Universität
Basel

Juristische
Fakultät

# Gutachten zum grundrechtskonformen Einsatz von M365 durch die Gemeinden im Kanton Zürich

zuhanden von egovpartner, Neumühlequai 10, Postfach, 8090 Zürich

erstattet von

Prof. Dr. Markus Schefer
Ordinarius für Staats- und Verwaltungsrecht

Dr. Philip Glass
Habilitand und Wissenschaftlicher Mitarbeiter

6. Juli 2023

Universität Basel
Juristische Fakultät
Peter Merian-Weg 8, Postfach
4002 Basel, Switzerland
ius.unibas.ch

Prof. Dr. Markus Schefer, LL.M.
Ordinarius für Staats- und Verwaltungsrecht
T +41 61 207 25 13
F +41 61 207 07 39
markus.schefer@unibas.ch

# Inhaltsverzeichnis

# 1 Fragestellung

Das vorliegende Gutachten erfolgt im Auftrag von egovpartner und untersucht die Frage, wie die Gemeinden im Kanton Zürich Cloud-Dienste (insbes. M365) verfassungs- und datenschutzkonform nutzen können. Gegenstand der Untersuchung sind die verfassungsrechtlichen Garantien von Art. 13 Abs. 2 BV sowie deren gesetzliche Konkretisierung im Datenschutzrecht und weiteren Erlassen des Kantons Zürich. Weitestgehend ausgeklammert werden hierbei die aktuell diskutierten Fragen zur sog. digitalen Souveränität.

Im Verlauf der Untersuchung werden zunächst die verfassungsrechtlichen Garantien von Art. 13 Abs. 2 BV, d.h. der Schutz vor Missbrauch von Personendaten und das Recht auf informationelle Selbstbestimmung analysiert und ihre Entwicklung über die letzten 30 Jahre nachgezeichnet. Dadurch lassen sich das Schutzobjekt der Persönlichkeit sowie die Schutzbereiche der verschiedenen Aspekte von Art. 13 Abs. 2 BV herausarbeiten. In einem weiteren Schritt wird die Eingriffsdogmatik des Datenschutzrechts rekonstruiert und hierdurch eine differenzierte Erfassung der mit der Bearbeitung von Personendaten verbundenen Eingriffsmomente ermöglicht, welche die Beurteilung von datenschutzrechtlichen Fragen in der Praxis widerspiegelt und verfassungsrechtlich aufschlüsselt. Hierbei wird gegebenenfalls auf unterschiedliche Rechtsgrundlagen für kantonale und kommunale Stellen eingegangen.

Die gewonnenen Erkenntnisse werden schliesslich für die Beurteilung der verfassungskonformen Ausgestaltung von Datenbearbeitung durch die Gemeinden im Kanton Zürich im Rahmen von M365 angewendet.

# 2 Anerkennung eines Rechts auf informationelle Selbstbestimmung in der Schweiz

## 2.1 Kantonales Verfassungsrecht

Die Verfassung des Kantons Zürich gewährleistet in Art. 11 KV ZH die «Menschenrechte und Grundrechte […] gemäss der Bundesverfassung, den für die Schweiz verbindlichen internationalen Abkommen und der Kantonsverfassung». Darüber hinaus enthält sie keine eigenständigen Garantien mit Bezug auf datenschutzrechtliche Grundrechte. Entsprechend sind auf Verfassungsebene die Garantien des Bundesrechts (Landes- und Völkerrecht) anzuwenden. Für öffentliche Organe des Kantons Zürich und der Gemeinden des Kantons Zürich werden diese in erster Linie durch das kantonale Datenschutzrecht konkretisiert.

## 2.2 Bundesverfassungsrecht

### 2.2.1 Ursprünge des Rechts auf informationelle Selbstbestimmung

Der konzeptionelle Ausgangspunkt des Rechts auf informationelle Selbstbestimmung war für die Schweiz der «Volkszählungsentscheid» des deutschen Bundesverfassungsgerichts aus dem

Jahr 1983.[1] Als Kern seines Urteils stellte das Gericht die folgende Überlegung zu den sozialen Voraussetzungen der Entwicklung und Entfaltung der Persönlichkeit ins Zentrum:

«Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.»[2]

Auf diesen grundlegenden Gedanken aufbauend umschrieb es das neue Recht auf informationelle Selbstbestimmung wie folgt:

„Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet *insoweit* die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“[3]

Dem fügte es eine weitere Einschränkung hinzu:

«Dieses Recht auf ‘informationelle Selbstbestimmung’ ist nicht schrankenlos gewährleistet. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ‘seine’ Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Das Grundgesetz hat, wie in der Rechtsprechung des Bundesverfassungsgerichts mehrfach hervorgehoben ist, die Spannung Individuum - Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden […]. Grundsätzlich muss daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen.»[4]

In neuerer Zeit hat das deutsche Bundesverfassungsgericht die klassische Formel des informationellen Selbstbestimmungsrechts präzisiert. Zwischen Privaten entfaltet das Grundrecht nunmehr ein «Recht auf substanzielle Mitentscheidung» bezüglich den gegenüber der eigenen Person erfolgenden Zuschreibungen von Informationen bzw. Daten.[5]

[1] Urteil des Deutschen Bundesverfassungsgerichts, BVerfGE 65, 1 [Volkszählung] vom 15.12.1983.
[2] BVerfGE 65, 1, C II. 1 a.
[3] BVerfGE 65, 1, C II. 1. a (Hervorhebung durch die Autoren).
[4] BVerfGE 65, 1, C II. 1. b.
[5] BVerfG, 06.11.2019 – 1 BvR 16/13 – Recht auf Vergessen I, N 86.

Für den weiteren Verlauf der vorliegenden Untersuchung erscheint es von entscheidender Bedeutung, den Vorgang der Übernahme dieses Grundrechts in das schweizerische Recht richtig einzuordnen. Hierbei ist zu betonen, dass die deutsche Rechtsprechung nicht «en bloc» in die schweizerische Verfassung verpflanzt wurde. Vielmehr übernahm das Bundesgericht das Konzept der informationellen Selbstbestimmung als Rechtsgrundsatz von Verfassungsrang und damit die Idee der Persönlichkeit als grundrechtliches Schutzobjekt gegenüber der Datenbearbeitung durch Dritte. Diese Idee setzte es in den Kontext der schweizerischen Rechtsordnung. In der Folge wurde allerdings die schweizerische Variante des Grundrechts nicht mit der erforderlichen strukturellen Klarheit in die Schweizer Verfassungs- und Rechtsordnung eingebettet, obwohl etwa die Totalrevision der Bundesverfassung von 1999 eine gute Möglichkeit dafür geboten hätte.

Der Blick zurück auf die Entstehungsgeschichte und die weitere Entwicklung der informationellen Selbstbestimmung in der Schweiz offenbart dementsprechend eine gewisse Vermischung der privatrechtlichen und öffentlich-rechtlichen Aspekte der Ausgestaltung eines solchen Rechts. Insgesamt bemühte sich das Bundesgericht auch nicht, die beiden Normenkomplexe des datenbasierten Persönlichkeitsschutzes dogmatisch mit der nötigen Präzision auseinanderzuhalten.

### 2.2.2 Die informationelle Selbstbestimmung im Bundesrecht

#### *2.2.2.1 Allgemeines*

Die schweizerische Bundesverfassung kennt, anders als das europäische Recht,[6] kein ausdrücklich geschriebenes Recht auf Datenschutz. Ebenso wenig kennt die Bundesverfassung – wie bereits angedeutet wurde – ein ausdrücklich geschriebenes Recht auf informationelle Selbstbestimmung.[7] Stattdessen wurde im Zuge der Nachführung im Rahmen der Totalrevision von 1999 mit Art. 13 Abs. 2 BV ein Recht auf Schutz vor Missbrauch der persönlichen Daten als Teilaspekt des in Art. 13 Abs. 1 BV garantierten Rechts auf eine persönliche Geheimsphäre eingeführt. Der Wortlaut von Art. 13 Abs. 2 BV ist anerkanntermassen zu eng geraten.[8] Die informationelle Selbstbestimmung ist nach wie vor ein ungeschriebener Teilgehalt von Art. 28 ZGB auf der einen und Art. 13 Abs. 2 BV i.V.m. Art. 10 BV auf der anderen Seite, was zu gewissen Unsicherheit in Bezug auf Auslegung und Dogmatik geführt hat.

Der Schutz von Art. 13 Abs. 2 BV enthält zwei Aspekte: einmal eine Schutzgarantie und einmal ein Abwehrrecht. Erstens dürfen staatliche Organe Personendaten nur bearbeiten, «wenn

[6] Vgl. Art. 8 Charta der Grundrechte der Europäischen Union (2012/C 326/02); Teilgehalte sind der Schutz der persönlichen Daten, die Durchsetzungsrechte sowie das Recht auf eine unabhängige Datenschutzaufsicht.

[7] In der Literatur werden indes die grundrechtlichen Ansprüche auf Missbrauchsschutz und informationelle Selbstbestimmung bisweilen als «Grundrecht auf Datenschutz» zusammengefasst; zuletzt SHK DSG-FEY, Art. 1 N 17 ff.

[8] BSK BV-DIGGELMANN, Art. 13 N 33; OFK BV-BIAGGINI, Art. 13 N 11; SGK-SCHWEIZER, Art. 13 BV N 72.

dies notwendig ist, wenn die Bearbeitung zweckgebunden erfolgt und verhältnismässig ist», und zweitens soll der Schutz vor Missbrauch «durch Einsichts- und Berichtigungsrechte der betroffenen Person sichergestellt» werden.[9] Die Einsichtsrechte sind mittlerweile in den Datenschutzgesetzen von Bund und Kantonen enthalten und wurden in der bundesgerichtlichen Praxis verschiedentlich bestätigt.[10]

#### *2.2.2.2 Entwicklung eines Einsichtsrechts zum Schutz der Persönlichkeitsentfaltung*

Die in der Botschaft von 1996 erwähnten Einsichtsrechte waren einige Jahre zuvor vom Bundesgericht anerkannt worden. In zwei grundlegenden Entscheiden aus dem Jahr 1987 beurteilte das Bundesgericht die Frage, welche Rechte jenen Personen zustehen, deren Personendaten von staatlichen Stellen bearbeitet werden.

In BGE 113 Ia 1 vom 28. Januar 1987 stellte das Bundesgericht mit Bezug auf die Einsichtnahme in ein polizeiliches Register fest, dass zur «umfassenden Wahrung» des Anspruchs auf rechtliches Gehör aus Art. 4 aBV «ein Anspruch auf Akteneinsicht für den unmittelbar Betroffenen grundsätzlich auch ausserhalb jeglichen Verfahrens» besteht.[11] Das hierzu unter den damaligen Regeln der Bundesrechtspflege erforderliche rechtlich geschützte Interesse erblickte es in einem allgemeinen Interesse an der Kenntnis der über die eigene Person festgehaltenen Daten und dem Bedürfnis, prüfen zu können, ob diese korrekt registriert worden seien. Dieses Interesse könne «angesichts der technischen Möglichkeiten der Datenbearbeitung nicht mehr als unerheblich bezeichnet werden». Weiter könne es «der einzelne Bürger durchaus als Unbehagen und als Beeinträchtigung seiner Privatsphäre empfinden, wenn die Verwaltung personenbezogene Daten über längere Zeit hinweg aufbewahrt und allenfalls weitere Verwaltungsstellen zu diesen Daten auf unbestimmte Zeit hinaus Zugang haben».[12]

Neben der möglichen Beeinträchtigung der Privatsphäre wies das Gericht weiter darauf hin, dass «die Einsicht in den streitigen Registereintrag […] darüber hinaus einen engen Bezug zu den verfassungsmässigen Rechten, insbesondere zum ungeschriebenen Grundrecht der persönlichen Freiheit» habe und entsprechend eng mit dem Schutz der elementaren Erscheinungen der Persönlichkeitsentfaltung verbunden sei. Wohl mit Blick auf den Volkszählungsentscheid des Bundesverfassungsgerichts, den es an anderer Stelle in einem Verweis erwähnte,[13] fügte das Bundesgericht einschränkend hinzu, dass «die persönliche Freiheit nicht die Funktion einer allgemeinen Handlungsfreiheit» habe.[14] Es verwies dabei auf seine Rechtsprechung,

[9] Botschaft über eine neue Bundesverfassung vom 20. November 1996, BBl 149 I 1, 153.
[10] OFK BV-BIAGGINI, Art. 13 N 14 m.w.H.
[11] BGE 113 Ia 1, E. 4.a.
[12] BGE 113 Ia 1, E. 4.b.aa.
[13] BGE 113 Ia 1, E. 5.a.
[14] BGE 113 Ia 1, E. 4.b.aa.

wonach die Intensität der Beeinträchtigung der persönlichen Entfaltung im Einzelfall ausschlaggebend ist.[15] Implizit passte das Gericht somit das aus dem deutschen Recht übernommene Konzept eines Rechts auf informationelle Selbstbestimmung an den Schutzbereich des (damals noch ungeschriebenen) Rechts auf Persönliche Freiheit an.[16]

In BGE 113 Ia 257 vom 3. Juni 1987 bestätigte das Gericht dieses Recht auf Einsicht in Daten, die über eine Person bei staatlichen Behörden bearbeitet werden. Es stützte sich wiederum auf die ungeschriebene Garantie der persönlichen Freiheit. Diese schütze «alle Grundfreiheiten, deren Ausübung für die Entwicklung der menschlichen Person wesentlich ist».[17] In Verbindung mit Art. 28 ZGB, der die Würde und den Wert des Menschen schütze und den Inhaber staatlicher Gewalt anhalte, in Ausübung seiner Macht die Persönlichkeit der Betroffenen zu respektieren, verleihe die Persönliche Freiheit, unabhängig von den gesetzlichen Regeln zur Akteneinsicht ein Recht, über die Bearbeitung von Personendaten zur eigenen Person durch die betreffende Behörde informiert zu werden.[18] Im Hinblick auf die zunehmende elektronische Datenbearbeitung auf allen Ebenen der Verwaltung forderte das Bundesgericht zudem, dass diesem Recht eine zunehmend wichtige Rolle für den Schutz des Individuums beigemessen werde.[19]

Im selben Zeitraum entwickelten auch Teile der Lehre zivilrechtliche Einsichtsrechte als Teilgehalt des Persönlichkeitsschutzes von Art. 28 ZGB.[20] Ähnlich wie in BGE 113 Ia 257 wurde dieses Recht im Hinblick auf das autonome Individuum als Träger der Persönlichkeitsrechte bzw. auf «das dem Art. 28 ZGB zugrundeliegende Menschenbild» entwickelt.[21] Dies stellte zugleich den Beginn einer Abkehr von der Sphärentheorie dar, die man für Fragen des Persönlichkeitsschutzes im Rahmen der elektronischen Datenbearbeitung für unpassend erklärte.[22] Als bessere Alternative wurde die Unterscheidung zwischen "sensiblen" und "freien", d.h. frei durch Dritte nutzbare persönliche Informationen vorgeschlagen,[23] die konzeptionell in der

[15] Siehe dazu BGE 107 Ia 52, 56, E. 3.b.
[16] Begründet in BGE 102 Ia 321; siehe dazu EVA MARIA BELSER, Der Grundrechtliche Rahmen des Datenschutzes, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann, Datenschutzrecht - Grundlagen und öffentliches Recht, Bern 2011, S. 325.
[17] BGE 113 Ia 257, E. 4.b.; «toutes les libertés élémentaires dont l'exercice est indispensable à l'épanouissement de la personne humaine».
[18] BGE 113 Ia 257, E. 4.b.
[19] BGE 113 Ia 257, E. 4.d.
[20] Siehe dazu ROLF HUBER, Rechtsprobleme der Personalakte, Diss. Univ. Zürich 1985, S. 41.
[21] ROLF HUBER, Rechtsprobleme der Personalakte, Diss. Univ. Zürich 1985, S. 44 f.;
[22] ROLF HUBER, Rechtsprobleme der Personalakte, Diss. Univ. Zürich 1985, S. 43 f. m.w.H.; PIERRE TERCIER, Le nouvea droit de la personnalité, Zürich 1984, N 467 ; REGINA E. AEBI-MÜLLER, Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes – Unter besonderer Berücksichtigung der Rechtslage in der Schweiz und in Deutschland, Bern 2005, N 611 f.; PHILIP GLASS, Die rechtsstaatliche Bearbeitung von Personendaten in der Schweiz, Zürich 2017, S. 168.
[23] PIERRE TERCIER, Le nouvea droit de la personnalité, Zürich 1984, N 468.

heutigen gesetzlichen Unterscheidung zwischen besonderen bzw. besonders schützenswerten und gewöhnlichen Personendaten zum Ausdruck kommt.

Mit diesen zwei parallelen Entwicklungen im Verfassungs- und Zivilrecht waren die Kerngedanken des datenschutzrechtlichen Privatsphären- und Persönlichkeitsschutzes bereits im schweizerischen Recht präsent, bevor sie ausdrücklich als «neues» Recht auf informationelle Selbstbestimmung in die bundesgerichtliche Rechtsprechung Eingang fanden. Zugleich wird deutlich, dass den Ursprüngen der informationellen Selbstbestimmung in der Schweiz ein mehrheitlich prozeduraler Charakter anhaftete, der die Rechtsdurchsetzung durch die Betroffenen betonte. Dies änderte sich im Rahmen der Ausarbeitung des ersten Datenschutzgesetzes des Bundes.

