VISCHER

ANMERKUNGEN ZUM GUTACHTEN SCHEFER/GLASS ZU "M365"

David Rosenthal,[i] *10. November 2023*

A. Ausgangslage

1 Am 6. Juli 2023 erstatteten Prof. Dr. Markus Schefer und Dr. Philip Glass der Universität Basel zuhanden von egovpartner in Zürich ein Gutachten zum "grundrechtskonformen Einsatz von M365 durch die Gemeinden im Kanton Zürich" (das **Gutachten**).

2 Es kommt im Wesentlichen zum Schluss, dass die Nutzung von M365[1] durch Zürcher Gemeinden eine unfreiwillige Speicherung von Personendaten "auf Vorrat" zu Handen von U.S. Behörden sei, weil diese die Daten via U.S. CLOUD Act bzw. SCA[2] beschaffen könnten. Das führe zu einem faktischen und rechtlichen Kontrollverlust über die Daten. Ein Zugriff durch die U.S. Behörden würde zudem gegen Art. 32 CCC[3] verletzen. Weil eine hohe Anzahl von Personen potenziell betroffen sei, sei dies ein grundsätzlich schwerer Eingriff in die informationelle Selbstbestimmung. Trotz der im Zürcher Datenschutzrecht[4] bestehenden Rechtsgrundlage für Auslagerungen betr. besonders schützenswerte Personendaten[5], sei dieser somit hinreichend zu rechtfertigen oder verhindern. Die Verhinderung des Eingriffs sei durch eine Verschlüsselung in einer Art und Weise zu bewerkstelligen, dass Microsoft keinen Zugang zum Schlüssel habe. Das Gutachten befasst sich ferner mit der "Methode Rosenthal" zur Analyse der Wahrscheinlichkeit eines U.S. Behördenzugriffs und hält das vom Kanton Zürich damit erzielte Ergebnis für plausibel, weist aber darauf hin, dass sich die Situation mit der zunehmenden Nutzung von M365 durch Behörden verändern könne. Hingewiesen wird ferner auf die wachsende Abhängigkeit von schweizerischen Behörden von Microsoft.

B. Zusammenfassung der Anmerkungen

3 Ich wurde verschiedentlich gebeten, zu diesem Gutachten Stellung zu nehmen, was ich gerne tue. Zusammenfassend:

- Es ist zu begrüssen, dass sich das Gutachten mit der Frage des U.S. Behördenzugriffs auf Daten in der Cloud und der "Methode Rosenthal" vertieft auseinandersetzt und seine Standpunkte auch

---

1 Ein Cloud-Service von Microsoft, bei welchem Microsoft im Rahmen einer Auslagerung u.a. den Mailserver, Speicherlaufwerke und Videokonferenzdienste für den Kunden betreibt.

2 Stored Communications Act.

3 Übereinkommen über die Cyberkriminalität (Cybercrime Convention), SR 0.311.43.

4 Gesetz über die Information und den Datenschutz (IDG) des Kantons Zürich, 170.4.

5 Im IDG heissen sie "besondere Personendaten".

wissenschaftlich begründet. Das geschah in der öffentlichen Diskussion bisher kaum.[6]

