ermöglichen). Beispielsweise muss ein Notfallplan vorliegen, nach welchem die Organisationseinheit der Stadt Zürich geheimnisrelevante Daten sofort und direkt über das Verwaltungspanel des Kundenportals löscht, sobald die Organisationseinheit der Stadt Zürich Kenntnis vom Konkurs des Providers erlangt – und zwar noch bevor der allenfalls bestellte Konkursverwalter der Organisationseinheit der Stadt Zürich die Zugänge auf die IT-Infrastrukturen des Providers sperrt.

[191] Eine Strafverfolgungsbehörde verlangt von der Organisationseinheit der Stadt Zürich oder von der Cloud-Anbieterin, ihr Zugriff zu gewähren auf Daten einer Bürgerin oder eines Bürgers bzw. einer sonstigen natürlichen Person (oder auf Daten der Organisationseinheit der Stadt Zürich). Sehr wenige Autoren diskutieren das Risiko eines ausländischen Strafverfolgungszugangs in angemessener Weise, d.h. ohne sich in die oft unscharfen Gespräche zu Themen wie dem CLOUD-Act, dem US-amerikanischen PATRIOT-Act und ähnlichen Regeln des Strafverfolgungsrechts ausländischer Regierungen zu äussern. Auch das Risiko eines Zugriffs durch inländische Behörden ist als Situation zu behandeln, die nicht dem Normalbetrieb zuzurechnen ist. Der Zugang einer Schweizer Behörde kann ähnliche oder sogar dramatischere Auswirkungen auf die Bürgerin bzw. den Bürger haben als der Zugang einer ausländischen Strafverfolgungsbehörde. Natürlich kann es auch andersherum sein. Die Organisationseinheit der Stadt Zürich weiss unter Umständen nicht, wie die Risikoexposition der Bürgerin bzw. des Bürgers diesbezüglich aussieht. Die Organisationseinheit der Stadt Zürich muss aber verstehen, mit welcher Wahrscheinlichkeit und unter welchen Umständen eine Behörde auf ihre Daten zugreifen kann (unabhängig vom Einsatz von Cloud-Angeboten).

SSA ist das stadtweite Serviceangebot der OIZ. Zum Teil erbringt OIZ ihr Serviceangebot unter Beizug von externen Leistungserbringerinnen, jeweils für bestimmte Dienste. Aus Sicht der OIZ steht SSA somit für die Gesamtheit der den Organisationseinheiten der Stadt Zürich angebotenen Dienste (Eigenleistungen der OIZ und bei externen Leistungserbringerinnen beschaffte Dienste). Das SSA ist entsprechend dem Bedarf der Stadt Zürich konfiguriert. Mit anderen Worten wird grundsätzlich (soweit sinnvoll) jeder Dienst in die städtischen Umsysteme integriert (IT-Basisinfrastruktur, IT-Prozesse, stadtweite Anwendungen und Endgeräte). Für das SSA sind technische und organisatorische Massnahmen implementiert, die die stadtweit relevanten Anforderungen an die Informationssicherheit und den Datenschutz erfüllen. Soweit eine Organisationseinheit der Stadt Zürich einen oder mehrere solcher bestimmten Dienste beziehen will, nutzt sie also (in der Regel: nur) einen Teil des SSA für sich. Aus der Nutzerinnensicht ist das SSA also jener von der Nutzerin konsumierte Dienst, den die Nutzerin (die Organisationseinheit der Stadt Zürich) von der OIZ bezieht (bzw. die Gesamtheit der über die OIZ bezogenen Dienste). Jede Organisationseinheit prüft selbständig, ob in Ergänzung zu den bereits eingerichteten Schutzmassnahmen (Technische, Organisatorische und vertragliche Massnahmen) weitere Massnahmen erforderlich sind.

Städtische ICT-Infrastruktur ist die Gesamtheit aller IT-Infrastrukturen (*siehe dort*), die dem von der OIZ geprüften und für gut befundenen Normalsetup entspricht. Die Städtische ICT-Infrastruktur kann entsprechend von der Stadt Zürich bzw. von ihren Organisationseinheiten verwendet werden. Die Städtische ICT-Infrastruktur kann aus eigenen IT-Infrastrukturen der Stadt Zürich und aus IT-Infrastrukturen im Eigentum von Dritten bestehen.

Städtisches Netzwerk ist eine Teilkomponente der städtischen ICT-Infrastruktur mit der Funktion, Geräte und dergleichen in kontrollierter Weise für die Zwecke der Stadt Zürich zu verbinden.

Stadtnetz: siehe städtisches Netzwerk.

Tenant ist die der Organisationseinheit der Stadt Zürich bereitgestellte, kundenindividuelle Nutzungsumgebung und damit ein Zugriffsbereich, der z.B. mit Mitteln der Netzwerktechnologie ausschliesslich der Organisationseinheit der Stadt Zürich und ihren Mitarbeitenden zur Nutzung bereitsteht. Ein Tenant wird meist über mehrere Basiskomponenten hinweg ermöglicht; eine genaue Zuordnung eines Tenant zu einer bestimmten Basiskomponente ist in zeitlicher Hinsicht variabel; bei Betrachtung nur in einem konkreten Augenblick («Snapshot») wäre eine Zuordnung zwar möglich, aber sehr aufwändig.

Verschlüsselung meint in diesem Gutachten die Umwandlung von Daten in ein Format, das von nicht autorisierten Personen kaum bearbeitet werden kann. Die Verschlüsselung hat nicht die Wirkung, Daten aus dem Anwendungsbereich des Datenschutzrechts auszunehmen. Verschlüsselung setzt voraus, dass griffige Verschlüsselungstechniken verfügbar sind.

Verwertung von Information[192] ist jede Benutzung von Information im Anschluss an den Zugriff auf Information.

Zugriff auf Information erfolgt (erst), wenn derjenige, der auf Daten zugreift, die in den Daten gespeicherte Information erkennen kann (z.B. weil er über eine Maschine oder eine Methode verfügt, die in den Daten gespeicherte Information für sich erkennbar zu machen). Synonym zum Klartext-Zugriff.

Züri-Netz: siehe städtisches Netzwerk oder Stadtnetz.

* * *

[192] **Verwertung von Daten**: Eine Verwertungshandlung (im hier verstandenen Sinne: Ausnutzen des Werts einer Speicherung) von Daten ohne auf die gespeicherte Information zuzugreifen, ist in der Praxis nicht von Bedeutung und wird hier deswegen nicht definiert.

Anhang 2: Abstrakte Beschreibung von Public Cloud Services (IaaS, PaaS, SaaS)

1. Nutzung von reinen IaaS-Angeboten

In einem reinen IaaS-Angebot nutzt die Organisationseinheit der Stadt Zürich IT-Infrastrukturen der Cloud-Anbieterin, und zwar im Wesentlichen Gebäude, Server, Virtualisierungsschichten und Storagekomponenten. Diese Ressourcen werden allerdings nicht isoliert genutzt, sondern sind die Basiskomponenten, auf deren Grundlage der Organisationseinheit der Stadt Zürich virtuelle Server bzw. virtuelle Maschinen zur Verfügung gestellt werden.[193] Diese virtuellen Maschinen benutzt die Organisationseinheit der Stadt Zürich in ähnlicher Weise, wie sie früher physische Serverkomponenten mit Datenträgern in eigenen Räumlichkeiten gehalten und verwaltet hat. Das Nutzungserlebnis für die Organisationseinheit der Stadt Zürich unterscheidet sich vom früheren Nutzungserlebnis (IT-Infrastrukturen bei der Organisationseinheit der Stadt Zürich) nicht wesentlich.

Die von der Cloud-Anbieterin eingesetzten Basiskomponenten werden von der Cloud-Anbieterin automatisiert verwaltet. Dazu dienen Steuerungssysteme, die es der Cloud-Anbieterin ermöglichen, die in grosser Zahl bereitgestellten Ressourcen mit angemessenem Aufwand und einem überaus hohen Mass an Automatisierung für die Organisationseinheit der Stadt Zürich nach einheitlichen Methoden (also gleich wie für andere Kundinnen) zu verwalten. Eine kundenindividuelle Betreuung zu Gunsten der Organisationseinheit der Stadt Zürich findet grundsätzlich nicht statt. Die Cloud-Anbieterin bedient die zentrale Automatisierungslösung in einer Weise, dass auf allen Ebenen der eingesetzten IT-Infrastrukturen Softwarekomponenten automatisiert aktualisiert werden oder die Aktualisierung für alle der eingesetzten Basiskomponenten (oder für eine nach abstrakten Kriterien definierte Auswahl der Basiskomponenten: Versionennummer, Alter der Hardware, etc.) einheitlich vorgenommen werden kann. Das Steuerungssystem ermöglicht also eine effizientere Steuerung von Handlungen zur Aufrechterhaltung und Verbesserung des Gesamtsystems. Die für die rechtliche Analyse zentrale Charakteristik dieses Vorgehens besteht darin, dass die eingesetzten Ressourcen der Cloud-Anbieterin nicht von menschlicher Hand und dediziert für die Organisationseinheit der Stadt Zürich verwaltet werden, sondern automatisiert und uniform für die gesamte Kundenbasis. Dieser Ansatz kann mit dem Schlagwort "Hyperscale" bezeichnet werden. Anders als in kleinen IT-Infrastrukturen sind Cloud-Angebote, die nach dem Hyperscaler-Ansatz aufgebaut sind, notwendigerweise anonym. Während zwar noch immer Menschen die zentrale Automatisierungslösung bedienen, steuern sie vielmehr die Verwaltungskriterien, als dass sie "für eine einzelne Kundin" Management-Aufgaben übernehmen.

Die Verwaltung der IT-Infrastrukturen mit dem Hyperscaler-Ansatz kommt zum Ausdruck in Abläufen, die Anonymität fördern:

- Genehmigungsprozesse sorgen dafür, dass zu keinem Zeitpunkt ein einzelner Mitarbeitender unbegründet Zugriff auf eine Steuerungskomponente nehmen kann; der Zugriff auf die Steuerungskomponente muss von einem Manager genehmigt werden, der nur für diesen Zweck Genehmigungsfunktionen hat, im Übrigen aber mit der zugriffsberechtigten Person nicht zusammenarbeitet. Solche Genehmigungsprozesse fördern auch innerhalb der Teams der Cloud-Anbieterin die Anonymität, so dass Interessenkonflikte und Kollusion zum Nachteil einer bestimmten Kundin minimiert, wenn nicht ausgeschlossen werden.
- Wird einem Mitarbeitenden der Zugriff gewährt, erfolgt dies nur für die Dauer, die der Mitarbeitende für den in der Genehmigungsanfrage angegebenen Grund – der selbstverständlich plausibilisiert werden muss – benötigt. Man spricht von "Just in Time"-Access. Die erteilten Rechte sind limitiert und dem Zweck des Zugriffsgesuchs angemessen ("Just enough"-Access).

[193] Zum Begriff "Basiskomponenten" siehe Anhang 1.

- Im IaaS-Modell wirken nicht nur organisatorische Massnahmen. Eine technische Limitierung der Zugriffsmöglichkeit von Personal der Cloud-Anbieterin resultiert aus der Funktionalität der zentralen Steuerungssoftware. Diese ist dafür da, Softwaresysteme zu aktualisieren. Sie ist aber nicht dazu da, Zugriffe auf Virtuelle Maschinen einzelner Kundinnen zu eröffnen (wozu es andere Systeme benötigt und auch die softwaretechnisch abgebildete Zustimmung der Kundin erforderlich ist).
- Alle Massnahmen werden in Logs protokolliert.

Diese anonymisierte Methodik der Bereitstellung und Verwaltung limitiert gesamthaft die Wahrscheinlichkeit, dass im Normalbetrieb ein Mitarbeitender einer Cloud-Anbieterin auf eine Virtuelle Maschine der Organisationseinheit der Stadt Zürich und die darauf sich befindlichen Daten zugreifen könnte. Die Virtuellen Maschinen sind durch softwaretechnische Massnahmen innerhalb der Virtualisierungsschicht vor unbefugten Zugriffen geschützt.

Die Organisationseinheit der Stadt Zürich ihrerseits ist im IaaS-Ansatz frei, das "Innenleben" der Virtuellen Maschine eigenständig zu definieren: Sie wählt die konkrete Softwarekonfiguration (Betriebssystem und Anwendungssoftware) auf der Virtuellen Maschine aus und definiert die in diesem Rahmen gewünschten Datenmodelle. Verliert die Organisationseinheit der Stadt Zürich die Zugriffsdaten für die Virtuelle Maschine oder für die auf dieser laufenden Applikationen, kann die Cloud-Anbieterin im Hyperscaler-Modell den Kunden nicht unterstützen, um Recovery-Massnahmen einzuleiten. Die Kundin muss diese Massnahmen dann selber treffen.

Ergänzend ist für das IaaS-Modell anzumerken, dass das Gesamtsystem selbstverständlich von der Cloud-Anbieterin koordiniert wird. Die Cloud-Anbieterin stellt den Administratoren der obersten Ebene.[194] Sollte ein Mitarbeitender der Cloud-Anbieterin Zugriff nehmen müssen und bei diesem Zugriff Daten der Kundin einsehen können, muss er über den Administratoren der Kundin berechtigt werden (ein Ablauf, der mittels technischer sowie organisatorischer Massnahmen abgebildet und gesichert wird). Der Administrator der Kundin ist im Gesamtsystem gleichsam der Administrator der zweitobersten Ebene[195] (der situativ von der Kundin zusätzlich freigeschaltete Supportmitarbeitende hätte die Rolle einer kurzfristigen Benutzerin oder subalternen Administratorin auf der dritten Ebene).[196]

Dies ist bei weitem keine vollständige Schilderung eines IaaS-Modells. Die Ausführungen sollen aber aufzeigen, dass je nach Service-Modell und mittels einer Vielzahl von ineinander hineingreifenden Massnahmen technischer und organisatorischer Natur die Wahrscheinlichkeit und in weitgehender Hinsicht auch die Möglichkeit reduziert oder gar ausgeschlossen wird, dass Mitarbeitende im Normalbetrieb auf Virtuelle Maschinen der Kundin und damit auf gespeicherte Daten überhaupt zugreifen können. Durch das dem Hyperscaler-Ansatz inhärente hohe Mass an Automatisierung und Anonymität ergibt sich somit für die Organisationseinheit der Stadt Zürich als Kundin ein natürlicher Schutz gegen unbefugte Klartext-Zugriffe einzelner Mitarbeitender der Cloud-Anbieterin.

Wenn die Cloud-Anbieterin einen derart wirkenden Mix an Massnahmen plausibel zu dokumentieren vermag, kann die Organisationseinheit der Stadt Zürich den Nachweis führen, dass ihre Wahl (z.B. "reines IaaS-Modell") in Verbindung mit den dokumentierten Massnahmen zu einem so verbindlich

[194] Administratorenrolle der obersten Ebene: Dieser Begriff wird aus Gründen der Verständlichkeit verwendet, ist aber aus technischer Sicht ungenau. Es geht eher um eine Aufgabentrennung, bei der die Cloud-Anbieterin die zugrunde liegenden Basiskomponenten verwaltet und mit den virtuellen Maschinen nichts zu tun hat. Der Administrator der Cloud-Anbieterin hätte die Möglichkeit, eine definierte virtuelle Maschine hoch- und herunterzufahren, ohne jedoch Zugriff auf die virtuelle Maschine zu erhalten. Die Möglichkeit, eine virtuelle Maschine herunterzufahren ist auf dringliche Fälle beschränkt, in welchen die betroffene virtuelle Maschine ausserhalb des Normalbetriebs läuft und dieser Zustand Auswirkungen auf die Stabilität der in derselben Umgebung ausgeführten virtuellen Maschinen hätte.

[195] Die Terminologie ist wiederum technisch nicht präzise. Es geht um Segregation. Die Administratoren der Kundin könnten als VM-Administratoren oder IaaS-Administratoren bezeichnet werden.

[196] Soweit die Cloud-Anbieterin aus technischen Gründen, z.B. für das Patching der Softwareschicht gewisse Softwarepakete automatisiert in die Virtuelle Maschine der Kundin verteilen muss, kann dies mittels standardisierten Einträgen in das Berechtigungssystem der Kundin erreicht werden. Man kennt für solche Zugriffe ohne Dateneinsichtnahme z.B. das Konzept des Eligible Admins. Es würde jedoch zu weit gehen, dieses Konzept hier zu vertiefen.

voraussehbaren Schutz gegen unbefugte Zugriffe führt, dass Klartext-Zugriffe im Normalbetrieb der Lösung nach menschlichem Ermessen ausgeschlossen werden können.