#### *2.2.2.3 Von der prozeduralen zur strukturellen Garantie*

Die Botschaft zum Datenschutzgesetz von 1988 erklärte die zentrale Formel des Rechts auf informationelle Selbstbestimmung – die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen – zur Grundlage des neuen Datenschutzgesetzes und bezog sich dabei ausdrücklich auf das Volkszählungsurteil des deutschen Bundesverfassungsgerichts.[24] Darüber hinaus führte der Bundesrat aus, dass ein Datenschutzgesetz verhindern müsse, «dass der einzelne zu einem rechtlosen Objekt von Informationstätigkeiten wird». Vielmehr solle er «Bild und Kenntnisse, die die Umwelt von ihm hat, mitbestimmen können». Aus diesem Grund habe jeder Mensch «grundsätzlich ein Recht, zu erfahren, wer was über ihn weiss und zu welchen Zwecken die entsprechenden Daten bearbeitet werden», da er nur so «in seiner privaten, beruflichen und gesellschaftlichen Tätigkeit jeweils situationsgereicht entscheiden» könne.[25]

Nach Auffassung des Bundesrates lag es nicht mehr primär in der Verantwortung des Einzelnen, den Überblick über die bei verschiedenen Dritten bearbeiteten «eigenen» Daten zu behalten. Vielmehr verschob sich das Gewicht hin zu einer Pflicht der Datenbearbeiter, die Betroffenen zu informieren bzw. deren Daten in transparenter Weise zu bearbeiten; ein Umstand, der sich in der Einführung des gesetzlichen Grundsatzes der erkennbaren Datenbearbeitung[26] sowie in gesetzlichen Informationspflichten der Bearbeiter niederschlug. Für den Kanton Zürich besteht zudem in § 12a IDG ZH eine Meldepflicht bei unbefugter Bearbeitung

[24] Botschaft DSG 1988, 418, Fn. 6.
[25] Botschaft DSG 1988, 418 (Hervorhebung durch die Autoren).
[26] Vgl. allg. Art. 4 Abs. 4 DSG betr. Grundsatz der Erkennbarkeit der Beschaffung sowie des Bearbeitungszwecks von Personendaten; vgl. spezifisch Art. 14 DSG betr. Beschaffung von besonders schützenswerten Personendaten durch Private; Art. 18 DSG bei der Beschaffung von Personendaten durch Bundesorgane; neu in Art. 19 nDSG betr. Information über die Bearbeitung von Personendaten durch Private oder Bundesbehörden sowie Transparenzpflicht; analog in Art. 25 nDSG im Rahmen der Auskunft; vgl. für den Kanton Zürich § 12 IDG ZH betreffend Informationspflicht über die Beschaffung von Personendaten.

oder Verlust von Daten mit Grundrechtsrelevanz. Auf Bundesebene wird neu in Art. 24 nDSG eine Meldepflicht in Bezug auf Verletzungen der Datensicherheit eingeführt.[27]

Wenige Jahre nach Inkrafttreten des ersten DSG des Bundes und vor der Totalrevision der Bundesverfassung fällte die zivilrechtliche Abteilung des Bundesgerichts mit BGE 120 II 118 den ersten publizierten bundesgerichtlichen Entscheid, der ausdrücklich ein Recht auf Informationelle Selbstbestimmung begründete. Dabei nahm es die vorangegangenen Diskussionen zu Art. 28 ZGB auf, ging indes nicht auf die analoge Rechtsprechung zu Art. 4 aBV ein. Vielmehr bezog es sich auf das noch ziemlich neue Datenschutzgesetz. In der Frage, welche Einsichtsrechte den Arbeitnehmenden bezüglich ihrer eigenen Personalakte zustehen, führte das Gericht aus, dass das Obligationenrecht ein solches Recht nicht ausdrücklich vorsehe, dass in «Übereinstimmung mit der überwiegenden Meinung in der Lehre […] ein solches Recht jedoch als Ausfluss des Persönlichkeitsschutzes des Arbeitnehmers (Art. 328 Abs. 1 OR) anzuerkennen» sei. Weiter stellte es fest, dass dieses Einsichtsrecht «als Teil des informationellen Selbstbestimmungsrechtes zu verstehen [sei], das auch der Datenschutzgesetzgebung des Bundes [zugrunde liege]».[28]

Seit diesem Entscheid aus dem Jahr 1994 hat das Bundesgericht seine Position in mehreren Entscheiden dem Grundsatz nach bestätigt und die Formel dahingehend erweitert. Nach konstanter Rechtsprechung bildet das Recht auf informationelle Selbstbestimmung einen Teilgehalt von Art. 13 Abs. 2 BV[29] sowie von Art. 8 EMRK[30] und «schützt den Einzelnen vor Beeinträchtigungen, die durch die staatliche Bearbeitung seiner persönlichen Daten entstehen»[31]. Als Rechtsgrundlage der Beeinträchtigung, und damit Teil des Schutzbereichs der informationellen Selbstbestimmung, anerkannte das Gericht verschiedene Grundrechte, insb. die Persönliche Freiheit bzw. die Entfaltung elementarer Aspekte der Persönlichkeit[32] und den Schutz der Geheim- und Privatsphäre (Art. 13 BV).[33]

Insgesamt hat das Gericht den sachlichen Schutzbereich nur vereinzelt konkretisiert, ihn aber weder allgemein umschrieben noch wesentlich begrenzt.[34] Insbesondere hat es nie präzisiert,

[27] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBL 2017 6941, 7063 f.
[28] BGE 120 II 118, 121 E. 3.
[29] BGE 147 I 346, E. 5.3.1.
[30] BGE 147 II 408, E. 6.3.
[31] BGE 122 I 360, E. 5; BGE 129 I 232
[32] BGE 113 Ia 1, E.4.; BGE 122 I 360, E. 5.
[33] BGE 129 I 232, E. 4.3.1.
[34] Vgl. etwa 138 II 346 (Google Street View), 359 f. bezüglich dem Recht am eigenen Bild; vgl. auch den Hinweis bei BEAT RUDIN, in: Beat Rudin/Bruno Baeriswyl (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt IDG, Zürich Basel Genf 2014 (zit. als PraKomm IDG BS-VERFASSERIN, Art. … N …), Grundlagen N 2, wonach sich das Gericht «nie vertieft und umfassend» mit dem Recht auf informationelle Selbstbestimmung auseinandergesetzt hat.

was unter einer Beeinträchtigung zu verstehen sei, bzw. wann eine rechtlich relevante Beeinträchtigung durch staatliche Datenbearbeitung angenommen werden könne. Entsprechend hat es sich auch nie zum qualitativen Unterschied zwischen der privaten und der verfassungsrechtlichen informationellen Selbstbestimmung geäussert. Die dadurch entstandene Rechtsunsicherheit hat im Lauf der Jahre zu kritischen Wortmeldungen in der Lehre geführt,[35] welche dem Recht verschiedentlich «Konturlosigkeit»[36] oder auch «Inhaltsleere»[37] attestierten.

In der neueren Rechtsprechung ist denn auch zu beobachten, dass die Bearbeitung von Personendaten grundsätzlich als Eingriff in Art. 13 abs. 2 BV bewertet wird, ohne dass eine Verbindung zu einem grundrechtlichen Schutzbereich erforderlich erscheint.[38] Das Gericht geht hierbei von einem sehr weiten Schutzbereich aus, wonach «grundsätzlich ohne Rücksicht darauf, wie sensibel die fraglichen Informationen tatsächlich sind, jede Person gegenüber fremder, staatlicher oder privater Bearbeitung von sie betreffenden Informationen bestimmen können muss, ob und zu welchem Zweck diese Informationen über sie bearbeitet werden».[39] Im Ergebnis sieht es danach aus, als würde das Bundesgericht seine ursprüngliche, eng an die Privat- und Geheimsphäre sowie die Persönliche Freiheit angelehnte Konzeption der informationellen Selbstbestimmung aufweichen und sich der deutschen Rechtsauffassung annähern. Auf die Strukturierung dieses doch sehr weit gezogenen Schutzbereichs wird noch zurückzukommen sein.[40]

Beachtenswert ist schliesslich, dass die Parlamentarische Initiative Vischer «Grundrecht auf informationelle Selbstbestimmung», welche die informationelle Selbstbestimmung ausdrücklich in der Verfassung verankern wollte,[41] mit Beschluss des Nationalrats abgeschrieben wurde.[42] Hierbei folgte die Ratsmehrheit dem Minderheitsantrag, der die Initiative für überflüssig erklärte, da das Recht auf informationelle Selbstbestimmung bereits in Art. 13 Abs. 2 BV garantiert sei.[43] Der Verzicht auf eine ausdrückliche Erwähnung in der Verfassung von 1999

[35] Siehe dazu die Übersicht über die (insb. deutsche) Lehre bei NADJA BRAUN BINDER/THOMAS BURRI/MELINDA FLORINA LOHMANN/MONIKA SIMMLER/FLORENT THOUVENIN/KERSTIN NOËLLE VOKINGER, Künstliche Intelligenz: Handlungsbedarf im Schweizer Recht, in: Jusletter 28. Juni 2021, Fn. 31.
[36] AEBI-MÜLLER (Fn. 20), N 597.
[37] THOMAS GÄCHTER/PHILIPP EGLI, Informationsaustausch im Umfeld der Sozialhilfe, in: Jusletter vom 6.9.2010, N 28.
[38] Vgl. zuletzt BGE 147 I 346, E. 5.3 betreffend einen automatischen Wasserzähler.
[39] BGE 144 I 126, E. 4.1.
[40] Siehe 4.
[41] Parlamentarische Initiative 14.413 vom 21. März 2014.
[42] Beschluss des Nationalrats vom 29. September 2017, 14.413 Ref. 15815.
[43] Vgl. Votum Nantermod 14.413/15815; Bericht der Staatspolitischen Kommission des Nationalrats vom 18. August 2017 zu 14.413/14.434, S. 4.

ist entsprechend nicht als Einschränkung des Gehalts von Art. 13 Abs. 2 BV zu verstehen, sondern lediglich als bewussten Verzicht auf eine ausdrückliche Aufnahme von ungeschriebenem Verfassungsrecht in den Text der damals neuen Bundesverfassung.[44]

#### *2.2.2.4 Konkretisierung auf Gesetzesebene*

Der offene Schutzbereich der informationellen Selbstbestimmung und der weiteren datenschutzrechtlichen Verfassungsgarantien wird im schweizerischen Recht auf Gesetzesebene konkretisiert.[45] Die Datenschutzgesetze des Bundes und des Kantons Zürich bezwecken ausdrücklich «den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden»[46] bzw. «die Grundrechte von Personen zu schützen, über welche die öffentlichen Organe Daten bearbeiten»[47]. Dieser enge Konnex zwischen Verfassung und Gesetz bedeutet, dass gewisse Gesetzesbestimmungen auch zur Konkretisierung der verfassungsrechtlichen Garantien heranzuziehen sind. Für den Kanton Zürich wurde dies nun ausdrücklich auf höchstrichterlicher Ebene bestätigt.

Im Entscheid VB.2020.00648 des Verwaltungsgerichts des Kantons Zürich vom 16. Dezember 2021 stellte das Gericht fest, dass gewisse gesetzliche Bestimmungen aus dem Datenschutzrecht für die Verfassungsauslegung herangezogen werden müssen und unabhängig von ihrer Grundlage im Datenschutzgesetz einen Schutzgehalt aufweisen, der im Rahmen von Art. 35 BV zu verwirklichen ist. Es handelt es sich hierbei um die folgenden Grundsätze der Datenbearbeitung: rechtmässige Beschaffung, Bearbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Verhältnismässigkeit, Datenrichtigkeit, Wahrung der Datensicherheit sowie Beschränkungen der Datenweitergabe ins Ausland, wenn kein gleichwertiger Persönlichkeits- bzw. Datenschutz besteht.[48] Daraus folgernd stellte das Gericht fest, dass öffentliche Organe, soweit ihre Tätigkeit vom Geltungsbereich des Datenschutzgesetzes ausgenommen sind, diese Grundsätze als verfassungsrechtliche Garantien umsetzen müssen.

#### *2.2.2.5 Rezeption in der Lehre*

In der Lehre wurde die bundesgerichtliche Konzeption des Rechts auf informationelle Selbstbestimmung unterschiedlich aufgenommen, überwiegend aber übernommen.[49] Kritische

[44] Siehe die Hinweise bei RAINER SCHWEIZER, in: Bernhard Ehrenzeller/Benjamin Schindler/Rainer J. Schweizer/Klaus A. Vallender (Hrsg.), Die schweizerische Bundesverfassung - St. Galler Kommentar, 3. A., St. Gallen 2014, Art. 13 N 70 (zit. als SG Komm-VERFASSERIN, BV … N …).

[45] EVA MARIA BELSER, Der Grundrechtliche Rahmen des Datenschutzes, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann, Datenschutzrecht - Grundlagen und öffentliches Recht, Bern 2011, S. 418.

[46] Art. 1 DSG bzw. Art. 1 nDSG, nunmehr beschränkt auf natürliche Personen.

[47] § 1 Abs. 2 Bst. b IDG ZH.

[48] VB.2020.00648, E. 4.1.

[49] JÖRG PAUL MÜLLER/ MARKUS SCHEFER, Grundrechte in der Schweiz - Im Rahmen der Bundesverfassung, der EMRK und der UNO-Pakte, 4. Auflage, Bern 2008, S. 164; SGK-SCHWEIZER, Art. 13 BV N 72; zurückhaltend OFK BV-BIAGGINI, Art. 13 N 11.

Stimmen wiesen insbesondere darauf hin, dass mit der Konzeption des Rechts auf informationelle Selbstbestimmung die damit verbundene informationsrechtliche Dimension der allgemeinen Handlungsfreiheit aus Art. 2 Abs. 1 GG[50] in das schweizerische Recht übernommen würde.[51] Dies würde dazu führen, dass «dem Einzelnen im Bereich der staatlichen Informationsbearbeitung ein umfassendes Verfügungsrecht über sämtliche ihn betreffenden Daten zukäme».[52] Im Hinblick auf die Auswirkungen auf den privatrechtlichen Persönlichkeitsschutz wurde zudem bemängelt, dass das neue Recht weit über das Ziel hinaus schiesse, da es diesen unnötig erweitere indem es eine eigentumsähnliche Position des Einzelnen im Hinblick auf die «eigenen» Daten suggeriere und dabei den Sozialbezug des Individuums ausser Acht lasse.[53]

# 3 Persönlicher Schutzbereich

Der persönliche Schutzbereich der Grundrechts auf informationelle Selbstbestimmung ist an die Persönlichkeit und damit an die Menschenwürde gekoppelt.[54] Träger sind sämtliche Person im Sinne des Zivilgesetzbuches im Umfang der ihnen zukommenden Persönlichkeitsrechte. Entsprechend erlischt der Schutz mit dem Tod,[55] wobei Gesetzgebung und Rechtsprechung gewisse Nachwirkungen der Persönlichkeit vorsehen, die das Datenschutzrecht betreffen.[56]

# 4 Sachlicher Schutzbereich

## 4.1 Allgemeines

Der sachliche Schutzbereich von Art. 13 Abs. 2 BV orientiert sich am Schutzobjekt der Persönlichkeit[57] und umfasst verschiedene Formen der Verletzung. Diese zeigen sich zum einen in einer personenbezogenen Verletzung rechtsstaatlicher Minimalstandards, und zum anderen in der Verletzung der informationellen Autonomie. Die Beeinträchtigung erfolgt durch eine informationelle Erfassung der Privat- bzw. Geheimsphäre, die zu einem «Unbehagen»[58] bzw.

[50] Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 (BGBl 1).
[51] AEBI-MÜLLER (Fn. 20), N 595; THOMAS GÄCHTER/PHILIPP EGLI, Informationsaustausch im Umfeld der Sozialhilfe, in: Jusletter vom 6.9.2010, N 24; EVA MARIA BELSER, Zur rechtlichen Tragweite des Grundrechts auf Datenschutz: Missbrauchsschutz oder Schutz der informationellen Selbstbestimmung?, in: Astrid Epiney/Tobias Fasnacht/Gaëtan Blaser (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung/Instruments de mise en oeuvre du droit à l'autodétermination informationnelle, Bern 2013, S. 33 ff.
[52] EVA MARIA BELSER, Der Grundrechtliche Rahmen des Datenschutzes, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann, Datenschutzrecht - Grundlagen und öffentliches Recht, Bern 2011, S. 400.
[53] AEBI-MÜLLER (Fn. 20), N 597.
[54] AEBI-MÜLLER (Fn. 20), N 17.
[55] Eingehend AEBI-MÜLLER (Fn. 20), N 327 ff.; siehe auch BK ZGB-BUCHER/AEBI-MÜLLER, ZGB 11 N 46; Stämpfli HK DSG-RUDIN, Art. 5 N 16 ff.
[56] Eingehend J.P. MÜLLER/SCHEFER (Fn. 50), S. 155 ff.
[57] Zum Konnex zwischen sachlichem Schutzbereich und Schutzobjekt siehe dazu MARKUS SCHEFER, Gefährdung von Grundrechten: eine grundrechtsdogmatische Skizze, in: Thomas Sutter-Somm/Felix Hafner/Gerhard Schmid/Kurt Seelmann (Hrsg.), Risiko und Recht – Festgabe zum schweizerischen Juristentag 2004, Basel 2004, S. 462 f.
[58] BGE 113 Ia 1, E. 4.b.aa.

einer subjektiv empfundenen Beeinträchtigung der Betroffenen führt, welche eine Selbstbeschränkung in der Ausübung von Grundrechten zur Folge haben kann. Diese Form der mittelbaren Einschränkung der Grundrechte wird als Einschüchterungseffekt bzw. Abschreckungswirkung oder auch *chilling effect* (franz. «effet dissuasif») bezeichnet.[59]

Das Bundesgericht äussert sich insgesamt nicht in kohärenter Weise zur Frage eines Massstabs zur Bestimmung der Abschreckungswirkung. Es deutet indes verschiedentlich an, dass es sich hierbei um einen vornehmlich subjektiven, auf Plausibilität im Einzelfall gestützten Massstab handelt, und dass der Nachweis einer tatsächlichen Einschüchterung nicht notwendig ist, um einen Grundrechtseingriff anzunehmen. So stellte es in BGE 146 I 11 bezüglich der Erhebung von Kontrollschild, Identität des Halters und Insassen, Zeitpunkt, Standort und Fahrtrichtung im Rahmen der Aufzeichnungen der automatischen Fahrzeugfahndung und Verkehrsüberwachung fest, dass «die Möglichkeit einer späteren (geheimen) Verwendung (dieser Daten; Anm. d. Autoren) durch die Behörden und das damit einhergehende *Gefühl der Überwachung* die Selbstbestimmung wesentlich hemmen [*könnten*]».[60] In BGE 140 I 2 erachtete das Gericht das Erfordernis eines konkreten Anhaltspunktes für einen Verdacht auf das Mitführen gefährlicher Gegenstände als Voraussetzung für die intensive körperliche Durchsuchung von Matchbesuchern als ausreichend, um die *Befürchtungen* der Beschwerdeführer zu entkräften, eine Vielzahl interessierter Personen würde durch die mögliche Durchsuchung unter den Kleidern und gar im Intimbereich vom Besuch eines Spiels abgehalten werden.[61] In BGE 133I 77 stellte es fest, dass eine gewisse Aufbewahrungsdauer von Videoaufzeichnungen zur nachträglichen repressiven Strafverfolgung notwendig sei, «um die durch eine wirksame Strafverfolgung *erhoffte Abschreckungswirkung* sicherzustellen».[62] Gemäss BGE 143 I 147 ist es für die Annahme einer Abschreckungswirkung schliesslich ausreichend, wenn eine gesetzliche Grundlage mangels Bestimmtheit «grundsätzlich geeignet» ist, die Betroffenen von der Ausübung ihrer Grundrechte abzuhalten.[63] Dies muss für sämtliche Aspekte einer Datenbearbeitung gelten, die eine solche Eignung zur Abschreckung aufweisen; mithin kann hierfür auf das zentrale Stichwort des Kontrollverlusts zurückgegriffen werden: Jedes Moment des Kontrollverlusts über Informationen, welche die Entwicklung der Persönlichkeit bzw. die Ausübung der hierzu instrumentalen Grundrechte abbildet, ist grundsätzlich geeignet, eine abschreckende Wirkung im Hinblick auf die Ausübung dieser Rechte zu entfalten.

[59] BGE 146 I 11, E. 3.2.; BGE 143 I 147, E. 3.3.; eingehend MARKUS SCHEFER, Gefährdung von Grundrechten: eine grundrechtsdogmatische Skizze, in: Thomas Sutter-Somm/Felix Hafner/Gerhard Schmid/Kurt Seelmann (Hrsg.), Risiko und Recht – Festgabe zum schweizerischen Juristentag 2004, Basel 2004, S. 449 f.
[60] BGE 146 I 11, E. 3.2 (Hervorhebung durch die Autoren).
[61] BGE 140 I 2, E. 10.6.3 (Hervorhebung durch die Autoren).
[62] BGE 133 I 77, E. 5.2 (Hervorhebung durch die Autoren).
[63] BGE 143 I 147, E. 11.