- Die Kernaussage des Gutachtens, wonach Daten in der Cloud einem wesentlichen Kontrollverlust gegenüber den U.S. Behörden unterliegen, basiert auf verschiedenen unzutreffenden Annahmen u.a. zum U.S. Recht. Es wird zum Beispiel davon ausgegangen, dass U.S. Behörden sich ungehindert an in der Cloud gespeicherten Daten bedienen können, was nicht zutrifft. Das Gegenteil trifft zu, jedenfalls wenn wie bei M365 üblich Abwehrmassnahmen getroffen werden. Daher ist die Schlussfolgerung, wonach ein schwerer Grundrechtseingriff vorliegt, nicht haltbar.
- Das Gutachten bestätigt die Zulässigkeit des risikobasierten Ansatzes beim Gang in die Cloud und widerspricht damit der Haltung u.a. der Datenschutzbeauftragten des Kantons Zürich.
- Das Gutachten bestätigt, dass ein etwaiger Grundrechtseingriff gerechtfertigt werden kann und dass die Datensicherheit für die Wahrung der Grundrechte ebenso wichtig ist. Kann demnach ein Gang in die Cloud zu einem überwiegenden "Kontrollgewinn" in Bezug auf das Niveau der Datensicherheit führen, vermag dies einen an sich tragbaren Kontrollverlust gegenüber U.S. Behörden zu rechtfertigen.
- Die vom Gutachten empfohlene umfassende *"end-to-end"*-Verschlüsselung für sensible Daten ist jedenfalls für M365 weder geeignet noch nötig. Eine solche Verschlüsselung mag zwar den Schutz der Daten weiter erhöhen, würde jedoch die Nutzung von M365 massiv beeinträchtigen bzw. vereiteln, was selbst in Kreisen der kantonalen Datenschützer unbestritten ist. Einem U.S. Behördenzugriff lässt sich auch mit weniger einschneidenden Massnahmen erfahrungsgemäss hinreichend entgegenwirken.
- Das Gutachten bestätigt, dass die "Methode Rosenthal" aus verfassungsrechtlicher Sicht tauglich und bisher alternativlos ist, da die Empfehlungen der Datenschutzbehörden nicht sagen, wie die Risiken konkret zu beurteilen sind. Es kritisiert jedoch zurecht, dass beim Einsatz der Methode im Kanton Zürich, die in der Sache nachvollziehbar erscheint, verbindliche Kriterien für die Vornahme einer Neubeurteilung fehlen. Das Gutachten weist zurecht darauf hin, dass eine solche aufgrund steigenden Interesses der U.S. Behörden an den Daten in der Cloud eines Tages nötig werden

---

6 Zu den wenigen Ausnahmen für den öffentlich-rechtlichen Bereich gehören der Bericht der Bundeskanzlei zum rechtlichen Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung (Version 1.1) vom 26. September 2023 (https://perma.cc/SP2Q-KVMB) und die Präsentation von Patrick Seemann am Winterkongress 2023 der Digitalen Gesellschaft (https://media.ccc.de/v/dgwk2023-56049-cloud-security-2-die-publ). Ich selbst habe mich über die von mir entwickelte "Methode Rosenthal" in einem FAQ-Dokument einlässlich geäussert (https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf).

könnte. Daher erfolgt die Beurteilung jeweils nur für einen befristeten Zeitraum.

C. Fehlerhafte Annahmen

4 Das Gutachten stützt die Kernaussage des rechtlichen und faktischen Kontrollverlusts gegenüber U.S. Behörden auf Grundlagen ab, die in dieser Form unzutreffend sind:

- **Erstens** geht das Gutachten davon aus, dass die von einem Herausgabebefehl einer U.S. Behörde betroffenen U.S. Provider nur dann ein Rechtsmittel haben bzw. beschwerdelegitimiert sind, wenn ein sog. *Executive Agreement* (**EA**) zwischen den USA und der Schweiz besteht, was nicht der Fall ist.[7] Daraus folgert das Gutachten, dass U.S. Behörden sonst immer freien Zugriff auf Daten in der Microsoft Cloud haben. Das ist ein Fehlverständnis des CLOUD Act/SCA. Die in einem Gutachten des Bundesamts für Justiz[8] als Beleg genannte Stelle ist etwas unglücklich formuliert und daher offenbar missverstanden worden; sie stützt die Aussage des Gutachtens jedenfalls nicht.[9]