Dass die Cloud-Anbieterin Direktzugriff auf die virtuelle Maschine der Kundin nimmt, kann technisch ausgeschlossen werden. Theoretisch betrachtet kann aber nicht ausgeschlossen werden, dass die Cloud-Anbieterin auf die verschlüsselte Speicherdatei[197] für die Virtuelle Maschine zugreift (die Cloud-Anbieterin stellt ja den Administratoren der obersten Ebene). Dass er diese Datei mittels sog. "Brute Force" entschlüsselt, kann technisch gesehen zwar nicht zu hundert Prozent ausgeschlossen werden. Diese Möglichkeit ist jedoch so marginal, dass man sie nicht ernsthaft als realistische Gefahr bezeichnen kann. Da (und soweit) aber technische und organisatorische Massnahmen eingerichtet sind, die sicherstellen, dass ein solcher Zugriff im Normalbetrieb nicht stattfindet, resultiert im IaaS-Modell kein strafrechtlich sanktionierbares Verhalten, wenn eine Organisationseinheit der Stadt Zürich Daten in die IT-Infrastrukturen der Cloud-Anbieterin migriert. Dieser Schluss stellt ab auf die jüngste Rechtsprechung des Bundesgerichts (wonach nur der tatsächliche Zugriff zählt).

2. Analyse bei Nutzung von reinen PaaS-Angeboten

Ein PaaS-Angebot unterscheidet sich von einem IaaS-Angebot dadurch, dass die Kundin die virtuellen Maschinen nicht selber verwaltet. Die Cloud-Anbieterin übernimmt die Verwaltung der virtuellen Maschinen, inklusive Betriebssystem und Plattformsoftware wie Datenbankensoftware und dergleichen, die ebenfalls vollständig durch die Cloud-Anbieterin betrieben werden. Die technischen Basiskomponenten, die für das PaaS-Modell zur Anwendung kommen, unterscheiden sich nicht von jenen, die beim IaaS-Modell eingesetzt werden. Die Bereitstellung wird aber anders aufgesetzt:

- Beim IaaS-Modell "bucht" eine Kundin aus ihrem Tenant heraus gewisse Ressourcen. In der Folge werden diese für die Kundin in deren Berechtigungssystem registriert, und zwar dediziert (mittels logischen Definitionen in Identitätssystemen und Netzwerksystemen). Die Cloud-Anbieterin stellt im Gesamtsystem wie bereits geschildert die Administratorin der obersten Ebene, die Kundin die Administratorin der zweitobersten Ebene.
- Beim PaaS-Modell wird ein Service zuerst im Sinne eines Standardprodukts von der Cloud-Anbieterin aufgesetzt. Damit stellt die Cloud-Anbieterin hier gleichsam auch den Administratoren der zweitobersten Ebene (zusätzlich zum Administratoren der obersten Ebene). Wenn die Kundin aus ihrem Tenant heraus solche Standardprodukte bucht, werden in ihrem Berechtigungssystem Einträge generiert, die mit logischen Methoden sicherstellen, dass die Datenhaltung für das Standardprodukt in eindeutiger Weise und ausschliesslich für sie (und nicht für eine andere Kundin) mit dem Standardprodukt verknüpft wird. Der Administrator der Kundin wird im Gesamtsystem gleichsam der Administrator der drittobersten Ebene. Sollte die Kundin von der Cloud-Anbieterin einen auf ihren Tenant bezogenen, dedizierten Support anfordern, würde der Administrator der Kundin den Supportmitarbeitenden auf die Tenant-Sicht der Kundin freischalten.

Die Nutzungsberechtigung der Kundin (d.h. der Organisationseinheit der Stadt Zürich) ergibt sich somit auch im PaaS-Modell über die Definition des Tenants. Das zentrale Stichwort dafür, wie die Kundin in einer PaaS-Umgebung Kontrolle über ihre Daten behält, lautet "Tenant Isolation" (oder "tenant level isolation" oder dergleichen). Zusätzlich kommen verstärkt organisatorische Massnahmen zum Tragen, um die Datenhaltung der Kundin gegen Zugriffe von Mitarbeitenden der Cloud-Anbieterin zu schützen. In Bezug auf die strafrechtlich entscheidende Frage, ob eine relevante Offenbarung von geheimnisgeschützten Informationen entsteht, ändert sich im Resultat nichts – solange eben im Gesamtsystem genügende Methoden zur Sicherung gegen unbeabsichtigte Zugriffe auf die Datenhaltung der Organisationseinheit der Stadt Zürich nachweisbar sind. Das Fazit zu IaaS kann somit auch auf das PaaS-Modell übertragen werden.

[197] Bei einer virtuellen Maschine werden die Daten in einem spezifischen Format (VHDX, VMDK, etc.) gespeichert und sind technisch gegen Klartext-Zugriffe geschützt.

3. Analyse bei der Nutzung von SaaS-Angeboten ohne Auslandsbezug (oder um SaaS-Komponenten ergänzte IaaS- oder PaaS-Angebote)

Bei einem SaaS-Modell verschiebt sich die Beherrschung des Gesamtsystems noch weiter hin zur Cloud-Anbieterin. Während im IaaS-Modell noch vielfältige Schutzmechanismen greifen, die inhärent technischen Architekturfragen geschuldet sind, entfallen solche technischen Schutzmechanismen in signifikantem Umfang. Mit anderen Worten werden organisatorische Schutzmassnahmen im SaaS-Modell noch wichtiger. Um welche Schutzmechanismen es geht, kann hier nicht abstrakt geschildert werden, weil in SaaS-Modellen die konkreten Wirkmechanismen sehr individuell sein können. Entscheidend ist, dass die Organisationseinheit der Stadt Zürich nach Analyse dieser Wirkmechanismen (die wie gesehen v.a. organisatorischer Natur sein werden) bestätigen kann, dass im Normalbetrieb mit genügender Verlässlichkeit Mitarbeitende der Cloud-Anbieterin nicht unbefugten Klartext-Zugriff auf geschützte Informationen der Organisationseinheit der Stadt Zürich nehmen werden.

* * *

Anhang 3: Zum Cloud-Merkblatt der Kantonalen Datenschutzbeauftragten

A. Vorbemerkungen

1 Die Datenschutzstelle des Kantons Zürich (www.datenschutz.ch) hat ein Merkblatt[198] für die öffentlichen Organe des Kantons Zürich erlassen, das ihnen Empfehlungen rund um den Einsatz des Cloud-Computings abgibt. Auf fünf Seiten schildert die kantonale Datenschutzstelle, was Cloud Computing ist und wie die Risikoanalyse bei der Cloud-Anbieterauswahl erfolgen sollte. Nach diesem Überblick erfolgt eine Schwerpunktsetzung auf das Vertragsverhältnis zwischen dem auslagernden Organ und der Cloud-Anbieterin. Da das auslagernde Organ auch bei einer Auslagerung verantwortlich bleibt, muss die Vertragsgestaltung derart erfolgen, dass das Organ diese Verantwortung auch weiterhin, d.h. auch nach einer Auslagerung, wahrnehmen kann. Dies betrifft beispielsweise die Verankerung von Kontrollrechten des Organs sowie die Gewährleistung der Betroffenenrechte sowie organisatorischer und technischer Schutzmassnahmen. Zuletzt wird im Cloud-Merkblatt angemerkt, dass das öffentliche Organ die Umsetzung der vertraglichen Rahmenbedingungen laufend überprüfen sollte.

2 Im Cloud-Merkblatt werden teilweise Massnahmen angeregt oder Voraussetzungen postuliert, die über das kantonalzürcherische Gesetzes- und Verordnungsrecht hinausgehen. Dies soll im vorliegenden Anhang 3 identifiziert werden, um diese Themen einer Diskussion zuführen zu können, damit abweichende Auffassungen einheitlich bereinigt werden können. Denkbar ist somit, dass die Ausführungen in diesem Anhang 3 über Zeit revidiert werden müssen, um dem fortgesetzten Gespräch Rechnung zu tragen.[199]

B. Zum Thema Datenschutzaudit

3 Das Cloud-Merkblatt (S. 3) sieht namentlich die folgenden weitergehenden Massnahmen vor:

4 **Kontrollmöglichkeiten vor Ort:** Dass es eine Kontrollmöglichkeit «vor Ort» geben soll, wird weder von § 35 IDG noch von der IDV gefordert. Eine solche Regelung wäre auch nicht sachgerecht, da es ihr einerseits an der Erforderlichkeit fehlt (es bestehen mildere Möglichkeiten wie Revisionsberichte der Prüfstelle des Providers), andererseits auch an der Geeignetheit. In der Tat gibt der Augenschein im Sinne des physischen Betretens eines Rechenzentrums nur über physische Kontrollen Aufschluss, nicht aber über die – deutlich wichtigeren – Massnahmen zum Schutz vor Zugriffen auf der sog. logischen Ebene (z.B. Netzwerkzugriff). Zur Überprüfung der logischen Sicherheit sind insofern über Distanz vorgenommene Prüfzugriffe (mit mehr oder weniger weit reichenden Sonderrechten) sowie das Studium von Konzeptdokumenten mit anschliessender Plausibilisierung geeignetere Lösungen. Darüber hinaus hätte das Erfordernis des «Vor-Ort-Audits» die Wirkung, dass Organisationseinheiten (z.B. der Stadt Zürich) nurmehr kleinere Anbieterinnen wählen und womöglich mit der Wahl von Hyperscalern Schwierigkeiten bekommen könnten, weswegen das Cloud-Merkblatt des Kantons Zürich diesbezüglich kritisch hinterfragt werden darf.

5 **Kontrollen nach internationalen Audit-Standards:** Gemäss Merkblatt muss die Organisationseinheit der Stadt Zürich den von ihr gewählten Cloud-Anbieter verpflichten, regelmässig Kontrollen nach internationalen Audit-Standards durchführen zu lassen. Es kann durchaus sinnvoll sein, solche Kontrollen

[198] Das Merkblatt ist hier abrufbar: www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/datenschutz/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf (angesehen am 20. August 2021).

[199] Die Gutachter verweisen an dieser Stelle auf den Umstand, dass sie auch schon Cloud-Anbieterinnen beraten haben und sich in diesem Zusammenhang zum hier diskutierten Cloud-Merkblatt geäussert haben. Hier vertretene Aussagen können so wirken, als ob sie im Interesse einer Cloud-Anbieterin formuliert wurden. Das ändert allerdings nichts daran, dass vorliegend eine abstrakte juristische Analyse angelegt werden muss. Wo eine Anforderung einer kantonalen Datenschutzstelle im Gesetz keine Stütze findet, darf sie der Stadt Zürich nicht als Vorgabe auferlegt werden. Die Handlungsfreiheit der Stadt Zürich würde ansonsten unverhältnismässig stark beeinträchtigt. Ausserdem stünde ein Merkblatt mit überschiessenden Vorgaben im Widerspruch zum Gebot, sich ans Gesetz gebunden zu sehen (Art. 3 der Kantonsverfassung). Entsprechend ist sorgfältig zu klären, inwiefern Vorgaben im Cloud-Merkblatt gerechtfertigt sind oder nicht.

(z.B. nach ISAE-Standards) vorzuschreiben. Generell muss sich das Vorgehen der Organisationseinheit aber an Kriterien der Verhältnismässigkeit messen lassen. So kann es durchaus sein, dass bei erhöhtem Schutzbedarf eine erhöhte Prüfpflicht verlangt werden darf und sollte. Der Verweis auf das Verhältnismässigkeitsprinzip bringt zum Ausdruck, welche Regel gelten wird: Es bedarf einer Angemessenheitsprüfung im Einzelfall, weshalb die pauschale Empfehlung der Kontrollen nach internationalen Audit-Standards in dieser Absolutheit abzulehnen ist.

C. In Bezug auf die Unterauftragsverhältnisse

6 Das Cloud-Merkblatt (S. 4) sieht in Bezug auf Unterauftragsverhältnisse die folgenden Massnahmen vor:

1. **Unterauftragsverhältnisse** müssen vor Vertragsabschluss offengelegt werden.

2. Die Unter-Auftragnehmer müssen verpflichtet werden, **Weisungen** des Cloud-Anbieters zu beachten.

3. **Nachträgliche Vereinbarungen** dürfen nur mit Kenntnis und Zustimmung des öffentlichen Organs unterzeichnet werden.

7 Generell ist festzuhalten, dass sowohl das IDG als auch die IDV nur Bestimmungen zur Auftragsbearbeitung kennen (§ 6 IDG, § 25 IDV). Die Konstellation, dass ein Unter-Auftragsbearbeiter beigezogen wird (sog. Unterauftragsverhältnis), ist darin also nicht geregelt. Dies ändert jedoch nichts daran, dass das öffentliche Organ nach § 6 Abs. 2 IDG für den Umgang mit Informationen nach dem IDG verantwortlich bleibt. Folglich ist das öffentliche Organ nicht nur für die Einhaltung der Datenschutzbestimmungen durch den Auftragsbearbeiter verantwortlich, sondern auch für deren Einhaltung durch den Unter-Auftragsbearbeiter.

8 Die drei oben aufgeführten Massnahmen, die aus dem Cloud-Merkblatt stammen, haben allesamt zum Ziel, dass das öffentliche Organ seiner Verantwortlichkeit nachkommen kann. Insofern sind dies Massnahmen, die im Interesse des öffentlichen Organs und letztlich der betroffenen Person liegen – und deshalb sinnvoll erscheinen. Zudem bestehen in Bezug auf die Verhältnismässigkeit der in Rz. 6 Punkt 1, Punkt 2 und zum Teil (soweit es um Kenntnis geht) in Punkt 3 genannten Anforderungen kaum Zweifel, da das öffentliche Organ erstens von den Unter-Auftragsbearbeitungen wissen können muss (vor und nach Vertragsschluss) und zweitens der Cloud-Anbieter dem Unter-Auftragsbearbeiter sinnvollerweise, da er näher an ihm dran ist, Weisungen erteilen können muss. Andernfalls wird es für das öffentliche Organ nicht oder nur schwer möglich sein, seiner Verantwortung nachkommen zu können.

9 Die Anforderung, dass neue Unterauftragnehmende nur mit vorgängiger Zustimmung der Organisationseinheit der Stadt Zürich beigezogen werden können sollen (Rz. 6, Punkt 3), sollte die Organisationseinheit der Stadt Zürich demgegenüber eher nicht bzw. nicht um jeden Preis durchsetzen. Ein Vetorecht erscheint nicht ohne Weiteres erforderlich, da alternative Lösungswege offen stehen (Meldung mit Kündigungsrecht, allenfalls könnten solche milderen Gestaltungsformen mit Übergangszeiten oder Moratorien verknüpft werden). Insofern ist diesbezüglich die Verhältnismässigkeit kritisch zu betrachten, zumal bei Cloud-Angeboten in einer typischen Situation eine grosse Vielzahl von Kundinnen involviert sind. Würde die Stadt Zürich das Veto-Recht als Standard etabliert sehen wollen, müsste ein solches Veto-Recht konzeptionell auch anderen Kundinnen offen stehen. Dies könnte dazu führen, dass Innovationen (aufgrund des Vetos anderer Kundinnen) verhindert werden, was dem eigentlichen Ziel der Stadt Zürich (Informationsschutz) zuwiderlaufen könnte. Einer solchen Gefährdungssituation sollte die Stadt Zürich nicht Vorschub leisten.

D. In Bezug auf das anwendbare Recht und Gerichtsstand

10 Das Cloud-Merkblatt (S. 4) sieht zudem die folgenden weitergehenden Massnahmen vor:

1. Es muss **Schweizer Recht** (insb. das IDG) anwendbar sein.

2. Es muss ein **Gerichtsstand in der Schweiz** vereinbart werden.

11 Weder zum anwendbaren Recht noch zum Gerichtsstand ist dem IDG oder IDV eine gesetzliche Bestimmung zu entnehmen. Die vom Cloud-Merkblatt geforderten Massnahmen sind überschiessend. Zudem hängt der Schutz der betroffenen Personen nicht damit zusammen, dass Schweizer Recht anwendbar oder ein Schweizer Gerichtsstand vereinbart ist, da insbesondere auch ausländische Staaten bzw. ihr Recht (und Gerichtsstand) ein gleichwertiges Datenschutzniveau wie die Schweiz aufweisen können. Folglich ist diese vom Cloud-Merkblatt vorgeschlagene Massnahme unverhältnismässig und nur mit Zurückhaltung anzuwenden.

12 Das IDG ist direkt anwendbar für die Organisationseinheiten der Stadt Zürich. Diese müssen dafür sorgen, dass sie keine Verträge eingehen, welche dazu führen, dass sie die Vorgaben im IDG nicht einhalten können. Auf den Vertrag zwischen der Cloud-Anbieterin und der Stadt Zürich kommen jedoch nur die Bestimmungen des eidgenössischen Rechts (Obligationenrecht) zur Anwendung, soweit dieses im Vertrag nicht zulässigerweise durch ein ausländisches Vertragsstatut ersetzt wurde.

13 Wenn im Cloud-Merkblatt nun schweizerisches Recht und ein Gerichtsstand in der Schweiz gefordert wird, hat dies auf der Kostenseite für die Organisationseinheiten der Stadt Zürich durchaus eine Bedeutung (mutmasslich ist die Rechtsverfolgung vor schweizerischen Gerichten für eine schweizerische Behörde weniger teuer und weniger umständlich als wenn Rechtsanwaltskanzleien im Ausland beauftragt werden müssten). Wenn man die Anforderungen so versteht, können sie aus vergaberechtlicher Sicht im Rahmen eines Zuschlagsentscheids durchaus von Bedeutung werden (im Rahmen von Zuschlagskriterien und somit bei der Bewertung eines Angebots). Die Anforderungen sind jedoch aus datenschutzrechtlicher Sicht nicht notwendig. Dass ein inländisches Vertragsstatut die im Rechtsgutachten diskutierten Fragen für eine Organisationseinheit der Stadt Zürich positiv beeinflussen würde, ist nicht ersichtlich.