## 4.2 Missbrauchsschutz als Minimalerfordernis der Datenbearbeitung

Nach seinem Wortlaut schützt Art. 13 Abs. 2 BV vor dem «Missbrauch» von «persönlichen Daten». Aus dem Missbrauchsverbot folgt, dass jeder staatliche Umgang mit «persönlichen» Daten gewissen Minimalerfordernissen unterworfen ist. Die Botschaft zum Vorentwurf von 1996 drückte dies dahingehen aus, dass „staatliche Organe Personendaten nur bearbeiten dürfen, wenn dies notwendig ist, wenn die Bearbeitung zweckgebunden erfolgt und verhältnismässig ist".[64] Für Datenbearbeitungen, die keinen Eingriff in die Grundrechte darstellen, entspricht dies weitestgehend den Grundsätzen staatlichen Handelns in Art. 5 BV.[65] Darüber hinaus muss aufgrund der Garantien in Art. 9 BV jede Datenbearbeitung willkürfrei und nach Treu und Glauben erfolgen. Sind diese Voraussetzungen nicht erfüllt, greift der Missbrauchsschutz von Art. 13 Abs. 2 BV.

Im Ergebnis bedeutet dies, dass Art. 13 Abs. 2 BV ausserhalb des Schutzbereichs der informationellen Selbstbestimmung dem Einzelnen einen Anspruch auf Durchsetzung seiner Datenschutzrechte gegen personenbezogene Datenbearbeitungen einräumt, welche diese grundsätzlichen Rechtsstaatsgarantien verletzen. Entsprechend wohnt den rechtsstaatlichen Grundsätzen i.V.m. Art. 13 Abs. 2 BV eine individualrechtliche Komponente des Persönlichkeitsschutzes inne.

## 4.3 Sachlicher Schutzbereich der informationellen Selbstbestimmung

Wie Art. 13 Abs. 2 BV insgesamt ist auch der Schutz des darin garantierten Rechts auf informationelle Selbstbestimmung auf das Schutzobjekt der Persönlichkeit gerichtet. Die Persönlichkeit ist kein statisches, sondern ein dynamisches, sich beständig veränderndes Schutzobjekt, dass sich gerade dadurch auszeichnet, von Mensch zu Mensch unterschiedlich ausgestaltet zu sein. Der Schutz kann sich deshalb nicht darin erschöpfen, einen Status quo zu bewahren, sondern muss vielmehr die Möglichkeit der Veränderung in sich aufnehmen.

Die Bundesverfassung trägt diesem Umstand Rechnung, indem sie einerseits Grundrechte garantiert, die spezifische Aspekte der Persönlichkeit erfassen, und andererseits die Persönlichkeit insgesamt durch eine subsidiäre Garantie schützt, die zum Tragen kommt, wenn grundlegende Aspekte menschlicher Existenz betroffen sind, die nicht durch ein spezifisches Grundrecht geschützt sind.[66] Zugleich garantiert die Bundesverfassung keinen umfassenden Schutz im Sinne einer allgemeinen Handlungsfreiheit.[67]

[64] Botschaft über eine neue Bundesverfassung vom 20. November 1996, BBl 1996 I 1, 153.
[65] Siehe den Hinweis bei PraKomm IDG BS-RUDIN, 9 N 14; vgl. auch den Hinweis bei OFK-BIAGGINI, Art. 36 N 23.
[66] J.P. MÜLLER/SCHEFER (Fn. 50), S. 43.
[67] Siehe dazu Fn. 14 u. 17.

Geschützt sind daher die zur Entwicklung der Persönlichkeit bzw. zur Ausübung der Grundrechte als Ausdruck der Persönlichen Freiheit[68] i.S.d. «elementaren Erscheinungen der Persönlichkeitsentfaltung»[69] notwendigen Bedingungen.[70] Ziel ist der Erhalt einer substanziellen Autonomie des Einzelnen angesichts staatlicher (und privater) Datenbearbeitung.

# 5 Eingriffe in den Schutzbereich durch Datenbearbeitung

## 5.1 Bearbeitung als Rechtsbegriff

Der Begriff der Bearbeitung umfasst im Geltungsbereich des Datenschutzrechts gemäss den jeweils ähnlich lautenden Definitionen in den Datenschutzgesetzen von Bund und Kantonen «[jeden] Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten» (nDSG) bzw. «[jeden] Umgang mit Informationen wie das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben oder Vernichten» (IDG ZH). Zusammengenommen beschreiben diese Formen der Bearbeitung zugleich den sog. Lebenszyklus von Personendaten.[71] Als Bearbeitung gelten im Umkehrschluss sämtliche Formen der Datenbearbeitung über den gesamten Lebenszyklus eines Datums hinweg.

## 5.2 Planung von Datenbearbeitungen

Von der Bearbeitung der Daten ist die Planung von Datenbearbeitungen zu unterscheiden. Mit Inkrafttreten des revidierten Datenschutzgesetzes im September 2023 wird die Planung von Datenbearbeitungen ausdrücklich in Art. 7 DSG geregelt sein, der die Pflichten zur Umsetzung des Datenschutzes durch Technik bzw. von datenschutzfreundlichen Voreinstellungen umschreibt.[72] Demgemäss muss der Verantwortliche für die Datenbearbeitung diese Pflichten nunmehr «ab der Planung» berücksichtigen.

Für das Recht des Kantons Zürich können diese beiden Pflichten im Sinne einer Gesamtanalogie aus den verschiedenen vorgelagerten Risikoanalyse- und Schutzpflichten hergeleitet werden. Zu nennen sind hier etwa die Datenschutzfolgenabschätzung und die Vorabkontrolle (§

[68] Vgl. dazu EVA MARIA BELSER, Zur rechtlichen Tragweite des Grundrechts auf Datenschutz: Missbrauchsschutz oder Schutz der informationellen Selbstbestimmung?, in: Astrid Epiney/Tobias Fasnacht/Gaëtan Blaser (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung / Instruments de mise en oeuvre du droit à l'autodétermination informationnelle, Zürich 2013, S. 27.
[69] BGE 113 Ia 1, 6.
[70] PHILIP GLASS, Datenschutzrecht für künstliche Intelligenz in der öffentlichen Verwaltung – Eine Auslegeordnung am Beispiel des Kantons Zürich, in: Michael Widmer (Hrsg.), Datenschutz – Rechtliche Schnittstellen, Zürich 2023, S. 202; EVA MARIA BELSER, Zur rechtlichen Tragweite des Grundrechts auf Datenschutz: Missbrauchsschutz oder Schutz der informationellen Selbstbestimmung?, in: Astrid Epiney/Tobias Fasnacht/Gaëtan Blaser (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung / Instruments de mise en oeuvre du droit à l'autodétermination informationnelle, Zürich 2013, S. 30 f.
[71] GLASS (Fn. 20), S. 119 f.
[72] Sog. *privacy by design* bzw. *privacy by default*; siehe 6.6.3.3.

10 IDG ZH), die Pflicht zur Gestaltung von Datenbearbeitungssystemen im Hinblick auf die Umsetzung des Grundsatzes der Vermeidung des Personenbezugs (Art. 11 IDG ZH) oder die Pflicht zur Qualitätssicherung (Art. 13 IDG). Entsprechend muss die Rechtmässigkeit einer künftigen Datenbearbeitung bereits im Zeitpunkt der Planung sichergestellt werden.

## 5.3 Begründung des Eingriffs

### 5.3.1 Eingriff durch persönlichkeitsrelevanten Umgang mit Daten

Lehre und Rechtsprechung gehen im Allgemeinen davon aus, dass der Schutzbereich des verfassungsrechtlichen Anspruchs auf Datenschutz aus Art. 13 Abs. 2 BV jeden Umgang mit Personendaten erfasst.[73] Ein Teil der Lehre folgert aus der Übernahme des Begriffs der informationellen Selbstbestimmung aus dem deutschen Verfassungsrecht zudem, dass jeder staatliche Umgang mit Personendaten einen zu rechtfertigenden Grundrechtseingriff darstellt.[74] Beide Ansichten erfordern eine Präzisierung.

Personenbezogene Datenbearbeitungen von öffentlichen Organen sind Mittel zur Erledigung von gesetzlichen Aufgaben und als solche dem Gesetzmässigkeitsprinzip unterworfen, d.h. sie erfolgen stets zweckgebunden bzw. sind stets auf einen Zweck auszurichten.[75] Sie können damit unter Umständen auch eine Form des tatsächliches Verwaltungshandelns und damit Realakte der Verwaltung darstellen. Als Realakt wird Verwaltungshandeln bezeichnet, das nicht auf einen rechtlichen, sondern einen tatsächlichen Erfolg gerichtet ist. Auch ohne unmittelbare Wirkung auf Rechte und Pflichten kann von solchen Handlungen eine mittelbare Rechtswirkung ausgehen.[76]

Der «tatsächliche Erfolg», auf den die personenbezogene Bearbeitung von Daten gerichtet ist, besteht darin, eine Person zu identifizieren und dieser nunmehr bestimmten Person die mittels der Daten nutzbar gemachte Information (oder auch die «Aufzeichnungen»[77] oder «Angaben»[78]) zuzuordnen. Für rechtliche Handlungsformen der öffentlichen Organe, etwa eine Verfügung, ein Vertrag oder auch eine Wegweisung unter Aufnahme der Personalien, hat dies die Zuordnung von normativen Entscheidungen und somit eine mittelbare rechtliche Wirkung

[73] SG Komm-SCHWEIZER, BV 13 N 74 m.w.H., «jeder Umgang »; OFK BV-Biaggini, Art. 13 N 11 m.w.H., «jede staatliche Bearbeitung»; SHK DSG-Fey, Art. 1 N 18, «jeder Umgang»; JÖRG PAUL MÜLLER/ MARKUS SCHEFER, Grundrechte in der Schweiz - Im Rahmen der Bundesverfassung, der EMRK und der UNO-Pakte, 4. Auflage, Bern 2008, S. 170.
[74] THOMAS GÄCHTER/PHILIPP EGLI, Informationsaustausch im Umfeld der Sozialhilfe, in: Jusletter vom 6.9.2010, N 28, «Jeder staatliche Umgang mit personenbezogenen Daten und Informationen erscheint dann als Grundrechtseingriff, wäre also grundsätzlich verboten, sofern er nicht über Art. 36 BV gerechtfertigt werden könnte».
[75] PraKomm IDG ZH-HARB, § 9 N 1.
[76] ULRICH HÄFELIN/GEORG MÜLLER/FELIX UHLMANN, Allgemeines Verwaltungsrecht, 8. üb. A. Zürich/St. Gallen 2020, N 1408.
[77] Siehe die Definition in § 3 Abs. 2 IDG ZH.
[78] Vgl. den Wortlaut von Art. 3 BSt. a DSG bzw. Art. 5 Bst. A nDSG.

für die Betroffenen zur Folge. Die mittelbare Rechtsfolge kann – muss aber nicht – einen Eingriff in die Grundrechte der Betroffenen bedeuten. Ob ein Grundrechtseingriff vorliegt, muss anhand des Schutzbereichs der informationellen Selbstbestimmung ermittelt werden.

Anlässlich der Darstellung des sachlichen Schutzbereichs wurde an anderer Stelle darauf hingewiesen, dass dieser durch das Schutzobjekt der Persönlichkeit bestimmt wird.[79] Das Gesetz konkretisiert den Eingriff in die Persönlichkeit und dessen Voraussetzungen in § 3 Abs. 4 Bst. a IDG i.V.m. § 8 Abs. 2 IDG sowie Art. 10 Abs. 2 KV ZH i.V.m. Art. 36 Abs. 1 BV, indem es Kriterien für die Qualifizierung und die Bearbeitung von besonderen Personendaten festlegt. Dadurch wird die verfassungsrechtliche Bewertung der Datenbearbeitung teilweise vorweggenommen, indem die Bearbeitung von besonderen Personendaten grundsätzlich als eigenständiger, schwerer Eingriff in die Grundrechte qualifiziert wird.[80]

Unterhalb der Schwelle des schweren Grundrechtseingriffs macht das Gesetz keine weiteren Vorgaben bezüglich Normstufe und –dichte. Für Datenbearbeitungen, die einen leichten Eingriff in die Grundrechte begründen und jene, die den Schutzbereich der Grundrechte mangels Eingriffsqualität nicht berühren, gelten damit grundsätzlich dieselben Voraussetzungen, namentlich zumindest das Erfordernis einer impliziten, durch die gesetzliche Aufgabe notwendigerweise begründete Ermächtigung zur personenbezogenen Datenbearbeitung.[81]

### 5.3.2 Bestimmung der Eingriffsqualität einer Datenbearbeitung

Die Kriterien zur Bestimmung der Eingriffsqualität einer personenbezogenen Datenbearbeitung ergeben sich aus der Formel der informationellen Selbstbestimmung. Sie umfassen erstens die Übersicht der Betroffenen über die staatliche Datenbearbeitung und zweitens die diesbezügliche Kontrollmöglichkeit durch Wahrnehmung von wirksamen Einsichts- und Durchsetzungsrechten. Es erscheint sinnvoll, hier zwischen dem tatsächlichen und dem rechtlichen Kontrollverlust zu unterscheiden. Ein tatsächlicher Kontrollverlust liegt vor, wenn eine Person die im Hinblick auf ihre Person erfolgenden Datenbearbeitungen nicht (mehr) überblicken und/oder nachvollziehen kann, in dieser Hinsicht unwissend ist oder faktisch zur Offenbarung von persönlichen Angaben gezwungen wird. Dagegen liegt ein rechtlicher Kontrollverlust vor, wenn die Person ihre diesbezüglichen Einsichts-, Berichtigungs-, Löschungs- und Beschwerderechte nicht wirksam nutzen kann. Zu beachten ist, dass ein Kontrollverlust der bearbeitenden Behörde sich als Kontrollverlust bei den Betroffenen manifestiert, auf diese in gewisser Weise durchschlägt.

[79] Siehe 4.
[80] SHK DSG-BAERISWYL, Art. 8 N 13; siehe auch SHK DSG-MUND, Art. 34 N 12.
[81] GLASS (Fn. 20), S. 193 f. m.w.H.

Drittens ist schliesslich vorausgesetzt, dass die Datenbearbeitung einen genügenden Bezug zur rechtlich geschützten Persönlichkeit einer Person, d.h. die erforderliche Persönlichkeitsnähe aufweist. Dies ist erfüllt, wenn die durch die bearbeiteten Daten genutzte Information die rechtlich geschützten Persönlichkeitsgüter und/oder die grundrechtlich geschützten Entfaltungsmöglichkeiten der Person betreffen, mithin dem Schutzbereich der informationellen Selbstbestimmung zugerechnet werden können. Der Eingriff wiegt umso schwerer, je grösser die Persönlichkeitsnähe der Datenbearbeitung ist.[82]

Zusammengefasst liegt ein Eingriff in die informationelle Selbstbestimmung dann vor, wenn die betroffene Person einen tatsächlichen und/oder rechtlichen Kontrollverlust über die ihr zugeschriebenen Daten erleidet, und die Datenbearbeitung genügend Persönlichkeitsnähe aufweist, um eine Persönlichkeitsverletzung zu begründen. Die Intensität des Eingriffs, auf die im Folgenden näher eingegangen wird, ergibt sich jeweils aus dem Zusammenwirken dieser beiden Aspekte der Datenbearbeitung.

## 5.4 Bestimmung der Intensität des Eingriffs

### 5.4.1 Vorweg: Datenbearbeitung als Bündel von Grundrechtseingriffen

Ein Problem der Bewertung von Eingriffen durch Datenbearbeitung kann darin liegen, dass diese oftmals Ergebnisse eines komplexes Zusammenspiels verschiedener Merkmale der Datenbearbeitung darstellen, die je für sich möglicherweise unbedenklich erscheinen, d.h. weder einen signifikanten Kontrollverlust noch eine intensive Persönlichkeitsnähe aufweisen, die aber erstens je einzeln und zweitens in einer Gesamtschau des Bearbeitungsprozesses einen Grundrechtseingriff begründen können.[83]

Aus diesem Grund erscheint es sinnvoll, vor der Bewertung der Gesamtschau zuerst den Bearbeitungsprozess im Hinblick auf seine grundrechtlichen Eingriffsmomente zu entbündeln. Als grundrechtliche Eingriffsmomente sollen hierbei jene Aspekte der Datenbearbeitung bezeichnet werden, die für sich je eigene, spezifische Verletzungen der Grundrechte bewirken können. Als «gebündelt» werden die Eingriffe deshalb bezeichnet, weil sie dasselbe Schutzobjekt, d.h. die Persönlichkeit derselben Person betreffen.

[82] BGE 107 Ia 52, 56, E. 3.b.; J.P. MÜLLER/ SCHEFER (FN. 50), S. 170.

[83] Implizit bei PraKomm IDG ZH-BAERISWYL, § 8 N 6 ff., wonach die Verhältnismässigkeit sich aus dem Zweck der Bearbeitung, den verwendeten Daten und den sichernden Massnahmen ergibt; siehe auch den Hinweis bei EVA MARIA BELSER, in: Belser/Epiney/Waldmann, Datenschutzrecht, Bern 2011, § 12 N 61, wonach die Verhältnismässigkeit der Datenbearbeitung sowohl die Zulässigkeit als auch für die Art und Weise sowie den Zweck einer zu prüfenden Datenbearbeitung betrifft.

Als typische Eingriffsmomente gelten die Kriterien zur Bestimmung von besonderen Personendaten, insb. die Art der Daten, der Zweck der Bearbeitung sowie Aspekte der Art, des Umfangs und der Umstände der Bearbeitung.[84] Das Gesetz nennt überdies zwei spezifische Merkmale der Bearbeitung, die für sich je einen Eingriff von hoher Intensität begründen, namentlich die Möglichkeit der Verknüpfung von Daten mit anderen Daten i.S.v. § 3 Abs. 4 Bst. a IDG sowie die Bearbeitung von «Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit natürlicher Personen erlauben» (Profilbildung) i.S.v. § 3 Abs. 4 Bst. b IDG. Schliesslich sind die Dauer der Bearbeitung[85] sowie die Komplexität des Gesamtprozesses[86] zu beachten.

Zu beachten ist, dass jedes Eingriffsmoment der Datenbearbeitung einen je eigenen Eingriff in die Grundrechte der Betroffenen darstellt und als solcher je einzeln gemäss Art. 36 BV gerechtfertigt werden muss. Jeder dieser Eingriffe ist somit unabhängig von den übrigen Bearbeitungsmodalitäten darauf hin zu überprüfen, ob eine genügende gesetzliche Grundlage sowie ein genügendes öffentliches Interesse besteht und ob die spezifische Ausgestaltung dieses Aspekts der Bearbeitung verhältnismässig ist. Soweit ein Eingriffsmoment von geringer Intensität notwendigerweise mit gesetzlich legitimierten Eingriffsmomenten verknüpft ist, kann – analog der impliziten Bearbeitungsgrundlage für unbedenkliche Datenbearbeitungen – dieses Moment als implizit mitgeregelt gelten.

Da die gebündelten Eingriffe alle dasselbe Schutzobjekt betreffen, muss schliesslich geprüft werden, ob sie in ihrem Zusammenspiel im Rahmen des Bearbeitungsprozesses eine unverhältnismässige Belastung für die Betroffenen begründen. Während also jedes Eingriffsmoment für sich nach seiner Intensität grundrechtlich zu rechtfertigen ist, muss die resultierende Gesamtbelastung der Datenbearbeitung für die Betroffenen im Rahmen von Art. 36 BV gerechtfertigt erscheinen.