  Das US-Recht bietet einem U.S. Provider auch ohne EA die Möglichkeit, sich gegen solche Herausgabebefehle zu wehren. Trifft ein Cloud-Kunde die nötigen Vorkehrungen, sind Abwehrmöglichkeiten nach U.S. Recht durchaus wirksam und Microsoft ist zur Ausschöpfung des Rechtswegs verpflichtet; den Kunden braucht es hierzu nicht.[10] Genau diese Argumente werden auch in der "Methode Rosenthal" geprüft (was das Gutachten als plausibel erachtet). Das U.S. Recht sieht sogar ohne EA die Berufung auf Schweizer Recht vor (Prinzip der *International Comity*[11]), was in der Praxis bei Zugriffsversuchen von U.S. Behörden auf in der Schweiz gelegenen Daten bisher gut funktioniert hat. Herausgabebefehle und ihre

---

7 Gutachten, S. 28.

8 Bundesamt für Justiz (BJ), Bericht zum US CLOUD Act vom 17. September 2021 (https://www.bj.admin.ch/bj/de/home/publiservice/publikationen/berichte-gutachten/2021-09-17.html).

9 Im Gutachten des BJ geht es um die Folgen eines EA. Es beschreibt auf S. 7 nur ein spezifisches Rechtsmittel, das im Falle eines EA zur Verfügung stehen würde (nicht aber alle Rechtsmittel unter dem SCA), weil (nur) dieses mit dem CLOUD Act dem SCA für die Zwecke von EA hinzugefügt worden ist (CLOUD Act, § 103(b)). Ein Provider konnte sich unter dem SCA schon zuvor gestützt auf andere rechtliche Gründe gegen Herausgabebefehle wehren (nur deswegen kam es überhaupt zum CLOUD Act, wie das BJ auf S. 6 selbst schreibt) und sogar eine Verletzung ausländischen Rechts ins Feld führen, die dann nach dem Prinzip der International Comity geprüft werden müsste (vgl. dazu FN 11; das Gutachten des BJ erwähnt dies allerdings ebenfalls nicht; CLOUD Act, § 103(c), https://docs.house.gov/billsthisweek/20180319/BILLS-115SAHR1625-RCP115-66.pdf#page=2208, archiviert unter https://perma.cc/T2VY-CYYU).

10 Für weiterführende Informationen vgl. die Ausführungen in der FAQ zur "Methode Rosenthal" (https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf), dort u.a. Q31, Q35 und Q37.

11 Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa, 482 U.S. 522, 544 n.28 (1987); siehe etwa William S. Dodge, International Comity in American Law, in: Columbia Law Review, Vol. 115, No. 8, December 2015 (https://columbialawreview.org/wpcontent/uploads/2016/03/Dodge-William-S..pdf, archiviert unter https://perma.cc/A4WL-B8HU).

rechtlichen Grundlagen (wie das hier wichtige Prinzip *"possession, custody or control"*) sind im U.S. Recht kein Neuland; es existiert Erfahrung, die folglich eine vernünftige Beurteilung zulässt.[12]

Leider wird das Gutachten des BJ immer wieder missverstanden. Es befasst sich primär mit der Frage, ob die Schweiz ein EA abschliessen sollte und kommt – richtigerweise – zum Schluss, dass eben dies mit dem Schweizer Recht nicht vereinbar wäre. Es würde nämlich U.S. Behörden das Recht geben, *direkt* auf Schweizer Provider zuzugehen und sie zur Herausgabe von Kundendaten zu zwingen; die Schweiz hätte Gegenrecht. Ohne EA geht das grundsätzlich nicht.[13] Die zitierte Stelle des Gutachtens des BJ beschäftigt sich mit der Frage, welcher zusätzliche Rechtsschutz in diesen hypothetischen Sonderfällen bestehen würde. Für die Diskussion hier ist das irrelevant. Vorliegend geht es um einen anderen Aspekt des CLOUD Act.

