www.jusletter-it.eu

David Rosenthal

Eine Replik auf das «Cloud»-Gutachten

Ein von Markus Schefer und Philip Glass hier publiziertes Gutachten zum Einsatz von M365 in öffentlichen Organen sieht darin einen schweren Grundrechtseingriff, weil US-Behörden angeblich frei auf die Daten zugreifen können. In einer Replik zeigt David Rosenthal auf, warum diese Annahmen fehlerhaft sind und daher auch ihre Schlussfolgerungen unhaltbar. Einig sind sich die drei aber bei der Geltung des risikobasierten Ansatzes, der nach Rosenthal den Cloud-Einsatz auch ohne die oft verlangte, aber oft unpraktikable «end-to-end»-Verschlüsselung erlaubt, etwa weil der Gewinn an Datensicherheit etwaige Eingriffe rechtfertigt.

Beitragsart: Datenschutz
Rechtsgebiete: Datenschutz, Grundrechte, Cloud Computing

Zitiervorschlag: David Rosenthal, Eine Replik auf das «Cloud»-Gutachten, in: Jusletter IT 15. Februar 2024

Inhaltsübersicht

A. Anlass der Replik

[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] verstossen. 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[6] 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.

[3] Das Gutachten wurde am 20. Dezember 2023 im Jusletter IT publiziert und darin um ein Addendum (das **Addendum**) ergänzt. Das Addendum wurde verfasst, nachdem das Gutachten aufgrund einiger Aussagen bereits vor seiner Publikation für Gesprächsstoff und auch Kritik sorgte. Der Autor dieser Replik, dessen Methode im Gutachten direkt angesprochen ist, wurde von ver-

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».

6 Unterlagen zur «Methode Rosenthal» gibt es auf https://www.rosenthal.ch: Das entsprechende Excel zur Durchführung ist Open Source und unter https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx abrufbar, zusammen mit einer ausführlichen FAQ unter https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf.

schiedenen öffentlichen Stellen um eine Stellungnahme gebeten, die er auch abgegeben und selbst öffentlich zugänglich gemacht hat.[7] Das Addendum geht darauf und auf offenbar noch weitere Rückmeldungen ein. Allerdings vermag das Addendum die aufgeworfenen Kritikpunkte nach der hier vertretenen Auffassung nicht zu entkräften.

[4] Da einige der Aussagen im Gutachten und Addendum aus Sicht des Autors nicht unkommentiert der Lehre und Praxis überlassen werden können, hat er sich zur vorliegenden Replik im selben Medium entschlossen.[8]

[5] Eine weitere Kritik des Gutachtens ist nach der Publikation bereits von David Vasella publiziert worden.[9]

B. Zusammenfassung der Replik

[6] 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 wissenschaftlich begründet. Das geschah in der öffentlichen Diskussion bisher kaum.[10]

[7] 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.

[8] Das Gutachten bestätigt immerhin 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 auch, 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.

[9] Die vom Gutachten *de facto* 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.

---

7 https://www.rosenthal.ch/downloads/Rosenthal_Anmerkungen_Gutachten-Schefer-Glass-M365.pdf.

8 Die Replik entspricht materiell den bisherigen Anmerkungen, wurde aber aufgrund der Ausführungen im Addendum um einige weitere Entgegnungen ergänzt. Die Referenzen auf das Gutachten in den Fussnoten wurden um die Seitenzahlen in der publizierten Fassung des Gutachtens ergänzt.

9 https://datenrecht.ch/glass-schefer-gutachten-der-grundrechtskonforme-einsatz-von-m365-durch-oeffentliche-organe-in-der-schweiz/, archiviert unter https://perma.cc/2HJW-B4XY.

10 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).

Einem U.S. Behördenzugriff lässt sich auch mit weniger einschneidenden Massnahmen erfahrungsgemäss hinreichend entgegenwirken.

[10] 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 zu Recht, 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 zu Recht darauf hin, dass eine solche aufgrund steigenden Interesses der U.S. Behörden an den Daten in der Cloud eines Tages nötig werden könnte. Daher erfolgt die Beurteilung jeweils nur für einen befristeten Zeitraum.