### 5.4.2 Die Eingriffsmomente im Einzelnen

#### *5.4.2.1 Art der Daten*

Die Frage nach der Art der Daten verweist auf die gesetzliche Unterscheidung zwischen Personendaten und besonderen/besonders schützenswerten Personendaten.[87] Eine dritte Kategorie, die allerdings *prima vista* keine Gefahr für die Persönlichkeit indiziert, bilden die Sachdaten, d.h. Daten ohne (genügenden) Personenbezug.[88]

[84] SHK DSG-Baeriswyl, Art. 8 N 21 ff.; Bewertung der Angemessenheit von Massnahmen der Datensicherheit.
[85] GLASS (Fn. 20), S. 136 f.
[86] Implizit bei SHK DSG-MUND, Art. 34 N 9; «Komplexität der zu treffenden Entscheidungen»; ebenso EVA MARIA BELSER, in: Belser/Epiney/Waldmann, Datenschutzrecht, Bern 2011, § 12 N 45.
[87] SHK DSG-BAERISWYL, Art. 8 N 21;
[88] Zum Personenbezug siehe PraKomm IDG ZH-BAERISWYL, § 3 N 16 f.

Die Kategorie der besonderen Personendaten umfasst nach kantonal-zürcherischem Recht alle Daten, die vom Gesetzgeber als besonders sensitiv qualifiziert werden. Inhaltlich umfasst der Begriff zunächst Daten, durch welche Informationen aus einem gesetzlich geschützten Lebensbereich i.S.v. § 3 Abs. 4 Bst. a Ziff. 1-4 IDG abgebildet werden oder die ein Persönlichkeitsprofil i.S.v. § 3 Abs. 4 Bst. b IDG bilden. Darüber hinaus erfasst der Begriff gemäss § 3 Abs. 4 Bst. a IDG auch Daten, die wegen ihrer Bedeutung, d.h. inhaltlich eine den gesetzlichen Datenkategorien gleichwertige Gefahr der Persönlichkeitsverletzung begründen. Weiter fallen unter den Begriff der besonderen Personendaten gemäss § 3 Abs. 4 Bst. a IDG Daten, die mit anderen Daten verknüpfbar sind. Es handelt sich somit nicht um ein inhaltliches, sondern um ein technisches Kriterium.

Schliesslich bezeichnet das Gesetz als besondere Personendaten auch Daten, von denen aufgrund der Art ihrer Bearbeitung eine besondere Gefahr einer Persönlichkeitsverletzung ausgeht. Dies betrifft offensichtlich nicht die «Art der Daten», sondern die Modalitäten des Bearbeitungsprozesses, worauf sogleich näher eingegangen wird. Wichtig ist, dass auch der Umgang mit Daten, die inhaltlich an und für sich unbedenklich erscheinen, eine Bearbeitung von besonderen Personendaten darstellen kann.[89]

#### *5.4.2.2 Zweck*

Der Zweck der Bearbeitung kann in verschiedener Hinsicht einen eigenständigen schweren Eingriff in die informationelle Selbstbestimmung begründen. Grundsätzlich besteht für Aufgaben der öffentlichen Organe die gesetzliche Eingriffsvermutung der Bearbeitung von besonderen Personendaten i.S.v. § 3 Abs. 4 Bst. a IDG ZH, soweit sich aus der Verknüpfung der staatlichen Aufgabe mit einer Person eine Gefahr für die Persönlichkeit ergibt. Dies trifft insbesondere für Aufgaben zu, die vom Gesetzgeber als sensitiv beurteilt werden. So gelten sämtliche Daten, die zur Erfüllung von gesetzlichen Aufgaben in den Bereichen der sozialen Hilfe (§ 3 Abs. 4 Bst. a Ziff. 3 IDG) oder der administrativen bzw. strafrechtlichen Verfolgung und Sanktionen (§ 3 Abs. 4 Bst. a Ziff. 4 IDG) als besondere Personendaten.[90]

#### *5.4.2.3 Art und Umfang der Bearbeitung*

Der Begriff der Art der Bearbeitung bezeichnet die technischen Verfahren des Umgangs mit Daten, worunter auch die technische Infrastruktur sowie insbesondere der Einsatz von Clouddiensten fällt.[91] Es handelt sich hierbei um eines der gesetzlich geregelten Kriterien für die Bestimmung von besonderen Personendaten gemäss § 3 Abs. 4 Bst. a IDG. Demgemäss gelten als besondere Personendaten alle Daten, «bei denen wegen […] der Art ihrer Bearbeitung […] eine besondere Gefahr der Persönlichkeitsverletzung besteht». Für die Annahme eines eigenständigen Eingriffs ist entscheidend, dass die Art der Bearbeitung eine vom Inhalt der Daten

[89] Siehe 5.4.2.3.
[90] Zu diesen Kategorien im Einzelnen SHK DSG-RUDIN, § 5 N 32 f.
[91] SHK DSG-BAERISWYL, Art. 8 N 23.

zu unterscheidende Gefahr der Persönlichkeitsverletzung begründet. Dies bedeutet umgekehrt, dass Personendaten, die nicht aufgrund ihres Inhalts als sensitiv zu werten sind, je nach Art der Bearbeitung dennoch als besondere Personendaten gelten können.

Der Begriff des Umfangs der Datenbearbeitung umfasst zwei unterschiedliche Aspekte, die je eigene spezifische Gefahren der Persönlichkeitsverletzung bergen, und die entsprechend je ein gesetzliches Kriterium für die Beurteilung des Risikos im Rahmen der Vorabkontrolle bilden. Zum einen kann damit die Anzahl der Personen bezeichnet werden, die von einer Datenbearbeitung betroffen sind (§ 24 Abs. 1 Bst. e IDV), zum anderen die Anzahl der bearbeiteten Datenkategorien (§24 Abs. 1 Bst. b IDV). Entsprechend kann eine Bearbeitung zugleich im Hinblick auf die Zahl der Betroffenen sowie im Hinblick auf den Umfang der bearbeiteten Datenkategorien je für sich einen schwerwiegenden Eingriff darstellen.

Weitere ausdrücklich festgelegte Kriterien der Art der Bearbeitung, die ein eigenes schweres Eingriffsmoment begründen, sind die Bereitstellung von Personendaten im Abrufverfahren (§ 24 Abs. 1 Bst. a IDV), der Einsatz neuer Technologien (§ 24 Abs. 1 Bst. c IDV) und die gemeinsame Bearbeitung durch mindestens drei öffentliche Organe (§ 24 Abs. 1 Bst. d IDV).

#### *5.4.2.4 Umstände der Bearbeitung*

Der Begriff der Umstände der Bearbeitung ist in Literatur und Praxis wenig ausgebildet bzw. lediglich vage umschrieben und wird vorwiegend anhand von Beispielen definiert; so werden etwa die Dauer der Bearbeitung, Aspekte der Datenerhebung oder die Bekanntgabe ins Ausland genannt.[92] Es handelt sich hierbei offenbar um ein Auffangkriterium, das jene Eingriffsmomente erfasst, die keiner der übrigen Kategorien zugerechnet werden. Im Hinblick auf die genannten Beispiele sowie die Notwendigkeit einer Abgrenzung zu den übrigen Kategorien scheint es naheliegend, dass damit vor allem Begleitumstände der «Art der Bearbeitung» gemeint sind, die allenfalls ein eigenes Risiko für die Persönlichkeit der Betroffenen begründen. Als weitere Beispiele können hier wohl die Datensicherheit und die tatsächliche Datenherrschaft sowie die Ausbildung der mit der Bearbeitung betrauten Mitarbeiterinnen, deren Spielraum mit Bezug auf rechtlich relevante Aspekte der Bearbeitung oder auch das für die Bearbeitung verfügbare Budget genannt werden.

# 6 Verfassungsrechtliche Beurteilung des Einsatzes von M365

## 6.1 Einleitend zum Begriff Cloud-Computing

Der Begriff Cloud-Computing bezeichnet ein Modell der Datenbearbeitung, bei dem ein Teil der benötigten Computerressourcen (Server, Speicher, Applikationen, Rechenleistung, Nutzeraccounts etc.) flächendeckend über ein Netzwerk von einem Dritten als Dienstleistung zur Verfügung gestellt werden. Es ist auf die Bereitstellung eines «allgegenwärtigen, bequemen

[92] SHK DSG-BAERISWYL, Art. 8 N 25.

und bedarfsgerechten Netzzugangs zu einem gemeinsamen Pool konfigurierbarer Rechenressourcen»[93] ausgerichtet. Im Rahmen von Cloud-Computing findet keine dauerhafte Zuweisung von physischer Hardware statt, vielmehr werden die Ressourcen des Anbieters von seinen Kundinnen und Kunden nach Bedarf geteilt.[94] Dies ermöglicht es den Anbietern, ihre Ressourcen optimal auszulasten bzw. im Sinne einer «elastische Skalierung» den Bedürfnissen der Kunden anzupassen.[95] Die folgenden Funktionen definieren das Modell:[96]

- *on-demand self-service*, der es den Usern erlaubt, die benötigten Ressourcen in Anspruch zu nehmen;
- ein universeller, netzbasierter Zugriff für die Datenbearbeitung auf verschiedenen Gerätekategorien;
- geteilte physische und virtuelle Ressourcen, die je nach Nachfrage der Nutzerinnen und Nutzer dynamisch und stets wieder neu zugewiesen werden;
- eine dynamische oder elastische, allenfalls auch automatisierte Skalierung der Kapazitäten nach Bedarf;
- eine Quantifizierung von Nutzungsparametern, die Monitoring, Kontrolle und Transparenz mit Bezug auf die tatsächlich genutzten Ressourcen ermöglichen.

In der Praxis wird zwischen drei Grundmodellen von Dienstleistungspaketen unterschieden, namentlich Software as a Service (SaaS), d.h. die Online-Verfügbarkeit von Software (die vor Ort/on-premise oder online betrieben werden kann), Plattform as a Service (PaaS), d.h. Nutzbarmachung einer Plattform für die Softwareentwicklung, insb. Laufzeit- und Entwicklungsumgebungen sowie Infrastructure as a Service (IaaS), d.h. Nutzbarmachung von IT-Infrastruktur mittels Fernzugriff.[97] Im letzteren Fall wird nicht Software, sondern Hardwareleistung (z.B. Rechenleistung, Speicher, Netzwerkarchitektur) über das Netz zur Verfügung gestellt. Die Un-

[93] PETER MELL/TIMOTHY GRANCE, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, US Department of Commerce, Special Publication 800-145, Gaithersburg 2011, S. 2 f.
[94] AXEL FREIHERR VON DEM BUSSCHE, Branchenübergreifende Sonderkonstellationen im IT-Sicherheitsrecht – I. Cloud Computing, in: Dennis-Kenji Kipker (Hrsg.), Cybersecurity – Rechtshandbuch, 1. Auflage, München 2020, Kapitel 4 N 69.
[95] VON DEM BUSSCHE, Branchenübergreifende Sonderkonstellationen im IT-Sicherheitsrecht, in: Dennis-Kenji Kipker (Hrsg.), Cybersecurity – Rechtshandbuch, 1. Auflage, München 2020, Kapitel 4 N 69.
[96] Siehe die Zusammenfassung bei PETER MELL/TIMOTHY GRANCE, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, US Department of Commerce, Special Publication 800-145, 2011, S. 2 f.
[97] PETER MELL/TIMOTHY GRANCE, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, US Department of Commerce, Special Publication 800-145, 2011, S. 2 f.; EDÖB, Erläuterungen zu Cloud Computing, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/cloud-computing/erlaeuterungen-zu-cloud-computing.html (undatiert; Abruf 23. März 2023); VON DEM BUSSCHE, Branchenübergreifende Sonderkonstellationen im IT-Sicherheitsrecht, in: Dennis-Kenji Kipker (Hrsg.), Cybersecurity – Rechtshandbuch, 1. Auflage, München 2020, Kapitel 4 N 70.

terscheidung zwischen den drei Grundmodellen erfolgt danach, welche Komponenten des Gesamtsystems vom Anbieter kontrolliert werden und welcher Teil die Kundin oder der Kunde selber kontrolliert.[98]

Schliesslich wird danach unterschieden, wer die Cloud wo und für wen betreibt. Die Bandbreite erstreckt sich diesbezüglich von internen, für eine bestimmte Gruppe von Usern betriebenen *private clouds*, über öffentlich zugängliche *public clouds* bis hin zu Mischformen, sog. *hybrid clouds*.[99] Daraus ergibt sich, dass Cloud-Architekturen Mit Bezug die Betreiber, den physischen Ort sowie den Nutzerkreis in verschiedenen Graden offen oder geschlossen sein können, was sich jeweils auf die mit der Nutzung zusammenhängenden Cloudrisiken auswirkt.

## 6.2 Regulatorisches Umfeld der Nutzung von M365 im Kanton Zürich

Aktuell ist die Nutzung von M365 durch öffentliche Organe des Kantons Zürich grundsätzlich vorgesehen.[100] Zur Durchsetzung der rechtlichen Anforderungen an die Datenbearbeitung wurden gewisse Grundsätze und Regeln erlassen (RL M365 ZH).[101] Die öffentlichen Organe werden angehalten, die von ihnen bearbeiteten Daten nach zwei Klassifikationssystemen zu beurteilen. Aus geschäftlicher Sicht sind dies die Kategorien der öffentlichen, internen, vertraulichen und geheimen Daten, aus datenschutzrechtlicher Sicht jene der besonderen Personendaten und übrigen Personendaten.[102]

In einem zweiten Schritt wird festgelegt, welche Formen der Nutzung von M365 für die jeweiligen Datenkategorien zulässig sind. Hierbei gelten für besondere Personendaten dieselben Grundsätze wie für vertrauliche und geheime Daten.

- Lokale Office 365 Apps (SaaS on premise): Uneingeschränkte Bearbeitung im Rahmen der rechtlichen Bearbeitungsbefugnis des öffentlichen Organs;
- Online Office 365 Apps (SaaS online): Keine Bearbeitung;
- Exchange Online (Outlook, E-Mail): Bearbeitung beschränkt auf verschlüsselte Daten;
- MS Teams ohne Aufzeichnung: Uneingeschränkte Bearbeitung im Rahmen der rechtlichen Bearbeitungsbefugnis des öffentlichen Organs.

[98] MELL/GRANCE (Fn. 101), S. 3.
[99] MELL/GRANCE (Fn. 101), S. 3.
[100] Siehe den Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich, Sitzung vom 30. März 2022 - 542. Einsatz von Cloud-Lösungen in der kantonalen Verwaltung (Microsoft 365), Zulassung (zit. RRB NR. 542/2022), Ziff. 1 i.V.m. IKT-Strategie Kanton Zürich, Ziff. 3; jeweils keine rechtliche Geltung gegenüber den Gemeinden.
[101] Finanzdirektion des Kantons Zürich, Allgemeine Nutzungsrichtlinie Microsoft 365, RL vom 27. Januar 2023 (Stand 1. Februar 2023; zit. RL M365 ZH); keine rechtliche Geltung gegenüber den Gemeinden.
[102] RL M365 ZH, Ziff. 1.5.

Weitere Apps, namentlich weitere Funktionen von Teams (insb. Aufzeichnung, Hochladen von Dateien in den Chat), Share Point sowie OneDrive for Business (Speicherung/Zugänglichmachen von Daten in der MS Cloud), dürfen nicht zur Bearbeitung von besonderen Personendaten eingesetzt werden.[103]

Neben der RL M365 ZH sind auch die Vorgaben zur Bearbeitung von Personendaten in Clouddiensten von U.S.-Anbietern der DSB Kanton Zürich zu beachten.[104] Diese präzisieren insbesondere die Frage der Verschlüsselung. Für besondere Personendaten und aus geschäftlicher Sicht ähnlich sensible Daten gilt, dass sie verschlüsselt werden müssen und das Schlüsselmanagement beim öffentlichen Organ liegt. Dies bedeutet, dass eine lediglich vertragliche Absicherung des Einsatzes von Schlüsseln durch Microsoft nicht genügt.[105]

Unklar ist, was dies im Einzelnen bedeutet, insbesondere ob das öffentliche Organe das Schlüsselmanagement beispielsweise an das Amt für Informatik des Kantons oder an Dritte abtreten darf. Aus den Vorgaben wird zumindest ersichtlich, dass das Ziel des differenzierten Schlüsselmanagements für die Bearbeitung von verschlüsselten besonderen Personaldaten darin besteht, dass die Kontrolle über die Schlüssel nicht beim Anbieter des Clouddienstes verbleibt.

## 6.3 Spezifische Eingriffsmomente der Nutzung von M365

### 6.3.1 Cloud-Computing als Bearbeiten im Auftrag i.S.v. § 6 IDG

Cloud-Anwendungen, wie sie im Rahmen von M365 angeboten werden, ermöglichen verschiedene Kombinationen von Software- und Infrastrukturdienstleistungen, also eine Mischform mit Elementen von SaaS und IaaS. Die in der Suite enthaltenen Apps, insb. MS Office, können entweder vor Ort (*on premise*) oder online benutzt werden.[106] Der Kern des Modells «Cloud-Computing» im Sinne von SaaS (online) und IaaS liegt in der Bearbeitung von Daten im Herrschaftsbereich eines Dritten. Daten der Bearbeiterin werden auf Datenträgern bzw. einer informationstechnologischen Infrastruktur bearbeitet, die unter der organisatorischen sowie rechtlichen Kontrolle eines Dritten stehen – je nach Konfiguration der Cloud über den gesamten Lebenszyklus der Daten hinweg, d.h. die einzelnen Bearbeitungsformen Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Zugänglichmachen oder Vernichten i.S.v. § 3 Abs. 5 IDG.[107] Von Interesse sind vorliegend zwei Konstellationen: erstens die Bearbeitung

[103] RL M365, Ziff. 2.
[104] DSB Kanton Zürich, Besondere datenschutzrechtliche Aspekte der Cloud Nutzung – unter Berücksichtigung des «CLOUD Act» (ausgenommen Schulen), V 1.2. / September 2022; diese beanspruchen keine Rechtsverbindlichkeit, können indes im Einzelfall mittels einer Empfehlung i.S.v. § 36 IDG und nachfolgender Verfügung gegenüber dem öffentlichen Organ gemäss § 36a IDG Verbindlichkeit erlangen.
[105] Vgl. dazu DSB Kanton ZH, Verschlüsselung der Daten im Rahmen der Auslagerung – unter Inanspruchnahme von Informatikleistungen und unter Berücksichtigung der Geheimnispflichten, V 2.3. Juli 2022, Fn 2.
[106] Siehe 6.2.
[107] DSB Kanton Zürich, Leitfaden Bearbeiten im Auftrag, V. 1.12/August 2022, https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf (Abruf 16. Mai 2023), Ziff. 2.1.

von Daten mittels Apps, die auf einem Cloudserver betrieben werden (SaaS(online)), und zweitens die Speicherung von Daten auf einem Cloudserver (IaaS).