Aufgrund eines falschen Verständnisses des U.S. Rechts (wonach U.S. Behörden auf Daten in der Cloud gewissermassen jederzeit und frei zugreifen können sollen), kommt das Gutachten verständlicherweise zu entsprechend falschen Ergebnissen. So ist die Aussage, die Speicherung von Daten in der Microsoft Cloud diene immer auch dem Zweck der Speicherung dieser Daten zwecks Bekanntgabe an die U.S. Behörden – mithin als Speicherung "auf Vorrat",[14] angesichts der technischen und rechtlichen Realität unzutreffend und unpassend: Wenn es lediglich ein theoretisches Risiko ist, dass in der Cloud gespeicherte Daten von U.S. Behörden benutzt werden können, dann ist nicht nachvollziehbar, warum die Speicherung der Daten eben diesem Zweck dienen soll. Es würde auch niemand vertreten, die Akten einer Schweizer Behörde dienten den privaten Zwecken ihrer Mitarbeiter, nur weil sie solche beschäftigt und es immer wieder welche gibt, die Informationen aus diesen Akten für persönliche Zwecke missbrauchen. Solche Missbräuche sind zudem i.d.R. wesentlich wahrscheinlicher als Zugriffe durch U.S. Behörden.

- **Zweitens** führt das Gutachten aus, ein Zugriff der U.S. Behörden auf dem Weg des CLOUD Acts/SCA sei eine Verletzung von Art. 32 CCC, welcher den Zugriff von Behörden auf Computerdaten im Ausland regelt.[15] Auch das ist ein Missverständnis.

---

12 Mit dem CLOUD Act wurde in Bezug auf Herausgabebefehle im Wesentlichen nur ein Aspekt klargestellt, der über viele Jahre unbestritten war, in einem von Microsoft provozierten Gerichtsentscheid aber in Frage gestellt worden ist, weil der Provider sich übungsgemäss gegen einen Herausgabebefehl gewehrt hatte. Der CLOUD Act wurde erlassen, um die bis dahin an sich gefestigte Praxis zu kodifizieren.

13 Siehe Q32 der FAQ zur "Methode Rosenthal" (https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf).

14 Gutachten, S. 33.

15 Gutachten, S. 29 f. und S. 34.

Art. 32 CCC regelt nur die von den Behörden *selbst* grenzüberschreitend durchgeführten Zugriffe (z.B. U.S. Staatsanwaltschaft, die Inhalte einer ausländischen Website abruft), aber nicht die Zugriffe, wie sie beim CLOUD Act/SCA (ohne EA) erfolgen, nämlich mittels Herausgabebefehl an einen *in den USA ansässigen* Provider (das ist Microsoft bei Schweizer Kunden *nota bene* nicht). Dieser Fall ist in Art. 18 Abs. 1 CCC geregelt und dort ausdrücklich vorgesehen.[16] Der CLOUD Act/SCA steht also nicht wie behauptet im Widerspruch, sondern im Gegenteil im Einklang mit der Cybercrime-Konvention, welche die Schweiz ratifiziert hat.

Das Gutachten behauptet weiter, dass der CLOUD Act mit den Grundsätzen des Schweizer Rechts "schwer vereinbar" sei und zitiert als Beispiel die Möglichkeit von Mitteilungsverboten, die Providern in den USA im Falle von Herausgabebefehlen auferlegt werden können.[17] Doch solche Mitteilungsverbote sind bei strafrechtlichen Editionsbegehren in der Schweiz nicht weniger üblich als in den USA (Art. 73 StPO).[18] Auch die Herausgabebefehle, die Schweizer Staatsanwaltschaften an Schweizer Cloud-Provider richten, sind durchaus mit solchen unter dem CLOUD Act/SCA zu vergleichen und können ebenso extraterritorial wirken, falls ein Schweizer Provider von ihm kontrollierte Server im Ausland betreibt. Die Europaratskonvention 108 zum Datenschutz sieht in Artikel 9 ausdrücklich vor, dass ein Staat unter anderem zur Verfolgung von Straftaten von gewissen Grundsätzen des Datenschutzes abweichen darf, ohne, dass dies datenschutzrechtlich als unangemessen gilt. Das Instrument des Herausgabebefehls mit Mitteilungsverbot ist mit dem europäischen Datenschutzrecht also vereinbar. Das gilt auch für den CLOUD Act/SCA, wie die Europäische Kommission dies in ihrem Angemessenheitsentscheid im Rahmen der EU-Datenschutz-Grundverordnung (**DSGVO**) kürzlich bestätigt hat.[19] Das Gutachten geht freilich nicht so weit wie einzelne kantonale Datenschutzbehörden, welche Herausgabebefehle gemäss CLOUD Act gar als *ordre public*-widrig bezeichnen,[20] weil sie die Rechtslage mit und ohne EA verwechseln.