C. Fehlerhafte Annahmen

[11] Das Gutachten stützt die Kernaussage des rechtlichen und faktischen Kontrollverlusts gegenüber U.S. Behörden auf Grundlagen ab, die in dieser Form unzutreffend sind. Hier sind vier Punkte zu beachten:

1. Missverständnis betreffend das U.S. Recht

[12] 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.[11] 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[12] als Beleg genannte Stelle ist etwas unglücklich formuliert und daher offenbar missverstanden worden; sie stützt die Aussage des Gutachtens jedenfalls nicht.[13]

[13] 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.[14] Genau diese Argumente werden auch in der «Methode Rosenthal» geprüft (was das Gutachten als plausibel erachtet). Das U.S.

11 Gutachten, S. 28 bzw. S. 33 in der publizierten Fassung.

12 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).

13 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. 15; 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).

14 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.

Recht sieht sogar ohne EA die Berufung auf Schweizer Recht vor (Prinzip der *International Comity*[15]), was in der Praxis bei Zugriffsversuchen von U.S. Behörden auf in der Schweiz gelegene Daten bisher gut funktioniert hat. Herausgabebefehle und ihre 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.[16]

[14] 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.[17] 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.

[15] 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»,[18] 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.

[16] Das Addendum geht auf diese Punkte nicht wirklich ein, ausser, dass es eine der falschen Annahmen zum U.S.-Recht wiederholt.[19] Es sagt gleichzeitig, dass das Gutachten gar nicht bestreite, dass Microsoft eine Herausgabe mit rechtlichen Mitteln verhindern kann. Begründet wird der behauptete schwere Eingriff aber damit, dass die Behörden als Kunden des Providers nicht Partei eines solchen Verfahrens nach CLOUD Act wären und über den Zugriff nicht informiert würden. Hier sei darauf hingewiesen, dass es in der Schweiz bei Beschlagnahmungen von Cloud-Providern nicht anders wäre. Ist ein etwaiges Mitteilungsverbot aufgehoben, kann und im Falle von Microsoft wird der Provider den Kunden zudem informieren, und er kann dann auch Ansprüche geltend machen.

---

15 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).

16 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.

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

18 Gutachten, S. 33 bzw. S. 40 in der publizierten Fassung.

19 Addendum, S. 61 f.

[17] Weiter wird im Addendum in Erwiderung auf den obigen Punkt argumentiert, dass auch die bloss theoretische Möglichkeit eines Zugriffs durch die U.S.-Behörden auf in der Cloud gespeicherte Daten bereits zur Folge habe, dass ihre Bearbeitung automatisch auch dem Zweck der Bearbeitung durch die U.S. Behörden dienen.[20] Diese Ansicht scheint dem Autor dieser Replik noch weiter hergeholt: Wäre dem nämlich so, müsste folgerichtig jede automatisierte Bearbeitung von Personendaten immer automatisch auch dem Zweck der Bearbeitung durch Cyberkriminelle und die bereits erwähnten untreuen Mitarbeitenden dienen, weil ja die (sogar höhere) Wahrscheinlichkeit besteht, dass auch sie darauf zugreifen, wenn die Abwehrmassnahmen versagen. Die Argumentation der angeblichen Zweckänderung erscheint allerdings eher ein Schattenboxen. Entscheidend ist einzig, dass die Wahrscheinlichkeit eines ausländischen Behördenzugriffs mit entsprechenden Massnahmen so weit reduziert werden kann, dass nicht mehr vernünftigerweise damit gerechnet werden muss. Das minimale Restrisiko kann durch die Vorteile auch aus Sicht der betroffenen Personen (wie z.B. höhere Datensicherheit) wettgemacht werden. Dass dies grundsätzlich geht, bestätigen auch die Autoren des Gutachtens (N 26).

2. Keine Verletzung der Cybercrime Convention und des Ordre Public

[18] 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.[21] Auch das ist ein Missverständnis.

[19] 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.[22] 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.

[20] Daran ändern auch die Präzisierungen im Addendum[23] nichts. Es liegt hier seitens der Autoren vermutlich ein Missverständnis darüber vor, wie Zugriffe nach dem CLOUD Act/SCA funktionieren: Der US-Staatsanwalt, welcher sich die Daten edieren lässt, «empfängt» überhaupt nichts aus der Schweiz im Sinne von Art. 32 CCC, weil die handelnde Person in den USA sitzt: Der Staatsanwalt lässt sich die Daten vom Provider in den USA herausgeben, ganz gleich, wo dieser sie physisch gespeichert hat; der Staatsanwalt wird den Datenstandort oft nicht einmal kennen. Es ist unbestritten, dass Schweizer Hoheitsrechte verletzen kann, wenn die Daten in der Schweiz liegen (was gerade eine der Rechtsgrundlagen ist, um solche Zugriffe abzuwehren). Das hat aber nichts mit Art. 32 CCC zu tun.[24] Die vom Addendum zitierte Stelle der Botschaft zur

20 Addendum, S. 63.

21 Gutachten, S. 29 f. und S. 34 bzw. S. 35 und S. 40 f.

22 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.