Aus datenschutzrechtlicher Sicht stellt die Nutzung von Cloud-Diensten eine Bearbeitung im Auftrag i.S.v. § 6 IDG ZH i.V.m. § 25 IDV oder auch eine «Auslagerung» oder ein «Outsourcing» von Datenbearbeitungen dar.[108] Kennzeichnend für die Auslagerung ist, dass Daten durch Dritte bearbeitet werden, die nicht derselben Verwaltungsabteilung angehören bzw. unterstellt sind,[109] und dass die Auftragnehmerin diese Daten nicht zur Erfüllung einer ihr übertragenen gesetzlichen Aufgabe benötigt, d.h. keine Datenbekanntgabe i.S.v. § 16 u. 17 IDG vorliegt.[110] Von Bedeutung ist die Abgrenzung deshalb, weil ein bekanntgebendes öffentliches Organ Datenherrschaft überträgt und nicht mehr für die nunmehr durch die Empfängerin bearbeiteten Daten verantwortlich ist, während es bei einer Auslagerung als Datenherrin verantwortlich bleibt.[111]

Das Modell des Cloud-Computing geht über die klassische Auslagerung von Datenbearbeitungen hinaus, indem es die Nutzung einer geteilten ITC-Infrastruktur mitumfasst, die nach den Bedürfnissen der Nutzerinnen und Nutzer skaliert werden kann. Zu beachten ist, dass Nutzer einer Cloud keinen physischen Zugriff auf die Hardware haben, auf welcher die Clouddienste betrieben werden.[112] Ebenso wenig haben sie einen Einfluss auf die softwareseitige Absicherung der Bearbeitungsumgebung.

---

[108] DSB Kanton Zürich, Merkblatt Cloud Computing, V. 1.6/Juli 2022, https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf (Abruf 16. Mai 2023), Ziff. 1.

[109] PraKomm IDG ZH-BLATTMANN, § 6 N 6; DSB Kanton Zürich, Leitfaden Bearbeiten im Auftrag, V. 1.12/August 2022, https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf (Abruf 16. Mai 2023), Ziff. 3.2.

[110] PraKomm IDG ZH-BLATTMANN, § 6 N 5; DSB Kanton Zürich, Leitfaden Bearbeiten im Auftrag, V. 1.12/August 2022, https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf (Abruf 16. Mai 2023), Ziff. 3.1 *e contrario*; bezüglich Bundesrecht a.M. ASTRID EPINEY/TOBIAS FASNACHT, in: Belser/Epiney/Waldmann, Datenschutzrecht, Bern 2011, § 10 N 8, die für das Vorliegen einer Bekanntgabe ins Ausland darauf abstellen, ob die Daten dem territorialen Anwendungsbereich des DSG entzogen werden; ebenso JOEL DRITTENBASS, Regulierung von autonomen Robotern - Angewendet auf den Einsatz von autonomen Medizinrobotern: Eine datenschutzrechtliche und medizinprodukterechtliche Untersuchung, Zürich/Baden-Baden 2021, N 227; EDÖB, Stellungnahme zur Datenschutz Risikobeurteilung der Suva zum Projekt Digital Workplace «M365» unter besonderer Berücksichtigung des von der Suva thematisierten Zugriffs von US-amerikanischen Behörden auf Personendaten, die das Unternehmen in eine von der Firma Microsoft betriebene Cloud auslagert, 10. Mai 2023, N 14, wonach bereits die Auslagerung der Daten in die MS-Cloud eine Bekanntgabe darstellt; diese Auffassung wird indes nicht weiter begründet.

[111] PraKomm IDG BS-RUDIN, § 7 N 17; SHK DSG-BAERISWYL, Art. 9 N 10 ff.; ausdrücklich in § 1 Abs. 3 des Gesetzes über die Auslagerung von Informatikdienstleistungen des Kantons Zürich vom 23. August 1999 (ON 172.71; zit. AuIG).

[112] AXEL FREIHERR VON DEM BUSSCHE, Branchenübergreifende Sonderkonstellationen im IT-Sicherheitsrecht – I. Cloud Computing, in: Dennis-Kenji Kipker (Hrsg.), Cybersecurity – Rechtshandbuch, 1. Auflage, München 2020, Kapitel 4 N 76.

### 6.3.2 Übertragung von Datenherrschaft als spezifische Eingriffskategorie

Im Rahmen der Nutzung eines Clouddienstes i.S. von SaaS(online) und IaaS überträgt die Datenherrin die Datenherrschaft über die Cloud-Daten, da diese notwendigerweise der Auftragsnehmerin zugänglich gemacht werden müssen, um auf ihren Systemen bearbeitet werden zu können. In welchem Umfang die Datenherrschaft auf den Dritten übergeht, hängt zunächst von der gewählten Cloud-Dienstleistung sowie vom Umfang der Nutzung dieser Dienste ab. Für SaaS(online) betrifft dies sämtliche Daten, die bei der Nutzung der betreffenden Software auf den Servern der Anbieterin zur Erledigung der gesetzlichen Aufgaben bearbeitet werden. Soweit Infrastruktur als Dienstleistung (IaaS) genutzt wird, beispielsweise in der Form eines Onlinespeichers, betrifft dies sämtliche Daten, die dort gespeichert werden.

Im Umfang der Übertragung von Datenherrschaft begründen Cloud-Dienste spezifische Risiken, typischerweise durch Verlust der faktischen und rechtlichen Kontrolle über die Bearbeitung, erschwerte Rechtsdurchsetzung oder Auslagerung der Bearbeitung in den Geltungsbereich von ausländischem Recht. Überdies beeinflussen die Umstände der ausgelagerten Datenbearbeitung die Risikoprofile für die Durchsetzung von Löschungs- und Berichtigungsansprüchen der Betroffenen, die Nachvollziehbarkeit der Datenbearbeitung und die Umsetzung von IT-Sicherheitsmassnahmen. Zudem begründen sie ein eigenes Risiko des Datenmissbrauchs durch Hilfspersonen der Auftragnehmerin.[113]

Im Ergebnis verliert das zuständige öffentliche Organ durch die Auslagerung in einem gewissen Umfang die zur Wahrnehmung der bei ihm verbleibenden Verantwortlichkeit i.S.v. § 6 Abs. 2 IDG notwendige rechtliche und tatsächliche Kontrolle über gewisse Aspekte der Datenbearbeitung.[114] Kontrollverluste dieser Art schlagen auf die Betroffenen der Bearbeitung von Personendaten durch und können bei genügender Persönlichkeitsnähe der Datenbearbeitung entsprechende Eingriffe in die informationelle Selbstbestimmung begründen.[115]

### 6.3.3 Kontrollverluste im Geltungsbereich von CLOUD Act/SCA

Die im Rahmen dieses Gutachtens diskutierte Kategorie von Cloud-Diensten, d.h. M365 und ähnliche Produkte, zeichnen sich dadurch aus, dass die zugrundeliegende Infrastruktur global aufgebaut ist. Es handelt sich hierbei um Angebote weltweit tätiger Konzerne, deren Daten in vielfacher Hinsicht auch ausländischem Recht und damit der Möglichkeit eines *lawful access* durch ausländische Behörden unterstehen.[116] Mit der Nutzung eines U.S.-Clouddienstes tritt

[113] Vgl. zum Ganzen die Liste der spezifischen Risiken in DSB Kanton Zürich, Merkblatt Cloud Computing, V. 1.6/Juli 2022, https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf (Abruf 16. Mai 2023), Ziff. 3.
[114] So auch RRB Nr. 542/2022, Ziff. 7.
[115] Zur Begründung von Eingriffen durch Datenbearbeitung siehe 5.3.
[116] RRB Nr. 542/2022, Ziff. 3.

deshalb zu der bereits besprochenen Einschränkung der Herrschaft über die Daten ein zusätzlicher Kontrollverlust – und damit ein zusätzliches Eingriffsmoment – durch die Anwendbarkeit von U.S.-amerikanischem Recht hinzu.

Im Falle von Microsoft und insbesondere in Zusammenhang mit M365 wird in diesem Zusammenhang über die globale Anwendbarkeit von US-Amerikanische Recht durch den *Clarifying Lawful Overseas Use of Data (CLOUD) Act*[117] von 2018 diskutiert.[118] Wie der Titel bereits andeutet, stellt der Erlass eine Präzisierung bisherigen Rechts dar, genauer die ausdrückliche extraterritoriale Erweiterung der Pflichten aus dem *Stored Communications Act (SCA)*[119] auf gewisse Daten, die auf Servern ausserhalb der Vereinigten Staaten gespeichert sind. Es handelt sich mithin um einen Erlass mit Rechtswirkung auf Unternehmen mit Sitz in der Schweiz, die einen rechtlichen Mindestbezug zu den Vereinigten Staaten aufweisen.

Im Geltungsbereich von CLOUD Act/SCA stehen den betroffenen U.S.-Anbietern gewisse Rechtsmittel zur Verfügung, um eine Herausgabeanordnung gegebenenfalls anzufechten, nicht aber ihren Kunden (z.B. staatliche Organe, die M365 nutzen); dies aber nur dann, wenn ein zusätzliches *executive agreement* CH-USA dies ermöglicht.[120] Es findet mithin eine unfreiwillig vollständige Übertragung der faktischen und rechtlichen Kontrolle an den Clouddienstleister statt, die zu einem entsprechend umfassenden Kontrollverlust seitens des öffentlichen Organs führt, der entsprechend auch auf die Betroffenen durschlägt.

Darüber hinaus stehen Bestimmungen des Cloud-Acts verschiedentlich im Widerspruch zu Bearbeitungsgrundsätzen des schweizerischen Datenschutzrechts bzw. sind mit diesem «nur schwer vereinbar».[121] So etwa im Hinblick auf den Grundsatz der transparenten Datenbearbeitung, indem eine Bekanntgabe den Betroffenen aufgrund der Bestimmungen des Cloud-Acts nicht mitgeteilt werden darf sowie gegen die Zweckbindung, da Daten von U.S.-Behörden im Rahmen eines (durch schweizerisches Recht nicht vorgesehenen) Zwecks bearbeitet werden können.

Im Ergebnis können dadurch die vom Bundesgericht konkretisierten Anforderungen zur Durchsetzung der informationellen Selbstbestimmung verletzt werden, indem den Betroffenen weder eine rechtmässige Bearbeitung, noch Kenntnis unrechtmässiger Bearbeitung, noch eine wirksame Rechtsdurchsetzung garantiert werden kann. Ist für Personendaten, welche

[117] Pub. L. No. 115-141, 132 Stat. 348 (2018).
[118] Siehe sowie die Zusammenfassung der strafrechtlichen Lehre bei DAVID ROSENTHAL, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, Jusletter 10. August2020, N. 15 ff., fokussiert auf die Frage der Hilfsperson;
[119] 18 U.S.C. §§ 2701 et seq.
[120] Bundesamt für Justiz BJ, Bericht zum US CLOUD Act vom 17. September 2021, S. 7; überdies könnten aufgrund eines solchen Abkommens Schweizer Behörden bei Behörden in den USA Daten beschaffen, die über den CLOUD Act von Firmen in der Schweiz herausverlangt wurden.
[121] SHK DSG-BAERISWYL, Art. 9 N 70.

dem Cloud Act unterstehen, das Kriterium der genügenden Persönlichkeitsnähe erfüllt, liegt somit ein Grundrechtseingriff vor, der nach Art. 36 zu rechtfertigen ist.

### 6.3.4 Insbesondere: Speicherung und Zugriff als diskrete Eingriffsmomente

#### *6.3.4.1 Allgemeines*

Die Intensität des Eingriffs durch *lawful access* bezüglich Daten in einer U.S.-Cloud ist gemäss einiger in jüngerer Zeit veröffentlichter Gutachten nach der Wahrscheinlichkeit eines Zugangs zu Daten durch U.S.-Behörden zu bestimmen.[122] Dies ist grundsätzlich richtig, betrifft indes die Intensität des durch das Risiko des Zugangs (=access) bewirkten Eingriffs und nicht das Problem der Speicherung an sich, die als eigenständige Form der Bearbeitung i.S. der Entbündelung der Eingriffsmomente separat zu beurteilen ist.[123]

Eine derartige doppelte Analyse des Eingriffs entspricht der Rechtsprechung des Bundesgerichts, das in Anlehnung an die Rechtsprechung des EGMR für die Speicherung von Daten im Hinblick auf eine mögliche spätere Bekanntgabe an öffentliche Organe zwischen der Speicherung und der späteren Übermittlung von Daten unterscheidet, und diese je als separate Eingriffe behandelt.[124]

#### *6.3.4.2 Eingriff durch Schaffung eines Risikos der Bekanntgabe an US-Behörden*

##### 6.3.4.2.1 Verletzung von innerstaatlichem und internationalem Recht

Ausschlaggebend für die Beurteilung des ersten Elements – jenem des Eingriffs durch Bekanntgabe an U.S.-Behörden durch den Clouddienst – ist, dass die Frage der Zulässigkeit eines Zugriffs auf Clouddaten in diesen Fällen nicht durch das schweizerische, sondern durch das U.S.-amerikanische Recht beantwortet wird.[125] Dies bedeutet erstens, dass der Eingriff, den ein solcher Datenzugriff durch US-Behörden im Einzelfall begründet, nicht auf seine Verfassungsmässigkeit i.S.v. Art. 36 BV geprüft werden kann. Mit anderen Worten erfolgt die Speicherung der Daten nicht im Hinblick auf einen rechtlich vorgesehenen Zugriff auf diese Daten durch inländische Behörden, sondern mit dem Risiko einer möglichen, aber nach schweizerischem Recht nicht vorgesehenen Bearbeitung dieser Daten durch einen anderen Staat.

Zweitens wird durch eine Beschaffung der Daten durch U.S.-Behörden gestützt auf CLOUD Act/SCA der übliche völkerrechtliche Rechtsweg der Rechtshilfe umgangen, und dies ohne Zustimmung und möglicherweise auch ohne Kenntnis des bearbeitenden Organs. Dies steht in

---

[122] Apodiktisch CHRISTIAN LAUX/ALEXANDER HOFFMANN, Rechtsgutachten betreffend Rechtsmässigkeit von Public Cloud Services «Cloud Gutachten» (unter Berücksichtigung des CLOUD Act) vom 16. September 2021 zuhanden Organisation und Informatik der Stadt Zürich, N 142; DAVID ROSENTHAL, Leitfaden zur Einführung von Cloud-Services in öffentlichen Organen und Schweizer Spitälern vom 22. November 2022, S. 3; vgl. auch die Prüfung im Hinblick auf M365 in RRB Nr. 542/2022, Ziff. 4.

[123] Siehe sogleich 6.3.4.3.

[124] BGer Urteil 1C_598/2016 vom 2. März 2018, E.5.4.

[125] Bundeskanzlei, Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung Bericht in Umsetzung vom Meilenstein 5 der Cloud-Strategie des Bundesrates, Bern 2021, S. 21.

Widerspruch zu Art. 32 der des Übereinkommens über die Cyberkriminalität[126]. Gemäss Marginalie regelt diese Bestimmung den grenzüberschreitenden Zugriff auf gespeicherte Computerdaten zwischen Vertragspartnern. Diese sind nur mit Genehmigung des Vertragspartners zulässig, es sei denn, es handle sich um öffentlich zugängliche Daten (Art. 32 Bst. a CCC). Eine weitere Ausnahme besteht dann, wenn die Daten in einem Drittstaat gespeichert sind und die zuständige Behörde dieses Staates eine Freigabezustimmung abgibt (Art. 32 Bst. b CCC). Sowohl die Schweiz als auch die USA sind Signatarstaaten der Konvention; Vorbehalte gegen die Bestimmungen in Art. 32 CCC sind gemäss Art. 42 CCC nicht zulässig.

Im Ergebnis bedroht der mögliche Zugriff auf Clouddaten von öffentlichen Organen in der Schweiz durch U.S.-Behörden grundsätzlich die Grundrechte der Betroffenen und ermöglicht zudem eine Verletzung der aus der Cyberkonvention fliessenden vertraglichen Rechte der Schweiz.[127] Insgesamt begründet dies eine Verletzung von grundrechtlichen Schutzpflichten,[128] d.h. einen Gefährdungseingriff, der gemäss Art. 36 BV zu rechtfertigen ist.

#### 6.3.4.2.2 Intensität des hierdurch bewirkten Grundrechtseingriffs

Für die Beurteilung der Intensität des Gefährdungseingriffs ist nun, im Einklang mit den erwähnten Gutachten, auf die Schwere der drohenden individuellen Verletzung sowie die Wahrscheinlichkeit einer Verletzung abzustellen. Die beiden Aspekte sollen es ermöglichen, die Qualität der grundrechtlichen Bedrohung zu bestimmen.[129] Dabei ist von Bedeutung, das zwischen beiden Kriterien eine Wechselwirkung besteht. Einerseits steigt die Intensität des Eingriffs, je wahrscheinlicher eine künftige Verletzung anzunehmen ist. Umgekehrt ist andererseits bei geringer Eintrittswahrscheinlichkeit eine relevante Grundrechtsgefährdung nur anzunehmen, wenn die Schwere der möglichen Verletzung und der Kreis der Betroffenen gross sind.[130] Im Hinblick darauf, dass die Datenbearbeitung durch öffentliche Organe im Kanton Zürich mittels M365 im Rahmen der IKT-Grundversorgung grundsätzlich flächendeckend eingeführt werden soll,[131] ist letzteres Kriterium (grosser Kreis der Betroffenen) erfüllt.[132] Die

[126] Übereinkommen über die Cyberkriminalität (CCC; SR. 0.311.43), abgeschlossen in Budapest am 23. November 2001, von der Bundesversammlung genehmigt am 18. März 20112, Schweizerische Ratifikationsurkunde hinterlegt am 21. September 2011, in Kraft getreten für die Schweiz am 1. Januar 2012.
[127] Theoretisch denkbar wäre immerhin, eine vertragliche Regelung zu vereinbaren, über die eine Genehmigung gemäss Art. 32 CCC erwirkt werden könnte.
[128] Zum Begriff siehe MARKUS SCHEFER, Gefährdung von Grundrechten: eine grundrechtsdogmatische Skizze, in: Thomas Sutter-Somm/Felix Hafner/Gerhard Schmid/Kurt Seelmann (Hrsg.), Risiko und Recht – Festgabe zum schweizerischen Juristentag 2004, Basel 2004, S. 445 f.
[129] GLASS (Fn. 20), S. 138 f.
[130] SCHEFER (Fn. 128), S. 477.
[131] RRB Nr. 542/2022, Ziff. 2.;
[132] Nicht vom Geltungsbereich des RRB Nr. 542/2022 erfasst sind die Gemeinden, für welche die Überlegungen analog gelten.