- **Drittens** weist das Gutachten darauf hin, dass eine Auslagerung der Bearbeitung ins Ausland nur zulässig sei, wenn der betreffende Standort ein gleichwertiges (recte: angemessenes)

---

16 https://www.fedlex.admin.ch/eli/cc/2011/888/de#art_18; vgl. auch Q31 in der FAQ zur "Methode Rosenthal" unter https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf.

17 Gutachten, S. 28.

18 Das Gutachten erwähnt die auch im U.S. Recht bestehende Möglichkeit von Mitteilungsverboten (*gag orders*) als Beispiel, S. 28.

19 Entscheid der Europäischen Kommission vom 10. Juli 2023 zum EU-US Data Privacy Framework, C(2023) 4745, Erw. 203 (https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf, archiviert unter https://perma.cc/ZJT8-28BT).

20 Vgl. etwa die Datenschutzbeauftragte des Kantons Zürich, Tätigkeitsbericht 2022, https://www.datenschutz.ch/tb/2022/risiken-und-regeln.

Datenschutzniveau verfüge, was bei der Cloud eines U.S. Anbieters regelmässig nicht erfüllt ist.[21] Dies geht an der Sache vorbei: Die Auslagerung erfolgt im Falle der Microsoft Cloud für Schweizer Kunden an Microsoft Ireland Operations Ltd., d.h. eine Gesellschaft in Irland, wo ein angemessenes Datenschutzniveau besteht; aus den USA erfolgen höchstens ausnahmsweise Zugriffe und nicht zwingend auf Personendaten.[22]

Zudem wird der Bundesrat in den kommenden Monaten aller Voraussicht nach die USA wieder auf die Liste der Drittstaaten mit angemessenem Datenschutzniveau setzen für Unternehmen, die sich dem *Data Privacy Framework* verpflichtet haben, was die grossen U.S. Cloud Provider getan haben. In der EU ist dieser Schritt, wie vorstehend erwähnt, bereits erfolgt, was die datenschutzrechtliche Diskussion des Zugriffs durch U.S. Behörden dort im Wesentlichen beendet hat. Das Gutachten geht darauf nicht ein, obwohl es datenschutzrechtlich entscheidend ist; mit dem erwarteten Angemessenheitsentscheid gemäss Art. 16 Datenschutzgesetz dürfte auch hierzulande die Frage der datenschutzrechtlichen Zulässigkeit der Datenbekanntgabe in die USA (die bei M365 wie gesagt die absolute Ausnahme ist) vom Tisch sein, auch wenn der Entscheid nur auf Bundesebene unmittelbar wirkt (was bleibt, sind Fragen des Amts- und Berufsgeheimnisses; für diese wird die Eintrittswahrscheinlichkeit eines ausländischen Behördenzugriffs weiterhin beurteilt werden müssen).