23 Addendum, S. 63 f.

24 Weil sich die Vertragsparteien bei Art. 32 CCC nicht einigen konnten, was sonst noch zulässig oder verboten sein soll, hielten sie in Art. 39 Abs. 3 CCC fest, dass von der Konvention nicht adressierte Fälle von ihr weder erlaubt noch verboten sind. Vgl. hierzu die CoE Explanatory Report to the Convention on Cybercrime, European Treaty Series No. 185, Budapest 23.11.2001, S. 53.

CCC hält selbst fest: «Die rechtmässige Befugnis der Person, über die Daten zu verfügen und sie an eine staatliche Stelle weiterzuleiten, beurteilt sich primär nach dem nationalen Recht des Staates, in welchem die betreffende Person handelt.»[25] Dies ist hier das U.S. Recht, und für dieses gilt Art. 18 CCC, dessen U.S. Implementierung übrigens die vom Addendum geforderten prozessualen Regelungen und Rechtsgrundlagen aufweist. Weil sich die Vertragsparteien bei Art. 32 CCC nicht einigen konnten, was darüber hinaus zulässig oder verboten sein sollte, hielten sie in Art. 39 Abs. 3 CCC fest, dass von der Konvention nicht adressierte Fälle von ihr weder erlaubt noch verboten sind.[26]

[21] 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.[27] Doch solche Mitteilungsverbote sind bei strafrechtlichen Editionsbegehren in der Schweiz nicht weniger üblich als in den USA (Art. 73 StPO).[28] 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.[29] Das Gutachten geht freilich nicht so weit wie einzelne kantonale Datenschutzbehörden, welche Herausgabebefehle gemäss CLOUD Act gar als *ordre public*-widrig bezeichnen,[30] weil sie die Rechtslage mit und ohne EA verwechseln.

3. Ein Angemessenheitsbeschluss für die U.S.A. steht kurz bevor

[22] Drittens weist das Gutachten darauf hin, dass eine Auslagerung der Bearbeitung ins Ausland nur zulässig sei, wenn der betreffende Standort ein gleichwertiges (recte: angemessenes) Datenschutzniveau verfüge, was bei der Cloud eines U.S. Anbieters regelmässig nicht erfüllt ist.[31] 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 angemes-

25 Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18. Juni 2010, BBl 2010 4697, 4738.

26 CoE Explanatory Report to the Convention on Cybercrime, European Treaty Series No. 185, Budapest 23.11.2001, S. 53.

27 Gutachten, S. 28 bzw. S. 33 f. in der publizierten Fassung.

28 Das Gutachten erwähnt die auch im U.S. Recht bestehende Möglichkeit von Mitteilungsverboten (*gag orders*) als Beispiel, S. 28 bzw. S. 33 f. in der publizierten Fassung.

29 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).

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

31 Gutachten, S. 41 bzw. S. 50 in der publizierten Fassung.

senes Datenschutzniveau besteht; aus den USA erfolgen höchstens ausnahmsweise Zugriffe und nicht zwingend auf Personendaten.[32]

[23] 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).

4. Der theoretische Zugriff ist noch kein tatsächlicher

[24] Viertens weist das Gutachten richtigerweise darauf hin, dass der Moment des Behördenzugriffs und die Speicherung in der Cloud zwei diskrete Eingriffsmomente darstellen,[33] 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.[34] 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

[25] Das Gutachten begründet den von ihm identifizierten «schweren Grundrechtseingriff»[35] durch die Speicherung von Daten in der Microsoft 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».[36]Der sich daraus ergebende Widerspruch zu den eigenen Aussagen des Gutachtens zum U.S. Recht vermag auch das Addendum nicht aufzulösen. Dass es für die Annahme eines schweren Grundrechtseingriffs scheinbar gar nicht darauf ankommen soll, ob ein U.S.

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

33 Gutachten, S. 29 bzw. S. 34 f. in der publizierten Fassung.

34 Vgl. dazu oben unter «Erstens» die Ausführungen zur Speicherung «auf Vorrat».

35 Gutachten, S. 34 bzw. S. 41 in der publizierten Fassung.

36 Gutachten, S. 46 bzw. S. 57 in der publizierten Fassung.

Behördenzugriff ein echtes oder ein nur theoretisches Risiko darstellt, leuchtet jedenfalls nicht ein. Es passt dies auch nicht zum risikobasierten Ansatz, den selbst das Gutachten vertritt (dazu sogleich).