Schwere der möglichen Verletzung bestimmt sich demgegenüber nach den bereits besprochenen Kriterien zur Bestimmung der Schwelle zum schweren Eingriff durch Datenbearbeitung.[133]

Zur Bestimmung der Wahrscheinlichkeit der möglichen Verletzung müssen notwendigerweise Methoden der Risikoanalyse eigesetzt, d.h. auf Elemente des Risikomanagements zurückgegriffen werden.[134] Als herausfordernd erweist sich in diesem Zusammenhang die zunehmende Komplexität der rechtlichen, technischen und politischen Umstände der Datenbearbeitung, die in ihrem Zusammenspiel darauf hinauslaufen, dass die Ermittlung einer Wahrscheinlichkeit der Verwirklichung eines Risikos regelmässig von erheblicher Ungewissheit geprägt ist.[135] Um diesem Problem zu begegnen, stützt sich der Regierungsrat des Kantons Zürich auf die von ROSENTHAL entwickelte Methode zur Berechnung von Risiken in Zusammenhang mit *lawful access* zu Clouddaten und legt diese als Standard für den Kanton fest.[136]

Die Berechnung gründet auf fünf Schritten:

- Erstens wird festgelegt, welche Daten für welche Zeitdauer analysiert werden;
- Zweitens wird geschätzt, wie oft eine Anfrage durch US-Behörden zu erwarten ist;
- Drittens wird abgeschätzt, ob die Voraussetzungen für ein *lawful access* in den zu erwartenden Einzelfällen erfüllt sein werden;
- Viertens wird geschätzt, mit welcher Wahrscheinlichkeit der Anbieter von einer Massenüberwachung betroffen sein wird («Schrems II»);
- Fünftens werden die ermittelten Wahrscheinlichkeiten zusammengerechnet.[137]

Eine umfassende Analyse dieser Methode kann an dieser Stelle nicht geleistet werden. Dennoch erscheinen einige Hinweise angebracht. Zunächst ist festzustellen, dass bisher neben der «Methode Rosenthal» keine alternative Methode entwickelt wurde, die eine vergleichbar strukturierte Argumentation in Bezug auf das Risiko eines *lawful access* im Rahmen von CLOUD Act/SCA ermöglicht. Die von den Datenschutzbehörden veröffentlichten Leitfäden und Merkblätter benennen typischerweise die mit der Cloudnutzung verbundenen Risiken, geben aber wenig Anleitung, wie diese rechtsgenüglich beurteilt werden könnten.[138] Zugleich zeigt die Methode aber auch, wo die Probleme einer solchen Risikoermittlung liegen.

---

[133] Siehe 5.4.
[134] GLASS (Fn. 20), S. 139.
[135] GLASS (FN. 20), S. 147 ff.
[136] RRB Nr. 542/2022, Ziff. 5.
[137] DAVID ROSENTHAL, Memorandum Berechnung des ausländischen Lawful Access / US CLOUD Act vom 24. März 2022 zuhanden Amt für Informatik Zürich, N 25.
[138] Vgl. beispielsweise DSB Kanton Zürich, Merkblatt Cloud Computing, V. 1.6/Juli 2022, https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf (Abruf 16. Mai 2023), Ziff. 3.; Konferenz der schweizerischen Datenschutzbeauftragten (privatim), Merkblatt Cloud-spezifische Risiken und Massnahmen, V3.0 / 03.02.2022, https://www.privatim.ch/wp-content/uploads/2022/02/privatim_Cloud-Merkblatt_v3_0_20220203_def._DE-1.pdf (Abruf 30.05.2023), S. 3 f.

Die eigentliche Berechnung findet auf einem Excel-Sheet statt, das einen Fragenkatalog bezüglich der Wahrscheinlichkeit verschiedener Aspekte eines möglichen *lawful access* enthält.[139] Jeder dieser Fragen wird ein Prozentwert zugewiesen, der jeweils von einer schriftlichen Erläuterung begleitet wird. Die Festlegung der Prozentwerte wird schriftlich begründet, doch ist nicht immer ersichtlich, inwiefern der Wert aus der Begründung folgt. Indes reicht es aus verfassungsrechtlicher Sicht aus, wenn die Methode schlussendlich eine plausible Begründung für die angenommene Wahrscheinlichkeit einer Verwirklichung der grundrechtlichen Gefahr erlaubt. Dies erscheint unter dem Vorbehalt möglich, dass mehr Gewicht auf die Frage der Qualität der Erfahrungsdaten gelegt wird. Anzumerken ist, dass der Erfahrungswert den *status quo* abbildet, der sich gerade dadurch auszeichnet, dass öffentliche Organe in der Schweiz mangels Rechtsicherheit in der Regel keine Personendaten in Clouds von U.S.-Anbietern bearbeiten. Sollte sich dies ändern, ist auch eine Änderung im Anfragevolumen seitens U.S.-Behörden kein abwegiger Gedanke.

Zweitens fehlen verbindliche Kriterien für die Vornahme einer Neubeurteilung. Zu denken ist hier etwa an die tatsächliche Beschaffung von Clouddaten des Kantons Zürich durch U.S.-Behörden gestützt auf Cloud Act/SCA. Eine solche wird im Memorandum Rosenthal als sehr unwahrscheinlich eingestuft und müsste folglich, falls sie trotzdem eintreten sollte, eine grundsätzliche Neubeurteilung der Wahrscheinlichkeit auslösen.

Im Ergebnis legt die Quantifizierung durch geschätzte prozentuale Wahrscheinlichkeiten für eine Prognose zur Festlegung der Intensität eines Gefährdungseingriffs eine Präzision nahe, die tatsächlich kaum je bestehen dürfte. Das Gutachten ist sich dieser Problematik durchaus bewusst und relativiert die Aussagekraft der in Prozenten angegebenen Wahrscheinlichkeit. Insgesamt geht es aber davon aus, dass dennoch eine belastbare Aussage bezüglich der Grössenordnung der mit einer Cloudnutzung verbundenen Risiken möglich sei.[140]

In diesem Zusammenhang ist schliesslich darauf hinzuweisen, dass die genannte Methode ursprünglich entwickelt wurde, um die Wahrnehmung der Sorgfaltspflichten zur Vermeidung von Strafbarkeit von Privatpersonen in Zusammenhang mit dem Berufsgeheimnis argumentativ zu strukturieren.[141] Der Massstab der Datenbearbeitung durch öffentliche Organe ist indes nicht primär die Vermeidung von Strafbarkeit, sondern die rechtmässige Erfüllung der jeweiligen Aufgabe sowie die Beförderung der hiermit verbundenen öffentlichen Interessen. Wie

[139] DAVID ROSENTHAL, Memorandum Berechnung des ausländischen Lawful Access / US CLOUD Act vom 24. März 2022 zuhanden Amt für Informatik Zürich, Anhang: Cloud-Computing: Risikobeurteilung eines Lawful Access durch ausländische Behörden, Template: Version 5.04 (1. September 2021).
[140] DAVID ROSENTHAL, Memorandum Berechnung des ausländischen Lawful Access / US CLOUD Act vom 24. März 2022 zuhanden Amt für Informatik Zürich, N 23.
[141] Vgl. dazu DAVID ROSENTHAL, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, Jusletter vom 10. August 2020.

bereits gezeigt wurde, ergibt sich die Intensität der Grundrechtsgefährdung aus der Wahrscheinlichkeit des Eintritts und der Schwere der zu erwartenden Verletzung, wobei mit der Schwere der Verletzung die Höhe der zulässigen Wahrscheinlichkeit sinkt.[142] Dies bedeutet, dass die spezifischen Risiken mit Bezug auf grundrechtlich geschützte Datenbearbeitungen, mögen die Eintrittswahrscheinlichkeit auch noch so gering sein, grundsätzlich gemäss Art. 36 BV zu rechtfertigen sind. Es bedeutet insbesondere aber auch, dass solche Risiken, sofern sie den Kerngehalt von Grundrechten tangieren, gemäss Art. 36 Abs. 4 BV nicht eingegangen werden dürfen.

#### *6.3.4.3 Eingriff durch Speicherung*

Im Hinblick auf das zweite Element, die Speicherung der Daten in der Cloud, weisen die aus Sicht des innerstaatlichen Rechts grundsätzlich unbeschränkten Möglichkeiten des Zugriffs und der Zweckänderung von Clouddaten durch U.S.-Behörden im Rahmen von Cloud Act und SCA[143] eine dem Datenzugriff vorgelagerte Eingriffswirkung auf. Da das verantwortliche öffentliche Organ mit der Nutzung des Dienstes die Kontrolle über die bearbeiteten Daten faktisch und rechtlich (insb. mangels Beschwerdelegitimation im Rahmen von CLOUD Act/SCA) an den U.S.-Clouddienst abtritt, besteht parallel zur ordentlichen Bearbeitung durch dieses Organ ein zusätzlicher Zweck der Speicherung, der durch ausländisches Recht definiert wird und in der Bekanntgabe der Daten durch den Dienstanbieter an ausländische Behörden besteht. Mithin läuft dies auf die Speicherung von Daten auf Vorrat zuhanden ausländischer Behörden hinaus.

Die Speicherung von Personendaten «auf Vorrat» stellt gemäss Rechtsprechung des Bundesgerichts unabhängig von einer späteren Verwendung einen selbständigen Eingriff in das Recht auf informationelle Selbstbestimmung dar.[144] Hierbei kann die Eingriffsintensität variieren. Als Kriterien für deren Beurteilung nennt das Gericht neben der «Masse der erfassten Daten» sowie Anzahl der betroffenen Personen[145] zusätzlich die Art und Sensibilität der Daten,[146] die Aussagekraft der Daten bezüglich einer möglichen Profilbildung,[147] sowie implizit auch die Dauer der anlasslosen Speicherung.[148] Vorliegend stellt insbesondere die Dauer einen schweren Eingriff dar, da die Bearbeitung in zeitlicher Hinsicht lediglich durch das Gesetzmässigkeitsgebot (§ 8 IDG ZH), den Grundsatz der Zweckbindung (§ 9 IDG ZH) i.V.m. der Löschpflicht (Art.

[142] Siehe 6.3.3.2.2.
[143] D.h. Umfang und Voraussetzungen sind durch das US-amerikanische Recht definiert und können sich jederzeit ändern.
[144] BGE 144 I 126, E. 4.2
[145] BGE 144 I 126, E.5.4.
[146] BGE 144 I 126, E.5.3.
[147] BGE 144 I 126, E.5.4.
[148] BGE 144 I 126, E.8.3.9. im Rahmen der Verhältnismässigkeitsprüfung.

11 Abs. 2 IDG ZH) begrenzt wird. Entsprechend werden Personendaten regelmässig über Jahre bzw. Jahrzehnte gespeichert.[149]

Zusätzlich zur Intensität gemäss den bundesgerichtlichen Kriterien ist zu beachten, dass die Speicherung indirekt eine (latente) Bekanntgabe an U.S.-Behörden darstellt, welche die Voraussetzungen der Cyberkonvention nicht erfüllt. Insbesondere darf die Speicherung von Daten in der Cloud eines U.S.-Anbieters nicht als Genehmigung zur Bekanntgabe i.S.v. Art. 32 CCC ausgelegt werden. Mit der möglichen Umgehung der durch die Konvention vorgeschriebenen sichernden Massnahmen (Notwendigkeit einer Genehmigung), geht ein weiterer, erschwerender rechtlicher Kontrollverlust einher.

Insgesamt betrachtet, stellt die Bearbeitung bzw. Speicherung von besonderen Personendaten in der Cloud eines U.S.-Anbieters wie Microsoft unabhängig von dem mit einem möglichen Zugriff auf solche Daten verbundenen Gefährdungseingriff für sich bereits einen schweren Grundrechtseingriff dar, der nach Art. 36 BV entsprechend zu rechtfertigen ist.

### 6.3.5 Insbesondere: Lieferantenabhängigkeit des öffentlichen Organs

Mit Bezug auf die Nutzung von Microsoft Office bzw. M365 sind öffentliche Verwaltungen in der Schweiz faktisch abhängig von der Firma Microsoft. Für den Kanton Zürich hat der Regierungsrat festgestellt, dass sich die öffentlichen Organe durch die Wahl von M365 «grundsätzlich in eine Lieferantenabhängigkeit» gegenüber Microsoft begeben.[150] Auf Bundesebene bestätigte der Bundesrat eine Abhängigkeit im Hinblick auf die Evaluation von MS 365 für die Bundesverwaltung. Gemäss DSB Kanton Basel-Stadt dürfte die Beurteilung für die Kantone ähnlich ausfallen.[151] Bereits verfügbar ist eine entsprechende Einschätzung des DSB Kanton Bern[152] sowie des Amtes für Informatik und Organisation des Kantons Bern.[153]

Der hierdurch begründete tatsächliche Kontrollverlust wirkt sich negativ auf die auftragsrechtlichen Sorgfaltspflichten des öffentlichen Organs aus, indem sie eine sorgfältige Auswahl des Anbieters,[154] zumindest mit Bezug auf das Grundprodukt M365, verunmöglicht.

Des weiteren wird dadurch die datenschutzrechtliche Ausgestaltung der betreffenden Produkte grundsätzlich der Anbieterin überlassen,[155] die sich als globale U.S.-Dienstleisterin nicht

[149] Beispielsweise werden Personendaten bei der Einwohnerkontrolle für die Dauer des Wohnsitzes gespeichert.
[150] Siehe auch den Hinweis in RRB Nr. 542/2022, Ziff. 7.
[151] DSB Kanton Basel-Stadt, Tätigkeitsbericht 2022, https://www.dsb.bs.ch/dam/jcr:50c7b260-131e-4c30-9e84-37fc52aa9c8e/TB_DSB2022-20230428.pdf) (Abruf 22. Mai 2023), S.25;
[152] DSB Kanton Bern, Tätigkeitsbericht 2022, https://www.dsa.be.ch/content/dam/dsa/dokumente/de/jahresberichte/KKB_DSA_Jahresbericht2022_DE_RZ2.pdf (Abruf 22. Mai 2023), S. 15 f.
[153] Amt für Informatik und Organisation Kanton Bern, Restrisiken beim Einsatz von M365 - Bericht an den Regierungsrat vom 7. Juni 2023, Ziff. 3.8.
[154] DSB Kanton Zürich, Leitfaden Bearbeiten im Auftrag, V. 1.12/August 2022, https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf (Abruf 16. Mai 2023), Ziff. 4.4.
[155] Ausführlich Amt für Informatik und Organisation Kanton Bern, Restrisiken beim Einsatz von M365 - Bericht an den Regierungsrat vom 7. Juni 2023, Ziff. 3.5.

notwendigerweise am schweizerischen Datenschutzrecht orientiert. Der hieraus resultierende rechtliche Kontrollverlust könnte in gewissen Konstellationen zu schweren Gefährdungseingriffen in das Recht auf informationelle Selbstbestimmung führen. Dies wäre beispielsweise der Fall, wenn M365 Apps nur noch online genutzt, d.h. Datenbearbeitungen nur mittels einer Onlineversion der Apps durchgeführt werden könnten (SaaS(Online)/IaaS). Dies ist offenbar in absehbarer Zeit (noch) nicht der Fall, bleibt aber von der weiteren Entwicklung der Produkte durch Microsoft abhängig.

### 6.3.6 Zusammenfassend zu den spezifischen Eingriffsmomenten von M365

Die Untersuchung zur Wirkung der Datenbearbeitung mittels M365 hat gezeigt, dass diese in mehrfacher Hinsicht einen Eingriff in die informationelle Selbstbestimmung bewirken kann. Sie bezieht sich auf die Nutzung von M365 in der Cloud, d.h. auf die Bearbeitung mittels online Apps und Speicherung auf den Servern von Microsoft mittels OneDrive. Über die üblichen Risiken der Bearbeitung im Auftrag hinaus wurden die folgenden spezifischen Eingriffe herausgearbeitet:

- Übertragung der faktischen und rechtlichen Kontrolle über diese Daten an Microsoft;
- Gefährdungseingriff durch Schaffung des Risikos eines möglichen Zugriffs auf Daten durch US-Behörden im Rahmen von CLOUD Act/SCA;
- Eingriff durch Speicherung der Daten im Hinblick auf eine Bekanntgabe durch Microsoft an US-Behörden im Rahmen von CLOUD Act/SCA;
- Gefährdungseingriff durch Schaffung der Gefahr einer Umgehung von sichernden rechtlichen Bestimmungen wie etwa die Voraussetzungen der zwischenstaatlichen Datenbekanntgabe in Art. 32 CCC.
- Gefährdungseingriff durch Schaffung einer Lieferantenabhängigkeit, die in einer unfreiwilligen Migration in die Cloud eines US-Anbieters (Microsoft) münden könnte.

## 6.4 Erfordernis der genügenden gesetzlichen Grundlage

### 6.4.1 Allgemeines zur gesetzlichen Grundlage für Eingriffe durch Datenbearbeitung

Grundrechtseingriffe müssen sich nach Art. 36 Abs. 1 BV auf eine genügende gesetzliche Grundlage stützen lassen. Als genügend gilt eine ausreichend bestimmte, rechtsatzförmige Grundlage in einem der Schwere des Eingriffs entsprechend demokratisch legitimierten Erlass.[156]

[156] Zum Ganzen RENÉ RHINOW/MARKUS SCHEFER/PETER ÜBERSAX, Schweizerisches Verfassungsrecht, 3. e.u.a. Auflage, Basel 2016, N 1198 ff.; REGINA KIENER, Grundrechtsschranken, in: Oliver Diggelmann/Maya Hertig Randall/Benjamin Schindler (Hrsg.), Verfassungsrecht der Schweiz - Droit constitutionel suisse, Band II: Rechtsstaatlichkeit, Gund- und Menschenrechte, Zürich Basel Genf 2020, S. 1309 ff.; GIORGIO MALINVERNI/MICHEL HOTTELIER/MAYA HERTIG RANDALL/ALEXANDRE FLÜCKIGER, Droit constitutionel suisse - Volume II: Les droits fondamentaux, 4. A. Bern 2021, N 194 ff.;ebenfalls REGINA KIENER, Allgemeine Grundrechtslehren, in: Giovanni Biaggini/Thomas Gächter/Regina Kiener (Hrsg.), Staatsrecht, 3.A. Zürich/St. Gallen 2021, S. 488.

Ein öffentliches Organ des Kantons Zürich oder einer seiner Gemeinden darf gemäss § 8 Abs. 1 IDG ZH Personendaten bearbeiten, «soweit dies zur Erfüllung seiner gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist». Dagegen erfordert die Bearbeitung von besonderen Personendaten gemäss § 8 Abs. 2 IDG ZH eine hinreichend bestimmte Regelung in einem formellen Gesetz». Unterhalb der Schwelle des schweren Grundrechtseingriffs macht das Gesetz keine weiteren Vorgaben bezüglich Normstufe und –dichte. Für Datenbearbeitungen, die einen leichten Eingriff in die Grundrechte begründen und jene, die den Schutzbereich der Grundrechte mangels Eingriffsqualität nicht berühren, gelten damit grundsätzlich dieselben Voraussetzungen, namentlich zumindest das Erfordernis einer impliziten, durch die gesetzliche Aufgabe notwendigerweise begründete Ermächtigung zur personenbezogenen Datenbearbeitung.[157]

Im Ergebnis bedeutet dies, dass die Ermächtigung zur Bearbeitung von gewöhnlichen Personendaten implizit und akzessorisch mit der jeweiligen gesetzlichen Aufgabe einhergeht. Somit genügt in diesen Fällen eine sog. mittelbare gesetzliche Grundlage zur Bearbeitung von Personendaten.[158] Geht mit der Bearbeitung eine besondere Gefahr einer Persönlichkeitsverletzung i.S.v. § 3 Abs. 4 Bst. a IDG einher, begründet die Datenbearbeitung mit anderen Worten einen Grundrechtseingriff i.S.v. Art. 36 BV, so reicht in der Regel eine implizite gesetzliche Bearbeitungsermächtigung nicht aus.[159] Vielmehr muss die Datenbearbeitung unabhängig von der mit ihr verknüpften Aufgabe hinreichend bestimmt i.S.v. § 8 Abs. 2 IDG gesetzlich geregelt sein.