E. In Bezug auf die Datensicherheit

14 Im Cloud Merkblatt werden vertragliche Regelungen zur Stützung der Datensicherheit empfohlen. Es sieht namentlich die folgenden weitergehenden Massnahmen vor (S. 4):

15 **Managementsystem für Informationssicherheit**: Nach dem Cloud-Merkblatt muss der Cloud-Anbieter beim Bearbeiten von *besonderen Personendaten* die organisatorischen und technischen Massnahmen in einem Managementsystem für Informationssicherheit verwalten. Was darunter genau zu verstehen ist, kann man nicht erkennen. Richtig ist sicherlich, dass der Cloud-Anbieter auch bei besonderen Personendaten ein hohes Mass an Sicherheit walten lassen muss. Allerdings scheint die Vorgabe eines spezifischen Managementsystems etwas formal. Zumal eine gesetzliche Grundlage hierfür fehlt, sollten Organisationseinheiten der Stadt Zürich diese Vorgabe zurückhaltend anwenden. Gleichwohl sollten sie nicht aus den Augen verlieren, dass sie für besondere Personendaten einen angemessenen Schutz erreichen sollen. In der Stadt Zürich ist hierfür das Handbuch Informationssicherheit (HISi) massgeblich.

16 **Massnahmen zur Umsetzung der Interoperabilität**: Das Cloud-Merkblatt empfiehlt Massnahmen, welche die Interoperabilität gewährleisten. Dies sei im Vertrag zu regeln. Diese Empfehlung findet keine rechtliche Grundlage im zürcherischen Datenschutzrecht.[200]

17 In Bezug auf die soeben geschilderten Vorgaben zum Managementsystem und zur Interoperabilität sollte aus datenschutzrechtlicher Sicht Zurückhaltung angewendet werden.

* * *

[200] Die Gutachter sehen diese Anforderung als absolut erwünscht und auch nicht unsachlich an. Diese Vorgabe motiviert sich jedoch nicht aus dem Datenschutzrecht, sondern ist aus anderen Gründen sinnvoll (finanzielle Nachhaltigkeit der gewählten Lösung sowie beschaffungsrechtliche Nachhaltigkeit).

Christian Laux
Dr. iur., LL.M., Rechtsanwalt, Senior Advisor
christian.laux@lauxlawyers.ch

LAUX LAWYERS AG
ZURICH | BASEL

V03 | 3. November 2021

Fact Sheet zum Anwendbaren Recht

A. Sachverhalt

1 Es ist langjährige Praxis der Stadt Zürich, für den Betrieb von IT-Infrastrukturen Dritte einzubinden. Künftig sollen auch Cloud-Anbieterinnen solche IT-Infrastrukturen bereitstellen. Die Stadt Zürich hat dazu ein Rechtsgutachten in Auftrag gegeben. Ergänzend zu diesem sollen verschiedene Einzelfragen detailliert diskutiert werden.

2 Mit der vorliegenden Detailbetrachtung wird untersucht, welchem Recht[1] die Vertragsbeziehung zwischen der Cloud-Kundin und der Cloud-Anbieterin unterstehen muss.

B. Zum Diskussionsstand

1 Die schweizerischen Gerichte haben sich mit dieser Frage soweit ersichtlich noch nicht beschäftigt. In der Lehre ist das Kriterium umstritten[2] bzw. wird nicht einheitlich[3] diskutiert. Soweit das Postulat nach schweizerischem Recht begründet wird, kommt Folgendes zum Ausdruck: Zu schützen sei – im Interesse des Informationsschutzes – vor dem Risiko, dass ausländisches Recht der Vertragsregel vorgehe; und ob dem so sei, sei eine Frage des *Vertragsstatuts*. Die ablehnende Haltung verneint dies.

2 Ziffer 18 der kantonalzürcherischen Allgemeinen Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen (AGB Auslagerung Informatikleistungen) hat die Forderung nach schweizerischem Vertragsstatut aber aufgegriffen und stellt die folgende Regelung auf: «Es gilt das im Vertrag vereinbarte schweizerische Recht.»[4] Die AGB Auslagerung Informatikleistungen wurden am 24. Juni 2015 vom Regierungsrat des Kantons Zürich erlassen. Sie haben in einem Vertrag Geltung, wenn der Vertrag die AGB in verbindlicher Weise zum Vertragsinhalt erklärt. Wie häufig die AGB Auslagerung Informatikleistungen eingesetzt werden, ist nicht bekannt.[5]

---

[1] Gemeint ist das Vertragsstatut, d.h. das Recht, nach welchem Ansprüche unter dem Vertrag zwischen der Behörde und der Cloud-Anbieterin beurteilt werden.

[2] **Ablehnend** David Rosenthal, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter 10. August 2020 N 116: «So trifft es z.B. nicht wie von kantonalen Datenschützern mitunter vertreten zu, dass nebst Verschlüsselung zwingend Schweizer Recht als Vertragsstatut und ein Schweizer Gerichtsstand nötig ist, um sich angemessen zu schützen. Ersteres hat zwar einen Effekt, doch darf dieser nicht überbewertet werden»; gl.M. Thomas Steiner, Digitaler Arztbesuch und Cloud-Nutzung im Lichte des Datenschutzrechts des Bundes und der Kantone, sic! 2020 677 ff., 684; ablehnend auch der Leitfaden «Öffentliche Auftragsvergabe» der euroCloud Swiss, Ziff. 5.4. Womöglich (aber nicht eindeutig) **bejahend** Ursula Widmer, Nutzung von Cloud Lösungen – Rechtliche Rahmenbedingungen für Behörden, Vortragsslides zu einem Vortrag an der Tagung für Informatik und Recht vom 12. November 2018 (abrufbar unter https://rechtsinformatik.ch/wp-content/uploads/2018/11/04_18-Widmer-Cloud-Behoerden_2018-11-12.pdf; angesehen am 11. Oktober 2021), Slide 21.

[3] «Schweizer Recht» als Vertragsstatut wird auch von privatim im überarbeiteten privatim-Merkblatt «Cloud-spezifische Risiken und Massnahmen» vom 17. Dezember 2019 gefordert: https://www.privatim.ch/de/uberarbeitetes-privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen (angesehen am 11. Oktober 2021): Ausnahmsweise könne «[d]ie Anwendbarkeit des Rechts eines anderen Staates … vereinbart werden, wenn die Daten durch Verschlüsselung wirksam vor dem Zugriff durch Dritte (sowie den Anbieter der Cloud-Dienstleistung) geschützt werden können». Im Anhang zum bereits (in FN 2) genannten Aufsatz (Anhang mit dem Titel «Ausländischer Lawful Access: Wahrscheinlichkeitsbeurteilung und Gegenmassnahmen im Detail», Jusletter 10. August 2020 N 79) weicht Rosenthal seine ablehnende Haltung auf: «Untersteht der Vertrag ausländischem Vertragsrecht, sieht dieses *möglicherweise* automatisch einen Vorbehalt zugunsten von Herausgabeanordnungen des betreffenden ausländischen Rechts vor.» (Hervorhebung nicht im Original) Anzumerken ist, dass diese Formulierung hypothetisch gehalten ist.

[4] https://www.zh.ch/content/dam/zhweb/bilder-dokumente/organisation/finanzdirektion/afi/agb_auslagerung_informatikleistungen.pdf

[5] Der Regierungsrat des Kantons Zürich hat auch noch die sog. AGB Datenbearbeitung durch Dritte erlassen (ebenfalls am 24. Juni 2015: https://www.zh.ch/content/dam/zhweb/bilder-dokumente/organisation/finanzdirektion/afi/agb_datenbearbeitung_durch_dritte.pdf). Diese beziehen sich aber nicht auf die Nutzung von Informatikmitteln, sondern darauf, dass die beigezogene Dritte den eigentlichen Informationsgehalt bearbeiten muss (was Klartextzugriff zwingend voraussetzt, da die Dritte auf dem sog. «Content Layer» arbeiten muss). Ziffer 1 der AGB Datenbearbeitung durch Dritte beschreiben den Einsatzbereich der Datenbearbeitung (für welche die AGB Datenbearbeitung durch Dritte gelten soll) wie folgt: «Diese AGB gelten für Vertragsverhältnisse, im Rahmen derer die Bearbeitung von Informationen für das öffentliche Organ zentraler Bestandteil, respektive der Hauptzweck des Auftrages ist. Beispiel: Mandatierung eines Anwalts zur Ausformulierung eines Beschlusses, Übertragen des Inkassos an ein Inkassounternehmen».

C. Positionsbezug

3 Im Behördenumfeld ist die Diskussion im Lichte des Informations- bzw. Datenschutzes von Bedeutung. Konkrete Gründe für das Postulat nach Schweizer Recht werden aber in der Diskussion nicht genannt.

4 Im *reinen Binnenverhältnis* ist die Rechtsanwendung einfacher als bei Vorliegen von internationalen Bezügen. Mit «reinem Binnenverhältnis» ist Folgendes gemeint: Es besteht ein Vertrag zwischen einer schweizerischen Cloud-Anbieterin und einer schweizerischen Behörde in Bezug auf die Nutzung eines Angebots, das aus schweizerischen Rechenzentren heraus erbracht wird. Wenn die Cloud-Anbieterin sich einem Herausgabebefehl einer schweizerischen Behörde konfrontiert sieht, gelten ohne Weiteres Art. 19 Abs. 2 OR bzw. Art. 20 Abs. 1 OR (eine Vertragspflicht, sich der rechtmässig erlassenen Behördenanordnung zu widersetzen, wäre nicht durchsetzbar) und Art. 14 StGB (wer der Behördenanordnung nachgibt, macht sich nicht nach Art. 320 und Art. 321 StGB strafbar). Dass zwingendes (schweizerisches) öffentliches Recht im Sinne der Einheit der Rechtsordnung eine Vertragspflicht wirksam übersteuern kann (z.B. Art. 119 OR), ist etabliert.

5 Im *umfassend internationalen Sachverhalt* (schweizerische Behörde und ausländische Cloud-Anbieterin) geht der im reinen Binnenverhältnis als intuitiv naheliegend erscheinende Gleichschritt des öffentlichen Rechts mit dem Vertragsstatut verloren. Das IPRG stellt Regeln auf, die mit dem Verwaltungs- und Strafrecht nicht interferieren sollen oder wollen.[6] Mit anderen Worten: Verwaltungs- und Strafrecht gehen dem Privatrecht vor. Dies führt zu verschiedenen Ableitungen, die wie folgt festzuhalten sind:

a) Selbst wenn schweizerisches Recht zum Vertragsstatut gemacht würde, könnte es nicht die sog. Eingriffsnormen («lois de police» oder «lois d'application immédiate») eines anderen Staates übersteuern; diese würden den Regeln des Vertragsstatuts vorgehen. Würde die schweizerische Rechtsordnung eine öffentlich-rechtlich wirkende und motivierte Rechtsregel der fremden Rechtsordnung übersteuern, obwohl diese eine viel stärkere Nähe zum Sachverhalt[7] hat, würde der schweizerische Entscheid im betreffenden Ausland nicht durchgesetzt werden.[8] Zwischenfazit: Das Vertragsstatut ist nicht massgeblich.

b) Wenn der Vertrag auf ein ausländisches Vertragsstatut verweist, bedeutet dies nicht, dass alle Regeln der fremden Rechtsordnung automatisch auch zur Anwendung gelangen.[9] Andernfalls würde dem ausländischen öffentlichen Recht (im fremden Forum) eine schematisch wirkende und möglicherweise extraterritoriale Wirkung zugebilligt, die es im Einzelfall allenfalls weder haben soll noch will.[10] Zwischenfazit also auch hier: Das Vertragsstatut ist nicht massgeblich.

6 Die lois de police (Eingriffsnormen) haben somit ihren eigenen, vom internationalen Privatrecht unabhängigen Geltungs- und Anwendungsbereich.[11] Kurz: Das Eingriffsrecht des ausländischen Staats (z.B. von Irland) gilt[12] ungeachtet dessen, ob die Parteien schweizerisches Recht wählen oder ausländisches Recht (z.B. irisches Recht).

---

[6] Frank Vischer, General Course on Private International Law, 232 RECUEIL DES COURS 9, Den Haag 1992, 150 ff. (zit. General Course): «The penal or administrative sanctions are not the concern of private international law.»

[7] Nähe zum Sachverhalt oder «proximity» lässt sich nicht trennscharf definieren. Siehe auch Vischer (General Course), 183, zur Diskussion, dass ausländisches öffentliches Recht im Interesse des ausländischen Staats erlassen wurde (also rein öffentlich-rechtlicher Natur ist) oder auch privatrechtliche Aspekte aufweist: «It is hardly possible to determine clear cut criteria which in each case enable the qualification of the rules in question.», und in 184: «There will always be a grey zone.».

[8] Siehe dazu z.B. Vischer (General Course), 178: « There is hardly a domain of civil law which is immune to the impact of foreign public enactments. Certainly, some fields are especially prone to foreign States' interference. The law of contracts is one, company law another example. If for instance the law governing the corporation is the law of incorporation, compulsory enactments of the law in force at the actual seat cannot be ignored, particularly because the State of the seat normally has the power to enforce its laws.»

[9] Jedenfalls ist die Frage (Schuldstatuttheorie, Einheitsanknüpfung) umstritten, siehe dazu Frank Vischer / Corinne Widmer Lüchinger, Zürcher Kommentar zum IPRG - Band I - Art. 1-108, 3. Auflage, Zürich 2018, IPRG 19 N 7. Zur Diskussion auch Vischer (General Course), 178 ff.

[10] Vischer (General Course), 183. Das Bundesgericht hat in BGE 80 II 53 – Royal Dutch Hinweise gegeben, wann eine Regel des öffentlichen Rechts nicht als extraterritoriale Wirkung von staatlicher Regelungsgewalt zu verstehen ist, sondern als Gegenstand einer Rechtswahl oder des Vertragsstatuts (Zweck der Regelung: Schutz von Privatinteressen oder Schutz von «egoistischen» Interessen des betreffenden Staats).

[11] ZK-Vischer / Widmer Lüchinger, IPRG 19 N 1.

[12] Dies gilt, obwohl ausländisches Recht kein Grund für Widerrechtlichkeit nach Art. 20 Abs. 1 OR sein kann (dazu Andreas Furrer / Markus Müller-Chen, Obligationenrecht, Zürich 2018, 151 ff., 5. Kapitel Rz. 80).

7 Cloud-Sachverhalte sind zwar oft vielschichtiger als «reine Binnensachverhalte» oder «umfassend internationale Sachverhalte», wobei die Ausgangslage gerade für die oft ausländisch beherrschten oder einer ausländisch beherrschten Gruppe angehörenden Hyperscaler nicht immer dieselbe ist (die vertragsschliessende Partei ist mal im Ausland und mal in der Schweiz, die Datenhaltung kann im Ausland sein oder in der Schweiz, die Behördenanordnung ergeht in der Schweiz oder im Ausland, etc.). *Dass das ausländische Eingriffsrecht weiterhin reale Wirkungen hat (wie im Fazit in Rz. 5 ausgedrückt), gilt aber stets.*

8 Hintergrund ist die allgemeine Tendenz im internationalen Privatrecht, die in einem US-amerikanischen Entscheid vom Gericht[13] wie folgt zum Ausdruck gekommen ist:

> *When foreign nations are involved, however, it is unwise to ignore the fact that foreign policy, reciprocity, comity and limitations of judicial powers are considerations that should have a bearing on the decision to exercise or to decline jurisdiction.*

Dies gilt jedenfalls immer dann, wenn der schweizerische Entscheid im Ausland vollstreckt werden müsste (z.B. wenn die Vertragspartei Sitz im Ausland hat).