D. Risikobasierter Ansatz und Datensicherheit

[26] Das Gutachten geht richtigerweise davon aus, dass selbst ein schwerer Grundrechtseingriff im Prinzip gerechtfertigt werden kann.[37] 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.[38] Dieser wird von einzelnen Datenschutzbehörden bei ausländischen Behördenzugriffen pauschal abgelehnt, auch wenn sie ihn bei anderen Drittzugriffen (z.B. durch Hacker) akzeptieren.[39] 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.[40]

[27] Wie das Restrisiko eines U.S. Behördenzugriffs konkret gerechtfertigt werden kann, erläutert das Gutachten aber nicht. Stattdessen legt es nahe, dem Kontrollverlust mit einer *end-to-end* Verschlüsselung für sensible Daten zu begegnen.[41] 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.

[28] M365 wäre mit einer solchen End-to-End-Verschlüsselung zudem nicht mehr vernünftig zu gebrauchen (siehe bereits N 3 oben). Wird beispielsweise das sog. *Double-Key-Encryption* (**DKE**) Verfahren von Microsoft eingesetzt, so ist der zur Entschlüsselung nötige Schlüssel nicht mehr in der Hand von Microsoft. Diverse Funktionalitäten von M365 stehen dann aber nicht mehr zur Verfügung, zum Beispiel Malware-Scanner, Suchfunktionen und das sog. eDiscovery, also Zugriffe, wie sie bei internen oder externen Untersuchungen nötig werden.[42] In der Praxis wird DKE daher so gut wie nie eingesetzt oder wenn, dann nur für eine möglichst geringe Anzahl von Dokumenten. Hinzu kommt, dass bei DKE der Kunde sich selbst um den Schlüssel kümmern muss, was für die meisten Organisationen eine zu grosse Herausforderung sein dürfte. Sie sind also abermals auf einen Dritten angewiesen, der den Schlüssel für sie verwaltet. Auch für die meisten Gemeinwesen (Gemeinden, manche Kantone) wird es also illusorisch oder zumindest problematisch sein, den Schlüssel selbst bei sich zu verwalten, und selbst dann sind noch Angriffsszenarien

37 Gutachten, S. 34 bzw. S. 41 in der publizierten Fassung.

38 Siehe auch Gutachten, S. 37 bzw. S. 45 in der Publikation, wo vom «verbleibenden Risiko» die Rede ist, das als vertretbar erachtet wird.

39 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).

40 Gutachten, S. 43 bzw. S. 53 in der publizierten Fassung.

41 Gutachten, S. 42 f. bzw. S. 53 in der Publikation; mit «end-to-end» ist gemeint, dass der Schlüssel einzig in der Hand des öffentlichen Organs bleibt und dem Provider nie zugänglich ist.

42 https://learn.microsoft.com/en-us/purview/double-key-encryption.

auf den Schlüssel denkbar. Auch für den Verkehr mit Dritten – die Verwaltung will ja nicht nur intern E-Mails versenden – sind Verfahren wie DKE nicht wirklich praxisnah.

[29] Die Autoren des Gutachtens halten in ihrem Addendum fest, dass sie gar nicht bestreiten, eine End-to-End-Verschlüsselung praxisfern und unnötig sei.[43] Sie betonen, auch sie würden keine solche Verschlüsselung fordern, sondern lediglich darauf hinweisen, dass damit der Personenbezug aufgehoben und die Kontrolle vollständig beim Staat bleibe, was natürlich zutrifft. Es bleibt also zu hoffen, dass die einzelnen Datenschutzbehörden, die derzeit noch eine End-to-End-Verschlüsselung fordern, einsehen, dass dies nicht zielführend ist.