### 6.4.2 Hinreichende Normdichte

Das IDG äussert sich nicht zur Frage, welche Kriterien die Normdichte einer ausdrücklichen Bearbeitungsermächtigung in einem Gesetz erfüllen muss. In der Praxis sind indes gewisse Aspekte der Datenbearbeitung anerkannt, die für Bearbeitungen von besondere Personendaten in den Grundzügen zwingend formell-gesetzlich zu regeln sind, namentlich das verantwortliche Organ, Ziel und Zweck der Datenbearbeitung, die Kategorien der bearbeiteten Daten sowie die Art und Weise der Datenbearbeitung.[160] Weiterführende, auf diesen Grundzügen aufbauende Regelungen können an den Verordnungsgeber delegiert werden, sofern die entsprechenden Bedingungen erfüllt sind.[161]

---

[157] GLASS (Fn. 20), S. 193 f. m.w.H.

[158] Zum Begriff siehe PraKomm IDG BS-RUDIN, Art. 9 N 17; die Anforderungen an die Normdichte richten sich dann an die Umschreibung der gesetzlichen Aufgabe.

[159] Zu den Ausnahmen im Bundesrecht siehe die Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941, 7081.

[160] Dazu im Einzelnen PraKomm IDG ZH-BAERISWYL, § 8 N 14 ff.; ähnlich PraKomm IDG BS-RUDIN § 9 N 33 ff.; EVA MARIA BELSER, in: Belser/Epiney/Waldmann, Datenschutzrecht, Bern 2011, § 12 N 45.

[161] PraKomm IDG ZH-BAERISWYL, § 8 N 23 f.; EVA MARIA BELSER, in: Belser/Epiney/Waldmann, Datenschutzrecht, Bern 2011, § 12 N 46.

Wie bereits dargelegt wurde, kann sich die Qualifikation einer Datenbearbeitung als Bearbeitung von besonderen Personendaten aus einem oder mehreren Eingriffsmomenten oder gar erst aus dem Zusammenspiel aller Eingriffsmomente einer Bearbeitung ergeben.[162] Damit die gesetzliche Grundlage die mit einer Datenbearbeitung einhergehenden Eingriffe in die Persönlichkeit der Betroffenen legitimatorisch einfangen kann, muss sie das Erfordernis von Art. 36 Abs. 1 BV für jedes Eingriffsmoment, dass die in § 3 Abs. 4 Bst. a IDG verankerte Schwelle zu einem eigenständigen schweren Grundrechtseingriff überschreitet, je separat erfüllen. Ergänzend zu den genannten Grundzügen müssen daher jene Eingriffsmomente gesetzlich geregelt sein, die einen schweren Eingriff in die informationelle Selbstbestimmung begründen. Zudem muss die rechtliche Grundlage erkennen lassen, welches verbleibende Risiko der Gesetzgeber als vertretbar erachtet und welches öffentliche Interesse dieses Risiko rechtfertigt.

### 6.4.3 Gesetzliche Grundlage im AuIG[163]

Ergänzend zum IDG regelt § 3 AuIG gewisse datenschutzrechtliche Aspekte der Auslagerung. Demnach dürfen öffentliche Organe grundsätzlich sowohl gewöhnliche als auch besondere Personendaten auslagern. Privatrechtlichen Anbietern dürfen sie diese Daten indes nur dann zur Bearbeitung zugänglich machen, «wenn sie durch organisatorische und technische Massnahmen vor unbefugter Einsichtnahme geschützt sind». Überdies müssen Mitarbeitende der Anbieterin, die besondere Personendaten bearbeiten, denselben Amts-, Berufs- und Spezialgeheimnissen unterstellt sein, wie die auslagernde Behörde.

Die Bestimmung zeichnet sich dadurch aus, dass die die Voraussetzungen für die Qualifikation einer Datenbearbeitung als Bearbeitung von besonderen Personendaten undifferenziert behandelt und nicht als Bündel von verschiedenen Eingriffen von variabler Intensität begreift. Wie aber gezeigt wurde, muss eine hinreichende gesetzliche Grundlage genügend Normdichte aufweisen, um sämtliche mit einer Datenbearbeitung zusammenhängenden schweren Eingriffsmomente i.S.v. Art. 36 zu rechtfertigen. Vorliegend wird übersehen, dass die Eingriffsqualität oftmals durch spezifische Eingriffsmomente der Art und Weise oder der Umstände der Bearbeitung begründet wird, die in § 3 IDG nur stichwortartig erwähnt werden.[164]

Im Ergebnis ändert sich durch die Bestimmungen in § 3 AuIG die Rechtslage im Hinblick auf die Auslagerung von besonderen Personendaten im Vergleich zu den allgemeinen Bestimmungen im IDG ZH nur unwesentlich. Für Daten, die allein aufgrund der Zugehörigkeit zu einer gesetzlichen Schutzkategorie als besondere Personendaten behandelt werden, sowie andere Eingriffe, die aufgrund von sichernden Massnahmen als gewöhnliche Eingriffe zu bewerten sind, ist § 3 AuIG ausreichend. Ebenso ist der Begriff der Auslagerung genügend klar, um die

[162] Siehe 5.3.
[163] Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1999 (AuIG; ON 172.71); gilt gemäss § 1 AuIG nicht für Gemeinden; hier wären eigene Rechtsgrundlagen zu schaffen.
[164] Vgl. 5.4.2.3 (Art und Umfang der Bearbeitung) bzw. 5.4.2.4 (Umstände der Bearbeitung).

mit der klassischen Auslagerung von Datenbearbeitungen verbundenen Eingriffe zu erfassen. Die im Rahmen dieses Gutachtens identifizierten zusätzlichen Eingriffsmomente können aber nicht legitimiert werden. Im Hinblick auf die identifizierten spezifischen Eingriffsmomente der Nutzung von M365 bedarf die Nutzung der Cloudversionen der Apps einer hinreichenden formell-gesetzlichen Grundlage i.S.v. § 8 Abs. 2 IDG.[165]

## 6.5 Öffentliches Interesse

Bei der Frage nach dem rechtfertigenden öffentlichen Interesse i.S.v. Art. 36 Abs. 2 BV ist – analog zur Frage der genügenden gesetzlichen Grundlage – jedes identifizierte Eingriffsmoment einzeln daraufhin zu prüfen, welche öffentlichen Interessen es zu befördern bezweckt. Letztere ergeben sich einerseits aus dem Bearbeitungszweck, d.h. aus der öffentlichen Aufgabe, zu deren Erfüllung die Daten bearbeitet werden, andererseits aus den Begründungen für die übrigen Aspekte der Bearbeitung, etwa deren Art oder spezifischen Begleitumstände.

Gemäss den Ausführungen des Regierungsrats soll mit der Einführung von MS 365 für die kantonale Verwaltung ein weiterer Schritt der Standardisierung in der IKT-Grundversorgung gemacht, aber auch eine «flexible, skalierbare, performante und sicherere Infrastruktur» ermöglicht werden, «die den Kanton Zürich in die Lage versetzt, zeitnah (sic) auf sich ändernde Geschäftsanforderungen zu reagieren».[166] Insbesondere durch die Standardisierung im Rahmen der IKT-Strategie wird insgesamt, in Verbindung mit weiteren Faktoren, namentlich dem «technologischen Fortschritt  sowie von der zentralen Beschaffung der IKT-Grundversorgung», eine Steigerung der Kosteneffizienz erwartet.[167] Damit soll sichergestellt werden, dass die Verwaltung ihre Ressourcen sinnvoll einsetzt und ihre Aufgaben kosteneffizient erfüllt, die mit anderen Worten ihre Aufgaben wirtschaftlich erfüllt, wie dies von Art. 85 KV ZH vorgeschrieben wird.[168]

Als weiteres öffentliches Interesse wird die Erhöhung der Datensicherheit genannt. Der Gedanke dahinter geht davon aus, dass Daten auf den Servern eines globalen Hyperscalers grundsätzlich sicherer sind vor unbefugten Bearbeitungen durch Dritte, als dies in lokalen Rechenzentren von Bund, Kantonen und Gemeinden der Fall sei.[169] Der Regierungsrat des Kantons Zürich geht davon aus, dass mit Cloud-Lösungen «Schutzziele wie Verfügbarkeit in der Cloud grundsätzlich besser erreicht werden können».[170] Überdies hätte ein Verzicht negative

[165] Dies gilt nicht für Apps, die wie bisher *on premise* betrieben und lediglich über die Cloud aktualisiert werden.
[166] RRB Nr. 542/2022, Ziff. 2.
[167] Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich Sitzung vom 26. Juni 2019, 625. Projekte im Programm zur Umsetzung der kantonalen IKT-Strategie (Freigabe, zusätzliche Ausgabe, Stellenplan), RRB Nr. 0625/2019, Ziff. 8.
[168] Verfassung des Kantons Zürich vom 27. Februar 2005 (ON 101).
[169] RRB Nr. 542/2022, Ziff. 7.
[170] RRB Nr. 542/2022, Ziff. 2.

Auswirkungen, namentlich eingeschränkte Kollaboration (übergreifende Arbeit in Teams) und etwa Wegfall von Optionen zur Prozessoptimierung.[171]

Mit Hinweis auf einen Bericht der Firma Gartner wird insgesamt davon ausgegangen, dass die Einführung von Cloud Computing zu bedeutenden Fortschritten in den Bereichen IT-Modernisierung, Effizienz, Sicherheit und Produktivität führe.[172] Insgesamt erscheinen die Zugewinne in der Beförderung der genannten öffentlichen Interessen als signifikant.

## 6.6 Einzelne Aspekte der Verhältnismässigkeit

### 6.6.1 Erforderlichkeit: Die Ermittlung des mildesten Eingriffsmittels

#### *6.6.1.1 Steuerung der Eingriffsintensität durch selektive Datenbearbeitung in der Cloud*

Mit dem Kriterium der Erforderlichkeit soll ein angemessenes Verhältnis zwischen Eingriffsmittel und Eingriffswirkung, d.h. eine vernünftige Zweck-Mittel-Relation, sichergestellt werden.[173] Für Datenbearbeitungen im Schutzbereich der informationellen Selbstbestimmung bedeutet dies eine Balance zwischen Kontrollverlust bzw. Missbrauchsrisiko, den sichernden Datenschutzrechten sowie der Persönlichkeitsnähe der Bearbeitung auf der einen sowie den verfolgten öffentlichen Interessen auf der anderen Seite. Ob eine Datenbearbeitung das mildeste Mittel zur Erfüllung des Bearbeitungszwecks darstellt, bestimmt sich nach «Eingriffspräzision»[174] oder auch Umfang der Bearbeitung, d.h. der Frage, ob nicht mehr Daten als notwendig bearbeitet werden sowie der Eingriffsintensität,[175] also die Frage ob nur gewöhnliche oder auch besondere Personendaten bearbeitet werden.

Sinnvollerweise ist zudem stets zu prüfen, ob der Zweck der Bearbeitung mit anonymisierten Daten erreicht werden kann.[176] Durch die Anonymisierung wird die Persönlichkeitsnähe – und damit die Eingriffsqualität der Bearbeitung – aufgehoben. In ähnlicher Weise können durch sichernde Massnahmen der Kontrollverlust und damit einhergehend die Eingriffsintensität einer Bearbeitung reduziert werden.[177]

### 6.6.2 Lokale Applikationen

Grundsätzlich ist festzuhalten, dass der Verzicht auf eine Bearbeitung, insbesondere aber Speicherung von Personendaten in der Cloud von Microsoft das mildere Mittel mit Bezug auf die grundrechtliche Problematik durch unbefugten Zugriff darstellt. Nach Darstellung der Bundesbehörden ist es nach wie vor möglich, die Apps der Office-Suite als lokale Applikationen bzw.

---

[171] RRB Nr. 542/2022, Ziff. 7.
[172] RRB Nr. 542/2022, Ziff. 1.
[173] OFK BV-Biaggini, Art. 36 N 23.
[174] Markus Schefer, Die Beeinträchtigung von Grundrechten: zur Dogmatik von Art. 36 BV, Bern 2006, S. 83 f.
[175] Eva Maria Belser, in: Belser/Epiney/Waldmann, Datenschutzrecht, Bern 2011, § 12 N 60; zur Eingriffsintensität siehe Ziff. 5.4.
[176] Eva Maria Belser, in: Belser/Epiney/Waldmann, Datenschutzrecht, Bern 2011, § 12 N 60; vgl. auch den Hinweis bei PraKomm IDG ZH-Baeriswyl, § 8 N 11.
[177] Vgl. zu Ganzen 6.6.3.ff.

im Rahmen eines klassischen Outsourcings zu nutzen.[178] Inwiefern eine solche Nutzung das öffentliche Interesse an der Datensicherheit in vergleichbarer Weise zu verwirklichen mag, kann nicht abstrakt, sondern nur im Einzelfall geprüft werden.

### 6.6.3 Insbesondere: Sichernde Massnahmen

Wie dargelegt wurde, begründen die für die Nutzung der Cloudversionen von M365 identifizierten Eingriffsmomente[179] einen tatsächlichen und/oder rechtlichen Kontrollverlust des bearbeitenden Organs, der auf die Betroffenen durchschlägt und bei genügender Persönlichkeitsnähe der jeweiligen Datenbearbeitung einen schweren Eingriff in Art. 13 Abs. 2 BV begründet. Mithin stellt die Nutzung der Cloudversionen von M365 einen Umstand der Bearbeitung dar, der bearbeitete Personendaten aufgrund der Art der Bearbeitung i.S.v. § 3 Abs. 4 Bst. a IDG als besondere Personendaten qualifiziert. Soweit diese Eingriffsmomente durch sichernde Massnahmen entschärft werden können, fällt auch das qualifizierende Moment weg, weshalb gewöhnliche Personendaten auch im Rahmen einer Bearbeitung mittels M365 gewöhnliche Personendaten bleiben würden.

Das Gesetz konkretisiert die Erforderlichkeit an verschiedenen Stellen, indem es die öffentlichen Organe anweist, erkannte Datenschutzrisiken durch sichernde Massnahmen zu reduzieren oder gewisse sichernde Massnahmen direkt vorschreibt, beispielsweise in der Form von Informationspflichten,[180] Mindeststandards für eine sichere Datenbearbeitung[181] oder Vorschriften zur Vermeidung des Personenbezugs[182] von Datenbearbeitungen.

Im Hinblick auf die Nutzung von Clouddiensten enthalten verschiedene Merkblätter und Leitfäden jeweils ähnlich lautende Ansätze für eine *best practice* zur Verminderung der damit verbundenen spezifischen Risiken.[183] Im Vordergrund stehen Massnahmen zur Kompensation des durch die Auslagerung bewirkten rechtlichen und faktischen Kontrollverlusts.

#### *6.6.3.1 Kompensation des rechtlichen Kontrollverlusts*

Als sichernde Massnahmen mit Bezug auf den rechtlichen Kontrollverlust gelten insbesondere die Vereinbarung der Anwendung von schweizerischem Recht und die Festlegung eines schweizerischen Gerichtsstands. Weiter ist die Anbieterin zu einem transparenten Umgang mit den betroffenen Daten zu verpflichten, insbesondere im Hinblick auf Unterauftragsverhältnisse sowie den geographischen Ort der Datenbearbeitung. Weiter wird auf die Bestimmungen über die Voraussetzungen der Bekanntgabe ins Ausland in § 19 IDG verwiesen und

[178] Medienmitteilung des Bundes vom 15. Februar 2023, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-93076.html (Abruf 19. Mai 2023).
[179] Siehe 6.3.5.
[180] Vgl. § 12 IDG ZH (Information über die Beschaffung).
[181] Vgl. § 7 IDG ZH (Informationssicherheit).
[182] Vgl. § 11 IDG ZH (Vermeidung des Personenbezugs)
[183] Siehe unter https://www.datenschutz.ch/datenschutz-in-oeffentlichen-organen/auslagerung.

betont, dass eine Auslagerung der Bearbeitung ins Ausland nur rechtmässig ist, wenn der betreffende Standort über ein gleichwertiges Datenschutzniveau verfügt oder durch weitere Sicherheitsmassnahmen ein analoges Niveau für die betreffende Dienstleistung garantiert werden kann.[184]

Für Datenbearbeitungen, die in der Cloud eines U.S.-Anbieters erfolgen, ist die letzte Voraussetzung regelmässig nicht erfüllt. Zum einen sind die Vereinigten Staaten nicht in der Liste der Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organen mit einem angemessenen Datenschutz im Anhang 1 der Datenschutzverordnung des Bundes aufgeführt.[185] Zum anderen stellt der Cloud Act keine Rechtsmittel für die Kunden von Cloud-Anbietern oder für die Betroffenen einer darauf basierenden Datenbekanntgabe zur Verfügung.[186]

Im Ergebnis könnte die Bekanntgabe durch Microsoft von Personendaten an U.S.-Behörden auf der Grundlage des Cloud Acts eine Verletzung schweizerischen Rechts darstellen. Als sichernde Massnahme wird beispielsweise empfohlen, das «Risiko einer solchen Rechtsverletzung [in] der Analyse zu berücksichtigen und durch vertragliche Massnahmen so weit als möglich zu reduzieren».[187] Indes sind den Massnahmen gegen antizipierte Rechtsverletzung enge Grenzen gesetzt, auch wenn das Risiko einer tatsächlichen Bekanntgabe als gering eingeschätzt wird.[188]

#### *6.6.3.2 Kompensation des faktischen Kontrollverlusts*

Für die Kompensation des Verlustes der faktischen Kontrolle sollen sich die öffentlichen Organe vertragliche Kontrollrechte zusichern lassen, welche jenen der verwaltungsrechtlichen Weisungs- und Aufsichtsrechte zumindest funktional ähnlich sind. Empfohlen wird insbesondere auch die vertragliche Verpflichtung des Anbieters, regelmässige Audits nach internationalen Standards durchführen zu lassen.[189] Mit Bezug auf einen erfolgten Zugriff auf Daten durch U.S.-Behörden erscheint dies indes nicht möglich.

---

[184] Siehe zum Ganzen DSB Kanton Zürich, Merkblatt Cloud Computing, V. 1.6/Juli 2022, https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf (Abruf 16. Mai 2023), S. 2 ff.

[185] Verordnung über den Datenschutz vom 31. August 2022 (Datenschutzverordnung, DSV; SR 235.11); vgl. auch DSB Kanton Zürich, Tätigkeitsbericht 2021, S. 21.

[186] Sieh Fn. 119.

[187] Konferenz der schweizerischen Datenschutzbeauftragten (privatim), Merkblatt Cloud-spezifische Risiken und Massnahmen, V3.0 / 03.02.2022, https://www.privatim.ch/wp-content/uploads/2022/02/privatim_Cloud-Merkblatt_v3_0_20220203_def._DE-1.pdf (Abruf 30.05.2023), S. 4.

[188] SHK DSG-Baeriswyl, § 9 N 73.

[189] DSB Kanton Zürich, Merkblatt Cloud Computing, V. 1.6/Juli 2022, https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf (Abruf 16. Mai 2023), Ziff. 4.1.

Als weitere sichernde Massnahmen gelten die Sorgfaltspflichten des Auftraggebers, wobei Art. 55 OR in gewisser Hinsicht allenfalls als Analogiebasis dienen könnte.[190] Durch faktische Abhängigkeiten der Verwaltungen in der Schweiz sind diese allerdings insofern nur beschränkt umsetzbar, als eine Sorgfältige Auswahl des Anbieters, zumindest in Bezug auf das Grundprodukt MS Office 365, nicht möglich ist. Hingegen kommen sie für die konkrete Nutzung von Clouddiensten zur Geltung, insbesondere bei der Auswahl der Verschlüsselungslösung.