9 Vor diesem Hintergrund verbleibt noch die Diskussion, wie sich eine ausländische Behördenanordnung auf Vertragspflichten und – bei unterstellter Verletzung – auf die *vertragliche Haftung* auswirken würde:

a) *Bei ausdrücklicher Regelung*: Nach Art. 97 ff. OR (also unter der Geltung des schweizerischen Rechts) können die Parteien vertraglich jedenfalls ausdrücklich vereinbaren, dass Behördenanordnungen nach ausländischem Recht keine Vertragsverletzung darstellen (Art. 19 Abs. 1 OR). Mit anderen Worten ist mit der Anwendbarkeit des schweizerischen Rechts in Fällen, in denen sich der Vertrag zum Szenario des Behördenzugriffs im Ausland explizit äussert, nichts «gewonnen».

b) *Bei Fehlen einer Regelung*: Dass ein Gericht in Anwendung schweizerischen Rechts eine vertragliche Haftung für das hier massgebliche Szenario[14] bei vertraglichem Schweigen[15] feststellen würde, ist ebenfalls nicht gesagt. Selbst wenn das schweizerische Gericht (bei Anwendbarkeit des schweizerischen Rechts) nach der Schuldstatuttheorie[16] entscheiden würde, würde es im Rahmen der Prüfung z.B. nach Art. 97 OR den im Ausland entstehenden Zwang immer noch unter den Stichworten der *unverschuldeten Unmöglichkeit* oder *Unzumutbarkeit der Erfüllung* behandeln können[17] und würde dies wohl auch so handhaben[18], zumal dies auch der Wertung z.B. in Art. 9 Abs. 3 der Rom I-Verordnung entspricht.[19] Dies läuft im Resultat auch bei vertraglichem Schweigen auf eine wirksame Berücksichtigung der im Ausland geltenden öffentlich-rechtlichen Regel ((«lois de police», d.h. der ausländischen behördlichen Anordnung) hinaus, sogar bei schweizerischem Vertragsstatut. Die ausländische, hoheitlich motivierte Regelung (Behördenanordnung) wird so oder so relevant. Wiederum: Das Vertragsstatut leistet keinen Beitrag zur Lösung.

10 <u>Zwischenresultat</u>: Dass das Vertragsstatut für den massgeblichen Vorgang (Behördenzugriffe) von besonderer Relevanz wäre, ist nicht ersichtlich. Zur Erinnerung: Anlass der Diskussion ist für Behörden das Anliegen, (Personen-)Daten wirksam zu schützen. Die Ausführungen haben aber gezeigt, dass die Frage des auf den Vertrag anwendbaren Schuldrechts keinen wirksamen Beitrag für den faktischen Schutz von Daten oder Geheimnissen leistet. Es wäre damit zufolge mangelnder Geeignetheit verwaltungsrechtlich unzulässig, die behördliche Cloud-Nutzung unter einem ausländischen Vertragsstatut als widerrechtlich zu bezeichnen. Schweizerisches Vertragsstatut ist keine *conditio sine qua non*.

[13] United States Court of Appeals, Third Circuit, 595 F. 2d at 1296 – Mannington.

[14] Ausländische Behördenanordnung betreffend Herausgabe von Daten, in Konflikt zu einer vertraglich vereinbarten Geheimhaltungsverpflichtung.

[15] Wenn der Vertrag sich nicht dazu äussert, ob auch der Behördenzugriff im Ausland als Rechtfertigungsgrund oder Verschuldensausschluss gilt.

[16] Dazu FN 9.

[17] ZK-Vischer/Widmer, IPRG 19 N 11.

[18] Berücksichtigung einer ausländischen Regel z.B. im Entscheid 4C.172/2000 des Bundesgerichts vom 28. März 2001 - Beverly Overseas SA, E. 5f, zit. in Vischer/Widmer, IPRG 19 N 12.

[19] Relevant wäre hier z.B. die *lex loci solutionis* (Recht am Erfüllungsort), wobei als Erfüllungsort in diesem Sinn das Ausführen von Datenverarbeitungsvorgängen im Rechenzentrum mit Standort im Ausland wäre. Siehe auch Art 7 Abs. 1 des Europäischen Schuldrechtsübereinkommens.

11 Anknüpfende Klarstellung: Was mit den vorstehenden Ausführungen nicht gesagt ist: Ob das gewählte Vertragsrecht an irgendeiner Stelle eine Schwäche aufweist, welche eine nachteilige Wirkung auf die Bearbeitung und den Schutz von (Personen-)Daten hat. Sollte das anwendbare Vertragsrecht eine Regel enthalten, die sich nachteilig auf den Schutz von (Personen-)Daten auswirkt (Relevanz), muss in einem zweiten Schritt eine Risikoabwägung vorgenommen werden. Die identifizierten Risiken sind angemessen zu mitigieren, wobei diesbezüglich eine Vielzahl möglicher Massnahmen (nicht nur solche auf vertraglicher Ebene zur Verfügung stehen). Ist eine Risikominderung nicht in einem Umfang möglich, der das Risiko vertretbar werden lässt, könnte dies so weit führen, dass sogar von der Wahl der entsprechenden Cloud-Anbieterin abzusehen ist.

12 Ergänzende Anmerkung: Der schematische Schluss, dass im Fall, dass eine Mitigierung eines Vertrags unter ausländischem Recht nicht möglich sein sollte, stattdessen schweizerisches Recht zu wählen wäre, kann wohl in dieser Abstraktheit nicht zulässig sein. Das Schweizerische Recht weist gerade im Cloud-Kontext einige Unschärfen auf, die vielleicht nach einem ausländischen Vertragsrecht nicht bestehen würden. Man muss also aufpassen, dass nicht das eine Risiko durch ein anderes ausgetauscht wird, nur weil man «schematisch» oder «abstrakt» ans schweizerische Recht gewohnt ist.

* * *

Christian Laux
Dr. iur., LL.M., Rechtsanwalt, Senior Advisor
christian.laux@lauxlawyers.ch

LAUX LAWYERS AG
ZURICH | BASEL

V02 | 29. Oktober 2021

Fact Sheet zum Gerichtsstand

A. Sachverhalt

1 Es ist langjährige Praxis der Stadt Zürich, für den Betrieb von IT-Infrastrukturen Dritte einzubinden. Künftig sollen auch Cloud-Anbieterinnen solche IT-Infrastrukturen bereitstellen. Die Stadt Zürich hat dazu ein Rechtsgutachten in Auftrag gegeben. Ergänzend zu diesem sollen verschiedene Einzelfragen detailliert diskutiert werden.

2 Mit der vorliegenden Detailbetrachtung wird untersucht, ob der Vertrag zwischen der Cloud-Kundin und der Cloud-Anbieterin für Streitigkeiten einen Gerichtsstand in der Schweiz vorsehen muss.

B. Zum Diskussionsstand

3 In der Lehre ist das Kriterium umstritten[1] bzw. wird nicht einheitlich[2] diskutiert. Die schweizerischen Gerichte haben sich mit dieser Frage soweit ersichtlich noch nicht beschäftigt.

4 Soweit die Forderung nach einem Gerichtsstand in der Lehre aufgegriffen wird, geschieht dies im Wesentlichen ohne Begründung. Im Leitfaden «Öffentliche Auftragsvergabe» der euroCloud Swiss aus dem Jahr 2013 wurde wie folgt begründet, warum ein Gerichtsstand Schweiz nicht verlangt werden müsse: (a) Man müsse spätestens bei der Durchsetzung doch vor ein ausländisches Gericht gelangen und (b) könne den ausländischen Gerichtsstand auch für vorsorgliche Massnahmen nicht ausschliessen.[3] Verwaltungsrechtlich gesprochen fehlt es dem Erfordernis nach einem schweizerischen Gerichtsstand gemäss dem Leitfaden an der Eignung. Eine solche Vorgabe wäre somit nicht verhältnismässig.

5 Ziffer 19 der kantonalzürcherischen Allgemeinen Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen (AGB Auslagerung Informatikleistungen) hat die Forderung aber aufgegriffen und die folgende Regelung aufgestellt: «Es gilt der Gerichtsstand des öffentlichen Organs.»[4] Die AGB Auslagerung Informatikleistungen wurden am 24. Juni 2015 vom Regierungsrat des Kantons Zürich erlassen. Sie haben in einem Vertrag Geltung, wenn der Vertrag die AGB in verbindlicher Weise zum Vertragsinhalt erklärt.[5] Statistische Angaben über die Verwendung der AGB Auslagerung Informatikleistungen im Cloud-Kontext sind nicht bekannt.

---

[1] Ablehnend David Rosenthal, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter 10. August 2020, N 116; womöglich (aber nicht eindeutig) bejahend Ursula Widmer, Nutzung von Cloud Lösungen – Rechtliche Rahmenbedingungen für Behörden, Vortragsslides zu einem Vortrag an der Tagung für Informatik und Recht vom 12. November 2018 (abrufbar unter https://rechtsinformatik.ch/wp-content/uploads/2018/11/04_18-Widmer-Cloud-Behoerden_2018-11-12.pdf; angesehen am 11. Oktober 2021), Slide 21.

[2] Gerichtsstand Schweiz wird von privatim im überarbeiteten privatim-Merkblatt «Cloud-spezifische Risiken und Massnahmen» vom 17. Dezember 2019 gefordert: https://www.privatim.ch/de/uberarbeitetes-privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen (angesehen am 11. Oktober 2021): Ausnahmsweise kann «ein ausländischer Gerichtsstand … vereinbart werden, wenn die Daten durch Verschlüsselung wirksam vor dem Zugriff durch Dritte (sowie den Anbieter der Cloud-Dienstleistung) geschützt werden können».

[3] Der Leitfaden «Öffentliche Auftragsvergabe» war lange Zeit unter https://eurocloudswiss.ch/index.php/publikationen/leitfaden abrufbar, was heute jedoch nicht mehr der Fall ist. Die Publikation liegt dem Verfasser vor.

[4] https://www.zh.ch/content/dam/zhweb/bilder-dokumente/organisation/finanzdirektion/afi/agb_auslagerung_informatikleistungen.pdf

[5] Der Regierungsrat hat auch noch die sog. AGB Datenbearbeitung durch Dritte erlassen (ebenfalls am 24. Juni 2015: https://www.zh.ch/content/dam/zhweb/bilder-dokumente/organisation/finanzdirektion/afi/agb_datenbearbeitung_durch_dritte.pdf). Diese beziehen sich aber nicht auf die Nutzung von Informatikmitteln, sondern darauf, dass die beigezogene Dritte den eigentlichen Informationsgehalt bearbeiten muss (was Klartextzugriff zwingend voraussetzt, da die Dritte auf dem sog. «Content Layer» arbeiten muss). Ziffer 1 der AGB Datenbearbeitung durch Dritte

C. Positionsbezug

6 Die Diskussion über den Gerichtstand wird mit dem Ziel verfolgt, die Daten bzw. Information der öffentlichen Hand besser zu schützen. Es fragt sich, ob ein Gerichtsstand Schweiz hierfür einen Nutzen entfaltet.

7 Der Gerichtsstand kann einen Einfluss auf das Recht haben, nach welchem das Gericht den Vertrag zwischen der schweizerischen Behörde und der ausländischen Cloud-Anbieterin beurteilt (soweit Regeln der *lex fori* zur Anwendung kommen). Wäre das auf den Vertrag anwendbare Recht relevant für das verfolgte Ziel (Rz. 6), könnte somit auch die Wahl des Gerichtsstands eine solche Wirkung haben. Wie separat gezeigt, ergibt sich im behördlichen Umfeld aber kein ersichtlicher Nutzen, wenn der Vertrag zwischen der Kundin (öffentliche Hand) und der Cloud-Anbieterin dem schweizerischen Recht unterstellt wird (→ *siehe Fact Sheet zum Anwendbaren Recht*). Somit ist auch dem Gerichtsstand für das zu realisierende Ziel (besserer Schutz von Informationen und Daten dank Gerichtsstand in der Schweiz) eine Bedeutung abzusprechen.

8 Nach dieser Ergänzung ist die Auffassung im Leitfaden der euroCloud Swiss (Rz. 4) überzeugend. Ein Gerichtsstand Schweiz hat **keinen rechtlichen Nutzen** und es wäre verwaltungsrechtlich verkehrt, den Gerichtsstand Schweiz als notwendige Voraussetzung der Cloud-Nutzung durch die Behörde darzustellen (fehlende Eignung).

9 Man kann in Bezug auf den Gerichtsstand in der Schweiz zwar durchaus von einem **faktischen Nutzen** sprechen: (a) reduzierte Kosten der Rechtsverfolgung; (b) Vereinfachung für die Behörde, auch vertragsrechtliche Enttäuschungen minderer Art vors Gericht zu bringen. Zudem darf man bei Auswahl von seriösen Providern davon ausgehen, dass sie es nicht auf ein Rechtsdurchsetzungsverfahren an ihrem Sitz ankommen lassen, wenn sie schon in der Schweiz rechtskräftig zu einer Leistung verurteilt worden sind (was Punkt [a] gemäss den Ausführungen in Rz. 4 in der Praxis weitgehend entkräftet). Man kann somit feststellen, dass man durchaus gute Gründe finden kann, warum sich eine Behörde für einen Gerichtsstand in der Schweiz einsetzen will. Eine rechtliche Notwendigkeit, den Gerichtsstand Schweiz zu fordern, gibt es aber – wie bereits festgestellt – nicht.

* * *

beschreiben den Einsatzbereich der Datenbearbeitung (für welche die AGB Datenbearbeitung durch Dritte gelten soll) wie folgt: «Diese AGB gelten für Vertragsverhältnisse, im Rahmen derer die Bearbeitung von Informationen für das öffentliche Organ zentraler Bestandteil, respektive der Hauptzweck des Auftrages ist. Beispiel: Mandatierung eines Anwalts zur Ausformulierung eines Beschlusses, Übertragen des Inkassos an ein Inkassounternehmen».

Christian Laux
Dr. iur., LL.M., Rechtsanwalt, Senior Advisor
christian.laux@lauxlawyers.ch

LAUX LAWYERS AG
ZURICH | BASEL

V02 | 29. Oktober 2021 (r)

Fact Sheet zur Verschlüsselung

A. Sachverhalt

1 Es ist langjährige Praxis der Stadt Zürich, für den Betrieb von IT-Infrastrukturen Dritte einzubinden. Künftig sollen auch Cloud-Anbieterinnen solche IT-Infrastrukturen bereitstellen. Die Stadt Zürich hat dazu ein Rechtsgutachten in Auftrag gegeben. Ergänzend zu diesem sollen verschiedene Einzelfragen detailliert diskutiert werden.

2 Mit der vorliegenden Detailbetrachtung wird untersucht, welche Vorgaben das Recht in Bezug auf die Verschlüsselung aufstellt bzw. was beachtet werden muss, damit die Behörde kein Recht verletzt.

B. Verschlüsselung (Grundlagen)

3 Verschlüsselung ist mit Bezug auf die Sicherheit von Daten in einer Cloud-Umgebung von grosser Bedeutung und stellt eines von zahlreichen Mitteln dar, um ein Offenbaren von Geheimnissen wirkungsvoll zu verhindern. Inhalte, welche eine Cloud-Kundin auf der Cloud-Umgebung speichert, können differenziert nach zwei verschiedenen «Aggregatszuständen» betrachtet werden: (a) «Data-at-Rest»: «ruhend» meint, dass die Daten nicht gerade bearbeitet oder übermittelt werden; (b) «Data-in-Transit»: «in transit» meint den Übermittlungsvorgang oder den Umstand, dass Daten gerade bearbeitet werden (Letzteres auch als «Data-in-Use» bezeichnet).

4 Verschlüsselung von Data-at-Rest kann auf vielen Ebenen stattfinden: (i) *Verschlüsselung des Datenspeichers* (Verschlüsselung der Datenspeichermedien, d.h. der «disk drives»); (ii) *Verschlüsselung der Datei* (z.B. eine Präsentation, welche von Meetingteilnehmerinnen in einer Webkonferenz hochgeladen wurde); (iii) *Verschlüsselung in der Mailbox*; (iv) *Verschlüsselung in der Datenbank*; (v) *Verschlüsselung der virtuellen Maschine*, etc. In der Kombination mehrerer Verschlüsselungsmassnahmen resultiert faktisch eine starke Verschlüsselungswirkung.[1] Zur Verschlüsselung von Data-in-Transit oder «Transportverschlüsselung»: Es gehört zum Stand der Technik, solche Kommunikation mit guter Verschlüsselungstechnologie zu sichern (TLS oder IPsec[2]).

5 Verschlüsselung als Aufgabenstellung kann weiter danach differenziert werden, wer die Verschlüsselung appliziert bzw. aktiviert. Neben den von der Cloud-Anbieterin eingesetzten Verschlüsselungsmethoden bieten viele Cloud-Dienste die Möglichkeit an oder schliessen jedenfalls nicht aus, dass die Kundin ihrerseits eigene Verschlüsselungen auf Dateiebene anlegt.[3]

6 Es ist ein Unterschied, ob die Kundin das Schlüsselmanagement und die übrigen kryptographischen Vorgänge (Ver-/Entschlüsselung) selber vornimmt («Hold your own Key» oder «HYOK») oder lediglich das Schlüsselmanagement selber kontrolliert («Bring Your Own Key» bzw. «BYOK»). In vielen Fällen

[1] Siehe aber die Diskussion bei David Rosenthal, Ausländischer Lawful Access: Wahrscheinlichkeitsbeurteilung und Gegenmassnahmen im Detail, Jusletter 10. August 2020 N 13 ff., woraus sich ergibt, dass selbst bei Einsatz von kombinierten Verschlüsselungsszenarien ein Zugriff durch die Cloud-Anbieterin unter Umständen nicht absolut und zu gut 100% ausgeschlossen werden kann.