- **Viertens** weist das Gutachten richtigerweise darauf hin, dass der Moment des Behördenzugriffs und die Speicherung in der Cloud zwei diskrete Eingriffsmomente darstellen,[23] übersieht jedoch die Doppelrelevanz der Berechnung der Wahrscheinlichkeit eines Behördenzugriffs. Die Speicherung von Personendaten in der Cloud stellt im Hinblick auf Behördenzugriffe überhaupt nur dann ein Problem dar, wenn damit ein Kontrollverlust (in diesem Fall gegenüber ausländischen Behörden) verbunden ist. Ist die Möglichkeit eines Behördenzugriffs lediglich theoretischer Natur, gilt dies folgerichtig auch für den Kontrollverlust. Ohne relevanten Kontrollverlust ist auch die Speicherung kein Problem.[24] Daran ändert der Verweis auf den Eingriff durch die blosse "Gefährdung" nichts: Auch sie wird sachlogisch nur und erst dann relevant, wenn sie in relevanter Weise besteht.

5 **Fazit:** Das Gutachten begründet den von ihm identifizierten "schweren Grundrechtseingriff"[25] durch die Speicherung von Daten in der Microsoft

---

21 Gutachten, S. 41.

22 Vgl. https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn.

23 Gutachten, S. 29.

24 Vgl. dazu oben unter "Erstens" die Ausführungen zur Speicherung "auf Vorrat".

25 Gutachten, S. 34.

Cloud mit verschiedenen Annahmen, die unserer Ansicht nach unzutreffend sind. Damit ist auch die Schlussfolgerung nicht mehr haltbar. Die Risikobeurteilung des Kantons Zürich, die nach Beurteilung der diversen, vorgenannten Punkte ein minimales Restrisiko eines U.S. Behördenzugriffs ausweist, erachtet das Gutachten hingegen als "plausibel".[26]

D. Risikobasierter Ansatz und Datensicherheit

6 Das Gutachten geht richtigerweise davon aus, dass selbst ein schwerer Grundrechtseingriff im Prinzip gerechtfertigt werden kann.[27] Ist das Restrisiko eines U.S. Behördenzugriffs, wie hier, nur minimal, muss das umso mehr gelten. Daraus kann weiter gefolgert werden, dass selbst im Schweizer Recht bei Grundrechtseingriffen ein risikobasierter Ansatz gilt.[28] Dieser wird von einzelnen Datenschutzbehörden bei ausländischen Behördenzugriffen pauschal abgelehnt, auch wenn sie ihn bei anderen Drittzugriffen (z.B. durch Hacker) akzeptieren.[29] Das Gutachten führt dagegen (richtigerweise) an, dass letztlich immer eine Interessenabwägung im Einzelfall nötig ist. Für die Rechtfertigung etwaiger Grundrechtseingriffe durch Cloud-Anwendungen sei entscheidend, wie die Prognose für den jeweiligen "Zugewinn an Effizienz, Sicherheit und Produktivität" ausfalle.[30]

7 Wie das Restrisiko eines U.S. Behördenzugriffs konkret gerechtfertigt werden kann, erläutert das Gutachten aber nicht. Stattdessen empfiehlt es, dem Kontrollverlust mit einer *end-to-end* Verschlüsselung für sensible Daten zu begegnen.[31] Das ist nach dem Gesagten weder nötig noch zielführend, weil der Kontrollverlust bereits mit anderen Massnahmen so stark reduziert werden kann, dass er gemäss regelmässiger Beurteilung minimal ist. M365 wäre mit einer solchen Verschlüsselung zudem nicht mehr vernünftig zu gebrauchen (siehe N 3 oben).

8 Richtiggestellt werden muss weiter die Behauptung im Gutachten, dass die lokale Speicherung von Personendaten im Vergleich zur Speicherung in der Cloud das "mildere Mittel", also sicherer sei.[32] Diese Aussage ist aufgrund der zitierten fehlerhaften Annahmen zwar verständlich. Viele Experten gehen inzwischen jedoch davon aus, dass der Einsatz von M365 einer Organisation eine deutlich höhere Datensicherheit erlaubt, als wenn sie dieselben Anwendungen lokal betreibt. Diese mittel- und