[30] In der Praxis werden die Schlüssel zur Entschlüsselung der Daten praktisch immer in der Umgebung von Microsoft gespeichert. Unterschiedlich weit gehen die Kunden, was die Schlüsselverwaltung und die Ebene der Verschlüsselung betrifft. So ist es durchaus möglich, die Schlüssel zwar physisch bei Microsoft gespeichert zu haben, dies jedoch in einem Schlüsseltresor, den nur der Kunde bedienen kann; allerdings lastet dann auch wieder die Verantwortung auf ihm, was in der Vergangenheit bereits zu einigen Totalverlusten aller Daten geführt hat. Darum sieht Microsoft inzwischen vor, dass ein Zweitschlüssel für den Notfall bei ihr hinterlegt ist (der «Availability Key»). Aus rechtlicher Sicht und dem CLOUD Act ist das nicht entscheidend, sondern unter anderem welchen Zugriff Microsoft rechtlich und im Tagesgeschäft hat: Dieser wird in der Praxis nebst Funktionen wie die «Customer Lockbox» durch eine Verschlüsselung der ruhenden Daten auf Benutzer- oder neu auch Service-Ebene so weit wie möglich eingeschränkt. Ohne einen Schlüssel bei Microsoft geht es allerdings auch in diesen Fällen nicht.

[31] Dies genügt womöglich auch nach Ansicht der Autoren. Denn im Addendum argumentieren sie, dass selbst im Kontext des CLOUD Act/SCA eine Verschlüsselung keinen 100%igen Schutz gewährleisten muss, sondern es genügt, dass der Aufwand für eine Entschlüsselung gross genug ist, dass nicht damit gerechnet werden muss, dass die Dritten (hier: Microsoft, U.S. Behörden) den für eine Entschlüsselung erforderlichen Aufwand auf sich nehmen.[44] Es genügt somit, dass die Wahrscheinlichkeit hinreichend gering ist. Damit sind wir wieder bei der «Methode Rosenthal» (dazu nachfolgend).

[32] 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.[45] 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 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).[46]

43 Addendum, S. 62.

44 Addendum, S. 63.

45 Gutachten, S. 39 bzw. S. 49 in der publizierten Fassung.

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

[33] Da selbst das Gutachten betont, dass die Gewährleistung der Datensicherheit aus grundrechtlicher Sicht ebenso wichtig ist wie die Verhinderung eines ausländischen Behördenzugriffs,[47] 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.

[34] 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»

[35] Das Gutachten bestätigt, dass die «Methode Rosenthal» aus grundrechtlicher Sicht ihren Zweck erfüllen kann.[48] Zur Bestimmung der Wahrscheinlichkeit einer möglichen Verletzung müssten gemäss Gutachten notwendigerweise Methoden der Risikoanalyse eingesetzt, d.h. auf Elemente des Risikomanagements zurückgegriffen werden.[49] 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.»[50] Es hält weiter fest, dass die Leitfäden und Merkblätter der Datenschutzbehörden nicht wirklich sagen, was zur Beurteilung der Risiken genau zu tun ist.[51]

[36] Das Gutachten führt im Wesentlichen drei Vorbehalte zur Methode Rosenthal bzw. ihrer Anwendung in konkreten Fällen an:[52]

- 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 Behör-

47 Gutachten, S. 12 bzw. ebenfalls S. 12 in der Publikation, wo auch die Wahrung der Datensicherheit als «verfassungsrechtliche Garantie» bezeichnet wird.

48 Gutachten, S. 31 f. bzw. S. 37 ff. in der publizierten Fassung.

49 Gutachten, S. 31, m.w.H. bzw. S. 37 in der publizierten Fassung.

50 Gutachten, S. 31 bzw. S. 37 f. in der publizierten Fassung.

51 Gutachten, S. 31 bzw. S. 37 f. in der publizierten Fassung.

52 Gutachten, S. 32 bzw. S. 38 f. in der publizierten Fassung.

de 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 11 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.

Die Autoren des Gutachtens schliessen, dass, auch wenn die Methode für die Verwendung im öffentlich-rechtlichen Bereich als noch nicht genügend ausgereift erscheint, sie «doch gewisse Aussagen über die Grössenordnung der Wahrscheinlichkeit einer Verletzung zu liefern» vermag.[53]

[37] 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.[54] 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»,[55] jedenfalls was die Grössenordnung der Eintrittswahrscheinlichkeit betrifft. Welche Schlüsse daraus gezogen werden, gibt die Methode nicht vor; sie ist agnostisch.[56] Es dürfte jedoch unbestritten sein, dass auch der Staat nicht in einem risikoleeren Raum agiert und es ohne die Beurteilung und Übernahme von Risiken nicht geht.

David Rosenthal, Partner, VISCHER AG, Dozent an der ETH Zürich und Universität Basel.

53 Gutachten, S. 45 f. bzw. S. 57 in der publizierten Fassung.

54 Gutachten, S. 32 bzw. S. 39 in der publizierten Fassung.

55 Gutachten, S. 46 bzw. S. 57 in der publizierten Fassung.

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