[2] Internet Protocol Security ist eine Protokoll-Suite, die eine gesicherte Kommunikation über potentiell unsichere IP-Netze wie das Internet ermöglichen soll, siehe https://de.wikipedia.org/wiki/IPsec

[3] Siehe auch David Rosenthal, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter 10. August 2020 N 10 und David Rosenthal, Ausländischer Lawful Access: Wahrscheinlichkeitsbeurteilung und Gegenmassnahmen im Detail, Jusletter 10. August 2020 N 13.

wird jedoch selbst bei HYOK ein dritter Dienstleister einbezogen, was die erhoffte Wirkung (Schutz mit absoluter Wirkung) oft wieder relativiert.

C. Zum Diskussionsstand

7 Nicht alle Stellungnahmen differenzieren nach Transportverschlüsselung und Verschlüsselung der Datenhaltung. Wo eine Zuordnung eines Positionsbezugs zum einen oder zum andern Thema zu finden ist, wird dies unten dargestellt. Jene Autoren, welche eine Verschlüsselung nicht explizit fordern[4], sind nicht zitiert, was man bei Lektüre der nachstehenden Notiz beachten sollte.

8 Verschlüsselung von Data-in-Transit ist nach dem wohl überwiegenden Meinungsstand in den meisten Fällen standardmässig vorzukehren.[5]

9 Auch die Verschlüsselung von Data-at-Rest wird gefordert[6], wobei die vorn aufgezeigten Differenzierungen (Rz. 4) meist[7] nicht zur Sprache kommen. Dafür wird intensiv erörtert, wer das Schlüsselmanagement ausüben soll.[8] Die Datenschutzbeauftragte des Kantons Zürich differenziert weiter danach, ob der US CLOUD Act zur Anwendung kommt[9] oder nicht[10]. Ebenso wie privatim unterscheidet sie dabei das Amtsgeheimnis als solches von besonderen Amtsgeheimnispflichten, für welche strengere Anforderungen gelten sollen (Steuergeheimnis, Sozialhilfegeheimnis oder Berufsgeheimnis, allerdings ohne Begründung). Eine Differenzierung zwischen Data-at-Rest und Data-in-Transit wird nicht gemacht.

[4] Zum Beispiel David Schwaninger und Stephanie Lattmann: Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke 2.0, in: Jusletter 21. Juni 2021.

[5] Ausdrücklich: Thomas Kessler, Informationssicherheit beim Cloud Computing, saez 2017 1493 ff., 1494 (generell für den Gesundheitsbereich); Erik Dinkel / Philip Gut: Clouddienste im Gesundheitsalltag, saez 2021 1163 ff., 1165 (für das Universitätsspital Zürich); Überarbeitetes privatim-Merkblatt «Cloud-spezifische Risiken und Massnahmen» vom 17. Dezember 2019, https://www.privatim.ch/de/uberarbeitetes-privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen (angesehen am 11. Oktober 2021); siehe aber auch die Ausführungen in FN 8, wonach eine Verschlüsselung auch gemäss den Vorgaben von Privatim situativ bzw. offener gehandhabt werden könnte.

[6] Eine Pflicht Verschlüsselung der Datenhaltung ergibt sich im Resultat auf jeden Fall nach Ziffer 13 der AGB Auslagerung Informatikleistungen (die Pflicht erstreckt sich auch auf die Datenhaltung, weil die AGB Auslagerung Informatikleistungen explizit den «gesamten Bearbeitungsprozess» abdecken). Anzumerken ist, dass die AGB Auslagerung Informatikleistungen erst zum Vertragsinhalt gemacht werden müssen, damit diese Pflicht greift. – Siehe auch Rechtliche Grundlagen im medizinischen Alltag – ein Leitfaden für die Praxis, herausgegeben von der Schweizerischen Akademie für Medizinische Wissenschaften und der Verbindung der Schweizer Ärztinnen und Ärzte FMH, 2. Auflage, 48: «Bei Nutzung von Speichern im Internet («Cloud») ist darauf zu achten, dass die Daten vor dem Speichern in der Cloud lokal verschlüsselt werden. Bei der Auswahl des Anbieters sollen seine Datensicherheits- und Datenschutzregeln kritisch geprüft und sein diesbezüglicher Ruf beachtet werden; die verbreitetste Lösung ist nicht immer die beste». – Auch der EDÖB hat im Tätigkeitsbericht 2014/2015 dafürgehalten, dass Patientendaten nur verschlüsselt in «einer Cloud» gespeichert werden dürfen: https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/aeltere-berichte/22--taetigkeitsbericht-2014-2015/aufbewahrung-von-patientenakten-in-einer-cloud.html: «konsequent clientbasiert verschlüsselt …, was heisst, dass der Arzt als Dateninhaber als einzige Person den Schlüssel zu den sich in der Cloud befindlichen Daten hat. Der Cloud-Anbieter darf nicht in Besitz des Schlüssels kommen. Der Dateninhaber bzw. der Arzt kann Daten, die durch ihn vorgängig vollständig anonymisiert wurden, für Statistikzwecke zur Verfügung stellen.»

[7] Ausnahme z.B. David Rosenthal, Ausländischer Lawful Access: Wahrscheinlichkeitsbeurteilung und Gegenmassnahmen im Detail, Jusletter 10. August 2020 N 18 ff., der den Vorgang der Entschlüsselung und die dabei entstehenden Risiken genauer beleuchtet.

[8] Überarbeitetes privatim-Merkblatt «Cloud-spezifische Risiken und Massnahmen» vom 17. Dezember 2019, https://www.privatim.ch/de/uberarbeitetes-privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen (angesehen am 11. Oktober 2021). Bei besonders schützenswerten Personendaten (inkl. Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen) seien zusätzliche Anforderungen an die Verschlüsselung und das Schlüsselmanagement zu stellen und in der Risikoabwägung zu berücksichtigen: (a) die Verschlüsselung solle durch das öffentliche Organ erfolgen (und die Schlüssel dürften «grundsätzlich» nur für das öffentliche Organ verfügbar sein; die Schlüssel seien vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme zu schützen); (b) wenn die Vorkehrungen unter (a) nicht möglich seien, könnten die Schlüssel beim Cloud-Anbieter aufbewahrt werden, wenn er sich vertraglich verpflichtet, sie nur mit der ausdrücklichen Zustimmung des öffentlichen Organs zu verwenden, es seien zusätzliche Massnahmen zu treffen (Zugriffe seien zu protokollieren; der Cloud-Anbieter müsse die Schlüssel vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme schützen und sicherstellen, dass die Daten beim Verschlüsselungsvorgang nicht kompromittiert werden könnten). – siehe auch Wolfgang Wohlers: Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), 20, m.w.H.

[9] Besondere datenschutzrechtliche Aspekte der Cloud Nutzung – unter Berücksichtigung des «CLOUD Act» (ausgenommen Schulen), https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/datenschutz/publikationen/leitfaeden/leitfaden_auslagerung_beruecksichtigung_des_cloud_act.pdf (angesehen am 11. Oktober 2021).

[10] https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/datenschutz/weitere-themen/outsourcing/verschluesselung_der_datenablage_im_rahmen_der_auslagerung.pdf (angesehen am 11. Oktober 2021).

10 Es fällt dabei auf, dass die in Rz. 9 genannten Positionsbezüge, welche eine Verschlüsselung zwingend fordern (bei gegebenen Voraussetzungen), keine holistische Sicht auf die Risikokontrolle nehmen (können), da sie notgedrungen abstrakt bleiben müssen; einzelne Anforderungen erscheinen so zum Teil etwas isoliert. Eine kombinierte Sicht auf Risiken und Massnahmen dürfte erst im konkreten Anwendungsfall gelingen.

11 Anders als für die in Rz. 9 genannten Positionsbezüge ist die Verschlüsselung für die überwiegende Lehre nur eine von vielen möglichen Schutzmassnahmen.[11] Zum Teil wird dabei nach Datenkategorie differenziert.[12]

D. Positionsbezug

12 Für den Positionsbezug in diesem Fact Sheet kann auf das bereits für die OIZ erstellte Rechtsgutachten verwiesen werden.[13] Die Verweise auf das Gutachten zeigen, dass sich im für die Stadt Zürich relevanten Gesetzesrecht keine Vorgabe findet, welche die Verschlüsselung von Daten ausdrücklich (im Sinne einer verbindlichen Pflicht) fordert. Damit kann sich der Verfasser der Mehrheitsmeinung (dazu Rz. 11) anschliessen, dass zwar angemessen zu schützen ist, dass aber die Verschlüsselung nur eine von vielen dafür in Frage kommenden Massnahmen darstellt.

13 Eine Transportverschlüsselung ist allerdings häufig ohne Funktionseinbussen möglich. Viele Lösungen ermöglichen eine solche (auch z.B. Datenübermittlungen zwischen Teilkomponenten einer technischen Lösung). Entsprechend kann man eine Tendenz ausmachen, dass Transportverschlüsselung eher gefordert werden kann als eine Verschlüsselung der Datenhaltung zu verlangen (Data-at-Rest).

14 Auf Ebene der Datenhaltung lässt sich eine Lösung demgegenüber oft mit alternativen (sich gegebenenfalls ergänzenden) Schutzmassnahmen erreichen, was dazu führt, dass sich diesbezüglich eine abstrakte Forderung nach Verschlüsselung nicht aufrecht erhalten lässt.

15 Da eine Verschlüsselung per se kein zwingendes Erfordernis ist, erübrigt es sich, über verschiedene Verschlüsselungsformen zu sprechen. Es wäre verfehlt, für gewisse besonders relevanten Daten eine Verschlüsselung mit Key-Management durch die Cloud-Kundin zu verlangen (z.B. Hold Your Own Key). Es gibt Verschlüsselungsformen, die besonders wirksam sind, um Daten in der Cloud-Umgebung umgehend unbrauchbar zu machen (BYOK). Damit wird jedoch nicht das Schutzziel Vertraulichkeit, sondern das Schutzziel Verfügbarkeit adressiert.

[11] Veronica Blattmann, in Baeriswyl/Rudin, Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich (IDG), 2012, §6 N 13; Roman Dolf / Rebekka Grassmayr, Die Zukunft ist die Cloud?, Positionspaper vom 18. September 2021. Die Autoren sprechen von BYOK und BYOE. HYOK wird nicht diskutiert; David Rosenthal, Ausländischer Lawful Access: Wahrscheinlichkeitsbeurteilung und Gegenmassnahmen im Detail, Jusletter 10. August 2020 N 13; Ursula Widmer: Gesundheitsdaten in der Cloud, in P. Schartner / J. Taeger (Hrsg.): DACH Security 2011, syssec (2011) 166-177; Wolfgang Wohlers: Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), 20, m.w.H.; Martin Zobl / Christine Schweikard: Patientendaten in die Cloud? Ja, aber gewusst wie!, https://www.heimeundspitaeler.ch/news/news-details/patientendaten-in-die-cloud-ja-aber-gewusst-wie (angesehen am 11. Oktober 2021);

[12] Überarbeitetes privatim-Merkblatt «Cloud-spezifische Risiken und Massnahmen» vom 17. Dezember 2019, https://www.privatim.ch/de/uberarbeitetes-privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen (angesehen am 11. Oktober 2021). Bei besonders schützenswerten Personendaten (inkl. Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen) seien zusätzliche Anforderungen an die Verschlüsselung und das Schlüsselmanagement zu stellen und in der Risikoabwägung zu berücksichtigen: (a) die Verschlüsselung solle durch das öffentliche Organ erfolgen (und die Schlüssel dürften «grundsätzlich» nur für das öffentliche Organ verfügbar sein; die Schlüssel seien vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme zu schützen); (b) wenn die Vorkehrungen unter (a) nicht möglich seien, könnten die Schlüssel beim Cloud-Anbieter aufbewahrt werden, wenn er sich vertraglich verpflichtet, sie nur mit der ausdrücklichen Zustimmung des öffentlichen Organs zu verwenden, es seien zusätzliche Massnahmen zu treffen (Zugriffe seien zu protokollieren; der Cloud-Anbieter müsse die Schlüssel vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme schützen und sicherstellen, dass die Daten beim Verschlüsselungsvorgang nicht kompromittiert werden könnten).

[13] Christian Laux / Alexander Hofmann: Rechtmässigkeit von Public Cloud Services, «Cloud-Gutachten» (unter Berücksichtigung des CLOUD Act) vom 16. September 2021 (V 0.99), v.a. Rz. 32 und Rz. 37 (beide zu den verwaltungsrechtlich geforderten Schutzmassnahmen), Rz. 78 (zu datenschutzrechtlich geforderten Schutzmassnahmen) und Rz. 87, Rz. 91 und Rz. 112 (zu den aus strafrechtlicher Sicht geforderten Schutzmassnahmen).

16 Generell lässt sich festhalten, dass die Diskussion der Verschlüsselungsformen in der juristischen Diskussion eine zu gewichtige Rolle einnimmt. In der juristischen Diskussion kommen die diesbezüglich möglichen und nötigen Differenzierungen oft nicht zum Tragen, was mit Blick auf die Bedeutung, die man den juristischen Voten gibt, überaus problematisch ist.

17 Oft ist die in einer juristischen Fachpublikation vorgenommene Sicht auf das Thema Sicherheit von einer sehr grossen Distanz geprägt. Die Voten, die sich zu besonderen Formen der Verschlüsselung äussern, bleiben in der Regel bruchstückhaft oder beleuchten das Thema nur unter zu wenigen Aspekten:

18 Aus einem Umsetzungsprojekt kann der Verfasser dieser Notiz berichten, dass die Kundin im Rahmen der sog. «Security Baselines» hunderte von einzelnen Einstellungsmöglichkeiten in der Umgebung der Cloud-Anbieterin selber vornehmen konnte. Wenn man berücksichtigt, dass diese Security Baselines nur jene Einstellungen abbildet, welche die Kundin selber wählen konnte, aber jene ausblendet, die die Cloud-Anbieterin von sich aus auf ihren IT-Infrastrukturen umgesetzt hat, dann wirken Diskussionen zum Thema «BYOK oder HYOK» geradezu flagrant oberflächlich.

19 Die Diskussion über Verschlüsselung sollte ins technisch geprägte Umsetzungsprojekt verschoben werden.

20 Es wäre nicht sachgerecht, Forderungen betreffend konkrete Verschlüsselungsmassnahmen allein auf Basis von abstrakt gehaltenen juristischen Positionsbezügen zu formulieren.

* * *

Christian Laux
Dr. iur., LL.M., Rechtsanwalt, Senior Advisor
christian.laux@lauxlawyers.ch

LAUX LAWYERS AG
ZURICH | BASEL

V02 | 1. November 2021

Fact Sheet zum Berufsgeheimnis

A. Sachverhalt

1 Es ist langjährige Praxis der Stadt Zürich, für den Betrieb von IT-Infrastrukturen Dritte einzubinden. Künftig sollen auch Cloud-Anbieterinnen solche IT-Infrastrukturen bereitstellen. Die Stadt Zürich hat dazu ein Rechtsgutachten in Auftrag gegeben. Ergänzend zu diesem sollen verschiedene Einzelfragen detailliert diskutiert werden.

2 Mit der vorliegenden Detailbetrachtung werden die Regeln zum Berufsgeheimnis, wie es z.B. in Gesundheitsberufen zum Tragen kommt, besonders beleuchtet und in eine Beziehung zu den Aussagen im Rechtsgutachten gesetzt.

B. Verortung

3 Angaben zum Gesundheitszustand können für das Leben eines Menschen gravierende soziale und wirtschaftliche Folgen haben (z.B. Stigmatisierung und damit verbundene Folgen am Arbeitsplatz). Die Patientin muss sich darauf verlassen können, dass die Ärztin nichts «ausplaudert» oder in einer Konfliktsituation zwischen der Patientin und einer Dritten (z.B. einer Arbeitgeberin) keine Angaben zum Gesundheitszustand der Patientin preisgibt. Das Patientengeheimnis ist von grosser gesellschaftlicher Bedeutung.

4 Der Wortlaut von § 3 Abs. 4 lit. a Ziff. 2 IDG nennt Informationen über «die Gesundheit, die Intimsphäre, die ethnische Herkunft sowie genetische und biometrische Daten» als besondere Personendaten. Nach dem IDG sollen offenbar «Informationen über die Gesundheit» von «genetischen Daten» getrennt begriffen werden. Die folgenden Beispiele unterstützen dies:

- Biomaterial: «Biomaterial enthält prinzipiell immer auch Daten über verwandte Personen wie beispielsweise Kinder, Eltern, Enkel».[1]
- Haar- und Augenfarbe: Nicht alle genetischen Daten sind auch Gesundheitsdaten (z.B. Haar- und Augenfarbe).

Es besteht deshalb zwar ein Überschneidungsbereich (z.B. genetische Erkrankungen). Genetische Daten sind wohl aber nicht generell eine Unterkategorie von Gesundheitsdaten; sie können auch über die Gruppe der Gesundheitsdaten hinausgehen.