---

26 Gutachten, S. 46.

27 Gutachten, S. 34.

28 Siehe auch Gutachten, S. 37, wo vom "verbleibenden Risiko" die Rede ist, das als vertretbar erachtet wird.

29 So etwa die Datenschutzbeauftragte des Kantons Zürich, die selbst eine Zugriffswahrscheinlichkeit von 0.0001 Prozent für unzulässig hält (Thomas Schwendener, Zürcher Datenschützerin zum Cloudeinsatz: "Der Regierungsratsbeschluss ändert gar nichts", Inside IT, 30. September 2022, https://www.inside-it.ch/zuercher-datenschuetzerin-zum-cloudeinsatz-der-regierungsratsbeschluss-aendert-gar-nichts-20220930, archiviert unter https://perma.cc/NTQ9-5EBM).

30 Gutachten, S. 43.

31 Gutachten, S. 42 f.; mit "end-to-end" ist gemeint, dass der Schlüssel einzig in der Hand des öffentlichen Organs bleibt und dem Provider nie zugänglich ist.

32 Gutachten, S. 39.

langfristige Erhöhung der Datensicherheit ist für viele öffentliche Organe ein wichtiger Grund für den Gang in die Cloud. M365 bietet beispielsweise einen Schutz von Dokumenten vor unbefugten Zugriffen, selbst wenn sie in die falschen Hände gelangen (z.B. von einem Hacker gestohlen werden); "on-prem" steht das nicht zur Verfügung.[33]

9 Da selbst das Gutachten betont, dass die Gewährleistung der Datensicherheit aus grundrechtlicher Sicht ebenso wichtig ist wie die Verhinderung eines ausländischen Behördenzugriffs,[34] muss dies konsequenterweise berücksichtigt werden. Denn nicht nur Zugriffe durch ausländische Behörden stellen Grundrechtseingriffe dar, sondern ebenso Zugriffe durch Hacker, untreue Mitarbeitende und andere Angreifer. Darauf geht das Gutachten leider auch nicht ein, sondern betrachtet nur isoliert das Risiko des ausländischen Behördenzugriffs, obwohl ein Zugriff durch andere unbefugte Personen wesentlich wahrscheinlicher erscheint.

10 Für eine gesamtheitliche Beurteilung wäre das jedoch von wesentlicher Bedeutung gewesen, da bei M365 dem minimalen Kontrollverlust im Bereich von U.S. Behördenzugriffen ein deutlich höherer "Kontrollgewinn" beim Schutz vor Hackern und anderen Gefahren gegenübersteht. Das erklären uns die Experten für Informationssicherheit auch jener Klienten, die im Bereich hochsensibler Daten tätig sind, wie etwa Schweizer Banken. Wenn dem aber so ist, wird der Kontrollverlust gegenüber U.S. Behörden nicht nur gerechtfertigt, sondern er ist grundrechtlich als das "mildere Mittel" geradezu angezeigt.

E. Die "Methode Rosenthal"

11 Das Gutachten bestätigt, dass die "Methode Rosenthal" aus grundrechtlicher Sicht ihren Zweck erfüllen kann.[35] Zur Bestimmung der Wahrscheinlichkeit einer möglichen Verletzung müssten gemäss Gutachten notwendigerweise Methoden der Risikoanalyse eingesetzt, d.h. auf Elemente des Risikomanagements zurückgegriffen werden.[36] Das Gutachten hält fest, dass bisher "keine alternative Methode entwickelt wurde, die eine vergleichbar strukturierte Argumentation in Bezug auf das Risiko eines *lawful access* im Rahmen CLOUD Act/SCA ermöglicht."[37] Es hält weiter fest, dass die Leitfäden und Merkblätter der Datenschutzbehörden nicht wirklich sagen, was zur Beurteilung der Risiken genau zu tun ist.[38]

---

33 Bekannt als "Microsoft Purview Information Protection" (https://learn.microsoft.com/en-us/purview/information-protection).