#### *6.6.3.3 Insbesondere: Verschlüsselung*

Ein bedeutender Aspekt der Wahl des mildesten Mittels für Eingriffe durch Datenbearbeitung ist der Datenbearbeitung vorgelagert und ergibt sich aus der normativen Folgewirkung von Technologie. Es handelt sich um das Konzept der datenschutzgerechten Ausgestaltung von Informationssystemen durch Technologiedesign. Die hier im Vordergrund stehenden Konzepte, die in der schweizerischen wie in der internationalen Literatur unter den Stichworten *privacy by design* und *privacy by default* diskutiert werden, sind mittlerweile als «Datenschutz durch Technik» und «datenschutzfreundliche Voreinstellungen» in Art. 7 nDSG ausdrücklich im Bundesrecht verankert.[191]

Für die Bearbeitung von Daten in der Cloud wird als wirksame technologische Einschränkung der Datenbearbeitung durch Dritte die Verschlüsselung der ausgelagerten Daten empfohlen.[192] Dadurch kann die Bearbeitung der Daten durch unbefugte Dritte entscheidend erschwert oder gar verhindert werden. Überdies ist es in Bezug auf CLOUD Act/SCA offenbar so, dass U.S.-Behörden nur berechtigt sind, von den Clouddienstleistern Daten ihrer Kunden in Klartext zu beschaffen.[193] Zudem bietet der CLOUD-Act keine Rechtsgrundlage dafür, den Anbieter zur Entschlüsselung von Daten zu zwingen.[194] Im Hinblick auf die aktuelle Rechtslage kann daher davon ausgegangen werden, dass eine Verschlüsslung von Personendaten unter Wahrung der Schlüsselkontrolle durch das öffentlichen Organ einen verfassungskonformen

---

[190] Vgl. DSB Kanton Zürich, Leitfaden Bearbeiten im Auftrag, V 1.3./Mai 2023, Leitfaden_Bearbeiten_im_A https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf uftrag (datenschutz.ch), (Abruf 1. Juni 2023), Ziff. 6.3.

[191] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941, 7028 ff., hier noch in Art. 6 E-DSG.

[192] Siehe im Einzelnen DSB Kanton Zürich, Merkblatt Cloud Computing, V. 1.6/Juli 2022, https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf (Abruf 16. Mai 2023), Ziff. 4.7; DSB Kanton Zürich, Verschlüsselung der Daten im Rahmen der Auslagerung - unter Inanspruchnahme von Informatikleistungen und unter Berücksichtigung der Geheimnispflichten, V 2.3 Juli 2022, https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/verschluesselung_der_datenablage_im_rahmen_der_auslagerung.pdf (Abruf 31. Mai 2023; Konferenz der schweizerischen Datenschutzbeauftragten (privatim), Merkblatt Cloud-spezifische Risiken und Massnahmen, V3.0/03.02.2022, https://www.privatim.ch/wp-content/uploads/2022/02/privatim_Cloud-Merkblatt_v3_0_20220203_def._DE-1.pdf (Abruf 30.05.2023), S. 4 f.

[193] DAVID ROSENTHAL, Memorandum Berechnung des ausländischen Lawful Access / US CLOUD Act vom 24. März 2022 zuhanden Amt für Informatik Zürich, N 30.

[194] U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, https://www.justice.gov/opa/press-release/file/1153446/download (Abruf 10. Juni 2023), White Paper April 2019, S. 18.

Betrieb von M365 ermöglichen kann.[195] Dies in dem Umfang, in dem die Verschlüsselung den festgestellten mehrfachen Kontrollverlust über die jeweils in der Cloud bearbeiteten Daten kompensiert.

### 6.6.4 Zumutbarkeit des kumulativen Restrisikos

Im Gegensatz zu den übrigen Prüfpunkten der Rechtfertigung, d.h. gesetzliche Grundlage, öffentliches Interesse und Erforderlichkeit, muss die Zumutbarkeit des Restrisikos gesamthaft, d.h. über den gesamten Bearbeitungsprozess hinweg, geprüft werden. Dies bedeutet, dass das kumulative Restrisiko sämtlicher bisher geprüften Teilrisiken der grundrechtlichen Belastung der Betroffenen gegenüberzustellen ist.

Die hier besprochenen öffentlichen Interessen erscheinen sehr abstrakt und können kaum in allgemeiner Weise bewertet werden. Insofern werden öffentliche Organe diese im Einzelfall selbst vornehmen müssen. Wenn sie auch in grundsätzlicher Weise als wichtig genug erscheinen, um gegebenenfalls Eingriffe in die durch Art. 13 Abs. 2 BV garantierten Grundrechte zu rechtfertigen, wird von entscheidender Bedeutung sein, wie die Prognose für den jeweiligen Zugewinn an Effizienz, Sicherheit und Produktivität ausfällt.

Mit Bezug auf die Nutzung von Clouddienstleistungen kann insgesamt im Sinne einer Zusammenfassung resümiert werden, dass nicht alle damit zusammenhängenden spezifischen Grundrechtseingriffe durch sichernde Massnahmen auf ein grundrechtlich vertretbares Mass reduziert werden können. Als grösste Herausforderung eines verfassungskonformen Einsatzes von Clouddiensten wie M365 erscheint die Tatsache, dass mit der Bearbeitung von Personendaten im Rahmen von Clouddiensten von U.S.-Anbietern diese Daten in den Geltungsbereich des CLOUD Act gelangen und dadurch neben ihrem eigentlichen Bearbeitungszweck unfreiwillig zuhanden von U.S.-Behörden gespeichert werden und im Rahmen eines *lawful access* zugänglich gemacht werden könnten.

Die Nutzung von MS Office durch Verwaltungen in der ganzen Schweiz hat gemäss Feststellung des Bundes zu einer Abhängigkeit geführt,[196] die sich nun darin äussert, dass die Umstellung auf Versionen der Applikationen mit Cloud-Anbindung in den nächsten Jahren nachvollzogen werden muss, um diese weiterhin nutzen zu können. Dies bedeutet aber (noch) nicht, dass sämtliche mit diesen Apps vorgenommenen Datenbearbeitungen in der Cloud vorgenommen werden müssen. Gemäss Darstellung der Bundesbehörden ist es nach wie vor möglich, Apps und Speicher *on-premises* in Rechenzentren des Bundes zu halten. Entsprechend kann vorerst noch darüber bestimmt werden, ob und in welchem Umfang Daten in der Cloud von Microsoft online bearbeitet und gespeichert werden.

[195] So auch DSB Kanton Zürich, Tätigkeitsbericht 2022, https://www.datenschutz.ch/tb/2022 (online only).
[196] Siehe 6.3.5.

Dennoch hält dies die Bundesverwaltung M356 offenbar nicht für eine nachhaltige Lösung. Insbesondere seien die Cloudversionen der Apps nicht für die Bearbeitung von besonderen Personendaten geeignet, d.h. der Eingriff durch die Bearbeitung dieser Daten in der Cloud für diese Daten wird als zu schwer erachtet, als dass er durch die mit der Nutzung des Clouddienstes von Microsoft verbundenen Vorteile gerechtfertigt werden könnte.

# 7 Zusammenfassung

## 7.1 Befunde

1. Die Garantien von Art. 13 Bas. 2 BV umfassen zwei Aspekte des Schutzes vor Missbrauch persönlicher Daten. Der erste Aspekt ist der Schutz vor Missbrauch im Sinne einer minimalen Garantie der rechtmässigen Datenbearbeitung. Sie vermittelt ein rechtlich geschütztes Interesse der Betroffenen an einer rechtsstaatlich korrekten Bearbeitung ihrer Daten i.S.v. Art. 5 BV sowie Schutz vor willkürlicher und treuwidriger Bearbeitung. Der zweite Aspekt umfasst den Schutz der informationellen Selbstbestimmung, deren Schutzbereich sich am Schutzobjekt der Persönlichkeit orientiert und die Ausübung der Grundrechte sichert.
2. Eingriffe in die informationelle Selbstbestimmung durch Datenbearbeitung bestehen typischerweise aus mehreren Eingriffsmomenten, die dasselbe Schutzobjekt, namentlich die Persönlichkeit derselben Person beeinträchtigen. Soweit solche Eingriffsmomente je eine Bearbeitung von besonderen Personendaten darstellen und damit einen schweren Eingriff begründen, müssen sie je einzeln nach Art. 36 BV gerechtfertigt werden. Schliesslich müssen die durch eine Datenbearbeitung begründeten Eingriffsmomente gesamthaft betrachtet als Eingriff in die informationelle Selbstbestimmung für die Betroffenen zumutbar sein.
3. Beeinträchtigt wird die informationelle Selbstbestimmung insbesondere dann, wenn die Bearbeitung von Personendaten zu einer Selbstbeschränkung in der Ausübung der Grundrechte durch die Betroffenen führen kann (Abschreckungswirkung). Das Bundesgericht legt hier einen auf die betroffenen Einzelnen gerichteten Massstab an. Die Voraussetzung ist erfüllt, wenn ein Aspekt der Bearbeitung aufgrund eines Kontrollverlustes der Betroffenen plausibel als geeignet erscheint, letztere von der Ausübung ihrer Grundrechte abzuhalten. Dieser Kontrollverlust bildet das erste Element des Eingriffs durch Datenbearbeitung. Das zweite Element betrifft die Datenschutzrechte, die das Bundesgericht entwickelt hat, um einem Kontrollverlust vorzubeugen bzw. ihn gegebenenfalls abzumildern. Es wird durch das Fehlen von wirksamen Rechten der Betroffenen zur Überprüfung der Datenbearbeitung begründet.
4. Die Intensität eines Eingriffsmoments ergibt sich zum einen aus dem Zusammenspiel von Kontrollverlust sowie der Wirksamkeit von Rechtsbehelfen dagegen, zum anderen

aus der Persönlichkeitsnähe der Datenbearbeitung. Letztere ist wiederum von den Lebensbereichen abhängig, aus welchen eine Datenbearbeitung Informationen abbildet und nutzbar macht. Absolut geschützt ist das *forum internum* als Kerngehalt der Persönlichen Freiheit. Ein Kontrollverlust lässt sich gegebenenfalls durch sichernde Massnahmen kompensieren, während die Persönlichkeitsnähe durch Anonymisierung aufgehoben oder gemildert werden kann. Diese Möglichkeiten sind jeweils im Einzelfall zu prüfen.

5. Für die identifizierten Eingriffe in das Grundrecht der informationellen Selbstbestimmung in Zusammenhang mit der Nutzung von M365 in der Cloud besteht teilweise die Möglichkeit, deren Intensität durch sichernde Massnahmen zu vermindern. Im Rahmen der innerstaatlichen Rechtsbeziehung zwischen öffentlichem Organ und Cloudanbieterin können die Eingriffsmomente der Übertragung der faktischen und rechtlichen Datenherrschaft durch die in den verschiedenen Merkblättern und Leitbildern ausgeführten vertraglichen und technischen Massnahmen gemildert und entsprechend grundrechtsverträglicher ausgestaltet werden.
6. Als sichernde Massnahmen stehen die in der Praxis gängigen Massnahmen der Datensicherheit sowie einer vertraglichen Überbindung der Pflichten aus dem IDG auf die Anbieterin zur Verfügung. In Bezug auf die Aufhebung oder Verminderung der Persönlichkeitsnähe kann auf die Verschlüsselung von sensiblen Daten verwiesen werden, wobei deren Wirksamkeit gegenüber der Anbieterin sicherzustellen ist.
7. Die Speicherung von Personendaten in der Cloud, und damit unfreiwillig «auf Vorrat» zuhanden von U.S.-Behörden, welche diese mittels CLOUD Act/SCA u.U. beschaffen könnten, stellt ein spezifisches Eingriffsmoment dar, das gemäss Art. 36 BV zu rechtfertigen ist. Aufgrund der Anzahl der Betroffenen (sämtliche Personen im Zuständigkeitsbereich des Organs) und des faktischen und rechtlichen Kontrollverlusts des öffentlichen Organs ist grundsätzlich von einem schwerwiegenden Eingriff in Art. 13 Abs. 2 BV im Sinne von Art. 36 Abs. 1 Satz 2 BV auszugehen.
8. In Anlehnung an die bundesgerichtliche Rechtsprechung stellt die Grundrechtsgefährdung durch eine mögliche Bekanntgabe von Clouddaten an U.S.-Behörden durch die Anbieterin einen von der Speicherung zu unterscheidenden Gefährdungseingriff in Art. 13 Abs. 2 BV dar. Aufgrund des rechtlichen Kontrollverlusts des öffentlichen Organs sowie der antizipierten Verletzung von Art. 32 CCC und der Schwächung des rechtsstaatlichen Schutzes, den diese Bestimmung vermitteln soll, ist grundsätzlich von einem schweren Gefährdungseingriff auszugehen. Ob dem im konkreten Fall so ist, muss durch Risikoanalyse im Einzelfall ermittelt werden. Auch wenn die durch den Regierungsrat des Kantons Zürich verwendete «Methode Rosenthal» für die Verwendung im öffentlich-rechtlichen Bereich als noch nicht genügend ausgereift erscheint, vermag

sie doch gewisse Aussagen über die Grössenordnung der Wahrscheinlichkeit einer Verletzung zu liefern. Das Ergebnis, wonach ein geringes Risiko eines Zugriffs besteht, erscheint unter den gegebenen Umständen als plausibel, kann sich aber insbesondere mit der zunehmenden Verwendung von M365 durch Behörden in der Schweiz (und weltweit) ändern.

9. Die identifizierten Eingriffe gewinnen zusätzlich an Intensität, wenn sie im Hinblick auf die Abhängigkeit der schweizerischen Behörden von den Office-Produkten der Firma Microsoft beurteilt werden. Insbesondere gilt es zu beachten, dass die weitere Entwicklung dieser Produkte im privatautonomen Belieben der Anbieterin steht und aktuell für den Fall einer im Lichte der informationellen Selbstbestimmung negativen Veränderung der Lage für die öffentliche Verwaltung keine Alternativen zur Verfügung stehen. Dies bedeutet einen weiteren tatsächlichen Kontrollverlust der öffentlichen Organe, welche diese Produkte einsetzen.
10. Seitens des Regierungsrates des Kantons Zürich werden signifikante Zugewinne in der Beförderung von öffentlichen Interessen geltend gemacht. Durch den Wechsel auf M365 könne die IKT-Infrastruktur des Kantons Zürich sicherer, effizienter und kollaborativer (Stichwort Teams) werden. Dies sei insbesondere auch in der internationalen Zusammenarbeit wichtig.
11. Die Rechtsgrundlagen in IDG und § 3 AuIG ermöglichen eine Bearbeitung von besonderen Personendaten im Rahmen der klassischen Auslagerung von Datenbearbeitungen durch öffentliche Organe. Für die spezifischen Eingriffsmomente der Auslagerung in die Cloud eines US-Unternehmens reichen sie indes nicht aus.

Im Hinblick auf die dargelegten Eingriffe und deren Intensität sowie der ungenügenden rechtlichen Grundlage für die Übernahme der korrespondierenden Risiken durch öffentliche Organe im Kanton Zürich muss zum aktuellen Zeitpunkt ein Verzicht auf gewisse Formen der Bearbeitung von besonderen Personendaten (= schwere Eingriffe in die informationelle Selbstbestimmung)[197] mittels M365 empfohlen werden. Dies betrifft sämtliche Formen der Bearbeitung, die eine Speicherung von Daten in der Cloud von Microsoft umfassen. Hier sei als milderes Mittel auf absehbare Zeit auf die Möglichkeit verwiesen, solche Applikationen auf eigenen Rechenzentren betreiben zu lassen und lediglich die Aktualisierungen über den Clouddienst vorzunehmen. Alternativ kann eine klassische Auslagerung in Rechenzentren eines Dritten, der nicht dem U.S.-amerikanischen Recht untersteht, ins Auge gefasst werden. Diese Einschätzung bleibt im Lichte der künftigen rechtlichen und technischen Entwicklung stetig zu überprüfen.

[197] Siehe 5.3.1.

Die vorliegende Beurteilung entspricht im Ergebnis in weiten Teilen der allgemeinen Nutzungsrichtlinie M365 der Finanzdirektion des Kantons Zürich vom 27. Januar 2023, die von den Gemeinden analog angewendet werden können.[198] Diese sieht für die Bearbeitung von gewöhnlichen Personendaten eine uneingeschränkte Nutzung von M365 Clouddiensten vor. Im Hinblick auf die Bearbeitung von besonderen Personendaten sollen dagegen lokale Apps genutzt werden. Ebenso ist es nicht gestattet, besondere Personendaten mit den online-Funktionen von Teams oder über SharePoint zu bearbeitet bzw. auf OneDrive zu speichern. Diese Einschränkungen betreffen sämtliche Datenbearbeitungen, die aufgrund eines Aspekts der Bearbeitung als Bearbeitung von besonderen Personendaten zu qualifizieren sind, d.h. aufgrund der Zugehörigkeit zu einer gesetzlichen Kategorie sowie aufgrund der Art und Weise, des Zwecks oder der Umstände der Bearbeitung.[199] Anzumerken ist, dass die Persönlichkeitsnähe, und damit die Eingriffsqualität einer Datenbearbeitung, durch Verschlüsselung aufgehoben oder vermindert werden kann, soweit diese eine gegenüber dem Anbieter wirksame Anonymisierung bewirkt.

In Ergänzung zu diesen Vorgaben wird empfohlen, die gesetzlichen Grundlagen im Hinblick auf die mit der Nutzung von M365 verbundenen grundrechtlichen Eingriffsmomente sowie auf die entsprechenden rechtfertigenden öffentlichen Interessen zu ergänzen.

Schliesslich ist sicherzustellen, dass in Clouds von U.S.-Anbietern keine Datenbearbeitungen vorgenommen werden, die eine unkontrollierte Preisgabe von Informationen aus einem grundrechtlich geschützten Kerngehaltsbereich ermöglichen.

## 7.2 Evaluierung von Alternativen

Das Problem der faktischen Abhängigkeit der Behörden in der Schweiz von den Office-Produkten der Firma Microsoft wurde bereits im Zusammenhang mit der Diskussion der Eingriffe erörtert.[200] Im Hinblick auf diese Entwicklung haben die Bundesbehörden beschlossen, im Rahmen einer «Exitstrategie» die Entwicklung von Ersatzprodukten voranzutreiben, die keine proprietäre Software enthalten; es wird angeregt, im Hinblick auf eine mögliche vollständige Verlagerung von MS Office in die Cloud, mittelfristig alternative Applikationen zu entwickeln, die auf Open-Source-Standards basieren.[201] Aus dieser Sicht könnte es sich für die Gemeinden des Kantons Zürich als nützlich erweisen, die entsprechenden Bemühungen der Bundesbehörden im Auge zu behalten.

[198] Siehe Fn. 101.
[199] Siehe zum Ganzen 5.4.2. ff.
[200] Siehe 6.3.5.
[201] So die Medienmitteilung des Bundes vom 15. Februar 2023, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-93076.html (Abruf 19. Mai 2023).

Basel, 6. Juli 2023

Prof. Dr. Markus Schefer

Dr. Philip Glass