5 In einer vernetzten Welt ist eine Ärztin darauf angewiesen, moderne Techniken einsetzen zu können und sich im Betrieb von dieser Technik helfen zu lassen. Dies verbessert die Leistung der Ärztin im Dienst der Patientin. Auch die Datenhaltung und -verwaltung kann mit hochwertiger Technik besser werden, und auch dies ist im Interesse der Patientin. Moderne Technik der Datenhaltung und -verwaltung kann zu besserer IT-Sicherheit und höherer Leistungsfähigkeit der Systeme führen, was beides den Schutz von Patientendaten erhöhen kann.

[1] https://gesundheitsdatenschutz.org/download/datenschutz_klin-register.pdf (S. 44).

C. Zusammengreifen verschiedener rechtlicher Pflichten am Beispiel der GZA

6 Die Stellen innerhalb der Stadt Zürich haben, je nach ihrer Rolle, vielfältige Geheimnispflichten zu wahren. Diese knüpfen an der inhaltlichen bzw. sachlichen Aufgabe bzw. der Tätigkeit der jeweiligen Stelle an. Bekannt ist das sog. «Steuergeheimnis», es gibt ein Berufsgeheimnis für Beiständinnen[2], ein Sozialhilfegeheimnis[3], die Schweigepflicht des städtischen Datenschutzbeauftragten[4], die Schweigepflicht der Mitglieder des Gemeinderats[5] oder eine Verschwiegenheitspflicht von Case Managern am Arbeitsplatz[6], um nur einige zu nennen. Im Sinne eines Beispiels zur Illustration ist die Verschwiegenheitspflicht im Tätigkeitsbereich der Pflegezentren darzustellen, um zu zeigen, wie verschiedene Vertraulichkeitsregeln ineinandergreifen können:

7 Die Verordnung Pflegezentren der Stadt Zürich (Pflegezentrenverordnung, 813.141) sieht vor, dass die Stadt Zürich zur Sicherstellung der Versorgung ihrer pflegebedürftigen Einwohnerinnen und Einwohner eigene Pflegeeinrichtungen für Langzeit- und temporäre Aufenthalte führt (§ 2 Abs. 1 Satz 1 Pflegezentrenverordnung). Das Personal der Dienstabteilung GZA («Gesundheitszentren für das Alter») hat eine Verschwiegenheitspflicht[7]; Offenbarungen sind damit verboten. Ergänzend:

- das *pflegende Personal* übt einen Beruf des Gesundheitswesens aus. Gemäss § 15 Abs. 1 des kantonalzürcherischen Gesundheitsgesetzes (GesG) sind Personen, die einen Beruf des Gesundheitswesens ausüben sowie ihre Hilfspersonen, dazu verpflichtet, Stillschweigen über Geheimnisse zu wahren, die ihnen infolge ihres Berufes anvertraut worden sind oder die sie in dessen Ausübung wahrgenommen haben. Das Pflegepersonal kann unter Umständen auch nach dem Bundesgesetz über die universitären Medizinalberufe (Medizinalberufegesetz, MedBG), namentlich Art. 40 MedBG (Berufspflichten), zur Geheimhaltung verpflichtet sein (lit. f: «Sie wahren das Berufsgeheimnis nach Massgabe der einschlägigen Vorschriften.»).
- soweit *administratives Personal* nicht ebenfalls als Angehörige eines Berufs des Gesundheitswesens gilt, untersteht es nur den allgemeinen verwaltungsrechtlichen Verschwiegenheitspflichten.[8]

[2] Art. 413 Abs. 2 ZGB.

[3] § 47 Sozialhilfegesetz des Kantons Zürich (SHG), LS 851.1.

[4] «Die bzw. der Beauftragte ihrerseits bzw. seinerseits wahrt das Amtsgeheimnis, soweit es schutzwürdige öffentliche oder private Interessen gebieten.» (Art. 39 Abs. 3 Satz 5 i.V.m. Art. 39bis Satz 2 Gemeindeordnung, 101.100). Nachdem die Stadt Zürich einen eigenen Datenschutzbeauftragten bestellt hat, gilt § 33 Abs. 2 IDG: «Die Gemeinden […] regeln Wahl und Organisation selbstständig. Sie stellen sicher, dass die Beauftragten über die notwendigen fachlichen Voraussetzungen verfügen und in der Ausübung ihrer Aufgaben und Befugnisse unabhängig sind. Die oder der kantonale Beauftragte übt die Oberaufsicht aus.» Diesbezüglich ergibt sich ein scheinbarer Normenkonflikt mit § 38 IDG: «*Die oder der Beauftragte sowie die Mitarbeitenden sind in Bezug auf Informationen, die sie bei ihrer Tätigkeit zur Kenntnis nehmen, zur gleichen Verschwiegenheit verpflichtet wie das bearbeitende öffentliche Organ.*» Ergänzend regelt § 39a Abs. 2 IDG die Schweigepflicht für Rechtsmittelinstanzen in Personalstreitigkeiten im Sinne von § 39a IDG: «Die Schweigepflicht gemäss § 38 gilt auch für die Rechtsmittelinstanzen.»

[5] «*Bei geheimer Beratung besteht für die Mitglieder des Gemeinderates Schweigepflicht.*» (Art. 31 Abs. 2 Gemeindeordnung).

[6] «***(1)** Der Stadtrat schafft zur Verminderung von Langzeitabsenzen und Invaliditätsfällen die Möglichkeit, Angestellte in beruflich und gesundheitlich schwierigen Situationen zu unterstützen. Er führt zu diesem Zweck im Rahmen der mit dem Budget bewilligten Mittel in der gesamten Verwaltung oder in einzelnen Dienstabteilungen das Case Management am Arbeitsplatz ein. **(2)** Unterstützungshandlungen und Datenbearbeitungen durch die Case Managerinnen und Case Manager bedürfen der Einwilligung durch die betroffenen Angestellten. **(3)** Die Case Managerinnen und Case Manager sind in Bezug auf die Informationen, die sie über die betroffenen Angestellten bearbeiten, zur Verschwiegenheit verpflichtet. Die Fallakten sind keine Personalakten. Akteneinsicht oder Datenbekanntgaben dürfen nur mit Zustimmung der betroffenen Angestellten gewährt werden. Art. 46 findet keine Anwendung.*" (Art. 3bis des Personalrechts, PR; 177.100)

[7] Landolt, Hardy, Öffentliches Gesundheitsrecht, Public Health Law, Zürich 2009, S. 261 ff.

[8] Die kantonalzürcherische Datenschutzbeauftragte unterscheidet im Bereich des Amtsgeheimnisses nach dem allgemeinen Amtsgeheimnis und besonderen Amtsgeheimnissen, wobei die Unterschiede (Besonderheiten) zwischen dem ersten und den anderen nicht erkennbar sind: Besondere datenschutzrechtliche Aspekte der Cloud Nutzung – unter Berücksichtigung des «CLOUD Act» (ausgenommen Schulen), https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/datenschutz/publikationen/leitfaeden/leitfaden_auslagerung_berueecksichtigung_des_cloud_act.pdf (angesehen am 11. Oktober 2021). Als besondere Amtsgeheimnisse werden etwa das Steuergeheimnis, das Sozialhilfegeheimnis und das Berufsgeheimnis bezeichnet.

- *für den gesamten Personalbestand* des GZA gilt grundsätzlich das IDG, ausser im Wettbewerbsbereich, soweit die GZA hier tätig ist (dort gilt das DSG).[9] Für besondere Personendaten gelten (nur) wenige Besonderheiten: Zentral sind gesteigerte Schutzpflichten einerseits (insbesondere mit Blick auf die Bedeutung, vorn Rz. 3) und besondere Verfahrensbestimmungen (siehe Rechtsgutachten).

8 Die straf- und aufsichtsrechtliche «Verstärkung» der genannten Verschwiegenheitspflichten ist im Bereich des Gesundheitswesens besonders vielschichtig. Insofern lohnt sich ein vertiefender Blick. Alle vorgenannten Personen unterstehen in ihrem Aufgabenbereich der Strafsanktion nach Art. 320 StGB. Für eine Berufsträgerin (die Ärztin, die Pflegerin, etc.) gelten die folgenden strafrechtlichen Verstärkungen ihrer Verschwiegenheiten:

- sie untersteht auch der Strafsanktion von Art. 321 StGB (Berufsgeheimnis)[10]
- auch aus Art. 35 Abs. 2 DSG ergibt sich eine strafrechtliche Verstärkung: Die Regelung verlangt Vorsatz. Sie gilt zudem von vornherein nur für die Berufsträgerin, nicht dort, wo nur kantonale Behördentätigkeit zur Diskussion steht.[11] Tatbestandsmässig ist nach geltendem[12] DSG die «Bekanntgabe», und zwar nur dann, wenn sie sich auf besonders schützenswerten Personendaten oder auf Persönlichkeitsprofile bezieht.
- eine weitere Sicherung der Verschwiegenheitspflicht ergibt sich aus Art. 33 ATSG, soweit das Personal der GZA an der Durchführung der Sozialversicherungsgesetze (oder Kontrolle / Beaufsichtigung) beteiligt sein sollte; eine strafbare Handlung gilt aber nicht als erfolgt, wo Personal die Daten nur gegenüber der beigezogenen Dritten offenbart. Der Beizug von ICT-Anbietern ist damit zulässig.[13]

9 Aufsichtsbehörde über die Tätigkeit der GZA im Anwendungsbereich des GesG ist der Bezirksrat mit Oberaufsicht durch die Gesundheitsdirektion des Kantons Zürich (§ 37 GesG). Beide unterstehen dem kantonalzürcherischen und nicht dem städtischen Beamtenrecht. Hier gelten die allgemeine verwaltungsrechtliche Verschwiegenheitspflicht und Art. 320 StGB.

10 Soweit das kantonalzürcherische Gesundheitsrecht zur Anwendung kommt, dürfte auch das kantonale Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1999 (LS 172.71) gelten. Nach dessen § 3 Abs. 1 muss die auslagernde Stelle sicherstellen, dass nur solche Mitarbeiter des Auftragnehmers Gesundheitsdaten (oder sonstige besondere Daten) bearbeiten können, welche dem Kontroll- und Weisungsrecht der auslagernden Stelle unterworfen werden und an die Geheimhaltung gebunden werden.

[9] Zur Abgrenzung der anwendbaren Rechtsregeln siehe Bernhard Rütsche, Datenschutzrechtliche Aufsicht über Spitäler, in: Baeriswyl/Rudin (Hrsg): digma Schriften zum Datenrecht Bd. 6, Zürich 2012, 51; Thomas Steiner: Digitalisierter Arztbesuch und Cloud-Nutzung im Lichte des Datenschutzrechts des Bundes und der Kantone, in sic! 12/2020 679; Martin Zobl / Christine Schweikard: Patientendaten in die Cloud? Ja, aber gewusst wie!, https://www.heimeundspitaeler.ch/news/news-details/patientendaten-in-die-cloud-ja-aber-gewusst-wie (angesehen am 11. Oktober 2021), zu «öffentlich-rechtliche Institutionen» (sonst mit dem abzulehnenden Vorschlag, dass die Verfügungsgewalt zur Abgrenzung relevant sei).

[10] Ursula Uttinger: Regulatorische Anforderungen an IT-Outsourcing: Gesundheits- und Versicherungsbereich, in: Rolf H. Weber / Mathis Berger / Rolf auf der Maur: IT-Outsourcing, ZIK – Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich, Bd. 23 Zürich 2003, 255 ff., 261.

[11] Ursula Widmer: Gesundheitsdaten in der Cloud, in P. Schartner / J. Taeger (Hrsg.): DACH Security 2011, syssec (2011) 166-177: «Die Bestimmung gilt nicht für Tätigkeiten im Bereich der kantonalen Verwaltungen und der Erfüllung kantonaler öffentlicher Aufgaben, da diese nicht in den Geltungsbereich des DSG fallen».

[12] Mit dem revidierten Datenschutzgesetz werden sich diesbezüglich Neuerungen ergeben: Was die Tathandlung angeht (Offenbarung statt Bekanntgabe) wird der objektive Tatbestand offener formuliert und die Strafbarkeit somit grundsätzlich erweitert. Beim Tatobjekt wirkt die Revision in zwei Richtungen: Neu sind nicht mehr nur besondere Personendaten (sondern neu alle Personendaten) im Anwendungsbereich, dies jedoch – einschränkend – nur dann, wenn sie (a) geheim sind und (b) bei Ausübung eines Berufs eingesehen wurden und (c) der Beruf die Kenntnis dieser Personendaten (normativ gesprochen) auch erfordert.

[13] Widmer (FN 11), 171.

D. Zum Diskussionsstand

11 Zum Teil wird gesagt, dass die Cloud-Nutzung für ein öffentliches Spital weniger leicht möglich ist als für ein Privatspital; generell sei die Cloud-Nutzung im Gesundheitswesen aber möglich.[14]

12 Diese Sichtweise wird namentlich von Wolfgang Wohlers abgelehnt.[15] Wohlers beurteilt den Beizug von Dritten durch Trägerinnen des Berufsgeheimnisses als problematisch. Wohlers stellt den seiner Beurteilung zu Grunde liegenden Sachverhalt wie folgt dar: Wohlers führt zunächst im Sinne eines Beispiels aus, dass «sich z.B. die Fernwartung von Software und die Behebung von Systemfehlern ohne gleichzeitigen Zugriff auf die Anwendungsdaten durch den spezialisierte[n] Dienstleister gar nicht realisieren lässt». Daraus schliesst er, dass mit einem Outsourcing von Dienstleistungen stets «der Zugriff Dritter auf personenbezogene Anwendungsdaten einhergeht». Ausgenommen seien einzig «Fälle[n], in denen es allein und ausschliesslich um die Archivierung von Datenbeständen geht». Ein Rechtsgutachten zum Bankgeheimnis tritt dieser Problemschilderung jedenfalls für den Cloud-Kontext entgegen.[16]

13 In der Debatte wird der Fokus auf die folgenden Themen gelegt:

1. *Begehungsdelikt oder Unterlassungsdelikt*: Diskutiert wird, ob Strafbarkeit bereits mit dem Upload von Daten in die Cloud (Begehungsdelikt)[17] oder ob erst bei erfolgten Klartextzugriffen wegen unterlassener Sicherung anzunehmen ist (Unterlassungsdelikt)[18].
2. *Datenstandort Schweiz*: Vereinzelt wird Datenstandort Schweiz gefordert.[19]
3. *Zugriffe nur durch Personen in der Schweiz*: Auch dies wird nur vereinzelt gefordert.[20]
4. *Hilfspersoneneigenschaft*: Der Begriff der Hilfsperson ist noch immer nicht restlos geklärt.[21] Es wird kontrovers diskutiert, ob externe Anbieterinnen von Leistungen wie z.B. Cloud-Anbieterinnen als Hilfspersonen anerkannt werden[22], ob ein sog. Datenschutzrevers oder Geheimnisrevers[23] «auf die Mitarbeitenden hinunter» Voraussetzung für die Bestellung als Hilfsperson ist[24] und ob Cloud-Anbieterinnen mit Sitz im Ausland als Hilfspersonen anerkannt werden können.[25]

[14] Ursula Uttinger, Inwieweit bestimmen Patienten noch über ihre Daten?, in: Harry Landolt et al. (Hrsg.), Pflegerecht - Pflegewissenschaft 2015, 6; Ursula Uttinger / Michael Liebrenz, Nutzung medizinischer Schreibservices - eine datenschutzrechtliche Sicht, Schweizerische Ärztezeitung 2014, 95 f.; Widmer (FN 11), 166-177: «So ist es denkbar, dass z.B. für ein Privatspital Cloud Computing unter Voraussetzungen möglich ist, welche für ein kantonales öffentliches Spital ausgeschlossen sind.»

[15] Wolfgang Wohlers, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), in: Bruno Baeriswyl / Beat Rudin: Schriften zum Datenrecht Band 9, Zürich 2016, 16.

[16] Christian Laux / Alexander Hofmann / Mark Schieweck / Jürg Hess: Nutzung von Cloud-Angeboten durch Banken: Zur Zulässigkeit nach Art. 47 BankG, Zürich 2019, Rz. 67 ff., 69, abrufbar unter: https://www.lauxlawyers.ch/rechtsgutachten-bankgeheimnis-und-cloud.. Siehe dazu auch Anhang 2 zum Rechtsgutachten, das die Stadt Zürich in Auftrag gegeben hat.

[17] So wohl Wohlers (FN 15), 20 (Hinweise auf Rechtsprechung und Lehre bei Wohlers [FN 15], 17, Fussnote 63) und Widmer (FN 11), 166-177.

[18] Laux / Hofmann / Schieweck / Hess (FN 16), Rz. 21 ff.

[19] Thomas Kessler, Informationssicherheit beim Cloud Computing, saez 2017 1493 ff., 1494: Kessler hält dafür, dass das Berufsgeheimnis nach Art. 321 StGB nur durchgesetzt werden könne, «wenn sich die Daten … in der Schweiz befinden.»

[20] Kessler (FN 19), mit derselben Begründung wie für den Datenstandort Schweiz.

[21] Nachweise bei Wohlers (FN 15), 22 ff.