34 Gutachten, S. 12, wo auch die Wahrung der Datensicherheit als "verfassungsrechtliche Garantie" bezeichnet wird.

35 Gutachten, S. 31 f.

36 Gutachten, S. 31, m.w.H.

37 Gutachten, S. 31.

38 Gutachten, S. 31.

12 Das Gutachten führt im Wesentlichen drei Vorbehalte zur Methode Rosenthal bzw. ihrer Anwendung in konkreten Fällen an:[39]

- Je nachdem, wie das Excel ausgefüllt wird, wird nicht immer klar sein, wie der Wert der Beurteilung der Begründung folgt. Das ist grundsätzlich zutreffend. Darauf ist zu achten.
- Die Qualität des Ergebnisses hängt von der Qualität der Erfahrungsdaten ab, und diese können sich ändern. Das ist im Prinzip ebenfalls zutreffend. Immerhin beinhalten die verwendeten Werte erfahrungsgemäss aus Vorsicht regelmässig Zuschläge. Die Werte basieren wiederum auf Erfahrungswerten, die das Interesse von U.S. Behörden an Daten eines Kantons reflektieren. Ein Kausalzusammenhang zwischen der Speicherung von Daten in der Cloud und dem Interesse von U.S. Behörden ist aber entgegen dahingehender Aussagen im Gutachten nicht ausgewiesen, weil das Interesse sich nicht danach richtet, wo eine Behörde die Daten gespeichert hat und die U.S. Behörden diese in den für den CLOUD Act/SCA relevanten Fällen grundsätzlich einfacher, erfolgreicher und schneller via Rechtshilfe erhalten. Der Weg über den CLOUD Act/SCA ist viel steiniger als das Gutachten aufgrund der erwähnten Missverständnisse annimmt (siehe N 4 hiervor).
- Es fehlen verbindliche Kriterien für die Vornahme einer Neubeurteilung, da die getroffenen Annahmen sich ändern können. Diese Kritik ist *i.c.* wohl zutreffend, hat aber nichts mit der Methode zu tun, sondern ist Sache des Anwenders. Die Methode selbst erfolgt für einen definierten Zeitraum; spätestens danach ist die Beurteilung zu wiederholen, wenn sich die Umstände nicht schon vorher ändern.

13 Es wird im Gutachten weiter darauf hingewiesen, dass die Methode ursprünglich entwickelt worden ist, um die Wahrnehmung von Sorgfaltspflichten und damit die Strafbarkeit von Privatpersonen zu beurteilen; im öffentlichen Bereich geht es jedoch um die Rechtmässigkeit der Erfüllung der öffentlichen Aufgabe und die Wahrung öffentlicher Interessen geht.[40] Das ändert jedoch nichts daran, dass auch im öffentlichen Bereich die Eintrittswahrscheinlichkeit eines ausländischen Behördenzugriffs oder – umgekehrt formuliert – die Wirksamkeit der Massnahmen zur Verhinderung eines solchen ermittelt werden müssen. Dies erlaubt die Methode und auch das Gutachten hält das Ergebnis für "plausibel",[41] jedenfalls was die Grössenordnung der Eintrittswahrscheinlichkeit betrifft. Welche Schlüsse daraus gezogen werden, gibt die Methode nicht vor; sie ist agnostisch.[42] Es dürfte jedoch unbestritten sein, dass auch

---

39 Gutachten, S. 32.

40 Gutachten, S. 32.

41 Gutachten, S. 46.

42 Vgl. hierzu die Erläuterungen und Hinweise im FAQ-Dokument zur "Methode Rosenthal" (https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf).

der Staat nicht in einem risikoleeren Raum agiert und es ohne die Beurteilung und Übernahme von Risiken nicht geht.

---

[i] Partner, VISCHER AG, Dozent an der ETH Zürich und Universität Basel Kontakt: drosenthal@vischer.com; Unterlagen zur "Methode Rosenthal" gibt es auf https://www.rosenthal.ch.