[22] Die Frage wird zunächst ohne Differenzierung nach «Inland v. Ausland» diskutiert, die folgenden Stellungnahmen müssen so verstanden werden, dass sie für Anbieterinnen ohne Auslandsbezüge zu verstehen sind: **Bejahend**: Veronika Blattmann: in Baeriswyl/Rudin, Praxiskommentar zum IDG, Zürich 2012, § 6 N 10; Uttinger (FN 10), S. 258 f. **Ablehnend**: Wohlers, 26.

[23] Was mit dem sog. «Datenschutz-Revers» gemeint ist, erklärt sich am besten unter Verweis auf die Musterformulierungen aus dem Kanton Basel Landschaft: https://www.baselland.ch/politik-und-behorden/besondere-behorden/datenschutz/publikationen/merkblatter-musterschreiben/downloads/mustertext_datenschutz.pdf/@@download/file/mustertext_datenschutz.pdf (angesehen am 11. Oktober 2021) oder der Stadt Aarau: https://www.aarau.ch/public/upload/assets/679/Datenschutzrevers_Homepage.pdf (angesehen am 11. Oktober 2021).

[24] Widmer (FN 11), 166-177., bezeichnet dies als «fraglich».

[25] **Bejahend**: Bezirksgericht ZH, Urteil vom 18. November 2015 (GG150233): «Das Schreibbüro H. hat damit vorliegend ebenfalls als Hilfsperson im Sinne von Art. 321 Ziff. 1 Abs. 1 StGB zu gelten. Daran ändert vorliegend auch der Umstand, dass Frau I. vom Schreibbüro H. ihre Arbeiten nicht in der Schweiz, sondern in Deutschland ausübt, nichts.»; gl.M. Steiner (FN 9), 683. **Ablehnend**: Christian Peter: Nutzung von Cloud-Diensten im medizinischen Alltag, Schweizerische Ärztezeitung, 2013;94: 37, 1404 ff., 1405.

5. *Einwilligungserfordernis*: Ob für den Beizug der Cloud-Anbieterin per se sei die Einwilligung der Patientin erforderlich ist, ist ebenfalls streitig, und zwar sowohl in Bezug auf Cloud-Angebote mit Bezug nur zur Schweiz[26] wie auch in Bezug auf Cloud-Angebote mit Auslandsbezügen[27].

6. *Informationsobliegenheit*: Keine Einigkeit besteht auch in Bezug auf die Frage, ob die Patientin zu informieren ist.[28]

7. *Behördenzugriffe im Ausland als Risiko*: Widmer identifiziert Behördenzugriffe auf Daten als Risiko, auch wenn diese Zugriffe nach ausländischem Recht rechtmässig sein könnten (*lawful access*). Problematisch sei, wenn die ausländischen Voraussetzungen nicht dieselben seien wie jene nach dem schweizerischen Recht.[29]

8. *Notwendigkeit der Verschlüsselung*: Vereinzelt (soweit ersichtlich nur für das Universitätsspital Zürich, differenzierend nach Aufgabenstellungen[30]) wird gefordert, dass die AGB Auslagerung Informatikleistungen des Kantons Zürich zur Anwendung gebracht werden.[31] In deren Ziffer 13 ist Verschlüsselung gefordert. Ansonsten wird Verschlüsselung nur als eine von vielen Möglichkeiten zum Schutz von Geheimnissen angesehen.

9. *Wahl des Schweizerischen Rechts* (Vertragsstatut): Dies wird soweit ersichtlich ebenfalls nur für das Universitätsspital Zürich gefordert (und zwar dadurch, dass die die AGB Auslagerung Informatikleistungen des Kantons Zürich zur Anwendung gebracht werden sollen).[32]

10. *Gerichtsstand Schweiz*: Es wird auf die vorstehenden Ziffern 8 und 9 verwiesen. Eine solche Forderung wird spezifisch für das Gesundheitsrecht soweit ersichtlich nur für das Universitätsspital Zürich gefordert.

[26] **Bejahend**: Wolfgang Wohlers, 27. **Ablehnend**: Yves Gogniat, Datenschutz in Spitälern, in: Jusletter 20. Juni 2016, Rz. 40; Christian Peter, Die Zulässigkeit der Auslagerung der Bearbeitung der Patientendaten von Spitälern an externe Informationsdienstleister, in: Jusletter 22. Juni 2009, 3; Peter (FN 25), 1405; Widmer (FN 11), 166-177: «Voraussetzung für den Beizug externer Anbieter als Hilfspersonen ist jedoch, dass diese durch ausdrückliche vertragliche Regelung der Geheimhaltungspflicht unterstellt werden.»; implizit auch Uttinger (FN 10), 259.

[27] **Bejahend** die folgenden Stellungnahmen, wobei die Begründung variiert: Ursula Widmer führt als Grund an, dass es zu Behördenzugriffen im Ausland kommen könne: Widmer (FN 11), 166-177.: «Aus der mangelnden Durchsetzbarkeit des Schweizer Strafrechts im Ausland wird der Schluss gezogen, dass im Ausland befindliche Personen nicht als Hilfspersonen im Sinne des Gesetzes anerkannt werden können, mit der Folge, dass die Weitergabe von Patientendaten ins Ausland nur mit Zustimmung der betroffenen Patienten zulässig ist.»; Peter (FN 25), 1405, führt als Grund an, dass das schweizerische Strafrecht im Ausland nicht durchsetzbar sei. **Ablehnend**: Steiner (FN 9), 684.

[28] **Bejahend**: Peter (FN 25), 1406. Auch die Ärzteschaft empfiehlt eine Information der Patientin, wenn ein Outsourcing-Dienstleister beigezogen wird: Rechtliche Grundlagen im medizinischen Alltag – ein Leitfaden für die Praxis, herausgegeben von der Schweizerischen Akademie für Medizinische Wissenschaften und der Verbindung der Schweizer Ärztinnen und Ärzte FMH, 2. Auflage, 99 ff. – zitiert von Ursula Uttinger: Inwieweit bestimmen Patienten noch über ihre Daten? In: Hardy Landolt / Brigitte Blum-Schneider et al.: Pflegerecht 2015, Pflege in Politik, Wissenschaft und Ökonomie, Bern 2015, 6. **Ablehnend**: Ursula Uttinger: Inwieweit bestimmen Patienten noch über ihre Daten? In: Hardy Landolt / Brigitte Blum-Schneider et al.: Pflegerecht 2015, Pflege in Politik, Wissenschaft und Ökonomie, Bern 2015, 6; Ursula Uttinger/Michael Liebrenz (FN 14), 95 f.

[29] Widmer (FN 11), 170.

[30] Die AGB Auslagerung Informatikdienstleistungen werden jedoch nicht gefordert für die folgenden Szenarien (dazu Erik Dinkel / Philip Gut: Clouddienste im Gesundheitsalltag, saez 2021 1163 ff., 1165): Geheime Daten, wenn sie keinen Personenbezug haben; Patientendaten und besondere Mitarbeiterdaten sowie vertrauliche Mitarbeiterdaten (Salär und private Adresse), wenn sie anonymisiert sind; Vertrauliche Daten ohne Personenbezug (Forschungsresultate, strategische oder taktische Angaben, finanzrelevante Daten); interne Daten (alle nicht klassifizierten Informationen, die nicht öffentlich sind). Gar keine Vorgaben an die vertragliche Grundlagen bestünden bei öffentlichen Daten.

[31] Dinkel / Gut (FN 30), 1165.

[32] Dinkel / Gut (FN 30), 1165.

E. Positionsbezug

14 Im Rahmen des hier folgenden Positionsbezugs ist zunächst zu klären, ob die einleitend erwähnten Spezialgeheimnisse (vorn Rz. 6) eine eigenständige Bedeutung für die hier interessierende Frage («Relevanz für ein Cloud Computing-Projekt?») haben oder nicht (Ziffer 1). Dann kann zu den Themen der Debatte (dazu vorn, Rz. 13) Stellung genommen werden (Ziffer 2).

1. Warum Spezialgeheimnisse?

a. Wirksamkeit

15 Dass es mehrere solcher fachspezifischen Geheimhaltungsregeln gibt, dürfte damit zusammenhängen, dass die Legislative das Schutzziel – Vertraulichkeit der Information (Content Layer[33]) – wirklich wirksam absichern wollte. Anlass hierfür dürfte sein, dass die konkrete Ausgestaltung der Leistungserbringung der öffentlichen Hand nicht standardisiert ist. Verwaltungstätigkeit kann durch ein vielschichtiges Gewebe von Einzelnormen bestimmt sein. Dieses in einer abstrakten Regel zu antizipieren, ist schwierig. Zum Beispiel würde es zu kurz greifen, nur die allgemeine verwaltungsrechtliche Verschwiegenheitspflicht zu regeln. Privatrechtlich angestellte Personen könnten dann durch die Maschen fallen.

16 Das Berufsgeheimnis der Beiständinnen zeigt dies deutlich: Die sachliche Tätigkeit verpflichtet zur Geheimhaltung, und zwar selbst dann, wenn die Beiständin selber keiner verwaltungsrechtlichen Verschwiegenheitspflicht untersteht. Vor diesem Hintergrund ist es sinnvoll, dass bereits das ZGB festhält, dass eine Beiständin eine besondere Vertrauensstellung nicht nur geniesst, sondern dieser auch gerecht werden muss (Verschwiegenheitspflicht).

b. Fachspezifika

17 Der Umgang mit Informationen ist delikat. Wer der falschen Person zu viele Informationen gibt, kann einem Anliegen vieler Personen oder einer einzelnen Person Schaden zufügen. Dabei kann die Konstellation im konkreten Einzelfall die ein und dieselbe Aussage mal als besonders gefährlich und mal als sehr belanglos erscheinen lassen.[34] Wenn Spezialgeheimnisse erlassen wurden, um darauf aufmerksam zu machen, dass die Mitarbeiterin im Steueramt sich andere Überlegungen anstellen muss als die Beiständin, dann ist dies durchaus sachgerecht. Die Bedeutung von Fachspezifika zeigt sich auch im Sozialhilferecht, wo nicht nur der Grundsatz der Verschwiegenheitspflicht, sondern auch dessen Ausnahmen besonders geregelt sind, um auf sachlich geforderte Differenzierungen eingehen zu können.[35]

18 Allerdings geht es bei diesen Differenzierungen um den ursprünglichen Gehalt der Verschwiegenheitspflicht («do not tell»[36]). In der Informationsgesellschaft und für die Zwecke des vorliegenden Fact Sheets geht es um mehr. Man muss genauer differenzieren. Man muss unterscheiden zwischen Folgendem[37]:

[33] Siehe dazu FN 37.

[34] Die Aussage «Ich war um 12h15 am Kiosk beim Bahnhof.» ist wenig bedeutsam, wenn man sich im Kreis von Bekannten zu einer Zugfahrt verabredet hat, die fünfzehn Minuten später beginnen würde. Aber sie kann bedeutsamer sein, wenn es sich bei der Aussage um ein Alibi handelt, die ausschliesst, dass die betreffende Person anderswo eine Straftat verübt hat.

[35] Der Grundsatz findet sich in der bereits erwähnten Regelung aus § 47 SHG: «Die Fürsorgebehörde und die mit der Durchführung der öffentlichen Sozialhilfe betrauten Organe und Personen (Sozialhilfeorgane) sind unter **Vorbehalt der nachfolgenden Bestimmungen** zur Verschwiegenheit über ihre Wahrnehmungen verpflichtet». (Hervorhebung nicht im Original). Zur Ausnahme in § 47a SHG siehe FN 38.

[36] Zum Beispiel § 47 SHG (FN 35).

[37] Die Darstellung stellt ab auf die Begrifflichkeiten zum Content Layer, Code Layer und Physical Layer, wie sie in Fussnote 12 zum Rechtsgutachten bereits dargestellt wurden. Zur Vereinfachung der Lesbarkeit wird hier die entsprechende Formulierung hier nochmals wiedergegeben: «HERBERT ZECH, Information als Schutzgegenstand, Basel 2012; nach Herbert Zech kann und muss man Information auf drei Ebenen beschreiben: Semantische Information wird durch ihren Aussagegehalt abgegrenzt (bei Lessig: «Content Layer», im IDG und damit auch in diesem Rechtsgutachten: «Informationen», ausser wenn es um Angaben über Personen geht, dann «Personendaten»), syntaktische Information durch ihre Darstellung als eine Menge von Zeichen (bei Lessig: «Code Layer», im IDG gibt es dafür keine Kategorie; in diesem Rechtsgutachten «Daten», ausser wenn der Begriff «Personendaten» verwendet wird – diesen Begriff verwenden wir in diesem Rechtsgutachten gleich wie das IDG, auf

1. jemand offenbart, damit die Empfängerin mit dem Gehalt der eigentlichen Information umgehen kann (d.h. es geht darum, den *Content Layer* zugänglich zu machen):

   Beispiele:

   Arbeit auf dem Content Layer*: Eine Journalistin beantragt nach § 24 Abs. 1 IDG, darüber informiert zu werden, welche Datenbanken das Steueramt für seine Tätigkeit verwendet.*

   Arbeit auf dem Content Layer*: Die Ärztin am Triemli-Spital gibt auf Ersuchen der Patientin gegenüber einer Spezialistin ausserhalb des Spitals im Rahmen eines Überweisungsschreibens Auskunft über den bisherigen Verlauf der Behandlung.*

   Arbeit auf dem Content Layer*: Die KESB zieht eine Digitalisierungsexpertin bei, damit alle bei der Fürsorgebehörde in Papierform bestehenden Daten auf einen Datenträger überführt werden, der fortan die elektronische Bearbeitung zulässt.*

   Arbeiten auf dem Content Layer: *Eine als Sozialhilfeorgan tätige Stelle meldet der zuständigen Ausländerbehörde, ab wann und in welchem Umfang eine Ausländerin Sozialleistungen bezieht. Ausserdem meldet sie weitere ihr aufgefallene Beobachtungen. Sie stellt dabei auf § 47a SHG*[38] *ab.*

2. die Arbeit zielt auf den *Physical Layer* oder den *Code Layer* der Informationsverarbeitung ab, aber es kann dabei trotzdem zu beiläufiger Kenntnis auch von Teilinformationen auf dem Content Layer kommen («incidental access»):

   Beispiele:

   Arbeit auf dem Physical Layer*: Die KESB will nach Durchlaufen der notwendigen Digitalisierungsschritte (siehe dazu das dritte Beispiel unter Punkt 1) die bei ihr noch bestehenden Papierakten vernichten («shreddern lassen»). Sie zieht ein auf solche Arbeiten spezialisiertes Dienstleistungsunternehmen bei. Deren Mitarbeiterinnen holen Papierstapel ab und werfen sie in Container. Es kann vorkommen, dass die Mitarbeiterinnen z.B. auf Ordnerrücken oder bei grosser Druckschrift auf dem Papier noch Überschriften oder andere Stichworte erkennen können, die bei fokussierter Aufmerksamkeit allenfalls gewisse (wenn auch marginale) Rückschlüsse auf den Inhalt der Papierakten zulassen würden.*

   Arbeit auf dem Code Layer*: Ein Softwareunternehmen unterstützt das Steueramt bei der Bedienung eines Computerprogramms. Im Rahmen von Supportleistungen kann es vorkommen, dass eine Mitarbeiterin des Softwareunternehmens den Bildschirminhalt einer Mitarbeiterin des Steueramts erkennen kann.*

3. jemand erhält Zugriffsgewalt über Daten, ohne dass der *Content Layer* bekannt würde[39] (Arbeit nur auf dem Physical Layer oder auf dem Code Layer):

   Beispiele:

   Arbeit auf dem Code Layer*: Die Behörde speichert verschlüsselte Daten auf einem Server einer Drittanbieterin.*

   Arbeit auf dem Code Layer*: Die Behörde speichert unverschlüsselte Daten auf einem Server einer Drittanbieterin; durch technische und organisatorische Massnahmen sind die Daten gegen den Zugriff der Mitarbeiterinnen der Drittanbieterin geschützt.*

   Arbeit auf dem Physical Layer*: Die Behörde zieht eine Dienstleisterin bei, damit diese Datenträger, auf denen vertrauliche Informationen gespeichert sind, fachkundig vernichtet («Stanzung der Datenträger»).*

19 Dass bei den in Rz. 18 geschilderten Szenarien unterschiedliche Risiken zum Tragen kommen, liegt auf der Hand. Eine Differenzierung nach dem Inhalt der geheim zu haltenden Informationen (Steuergeheimnis, Sozialhilfegeheimnis, Fürsorgegeheimnis, etc.) ist für die Beispiele in Ziffer 1 unter Rz. 18 mutmasslich sinnvoll (damit die konkreten Umstände der Informationsverwaltung berücksichtigt werden können); denn bei diesen Beispielen geht es um Austausche auf dem Content Layer, wo die ebenfalls nach dem

der Ebene des Content Layer) und strukturelle Information durch ihre Verkörperung (die Beschaffenheit der Oberfläche einer Schiefertafel spricht ebenfalls zum Menschen …).»

[38] §47a SHG lautet wie folgt: «Die Sozialhilfeorgane erstatten der zuständigen Ausländerbehörde unaufgefordert die nach Bundesrecht vorgesehenen Meldungen. Sie melden insbesondere: a. Beginn, Umfang und Beendigung des Bezugs …; b. sonstige Umstände, …».

[39] Mit Blick darauf, dass solche Szenarien möglich sind, erscheint die vorn (Rz. 12) zitierte Sachverhaltsschilderung durch Wolfgang Wohlers als ungenau und zu wenig differenziert. Die Publikation von Wolfgang Wohlers (Verweis in FN 15) adressiert Szenarien wie jene, die hier unter Punkt 3 diskutiert werden, nicht umfassend (nur die Verschlüsselung wird bei Wohlers als geeignete Schutzmassnahme aufgegriffen, andere Schutzmassnahmen bleiben ausgeklammert). Dies limitiert die Tragweite der Ausführungen von Wohlers erheblich.

Content Layer differenzierenden Spezialgeheimnisse (Steuergeheimnis, Sozialhilfegeheimnis, Fürsorgegeheimnis, etc.) allenfalls einen Unterschied machen.

20 Für die Szenarien in Ziffer 2 und Ziffer 3 von Rz. 18 kann der eigentliche Informationsgehalt jedoch nicht im Zentrum stehen, da es bei diesen Szenarien ja gerade nicht darum geht, dass die Empfängerin der Information auf dem *Content Layer* arbeiten soll (eben gerade nicht!). Es geht beim Beispiel des Aktenvernichtungsunternehmens (erstes Beispiel unter Ziffer 2 von Rz. 18) darum, dass mit den Informationsträgern gearbeitet werden soll (also auf dem *Physical Layer*). Und bei den Beispielen in Ziffer 3 von Rz. 18 geht es darum, dass mit den Daten (den eigentlichen «Informationsbehältern») gearbeitet werden soll, aber nicht mit der Information als solcher (also keine Arbeit auf dem *Content Layer*, sondern auf dem *Code Layer* – Beispiele 1 und 2 unter Ziffer 3 von Rz. 18; oder auf dem Physical Layer – Beispiel 3 unter Ziffer 3 von Rz. 18). Wo die zu beurteilenden Arbeit ihren Fokus auf den *Physical Layer* (erstes Beispiel von Ziffer 2 von Rz. 18) oder auf den *Code Layer* (Beispiele 1 und 2 unter Ziffer 3 von Rz. 18) legen, lohnt es sich nicht, die rein nach dem *Content Layer* differenzierenden Spezialgeheimnisse besonders zu unterscheiden.

c. Fazit

21 Spezialgeheimnisse entfalten ihre Wirkung allein auf dem *Content Layer*. Bei der Aufgabenstellung «Cloud» geht es allerdings um das Organisieren von *Code Layer* und *Physical Layer*. Auf dieser Ebene ist die Unterscheidung nach Spezialgeheimnissen nicht weiterführend. [40]

2. Positionsbezug zu den zehn Themen in der Debatte

22 In der Debatte wird der Fokus auf die folgenden Themen gelegt:

1. *Begehungsdelikt oder Unterlassungsdelikt*: Im Rechtsgutachten für die Stadt Zürich wird dargelegt, dass die Offenbarungsdelikte (Art. 320, Art. 321 StGB etc.) als unechte Unterlassungsdelikte zu prüfen sind.[41] Eine Tatbestandsmässigkeit als Begehungsdelikt liegt fern.

2. *Datenstandort Schweiz*: Die Analyse zu diesem Punkt weist zwei Aspekte auf. Einerseits geht es um die Beurteilung, wie effektiver Schutz gestaltet wird (Teilaspekt a), andererseits geht es um eine Analyse der oben (bei FN 19) genannten Einschätzung, dass sich schweizerisches Geheimnisrecht im Ausland nicht durchsetzen lasse (Teilaspekt b):

   - Teilaspekt a): Daten lassen sich auch bei Datenhaltung im Ausland angemessen schützen (besondere Fälle vorbehalten[42]). Im Einzelfall lassen sich bei Datenhaltung in der Schweiz aber Kosten im Umsetzungsprojekt reduzieren.[43] Wenn solche Ersparnisse im Projekt langfristig nicht durch andere Aspekte aufgewogen werden, ist ein Entscheid für Datenhaltung in der Schweiz sachlich begründbar. Für *biometrische Daten*[44] lässt sich eine Notwendigkeit der Datenhaltung in der Schweiz dann begründen, wenn diese Daten sonst nicht vor unkontrolliertem

[40] Auf Wunsch kann in separaten Fact Sheets auf weitere Spezialgeheimnisse eingegangen werden.

[41] Rechtsgutachten. Rz 90.

[42] Wenn Datenstandorte in besonders unsicheren Gegenden gewählt würden (z.B. in einem Krisengebiet), müsste man diese Würdigung neu evaluieren.

[43] In Einzelfällen kann ein Projekt mit Datenhaltung in der Schweiz auch die Kosten des Projekts reduzieren. Angesprochen ist z.B. die Schrems II-Rechtsprechung. Diese zielt auf den Schutz gegen sog. «Bulk Review» ab. Die Schrems II-Rechtsprechung bzw. die in der Folge etablierte Praxis verlangt besondere Schutzmassnahmen, welche Projekte teurer machen können. Demgegenüber entfallen solche besonderen Schutzmassnahmen bei Umsetzungsprojekten mit Datenhaltungsstandort Schweiz. Massgeblich ist die Formel «Bulk Review requires Bulk Data». Insofern reduzieren Projekte mit Datenstandort Schweiz den Aufwand im Projekt.

[44] Die Unterscheidung zwischen biometrischen Daten und Gesundheitsdaten wird hier bewusst vorgenommen. Biometrische Daten ziehen häufig eine längerfristige Gefährdung nach sich, und es können diesbezüglich potentiell sogar geopolitische Risiken ausgemacht werden. Demgegenüber ergibt sich die Schutzbedürftigkeit, die sich aus Gesundheitsdaten ergibt, in aller Regel eher aufgrund einer besonderen Nähe der betroffenen Person einerseits und der Drittperson, die darüber Kenntnis erhält (siehe vorn, Rz. 3 ff.). Daraus ergibt sich eine unterschiedliche Verortung der Risiken für biometrische Daten und Gesundheitsdaten (wobei die Risikobeurteilung für jedes Umsetzungsprojekt im Einzelfall vorzunehmen ist).

Abfluss an eine Stelle geschützt werden können und wenn die Risikoprüfung ein hohes Risiko indiziert (siehe unten, Punkt 7).

- Teilaspekt b): Eine Strafnorm kann dank ihrer Präventivwirkung als eine Art «synthetische Schutzmassnahme» betrachtet werden. Im Vergleich zu technischen und organisatorischen Massnahmen zum Schutz von Daten in der Cloud hat diese Präventivwirkung allerdings eine um Faktoren geringere Bedeutung. Wenn Daten im Ausland liegen, sind die Geheimnisdelikte in der Schweiz immer noch anwendbar (Tathandlung im Inland). Handelt die Täterin im Ausland (z.B. Offenbarung findet im Ausland statt), bleiben die Geheimnisdelikte für «schweizerische Geheimnisse» ebenfalls anwendbar.[45] Allenfalls wird die Strafverfolgung faktisch schwerer, was potentiell die Präventivwirkung abschwächen könnte. Diese Wirkung ist aber hypothetisch und würde ohnehin nur zu einer marginalen Anpassung der Risikobeurteilung im Projekt führen.

Zusammenfassend ergibt sich aus dem Geheimnisrecht (Amtsgeheimnis, Berufsgeheimnis) kein generelles Erfordernis, dass ein «Datenstandort Schweiz» gewählt werden müsste.

3. *Zugriffe nur durch Personen in der Schweiz*: Aus dem Geheimnisrecht ergibt sich keine solche Anforderung. Zur Begründung wird auf den vorstehenden Punkt 2, Teilaspekt b), verwiesen.

4. *Hilfspersoneneigenschaft*: Hier wird die Auffassung vertreten, dass als Hilfsperson gilt, wer als solche vertraglich eingebunden wurde. Es genügt Tätigwerden für die Organisationseinheit auf Basis eines Leistungsvertrags *in Kenntnis der Sondersituation*[46] der Organisationseinheit.[47] Wenn aus dem Leistungsvertrag zumindest implizit ersichtlich ist, dass die Leistungserbringerin mit Schutzpflichten für die Informationen der Organisationseinheit tätig wird, ist dies ausreichend. Cloud-Anbieterinnen können Hilfspersonen[48] sein. Dies gilt auch für Cloud-Anbieterinnen mit Sitz im Ausland.[49] Der Vertrag zur Einbindung der Hilfsperson muss Schutzpflichten zu Gunsten der Organisationseinheit vorsehen. Einen «Revers» (vertragliche Direktbeziehung zwischen der Organisationseinheit und den Mitarbeitenden der Cloud-Anbieterin) muss die Organisationseinheit nicht verlangen.

5. *Einwilligungserfordernis*: Die Nutzung von Cloud-Infrastrukturen zur Erledigung von Behördenaufgaben kann als faktisches Verwaltungshandeln verstanden werden.[50] Die Cloud-Nutzung ist rechtmässig, wenn die Voraussetzungen der sog. Schrankentrias erfüllt sind. Ist dies der Fall, ist das Staatshandeln rechtmässig.[51] Einer Einwilligung bedarf es somit nicht. Dies gilt nicht nur für den Bereich von Art. 320 StGB, sondern auch im Anwendungsbereich von Art. 321 StGB und

[45] Gl.M. Damian K. Graf: Strafbewehrter Geheimnisverrat im grenzüberschreitenden Kontext. Zu den Anwendungsgrenzen schweizerischen Strafrechts bei Geschäftsgeheimnisverletzungen, SJZ 112/2016 193 ff.

[46] Als Sondersituation wird hier bezeichnet, dass die Amtsstelle Verschwiegenheitspflichten unter dem Amtsgeheimnis (verwaltungsrechtlich und strafrechtlich) und gegebenenfalls auch unter einem Berufsgeheimnis hat.

[47] Mit dem vorliegenden Positionsbezug wird somit zum Ausdruck gebracht, dass es für die Eigenschaft als Hilfsperson nicht relevant ist, auf welche Weise die beigezogene Dienstleisterin für die Organisationseinheit tätig wird. Gleichermassen ist nicht relevant, ob die beigezogene Dienstleisterin tatsächlich Klartextzugriffe auf geschützte Informationen erhält.

[48] Im Rechtsgutachten für die Stadt Zürich wurde erörtert, dass Art. 320 StGB heute die Hilfspersoneneigenschaft noch nicht im Wortlaut vorsieht, dass der Nachvollzug dieser Regel entsprechend Art. 321 StGB aber vom Parlament bereits rechtskräftig entschieden wurde und es somit nur noch eine Frage der Zeit ist, bis die entsprechende Anpassung zum Gesetz wird. Bis dahin ergibt sich nach der hier vertretenen Auffassung diese Wirkung schon aus der Formulierung in Art. 110 Abs. 3 StGB («amtliche Funktionen ausüben»).

[49] Begründung: Das Gesetz differenziert für die Strafbarkeit der Hilfsperson nicht nach Inland und Ausland. Die Hilfsperson macht sich somit auch bei Tathandlungen im Ausland strafbar (zur Begründung siehe Punkt 2, Teilaspekt b)). Spiegelbildlich dazu ergibt sich die Privilegierungswirkung zu Gunsten der Geheimnisträgerin, die sich aus dem Hilfspersonenbegriff ergibt. Würde die Privilegierung auf Hilfspersonen «in der Schweiz» beschränkt, ergäbe sich eine Verschärfung der Strafnormen (Art. 320, Art. 321 StGB) und das Gewähren von Klartextzugriff an (nur vermeintliche) Hilfspersonen im Ausland wäre strafbar. Diese Wirkung ist im Gesetz nicht vorgesehen und ist entsprechend nach Art. 1 StGB ausgeschlossen.

[50] Vgl. PETER KARLEN, in: Peter Karlen/Susan Hodel (Hrsg.), Schweizerisches Verwaltungsrecht: Gesamtdarstellung unter Einbezug des europäischen Kontextes, 7. Auflage, Zürich 2018, 260 f.

[51] Rechtmässiges Verwaltungshandeln im Rahmen von Art. 5 BV möglich, auch wenn private Geheimhaltungsinteressen tangiert sind (Rechtsgutachten, Rz. 31).

allfälliger besonderer Verschwiegenheitspflichten. Diese Analyse gilt gleichermassen für Cloud-Angebote mit Auslandsbezügen wie für solche mit rein inländischen Bezügen.

6. *Informationsobliegenheit*: Im Umfang, wie Privatgeheimnisse bestehen, ist auf schonende Handhabung privater Interessen Rücksicht zu nehmen. Insofern ist eine Informationspflicht zu bejahen:
   - Bestehen der Pflicht: Eine Privatperson kann in vielen Fällen den Entscheid darüber, sich z.B. in ein städtisches Altersheim zu begeben oder Pflegeleistungen anderswo abzudecken, autonom fällen. Den insoweit bestehenden privaten Entscheidungsfreiraum soll die Behörde ermöglichen. Die Informationspflicht leitet sich ab aus dem allgemeinen Transparenzgebot (§ 14 Abs. 1 IDG) und aus dem Verhältnismässigkeitsgebot (soweit das Staatshandeln – dazu Punkt 5 – zu Beeinträchtigungen privater Rechtspositionen führt, ist das mildere Vorgehen zu wählen). Wo alternative Angebote zur Tätigkeit des Staats bestehen (Beispiel städtische Alterszentren), tritt auch die Wettbewerbsneutralität des Staats als Grundlage der Informationspflicht hinzu.
   - Umfang der Pflicht: Das Mass der Information kann nicht abstrakt umschrieben werden. Nach der hier vertretenen Auffassung muss die Information nicht umfassend sein und Details über die technische Lösung müssen nicht mitgeteilt werden. Die Information muss aber so substanziell sein, dass die Privatperson eine ernsthafte Möglichkeit zur Rückfrage erhält. Alsdann hat die Organisationseinheit gestützt auf § 20 Abs. 1 IDG jene Angaben offenzulegen, welche die Privatperson anfragt (Die Anfrage definiert sodann den Umfang der Informationspflicht, in den Schranken des Gesetzes).

7. *Behördenzugriffe im Ausland als Risiko*: Behördenzugriffe im Ausland sind im Bereich der hier diskutierten Aufgabenstellung (Gesundheitsdaten) nicht per se anders zu beurteilen als bereits im Rechtsgutachten beschrieben. Das Bestehen des CLOUD Act per se und die damit einhergehende Risikobeurteilung steht einer Cloud-Nutzung auch für besondere Personendaten, Gesundheitsdaten und biometrische Daten nicht entgegen. Wenn die Cloud-Nutzung standardmässig zu Datenspeicherungen in den USA führt, kann sich aus der «Schrems II»-Rechtsprechung v.a. aus Kostengründen eine Indikation für einen *Datenhaltungsstandort in der Schweiz* für *biometrische Daten*[52] ergeben (auch dann, wenn sich die diesbezüglich im Einzelfall identifizierten Risiken mit den zur Verfügung stehenden Massnahmen nicht in genügender Weise mildern lassen).

8. *Notwendigkeit der Verschlüsselung*: Für die Fragen rund um die Verschlüsselung wird auf das Fact Sheet Nr. 03 «Verschlüsselung» verwiesen («eine abstrakte Forderung nach Verschlüsselung [lässt sich] nicht aufrecht erhalten»).

9. *Wahl des Schweizerischen Rechts* (Vertragsstatut): Für die Fragen rund um das Vertragsstatut wird auf das Fact Sheet Nr. 01 «Anwendbares Recht» verwiesen («Frage des auf den Vertrag anwendbaren Schuldrechts [leistet] keinen wirksamen Beitrag für den faktischen Schutz von Daten oder Geheimnissen»). Dieses Fazit gilt gleichermassen im Anwendungsbereich des Amtsgeheimnisses wie im Anwendungsbereich des Berufs- oder anderer Spezialgeheimnisse.

10. *Gerichtsstand Schweiz*: Für die Fragen rund um den Gerichtsstand wird auf das Fact Sheet Nr. 02 «Gerichtsstand» verwiesen. Ein Vertrag mit Gerichtsstand «Schweiz» stellt keine *conditio sine qua non* für die Cloud-Nutzung dar. Dieses Fazit gilt gleichermassen im Anwendungsbereich des Amtsgeheimnisses wie im Anwendungsbereich des Berufs- oder anderer Spezialgeheimnisse.

* * *

[52] Die effektive Gefährdung durch die in Frage stehende Biometrie sollte konkret und nicht schematisch geprüft werden. Es gibt z.B. die Diskussion darüber, ob ein Passfoto ein biometrisches Personendatum darstellt (zu einem Anwendungsbeispiel siehe: https://e-idblog.ch/2021/02/20/e-id-und-biometrische-daten-worum-geht-es). Klar ist jedenfalls, dass sich bei Speicherung nur von Passfotos keine besonders schwere Gefährdung ergibt, selbst wenn das Passfoto als biometrische Angabe verstanden werden sollte.